Lemma 1.28 *There is a* $1-1$ *correspondence between any two right cosets of H in G.*

Theorem 1.29 ***Lagrange's Theorem:*** *If G is a finite group and H is a subgroup of G, then* $O(H)$ *is the divisor of* $O(G)$*, converse of the Lagrange's theorem need not be true.*

Example 1.30 1. *Let* $G = \{1, -1, i, -i\}$, $H = \{i, -1\}$. *Then* $O(H)/O(G)$ *but H is not a subgroup of G.*

2. *Let* $G = S_3 = \{e, p_1, p_2, p_3, p_4, p_5\}$, $H = \{p - 1, p_2\}$. *Then* $O(H)/O(G)$ *but H is not a subgroup of G.*

Definition 1.31 Index: *If H is a subgroup of G, the index of H in G is the number of distinct right cosets of H in G. It is denoted by* $i_G(H)$.

Remark 1.32 $i_G(H) = \frac{O(G)}{O(H)}$

Example 1.33 *Let* $G = \{Z_{12}, \oplus_{12}\}$; $H = \{0, 4, 8\}$. *Then* $i_G(H) = 4 = 12/3 = \frac{O(G)}{O(H)}$

Definition 1.34 *If G is a group and* $a \in G$*. The order of a (period of a) is the least positive integer m such that* $a^m = e$*. If no such integer exists, we say that a is of infinite order.*

Example 1.35 *Let* $G = \{1, -1, i, -i\}$

1. $a = -1 \Rightarrow a^2 = (-1)^2 = 1 \Rightarrow O(a) = 2$

2. $a = i \Rightarrow a^4 = i^4 = 1 \Rightarrow O(a) = 4$.

Example 1.36 *In* $(Z_{12}, \oplus)$, $O[2] \in Z_{12}$
Now, $O([2]) = 6$ $\{\because [2]^6 = [2] + [2] + [2] + [2] + [2] + [2] = 0\}$
$O[3] = 4$; $O([6]) = 2$.

Example 1.37 *Let* $(Z, +)$, $e=0$. *Then* $1 \in Z$ *is of infinite order.*

Corollary 1.38 *If G is a finite group and* $a \in G$*, then* $O(a)$ *divides* $O(G)$.

Corollary 1.39 *If G is finite and* $a \in G$*, then* $a^{O(G)} = e$.

Definition 1.40 ***Euler function*** $\varphi(n)$: $\varphi(1) = 1$, $\varphi(n)$ = *number of posi- tive integers less than n and relatively prime to n for* $n > 1$.
$\varphi(8) = 4$ ($\because$ 1, 3, 5, 7 *are relatively prime to* 8), $\varphi(5) = 4$, $\varphi(7) = 6$, $\varphi(10) = 4$, $\varphi(15) = 7$.

Example 1.94

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4) \quad = \quad \textit{even permutation}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = (1\ 2)\ (3)\ (4\ 5) = \textit{odd permutation}$$

Result 1.95 *A permutation can be written either as a product of an even number of transpositions or as a product of an odd number of transpositions and not both.*

Proof: Let $\vartheta \in S_n$

Suppose ϑ can be written as a product of X transpositions in one way and can be written as a product of Y transpositions in another way. Consider a polynomial in variables $x_1, x_2, ..., x_n$ which are the elements of S.

$$P\,(x_1, x_2, ..., x_n) = \prod_{i<j} (x_i - x_j).$$

Let $\vartheta \in S_n$ be a permutation on n-symbols $1, 2, ..., n$. Let ϑ be act on $P\,(x_1, x_2, ..., x_n)$ by

$$\vartheta : P\,(x_1, x_2, ..., x_n) = \prod_{i<j} (x_i - x_j) \to \prod_{i<j} (x_{\vartheta(i)} - x_{\vartheta(j)}).$$

It is clear that $\vartheta : P\,(x_1, x_2, ..., x_n) \to \pm P\,(x_1, x_2, ..., x_n)$. For example, consider $\vartheta = (1\ 3\ 4)\ (2\ 5) \in S_5$. Then $P\,(x_1, x_2, ..., x_5) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)$; $\vartheta(P\,(x_1, x_2, ..., x_5)) = (x_3 - x_5)(x_3 - x_4)(x_3 - x_1)(x_3 - x_2)(x_5 - x_4)(x_5 - x_1)(x_5 - x_2)(x_4 - x_1)(x_4 - x_2)(x_1 - x_2) = -[(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)] = -P\,(x_1, x_2, ..., x_5)$.
Suppose $\vartheta = (1, 2) \in S_2$; $P\,(x_1, x_2) = (x_1 - x_2)$; $\vartheta(P\,(x_1, x_2)) = (x_2 - x_1) = -(x_1 - x_2) = -P\,(x_1, x_2)$. (i.e)The effect of a transposition on P is to change the sign of P. Now the operation by a transposition (rs) where $r < s$ has the following effects on P.

