D.K.M. COLLEGE FOR WOMEN

(AUTONOMOUS), VELLORE

eRESOURCES

Digital Learning

E CONTENT TITLE : ALGEBRA

DEPARTMENT : MATHEMATICS -PG

DESIGNED BY :

1. Mrs. G.Chithra, M.Phil,
2. Ms. K. Geetha Priya, M.Phil,
3. Mrs. R. Ramya, M.Phil,
4. Mrs.D. Vijayalakshmi, M.Phil,
5. Mrs. C. Revathi, M. Phil,
6. Ms. R. Chithra, M.Phil,
7. Mrs.V. Vandar Kuzhali, M.Phil,
8. Dr. M. Kathuri, Ph.D
9. Dr. T. Ranjani, Ph.D
10. Dr. M. Devi, Ph.D

ALGEBRA - I

UNIT - I - GROUP THEORY 18hrs

Another Counting Principle –Class Equation for Finite groups and its applications – Sylow's theorems [For theorem 2.12.1, Only First proof].

Chapter 2: Sections 2.11 and 2.12 [omit Lemma 2.11.3, 2.12.2, 2.12.5]

2.11 ANOTHER COUNTING PRINCIPLE

Definition:

Let G be a group and if a, b ∈ G then b is said to be ***conjugate*** to a in G, there exists an element c $\in G$ such that b = $c^{-1}ac$. Symbolically a ∼ c.

Lemma 2.11.1:

The above relation is an equivalence relation.

Or

Conjugacy is an equivalence relation on G.

Proof:

Now we have to prove that the above relation is an equivalence relation.

That is to prove that

i). Reflexive: a ∼ a

ii). Symmetric: a ∼ b → b ∼ a

iii). Transitive: a ∼ b, b ∼ c → a ∼ c

i). Reflexive:

Since e ∈ G, a = $e^{-1}ae$

Therefore a $\in G$.

Hence $a \sim a$

ii). Symmetric:

Let $a \sim b$.

Then $b = c^{-1}ac$.

Now $cbc^{-1} = b = c^{-1}cac\, c^{-1}$

$= e\, a\, e = a$

Therefore $b \sim a$.

iii). Transitive:

Let $a \sim b$ and $b \sim c$.

Then there exists an element $x \in G$ such that $b = x^{-1}ax$ and also there exists an element $y \in G$ such that $c = y^{-1}ay$.

Now $c = y^{-1}ay$

$= y^{-1} (x^{-1}ax) y$

$= (y^{-1}x^{-1})a (x y)$

$= (xy)^{-1} a (xy)$

$= z^{-1}a z$

Therefore, $a \sim c$.

Hence the conjugacy relation is an equivalence relation.

Hence the lemma.

Definition:

Let a in G. Then $C(a) = \{ x \in G / x \sim a \}=\{ x \in G / x = y^{-1}ay, y \in G\}$ where C(a) is called the **conjugate class of a**.

Definition:

If a in G then N(a) is the **normalize of a in G** such that N(a) = { $x \in G$ / ax = xa }.

Lemma 2.11.2

Prove that N(a) is a sub group of G.

Proof:

Given that g is a group.

To prove that N(a) is a subgroup of G.

It is enough to prove that N(a) satisfies

i). Closure

ii). Associative

By definition of N(a), N(a) is a subset of G.

Since e and a in G, ae = ea

Hence $e \in N(a)$.

Therefore, N(a) is non-empty.

Now to prove closure:

Let $x, y \in N(a)$.

Then xa = ax and ya = ay.

Consider,

$$
\begin{aligned}
(xy)a &= x(ya) \\
&= x(ay) \\
&= (xa)\, y
\end{aligned}
$$

$= (ax)y$

That is, $(xy)a = a(xy)$

Therefore, $xy \in N(a)$.

Closure is satisfied.

Now to prove the inverse:

Let $x \in N(a)$.

Then $xa = ax$.

Consider

$x^{-1} a = (x^{-1}a)(xx^{-1})$

$= ax^{-1}$

Hence $x^{-1} \in N(a)$.

Thus inverse is satisfied.

Therefore N(a) is a subgroup of G.

Hence the lemma proved.

Theorem 2.11.1 SECOND COUNTING PRINCIPLE

If G is a finite group, then $c_a = O(G) / O(N(a))$; in other words, the number of elements conjugate to a in G is the index of normalize of a in G.

Proof:

For $a \in G$, $c(a) = \{ x \in G / x \sim a \}$

$= \{ x \in G / x = y^{-1}ay, y \in G \}$

Therefore c(a) consist exactly of all the elements $x^{-1}ax$ as x ranges over G.

Hence c_a measures the number of distinct $x^{-1}ax$'s.

Now to show that two elements in the same right coset of N(a) in G yield the same conjugate of a whereas two elements in different right cosets of N(a) in G give rise to different conjugates of a.

In this way we shall prove that there exists a one-to-one correspondence between conjugates of a and right cosets of N(a).

Suppose that x, y $\in$ G are in the same right coset of N(a) in G.

thus y = nx where n $\in$ N(a).

So na = an.

Therefore, since $y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$, $y^{-1}ay = x^{-1}n^{-1}anx = x^{-1}ax$.

Thus we proved that two elements in the same right coset of N(a) in G yield the same conjugate of a.

On the other hand, x and y are in different cosets of N(a) in G.

We claim that $x^{-1}ax \neq y^{-1}ay$.

Let us assume that $x^{-1}ax = y^{-1}ay$.

Then x $\in$N(a) x and y $\in$ N(a) y

Now $x^{-1}ax = y^{-1}ay$.

Pre-multiply by x and post multiply by y^{-1} we get,

N(a)x = N(a) y,which is a contradiction.

Hence two elements in different right cosets of N(a) in G give rise to different conjugates of a.

Thus we proved that one-to-one correspondence between conjugates of a and right cosets of N(a).

Therefore $c_a = \frac{O(G)}{O(N(a))}$.

Hence the theorem.

Corollary: CLASS EQUATION OF G

$$O(G) = \sum \frac{O(G)}{O(N(a))}$$

where this sum runs over one element a in each conjugate class.

Proof:

By applying theorem 2.11.1, we have

$O(G) = \sum \frac{O(G)}{O(N(a))}$

Now consider c_a, c_b, ….. are distinct conjugate classes and also $c_a \cup c_b \cup$ …. = G.

Therefore, $\sum c_a$ = O(G).

Hence the equation $O(G) = \sum \frac{O(G)}{O(N(a))}$.

Hence the corollary was proved.

Sub Lemma 1:

Prove that a ∈ Z if and only if N(a) = G. If G is finite, a ∈ Z and only if O(N(a)) = O(G).

Proof:

Necessary Part:

Let a in Z(G).

To prove that N(a) = G.

By definition of N(a), N(a) is a subset of G.

By lemma 2.11.1, N(a) is a subgroup of G.

That is N(a) $\underline{C}$ G ………………………………….. (1)

Now to show that G $\underline{C}$ N(a).

Let g in G.

Then ag = ga.

Therefore g is in N(a).

Hence G $\underline{C}$ N(a) ……………………………………(2)

From equation (1) and (2), G = N(a).

Sufficient Part:

Let G = N(a).

To prove that a in Z(G).

Let x in G.

Then xa = ax.

Hence a in Z(G).

Let G be a finite group.

Let a in Z(G).

Then N(a) = G.

Hence O(N(a)) = O(G).

Hence the lemma was proved.

Theorem 2.11.2

If O(G) = p^n where p is a prime number then Z(G) $\neq$ (e).

Proof:

Let G be a finite group.

given that O(G) = p^n where p is a prime number.

To prove that Z(G) $\neq$ (e).

Let a in G.

Since N(a) is a subgroup of G and G is a finite group then by Langrange's theorem $\frac{O(G)}{O(N(a))}$

Hence $\frac{p^n}{O(N(a))}$.

That is O(N(a)) = p^{na}, where $1 \leq a \leq$ n.

If a is not in centre of G then by sub lemma 1 O(N(a)) = O(G).

Therefore $p^n = p^{na}$.

Hence n = na.

If a in Z(G) then na < n.

Consider the class equation

O(G) $\quad = \sum \frac{O(G)}{O(N(a))}$.

$= \sum_{a\ in\ Z(G)} \frac{O(G)}{O(N(a))} + \sum_{a\ not\ in\ Z(G)} \frac{O(G)}{O(N(a))}$

$= \frac{p^n}{p^{na}} + \sum_{a\ not\ in\ Z(G)} \frac{O(G)}{O(N(a))}$

= z + $\sum_{a\ not\ in\ Z(G)} \frac{O(G)}{O(N(a))}$

$p^n \quad$ = z + $\sum_{n<na} \frac{p^n}{p^{na}}$

z = p^n - $\sum_{n<na} \frac{p^n}{p^{na}}$ ………………………………………(1)

p divides the R.H.S of (1).

p divides the L.H.S of (1).

Therefore p divides z, which gives p is either 0 or integral power of p.

Hence z is not equal to 0.

Therefore z must be a integral power of p.

Hence Z(G) ≠ (e).

Corollary:

If O(G) $= p^2$ where p is a prime number then G is abelian.

Proof:

Suppose O(G) $= p^2$ where p is a prime number

Now to prove that G is abelian.

It is enough to prove that G = Z(G) is abelian, where Z(G) = { x in G such that ax = xa for all x in G }.

Since G is a finite group and Z(G) is a subgroup of G then by Lagrange's theorem, $\frac{O(G)}{O(Z(G))}$

That is, $\frac{p^2}{O(Z(G))}$ ……………………………………….(1)

that is O(Z(G)) = 1 or p or p^2.

By theorem 2.11.2, Z(G) ≠ (e).

That is, O(Z(G) ≠1.

Hence the possibilities are either p or p^2.

Suppose O(Z(G) = p.

Then there exists an element a in G but not in Z(G).

Since N(a) is a subgroup of G and G is a finite group again by lagrange's theorem $\frac{O(G)}{O(N(a))}$

That is $\frac{p^2}{O(N(a))}$.

Hence O(N(a)) = 1 or p or p^2

Since N(a) is a subgroup of G, a and e in N(a) we have O(N(a)) $\neq$1.

Thus either O(Na)) = p or p^2

let z in Z(G).

Then az = za for all a in G.

Hence Z(G) is a subset of N(a).

Since a in N(a) and Z(G) is not equal to N(a) we have O(N(a)) $\neq$ p^2.

Therefore O(N(a)) = O(G)

Hence a is in Z(G), which is a contradiction to our assumption that a does not belong to Z(G).

Therefore Z(G) = G.

Thus G is abelian.

Example 2.11.1

A group of order 121 is an abelian group.

Solution:

Let O(G) = 121 = 11^2.

By using above corollary, a group of order 121 is an abelian group.

Theorem 2.11.3 CAUCHY

If p is a prime number and p| O(G) then G has an element of order p.

Proof:

Suppose G is a finite group and p| O(G), where p is a prime number.

To prove G has an element of order p.

To prove that there exists an element a ≠ e ∈ G such that $a^p = e$.

That is to prove that O(a) = p.

We prove this theorem by induction on O(G).

Let O(G) = 1.

Therefore O(G) = {e} and e^1 = e.

Thus O(e) = 1.

Hence the theorem is true for O(G) = 1.

Assume that the theorem is true for all group of order is less than q.

Now we prove the theorem for O(G).

Then there exists a subgroup H which is not equal to G such that p divides O(H).

Hence the theorem is true for H because O(H) < OG).

Therefore O(a) = p.

Since a is in H, a is also in G, there exists an element a is in G such that O(a) = p..

Thus we may assume that p is not a divisor of any proper subgroup of G.

Let Z(G) be the centre of G.

Consider the class equation

O(G) $= \sum \frac{O(G)}{O(N(a))}$.

$= \sum_{a\ in\ Z(G)} \frac{O(G)}{O(N(a))} + \sum_{a\ not\ \ in\ Z(G)} \frac{O(G)}{O(N(a))}$

= O(Z(G)) + $\sum_{a\ not\ \ in\ Z(G)} \frac{O(G)}{O(N(a))}$

$O(Z(G)) = O(G) - \sum_{a \ not \ in \ Z(G)} \frac{O(G)}{O(N(a))}$

Hence p divides O(Z(G)).

Thus Z(G) is a subgroup of G whose order is divisible by p.

But we may assume that p does not divide any proper subgroup of G.

Hence Z(G) = G.

Since Z is an abelian nd G is also an abelian group.

Therefore by applying Cauchy theorem for abelian group, the theorem is true for O(G).

Thus G has an element of order p.

Lemma 2.11.3

The number of conjugate classes in S_n, is p(n), the number of partitions of n.

Proof:

Let the permutation be (1 2) in S_n. There are (n - 2)!

Also (1, 2) commutes with itself.

This way we get 2(n-2)! elements in the group generated by (1 2) and the n(n-1)/2 transpositions and these are conjugates of (1,2).

By counting principle

$\frac{n(n-1)}{2} = \frac{O(S_n)}{r} = \frac{n\,!}{r}$

Thus r = 2(n-2)!.

That is the order of the normalize of (1,2) is 2(n-2).

Now any n-cycle is conjugate to (1,2,…n) and there are (n-1)! distinct n-cycles in S_n.

Thus if u denotes the order of the normalize of(1,2,..n) in S_n, $O(S_n)$ / u = number of conjugates of (1,2,…n) in S_n = (n-1)!

Therefore u = $\frac{n!}{(n-1)!}$ = n.

Hence the order of the normalize of (1,2,…n) in S_n is n.

The powers of (1,2,…n) having given as n such elements.

Hence the lemma was proved.

Theorem 2.12.1 First part of Sylow's Theorem

If P is a prime number and $P^\alpha|O(G)$ then G has a subgroup of order P^α.

Proof:

Given P is a prime number and $P^\alpha|O(G)$

==> $O(G) = P^\alpha m$

We know that, nC_k = n!

k!(n−k)! ---------(1)

Let $n = P^\alpha m$

Where P is a prime number and if $P^\alpha|m$ but $P^\alpha\nmid m$

Take $k = P^\alpha$ substitute this in (1)

We get, $P^\alpha mCP^\alpha = {}^{P\alpha}m!$

$P^\alpha!(P^\alpha m-P^\alpha)!$

$= P^\alpha (P^\alpha m-_1) (P^\alpha m-_2)............(P^\alpha m-_1).....(P^\alpha m-P^\alpha+1)$

$P^\alpha(P^\alpha-1)..........(P^\alpha-i)......(P^\alpha m-P^\alpha+1)$

$= P^\alpha m (P^\alpha m-1)..........(P^\alpha m-1).......(P^\alpha m-P^\alpha+1) P^\alpha(P^\alpha-1)......(P^\alpha-i)$......3.2.1

Now, we show that the power of P dividing (P^α m-i) in the numerator is the same as the power of P dividing $(P^\alpha{}_{m-i})$ in the denominator.

Let $P^\alpha(P^\alpha-1)$ -----------(2)

==>$P^\alpha-i = aP^k$ where $k\leq\alpha$

==> $-i = aP^k-P^\alpha$

Add both sides by $P^\alpha m$,

We get,

$P^{\alpha}m-i = aP^{k}-P^{k}+P^{\alpha}m$

$= aP^{k}+P^{\alpha}(m-1)$

$P^{\alpha}m-i= P^{k}[a+P^{\alpha-k}(m-1)]$

$==> P^{k}|P^{\alpha}m-i$

Conversely,

Let P^{k} divides $P^{\alpha}m-i$

$==>P^{\alpha}m-1 = aP^{k}=P^{\alpha}-i$

$==>aP^{k} = P^{\alpha}-i$

$==>P^{k}|P^{\alpha}-i$

Hence, all the powers of P cancel out except the power which divides m.

Thus, $P^{r}|P^{\alpha}mCP^{\alpha}$ but $P^{r+1}\nmid P^{\alpha}mCP^{\alpha}$.

Let M be the set of all subsets of G which have P^{α} elements.

Thus, M has $P^{\alpha}mC_{P}\alpha$ elements. Given M_1, $M_2 \in$ M. Since M is a subset of G having P^{α} elements on likewise M_1 define $M_{1\sim}M2$, if there exist an element g∈g such that m1=m2g. Now To prove the relation, 'M' is an equivalence relation on M,

1)Reflexive:

Since $M_{1=M1e}$ $\therefore M_1=M_2$.

2)Symmetric:

Let M_1~M_2 then $M_1=_{M2g}$ where g∈G

$\therefore M_1g_1 = M_2$

$\therefore$there exist g^{-1}∈G such that $M_{2=M2g}$-1 M_2~M_1

3. **Transitive:**

Let M_1~M_2 and M_2~M_3 $\therefore$There exist g_1∈G such that $M_1=M_2g_1$ and g1∈G such that $M_{2\ =M3g2}$ =M3

$M3g2g1 = M_{3(g2g1)} = M3g$ ∴M1~M3 Hence the relation '~' is an equivalence relation.

We claim that there is atleast on equivalent class of M such that the

number of elements in the class is not a multiple of P^{r+1} for if P^{r+1} is a divisor of

the size of each equivalence class then P^{r+1} is also a divisor of the number of

elements in M, which is not possible.

Since M has $P^{\alpha}mCP^{\alpha}$ elements and $P^{r+1} \nmid P^{\alpha}mCP^{\alpha}$ Let $\{M_1, M_2.....M n\}$ be such an equivalence class in M where Pr+1 does not divide n.

By our definition of equivalence class in M, g∈G for each i=1,2,....n

$M_{ig} = M_i$ for some j, $1 \leq j \leq n$

Let H={g∈G/M1g=M1}

Since g∈G, H is a subset of G

To prove: H is a subgroup of G

∴e∈H

Hence H is non-empty.

Let $g_{1,g2 \in H}$ Then $_{M1g1}$=M1 and $_{M1g2}$=M1

Now, $M_1(_{g1g2})$ = M1g1)g2 = M_{1g2} = M1

∴g1g2∈H

∴ Closure is satisfied.

Let g∈H then $_{M1g}$=M1

==>$M_{1\ =\ M1g}$-1

==>g^{-1}∈H

∴Inverse is also satisfied.

Hence H is a subgroup of G.

Now we show that there exist a one-one correspondence between the

equivalence class $\{M_1, M_2, ...Mn\}$ and the set of all right cosets of H in $G=\{H_{g/g\in H\}}$.

Let $M_{1g1=M2g2}$

$<==>_{M1g1g2}{}^{-1}=M_2$

$<==>g_{1g2}\text{-}1_{\in H}$

$<==>Hg1g2^{-1}=H <==>Hg_{1=Hg2}$

∴There exists a one-one correspondence between

thequivalence class and the set of all right coset of H in G.

Hence G is a finite group and H is a subgroup of G.

Then by Lagrange's theorem, o(G) 0(H)

Again, by using 2nd counting principle o(G)

0(H) = the number of distinct right cosets

of H in G.

Here the number of elements in the equivalence class in n,

i.e, $o(G)\ 0(H)^{=}\ n$

i.e, o(G)=n0(H)

$P^{r+1} \nmid P^{\alpha} m C_{P}\alpha$ and $P r+1_{\nmid n}$

i.e, $P^{r+1} \nmid n0(H)$

It follows that $P^{\alpha} | 0(H)$

$==>0(H)\geq P^{\alpha}$------------(3)

Let if $m_1 \in M_1$ and ∀ h∈H Then $m_{1h\in H}$ Thus, M_1 has atleast order of H distinct element. However

M_1 is a subset containing P^{α} elements $P^{\alpha}\geq 0(H)$-----------(4)

From equation (3) & (4)

$P^{\alpha}= 0(H)$

Hence, H is a subgroup of G having P^{α} elements.

Hence the proof.

COROLLARY:

If $p^m/o(G)$ and $p^{m+1}/o(G)$ then G has a subgroup of order p^m.

Proof:

Suppose $p^m/o(G)$ $p^{m+1}/o(G)$

To prove : G has a subgroup of order p^m.

By using first part of sylow's theorem

We get a subgroup of order p^m.

Definition:

Let n(k) be defined by $p^{(k)}/p^{(k)}!$ but $p^{n(k+1)}/p^{(k)}!$.

Definition :

subgroup of G of order p^m where $p^m/o(G)$ but $p^{m+1}/o(G)$ is called a p sylow subgroup of G.

Lemma 2.12.1

Prove that $n(k) = 1+p+\ldots\ldots.+ p^{k-1}$

Proof:

By the define of n(k), $p^{n(k)}/ p^{(k)}$, but $P^{n(k)+1}/p^{(k)}!$

We know that

$P! = 1.2\ldots\ldots..(p-1)p$

Hence $p/p!$ but $p^2 /p!$ if k=1 then $n(1) = 1$

Now $p^{(k)} ! = 1.2\ldots..2p\ldots.3p\ldots..p^{k-1}.p$

It is the expansion of $p^{(k)}!$

It is also the multiplies of p.

Hence the powers of p dividing $p^{(k)}!$

N(k) must be the powers of p which divides $(p) (2p) (3p)\ldots\ldots(p^{k-1}.p)$.

(i.e) $(p) (2p) (3p)\ldots\ldots.. (p^{k-1}.p) = p^{i(k-1)}(p^{k-1}j)!$

But $n(k) = n(k-1) + p^{k-1}$

& also $n(k-1) – n(k-2) = p^{k-2}$

$N(k-2) – n(k-3) = p^{k-3}$

$n(2) – n(1) = p^{-1}$ (i.e) $n(1) =1$.

Adding these we get

$n(k) = p^{k-1} + p^{k-2} + …….+ 1$ (i.e) $n(k) = 1 + p + ……..+p^{k-1}$

Hence the Lamma.

Lemma 2.12.2

$S_p{}^k$ has a p-sylow subgroup

proof:

If k=1 , then the element (1 2 ….p), is s_p is of order p, so generated a subgroup of order p.

since n(1)=1, suppose that the result is correct for k-1

we show that,it that must follow for k.Divide the integers $1,2,….,p^k$ into p.

$\{1,2,….,p^{k-1}\},\{p^{k-1}+1,p^{k-1}+2,….,2p^{k-1}\},….\{(p-1)p^{k-1} +1,…p^k\}$,

The permutation σ defined by $\sigma =(1,p^{k-1}+1,2p^{k-1}+1,…,(p-1)p^{k-1}+1)…(j,p^{k-1}+ j,2p^{k-1}+j,…,(p-1)p^{k-1}+1,..$

each p_i is isomorphic to p_1 so has order $p^{n(k-1)}$

∴ p=sylow subgroup of $s_p{}^k$.

DEFINITION :

Let G be a group,A,B two subgroups of G. if, x,y ∈ G defined x∼ y if y = axb where a∈A,b∈B .

Lemma : 2.12.3

The relation define above is an equivalence relation of G, the equivalence class x∈G is the set, AxB = { axb/a∈A,b∈B}.

Proof:

Here the set AxB is a double coset of a,b in G .Now to prove that the relation $x \sim y$.

If $y=axb$,$a \in A$, $b \in B$ is an equivalence relation.

Reflextive :

To prove $x \sim x$

$\rho_1 \in A$, $\rho_2 \in B$. We can write x as $\rho_1 x \rho_2$

$\therefore x \sim x$.

Symmetric :

Let $x \sim y$

To prove : $y \sim x$. Here $x \sim y$,y can be written as $y = axb$,$a \in A$, $b \in B$

$a^{-1} \in A$, $b^{-1} \in B$,Now $a^{-1}yb^{-1} = a^{-1}(axb)b^{-1}$

$$= (a^{-1}a)x(bb^{-1})$$

$$= x.$$

$\therefore y \sim x$.

Transtive :

Let $x \sim y$ & $y \sim z$

To prove : $x \sim z$

$x \sim y \Rightarrow y = a_1 x b_1$

$y \sim z \Rightarrow z = a_2 x b_2$, $a_1a_2 \in A$, $b_1b_2 \in B$

$$= a_2(a_1 x b_1) b_2$$

$$= (a_2a_1) x (b_1b_2)$$

$$= c_1 x c_2$$

$\therefore x \sim z$.

Here the given relation is an equivalence relation.

Definition :

A subgroup of G of order p^m where $p^m/o(G)$ but $p^{m+1}/o(G)$ is called a p sylow subgroup of G.

Lemma:2.12.4:

If A,B are finite subgroup of G then $o(AxB)= o(A).o(B)/o(A\cap xBx^{-1})$

proof;

Given that Gis a finite group and A,B are finite subgroups of G.

To prove that : $o(AxB)= o(a).o(b)/ o(A\cap xBx^{-1})$

The set xBx^{-1} is defined as

$xBx^{-1}=\{ xbx^{-1} /b \in B\}$

first we want to p.t xBx^{-1} is a subgroup of G.

let $xb_1x^{-1},xb_2x^{-1} \in xBx^{-1},b_1,b_2 \in B$

Now $(xb_1x^{-1`})(xb_2x^{-1}) = xb_1x^{-1},xb_2x^{-1}$

$= xb_1(x^{-1}x)b_2x^{-1} = xBx^{-1}$ [$\therefore b_1b_2\in B$]

$\therefore xBx^{-1}$ is a subgroup of G.

Here, we get A and xBx^{-1} are two finite subgroup of G.