(i) Any factor of P which contains neither the suffix r nor s remains un- changed

(ii) The single factor $(x_r - x_s)$ changes its sign by replacing r by s and s by r

(iii) The remaining factor which contain either the suffix r (or) s but not both can be grouped into the following 3 types of products.

(a) $[(x_1 - x_r)(x_1 - x_s)][(x_2 - x_r)(x_2 - x_s)]...[(x_{r-1} - x_r)(x_{r-1} - x_s)]$

(b) $[(x_r - x_{r+1})(x_{r+1} - x_s)][(x_r - x_{r+2})(x_{r+2} - x_s)]...[(x_r - x_{s-1})(x_{s-1} - x_s)]$

(c) $[(x_r - x_{s+1})(x_s - x_{s+1})][(x_r - x_{s+2})(x_s - x_{s+2})]...[(x_r - x_n)(x_s - x_n)]$ On replacing r by s and s by r, the signs of all types of products do not change. Hence effect of the transposition (rs) on P is to change the sign of

2. UNIT II

Another Counting Principle

Definition 2.1 *If $a, b \in G$, then b is said to be a conjugate of a in G if there exists an element $c \in G$ such that $b = c^{-1}ac$. We shall write this conjugate relation as $a \sim b$. (i.e.) $a \sim b \Rightarrow b$ is conjugate to $a \Rightarrow b = c^{-1}ac$, $c \in G$.*

Lemma 2.2 *Conjugation is an equivalence relation on G.*
Proof: (i) $\sim$ is reflexive:
Let $a \in G$, then $a = a^{-1}ae$, $a \in G \Rightarrow a \sim a$ $\forall a \in G$. $\therefore \sim$ is reflexive.
(ii) $\sim$ is symmetric:
Suppose, $a \sim b \Rightarrow b = c^{-1}ac$, $c \in G$. $\Rightarrow a = c\,b\,c^{-1} = (c^{-1})^{-1}b(c^{-1}) = x^{-1}bx$, $x = c^{-1} \in G \Rightarrow b \sim a$. $\sim$ is symmetric. (iii) $\sim$ is transitive:
Suppose $a \sim b$ and $b \sim c$. Then $a \sim b \Rightarrow b = x^{-1}ax$, $x \in G$; $b \sim c \Rightarrow c = y^{-1}by$, $y \in G$. Now, $c = y^{-1}by = y^{-1}(x^{-1}ax)y = (y^{-1}x^{-1})a(xy) = (xy)^{-1}a(xy) = z^{-1}az$, $z = xy \in G \Rightarrow a \sim c$. $\therefore \sim$ is transitive.
Hence, $\sim$ is an equivalence relation.

Definition 2.3 *For any $a \in G$, let $C(a) = \{x \in G | x \sim a\}$, $C(a)$ is the equivalence class a in G, under the relation $\sim$. It is usually called the conjugate class of $a \in G$*

Remark 2.4 $C(a) = \{x \in G | x \sim a\} = \{x \in G | a \sim x\} = \{x \in G | x = y^{-1}ay,\ y \in G\} = \{y^{-1}ay | y \in G\}$. *It consists of the set of all distinct el- ements of the form $x^{-1}ax$ as x ranges over G. Suppose the number of elements in $C(a)$ is denoted by Ca. Since the union of all distinct conjugate classes is G*

$$G = C(a_1) \cup C(a_2) \cup \dots \cup C(a_n)$$

$$O(G) = Ca_1 + Ca_2 + \dots + Ca_n = \sum_{a_i \in G} Ca_i$$

Where the summation runs over each element a in each conjugate classes.