Now, By using "First counting principle"

" If H & K are finite subgroup of G then $o(HK) = o(H)o(K)/o(H\cap K)$

we write,

$o(AxBx^{-1}) = o(A).o(xBx^{-1})/ o(A\cap xBx^{-1})$

(i.e) $o(AxBx^{-1}) = o(A).o(B)/ o(A\cap xBx^{-1})$----------(1) [$\therefore o(xBx^{-1}) = o(B)$]

Now to prove thato$(AxBx^{-1}) = o(AxB)$.

consider the mapping f: $AxB \rightarrow AxBx^{-1}$ such that $f(axb) = axb^{-1}$, where $a \in A,b \in B$.

To prove : f is ono-one and onto

$a_1xb_1,a_2xb_2 \in AxB$

To prove f is one-one and onto

$axb_1, a_2\ xb_2 \in AxB$

$\therefore f(a_1xb) = f(a_2xb_2)$

$a_1xb_1 = a_2xb_2$

f is one-one

Now to prove : f is onto

Let $axbx^{-1} \in AxBx^{-1}$, where $a \in A$, $b \in B$ $a \in axb \in AxB$,

Here $f(axb)=axbx^{-1}$

Hence f is on to.

Thus there is a onto corresponding between AxB & $AxBx^{-1}$

$$\therefore\ o(AxB)=o(AxBx^{-1)}$$

Substituting in equation (1) we get ,

$$o(AxBx^{-1})=[o(A).o(B)]/o(A\cap xBx^{-1})\rightarrow 1$$

$$o(AxB)=[o(A).0(B)]/o(A\cap xB\text{-}1)$$

Hence proved.

Lemma 2.12.5

Let G be a finite group and suppose that G is a subgroup of the finite group M. suppose further that M has a sylow subgroup Q . Then G has a p-sylow subgroup p.In fact, $p = G\cap xQx^{-1}$ for some $x \in M$.

Proof :

suppose that $p^m/o(M)$,$p^{m+1}\nmid o(M)$, Q is a subgroup of M of order $p^{m.}$

Let $o(G) = p^n t$ where $p\nmid t$

By Lemma 2.12.4

p is a subgroup of G and has order p^n , the lemma is proved.

THEOREM: 2.12.2 SECOND PART OF SYLOW'S THEOREM

If G is a finite group, P is a prime and $P^n|O(G)$ but $P^{n+1}|O(G)$then any two

subgroup of G order P^n are conjugate.

Proof:

Let A,B be subgroup of G, each of order P^n where $P^n|O(G)$

but $P^{n+1}\nmid O(G)$-------(1)

$\therefore O(A) = O(B) = P^n$

To prove that A and B are conjugate in G.

It is enough to prove that $A=gBg^{-1}$ for some $g\in G$.

Let if equation (1) is possible then $A=xBx^{-1}\ \forall x\in G$

Now we decompose G into double cosets of A and B.

$\therefore$G can be written as $G=\cup AxB$

Now by using O(AxB) = O(A) O(B) ---------(2)

$O(A\cap xBx^{-1})$ Here A and B are subgroups of G and $O(A) = O(B) = P^n$ and also $A\cap xBx^{-1}$ is a

proper subgroup of G if $A\neq xBx^{-1}\ \forall x\in G$

Then $O(A\cap xBx^{-1}) = P^m$ where m<n

$\therefore$ Equation (2) becomes $O(AxB) = P^n.P^m = P^{2m-n}$

==> n-m>0

==> n-m≥1

The above relation $P^{n+1}|O(AxB)$ for every x.

Since, $O(G)=\Sigma O(AxB)$ which is a contradiction to our assumption that

$P^{n+1}\nmid O(G)$.

Hence $A=gBg^{-1}$ for some $g\in G$. Hence A and B are conjugate in G.

Lemma 2.12.6

The number of p-sylow subgroups in G equals o(G)/o(N(p)), Where p is any p-sylow subgroup of G. In particular , this number is a divisor of o(G).

Proof:

P-sylow subgroups for a given prime p, in G.

Theorem: 2.12.3 THIRD PART OF SYLOW THEOREM:

Prove that the number of p-sylow subgroups in G for a given prime is of the form 1+kp.

Proof:

Let p be a p.sylow subgroup of G

To prove that the number of p-sylow subgroup in G is of the form 1+kp where p is a prime number .

Now, we decompose G is a double cosets of p and p .

Thus $G=\cup pxp$

By using theorem 2.12.14

$o(pxp)=[o(p).o(p)]/o(p\cap xpx^{-1})$----------(1)

$o(pxp)=(o(p))^2/o(p\cap xpx^{-1})$------------------(2)

Also $o(G) = \sum o(pxp)$-----------------------(3) [By eqn(1)]

If $p\cap(xpx^{-1}) \neq p$ then $p^{n+1}/o(pxp0$

where $o(p) = p^n$--------------(4)

Also, if $x \in N(p)$

then $pxp = p(xp)$

$= p(px) = (pp)x$

(i.e) $pxp = px$.

$\therefore u(pxp) = \cup px$

Since $p < N(p)$, $\sum_{x \in N(p)} o(pxp) = o(N(p))$---------(5)

eqn(5) becomes

$o(G) = \sum_{x \in N(p)} o(pxp) + \sum_{x \notin N(p)} o(pxp)$-------(6)

where each sum runs over one element from each double cosets.

If $x \notin N(p)$ then $xpx^{-1} \neq p$

$\Rightarrow p \cap xpx^{-1} < p$

$\Rightarrow o(p \cap xpx^{-1})/o(p)$

$\Rightarrow o(p \cap xpx^{-1)} = p^m$ where $m<n$

Equation (3) becomes

$o(pxp) = p^n p^m / p^m$ where $m<n$,

$o(pxp) = p^{n+(n-m)}$

Since n-m> 0 $and\ n - m \geq 1$, if follows

That $p^{n+1}/o\,(pxp)\ \forall x \notin N(p)$

$\Rightarrow P^{n+1}/\sum_{x \notin N(p)} o(pxp) = p^{n+1}.\ u$ ---------(7) for some integer u

Using (5) and (7) in equation (6) we get

$O(G)=o(N(p))+p^{n+1}.u$

$O(G)(o(N(p))=1+[p^{n+1}.u]/o(N(p))$ ----------(8)

Since N(p) is subgroup of G and G is finite group

By Lagrange's theorem.

o(G)/o(N(p)) and it is an integers.

Since p is a p-sylow's subgroup of G and by defn p^n/ o(G) and p^{n+1}/ o(G)

Hence p^{n+1} cannot divide o(N(p)).

But, $p^{n+1}.u/o(N(p))$ must be divisible by p.

$p^{n+1}.u/o(N(p))$ is of the form k_p.

where k is an integers.

(i.e) $p^{n+1}.u/o(N(p)) = kp$

Eqn(8) becomes,

$o(G)/o(N(p)) = 1+ kp$,

Hence, the number of P- sylow's sub groups in G = 1+kp.

UNIT II - FIELDS, VECTORS SPACES, MODULES 18hrs

Direct products – Finite abelian groups – Modules

Chapter 2: Sections 2.13 and 2.14 [only theorem 2.14.1]

Chapter 4: Section 4.5

2.13 DIRECT PRODUCTS

Section 2.13 GROUPS AND MODULES

Introduction

Let A and B be any two groups and consider the Cartesian product G = A $\times$ B of A and B.

G consist of all ordered pairs A,B. where a$\in$B,b$\in$B. In this way we define the product of (a_1, b_1) & (a_2, b_2) is $(a_1, b_1)(a_2, b_2) = (a_1 b_1, a_2 b_2)$. Now we prove the Cartesian product G=A$\times$B is a group.

(i) Closure

Let a_1, b_1 and $a_2, b_2 \in A\times B = G$ Where $a_1, a_2 \in A$ and $b_1, b_2 \in B$

Now , $(a_1, b_1) . (a_2, b_2) = (a_1 a_2\, b_1 b_2) \in G$

$= A\times B$

Therefore closure is satisfied.

(ii) Associative

Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G = A\times B$

Consider, $(a_1, b_1)\ [(a_2, b_2)(a_3, b_3)] = (a_1, b_1), (a_2 a_3, b_2 b_3) = (a_1 a_2 a_3, b_1 b_2 b_3)$------(1)

Similarly

$[(a_1, b_1)(a_2, b_2)]\ (a_3, b_3) = (a_1 a_2, b_1 b_2), (a_3, b_3) = (a_1 a_2 a_3, b_1 b_2 b_3)$------(2)

(iii) Identity

Let e and f be the identity elements of A and B respectively,

Now (a,b) (e,f) = (ae,bf) = (a,b)

Also (e,f) . (a,b) = (ea,fb) = (a,b)

(iv) Inverse

Let $(a_1, b_1), (a_1^{-1}, b_1^{-1}) \in G$

Now $(a_1, b_1) . (a_1^{-1}, b_1^{-1}) = (a_1\, a_1^{-1} . b_1 b_1^{-1})$b

$$= (e,f)$$

Hence $G = A \times B$ is a group.

Internal direct product

Let G be a group and $N_1, N_2, N_3 \ldots N_n$ be the normal subgroups of G such that,

1) $G = N_1 N_2 N_3 \ldots N_n$.
2) Given $g \in G$ then $g = m_1 m_2 \ldots . m_n$ where $m_i \in N_i$ in a unique way then we can say that G is the internal direct product of $N_1, N_2, N_3 \ldots N_n$.

Result

If G is the internal direct product of the groups A and B then G is the internal direct product of $\bar{A}$ and $\bar{B}$ where $\bar{A} = \{(a,f)/a \in A\}$ and $\{(e,b)/b \in B\}$. Here e and f are identity elements of A and B respectively. Also prove that , $A \cong \bar{A}$ and $B \cong \bar{B}$ (or)

If $G = A \times B$ then prove that, $G = \bar{A}\ \bar{B}$

Proof:

Given , $G = A \times B$

Where A and B are any two groups of G

To prove that, $A \cong \bar{A}$ and $B \cong \bar{B}$

Define a mapping $\emptyset : A \rightarrow \bar{A}$ by $\emptyset(a) = (a,f)$ for all $a \in A$

Now to prove one to one , Let $\emptyset(a_1) = \emptyset(a_2)$ that is $(a_1,f) = (a_2,f) \Rightarrow a_1 = a_2$

Therefore $\emptyset$ is one to one.

Now to prove, $\emptyset$ is onto

Let, $(a,f) \in \bar{A} \Rightarrow a \in A$ and f is the identity element of $\bar{A}$

Therefore $\emptyset(a) = (a,f)$, Hence $\emptyset$ is onto

Now to prove, $\emptyset$ is homomorphism,

Let, $(a_{1,}a_2) \in A$ then (i) $(a_1a_{2,}f) = (a_1,f) . (a_2,f)$ that is $\emptyset(a_{1,}a_2)= \emptyset(a_1). \emptyset(a_2)$

(ii) $(a_{1+}a_{2,}f) = (a_1,f) + (a_2,f)$ that is $\emptyset(a_{1+}a_2)= \emptyset(a_1)+ \emptyset(a_2)$

Therefore $\emptyset$ is homomorphism. Hence , $A \cong \bar{A}$

Similarly We can prove that $B \cong \bar{B}$

Next we want to prove that G is the internal direct product of $\bar{A}$ and $\bar{B}$ that is to prove that,

(i) $\bar{A}$ is the normal subgroup of G and $\bar{B}$ is the normal subgroup of G

(ii) Every element $g \in G$ can be written $G=\bar{a}\,\bar{b}$ for all $a \in A$, $b \in B$,$\bar{a} \in \bar{A}, \overline{\ b} \in \bar{B}$

Now to prove $\bar{A}$ is the normal subgroup of G, Let $(a,f),(b,f) \in \bar{A}$,

Now, $(a,f) . (b,f)^{-1} = (a,f) . (b^{-1},f)$

Therefore $\bar{A}$ is a subgroup of G. since , $\bar{A} \subset G=A \times B$ and $(a,f) \in \bar{A}$ that is $(a,f) \in G$

Therefore , $\bar{A} \subset G$

Let, $(a,b) \in G$ and $(a,f) \in \bar{A}$

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

$= (aaa^{-1}, bfb^{-1})$

$= (ae, fbb^{-1})$

$= (a,f) \in \bar{A}$

Therefore $\bar{A}$ is normal subgroup of G

Similarly $\bar{B}$ is normal subgroup of G

Hence we have an isomorphic copy $\bar{A}$ of A and $\bar{B}$ of B in G which is a normol subgroup of G.

Now we claim that G =$\bar{A}$ $\bar{B}$ for all g∈G is a uniquedecomposition in the form, g = $\bar{a}\,\bar{b}$.
where, $\bar{a} \in \bar{A}$, $\bar{b} \in \bar{B}$

Now, G= A × B

Let g∈ G , then g = (a,b), where a∈A , b∈ B

= (a,e).(f,b)

Since, (a,e) ∈ $\bar{A}$ and (f,b) ∈ $\bar{B}$

Therefore g = $\bar{a}\,\bar{b}$ with $\bar{a}$ =(a,e), $\bar{b}$=(f,b) that is g ∈ $\bar{A}\bar{B}$

Now to prove, this representation is unique.

Let G = $\bar{x}\,\bar{y}$, where $\bar{x}$ = (x,e) and $\bar{y}$ = (f,y) then,

g = (x,e) . (f,y)

=(xf,ey)

=(x,y)

But g = $\bar{a}\,\bar{b}$, Therefore, a=x and b=y

Hence G is the internal direct product of $\bar{A}$ and $\bar{B}$.

Lemma 2,13.1

Suppose that G is the internal direct product of $N_1, N_2 \ldots N_n$ then for i≠ j, $N_i \cap N_j = \{e\}$ and if a $\in N_i$,$b \in N_j$ then ab=ba.

Proof:

Given that , G is the internal direct product of $N_1, N_2 \ldots N_n$.

Therefore $N_1, N_2 \ldots N_n$

Where, $N_1, N_2 \ldots N_n$ are normal subgroup of G.

If g∈G then by definition of internal direct product of g = $m_1, m_2 \ldots m_n$ in a unique way.

Where, $m_i \subseteq N_i$

Now to prove $N_i \cap N_j=\{e\}$ for all $i\neq j$

Suppose that, $x\in N_i \cap N_j \Rightarrow x\in N_i$ and $x\in N_j$ then we can write 'x' as
$x = e_1, e_2 \ldots e_{i-1} x\, e_{i+1} + \ldots e_j \ldots e_n$---------(I)

Where $e_t = e$,viewing x as an element in N_i .

Similarly We can write, x as $x=e_1, e_2 \ldots e_i \ldots e_{j-1} x e_{j+1} \ldots e_n$-----------(II)

Where $e_t = e$, viewing x as an element in N_j, But, x as a unique representation in the form $m_1, m_2 \ldots m_n$, Where $m_1 \in N_1$, $m_2 \in N_2 \ldots m_n \in N_n$

From the equations (I) and (II)

The two decomposition in these form for 'x' must coincide, the entry from N_i in each must be equal. In our first decomposition(I). This entry is 'x' in the 2nd decomposition

Hence, x = e, Thus $N_i \cap N_j=\{e\}$ for all $i\neq j$

Suppose $a \in N_i$, $b \in N_j$ and $i\neq j$ then $aba^{-1} \in N_j$ and since N_j is the normal subgroup of G.

Thus, $aba^{-1}b^{-1} \in N_j$,(since $b\in N_j$, $b^{-1}\in N_j$)

Similarly, $a^{-1}\in N_i$, $ba^{-1}b^{-1}\in N_i$, where $aba^{-1}b^{-1}\in N_i$,

But then $aba^{-1}b^{-1}\in N_i \cap N_j=\{e\}$

$$aba^{-1}b^{-1}=e$$

$$ab(ba)^{-1}=e$$

$ab=e(ba)$ Hence the proof.

Lemma 2.131

Let G be a group and suppose that G is the internal direct product of $N_1, N_2 \ldots N_n$.

Let $T= N_1 \times N_2 \times \ldots \times N_n$. then G and T are isomorphic.

Proof:

Given that, G is the group and also G is the internal direct product of $N_{1,}N_2\ldots N_{n.}$

Also given that, $T = N_1\times_{,}N_2\times\ldots\times N_n$

To prove, G and T are isomorphic. Define the mapping, ψ: $T\rightarrow G$ by ψ $(b_1,b_2\ldots b_n) = b_1,b_2...b_n$

Where, each $b_i\in N_i$,i=1,2,…n. We claim that ψ is the isomorphic of T onto G.

Now to Prove , ψ is one to one.

Let, $x,y \in T$ then $x = (a_{1,}a_2,\ldots a_n)$ and $y = (b_1,b_2\ldots b_n)$ such that, ψ (x) = ψ(y)

$$\Rightarrow \psi\ (a_{1,}a_2,\ldots a_n) = \psi\ (b_1,b_2\ldots b_n)$$

$$\Rightarrow\ (a_{1,}a_2,\ldots a_n) = (b_1,b_2\ldots b_n)$$

$$\Rightarrow x_i = y_i$$

$$\Rightarrow x = y$$

Therefore ψ is one to one.

Now to prove , ψ is onto

Since ,G is the internal direct product of $N_{1,}N_2\ldots N_n$ and if $x\in G$ then $x = (a_{1,}a_2,\ldots a_n)$ for some $a_1\in N_{1\,,}$ $a_2\in N_2,\ldots a_n\in N_{n.}$ But then,

ψ $(a_{1,}a_2,\ldots a_n) = a_{1,}a_2,\ldots a_n = x$,Therefore ψ is onto

The mapping ψ is one to one by uniqueness of the representation of every element as a product of element of the form, $N_{1,}N_2\ldots N_n$. For if, ψ $(a_{1,}a_2,\ldots a_n) = c_{1,}c_2,\ldots c_{n.}$ Where, $a_i\in N_{i,}$ $c_i\in N_{i\,.}$ for i = 1,2,…n.

Then by definition of ψ , $a_{1,}a_2,\ldots a_n = c_{1,}c_2,\ldots c_{n.}$

$$\Rightarrow ai = c_{i\,,}\quad i=1,2\ldots n.$$

Thus ψ is one to one

Now to show that, ψ is a homomorphism of T onto G.

If x $(a_{1,}a_2,\ldots a_n)$, y = $(b_1,b_2\ldots b_n)$ are the elements of T.

Then, $\psi(xy) = \psi[(a_{1,}a_2,\ldots a_n)\ (b_1,b_2\ldots b_n)]$

$= \psi(a_1b_{1,}a_2b_2,\ldots a_nb_n)$

$= a_1b_{1,}a_2b_2,\ldots a_nb_n$ by lemma(2.13.1)

$a_ib_j = b_ja_i$ for $i \neq j$

This gives, $a_1b_1 . a_2b_2 \ldots a_nbn = a_1a_{2\ldots}a_{n\,.}\, b_1b_{2\ldots}b_n$

Therefore $\psi(xy) = a_1a_{2\ldots}a_{n\,.}\, b_1b_{2\ldots}b_n$

$= (a_{1,}a_2,\ldots a_n)\ (b_1,b_2\ldots b_n)$

$= \psi(x).\psi(y)$

That is $\psi(xy) = \psi(x).\psi(y)$

Ψ is homomorphism.

Hence, ψ is an isomorphism of T onto G.

Therefore G and T are isomorphic.

2.14 FINITE ABELIAN GROUPS

A finite abelian group is a group satisfying the following equivalent conditions.

(i) It is isomorphic to a direct product of finitely many finite cyclic groups.

(ii) It is isomorphic to a direct product of abelian groups of prime power order.

(iii) It is isomorphic to a direct product of cyclic groups of prime power order.

Theorem 2.14.1

Statement

Every finite abelian group is the direct product of cyclic groups

Proof:

Every finite abelian group G is finitely generated

Hence it is generated by the finite set consisting of all its elements.

Therefore Applying this theorem,

Let R be a Euclidean Ring, then any finitely generated R-Module, M is the direct sum of the finite number of cyclic sub-modules.

Proof:

Let M be the finitely generated R-Module. To prove that the theorem for ring of integers. Since the ring of integers is also a Euclidean ring. Hence we assume that M is an abelian group which has a finite generating set.

Now we prove the theorem by the induction on the rank of M.

Step-1: If the rank of M is one. Then M is generated has a single element.

∴ M is cyclic, Hence the theorem is proved for rank one.

Step-2: Let us assume that the theorem is proved for all abelian group of rank less than q.

That is the result is true for all abelian groups of rank for r-1, Hence any R-Module where rank is q-1 is the direct sum of finite number of cyclic sub-module.

Step-3: Now we prove the theorem for rank M = q. Let $a_1, a_2 \dots a_q$ be the minimal generating set of M. If any relation of the form $r_1a_1+r_2a_2+\dots+r_qa_q = 0$. Where $r_1, r_2 \dots r_q$ are integers then $r_1a_1 = 0$, $r_2a_2 = 0 \dots r_qa_q = 0$. Hence M is the direct sum of $M_1, M_2 \dots M_q$, where each M_i is the cyclic sub-Module generated by a_i.

Step-4: Let us assume that given any minimal generating set $b_1, b_2 \dots b_q$ of M must be integers $r_1, r_2 \dots r_q$ such that $r_1b_1+r_2b_2+\dots+r_qb_q = 0$ and in which not all $r_1a_1, r_2a_2, \dots, r_qa_q$ are zero.

Among all possible such relations for all minimal generating set, there is a smallest possible +ve integers occurring as coefficient. Let this integer be s_1 and let the generating set for which if occurs be $a_1, a_2 \ldots a_q$ thus $s_1a_1+s_2a_2+\ldots+s_qa_q = 0$.--------(1)

We claim that if $r_1a_1+r_2a_2+\ldots+r_qa_q = 0$. ------------(2)

if not $r_1 = ms_1 + t$ ------------(3) where $0\leq t\leq s_1$.

Now (1) multiplying by m and subtracting from eqn. (2) we get

(2)-(1)Xm $\Rightarrow (r_1-ms_1)a_1 +\ldots\ldots+(r_q-ms_q)a_q = 0$.

That is $ta_1+(r_2-ms_2)a_2 +\ldots\ldots+(r_q-ms_q)a_q = 0$. Since $t<s_1$ and s_1 is the smallest possible +ve integer in such a relation. We must have t=0.

$\therefore$eqn.(3) becomes $r_1 = ms_1$, therefore s_1/n.

Now we claim that s_1/s_i for I = 1,2….q

Suppose not then s_1 does not divide s_2, therefore $s_2 = m_2s_1 + t$ ---------(A), where $0\leq t<s_1$.

Now $a_1^1 = a_1+m_2a_2, a_2, a_3, \ldots a_q$ is also generated by m. Hence we have from eqn. (1)

$s_1a_1+s_2a_2+\ldots+s_qa_q = 0$

i.e., $s_1(a_1^1-m_2a_2)+s_2a_2+\ldots+s_qa_q = 0$

i.e., $s_1a_1^1-s_1m_2a_2+s_2a_2+\ldots..+s_qa_q = 0$

i.e., $s_1a_1^1-(s_2-s_1m_2)a_2+\ldots+s_qa_q = 0$

i.e., $s_1a_1^1 +ta_2+\ldots\ldots+s_qa_q = 0$ (by using (4))

Thus t occurs us a coefficient in some relation among elements of a minimal generating set. $\therefore$ By the very choice of s_1 that t = 0. Hence $s_2 = m_2s_1 \Rightarrow s_1/s_2$.

Similarly for the other s_i, hence we write $s_i = ms_1$ and also s_1/s_i , i=1,2,3….q

Consider the elements $a_1^* = a_1+m_2a_2+m_3a_3+\ldots+m_qa_q, a_2,\ldots,a_q$ where $a_2,a_3,\ldots,a_q$ generate M.

Moreover, $s_1a_1^* = s_1a_1+ s_1m_2a_2+ s_1m_3a_3+\ldots+ s_1m_qa_q = s_1a_1+s_2a_2+\ldots+s_qa_q$.

If $r_1 a_1^* + r_2a_2 + \ldots + r_qa_q = 0$. Substitute for a_1^*, we get

$r_1(a_1+m_2a_2+m_3a_3+\ldots+m_qa_q)+r_2a_2+\ldots+r_qa_q = 0$. $r_1a_1+(r_1m_2+r_2)a_2+\ldots+(r_1m_q+r_q)a_q = 0$.

Therefore the coefficient of a_1 is r_1, hence $r_1a_1^* = 0$.

If M_1 is the cyclic sub-module generated by a_1^* and M_2 is the sub-module of M generated by a_2, $a_3,\ldots,a_q$. We have $M_1 \cup M_2 = \{e\}$ and $M_1+M_2 = M$. since $a_1^*, a_2, a_3, \ldots, a_q$ generate M and M is the direct sum of M_1 and M_2. Since M_2 is the sub-module generated by $a_2, a_3, \ldots, a_q$ and its rank is atmost q-1. Hence by induction hypothesis M_2 is the direct sum of cyclic sub-modules.

Since M_1 is the cyclic sub-modules generated by a_1^* and hence M is the direct sum of cyclic sub-modules M_1 & M_2 whose rank is q. Now the proof can be modified to the Euclidean ring R as follows. Instead of taking s_1, let us take the elements of the ring R, whose value is maximal and whenever we take of t , where $r_1 = ms_1+t$ either $t=0$ or $d(t)<d(s)$

Hence the Euclidean ring R-Module is the direct sum of finite number of cyclic sub-module.

We get any finite abelian group is the direct product of cyclic group.

Section 4.5

Modules

Let R be any ring. A non-empty set M is said to be an R-Module over R. If M is an abelian group under the operation '+' such that for every $r \in R$, $m \in M$ there exist an element rm in M subject to

(i) $r(a+b) = r(a) + r(b)$
(ii) $r(sa) = (rs)a$
(iii) $(r+s)a = ra + sa$ for all $a,b \in M$, $r,s \in R$

Unital R-Module:

If R has a unit element one and if 1.m = m for every element m in M. Then M is called a unital R-Module.

Definition:

An additive subgroup A of the R-Module is called sub-module of M, if whenever $r \in R$, $a \in A$, $ra \in A$.

Examples:

(i) Every abelian group G is a module over the ring of integers.

(ii) Let R be any ring and let M be the left idle of R. Then M is an R-Module.

Definition:

If M is an R-Module and if $M_1, M_2, \ldots M_s$ are the sub-module of M, then M is said to be the direct sum of $M_1, M_2, \ldots M_s$

i.e., $M = M_1 \oplus M_2 \oplus \ldots \oplus M_s$, if every element $m \in M$ can be written in a unique manner as

$m_1 + m_2 + \ldots + m_s$, where $m_1 \in M_1$, $m_2 \in M_2 \ldots m_s \in M_s$.

Definition:

An R-Module is said to be cyclic if there is an element $m_0 \in M$, such that every $m \in M$ is of the form $m = rm_0$ where $r \in R$.

Definition:

An R-Module is said to be finitely generated if there exist elements $a_1, a_2, \ldots a_n \in M$, such that every M is of the form $r_1a_1 + r_2a_2 + \ldots + r_na_n$.

Definition:

If M is finitely generated R-Module. Then a generating set having a few elements as possible is called the minimal generating set.

Definition:

The number of elements in a minimal generating set is called rank of M.

Result:

Prove that the intersection of two sub-Modules is again a Sub-Module.

Proof:

Let M be an R-Module and s_1 and s_2 be the sub-modules of M.

To prove that $s_1 \cap s_2$ is a subset of M, we have, $s_1 \cap s_2 \neq \emptyset$.

We know that $s_1 \cap s_2$ is a additive subgroup of M. (since the number of two subgroups is again a subgroup)

Let $a,b \in s_1 \cap s_2 \Rightarrow a \in s_1$, $a \in s_2$ and $b \in s_1$, $b \in s_2$.

Therefore $(a,b) \in s_1 \cap s_2$

Therefore $(s_1, +)$ & $(s_2, +)$ is a additive subgroup.

Let $r \in R$ and $s \in s_1 \cap s_2 \Rightarrow r \in R$ and $s \in s_1$ and $s \in s_2$.

$\Rightarrow rs \in s_1$ and $rs \in s_2$.

$\Rightarrow rs \in s_1 \cap s_2$, Therefore $s_1 \cap s_2$ is sub-module.

Theorem:4.5.1: Fundamental theorem on finitely generated R-Module.

Let R be a Euclidean Ring, then any finitely generated R-Module, M is the direct sum of the finite number of cyclic sub-modules.

Proof:

Let M be the finitely generated R-Module. To prove that the theorem for ring of integers. Since the ring of integers is also a Euclidean ring. Hence we assume that M is an abelian group which has a finite generating set.

Now we prove the theorem by the induction on the rank of M.

Step-1: If the rank of M is one. Then M is generated has a single element.

$\therefore$ M is cyclic, Hence the theorem is proved for rank one.

Step-2: Let us assume that the theorem is proved for all abelian group of rank less than q.

That is the result is true for all abelian groups of rank for r-1, Hence any R-Module where rank is q-1 is the direct sum of finite number of cyclic sub-module.

Step-3: Now we prove the theorem for rank M = q. Let $a_1, a_2 \ldots. a_q$ be the minimal generating set of M. If any relation of the form $r_1a_1+r_2a_2+\ldots.+r_qa_q = 0$. Where $r_1, r_2 \ldots. r_q$ are integers then $r_1a_1 = 0$, $r_2a_2 = 0 \ldots. r_qa_q = 0$. Hence M is the direct sum of $M_1, M_2 \ldots M_q$, where each M_i is the cyclic sub-Module generated by a_i.

Step-4: Let us assume that given any minimal generating set $b_1, b_2 \ldots. b_q$ of M must be integers $r_1, r_2 \ldots. r_q$ such that $r_1b_1+r_2b_2+\ldots.+r_qb_q = 0$ and in which not all $r_1a_1, r_2a_2, \ldots., r_qa_q$ are zero.

Among all possible such relations for all minimal generating set, there is a smallest possible +ve integers occurring as coefficient. Let this integer be s_1 and let the generating set for which if occurs be $a_1, a_2 \ldots. a_q$ thus $s_1a_1+s_2a_2+\ldots.+s_qa_q = 0$.--------(1)

We claim that if $r_1a_1+r_2a_2+\ldots.+r_qa_q = 0$. ------------(2)

if not $r_1 = ms_1 + t$ ------------(3) where $0 \leq t \leq s_1$.

Now (1) multiplying by m and subtracting from eqn. (2) we get

(2)-(1)Xm $\Rightarrow (r_1-ms_1)a_1 +\ldots\ldots+(r_q-ms_q)a_q = 0$.

That is $ta_1+(r_2-ms_2)a_2 +\ldots\ldots+(r_q-ms_q)a_q = 0$. Since $t<s_1$ and s_1 is the smallest possible +ve integer in such a relation. We must have t=0.

$\therefore$eqn.(3) becomes $r_1 = ms_1$, therefore s_1/n.

Now we claim that s_1/s_i for I = 1,2….q

Suppose not then s_1 does not divide s_2, therefore $s_2 = m_2s_1 + t$ ---------(A), where $0 \leq t < s_1$.

Now $a_1^1 = a_1+m_2a_2, a_2, a_3, \ldots. a_q$ is also generated by m. Hence we have from eqn. (1)

$s_1a_1+s_2a_2+\ldots.+s_qa_q = 0$

i.e., $s_1(a_1^1-m_2a_2)+s_2a_2+\ldots.+s_qa_q = 0$

i.e., $s_1a_1^1-s_1m_2a_2+s_2a_2+\ldots..+s_qa_q = 0$

i.e., $s_1a_1^1-(s_2-s_1m_2)a_2+\ldots.+s_qa_q = 0$

i.e., $s_1a_1^1 +ta_2+\ldots\ldots+s_qa_q = 0$ (by using (4))

Thus t occurs us a coefficient in some relation among elements of a minimal generating set. ∴ By the very choice of s_1 that t = 0. Hence $s_2 = m_2s_1 \Rightarrow s_1/s_2$.

Similarly for the other s_i, hence we write $s_i = ms_1$ and also s_1/s_i , i=1,2,3….q

Consider the elements $a_1^* = a_1+m_2a_2+m_3a_3+\dots+m_qa_q$, $a_2,\dots,a_q$ where $a_2,a_3,\dots,a_q$ generate M.

Moreover, $s_1a_1^* = s_1a_1+ s_1m_2a_2+ s_1m_3a_3+\dots+ s_1m_qa_q = s_1a_1+s_2a_2+\dots+s_qa_q$.

If $r_1 a_1^*+r_2a_2+\dots+r_qa_q = 0$. Substitute for a_1^*, we get

$r_1(a_1+m_2a_2+m_3a_3+\dots+m_qa_q)+r_2a_2+\dots+r_qa_q = 0$. $r_1a_1+(r_1m_2+r_2)a_2+\dots+(r_1m_q+r_q)a_q = 0$.

Therefore the coefficient of a_1 is r_1, hence $r_1a_1^* = 0$.

If M_1 is the cyclic sub-module generated by a_1^* and M_2 is the sub-module of M generated by a_2, $a_3,\dots,a_q$. We have $M_1 \cup M_2 = \{e\}$ and $M_1+M_2 = M$. since $a_1^*,a_2,a_3,\dots,a_q$ generate M and M is the direct sum of M_1 and M_2. Since M_2 is the sub-module generated by $a_2,a_3,\dots,a_q$ and its rank is atmost q-1. Hence by induction hypothesis M_2 is the direct sum of cyclic sub-modules.

Since M_1 is the cyclic sub-modules generated by a_1^* and hence M is the direct sum of cyclic sub-modules M_1 & M_2 whose rank is q. Now the proof can be modified to the Euclidean ring R as follows. Instead of taking s_1, let us take the elements of the ring R, whose value is maximal and whenever we take of t , where $r_1 = ms_1+t$ either t=0 or $d(t)<d(s)$

Hence the Euclidean ring R-Module is the direct sum of finite number of cyclic sub-module.

Corollary: Fundamental theorem on finite abelian groups:

Statement:

Any finite abelian group is the direct product of cyclic groups.

Proof:

Every finite abelian group G is finitely generated. Hence it is generated by the finite set consisting of all its elements. Therefore applying the theorem of Fundamental theorem on finitely generated R-Module. Hence Any finite abelian group is the direct product of cyclic groups.

UNIT - III - LINEAR TRANSFORMATIONS 18hrs

Solvability by Radicals - Galois groups over the Rationals

Chapter 5: Sections: 5.7 and 5.8

5.7 Solvability by radicals:

Solvable:

A graph G is said to be solvable if we can find a finite chain of subgroups $N_0 \supset N_1 \supset N_2 \ldots \supset N_k = \{e\}$ where N_i is a normal subgroup of N_{i-1} and such that every factor group $\frac{N_{i-1}}{N_i}$ is abelian.

Result:

Prove that abelian group is solvable.

Proof:

Let G be am abelian group . To prove that G is solvable.

We take N_0=G and N_1={e} such that G= $N_0 \supset N_1 = \{e\}$. To prove N_1 is a normal subgroup N_0 = G. Let g∈G, Now $geg^{-1} = (gg^{-1})e = ee= e \in G$. Therefore $gg^{-1} \in N_1$.

Hence N_1 is a normal subgroup of N_0=G. Now to prove $\frac{N_0}{N_1}$ is abelian. Here the factor group $\frac{N_0}{N_1} = \frac{G}{\{e\}}$ = {ex=xe/x∈G}. Since G is abelian, $\frac{N_0}{N_1}$ is abelian. Hence G is solvable.

Every abelian is solvable.

Definition:

Let G be a group and the elements a,b∈G, then the commutator of a and bis the elements a^{-1}, b^{-1}, ab.

Definition:

The commutator subgroup G'of G is the subgroup of G generated by all the commutators in G.

Result:

Prove that the commutator subgroup G' is a subgroup of G.

Proof:

Let G be a group and S = { $a^{-1}b^{-1}ab$ such that a,b∈G} the commutator subgroup

G' = {S_1, S_2 …. S_m / S_i ∈G}, M is arbitrary. Let s∈S then S = $a^{-1} b^{-1}$ ab for some a,b∈G.

Consider $(a^{-1} b^{-1} ab)^{-1} = b^{-1} a^{-1} ba \in S$

No to prove G' is a subgroup of G, Let x,y ∈G' then x = S_1, S_2 …. S_m, S_i ∈S, m is arbitrary and y = S_1', S_2' …. S_n', S_i' ∈S, n is arbitrary.

Consider, $xy^{-1} = (S_1, S_2 \ldots. S_m)(S_1', S_2' \ldots. S_n')^{-1} = (S_1, S_2 \ldots. S_m)(S_1'^{-1}, S_2'^{-1} \ldots. S_n'^{-1})$

Therefore xy^{-1} is a finite product of finite number of elements of S.

Therefore xy^{-1} is a finite product of finite number of elements of G.

∴ xy^{-1}∈G', Hence G' is a subgroup of G.

Result:

Prove that the commutator subgroup G' is a normal subgroup of G.

Proof:

Let G be a group and G' be the commutator subgroup of G. Let x∈G and a∈G'

Consider, $xax^{-1} = (xax^{-1})(a^{-1}a)$

$= (xax^{-1} a^{-1})a \in G'$

By lemma(1), $xax^{-1} a^{-1}$∈S and s∈G'

Hence G' is a normal subgroup of G.

Result:

Let G be a group and G' be a commutator subgroup of G, then

(i) G/G' is abelian

(ii)If H is any normal subgroup of G such that G/H is a abelian than G'CH.

Proof:

Given G is a group and G' is the commutator subgroup of G.

i) To prove: G/G' is abelian. since G' is normal in G, G/G' is a factor group and G/G': {aG'/a∈G}.

Let aG',bG'∈ $\frac{G}{G'}$, where a,b∈G

Now, $aG'.bG' = abG'$, $bG'.aG' = baG'$ --------(1)

Now consider $(ab)^{-1}ba \in G'$

$(ab)^{-1}ba\, G' = G' \rightarrow baG' = G'(ab) \rightarrow baG' = abG$

Therefore $bG'.aG' = aG'.bG'$

Hence G/G' is abelian.

ii) Let G/H is a abelian

To prove $G' \subset H$

since G/H is a abelian

$aH.bH = bH.aH \rightarrow abH = baH \rightarrow (ba)^{-1}(ab)H = H$

$\rightarrow (ba)^{-1}(ab)H \in H$

$\therefore a^{-1}b^{-1}ab \in H$

therefore H contains all the elements of the form $a^{-1}b^{-1}a$.

Hence $G' \subset H$.

Lemma-5.7.1:

G is solvable $\leftrightarrow G^{(k)} = \{e\}$ for some integer k.

Proof:

Necessary part:

Let $G^{(k)} = \{e\}$

To prove G is solvable

Let $N_0 = G$, $N_1 = G^1$, $N_2 = G^{(2)}$ ….. $N_k = G^{(k)} = \{e\}$ we have $G = N_0 \subset N_1 \subset N_2$ …..$\subset N_k = \{e\}$

where each N_i is normal in G. By lemma (2) $G^{(i+1)}$ is a normal subgroup of $G^{(i)}$. Therefore $\frac{N_{i+1}}{N_i}$ $= \frac{G^{(i-1)}}{G^{(i)}} = \frac{G^{(i-1)}}{G^{(i-1)^1}}$

By lemma 3, $\frac{G^{(i)}}{G^{(i+1)}}$ is an abelian group.

Hence G is solvable.

Sufficient part:

Let G be a solvable group, To prove $G^{(k)} = \{e\}$

Since G is solvable there exist a chain $G= N_0 \subset N_1 \subset N_2 \ldots\ldots \subset N_k = \{e\}$ and N_i is a normal subgroup N_{i-1} and also $\frac{N_{i-1}}{N_i}$ is abelian. But then commutator subgroup $(N_{i-1})'$ must be contained in N_i.

i.e., $N_{i-1} \subset N_i$.

Thus, $N_i \supset N_0'$

$N_2 \supset N_1' = (G')' = G^{(2)} \ldots\ldots N_k \quad \supset N_{k-1} = G^{(k)}$ --------(1)

Also $N_k = \{e\}$ Eqn (1) which implies $G^{(k)} = \{e\}$.

Hence the theorem.

Corollary:

If G is a solvable group and $\bar{G}$ is homomorphism image of G, then $\bar{G}$ is solvable. Prove that homomorphic image of solvable group is solvable.

Proof:

Let $\emptyset$:G→ $\bar{G}$ be a onto homomorphism

Let $S = \{ a^{-1}b^{-1}ab / \ a,b \in G\}$ and $G' = \{ s_1 , s_2 \ldots. s_m / s_i \in S$, m is arbitrary}

Let $\bar{S} = \{\bar{a}^{-1}\bar{b}^{-1}\bar{a}\bar{b} \ / \ \bar{a}\bar{b} \in \bar{G}\}$

$\bar{G}' = \{\bar{s_1}, \bar{s_2} \ldots. \bar{s_n} / \ \bar{s_i} \in \bar{S}, n$ is arbitrary}

To prove: $\emptyset(S) = \bar{S}$

Let $s \in S$, then $S = a^{-1}b^{-1}ab$ where $a,b \in G$

Now, $\emptyset(S) = \emptyset(a^{-1}b^{-1}ab)$

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

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

$= \bar{a}^{-1}\bar{b}^{-1}\bar{a}\bar{b}$

$\emptyset(S) \in \bar{S}$ -------- (1)

Let $(\overline{a})^{-1}(\bar{b})^{-1}\bar{a}\bar{b} \in \bar{S}$, where $\bar{a}\bar{b} \in \bar{G}$

since $\emptyset$ is onto there exist a,b $\in$G such that $\emptyset(a) = \bar{a}$, $\emptyset(b) = \bar{b}$

Now$(\overline{a})^{-1}(\bar{b})^{-1}\bar{a}\bar{b} = (\emptyset(a^{-1}))^{-1} (\emptyset(b^{-1}))^{-1}\emptyset(a)\, \emptyset(b)$

$= \emptyset(a^{-1}b^{-1}ab) \in \emptyset(S)$

$\therefore \bar{S} \subset \emptyset(S)$ --------(2)

From (1) and (2) $\emptyset(S) = \bar{S}$

Now to prove $\emptyset(G') = \bar{G}'$

Let $s_1 , s_2 \ldots s_m \in G'$, $s_i \in S$, m is arbitrary.

Now $\emptyset(s_1 , s_2 \ldots s_m) = \emptyset(s_1)\, \emptyset(s_2)\ldots \emptyset(s_m)$

$= \overline{s_1}, \overline{s_2}\ldots\overline{s_m} \in \bar{G}'$

$\emptyset(G') \subset \bar{G}'$ --------(3)

Now to prove $\bar{G}' \subset \emptyset(G')$

Let $\bar{x} = \overline{s_1}, \overline{s_2}\ldots\overline{s_m} \in \bar{G}'$

since $\emptyset$ is onto there exist $s_i \in S$, such that $\emptyset(s_i)= \overline{s_i}$,

Let $x = s_1 , s_2 \ldots s_m \in G'$

$\emptyset(x) = \emptyset(s_1 , s_2 \ldots s_m) = \overline{s_1}, \overline{s_2}\ldots\overline{s_m}$

$\bar{G}' \supset \emptyset(G')$ --------- (4)

From (3) and (4) $\emptyset(G') = \bar{G}'$

Hence $\bar{G}'$ is a homomorphic image of $G^{(1)}$. implies that $(\bar{G}')'$ is a homomorphic image of $G^{(2)}\ldots(\overline{G}^{(k-1)})'$is a homomorphic image of $G^{(k)}$

Also $(G^{(k)})' = \{\bar{e}\}$ where $\bar{e}$ is the identity element of $\overline{G}$

A group G is solvable $G^{(k)} = \{e\}$. Here $\overline{G}$ is a homomorphic image of G and also $\overline{G}^{(k)}$ is the image of $G^{(k)}$.

Hence $\overline{G}$ is solvable.

Result:

Prove that subgroup of a solvable group is solvable.

Proof:

Let G be a solvable group and H its subgroup.

To prove that H is solvable

Since G is solvable, then by definition of solvable group

(i) G = G= $N_0 \supset N_1 \ldots. \supset N_k = \{e\}$
(ii) N_i is normal subgroup of N_{i-1}
(iii) $\frac{N_{i-1}}{N_i}$ is an abelian group, here G = G= $N_0 \supset N_1 \ldots. Ɔ\supset_k = \{e\}$

Now, $H \cap G = H \cap N_0 \supset H \cap N_1 \ldots. \supset H \cap N_k = \{e\}$

i.e., $H = H_0 \supset H_1 \ldots. \supset H_k = \{e\}$

Let $H \cap N_i = H_i \ \forall$ i, we know that N_i is a normal subgroup of N_{i-1}, then $H \cap N_i$ is a normal subgroup of $H \cap N_{i-1}$.

Implies that H_i is a normal subgroup of H_{i-1}.

Now, let us define the mapping F: $H_i \rightarrow \frac{N_{i-1}}{N_i}$, $f(x) = xN_{i+1}, \forall\ x \in H_i$

To prove F is well defined

Here $H_i = H \cap N_i \subset N_i$, ∴ $H_i \subset N_i$.

Let $x \in H_i$ implies that $x \in N_i$.

Therefore $xN_{i+1} \in \frac{N_i}{N_{i+1}}$,

∴ f is well defined.

Now to prove f is homomorphism

Let $x,y \in H_i$

i) $f(x+y) = (x+y) N_{i+1} = x N_{i+1} + y N_{i+1} = f(x) + f(y)$.
ii) $f(xy) = (xy) N_{i+1} = (x N_{i+1})(y N_{i+1}) = f(x)f(y)$.

Now to prove f is onto

$xN_{i+1} \in \frac{N_i}{N_{i+1}} \Rightarrow x \in N_i$.

$\Rightarrow x \in H \cap N_i \quad \Rightarrow x \in H_i$.

$\therefore f(x) = xN_{i+1}$

Now to prove $\ker f = H_{i+1}$, $\forall i$

We know that $\ker f = \{ x \in H_i / f(x) = N_{i+1} \}$

Let $x \in \ker f \Leftrightarrow f(x) = N_{i+1} \Leftrightarrow xN_{i+1} = N_{i+1} \Leftrightarrow x \in N_{i+1} \Leftrightarrow x \in H \cap N_{i+1}$

$\Leftrightarrow x \in H_{i+1} \Leftrightarrow \ker f = H_{i+1}$

Hence f is a onto homomorphism.

i.e.,$f: H_i \xrightarrow{\text{onto}} \frac{N_i}{N_{i+1}}$, homomorphism with $\ker f = H_{i+1}$, By using fundamental theorem of homomorphism $\frac{H_i}{H_{i+1}} \cong \frac{N_i}{N_{i+1}}$, Here $\frac{N_i}{N_{i+1}}$ and $\frac{H_i}{H_{i+1}}$ is an abelian group.

Hence H is an solvable group.

Lemma 5.7.2:

Prove that if $G = S_n$, where $n \geq 5$ then $G^{(k)}$ for k =1,2…. Contains every 3- cycle of S_n.

Proof:

Let $G = S_n$, $n \geq 5$, to prove $G^{(k)}$ for k =1,2…. Contains every 3 cycle of S_n.

We know that if N' is a normal subgroupof G then N' must also be a normal subgroup of G.

Step-1:

We claim that if N is a normal subgroup of $G = S_n$, where $n \geq 5$ which contains evry 3-cycle in S_n.

Suppose a= (1,2,3), b = (1,4,5) are in N. Then $a^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \end{pmatrix}$

Also $b = \begin{pmatrix} 1 & 4 & 5 \\ 4 & 5 & 1 \end{pmatrix} \quad b^{-1} = \begin{pmatrix} 1 & 4 & 5 \\ 5 & 4 & 1 \end{pmatrix}$

Then, $a^{-1}b^{-1}ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 4 & 5 \\ 5 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 4 & 5 \\ 4 & 5 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix} = \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}$ is a commutators of elements

$$4 \quad 1 \quad 3 \quad 2 \quad 5$$

Of N must be in N'. since N' is a normal subgroup of G equal to S_n for any $\pi \in S_n$,

$\pi^{-1}(1 \quad 4 \quad 2)\pi$ must also be in N'.

$\therefore \pi^{-1}(1 \quad 4 \quad 2)\pi \subset$N'. Now let i_1, i_2, i_3 be three distinct integer in the range from i=1,2,3…. n.

To prove $i_1, i_2, i_3 \in N'$, i.e., To prove $\pi^{-1}(1 \quad 4 \quad 2)\pi = (i_1, i_2, i_3)$ is in N'.

Since i_1, i_2, i_3 are 3-cycle in S_n. Choose $\pi \in S_n$ such that $\pi(1) = i_1$, $\pi(4) = i_2$, $\pi(2) = i_3$, where (i_1, i_2, i_3) are 3 distinct ineger range from i = 1,2,3 …..

Step-2:

Let G = S_n which is normal in G and contains all the 3-cycle in G. Also we have N' = G', N' contains every 3-cycle of S_n, we have G' also contains every 3-cycle of S_n.

Now , $(G')^{(1)} = G^{(2)}$ contains every 3-cycle of S_n. Since $G^{(2)}$ is normal in G, $G^{(2)}$ containing every 3-cycle of S_n. Also, $(G^{(2)})^{(1)} = G^{(3)}$ is normal in G, $G^{(3)}$ containing in this way we get $G^{(k)}$ contains every 3-cycle of S_n for arbitrary k.

Theorem: 5.7.1:

Prove that S_n is not solvable for $n \geq 5$.

Proof:

Let G = S_n, where $n \geq 5$,

Then by using lemma 5.7.2 , $G^{(k)}$ contains every 3-cycle of S_n

Hence G = S_n is not solvable for $n \geq 5$.

SECTION 5.8 GALOIS GROUPS OVER THE RATIONALS

In Theorem, Let $f(x) \in F(x)$ be of degree $n \geq 1$. Then there is an *E* of *F* of degree at most *n*! in which *f*(*x*) has *n* roots. We saw that given a field *F* and a polynomial *p*(*x*) over *F* has degree at most *n*! over *F*. In the preceding section we saw that this upper limit of *n*! is indeed, taken on for some choice of *F* and some polynomial *p*(*x*) of degree *n* over *F*. In fact, if F_0 is any field and if *F* is the field of rational functions in the variables a_1, a_2,…..a_n over F_0, it was shown that the splitting field K, of the polynomial $p(x) = x^n + a_1x^{n-1} + \ldots + a_n$ over F has degree exactly $n!$ over F. Moreover, it was shown that the Galois group of K over F is S_n, the symmetric group of degree n. This turned out to be the basis for the fact that the general polynomial of degree n, with $n \geq 5$, is not solvable by radicals.