Definition 2.5 *If $a \in G$, $N(a)$, normaliser of a is defined as $\{x \in G | ax = xa\}$*

Example 2.6 *(i) $G = \{1, -1, i, -i\}$. When $a = 1$, $N(a) = N(1) = \{1, -1, i, -i\} = G$; When $a = -1$, $N(-1) = G$.*
(ii) $G = \{Z_5, \oplus_5\}$. $a = [2]$, $N(a) = N([2]) = \{[0], [1], [2], [3], [4]\}$
(iii) $G = S_3 = \{e, \varphi, \psi, \varphi \cdot \psi, \psi \cdot \varphi, \psi^2\}$. $N(\varphi) = \{e, \varphi\}$; $N(\psi) = \{e, \psi, \psi^2\}$; $N(\psi^2) = \{e, \psi^2, \psi\}$.

Lemma 2.7 *$N(a)$ is a subgroup of G.*

Proof: Let $x, y \in N(a) \Rightarrow ax = xa$ and $ay = ya$ .... (1)

Now, $a(xy) = (ax)y = (xa)y$ [by(1)] $= x(ay) = x(ya)$ [by(1)] $= (xy)a \Rightarrow$ $xy \in N(a)\ \forall x, y \in N(a)$ .... (2)

Suppose $x \in N(a) \Rightarrow ax = xa \Rightarrow x^{-1}a = ax^{-1}$ [By premultiply and post multiply by x^{-1}] $\Rightarrow x^{-1} \in N(a)$ .... (3)

By (2) and (3), $N(a)$ is a subgroup of G.

Calculation for $C(a)$:

Let $G = S_3 = \{e, \varphi, \psi, \varphi\cdot\psi, \psi\cdot\varphi, \psi^2\}$. $C(\varphi) = \{x^{-1}\varphi x \mid x \in S_3\} =$ $\{e^{-1}\varphi e, \varphi^{-1}\varphi\varphi, \psi^{-1}\varphi\psi, (\varphi\cdot\psi)^{-1}\varphi(\varphi\cdot\psi), (\psi\cdot\varphi)^{-1}\varphi(\psi\cdot\varphi), (\psi^2)^{-1}\varphi\psi^2\}$

$C(1, 2) = \{e^{-1}(1, 2)e, (1, 2)^{-1}(1, 2)(1, 2), \psi^{-1}(1, 2)\psi, (\varphi\cdot\psi)^{-1}(1, 2)(\varphi\cdot\psi), (\psi\cdot\varphi)^{-1}(1, 2)(\psi\cdot\varphi), (\psi^2)^{-1}(1, 2)\psi^2\} = \{(1\,2\,3)\,(1\,2)\,(1\,2\,3), (1\,2)\,(1\,2)\,(1\,2),$ $(1\,3\,2)\,(1\,2)\,(1\,3\,2), (1\,3)\,(1\,2)\,(1\,3), (2\,3)\,(1\,2)\,(2\,3), (2\,3\,1)\,(1\,2)\,(1\,3\,2)\} =$ $\{(1\,2), (1\,2), (2\,3)\}$. $\therefore C(\varphi) = \{\varphi, \varphi\cdot\psi, \psi\cdot\varphi\}$

$C_{(1,2)} = O(C(1, 2)) = 3$. $\frac{O(G)}{O(N(1,2))} = \frac{6}{3} = 3$. $\therefore C_{(1,2)} = \frac{O(S_3)}{O(N(1,2))}$.

Theorem 2.8 *If G is a finite group, then $C_a = \frac{O(G)}{O(N(a))}$; In other wards, the number of elements conjugate to a in G is the index of $N(a)$ in G.* **Proof:** We shall show that two elements in the same right coset of $N(a)$ in G, yield the same conjugate of a in G, where as two elements in different cosets of $N(a)$ in G gives rise to different conjugate of a in G. In this way we shall have a 1 − 1 correspondence between conjugate of a in G and the right cosets of $N(a)$ in G. Suppose $x, y \in G$ are in the same right cosets of $N(a)$ in G. Then $y = nx$ where $n \in N(a)$, [$\because y \in N(a)\cdot x, y = nx$] $\Rightarrow y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$; $y^{-1}ay = x^{-1}n^{-1}ay =$ $x^{-1}n^{-1}anx = x^{-1}(n^{-1}an)x = x^{-1}ax$. Hence, x and y result in the same conjugate of a in G. In other wards if x and y are in different right cosets of $N(a)$ in G.