We shall make use of the fact that polynomials with rational coefficients have their roots in the complex field

Theorem 5.8

Let $q(x)$ is an irreducible polynomial of degree p, p a prime, over the field Q of rational numbers. Suppose that $q(x)$ has exactly two non real roots in the field of complex numbers then the Galois group of $q(x)$ over Q is S_p, the symmetric group of degree p. Thus the splitting field of $q(x)$ over Q has degree p over Q

Proof: Let K be the splitting field of the polynomial $q(x)$ over Q

If α is a root of $q(x)$ in K, since $q(x)$ is irreducible over 2, then by theorem 5.1.3 $[Q(\alpha) : Q] = p$

Since $K \supset Q(\alpha) \supset Q$ and according to theorem 5.1.1

$[K : Q] = [K : Q(\alpha)]\,[Q(\alpha) : Q] = [K : Q(\alpha)]p$

By theorem 5.6.4 $O(G) = [K : F]$. Thus $p / O(G)$

Hence by Cauchy's theorem, G has an element σ of order p to this point we have not used our hypothesis that $q(x)$ has exactly two non real roots. We use it now α_1, α_2 are these non-real roots, then $\alpha_1 = \overline{\alpha_2}, \alpha_2 = \overline{\alpha_1}$ where the bar denotes the complex conjugate.

If $\alpha_3, \ldots\ldots\alpha_p$ are the other roots since they are real $\overline{\alpha_i} = \alpha_1,\ i \geq 3$

Thus the complex conjugate mapping takes K into itself, is an automorphism τ of K over Q and interchanges α_1, α_2 leaving the other roots of $q(x)$ fixed.

Now the elements of G take roots of $q(x)$ into roots of $q(x)$. So induces permutations of $\alpha_1, \alpha_2, \ldots\ldots\alpha_p$

In this way we imbed G in S_p. The automorphism τ described above is the transposition (1, 2)

Since $\tau(\alpha_1) = \alpha_2,\ \ \tau(\alpha_2) = \alpha_1,$ and $\tau(\alpha_i) = \alpha_i,\ i \geq 3$

What about the element $\sigma \in G$. Which we mentioned above has order p? As an element of S_p. σ has order p, but the only elements of order p in S_p are p cycles. Thus S must be a p cycles

Therefore G has a subgroup of S_p contains a transposition and p cycles

To prove that any transposition and only p cycles in S_p generates S_p. Thus σ and τ genetrates S_p, but since they are in G, the group generated by σ and τ must be in G. $G = S_p$

In otherwords, the Galois group of $q(x)$ over Q indeed S_p

UNIT - IV - LINEAR TRANSFORMATIONS 18hrs

Linear Transformations: Canonical forms- Triangular form -Nilpotent transformations.

-Jordan form

Chapter 6: Sections 6.4, 6.5, 6.6

SECTION 6.4

CANONICAL FORM AND TRIANGULAR FORM

Definition: Linear Transformation

Let V be a vector space over a field F a mapping $T: V \to V$ is called a Linear transformation. If it satisfies the following conditions

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

(ii) $\alpha(vT) = \alpha v(T)$

Note: Hom(V, V) is the set of all homomorphism of V into itself and Hom(V, V) is a vector space and it is denoted by $A(V)$ and it is the set of all linear transformation from V to V

Definition: Matrices

Let V be an n-dimensional vector space over a field F. Let $\{v_1, v_2, ...v_n\}$ be a basis of V over F. If $T \in A(V)$ then T is determined by any vectors depends on the basis of V. Since $T \in A(V)$, $T(v_1), T(v_2), ...T(v_n)$ are belonging to V

$$T(v_1) = \alpha_{11}v_1 + \alpha_{12}v_2 + ... + \alpha_{1n}v_n$$
$$T(v_2) = \alpha_{21}v_1 + \alpha_{22}v_2 + ... + \alpha_{2n}v_n$$
....
$$.T(v_n) = \alpha_{n1}v_1 + \alpha_{n2}v_2 + ... + \alpha_{nn}v_n, \text{ where } \alpha_{ij} \in F$$

This system of linear equation can be written as $T(v_i)=\sum_{j=1}^{n}\alpha_{ij}v_j, \quad i=1,2,.....n$. Then the matrix of T is the basis $\{v_1,v_2,.......v_n\}$ is written as $m(T)=\begin{pmatrix} \alpha_{11} & \alpha_{12} \ .... \ \alpha_{1n} \\ \alpha_{21} & \alpha_{22} \ .... \ \alpha_{2n} \\ ..... \\ \alpha_{n1} & \alpha_{n2} \ .... \ \alpha_{nn} \end{pmatrix}$

Invariant: Let *W* be the subspace of a vector *V* over *F*. Suppose *W* is invariant under the transformation $T\in A(V)$ if $W(T)\subseteq W$

Invertible (or) Regular: An element $T\in A(V)$ is said to be invertible (or) regular. If there exist an element $S\in A(V)$ such that $ST = TS = 1$

Similar Linear Transformation: The Linear transformation $S,T\in A(V)$ is said to be similar transformation if there exist an invertible element $C\in A(V)$ such that $T\in CSC^{-1}$ then we say that *S* and *T* are similar to each other

Similar matrices: Let F_n be the set of all nxn matrices over *F*. The matrices $A, B\in F_n$ are said to similar if there exist an invertible matrix $C\in F_n$ such that $B=CAC^{-1}$

Minimal Polynomial: Let *V* be a *n*-dimensional vector space over *F* than for any element $T\in A(V)$ there exist a non-trivial polynomial $q(x)\in F(x)$ such that $q(T) = 0$

A non-trivial polynomial of lowest degree satisfying this property is called the minimal polynomial of *T* over *F*

Result: If $p(x)$ is the minimal polynomial of *T* and if *T* satisfies $h(x)\in F(x)$ then $p(x)$ is the divisor of $h(x)$

Proof: Given that $p(x)$ is the minimal polynomial of *T*.

Therefore $p(x)$ is the least degree polynomial of *T* and $p(T) = 0$. Also given that *T* satisfies $h(x)$

Therefore $h(T) = 0$

Since $p(x), h(x)\in F(x)$ there exist $q(x), r(x)\in F(x)$ such that $h(x)=p(x)q(x)+r(x)$

$\Rightarrow$ either $r(x) = 0$ (or) deg $r(x) <$ deg $p(x)$ since $h(T) = 0$

$\Rightarrow h(T)=p(T)q(T)+r(T)$

Now $r(T) = 0$ we get $h(x)=p(x)q(x)\Rightarrow p(x) / h(x)$

Hence $p(x)$ is a divisor of $h(x)$

Lemma: 6.4.1

If $W \subset V$ is invariant under T then T induces a linear mapping $\overline{T}$ on V/W defined by $(v+W)\overline{T} = vT+W$. If T satisfies the polynomial $q(x) \in F(x)$ then so does $\overline{T}$ (or)

If $p_1(x)$ is the minimal polynomial for $\overline{T}$ over F and if $p(x)$ is that for T then $p_1(x)/p(x)$

Proof:

Given that $W \subset V$ is invariant under $T \Rightarrow W(T) \subseteq W$

Define the mapping $\overline{T} : \frac{V}{W} \to \frac{V}{W}$ by $(v+W)\overline{T} = vT+W$

(i) To prove $\overline{T}$ is well defined

Let $v_1 + W,\, v_2 + W \in \frac{V}{W}$ such that $v_1 + W = v_2 + W$

$\Rightarrow v_1 - v_2 + W = W \Rightarrow v_1 - v_2 \in W$

$\Rightarrow (v_1 - v_2)T \in WT \subset W$

$v_1T - v_2T + W = W$

$(v_1T + W) - (v_2T + W) = W$

$(v_1T + W) = (v_2T + W)$

$(v_1 + W)\overline{T} = (v_2 + W)\overline{T}$

Therefore $\overline{T}$ is well defined.

(ii) To Prove $\overline{T}$ is a linear transformation

(1) $$\begin{aligned}(v_1 + W + v_2 + W)\overline{T} &= v_1T + v_2T + W \\ &= (v_1 + W)\overline{T} + (v_2 + W)\overline{T}\end{aligned}$$

(2) $$\begin{aligned}\alpha(v+W)\overline{T} &= \alpha(vT+W) \\ &= \alpha vT + W = (\alpha v + W)\overline{T}\end{aligned}$$

Therefore $\overline{T}$ is a linear transformation V / W

Let us take $q(x) = \alpha_\circ + \alpha_1 x + ... + \alpha_m x^m$ be minimal polynomial for T and its satisfy $q(T) = 0$

Now q($\overline{T}$) = 0

Consider, $(v_1 + W)\overline{T}^2 = vT^2 + W = (v + W)\overline{T}^2$

$\Rightarrow \overline{T^2} = (\overline{T})^2$

Similarly we can prove $\overline{T^k} = (\overline{T})^k$

Now consider $(v + W)q(\overline{T}) = vq(T) + W$

$$= v(\alpha_\circ + \alpha_1 T + ... + \alpha_m T^m) + W$$
$$= \alpha_\circ (v + W) + \alpha_1 (vT + W) + ... + \alpha_m (vT^m + W)$$
$$= \alpha_\circ (v + W) + \alpha_1 (v + W)\overline{T} + ... + \alpha_m (v + W)\overline{T}^m$$
$$= (v + W)(\alpha_\circ + \alpha_1 \overline{T} + ... + \alpha_m \overline{T}^m)$$

$$(v + W)\overline{q(T)} = (v + W)q(\overline{T}) \Rightarrow \overline{q(T)} = q(\overline{T})$$

Therefore for any $q(x) \in F(x)$ with q(T) = 0, Since $\overline{0}$ is the 0 transformation on V / W and have $\overline{q(T)} = q(\overline{T}) = 0$

$\overline{T}$ satisfies the minimal polynomial $q(x) \in F(x)$ then by using the result " If $p(x)$ is the minimal polynomial of T and if T satisfies $h(x)$ then $p(x)$ is the divisor of $h(x)$"

We get $p_1(x) / q(x)$

Therefore $p(x)$ is the minimal polynomial for T over F then $p(T) = 0$ hence p($\overline{T}$) = 0

Again by using the result $p_1(x) / p(x)$

Definition: If $T \in A(V) \& \lambda \in F$ is called a characteristic root (or) Eigen value of T then $\lambda - T$ is singular

Definition: The matrix A is called triangular if all the entries of above the main diagonal (or) above the main diagonal are zero

Definition: If T is linear transformation on V over F then matrix of T in the basis $\{v_1, v_2, ...v_n\}$ if triangular if

$$v_1T = \alpha_{11}v_1$$
$$v_2T = \alpha_{21}v_1 + \alpha_{22}v_2$$
$$.........$$
$$v_nT = \alpha_{n1}v_1 + \alpha_{n2}v_2 + ... + \alpha_{nn}v_n$$

Theorem: 6.4.1

If $T \in A(V)$ has all its characteristic root in F then there is a basis of V in which the matrix of T is triangular

Proof:

We shall prove this theorem by induction on n, where n is the dimension of V over F that is $\dim_F V = n$

Step 1:

Let $\dim_F V = 1$ then V has the basis with 1 element. Therefore $m(T)$ is a one by one matrix. Hence the theorem is true for $n = 1$

Step 2:

Assume that the theorem is true for all vector spaces over F of dimension $n - 1$

Step 3:

Let V be of dimension n over F

To prove the matrix of T is triangular in the basis of V over F

Let $\lambda_1 \in F$ be the characteristic root of T then there exist a non-zero vector v_1 such that $v_1T = \lambda_1 v_1$ ….(1)

Since by the property of characteristic root $\lambda \in F, T \in A(V)$ then $vT = \lambda v, v \neq 0$

Let $W = \{\alpha v_1 / \alpha \in F\}$ …….(2)

Here W is a one-dimensional subspace of V

To prove W is invariant under T

That is to prove $W(T) \subseteq W$

Let $\alpha v_1 T \in wT$

$\alpha v_1 T = (\alpha \lambda_1) v_1 \in W$ by equation(1)

Therefore $W(T) \subseteq W$

Hence W is invariant under T

Let $\overline{V} = \frac{V}{W}$, $\therefore \dim \overline{V} = \dim V - \dim W = n - 1$

By lemma 6.4.1, *T* induces in linear transformation $\overline{T}$ on $\overline{V}$ whose minimal polynomial over *F* divides the minimal polynomial of *T* over *F*

Thus all the roots of the minimal polynomial of $\overline{T}$ being the roots of the minimal polynomial of *T*, must be lie in *F*

$\overline{T}$ on $\overline{V}$ satisfies the hypothesis of the theorem, since $\overline{V}$ is n – 1 dimensional over *F*, our induction hypothesis there is a basis $\overline{v_2}, \overline{v_3}, ...\overline{v_n}$ over *F* such that

$$\begin{aligned}
&\overline{v_2}\overline{T} = \alpha_{22}\overline{v_2} \\
&\overline{v_3}\overline{T} = \alpha_{32}\overline{v_2} + \alpha_{33}\overline{v_3} \\
&......... \\
&\overline{v_n}\overline{T} = \alpha_{n2}\overline{v_2} + \alpha_{n3}\overline{v_3} + ... + \alpha_{nn}\overline{v_n}
\end{aligned}$$

Let $\{v_2, v_3, ...v_n\}$ be the elements of *V* into $\overline{v_2}, \overline{v_3}, ...\overline{v_n}$ respectively

To prove $\{v_1, v_2, v_3, ...v_n\}$ forms a basis of *V* over *F*

That is to prove that (i) $\{v_1, v_2, v_3, ...v_n\}$ are linearly independent (ii) Any element $v \in V$ is a linear combination of $\{v_1, v_2, v_3, ...v_n\}$

Let $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0, \ \ \alpha_i \in F$ …………….(3)

Now to prove all constants $\alpha_i = 0$

Equation (3) implies $\alpha_2 v_2 + ... + \alpha_n v_n = -\alpha_1 v_1 \in W$

$\alpha_2(v_2 + W) + ... + \alpha_n(v_n + W) = W$

$\alpha_2\overline{v_2} + ... + \alpha_n\overline{v_n} = W$

Since $\overline{v_2}, \overline{v_3}, ...\overline{v_n}$ is a basis of V / W and $\alpha_2\overline{v_2} + ... + \alpha_n\overline{v_n} = W,\ \alpha_2 = \alpha_3 = ...\alpha_n = 0$

Therefore eqn(3) becomes $\alpha_1 v_1 = 0 \Rightarrow \alpha_1 = 0 \because v_1 \neq 0$

Let $v \in V$ then $\bar{v} = v + W \in \frac{V}{W} = \overline{V}$ ....(4)

Let $v = \sum_{i=2}^{n} \alpha_i v_i$

$$v + W = \sum_{i=2}^{n} \alpha_i v_i + W$$

$$v - \sum_{i=2}^{n} \alpha_i v_i + W = W$$

$$v = \alpha_1 v_1 + \sum_{i=2}^{n} \alpha_i v_i$$

$$v = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$$

Hence any element $v \in V$ is a linear combination of $\{v_1, v_2, v_3, ...v_n\}$

Now to prove the matrix of T is triangular in the basis $\{v_1, v_2, v_3, ...v_n\}$

Now by (1) $v_1 T = \lambda_1 v_1 = \alpha_{11} v_1$

$$\overline{v_2}\,\overline{T} = \alpha_{22}\overline{v_2}$$

$$v_2 T - \alpha_{22} v_2 + W = W$$

$$v_2 T - \alpha_{22} v_2 \in W = W$$

$$v_2 T = \alpha_{21} v_1 + \alpha_{22} v_2$$

$$v_3 T = \alpha_{31} v_1 + \alpha_{32} v_2 + \alpha_{33} v_3$$

Similarly we can prove that $v_n T = \alpha_{n1} v_1 + \alpha_{n2} v_2 + ... + \alpha_{nn} v_n$

Hence $m(T) = \begin{pmatrix} \alpha_{11} & 0 & 0.... & 0 \\ \alpha_{21} & \alpha_{22} & 0.... & 0 \\ \alpha_{31} & \alpha_{32} & \alpha_{33}.. & 0 \\ ..... & & & \\ \alpha_{n1} & \alpha_{n2} & \alpha_{n3}.... & \alpha_{nn} \end{pmatrix}$

Therefore $m(T)$ is triangular

Alternate form of theorem 6.4.1:

If the matrix $A \in F_n$ has all its characteristic roots in F then there is a matrix $C \in F_n$ such that CAC^{-1} is triangular

Theorem 6.4.2:

If V is an n-dimensional vector space over F and if $T \in A(V)$ all has its characteristic roots in F then T satisfies the polynomial of degree n over F

Proof: Let V be an n-dimensional vector space over F

Suppose that $T \in A(V)$ has all its characteristic roots in F then by theorem 6.4.1, we can find a basis $\{v_1, v_2, v_3, ...v_n\}$ of V over F such that

$v_1 T = \lambda_1 v_1 = \alpha_{11} v_1$

$v_2 T = \alpha_{21} v_1 + \alpha_{22} v_2$

$v_3 T = \alpha_{31} v_1 + \alpha_{32} v_2 + \alpha_{33} v_3$

Here the above can be rewritten as

$v_1 T = \lambda_1 v_1$
$v_1 (T - \lambda_1) = 0 \ldots\ldots(1)$

Also $v_2 (T - \lambda_2) = \alpha_{21} v_1 \ldots\ldots(2)$

Similarly we can write $v_n (T - \lambda_n) = \alpha_{n1} v_1 + \alpha_{n2} v_2 + ... + \alpha_{nn-1} v_{n-1}$

Also $(T - \lambda_1)(T - \lambda_2) = (T - \lambda_2)(T - \lambda_1)$

Continuing in this way, we get

$(T-\lambda_1)(T-\lambda_2).......(T-\lambda_n)=0$

Multiplying both side by $(T-\lambda_1)$ in eqn(2) we get

$v_2(T-\lambda_2)(T-\lambda_1)=\alpha_{21}v_1(T-\lambda_1)=0$

Proceeding in this manner we get

$v_n(T-\lambda_n).......(T-\lambda_1)=0$

Let $S=(T-\lambda_1)(T-\lambda_2).......(T-\lambda_n)$ which satisfies

$v_1S=0,\ v_2S=0,......v_nS=0$

Hence $S = 0$, $v_i \neq 0$, $i = 1, 2,3,\ldots..n$

$(T-\lambda_1)(T-\lambda_2).......(T-\lambda_n)=0$

Therefore T is satisfies the polynomial $(x-\lambda_1)(x-\lambda_2).......(x-\lambda_n)\in F[x]$ of degree n

Hence T satisfies the polynomial of degree n over F

Section 6.5

Canonical Transformation – Nilpotent Transformation

Lemma: 6.5.1

If $V = v_1 \oplus v_2 \oplus \ldots\ldots \oplus v_k$ where each subspace v_i is of dimension n_i and is invariant under T, then a basis of V can be found so that, the matrix of T in this basis if of the form,

$$\begin{pmatrix} A_1 & 0 \ldots & 0 \\ 0 & A_2 \ldots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 \ldots & A_k \end{pmatrix}$$

Where each A_i is $n_i \times m_i$ matrix and the linear transformation induced by T on v_i.

Proof:

Choose a basis V as follows:

$\{v_1^{(1)}, v_2^{(1)} \ldots.. v_{n1}^{(1)}\}$ is a basis of V_1

$\{v_1^{(2)}, v_2^{(2)} \ldots.. v_{n2}^{(2)}\}$ is a basis of $V_2 \ldots\ldots$

$\{v_1^{(n)}, v_2^{(n)} \ldots.. v_{nk}^{(n)}\}$ is a basis of V_k

Since each V_i is invariant under T, $v_j^{(i)} T \in V_i$, i = 1..k and so it is a linear combination of $v_1^{(i)}$, $v_2^{(i)} \ldots.. v_{ni}^{(i)}$. thus the matrix of T this basis is the desired form.

ie, the matrix of T, in this basis is of the form $n_i \times n_i$

Let this matix be A_i. ie, each $A_i$is a matrix of T_i and T_i is the linear transformation induced by T on V_i

Hence we get, the matrix of T in the above basis of V as

$$\begin{pmatrix} A_1 & 0 \ldots & 0 \\ 0 & A_2 \ldots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 \ldots & A_k \end{pmatrix}$$

Hence the theorem.

Definition of Nilpotent:

An element T ∈ A(V) is said to be an invertable then there exist an element S ∈ A(V) such that ST = TS = 1

Lemma: 6.5.2.

If T ∈ A(V) is nilpotent then $\propto_0 . \propto_0 + \propto_1 T + \cdots . \propto_m T^m$ where the $\propto_i \in$ F is invertable $\propto_0 \neq 0$.

Proof:

Suppose that T is nilpotent, the definition of nilpotent have exist an integer r such that $\propto^r = 0$.

To prove $\propto_0 + \propto_1 T + \cdots . \propto_m T^m$ is invertible if $\propto_0 \neq 0$.

Let S = $\propto_0 + \propto_1 T + \cdots . \propto_m T^m$. Now to prove $\propto_0 + S$ is invertible.

Consider, $S^r = (\propto_1 T + \cdots . \propto_m T^m)^r$

$= (T(\propto_1 + \cdots . \propto_m T^m)^r)$

$= T^r(\propto_1 + \cdots . \propto_m T^m)^r$

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

Consider, $(\propto_0 + S) = \left(\frac{1}{\propto_0} - \frac{S}{{\propto_0}^2} + \frac{S^2}{{\propto_0}^3} + \cdots . + \frac{(-1)^{r-1}s^{r-1}}{{\propto_0}^r}\right)$

$= 1 - \frac{S}{\propto_0} + \ldots . . + \frac{(-1)^{r-1}s^{r-1}}{{\propto_0}^{r-1}} + \frac{S}{\propto_0} - \frac{S^2}{{\propto_0}^2} + \ldots . + \frac{(-1)^{r-1}s^r}{{\propto_0}^r}$

$= 1 + \frac{(-1)^{r-1}s^r}{{\propto_0}^r}$

$= 1$ (since $S^r = 0$)

Hence $\propto_0 + S$ is invertible. $\propto_0 + \propto_1 T + \cdots . \propto_m T^m$ is invertible if $\propto_0 \neq 0$.

Definition:

If $T \in A(V)$ is nilpotent then k is called the index of nilpotent of T. If $T^k = 0$ but $T^{k-1} \neq 0$.

Theorem 6.5.1:

If $T \in A(V)$ is nilpotent, of index of nilpotent n_1 then a basis of V can be found such that the matrix of T in this basis of the form

$$\begin{pmatrix} A_1 & 0 \ldots & 0 \\ 0 & A_2 \ldots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 \ldots & A_k \end{pmatrix}$$

Where $n_1 \geq n_2 \geq \ldots \ldots . n_r$ and where $n_1 + \ldots . . + n_r = \dim_F V$

Proof:

Given that $T \in A(V)$ is nilpotent. $T^n = 0$

Also given that, T is of index of nilpotents n_1. $T^{n1} = 0$ but $T^{n1-1} \neq 0$.----(1)

Now we can find a vector $v \in V$ such that $v\,T^{n1-1} \neq 0$.

We claim that the vectors v, v T…. $v\,T^{n1-1}$ are linearly independent over F

Suppose that the above vectors are not linearly independent then

$\propto_1 v + \propto_2 vT + \cdots . \propto_{n1} v\, T^{n1-1} = 0$ where $\propto_i \in F$, here all the ∝'s are not zero. Let ∝'s be the first non zero coefficient of the above equation.

$\propto s\, v\, T^{s-1} + \ldots .. + \propto_{n1} v\, T^{n1-1} = 0$

$v\, T^{s-1}(\propto s + \ldots .. + \propto_{n1} T^{n1-s}) = 0$ ----------(2)

since $\propto s \neq 0$ by using lemma 6.5.2 , we get$(\propto s + \propto sT + \ldots .. + \propto_{n1} T^{n1-s})$ is invertible.

Equation (2) becomes

$vT^{s-1} I = 0$

$vT^{s-1} I\, I^{-1} = 0\, I^{-1} = 0$

$vT^{s-1} = 0$. Which is a contradiction to $vT^{n1-1} \neq 0$ for $s < n_1$.

Hence v, vT, …. vT^{n1-1} are lineary independent . Let v_1 be the subspace of V spanned by

$v_1 = v$, $v_2 = vT$ …..$v_{n1} = vT^{n1-1}$

$v_1 T \subset V$. Hence v_1 is invariant under T

Thus in this bais the linear transformation induced by T on v_1 has the matrix M_{n1}

$$M_{n1} = \begin{pmatrix} 0 & 1 \ldots & 0 \\ 0 & 0 \ldots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 \ldots & 1 \end{pmatrix}$$

Now to prove the rest of the theorem we need the following lemma's

Lemma: 6.5.3.

If $u \in V_1$ is such that $u\, vT^{n1-k} = 0$ where $0<k\leq n_1$ then $u = uoT^k$ some $u_o \in V_1$

Proof:

Given that $u \in V_1$ and V_1 is a subspace of V spanned by $v, vT, \ldots vT^{n1-1}$. Also given that

$u\, T^{n1-k} = 0$.-----(3)

Then $u = \propto_1 v + \propto_2 vT + \cdots . \propto_{n1} v\, T^{n1-1}$

$u\, T^{n1-k} = (\propto_1 v + \propto_2 vT + \cdots . \propto_{n1} v\, T^{n1-1})\, T^{n1-k}$

$= \propto_1 vT^{n1-k} + \propto_2 vT^{n1-k+1} + \cdots . \propto_{n1} v\, T^{2n1-k-1}$

$=0$

$vT^{n1-k}, \ldots\ldots v\, T^{2n1-k-1}$ are linearly independent

Hence $\propto_1 = \propto_2 = \cdots . = \propto_k = 0$

$u = \propto_{(k+1)} vT^k + \ldots\ldots + \propto_{n1} T^{n1-1} = uoT^k$

$uo = \propto_{(k+1)} v + \ldots\ldots + \propto_{n1} T^{n1-k-1} \in V_1$

Lemma: 6.5.4.

There exist a subspace W of V, invariant under T such that $V = v_1 \oplus w$

Proof:

Let w be a subspace of v which is the largest possible such that

(i) $V_1 \cap W = \{0\}$

(ii) W is invariant under T

To show that $V = V_1 + W$. where V_1 is the subspace of V which is invariant under T

Suppose not $V \neq V_1 + W$. Then there exist an element $z \in V$ such that z does not belongs to $V_1 + W$. since $T^{n1} = 0$, there exist an integer k , $o< k \leq n_1$ such that $zT^k \in V_1 + W$ and such that zT^i does not belongs to $V_1 + W$, for $i <k$ ----------(4)

Thus $zT^k = u + w$ where $u \in V_1$ & $w \in W$ --------(5)

$zT^{n1} = 0$

$(zT^k) T^{n1-k} = 0$

$(u+w)T^{n1-k} = 0$

$u T^{n1-k} + w T^{n1-k} = 0$ -------(6)

Since W is invariant under T, $uT \in V_{1,}$ $wT \in W$

$u T^{n1-k} \in V_1$ & $w T^{n1-k} \in W$

Equation (6) becomes

$u T^{n1-k} + w T^{n1-k} \in V_1 \cap W = \{0\}$

$u T^{n1-k} = - w T^{n1-k} \in V_1 \cap W = \{0\}$

$u T^{n1-k} = 0$

Now by using lemma 6.5.3.

There exist an integer $u_o \in V_1$ Show that $u = uoT^k$

Equation (5) becomes

$zT^k = u+w$

$= uoT^k + w$

$zT^k = uoT^k = w$

$T^k(z – uo) = w \in W$

Let $u_1 = z – uo$ then $T^k uo = w \in W$

Since W is invariant under T, $wT \subset W$

$u.T^k\ T \in W$

$u_1 T^m \in W$, m>k

on the other hand if i > k then,

$u_1 T^1 = (z - uo)\ T^i$

$= (zT^i - uo\ T^i)$

Does not contains $V_1 + W$

For otherwise $u_1 T^i \in V_1 + W$. Which is a contradiction to equation (4)

Let W be the subspace of V spanned by W & $z_{1,}\ z_1 T \ldots.\ z_1 T^{k-1}$

Since $w \in W$ and $W \subset w_1$ Then dim W < dim w_1

dim w_1 must be larger than that of W

Since $z_1 T^k \in W$

If W is invariant under T, w_1 must be invariant under T

To prove $w_1 T \in W_1$ Where $w_1 \in W_1$. Here $w_1 = w_0 + \propto_1 z_1 T + \ldots + \propto_k\ z_1 T^{k-1}$ ----(7)

$w_1 T = w_0 T + \propto_1 z_1 T^2 + \ldots + \propto_k\ z_1 T^k$

$w_0 T \in W$ & $z_1 T^k \in W$

$w_1 T \in W_1$

hence W_1 is invariant under T. We have $V_1 \cap W_1 \neq \{0\}$, otherwise this will affect the maximum matrix of W. There exist an element $w_0 \in W$ is of the form, $\propto_0 + \propto_1 z_1 + \ldots + \propto_k$ $z_1 T^k \neq 0$ ---(8) in $V_1 \cap W$ have all the scalars $\propto_1 \ldots . \propto_k$ are non- zero. But $w_0 \in W \subset W_1$

$w_0 \neq 0$, which is a contradiction to our assumption that $V_1 \cap W_1 = \{0\}$,

Let $\propto$s be the first non –zero coefficient of equation (7)

$w_0 + \propto_1 z_1 + \ldots.. + \propto_k z_1 T^{k-1} \neq 0 \in V_1$

$w_0 + z_1 T^{s-1} (\propto_s + \ldots.. + \propto_k z_1 T^{k-s}) \in V_1$

Since $\propto s \neq 0$ by using lemma 6.5.2., we get

$\propto_s + \propto_{s+1} T + \ldots.. + \propto_k z_1 T^{k-s} = \frac{1}{R}$----(9)

Equation (9) becomes $w_0 + z_1 T^{s-1} = \frac{1}{R} \in V_1$

ie) $w_0 R + z_1 T^{s-1} \in V_1 R \subset V_1$

ie) $z_1 T^{s-1} \in V_1 + W$, since $s-1<k$ which is impossible.

Our assumption that $V_1 + W \neq V$. $V = V_1 + W$. Already we have $V_1 \cap W = \{0\}$. Hence we get, $V = V_1 \oplus W$.

Proof the main theorem, here $V = V_1 \oplus W$. Where W is invariant under T, Then by using lemma 6.5.1., the matrix of T in the basis $v_1, v_2, \ldots. v_n$ has the form $\begin{pmatrix} M_{n1} & 0 \\ 0 & n_2 \end{pmatrix}$. Where A_2 is the matrix of T_2 & T_2 is the linear transformation induced by T on W. since $T^{n1} = 0$, $T^{n2} = 0$ for some $n_2 \leq n_1$ repeating the above argument used for T on V for T_2 on W. Hence we get a basis of V in which the matrix of is the form

$$\begin{pmatrix} M_{n1} & 0 \ldots & 0 \\ 0 & M_{n2} \ldots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 \ldots & nr \end{pmatrix}$$

Where $n_1 \geq n_2 \geq \ldots\ldots \geq n_r$. Since the size of the matrix is $n \times n$. Hence we have,

$n_1 + n_2 + \ldots\ldots + n_r = \dim V$

(ie) $\dim V = n$

Hence the Theorem

Definition – 1:

The integer $n_1, n_2, \ldots\ldots n_r$ are called the invariants of T

Definition – 2:

If $T\in A(V)$ is nilpotent, the subspace M of V is of dimension m which is invariant under T is called cyclic with respect to T. If (i) $MT^m = 0$, $MT^{m-1}\neq 0$

(ii)There is an element $z\in M$ such that $z, zT,\ldots ZT^{m-1}$form a basis of M.

Lemma: 6.5.5.

If M is of dimension m is cyclic with respect to T. Then the dimension of MT^k is m-k for all $h\subseteq M$

Proof:

Given that M is cyclic with respect to T and M is of dimension m.

To prove that dim $MT^k = m-k$, for all $k\leq m$.

Since M is cyclic with respect to then by definition of cyclic

(i) $MT^m = 0$, $MT^{m-1}\neq 0$

(ii)There is an element $z\in M$ such that $z, zT,\ldots ZT^{m-1}$form a basis of M.

Claim:

$z, zT, \ldots\ldots zT^{m-1}$ of M leads to a basis $zT^k,zT^{k+1},\ldots zT^{m-1}$of mT^k.

First we want to prove, zT^k, $zT^{k+1}....zT^{m-1}$ are linearly independent

Let $\propto_1 zT^k+\propto_2 zT^{k+1}+\ldots+\propto_{m-k} zT^{m-1}= 0$

$0.z+0.zT+\ldots..\propto_1 zT^k+\propto_2 zT^{k+1}+\ldots+\propto_{m-k} zT^{m-1}= 0$

$\propto_I = o$ for all i

$\{zT^k,zT^{k+1},\ldots zT^{m-1}\}$ is linearly independent

Now to prove every element of mT^k is linear combination of $\{zT^k,zT^{k+1},\ldots zT^{m-1}\}$. Let $x\in M$

ie) $x = \propto_1 z+\propto_2 zT^k+\ldots+\propto_m zT^{m-1}$

$xT^k = \propto_1 zT^k + \propto_2 zT^{k+1} + \ldots + \propto_m zT^{m+k-1}$

$xT^k \in MT^k$

Every element of MT^k is a linear combination of $\{zT^k, zT^{k+1}, \ldots zT^{m-1}\}$ form a basis of MT^k.

dim MT^k = m- k

Hence the lemma.

Theorem: 6.5.2.

Two nilpotent linear transformation are similar iff they have the sae invariants.

Proof:

Necessary Part:

Let T& S be to similar nilpotent linear transformations.

To prove that, T & S have the same invariants

Given that T is a nilpotent linear transformation. By using 6.5.1. theorem, we can find a integers $n_1 \geq n_2 \geq \ldots \geq n_r$ and subspaces $v_1, v_2, \ldots v_r$ of V cyclic with respect to T and of dimensions $n_1, n_2, .. n_r$ respectively such that $V = v_1 \oplus v_2 \oplus \ldots \oplus v_r$

Again given that s is a nilpotent linear transformation then by using theorem 6.5.1.

We can find another integer, $m_1 \geq m_2 \geq \ldots m_s$ and subspaces $u_1, u_2, \ldots u_s$ of cyclic with respect to S and such of dimensions $m_1, m_2, \ldots m_s$ respectively such that that $V = U_1 \oplus U_2 \oplus \ldots \oplus U_s$

Claim:

$r = s$, $n_1 = m_1, n_2 = m_2 \ldots n_r = m_s$. Let us assume that the above one is not true. (ie) there exist atleast one integer k such that $nk \neq mk$.

Let I be the first integer such that $n_i \neq m_i$, where $n_1 = m_1, n_2 = m_2 \ldots n_{i-1} = m_{i-1}$ without loss of generality, let $m_i < n_i$. Since $V = v_1 \oplus v_2 \oplus \ldots \oplus v_r$ Now $VT^{mi} = v_1 T^{mi} \oplus v_2 T^{mi} \oplus \ldots \oplus v_r T^{mi}$

dim (VT^{mi}) = dim $v_1 T^{mi} + \ldots\ldots +$ dim $v_r T^{mi}$

$\geq (n_1 - m_i) + (n_2 - m_i) + \ldots + (n_r - m_i)$ also $V = U_1 \oplus U_2 \oplus_{\ldots} \oplus U_s$

Now $VT^{mi} = U_1 T^{mi} \oplus U_2 T^{mi} \oplus_{\ldots} \oplus U_s T^{mi}$

$\dim (VT^{mi}) = \dim U_1T^{mi} + \ldots\ldots + \dim U_sT^{mi}$

$\geq (m_1 - m_i) + (m_2 - m_i) + \ldots + (m_s - m_i)$, I is $n_1 = m_{1,}\ n_2 = m_2 \ldots . n_i = m_i = 1$

Where $VT^{mi} = (n_1 - m_i) + (n_2 - m_i) + \ldots + (n_{i-1} - m_i)$

Which is contradiction to dimension of , $\dim(VT^{mi}) \geq (n_i - m_i) \ldots . (n_r - m_i)$

Thus there is a unique set of integer, $n_1 \geq n_2 \geq_{\ldots\ldots} \geq n_r$. Such that V is the direct sum of subspaces, cyclic with respect to T of dimensions $n_1, n_{2,} \ldots . n_r$ thus they have the same invariants.

Sufficient Part:

Assume that two nilpotent linear transformation T & S have the same invariant. To prove that T & S are similar.

Let the invariants T & S be $n_1 \geq n_2 \geq_{\ldots\ldots} \geq n_r$, then by theorem 6.5.1. , there exist a basis $\{v_1, v_2 .. v_n\}$ and $\{w_1, w_{2,} .. w_n\}$ of V. Such that the matrix of T and the matrix of S are equal

$$M(T) = \begin{pmatrix} M_{n1} & 0 \ldots & 0 \\ 0 & M_{n2} \ldots & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 \ldots & M_{nr} \end{pmatrix}$$

But if A is a linear transformation defined on V by $v_iA = w_i$. Then $S = ATA^{-1}$(Since by using the result. Let T & S be linear transformation defined on V such that the matrix of T in one basis is equal to the matrix of S in another basis. Then a transformation A on B such that $T = ASA^{-1}$)

Thus T and S are similar linear transformations.

6.6 Canonical Forms: A Decomposition of V: Jordan Form

Lemma 6.6.1

Suppose that $V = V_1 \oplus V_2$, where V_1 and V_2 are subspaces of V invariant under T.

Let T_1 and T_2 be the linear transformations induced by T on V_1 and V_2 respectively. If the minimal polynomial of T_1 over F is $\mathrm{p}_1(\mathrm{x})$ while that of T_2 is $\mathrm{p}_2(\mathrm{x})$, then the minimal polynomial for T over F is the least common multiple of $\mathrm{p}_1(\mathrm{x})$ and $\mathrm{p}_2(\mathrm{x})$.

Proof:

Given that $V = V_1 \oplus V_2$, where V_1 and V_2 are subspaces of V invariant under T.

Let $p(x)$ be the minimal polynomial for T over F. Then $p(T) = 0$.

Therefore, $p(\mathrm{T}_1) = 0$ and $p(\mathrm{T}_2) = 0$.

Since $\mathrm{p}_1(\mathrm{x})$ is a minimal polynomial of T_1, we have $\mathrm{p}_1(\mathrm{T}_1) = 0$, which implies $\mathrm{p}_1(\mathrm{x})|p(x)$.

Similarly, $\mathrm{p}_2(\mathrm{x})$ is a minimal polynomial of T_2, we have $\mathrm{p}_2(\mathrm{T}_2) = 0$, which implies $\mathrm{p}_2(\mathrm{x})|p(x)$.

Hence, the L.C.M of $\mathrm{p}_1(\mathrm{x})$ and $\mathrm{p}_2(\mathrm{x})$ must divide $p(x)$.

Let $q(x)$ be the L.C.M of $\mathrm{p}_1(\mathrm{x})$ and $\mathrm{p}_2(\mathrm{x})$ then $q(\mathrm{x})|p(x)$ __________(1)

Since $q(x)$ is the L.C.M of $\mathrm{p}_1(\mathrm{x})$ and $\mathrm{p}_2(\mathrm{x})$, we have $\mathrm{p}_1(\mathrm{x})|q(x)$.

$\Longrightarrow q(x) = \mathrm{p}_1(\mathrm{x})h(x)$ where $h(x) \in F[x]$.

Also, $q(\mathrm{T}_1) = \mathrm{p}_1(\mathrm{T}_1)h(\mathrm{T}_1) \Longrightarrow q(\mathrm{T}_1) = 0$, (since $\mathrm{p}_1(\mathrm{T}_1) = 0$)

Consider, $v_1 \in V_1$, then $v_1 q(T) = v_1 q(\mathrm{T}_1)$,

$= v_1 \mathrm{p}_1(\mathrm{T}_1)h(\mathrm{T}_1) = 0$, (since $\mathrm{p}_1(\mathrm{T}_1) = 0$).

Similarly, $v_2 \in V_2$, then $v_2 q(T) = v_2 q(\mathrm{T}_2)$,

$= v_2 \mathrm{p}_2(\mathrm{T}_2)h(\mathrm{T}_2) = 0$, (since $\mathrm{p}_2(\mathrm{T}_2) = 0$).

Let $v \in V$, then $v_1 + v_2 = v, v_1 \in V_1$ and $v_2 \in V_2$

Now, $vq(T) = (v_1 + v_2)q(T)$

$= v_1 q(\mathrm{T}) + v_2 q(\mathrm{T})$

$vq(T) = 0 \implies q(T) = 0$ __________________(2)

From (1) and (2),

$q(x)$ is the minimal polynomial of T which is the L.C.M of $p_1(x)$ and $p_2(x)$.

Corollary:

If $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$, where V_i is invariant under T and if $p_i(x)$ is the minimal polynomial over F of T_i, the linear transformation induced by T on V_i, then the minimal polynomial of T over F is the least common multiple of $p_1(x), p_2(x) \dots, p_k(x)$.

Proof:

We prove this result by induction on k.

For $k = 1$, the result is obvious.

For $k = 2$ then $V = V_1 \oplus V_2$.

$\therefore$ By using previous theorem, we get the result.

Assume that, the result is true for $k - 1$, then by induction hypothesis the minimal polynomial $p_i(x)$ of T_i is the L.C.M of $p_1(x), p_2(x) \dots, p_{k-1}(x)$.

Now, $T = T_i + T_k$, then by using previous lemma,

The minimal polynomial of T over F is the L.C.M of $p_1(x), p_2(x) \dots, p_{k-1}(x)$.

Theorem: 6.6.1 [Jordan Theorem]

For each $i = 1,2, \dots k, V_i \neq (0)$ and $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$. The minimal polynomial of T_i is $q_i(x)^{l_i}$. **(OR)** Let $T \in A(V)$ and $p(x) = q_1(x)^{l_1}. q_2(x)^{l_2} \dots q_k(x)^{l_k}$, where $q_i(x)^{l_i}$ are distinct irreducible polynomial over F be the minimal polynomial for T over F then $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$, where each $V_i \neq (0)$ and $T(V_i) \subseteq V_i$ is a subspace of V is invariant under T. Then the minimal polynomial for T_i is the linear transformation induced by T on V_i is $q_i(x)^{l_i}$.

Proof:

Claim 1

To prove, each V_i is invariant under T.

If $k = 1$, then $V = V_1$ and $p(x) = q_1(x)^{l_1}$.

Then, $p(T) = q_1(T)^{l_1} = 0$.

$\Longrightarrow$ V is the subspace and T is the minimal $p(x)$, a power of the irreducible polynomial.

$\therefore$ The theorem is true for $k = 1$.

Let $k > 1$, then $p(x) = q_1(x)^{l_1}.\, q_2(x)^{l_2} \ldots q_k(x)^{l_k}$.

Let $V_1 = \{v \in V | v q_1(T)^{l_1} = 0\}$

$V_2 = \{v \in V | v q_2(T)^{l_2} = 0\}$

$\vdots$

$V_i = \{v \in V | v q_i(T)^{l_i} = 0\}$

$\vdots$

$V_k = \{v \in V | v q_k(T)^{l_k} = 0\}$

Clearly, $V_1, V_2, \ldots V_k$ are subspaces of V. Also if $v \in V_i$ then $v q_i(T)^{l_i} = 0$.

To prove $vT \in V_i$ for $v \in V_i$, i.e. To prove, $vTq_i(T)^{l_i} = 0$.

Now, $vTq_i(T)^{l_i} = v(q_i(T)^{l_i})T = 0$

$\therefore V_i$ is invariant under T.

Claim 2

Now, $h_1(x) = q_2(x)^{l_2}.\, q_3(x)^{l_3} \ldots q_k(x)^{l_k}$

$h_2(x) = q_1(x)^{l_1}.\, q_3(x)^{l_3} \ldots q_k(x)^{l_k}$

$\vdots$

$h_i(x) = \prod_{j \neq 0} q_j(x)^{l_j}$

$\vdots$

$h_k(x) = \mathrm{q}_1(\mathrm{x})^{\mathrm{l}_1}.\mathrm{q}_3(\mathrm{x})^{\mathrm{l}_3} \ldots \mathrm{q}_{\mathrm{k}-1}(\mathrm{x})^{\mathrm{l}_{\mathrm{k}-1}}$

Since $p(x)$ is the minimal polynomial for T, we have $p(T) = 0$.

Also $de\, g\big(\, h_i(x)\big) < deg\ (p(x))$

$\Longrightarrow\ h_i(T) \neq 0,\ \forall i = 1,2, \ldots k$

$\therefore \exists v_i \in V$ such that $v_i h_i(T) \neq 0$

Let $w_i = v_i h_i(T)$, then

$$w_i \mathrm{q}_\mathrm{i}(\mathrm{T})^{\mathrm{l}_\mathrm{i}} = (v_i h_i(T))\mathrm{q}_\mathrm{i}(\mathrm{T})^{\mathrm{l}_\mathrm{i}}$$

$$= \ v_i p(T)$$

$$w_i \mathrm{q}_\mathrm{i}(\mathrm{T})^{\mathrm{l}_\mathrm{i}} = 0,\ (\because p(T) = 0)$$

$\Longrightarrow w_i \neq 0 \in V_i,$ also $vh_i(T) \neq 0$ and for which $vh_i(T) \in Vh_i(T)$

i.e., $vh_i(T)\mathrm{q}_\mathrm{i}(\mathrm{T})^{\mathrm{l}_\mathrm{i}} = vp(T) = 0$

But $vh_i(T) \neq 0 \in V_i$, we have $v_j h_i(T) = 0, i \neq j$.

Thus, $\mathrm{q}_\mathrm{j}(x)^{\mathrm{l}_\mathrm{j}} | h_i(x)$.

Claim 3

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

We know that, $h_1(x), h_2(x), \ldots h_k(x)$ are distinct irreducible polynomials. Therefore, they are relatively prime.

Hence, we can find a polynomial $a_1(x), a_2(x), \ldots a_k(x) \in F[x]$, such that

$$a_1(x)h_1(x) + a_2(x)h_2(x) + \cdots + a_k(x)h_k(x) = 1$$

$$\Longrightarrow a_1(T)h_1(T) + a_2(T)h_2(T) + \cdots + a_k(T)h_k(T) = 1$$

Now for $v \in V$, we have

$$v(a_1(T)h_1(T) + a_2(T)h_2(T) + \cdots + a_k(T)h_k(T)) = 1.v$$

$$va_1(T)h_1(T) + va_2(T)h_2(T) + \cdots + va_k(T)h_k(T) = v$$

Now, each $va_i(T)h_i(T) \in Vh_i(T)$ and also each $v = v_1 + v_2 + \cdots + v_k$, where each $v_i = va_i(T)h_i(T)$ is in $Vh_i(T)$.

Thus, $V = V_1 + V_2 + \cdots + V_k$

Suppose that, $V_1 + V_2 + \cdots + V_k = 0$ for each $V_i \in V$.

Now, $(V_1 + V_2 + \cdots + V_k)h_1(T) = 0$

Let $v \in V$ then $v = v_1 + v_2 + \cdots + v_k$, then

$(v_1 + v_2 + \cdots + v_k)h_1(T) = 0$

$v_1 h_1(T) + v_2 h_1(T) + \cdots + v_k h_1(T) = 0$

Which implies that, $v_1 h_1(T) = 0$, $[\because v_j h_i(T) = 0,\ for\ i \neq j]$

Also, $v_i q_i(T)^{l_1} = 0$ and $h_1(x), q_1(x)^{l_1}$ are relatively prime, we get $p_1 = 0$.

By the same procedure we get, $v_2 = 0, v_3 = 0, \dots, v_k = 0$

Hence, $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$.

Claim 4

The minimal polynomial for T_i is the linear transformation induced by T on V_i is $q_i(x)^{l_i}$ on V_i.

By $V_i q_i(T)^{l_i} = 0 \Rightarrow q_i(T)^{l_i} = 0$

$\Rightarrow T_i$ satisfies the polynomial $q_i(x)^{l_i}$

$\Rightarrow$ The minimal polynomial for T_i must be the divisor of $q_i(x)^{l_i}$

Of the form $q_i(x)^{f_i}$ where $f_i \leq l_i$

By the **Corollary 6.6.1**, we get ,

The minimal polynomial of T over F is the L.C.M of $q_1(x)^{f_1}, q_2(x)^{f_2}, \dots q_k(x)^{f_k}$.

$\therefore q_1(x)^{l_1} q_2(x)^{l_2} \dots q_k(x)^{l_k} = q_1(x)^{f_1} q_2(x)^{f_2} \dots q_k(x)^{f_k}$

$\Rightarrow l_1 = f_1, l_2 = f_2, \dots l_k = f_k$

Thus the minimal polynomial for T_i is $q_i(x)^{l_i}$.

Corollary:

If all the distinct characteristic root $\lambda_1, \lambda_2, \dots \lambda_k$ of T lie in F then V can be written as $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$ where $V_i = \{v \in V / v(T - \lambda_i)^{l_i} = 0\}$ and where T_i has only one characteristic root λ_i on V_i.

Proof:

By the above **Theorem 6.6.1**,

we have proved that for the minimal polynomial,

$p(x) = q_1(x)^{l_1}, q_2(x)^{l_2}, \dots q_k(x)^{l_k}$, $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$ where

$V_i = \{x \in V / vq_i(T)^{l_i} = 0\}$.

We know that, the characteristic roots of T are the roots of the minimal polynomial $p(x)$, the characteristic roots lies in F, the factorization of $p(x)$ becomes,

$p(x) = (x - \lambda_1)^{l_1}(x - \lambda_2)^{l_2} \dots (x - \lambda_k)^{l_k}$

Where $\lambda_1, \lambda_2, \dots \lambda_k$ are distinct characteristic roots of T.

$\therefore$ The irreducible factors,

$$q_i(x) = x - \lambda_i$$

$$q_i(T) = T - \lambda_i$$

$\therefore$ T_i has only one characteristic root λ_i on V_i.

Definition: (Jordan Form)

The matrix $\begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & \cdots & \cdots & \cdots \\ \vdots & \dots & \cdots & \cdots & \cdots \\ \vdots & \dots & \dots & \dots & 1 \\ 0 & \dots & \dots & \dots & \lambda \end{pmatrix}$ with $\lambda's$ on the diagonal, $1's$ on the superdiagonal and $0's$ elsewhere, is a basic Jordan Block belonging to λ.

Theorem: 6.6.2

Let $T \in A_F(V)$ have all its distinct characteristic roots, $\lambda_1, \lambda_2, \dots \lambda_k$ in F. Then a basis of V can be found in which the matrix T is of the form $\begin{pmatrix} J_1 & & \\ & J_2 \ddots & \\ & & J_k \end{pmatrix}$ where each

$J_i = \begin{pmatrix} B_{i1} & & \\ & B_{i2} \ddots & \\ & & B_{ir_i} \end{pmatrix}$ and where $B_{i1}, B_{i2}, \dots B_{ir_i}$ are basic Jordan blocks belonging to λ_i.

Proof:

Let $T \in A_F(V)$ have all its distinct characteristic roots, $\lambda_1, \lambda_2, ... \lambda_k$ in F.

To prove, A basis of V can be found in which the matrix of T is of the form $\begin{pmatrix} J_1 & & \\ & J_2 \ddots & \\ & & J_k \end{pmatrix}$,

where $J_i = \begin{pmatrix} B_{i1} & & \\ & B_{i2} \ddots & \\ & & B_{ir_i} \end{pmatrix}$.

Since T has all its distinct roots in F.

By the **Corollary 6.6.1**, V can be written as,

$$V = V_1 \oplus V_2 \oplus ... \oplus V_k, \text{ where } V_i = \{v \in V / v(T - \lambda_i)^{l_i} = 0\} \quad (1)$$

And T_i has only one characteristic root λ_i on V_i.

Again by using **Lemma 6.5.1,**

The matrix of T, $m(T) = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & J_k \end{pmatrix}$

We know that, $v_i(T - \lambda_i) = 0$, (by (1))

Which implies that, $T - \lambda_i$ is nilpotent.

By using **Theorem 6.5.1**,

$$m(T - \lambda_i) = \begin{pmatrix} M_{i1} & 0 & \cdots & 0 \\ 0 & M_{i2} & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & M_{ir_i} \end{pmatrix}$$

Now T can be written as,

$$T = \lambda_i I + (T - \lambda_i)$$

$$\therefore m(T) = \lambda_i m(I) + m(T - \lambda_i)$$

$$= \lambda_i \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & 1 \end{pmatrix} + \begin{pmatrix} M_{i1} & 0 & \cdots & 0 \\ 0 & M_{i2} & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & M_{ir_i} \end{pmatrix}$$

$$= \begin{pmatrix} \lambda_i & 0 & \cdots & 0 \\ 0 & \lambda_i & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \lambda_i \end{pmatrix} + \begin{pmatrix} M_{i1} & 0 & \cdots & 0 \\ 0 & M_{i2} & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & M_{ir_i} \end{pmatrix}$$

$$= \begin{pmatrix} B_{i1} & 0 & \cdots & 0 \\ 0 & B_{i2} & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & b_{ir_i} \end{pmatrix}$$

$$\therefore m(T) = \begin{pmatrix} J_1 & 0 & \cdots & 0 \\ 0 & J_2 & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & J_k \end{pmatrix} = \begin{pmatrix} J_1 & & \\ & J_2 \ddots & \\ & & J_k \end{pmatrix}.$$

UNIT - V - LINEAR TRANSFORMATIONS 18hrs

Canonical Forms - Rational Canonical Form – Hermitian, Unitary, Normal transformations - Real Quadratic Forms.

Chapter 6: Sections6.7, 6.10 and 6.11[Omit 6.8 and 6.9]

.**6.7 Canonical Forms: Rational Canonical Form**

DEFINITION: (Companion Matrix)

If $f(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{r-1}x^{r-1} + x^r$ is in $F[x]$, then the $r \times r$ matrix
$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\gamma_0 & -\gamma_1 & \cdots & \cdots & -\gamma_{r-1} \end{pmatrix}$ is called the companion matrix of $f(x)$. We write it as $C(f(x))$.

THEOREM 6.7.1

If $T \in A_F(V)$ has as minimal polynomial $p(x) = q(x)^e$, where $q(x)$ is a monic, irreducible polynomial in $F[x]$, then a basis of V over F can be found in which the matrix of T is of the form $\begin{pmatrix} C(q(x)^{e_1}) & & \\ & C(q(x)^{e_2}) & \\ & & \ddots\ C(q(x)^{e_r}) \end{pmatrix}$ where, $e_1 \geq e_2 \geq \cdots \geq e_r$.

Proof:

Since V, as a module over $F[x]$, is finitely generated and since $F[x]$ is Euclidean, we can decompose $V = V_1 \oplus V_2 \oplus \dots \oplus V_r$, where the V_i are cyclic modules.

The V_i are thus invariant under T.

If T_i is the linear transformation induced by T on V_i, its minimal polynomial must be a divisor of $p(x) = q(x)^e$ so is of the form $q(x)^{e_i}$ where $e_i < e$, $(i = 1,2, \dots r)$.

$$\therefore e_1 \geq e_2 \geq \cdots \geq e_r$$

To prove, $e_1 = e$:

Now $q(T)^{e_1}$ annihilates each V_i.

i.e., $q(T)^{e_1}$ annihilates V, whence $q(T)^{e_1} = 0$, T satisfies this polynomial $q(x)^e$.

$\Rightarrow q(x)^e | q(x)^{e_1}$

$\Rightarrow e \leq e_1$ ___________ (1)

We have, $e_1 \leq e$ ____________ (2)

From (1) and (2), we get

$$e_1 = e$$

Since V_i is a cyclic module , there exist $q(x)^{e_i}$ is the minimal polynomial for T_i on V_i.

By **Lemma 6.7.1,**

There is a basis of v_i in which the matrix of T_i is $C(q(x)^{e_i})$.

By **Lemma 6.6.1,**

We get the basis of V and with respect to the basis of T we have,

$$m(T) = \begin{pmatrix} C(q(x)^{e_1}) & & \\ & C(q(x)^{e_2}) & \\ & & \ddots\ C(q(x)^{e_r}) \end{pmatrix}.$$

THEOREM 6.7.2

Let V and W be two vector spaces over F and suppose that ψ is a vector space isomorphism of V onto W. Suppose that $S \in A_F(V)$ and $T \in A_F(W)$ are such that for any $v \in V$, $(vS)\psi = (v\psi)T$. Then S and T have the same elementary divisors.

Proof:

Claim 1

S and T have the same minimal polynomial.

By hypothesis, for any $v \in V$,

$$(vS)\psi = (v\psi)T$$

$$(vS^2)\psi = \big((vS)S\big)\psi$$

$$= ((vS)\psi)T$$

$$= ((v\psi)T)T$$

$$(vS^2)\psi = (v\psi)T^2$$

$$\vdots$$

$$(vS^m)\psi = (v\psi)T^m$$

If $f(x) \in F[x]$, for any $v \in V$,

$$(vf(s))\psi = (v\psi)f(T)$$

If $f(s) = 0$ then $(v\psi)f(T) = 0$.

Since ψ maps V onto $W, f(T) = 0$.

Conversely, If $g(x) \in F[x]$, for any $v \in V$, then

$$(vg(s))\psi = (v\psi)g(T)$$

If $g(T) = 0$, then for any $v \in V$ we have $(vg(s))\psi = 0$.

Since ψ is an isomorphism,

$$vg(s) = 0$$

$$g(s) = 0$$

Thus S and T satisfies the same set of minimal polynomial in $F[x]$.

$\therefore$ S and T have the same minimal polynomial.

Claim 2

Let $p(x) = q_1(x)^{e_1}, q_2(x)^{e_2}, \dots q_k(x)^{e_k}$ be the minimal polynomial for both S and T.

If v is a subspace of V invariant under S, then $v\psi$ is a subspace of W invariant under T.

$$\therefore \quad (v\psi)T = vS\psi \subset v\psi$$

Let S_1 be the linear transformation induced by T on $v\psi$.

Now the minimal polynomial S on V is $(x) = q_1(x)^{e_1}, q_2(x)^{e_2}, \dots q_k(x)^{e_k}$.

As we have seen in Theorem 6.7.1 and its Corollary,

We take as the 1st elementary divisor of S as the polynomial $q_1(x)^{e_1}$ and we can find a subspace V_1 of V, which is invariant under S.

In terms of *S*:

1. $V = V_1 \oplus M$, where M is invariant under S.
2. The only elementary divisor of S_1 the linear transformation induced on $V_1$by S is $q_1(x)^{e_1}$.
3. The other elementary divisors of S are those of linear transformation S_2 induced by S on M.

In terms of *T*:

1. $W = W_1 \oplus N$, where $W_1 = V_1\psi$ and $N = M\psi$ are invariant under T.
2. The only elementary divisor of T_1 the linear transformation induced by T on W_1 is $q_1(x)^{e_1}$.
3. The other elementary divisor of T are those of the linear transformation T_2 induced by T on N.

Since $N = M\psi$, M and N are isomorphic vector spaces over F under the isomorphic ψ_2 induced by ψ.

If $u \in M$, then $u(S_2)\psi_2 = (uS)\psi = (u\psi)T = (u\psi_2)T_2$.

$\therefore$ S_2 and T_2 are in the same relation vis-à-vis ψ_2 as S and T were vis-à-vis ψ.

By induction on dimension S_2 and T_2 have the same elementary divisors.

$\therefore S$ and T have the same elementary divisors.

THEOREM: 6.7.3

The elements S and T in $A_F(V)$ are similar in $A_F(V)$ if and only if they have the same elementary divisors.

Proof:

Necessary Part:

Suppose S and T have the same elementary divisors. Then there are two bases

$\{v_1, v_2, \dots v_n\} \times \{w_1, w_2, \dots w_n\}$ of V over F such that matrix S in $\{v_1, v_2, \dots v_n\}$ equals the matrix of canonical form $\begin{pmatrix} R_{11} & 0 & \cdots & 0 \\ 0 & R_{12} & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & R_{1i} \end{pmatrix}$ ($\because By\ Corollary$ 6.7.1)

We know that, if V is a finite dimensional vector space over F, then any two bases of V have the same number of elements.

$$R_i = \begin{pmatrix} C(q_i(x)^{e_{i1}}) & & \\ & C(q_i(x)^{e_{i2}}) & \\ & & \ddots\ C(q_i(x)^{e_{ir_i}}) \end{pmatrix}$$, where each $e_i = e_{i1} \geq e_{i2} \geq \cdots e_{ir_i}$.

By the result,

"Let S and T be linear transformation defined on V. If the matrix on T in of $\{v_1, v_2, \dots v_n\}$ is equal to the matrix of S in $\{w_1, w_2, \dots w_n\}$. Then there exist a linear transformation A on V defined by $V_i A = w_i$, $\forall\, i$, such that $T = ASA^{-1}$ (or) $S = ATA^{-1}$ which gives S and T are similar".

Sufficient Part:

Suppose that, S and T are similar there exist a linear transformation A on V such that $T = ASA^{-1}$ (or) $S = ATA^{-1}$.

$\therefore T$ and S are same minimal polynomial.

Without loss of generality, We may assume that the minimal polynomial of T is $q(x)^e$, where $q(x)$ is irreducible in $F[x]$ of degree $'d'$.

" The rational canonical form" states that we can decomposed V as $V = V_1 \oplus V_2 \oplus \ldots \oplus V_r$, where V_i is invariant under T then the linear transformation induced by T on V_i as the matrix $q(x)^{e_i}$, where $e_1 \geq e_2 \geq \cdots e_r$.

i.e. $q(x)^{e_1}.q(x)^{e_2} \ldots q(x)^{e_r}$ are the elementary divisors of T _______ (A)

If $V = V_1 \oplus V_2 \oplus \ldots \oplus V_s$, where the subspace V_j is invariant under S, then the linear transformation induced by S on V_j as the matrix $q(x)^{f_j}$ where $f_1 \geq f_2 \geq \cdots \geq f_s$

i.e. $q(x)^{f_1}q(x)^{f_2} \ldots q(x)^{f_s}$ are the elementary divisor of S __________ (B)

From (A) and (B), we get

$$r = s, e_1 = f_1, e_2 = f_2, \ldots e_r = f_s$$

Claim

$r = s, e_1 = f_1, e_2 = f_2, \ldots e_r = f_s$

Suppose that, $e_i \neq f_i$

Then there exist a first inter m, such that $e_m \neq f_{m\,,}$ where

$$e_1 = f_1, e_2 = f_2, \ldots e_{m-1} = f_{m-1.}$$

Suppose that $e_m = f_{m\,,}$ now $q(T)^{f_m}$ annihilates $U_m, U_{m+1}, \ldots, U_s$.

i.e. $V_1 q(T)^{f_m} = 0$

Consider, $Vq(T)^{f_m} = (V_1 \oplus V_2 \oplus \ldots \oplus V_{m-1})q(T)^{f_m}$

$$= V_1 q(T)^{f_m} \oplus V_2 q(T)^{f_m} \oplus \ldots \oplus V_{m-1} q(T)^{f_m}$$

$$dim\, Uq(T)^{f_m} = dimU_1 q(T)^{f_m} + dimU_2 q(T)^{f_m} + \cdots + dimU_{m-1} q(T)^{f_m}$$

$$[\because\ dimU_i = df_i\ and\ dim\, q(T)^{f_m} = df_m\ , for\ i \leq m]$$

$$dim(U_i q(T)^{f_m}) = d(f_i - f_m) \quad \text{\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \quad (1)$$

$dim\,(Uq(T)^{f_m}) = d(f_1 - f_m) + d(f_2 - f_m) + \cdots + d(f_{m-1} - f_m)$

But, $Vq(T)^{f_m} > V_1 q(T)^{f_m} \oplus V_2 q(T)^{f_m} \oplus \ldots \oplus V_m q(T)^{f_m}$

Consider, $Vq(T)^{f_m} = (V_1 \oplus V_2 \oplus \ldots \oplus V_r)q(T)^{f_m}$

$$= V_1 q(T)^{f_m} \oplus V_2 q(T)^{f_m} \oplus \ldots \oplus V_r q(T)^{f_m}$$

$$dimVq(T)^{f_m} = dimV_1q(T)^{f_m} \oplus dimV_2q(T)^{f_m} \oplus \ldots \oplus dimV_rq(T)^{f_m}$$

$$[\because\ dimV_iq(T)^{f_m} \geq d(e_i - f_m),\ for\ i \leq m] \_\_\_\_\_\_\_\_ (2)$$

$\therefore$ By our choice of e_m, $e_1 = f_1, e_2 = f_2, \ldots e_{m-1} = f_{m-1.}$ and $e_m > f_m$

Substituting in (1), we have

$$\dim(Vq(T)^{f_m}) \geq d(f_1 - f_m) + d(f_2 - f_m) + \cdots + d(f_{m-1.} - f_m)$$

This is necessary and sufficient to the equality of (1).

Which is a contradiction to our assumption.

Hence, $r = s, e_i = f_i, \forall i$

Thus T and S have same elementary divisors.

COROLLARY:6.7.3

Suppose the two matrices A and B in F_n are similar in K_n where K is an extension of F. Then A and B are already similar in F_n.

Proof:

Suppose that $A, B \in F_n$ are similar in K_n such that $B = C^{-1}AC$ with $C \in K_n$.

Consider, $K^{(n)}$ is the vector space of n −tuples over K. Since K is an extension of F.

$$\therefore\ F^{(n)} \leq K^{(n)}$$

$F^{(n)}$ is a vector space over F but not over K.

$\therefore$ The image of $F^{(n)}$ is a subset of $K^{(n)}$.

Now, $F^{(n)}C$ is a subset of $K^{(n)}$.

Let V be the vector space $F^{(n)}$ over F and W be the vector space $F^{(n)}C$ over F.

For any $v \in V$, let $v\psi = vC$.

Now, $A \in A_F(V)$ and $B \in A_F(W)$ and for any $v \in V$,

$$(vA)\psi = vAC = vCB = (v\psi)B, (\because A = CBC^{-1} \Longrightarrow AC = CB)$$

(whence the conditions of Theorem 6.7.3 are satisfied)

Thus A and B have the same elementary divisors.

Therefore by **Theorem 6.7.3,** A and B are similar in F_n.

TRACE AND TRANSPOSE

TRACE:

Let F be a field and let A be a matrix in F_n. Then the *trace* of A is the sum of the elements on the main diagonal of A. We can write the trace of A as $tr\ A$. Let $A = (\alpha_{ij}) \in F$ then $tr\ A = \sum_{i=1}^{n} \alpha_{ii}$, where $A = (\alpha_{ij}) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix}$.

LEMMA 6.8.1

For $A, B \in F_n$ and $\lambda \in F$,

1. $tr(\lambda A) = \lambda\ tr\ A$.
2. $tr\ (A + B) = tr\ A + tr\ B$.
3. $tr\ (AB) = tr\ (BA)$.

Proof:

Let $A = (\alpha_{ij}), B = (\beta_{ij})$ then $AB = (\gamma_{ij})$ where $\gamma_{ij} = \sum_{k=1}^{n} \alpha_{ik}\beta_{kj}$

1. To prove $tr(\lambda A) = \lambda\ tr\ A$
   Let $A = (\alpha_{ij})$. Then
   $tr\ (A) \quad = \sum_{i=1}^{n} \alpha_{ii}$
   $tr\ (\lambda A) = \sum_{i=1}^{n} (\lambda \alpha_{ii})$
   $= \lambda \sum_{i=1}^{n} (\alpha_{ii})$
   $\therefore tr\ (\lambda A) = \lambda\ tr\ A$
2. To prove $tr\ (A + B) = tr\ A + tr\ B$
   Let $A = (\alpha_{ij}), B = (\beta_{ij})$. Then
   $A + B = (\alpha_{ij}) + (\beta_{ij})$
   $tr\ (A + B) = \sum_{i=1}^{n} (\alpha_{ii} + \beta_{ii})$
   $= \sum_{i=1}^{n} \alpha_{ii} + \sum_{i=1}^{n} \beta_{ii}$

   $\therefore tr\ (A + B) = tr\ A + tr\ B$

4. To prove $tr\ (AB) = tr\ (BA)$.
   Let $AB = (\gamma_{ij})$ where $\gamma_{ij} = \sum_{k=1}^{n} \alpha_{ik}\beta_{kj}$ and let $BA = (\mu\gamma_{ij})$ where $\mu_{ij} = \sum_{k=1}^{n} \beta_{ik}\alpha_{kj}$. Thus,

   $$tr\ (AB) = \sum_{i=1}^{n} \gamma_{ii} = \sum_{i=1}^{n} (\sum_{k=1}^{n} \alpha_{ik}\beta_{ki})$$

If we interchange the order of summation in this last sum, we get

$$tr\ (AB) = \sum_{k=1}^{n}(\sum_{i=1}^{n} \alpha_{ik}\beta_{ki})$$

$$= \sum_{k=1}^{n}(\sum_{i=1}^{n} \beta_{ki}\alpha_{ik})$$

$$= \sum_{k=1}^{n} \mu_{kk}$$

$$\therefore tr\ (AB) = tr\ (BA).$$

COROLLARY

If A is invertible then $ACA^{-1} = tr\ C$.

Proof:

Given A is invertible, then we have

$$AA^{-1} = 1 \quad \_\_\_\_\_\_\_\_\_\_ \quad (1)$$

Consider, $B = CA^{-1}$

$$AB = ACA^{-1}$$

$$tr\ (AB) = tr\ (BA) = tr\ (CA^{-1}A) = tr\ C.\ (\because\ AA^{-1} = 1\ )$$

DEFINITION: (Trace of *T*)

If $T \in A(V)$ then $tr\ T,$ then the trace of T is the trace of $m_1(T)$ where $m_1(T)$ is the matrix of T in some basis of V.

i.e. $tr\ T = tr\ m_1(T)$

LEMMA : 6.8.2

If $T \in A(V)$ then $tr\ T$ is the sum of the characteristic roots of T (using each characteristic root as often as its multiplicity).

Proof:

Assume that T is a matrix in F_n.

By using the result,

“ If K is the splitting field for the minimum polynomial of T over F then in K_n", we get

T can be brought to its Jordan form J, J is a matrix on whose diagonal appear the characteristic roots of T each root appearing as often as its multiplicity.

Thus, $tr\ J$=sum of the characteristic root T

J is of the form, $J = ATA^{-1}$

$$tr\ J = tr\ (ATA^{-1}) = tr\ T = sum\ of\ the\ characteristic\ root\ of\ T.$$

LEMMA: 6.8.3

If F is a field of characteristic zero and if $T \in A_F(V)$ is such that $tr\ (T^i) = 0, \forall\ i \geq 1$, then T is nilpotent.

Proof:

Since $T \in A_F(V)$ and T satisfies some minimal polynomial,

$$p(x) = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$$

$$p(T) = T^m + \alpha_1 T^{m-1} + \cdots + \alpha_m$$

Then, $tr\ \big(p(T)\big) = tr\ (T^m + \alpha_1 T^{m-1} + \cdots + \alpha_m)$

$\therefore tr\ T^m + \alpha_1\ tr\ T^{m-1} + \cdots + tr\ \alpha_m = 0$

Given $tr\ \left(T^i\right) = 0, \quad \forall\ i \geq 1$

Then we get, $tr(a_m) = 0$

If $\dim(V) = n$ then $tr(a_m) = n\alpha_m$ where $n\alpha_m = 0$. But the characteristic of F is zero.

$\therefore n \neq 0 \Longrightarrow \alpha_m = 0$

Since the constant term of the minimal polynomial $T = 0$.

By a theorem,

" If V is a 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 not zero"

$\therefore T$ is not invertible

i.e. T is singular.

$\therefore$ Zero is the characteristic root of T.

Consider T as a matrix in F_n, also as a matrix in K_n, where K contains all characteristic roof T.

By a theorem,

" If $T \in A(V)$ has all its characteristic roots in F_n then there is a basis of V in which the matrix of T is triangular".

We can bring T to triangular form. Since zero is the characteristic root of T we can bring it of the form,

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ \beta_2 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ \beta_n & * & \cdots & \alpha_n \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ * & T_2 \end{pmatrix} \text{ where } T_2 = \begin{pmatrix} \alpha_2 & 0 & \cdots & 0 \\ * & 0 & \cdots & \alpha_n \end{pmatrix}$$

T_2 is an $(n-1) \times (n-1)$ matrix.

Now, $\quad T^k = \begin{pmatrix} 0 & 0 \\ 0 & {T_2}^k \end{pmatrix}$

Hence $tr\,(T^k) = 0, \forall\, k \geq 1$ either induction on $'n'$ or repeating the arguments on T_2 used for T we get,

$\alpha_2, \alpha_3, \dots, \alpha_n$ are the characteristic root.

i.e. $\alpha_2 = \alpha_3 = \cdots \alpha_n = 0$

Thus when T is brought to triangular form all its entries on the main diagonals are zero.

$\therefore$ T is nilpotent.

DEFINITION: (Transpose)

If $A = (\alpha_{ij}) \in F_n$ then the transpose of A, written as A', is the matrix $A' = (\gamma_{ij})$ where $\gamma_{ij} = \alpha_{ji}$ for each i and j.

LEMMA: 6.8.5

For all $A, B \in F_n$,

1. $(A')' = A$
2. $(A+B)' = A' + B'$
3. $(AB)' = B'A'$

Proof:

(i) $(A')' = A$

Let $A = (\alpha_{ij})$

$A' = (\beta_{ij})$, where $\beta_{ij} = \alpha_{ji}, \forall\, i, j$

$(A')' = (\gamma_{ij})$, where $\gamma_{ij} = \beta_{ji}$, which implies that $\gamma_{ij} = \beta_{ji} = \alpha_{ij}$

$$\therefore (A')' = \beta_{ji} = \alpha_{ij} = A$$

(ii) $(A+B)' = A' + B'$

Let $A = (\alpha_{ij})$

$A' = (a_{ij})$ where $(a_{ij}) = \alpha_{ji}$, $\forall\, i, j$

$B = (\beta_{ij})$

$B' = (b_{ij})$ where $(b_{ij}) = \beta_{ji}$, $\forall i, j$

$A + B = (\gamma_{ij})$ where $\gamma_{ij} = \alpha_{ij} + \beta_{ij}$, $\forall i, j$

$(A+B)' = \delta_{ij} \Longrightarrow \delta_{ij} + \gamma_{ij} = \alpha_{ji} + \beta_{ji} = (a_{ij}) + (b_{ij}) \in A' + B'$

$$\therefore (A+B)' = A' + B'$$

(iii) $(AB)' = B'A'$

Let $A = (a_{ij}), A' = (\alpha_{ij})$ where $(\alpha_{ij}) = a_{ji}$

Let $B = (b_{ij})$, $B' = (\beta_{ij})$ where $\beta_{ij} = (b_{ji})$

Let $AB = (C_{ij})$, where $(C_{ij}) = \sum_{k=1}^{n} a_{ik}\, b_{kj}$

$(AB)' = (d_{ij})$ where $(d_{ij}) = (C_{ji})$

$B'A' = \lambda_{ji}$ where $\lambda_{ji} = \sum_{k=1}^{n} \beta_{ik}\, \alpha_{kj}$

Consider for every i, j,

$$\lambda_{ji} = \sum_{k=1}^{n} \beta_{ik}\, \alpha_{kj}$$

$$\lambda_{ji} = \sum_{k=1}^{n} b_{ki}\, a_{jk}$$

$$= \sum_{k=1}^{n} a_{jk}\, b_{ki} = C_{ji} = (d_{ij}) = (AB)'$$

$$\therefore (AB)' = B'A'$$

Definition:

Symmetric matrix:

If $A \in F_n$ be a square matrix is said to be symmetric if $A' = A$.

Eg:

$$A = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \qquad A' = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$$

Skew symmetric matrix:

If $A \in F_n$ be a skew square matrix is said to be skew symmetric if $A' = -A$.

Eg: $\begin{bmatrix} 0 & -a \\ a & 0 \end{bmatrix}$

Note 1:

In a skew symmetric matrix the leading diagonal elements are zero.

Note 2:

If A is square matrix $A + A'$ is symmetric and $A - A'$ is skew symmetric AA' and $A'A$ are symmetric.

Adjoint on F_n:

A mapping $*$: $F_n \to F_n$ is called adjoint on F_n if (i) $(A^*)^* = A$

(ii) $(A + B)^* = A^* + B^*$

(iii) $(AB)^* = B^*A^* \forall\, A, B \in F_n$

Hermitian adjoint on F_n:

Let consider the field of complex number for every matrix $A = (\alpha_{ij})$ and let $A^* = \gamma_{ij}$

where $\gamma_{ij} = \overline{\alpha}_{ji}$ in this case the $*$ is called the Hermitian adjoint on F_n.

Hermitian matrix:

Let f be a field of complex number and $*$ be a Hermitian adjoint every square matrix is called hermitian if $A^* = A$.

Eg:

$$\begin{bmatrix} 1 & -1 + 2i & 3 + 4i \\ -1 - 2i & -2 & 3 \\ 3 - 4i & 3 & -2 \end{bmatrix}$$

Remark:

1. If $A \neq 0 \in F_n$ then $tr(AA^*) > 0$

2. Let $A_1, A_2, \ldots A_n \in F_n$ if $A_1{A_1}^* + A_2{A_2}^* + \cdots + A_k{A_k}^* = 0$

then $A_1 = A_2 = \cdots = A_k = 0$

3. If λ is a scalar matrix then $\lambda^* = \overline{\lambda}$

Result :

The characteristic root of a Hermitian matrix are all real .

Proof :

Given that $A \in F_n$ be a hermitian matrix

To prove that the characteristic roots of A is real.

We shall prove this by the method of contradiction

Assume that the roots of A is a complex number ie) $\alpha + i\beta$ where α, β are real, by using the definition of characteristic roots $A - (\alpha + i\beta)$ is singular.

$\Rightarrow [A - (\alpha + i\beta)][A - (\alpha - i\beta)]$ is singular

$\Rightarrow (A - (\alpha + i\beta)][A - (\alpha - i\beta)]$ is not invertible

$\Rightarrow [(A - \alpha) + i\beta]\ [(A - \alpha) - i\beta]$ is not invertible

$\Rightarrow (A - \alpha)^2 - (i\beta)^2$ is not invertible

$\Rightarrow (A - \alpha)^2 + \beta^2$ is not invertible

By using the theorem,

If v is finite dimension vector space over F and if $A \in F_n$ is not invertible then there exist a matrix $B \neq 0$ such that $AB = BA = 0$ there exist a matrix $C \neq 0$ such that

$C[(A-\alpha)^2 + \beta^2] = 0$

Multiply C^* on R.H.S of both sides

$C[(A-\alpha)^2 + \beta^2]C^* = 0$

$C(A-\alpha)(A-\alpha)C^* + C\beta\beta C^* = 0 \rightarrow$ 1

Takes $D = C(A - \alpha)$ $\qquad E = C\beta$

$D^* = (A-\alpha)^* C^*$ $\qquad E^* = (C\beta)^*$

$= (A^* - \alpha^*)C^*$ $\qquad = \beta^* C^*$

$= (A - \alpha)C^*$ $\qquad = \beta C^*$

Since A is hermitian $\Rightarrow A^* = A$ and α, β are real $\Rightarrow \alpha^* = \alpha, \beta^* = \beta$

From 1 $\Rightarrow DD^* + EE^* = 0$

$$\Rightarrow D = E = 0 \ [since\ by\ remark\ 2]$$

In particular $E = 0$

$$\beta C = 0$$

$$\beta = 0 \quad [since\ C \neq 0]$$

Which contradicts our assumption is wrong

The characteristic roots of hermitian matrix A is real.

Result:

For $A \in F_n$. The real characteristic roots are AA^* are non negative.

Proof:

Given that $A \in F_n$

$A^* = A$

$(AA^*)^* = (A^*)^* A^*$

$= AA^*$

$\therefore AA^*$ is hermitian

To prove the real characteristic roots of AA^* is positive

We shall prove this by the method of contradiction

Let α be the characteristic roots of AA^* which is negative

ie) $\alpha = -\beta^2$ where β is real by using the definition of a characteristic root

$AA^* - (-\beta^2)$ is singular

$AA^* + \beta^2$ is singular

By the theorem there exist $C \neq 0$ such that $C(AA^* + \beta^2) = 0$

Multiply C^* in R.H.S on both sides $C(AA^* + \beta^2)C^* = 0$

$$CAA^*C^* + C\beta\beta C^* = 0$$

Take $D = CA$ $\qquad E = C\beta$

$D^* = (CA)^*$ $\qquad E^* = (C\beta)^*$

$= A^*C^* \qquad\qquad\qquad\qquad = \beta^*C^*$

1 $\Rightarrow DD^* + EE^* = 0$ $(since\ by\ remark\ 2)$

$\Rightarrow D = E = 0$

In particular $E = 0$

$\Rightarrow C\beta = 0$

$\Rightarrow \beta = 0$ $(since\ C \neq 0)$

Which contradicts our assumption that α is negative

So our assumption is wrong

∴ The real characteristic roots of AA^* are non – negative.

Definition:

Hermitian Unitary and Normal Transformation:

In this section F we denote the field of complex number.

Fact 1:

A polynomial with coefficient which are complex number has all its roots in complex field.

Fact 2:

The only irreducible non constant polynomial over the field of real number are either of degree 1 or of degree 2.

Lemma 6.10.1:

If $T\epsilon A(V)$ is such that the inner product $(vT, v) = 0\ \forall\ v \in V\ then\ T = 0$ (Here V is an inner product space over the complex field)

Proof:

Gn $T\epsilon A(V)$ such that inner product $(vT, v) = 0\ \forall\ v \in V \rightarrow$ 1

Here v is the inner product space over the complex field.

$u, w \in v$

$u + w \in v \quad u + w = v\ sub\ in$ equation 1

$u + w \in v$

1 $\Rightarrow \big((u+w)T,(u+w)\big)=0$

$\big((uT+wT),(u+w)\big)=0$

$(uT,u)+(uT,w)+(wT,u)+(wT,w)=0 \; by \; equation \; 1$

$(uT,w)+(wT,u)=0 \;\; \rightarrow$ 2

Take $w=iw$

$(uT,iw)+(iwT,u)=0$

$\Rightarrow i(uT.w)+i(wT,u)=0$

$-i(uT,w)+i(wt,u)=0$

$\div \; by \; i, -(uT,w)+(wT,u)=0 \;\; \rightarrow$ 3

2 + 3 $\Rightarrow 2(wT,u)=0$

$\Rightarrow (wT,u)=0$

Take $u=wT$

$\Rightarrow (wT,wT)=0$

$\Rightarrow wT=0$

$\Rightarrow T=0 \; (\because w\neq 0)$

Note:

If v is inner product space over the real field .This lemma is false.

Let $v=\{(\alpha,\beta\,)/\alpha,\beta are\; real\}$

Let $T:(\alpha,\beta)\rightarrow(-\beta,\alpha)$

Let $v\in V\Rightarrow v=(\alpha,\beta)\;\; [\because (vT,v)]=0$

$[(\alpha,\beta)T,(\alpha,\beta)]=0$

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

$-\beta\alpha+\alpha\beta=0$

$\Rightarrow (vT, v) = 0 \quad \forall\, v \in V$ and $T \neq 0$ $(\because T: (\alpha, \beta) \to (-\beta, \alpha))$

Hence if v is the inner product space over the real field then lame is not proved.

Definition:

Unitary Linear Transformation:

The linear transformation $T \in A(V)$ is said to be unitary

$$(uT, vT) = (u, v), \forall\, u.v \in V$$

Problem:

1. If $A \; and \; B$ are similar iff $tr(A) = tr(B)$

Proof

Necessary part:

Given that $A \; and \; B$ are similar

To prove $tr(A) = tr(B)$

$$A = CBC^{-1}$$

$$tr(A) = tr(CBC^{-1})$$

$$= tr(B)$$

Sufficient part:

To prove $A \; and \; B$ are similar

Given that $tr(A) = tr(B)$

$$tr(ACC^{-1}) = tr(B)$$

$$tr(B) = tr(CAC^{-1})$$

$$\Rightarrow B = CAC^{-1}$$

$\Rightarrow A \; and \; B$ are similar

2. $S = \{A \in F_n \,/ A^* = A\}$ and $K = \{A \epsilon F_n \,/ A^* = -A\}$ prove i) If $A, B \epsilon S \; then \; AB + BA \epsilon S$

ii) If $A, B \epsilon K \; then \; (AB - BA) \epsilon K$ iii) If $A \epsilon S, B \epsilon K \; then \; (AB - BA) \epsilon S \; and \; (AB + BA) \epsilon S$

proof:

i) To prove $(AB+BA)\epsilon S$

ie) To prove $(AB+BA)^*=(AB+BA)$

$$A\epsilon S \Rightarrow A^*=A$$

$$B\epsilon S \Rightarrow B^*=B$$

Now consider $(AB+BA)^*=(AB)^*+(BA)^*$

$$=B^*A^*+A^*B^*$$

$$=BA+AB\ (\because by\ equ\ 1)$$

$$=AB+BA$$

$$\Rightarrow (AB+BA)\epsilon S$$

ii) To prove $(AB-BA)\epsilon K$

ie) To prove $(AB-BA)^*=-(AB-BA)$

$$A\epsilon K \Rightarrow A^*=-A$$

$$B\epsilon K \Rightarrow B^*=-B$$

Now consider $(AB-BA)^*=-(AB)^*-(BA)^*$

$$=B^*A^*-A^*B^*$$

$$=(-B)(-A)-(-A)(-B)(\because by\ equ\ 2)$$

$$=BA-AB$$

$$=-(AB-BA)$$

$$\Rightarrow AB-BA\ \epsilon\ K$$

iii) $A\epsilon S, B\epsilon K\ then\ AB-BA\epsilon S\ and\ AB+BA\epsilon K$

$$\left.\begin{array}{l} A\epsilon S \Rightarrow A^*=A \\ B\epsilon K \Rightarrow B^*=-B \end{array}\right\} \rightarrow 3$$

To prove $(AB-BA)\epsilon S$

ie) To prove $(AB-BA)^*=-(AB-BA)$

Consider $(AB-BA)^*=-(AB)^*-(BA)^*$

$= B^*A^* - A^*B^*$

$= (-B)A - A(-B)$

$= BA + AB$

$= (AB - BA)$

$\Rightarrow AB - BA \epsilon S$

To prove $(AB = BA)\epsilon K$

ie) To prove $(AB + BA)^* = -(AB + BA)$

Consider $(AB + BA)^* = (AB)^* + (BA)^*$

$= B^*A^* + A^*B^*$

$= (-B)A + A(-B)$

$= -BA - AB$

$(AB + BA)^* = -(AB + BA)$

$\Rightarrow (AB + BA)\epsilon K$

Lemma 6.10.2:

If the inner product $(vT, vT) = (v, v) \forall\, v\epsilon V$ then T is unitary $\rightarrow$ 1

Proof:

ie)To prove $(uT, vT) = (u, v) \forall\, u, v\epsilon V$

Let $u, v\epsilon V$

$\Rightarrow u + v\epsilon V$

$\Rightarrow u + v = v$

Sub $u + v = v$ *in equation* 1

1 $\Rightarrow \big((u + v)T, (u + v)T\big) = ((u + v), (u + v))$

$\Rightarrow \big((uT + vT), (uT + vT)\big) = \big((u + v), (u + v)\big)$

$(uT, uT) + (uT, vT) + (vT, uT) + (vT, vT) = (u, u) + (u, v) + (v, u) + (v, v)$

$\Rightarrow (uT, vT) + (vT, uT) = (u, v) + (v, u) \rightarrow$ 2

Take $v = iv$

$$2 \Rightarrow (uT, ivT) + (ivT, uT) = (u, iv) + (iv, u)$$

$$-i(uT, vT) + i(vT, uT) = i(u, v) + i(v, u)$$

$\div \; by \; i$

$$-(uT, vT) + (vT, uT) = -(u, v) + (v, u) \rightarrow 3$$

Adding equation 2 and 3 we get

$$2(uT, vT) = 2(u, v)$$

$\Rightarrow (uT, vT) = (u, v) \; \forall \; u, v \epsilon V \quad \Rightarrow T$ is unitary

Theorem 6.10.1:

The Linear Transformation T on V is unitary iff it takes an orthonormal basis of V into an Orthonormal basis of V.

Proof:

Necessary part:

Suppose $\{v_1, v_2, \dots v_n\}$ be an Orthonormal basis of v then inner product

$(v_i, v_j) = 0 \; for \; (i \neq j)$

$(v_i, v_i) = 1 \; for \; (i = j) \; \rightarrow 1$

We have to prove if T is unitary then $\{v_1T, v_2T, \dots v_nT\}$ is also an Orthonormal basis of v

Consider $\left(v_iT, v_jT\right) = \left(v_i, v_j\right) \quad [\because T \; is \; unitary]$

$= 0 \quad [\because by \; equation \; 1]$

$\therefore \left(v_iT, v_jT\right) = 0 \; \forall \; i \neq j$

Consider $(v_iT, v_iT) = (v_i, v_i) \quad [\because t \; is \; unitary]$

$= 1 \quad [by \; equation \; 1]$

$\therefore \{v_1 T, v_2T, \dots v_nT\}$ is an Orthonormal basis of v.

Sufficient part:

If $T\epsilon A(V)$ such that both $\{v_1, v_2, \dots v_n\} and \; \{v_1T, v_2T, \dots v_nT\}$ are Orthonormal basis of v then prove T is unitary

$$\left.\begin{aligned}(v_i, v_j) &= 0 \; for \; (i \neq j) \\ (v_i, v_i) &= 1\end{aligned}\right\} \rightarrow \; 1$$

Similarly $$\left.\begin{aligned}(v_iT, v_jT) &= 0, \forall \; i \neq j \\ (v_iT, v_iT) &= 1\end{aligned}\right\} \rightarrow \; 2$$

Let $u, w\epsilon v \Rightarrow u = \sum_{i=1}^{n} \alpha_i v_i$ and $w = \sum_{i=1}^{n} \beta_i v_i$

Consider $(u, w) = (\sum_{i=1}^{n} \alpha_i v_i \, , \sum_{i=1}^{n} \beta_i v_i)$

$(u, w) = (\alpha_1 v_1 + \cdots + \alpha_n v_n, \beta_1 v_1 + \cdots + \beta_n v_n)$

$$= \alpha_1 \overline{\beta}_1 \; (v_1, v_1) + \alpha_2 \; \overline{\beta}_2 \; (v_2, v_2) + \cdots + \alpha_n \; \overline{\beta}_n \; (v_n, v_n)$$

Here $(v_i, v_j) = 0$

$$= \alpha_1 \overline{\beta}_1 + \alpha_2 \overline{\beta}_2 + \ldots + \alpha_n \overline{\beta}_n$$

Similarly $uT = \sum_{i=1}^{n} \alpha_i v_i T$ and $wT = \sum_{i=1}^{n} \beta_i v_i T$

Consider $(uT, wT) = (\sum_{i=1}^{n} \alpha_i v_i \; T, \sum_{i=1}^{n} \beta_i v_i T)$

$$(uT, wT) = (\alpha_1 v_1 T + \cdots + \alpha_n v_n T, \; \beta_1 v_1 T + \cdots + \beta_n v_n T)$$

$$= \alpha_1 \overline{\beta}_1 \; (v_1T, v_1T) + \alpha_2 \; \overline{\beta}_2 \; (v_2T, v_2T) + \cdots + \alpha_n \; \overline{\beta}_n \; (v_nT, v_nT)$$

Here $(v_iT, v_jT) = 0$

$$= \alpha_1 \overline{\beta}_1 + \alpha_2 \overline{\beta}_2 + \ldots + \alpha_n \overline{\beta}_n$$

$$(uT, wT) = \sum_{i=1}^{n} \alpha_i \overline{\beta}_i$$

$(uT, wT) = (u, w), u, w\epsilon V$

T is unitary.

Lemma 6.10.3:

If $T\epsilon A(V)$ then given any $v\epsilon V$ there exist an unique element $w\epsilon v$ depending on v and T .Such that $(uT, v) = (u, w) \forall \; u\epsilon V$

Proof:

Given that $T\epsilon A(V)$

To prove for any $v\epsilon V$ there exist an unique element $w\epsilon V$ depending on $v\ and\ T$

Such that $(uT,v)=(u,w)\ \forall u\epsilon v$

Let $\{u_1 u_2,\dots u_n\}$ be the orthonormal basis of V

$\therefore \left(u_i,u_j\right)=0$

$(u_i,u_i)=1$

Define $w=\sum_{i=1}^{n}\overline{(u_iT,v)}\ u_i$

Then $(u_i w)=(u_i,\sum_{i=1}^{n}\overline{(u_iT,v)}\ u_i$

$(u_i w)=(u_i,\overline{(u_1T,v)}\,u_1+\overline{(u_2T,v)}\,u_2+\cdots+\overline{(u_nT,v)}\,u_n)$

$=(u_i,\overline{(u_1T,v)}\,u_1)+(u_i,\overline{(u_2T,v)}\,u_2)+\cdots+(u_i,\overline{(u_nT,v)}\,u_n)$

$=(u_1T,v)(u_i,u_1)+\cdots+(u_nT,v)(u_i,u_n)$

$=(u_1T,v)(0)+\cdots+(u_nT,v)(0)$

$(u_i w)=(u_iT,v)$

To prove w is unique:

Ie) To prove $w_1=w_2$

Suppose that $(uT,v)=(u,w_1)$

$(uT,v)=(u,w_2)$

$\Rightarrow (u,w_1)=(u,w_2)$

$\Rightarrow (u,w_1)-(u,w_2)=0$

$\Rightarrow (u,w_1-w_2)=0$

Then take $u=w_1-w_2$

$\Rightarrow (w_1-w_2,w_1-w_2)=0$

$\Rightarrow w_1 - w_2 = 0$

$\Rightarrow w_1 = w_2$

Definition:

Hermitian adjoint of T:

If $T \epsilon A(V)$ then hermitian adjoint of T is denoted by $T^*$and is defined by

$(uT, v) = (u, vT^*) \forall u, v \epsilon V.$

Lemma 6.10.4:

If $T \epsilon A(V)$ then $T^* \epsilon A(V)$

i) $(T^*)^* = T$

$ii)$ $(S + T)^* = S^* + T^*$

iii) $(\lambda S)^* = \overline{\lambda}\, S^*$

iv) $(ST)^* = T^* S^* \forall S, T \epsilon A(v) and\ \alpha \epsilon F$

proof:

Given that $T \epsilon A(V)$ ie) T is linear transformation belongs to $A(v)$

$\therefore (v + w)T = vT + wT$

$(\lambda v)T = \lambda(vT)$

To prove $T^* \epsilon A(V)$

Ie) $(v + w)T^* = vT^* + wT^*$

$(\lambda v)T^* = \lambda(vT^*)$

Let $u, v, w \epsilon V$

Consider $(u(v + w)T^*) = (uT, v + w)$

$= (uT, v) + (uT, w)$

$= (u, vT^* + wT^*)$

$\Rightarrow (u + w)T^* = vT^* + wT^*$

Consider $(u(\lambda v)T^*) = (uT, \lambda v)$

$$= \bar{\lambda}\,(uT, v)$$

$$= (u, \lambda v T^*)$$

$$\Rightarrow (\lambda v)T^* = \lambda(vT^*)$$

i) To prove $(T^*)^* = T$

Consider $(u, v(T^*)^*) = (uT^*, v)$

$$= \overline{(v, uT^*)}$$

$$= (u, vT)$$

$$(T^*)^* = T$$

ii) To prove $(S+T)^* = S^* + T^*$

Consider $(u, v(S+T)^*) = (u(S+T), v)$

$$= (uS + uT, v)$$

$$= (u, vS^* + vT^*)$$

$$(S+T)^* = S^* + T^*$$

iii) To prove $(\lambda S)^* = \bar{\lambda}\,S^*$

Consider $(u, v(\lambda S)^*) = (u(\lambda S), v)$

$$= \lambda(uS + v)$$

$$= (u, v(\bar{\lambda}\,S^*))$$

$$(\lambda S)^* = \bar{\lambda}\,S^*$$

iv) To prove $(ST)^* = T^*S^*$

Consider $(u, v(ST)^*) = (u(ST), v)$

$$= ((uS)T, v)$$

$$= (uS, vT^*)$$

$$= (u, vT^*S^*)$$

$$= vT^*S^*$$

$$(ST)^* = T^*S^*$$

Lemma 6.10.5:

If $T\epsilon A(V)$ is unitary iff $TT^* = 1$

Proof:

Necessary part:

Given that is unitary

$\therefore (uT, vT) = (u, v) \forall u, v\epsilon V$

To prove $TT^* = 1$

Consider $\big(u, v(TT^*)\big) = (uT, vT)$

$$= (u, v)$$

$$\Rightarrow vTT^* = v$$

$$TT^* = 1$$

Sufficient part:

Given that $TT^* = 1$

To prove that T is unitary

Ie) To prove $(uT, vT) = (u, v)$

Consider $(u, v) = (u, vTT^*)$

$$= (uT, vT)$$

T is unitary.

Note:

A unitary transformation is non singular and its inverse is just a hermitian adjoint also $TT^* = 1 \Rightarrow T^*T = 1$

Theorem 6.10.2:

If $\{v_1 v_2 \dots v_n\}$ is an Orthonormal basis of v and if $m(T)\epsilon A(V)$ in this basis is (α_{ij}) then matrix T^* in this basis is β_{ij} where $\beta_{ij} = \overline{\alpha_{ji}}$

Proof:

Given $\{v_1 v_2 \ldots v_n\}$ is an orthonormal basis of v and matrix $m(T) \epsilon A(V)$ and

$(\alpha_{ij}) = matrix\ of\ (T) \epsilon A(V)$ in this basis,

To prove $\beta_{ij} = matrixof\ T^* \epsilon A(v)$ in this basis where $\beta_{ij} = \overline{\alpha_{ji}}$

Define $v_i T = \sum_{j=1}^{n} \alpha_{ij} v_j$

$$v_i T^* = \sum_{j=1}^{n} \beta_{ij} v_j \ , v_j$$

$$(v_i T^*, v_j) = (\sum_{j=1}^{n} \beta_{ij} v_j, v_j)$$

$$= (\beta_{i1} v_1 + \beta_{i2} v_2 + \cdots + \beta_{ij} v_j + \cdots + \beta_{in} v_n, v_j)$$

$$= (\beta_{i1} v_1, v_j + \beta_{i2} v_2, v_j + \cdots + \beta_{ij} v_j, v_j + \cdots + \beta_{in} v_n, v_j)$$

$$= \beta_{i1}(v_1, v_j) + \beta_{i2}(v_2, v_j) + \cdots + \beta_{ij}(v_j, v_j) + \cdots + \beta_{in(}v_n, v_j)$$

$$= \beta_{i1}(0) + \beta_{i2}(0) + \cdots + \beta_{ij}(1) + \cdots + \beta_{in}(0)$$

$$(v_i T^*, v_j) = \beta_{ij}$$

$$\beta_{ij} = (v_i T^*, v_j)$$

$$= (v_i, v_j T) = (v_i, (\sum_{i=1}^{n} \alpha_{ji}, v_i)$$

$$= (v_i, \alpha_{j1} v_1) + (v_i, \alpha_{j2} v_2) + \cdots + (v_i, \alpha_{ji} v_i) + \cdots + (v_i, \alpha_{jn} v_n)$$

$$= \overline{\alpha_{j1}}(v_i, v_1) + \overline{\alpha_{j2}}(v_i, v_2) + \cdots + \overline{\alpha_{ji}}(v_i, v_i) + \cdots + \overline{\alpha_{jn}}(v_i, v_n)$$

$$= \overline{\alpha_{j1}}(0) + \overline{\alpha_{j2}}(0) + \cdots + \overline{\alpha_{ji}}(1) + \cdots + \overline{\alpha_{jn}}(0)$$

$$\Rightarrow \beta_{ij} = \overline{\alpha_{j1}}$$

Definition:

Hermitian transformation:

$T \epsilon A(V)$ is called hermitian transformation or self adjoint if $T^* = T$

Skew hermitian transformation:

$T\epsilon A(V)$ is called Skew hermitian transformation if $T^* = -T$

Result:

If $S\epsilon A(v)$

$$S = \frac{S+S^*}{2} + i(\frac{S-S^*}{2i})$$

Where $\frac{S+S^*}{2}$ and $(\frac{S-S^*}{2i})$ are Hermitian ie) $S = A + iB$ where A and B are Hermitian.

Theorem 6.10.3:

All the characteristic roots of hermitian transformation are real.

Proof:

Let $T\epsilon A(V)$ be the hermitian transformation

Let λ be the characteristic roots of T there exist $av \neq 0$ $such\ that\ vT = \lambda v \rightarrow$ 1

Consider $\lambda(v.v) = (\lambda v, v)$

$$= (vT, v)$$

$$= (v, vT^*)$$

$$= (v, vT)$$

$$= \overline{\lambda}\,(v, v)$$

$$\Rightarrow \lambda(v, v) - \overline{\lambda}\,(v, v) = 0$$

$$\lambda - \overline{\lambda} = 0$$

$$\lambda = \overline{\lambda}$$

Hence λ is real .

Lemma 6.10.6:

If $S\epsilon A(V)$ and if $vSS^* = 0$ then $vS = 0$

Consider $(vSS^*, v) = (0, v) = 0$

$$(vSS^*, v) = 0$$

$(vS, vS) = 0$

$vS = 0$

Definition:

Normal linear transformation:

$T \epsilon A(V)$ is said to be a normal if $TT^* = T^*T$

Lemma 6.10.7:

If N is normal linear transformation and if $vN = 0, v\epsilon V$

$$vN^* = 0$$

Proof:

Given that $vN = 0$ for $v\epsilon V$

To prove $vN^* = 0$

Consider $(vN^*, vN^*) = (vN^*N, v)$

$= (vNN^*, v)$

$= (0.N^*, v)$

$= (0, v)$

$(vN^*, vN^*) = 0$

$vN^* = 0$

Corollary 1:

If λ is the characteristic roots of the normal transformation N and if $vN = \lambda v$

$then\ vN^* = \bar{\lambda}\, v$

Proof:

Given that λ is the characteristic roots of the normal transformation N and $vN = \lambda v \rightarrow 1$

Then To prove $vN^* = \bar{\lambda}\, v$ N is normal $\Rightarrow NN^* = N^*N$

Consider $(N - \lambda)(N - \lambda)^* = (N - \lambda)(N^* - \bar{\lambda})$

$$= NN^* - N\overline{\lambda} - \lambda N^* + \lambda\overline{\lambda}$$

$$= N^*(N - \lambda) - \overline{\lambda}(N - \lambda)$$

$$(N - \lambda)(N - \lambda)^* = (N - \lambda)(N^* - \overline{\lambda})$$

$\Rightarrow (N - \lambda)$ is normal

Consider $v(N - \lambda) = vN - v\lambda$

$$= v\lambda - v\lambda$$

$$v(N - \lambda) = 0$$

By the lemma "If N is normal and if $vN = 0$ then $vN^* = 0$

$\because (N - \lambda)$ is normal

$\Rightarrow v(N - \lambda) = 0$

$\Rightarrow v(N - \lambda)^*$

$\Rightarrow vN^* = v\overline{\lambda}$

$\therefore vN^* = \overline{\lambda} v$

Corollary 2:

If T is unitary and λ is the characteristic roots of T then $|\lambda| = 1$

To prove:

Given that T is unitary and λ is the characteristic root of T

To prove $|\lambda| = 1$

$\therefore T\ is$ unitary

$\Rightarrow TT^* = T^*T = 1$

$\Rightarrow T$ is normal

$\because \lambda$ is the characteristic root of T

There exist $v \neq 0$ such that $vT = \lambda u$

By the corollary $vT^* = \overline{\lambda} v$

Consider $v = v.1$

$= vTT^*$

$= \lambda v T^*$

$1 = \lambda \bar{\lambda}$

$1 = | \lambda |$

Corollary:

If T is hermitian and $vT^k = 0, k \geq 1$ $then\ vT = 0$

Proof:

Given that T is hermitian and $vT^k = 0, k \geq 1$

$$\Rightarrow T = T^*$$

To prove $vT = 0$

We show that if $vT^{2^m} = 0$ $then\ vT = 0\ for\ if\ S = T^{2^{m-1}}$

$$S^* = (T^{2^{m-1}})^*$$

$$= T^{2^{m-1}}$$

$$S^* = S$$

$$SS^* = \left(T^{2^{m-1}}\right)(T^{2^{m-1}})$$

$$= T^{(2^{m-1}+2^{m-1})}$$

$$= T^{2.2^{m-1}}$$

$$= T^{2.^{m-1+1}}$$

$$= T^{2^m}$$

Continuing down in this way we obtain $vT = 0$ if $vT^k = 0$ then $vT^{2m} = 0$ for 2m$> k$

Hence $vT = 0$.

.

Lemma 6.10.8 : If N is Normal and if $vN^k=0$ then $vN=0$.

Proof:

Let $S=NN^*$, To prove that S is Hermitian.

Consider, $S^k=(NN^*)^k$

$=(N)^k (N^*)^k$

$vS^k=v(N)^k (N^*)^k$

$=0. (N^*)^k$

$vS^k =0$

By the Corollary to Lemma 6.10.6, If T is Hermitian and $vT^k =0$ then $vT=0$

$vS^k =0$ which Implies $vS=0$

implies $v(NN^*)=0$

implies $v(NN^*)=0$

By the Lemma, "If $s \in A(v)$ and if $vSS^*=0$ then $vS=0$".

Implies $vN=0$.

Corollary:

If N is Normal and if for $\lambda\in F$, $v(N-\lambda)^k =0$ then $vN=\lambda v$.

Proof:

Given that N is Normal ===>$NN^* = N^*N$

To prove that $(N-\lambda)$ is normal.

That is To prove that $(N-\lambda) (N-\lambda)^*= (N-\lambda)^* (N-\lambda)$

Consider $(N-\lambda) (N-\lambda)^*= (N-\lambda) (N^*-\bar{\lambda})$

$= N^*N - N\bar{\lambda} - \lambda N^* + \lambda\bar{\lambda}$

$= N^*N - \lambda N^* - N\bar{\lambda} + \lambda\bar{\lambda}$

$= N^*(N-\lambda) - \bar{\lambda}(N-\lambda)$

$= (N^*-\bar{\lambda})(N-\lambda)$

$= (N-\lambda)^*(N-\lambda)$

Which implies $(N-\lambda)$ is Normal.

By the above Lemma, $v(N-\lambda)^k = 0$

$\Longrightarrow v(N-\lambda) = 0$

$\Longrightarrow vN - v\lambda = 0$

$\Longrightarrow vN-=v\lambda$

$\Longrightarrow vN-=\lambda v$

Lemma :6.10.9

Let N be a Normal transformation and suppose that λ and μ are 2 distinct characteristic roots of N. If v and w are in V and are such that $vN = \lambda v$, $wN = \mu w$

then $(v,w) = 0$.

Proof:

Given that N is Normal and λ and μ are 2 distinct characteristic roots of N and $vN = \lambda v$, $wN = \mu w$.

To prove that $(v,w) = 0$.

Consider $vN = \lambda v$

$(vN,w) = (\lambda v,w)$

$= \lambda(v,w)$ -------- (1)

Consider wN=μw.

In the Corollary, "If λ is a characteristic root of the normal transformation N and if vN $=\lambda$v then $vN^* = \bar{\lambda}$ v".

We get, wN^* = ⍰ w

(v,wN^*) = (v, ⍰ w)

= μ (v,w)

(vN,w) = μ (v,w) ------------ (2)

From (1) & (2) ===>

λ (v,w) = μ (v,w)

λ (v,w) - μ (v,w) = 0

(λ-μ) (v,w) = 0

===> (v,w) = 0.

Theorem : 6.10.4

If N is a Normal linear transformation on v, then there exists an orthonormal basis consisting of Characteristic vectors of N, in which the matrix of N is diagonal. Equivalently, if N is a normal matrix there exists an unitary matrix U such that UNU^{-1} (= UNU^*) is diagonal.

Proof:

Prove the corollary If N is Normal and if for $\lambda \in$ F, $v(N-\lambda)^k = 0$ then vN=λv

Let N be Normal. Let $\lambda_1,\lambda_2,\ldots\lambda_k$ be the distinct characteristic roots of N.

By the corollary, "If all the distinct characteristic roots $\lambda_1,\lambda_2,\ldots\lambda_k$ of T lying F then V can be written as $V=V_1 \oplus V_2 \oplus \ldots\ldots \oplus V_k$ where $v_i = \{v \in V \,/\, v(T-\lambda_i)^{l_i} = 0\}$ and where T_i has only one Characteristics roots λ_i on v_i.

We can decompose $V=V_1 \oplus V_2 \oplus \ldots\ldots \oplus V_k$ where every $v_i \in V_i$ is annihilated by $(N-\lambda_i)^{n_i}$.

By the above corollary, v_i consists only of characteristic vectors of N belonging to λ_i.

The inner product of V induces an inner product on v_i. By the theorem, let v be a finite dimensional inner product space then v has an orthonormal set as a basis. V_i has an orthonormal basis related to this inner product. By the lemma, elements lying in distinct v_i are orthogonal.

Thus putting together the orthonormal basis are v_i 's provides as with an orthonormal basis of v. This basis consists of characteristic vectors of N. Thus in this basis the matrix of n is diagonal.

Corollary:1

If T is an unitary transformation then there is an orthonormal basis in which the matrix of t is diagonal equivalently if T is a unitary matrix then there is a unitary matrix U such that UTU^{-1} (= UTU^*) is diagonal.

Corollary:2

If T is a Hermitian linear transformation then there is an orthonormal basis in which the matrix of t is diagonal equivalently if T is a Hermitian matrix then there is a unitary matrix U such that UTU^{-1} (= UTU^*) is diagonal.

Lemma 6.10.10

The Normal transformation N is

(i) Hermitian<===> its characteristics roots are real

(ii) Unitary <===> its characteristics roots are all of absolute value 1.

Proof:

Given that N is Hermitian and N is Normal.

(i) ===> N has only real characteristic roots . Hence if N is Hermitian then its characteristics roots are real.

If N is normal and has only real characteristics roots. To p.t N is Hermitian.

Consider for sum unitary matrix U , $D = UNU^{-1}$ $(= UNU^{*})$ where D is a diagonal matrix with real entries on the diagonal.

$\implies D^{*}=D$

Consider $D^{*}= (UNU^{*})^{*}$

$= (U^{*})^{*}N^{*}U^{*}$

$D^{*}= U N^{*}U^{*}$

$D^{*}=D \implies U N^{*}U^{*} = UN U^{*}$

$\implies N^{*}=N$

$\implies$ N is Hermitian.

(ii) **Proof:**

G.T N is unitary and N is normal. Let λ be the characteristics roots of N. by the corollary, " If T is unitary and if λ is a characteristics roots of T ".

Then $|\lambda| =1$, we have the characteristics roots of N are all of absolute value 1. Given that N is Normal and its characteristics roots are all of absolute value 1.

(ie)., $\lambda\bar{\lambda} = 1$ where λ is a characteristic roots of N.

Converse:

To Prove N is unitary.

By the Defn of characteristic roots, $vN = \lambda v$----- (1) with $v\neq 0$ in V.

By the corollary, if λ is a characteristic root of the Normal transformation N and $vN = \lambda v$ then $vN^{*} =\bar{\lambda} v$.

We get, $vN^{*} =\bar{\lambda} v$

$\lambda(vN^{*}) = \lambda(\bar{\lambda} v)$

$\lambda v N^{*} = \lambda\bar{\lambda}\, v$

$vNN^{*}=1.v$

$vNN^{*}=v.1$

$\Longrightarrow NN^{*}=1$

$\Longrightarrow$ N is unitary.

Note: $tr(AA^{*}) = 0 \Longleftrightarrow A = 0$

Lemma : 6.10.11

If N is Normal and AN=NA, then $A N^{*}= N^{*}A$.

Proof:

Given that N is Normal and AN=NA

To P.T, $A N^{*}= N^{*}A$. (ie)., $X= A N^{*}= N^{*}A=0$.

(ie)., to prove $tr(XX^{*}) = 0$

Consider, $XX^{*} = (A N^{*}- N^{*}A) (A N^{*}- N^{*}A)^{*}$

$=(A N^{*}- N^{*}A) [(N^{*})^{*}A^{*}- A^{*}(N^{*})^{*}]$

$= (A N^{*}- N^{*}A) (NA^{*}- A^{*}N)$

$= (A N^{*}- N^{*}A) NA^{*}- (A N^{*}- N^{*}A) A^{*}N$

$= N[(A N^{*}- N^{*}A) A^{*}] - [(A N^{*}- N^{*}A) A^{*}]N$

$= NB-BN=0$ [since AN=NA $\Longrightarrow$ AN-NA=0].

$(XX^{*}) = 0$

$tr(XX^{*}) = tr (0) =0$

By the above Note, X=0

(ie)., $(A N^* - N^* A) = 0$

$\Longrightarrow A N^* = N^* A$.

Definition :

T Positive (OR) Positive Definite (OR) Non-Negative

If the Hermitian Linear transformation $T \geq 0$ and in addition $(vT,v) > 0$ for $v \neq 0$ then T is called T Positive (OR) Positive Definite.

Lemma : 6.10.12

The Hermitian Linear transformation T is Non-Negative **(**Positive) <===> All of its characteristics roots are Non-Negative **(**Positive).

Proof:

Given that T is Non-Negative (ie)., $T \geq 0$.

Let λ be a characteristics root of T and $vT = \lambda v$ for some $v \neq 0$

Consider $vT = \lambda v$

$\Longrightarrow (vT,v) = (\lambda v,v)$

$0 \leq (vT,v) = \lambda(v,v)$

$\Longrightarrow 0 \leq \lambda(v,v)$

$\Longrightarrow \lambda(v,v) \geq 0$

$\Longrightarrow \lambda \geq 0$

===> All of its characteristics roots are Non-Negative **(**Positive).

Converse Part :

Given that T is Hermitian with non-negative characteristics roots.

To P.T $T \geq 0$.

Let $\{v_1,v_2,\ldots,v_n\}$ be an orthonormal basis consisting of characteristics vectors of T.

Let $\lambda_1,\lambda_2,\ldots\lambda_n$ be the non-negative characteristics roots of T under the basis $\{v_1,v_2,\ldots,v_n\}$.

$\Longrightarrow v_iT = \lambda_i v_i$ -----(1) where $\lambda_i \geq 0$

Define $v = \sum_{i=1}^{n} \alpha_i v_i$, $v \in V$

$vT = \sum_{i=1}^{n} \alpha_i v_i\ T$

$= \sum_{i=1}^{n} \alpha_i \lambda_i v_i$ (by (1))

$vT = \sum_{i=1}^{n} \alpha_i \lambda_i v_i$

$(vT,v) = (\sum_{i=1}^{n} \alpha_i \lambda_i v_i\ ,\ \sum_{i=1}^{n} \alpha_i v_i\ )$

$= (\lambda_1\alpha_1 v_1+\ldots+\lambda_n\alpha_n v_n\ ,\ \alpha_1 v_1+\ldots+\alpha_n v_n)$

$= (\lambda_1\alpha_1 v_1,\ \alpha_1 v_1)+\ldots+(\lambda_n\alpha_n v_n,\ \alpha_n v_n)$

$= \lambda_1\alpha_1 (v_1,\ \alpha_1 v_1) +\ldots+ \lambda_n\alpha_n (v_n,\ \alpha_n v_n)$

$= \lambda_1\alpha_1\overline{\alpha_1}\ (v_1,\ v_1) +\ldots+ \lambda_n\alpha_n\overline{\alpha_n}\ (v_n,\ v_n)$

$= \lambda_1\alpha_1\overline{\alpha_1}\ (1) +\ldots+ \lambda_n\alpha_n\overline{\alpha_n}\ (1)$ (since $(v_i,\ v_i) =1$, $(v_i,\ v_j) =0$)

Here $(v_i,\ v_j) =0$, we are not having the terms $\lambda_1\alpha_1\overline{\alpha_1}\ (v_1,\ v_2),\ldots\ldots$

$(vT,v) = \sum_{i=1}^{n} \alpha_i \lambda_i \overline{\alpha_i}$

$(vT,v) \geq 0$

Since by the lemma, " if $T \in A(V)$ is such that $(vT,v) = 0$ for all $v \in V$ then $T= 0$".

We have $T \geq 0$.

Lemma 6.10.13

$T \geq 0 \Longleftrightarrow T = AA^*$ for some A.

Proof :

(i) Consider T= AA^*

To P.t $T \geq 0$ (ie)., $AA^* \geq 0$

Consider, $(v\,AA^*, v) = (vA, v(A^*)^*$

$= (vA, vA)$

≥ 0 (by the defn of Inner Product)

$(v\,AA^*, v) \geq 0$

===> $AA^* \geq 0$ (by the defn of T Positive)

===> $T \geq 0$

(ii) $T \geq 0$ To P.t T= AA^*

Consider the Unitary matrix U such that $UTU^* = \begin{pmatrix} \sqrt{(\lambda_1)} \\ \ldots \\ \sqrt{(\lambda_n)} \end{pmatrix}$ where each λ_i is the characteristic root of T.

since $T \geq 0$ ===> each $\lambda_i \geq 0$

Let $S = \begin{pmatrix} \sqrt{(\lambda_1)} \\ \ldots \\ \sqrt{(\lambda_n)} \end{pmatrix}$ since each $\lambda_i \geq 0$ which implies $\sqrt{\lambda_i} \geq 0$

===> S is Hermitian

(ie)., $S=S^*$.

To Prove that USU^* is Hermitian.

Consider $(USU^*)^* = (U^*)^* S^* U^*$

$= U S^* U^*$

$= US U^*$

$\Longrightarrow (USU^*)^* = US\,U^*$ ------------(1)

$US\,U^*$ is Hermitian.

Consider $(U^* SU)^2 = (U^* SU)(U^* SU)$

$= (U^* SU\,U^* SU)$

$= (U^* S.1.\,SU)$

$= (U^* S^2 U)$

$$= U^*\begin{pmatrix}\sqrt{(\lambda_1)} \\ \dots \\ \sqrt{(\lambda_n)}\end{pmatrix}^2 \quad U$$

$$= U^*\begin{pmatrix}\sqrt{(\lambda_1)} \\ \dots \\ \sqrt{(\lambda_n)}\end{pmatrix} \quad U$$

$= U^*(UT\,U^*)U$

$= U^*UT\,U^*U$

$(U^* SU)^2 = 1.T.1 = T$ ------(2)

Take $A = (U^* SU)$

$\Longrightarrow A^* = (U^* SU)^*$

$A^* = (U^* SU)$ By (1)

(2) $\Longrightarrow T = (U^* SU)^2 = (U^* SU)\ (U^* SU)$

$T = AA^*$ for some A.

6.11 Real Quadratic forms

Definition : Quadratic form associated with A.

Let V be a Real Inner Product space and suppose that a is a (real) symmetric linear transformation on V. The real valued function Q(v) defined on V by Q(v) =(vA,v) is called the quadratic form associated with A.

Definition : Congruent Matrices

Two real symmetric matrices of A and B are congruent matrices if there is a non-singular real matrix T such that $B=TAT^{-1}$.

Lemma 6.11.1

Congruence is an equivalence relation.

Proof:

Let us denote A is congruent to B has $A \cong B$

(i) Reflexive:

To p.t $A \cong A$

$A= IAI^{-1}$ where I is an identity matrix. ===> $A \cong A$.

(ii) Symmetric:

Consider $A \cong B$ To P.t $B \cong A$

$A \cong B$ ===> $B = TAT^{-1}$ (where T is non-singular)

$T^{-1}B = T^{-1}TA\, T^{-1}$

$= IA\, T^{-1}$

$T^{-1}BT= A\, T^{-1}T$

$T^{-1}BT= A\, I$

$T^{-1}BT= A$

$T^{-1}B(T^{-1}) = A$

Let $(T^{-1}) = S$ ===> $SBS^{-1} = A$ where S is non-singular.

===> $B \cong A$.

(iii) Transitive:

Let $A \cong B$ & $B \cong C$. To p.t $A \cong C$.

$A \cong B$ ===> $B = TAT^{-1}$

$B \cong C$ ===> $C = SBS^{-1}$ where S & T are non-singular.

$C = SBS^{-1} = S(TAT^{-1})\, S^{-1}$

$= (ST)\, A(T^{-1}S^{-1})$

$= (ST)\, A\, (ST)^{-1} = RAR^{-1}$

$C = RAR^{-1}$

===> $C \cong A$.

Hence congruence is an equivalence relation.

Definition : Signature of A

If A is a real symmetric matrix congruent to $\begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0_t \end{pmatrix}$ then r-s is called the signature of A. The signature of a quadratic form is defined to be the signature of the associated symmetric matrix.

Result (1):

Let A be a symmetric matrix and let us consider associated quadratic form $Q(v) = (vA,v)$. If T is non-singular and real given $v \in F^{(n)}$, $v = wT$ for some $w \in F^{(n)}$. Hence $(vA,v) = (wTA,wT)$.

Thus A and ATA^{-1} effectively define the same quadratic form.

Result (2):

Given a real orthogonal matrix , we can fixed an orthogonal matrix T such that $TQT^{-1} = TQT^{'}$.

Theorem 6.11.1 (Sylvester's Law)

Given be the real symmetric matrix A there is an invertible matrix T such that

$TAT^{-1} = \begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0_t \end{pmatrix}$ where I_r and I_s are respectively r x r and s x s unit matrices and 0_t is the t x t zero matrix. The integer r+s which is be rank of A and r-s which is the signature of A ,characterize the congruence class of A. (ie)., two real symmetric matrices are congruent iff they have the same rank and signature.

Proof:

A isreal symmetric matrix , its characteristic roots are real. Let $\lambda_1, \lambda_2, \dots \lambda_r$ be its characteristic roots.Let $-\lambda_{r+1}, -\lambda_{r+2}, \dots, -\lambda_{r+s}$ be its negative characteristic roots .

We can find a real orthogonal matrix C, such that

$$CAC^{-1} = CAC^{'} = \begin{pmatrix} \lambda_1 & & & & & & & \\ & \ddots & & & & & & \\ & & \lambda_r & & & & & \\ & & & -\lambda_{r+1} & & & & \\ & & & & \ddots & & & \\ & & & & & -\lambda_{r+s} & & \\ & & & & & & \ddots & \\ & & & & & & & 0_t \end{pmatrix}$$

Where t=n- r s. (here n = r+s+t). Let T be the real diagonal matrix

$$D=\begin{pmatrix} \frac{1}{\sqrt{\lambda_1}} & & & & & & \\ & \ddots & & & & & \\ & & \frac{1}{\sqrt{\lambda_r}} & & & & \\ & & & \frac{1}{\sqrt{\lambda_{r+1}}} & & & \\ & & & & \ddots & & \\ & & & & & \frac{1}{\sqrt{\lambda_{r+s}}} & \\ & & & & & & I_t \end{pmatrix}$$ then the simple computation that

$DCAC' D' = (DC) A(C' D') = \begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0_t \end{pmatrix}$. Thus there is a matrix of the required form in the congruence class of A. Now, to show that this is the only matrix in the congruence class of this form (or) equivalently that $L=\begin{pmatrix} I_r & & \\ & -I_s & \\ & & 0_t \end{pmatrix}$ and $M = \begin{pmatrix} I_r{}' & & \\ & -I_s{}' & \\ & & 0_t{}' \end{pmatrix}$ are congruent only if $r = r'$, $s = s'$ and $t = t'$.

To p.t $r = r'$, $s = s'$ and $t = t'$.

Suppose that $M=TLT'$ where T is invertible (by lemma $L \cong M$)

If v is a finite dimensional vector space over F and if $S \in A(V)$ and $T \in A(V)$ is regular then $r(S) = r(TST^{-1})$.

$M = TLT^{-1} \Longrightarrow r(M) = r(TLT^{-1}) = r(L)$

$n-t' = n-t \Longrightarrow t' = t$.

To prove $r = r'$ and $s = s'$

Suppose $r < r'$, $n = r+s+t = r'+s'+t'$

$\Longrightarrow s - s' = r - r' \Longrightarrow s > s'$

Let U be the subspace of $F^{(n)}$ for all vectors having the first r and the last t coordinates 0. Therefore U is s-dimensional. For $u \neq 0 \in U$, $(uL,u) < 0$. Let W be the subspace of

$F^{(n)}$ for which $r'+1,\ldots,r'+s$ are zero.Since T is invertible and W is $(n-s')$dimensional. WT is $(n-s')$ dimensional. For $w \in W$, $(wM,w) \geq 0$. Hence $(wTL, wT) \geq 0$ for all elements.

Now dim (WT)+ dim U = $n-s' + r = n+s-s' > n$. by the corollary to lemma 4.2.6, $WT \cap U \neq 0$. This however is nonsense. For if $x \neq 0 \in WT \cap U$, $(xL,x) < 0$ while on the other hand, being in WT, $(xL,x) \geq 0$. Thus $r = r'$ and $s = s'$.

The rank r+s, and signature r-s , determine r,s and t = (n-r-s) , hence they determine the congruence class.

Distribution of Marks: Theory 100%

Text Books:

S.NO	**AUTHORS**	**TITLE**	**PUBLISHERS**	**YEAR OF PUBLICATION**
1.	I.N.Herstein	Topics in Algebra	Wesley Wiley Eastern Limited, New Delhi	1975, II Edition

Reference Books:

S.NO	**AUTHORS**	**TITLE**	**PUBLISHERS**	**YEAR OF PUBLICATION**

1	M.Artin	Algebra	Prentice Hall of India	1991
2	P.B.Bhattacharya, S.K.Jain, and S.R.Nagpaul	Basic Abstract Algebra	Cambridge University Press	1997
3	Rudin, W I.S. Luther and I.B.S.Passi	. Algebra, Vol. I- Groups and Vol.II Rings	Narosa Publishing House,New Delhi	1999.

Web Sources:

1. abstact.ups.edu>aata-20160809.

2. mathforum.org>…>Algebra