Claim that $x^{-1}ax$ $y^{-1}ay$. Suppose not $x^{-1}ax = y^{-1}ay$. Premultiply by y and post multiply by x^{-1}, then $yx^{-1}axx^{-1} = y(y^{-1}ay)x^{-1} \Rightarrow yx^{-1}a = ayx^{-1} \Rightarrow$ $(yx^{-1})a = a(yx^{-1}) \Rightarrow yx^{-1} \in N(a)$ [$\because ab^{-1} \in H \Leftrightarrow Ha = Hb$] $\Rightarrow N(a)\cdot y = N(a)\cdot x$ $\Rightarrow x$ and y to be in the same right cosets of $N(a)$ in $G \Rightarrow\Leftarrow$ to the fact that x and y are in different right coset of $N(a)$ in G. $\therefore x^{-1}ax \neq y^{-1}ay$. Hence x and y yield the different conjugate of a in G if they are in different right cosets of $N(a)$ in G. $\therefore$ The number of elements conjugate to a in G = number of distinct right cosets of $N(a)$ in G. (i.e.) the number of elements conjugate to a in G = the index of normaliser of a in G. (i.e.) $C_a = \frac{O(G)}{O(N(a))}$. Hence, the theorem.

Corollary 2.9

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

+ is well define:
Suppose $[a, b] = [a', b']$ and $[c, d] = [c', d']$, then $[a, b]+[c, d] = [a', b']+[c', d']$. To Prove: $[ad+bc, bd] = [a'd'+b'c', b'd']$. It is enough to prove $(ad+bc)b'd' = bd(a'd' + b'c')$. Now, $[a, b] = [a', b'] \Rightarrow ab' = ba'$ (1)
and $[c, d] = [c', d'] \Rightarrow cd' = dc'$ (2)

$$\begin{aligned}(ad+bc)b'd' &= adb'd' + bcb'd'\\ &= ab'dd' + bb'cd'\\ &= ba'dd' + bb'dc'\\ &= bd(a'd' + b'c')\end{aligned}$$

∴ + is well defined.
+ is closed:
Let $[a, b], [c, d] \in F$. Then D is an integral domain, $bd \neq 0$. Now, $[a, b] + [c, d] = [ad + bc, bd] \in F$ [∵ $bd \neq 0$]. ∴ + is closed.
+ is associative:

$$\begin{aligned}([a, b] + [c, d]) + (e, f) &= [ad + bc, bd] + (e, f)\\ &= [(ad + bc)f + (bd)e, (bd)f]\\ &= [adf + bcf + bde, bdf]\\ &= [adf + (bcf + bde), bdf]\\ &= [a(df) + b(cf + de), bdf]\\ &= [a, b] + [cf + de, df]\\ &= [a, b] + ([c, d] + [e, f])\end{aligned}$$

∴ + is associative.
Additive identity:
$[0, b] \in F$ acts as zero element for this addition. For $[a, b] + [0, b] = [ab + 0, b^2] = [ab, b^2] = [a, b]$.
Additive inverse:
$[-a, b]$ acts as a identive inverse of $[a, b]$. For $[-a, b]+[a, b] = [-ab+ba, b^2] = [0, b^2]$.
+ is commutative:
$[a, b]+[c, d] = [ad+bc, bd] = [bc+ad, bd] = [cb+da, bd] = [c, d]+[a, b]$ $\forall$ $[a, b]+ [c, d] \in F$.
∴ + is commutative.
∴ $(F, +)$ is an abelian group.
· is well defined:
Suppose $[a, b] = [a', b']$ and $[c, d] = [c', d']$. To Prove $[a, b] \cdot [c, d] = [a', b'] \cdot [c', d']$ (i.e.) $[ac, bd] = [a'c', b'd']$. It is enough to prove that $(ac)(b'd')=$

$\frac{d}{m}\lambda(x)$, where $d = (c_0, c_1, c_2, \ldots, c_n)$, $\lambda(x)$ is primitive and d and m are integers. Similarly $v(x) = \frac{d_1}{m_1} l_1(x)$, where d_1 and m_1 are integer and $l_1 x$ is primitive. $\therefore f(x) = u(x) \cdot v(x) = \frac{d}{m} \cdot \frac{d}{m_1} \cdot \lambda(x) l_1(x) = \frac{a}{b}\lambda(x) l_1(x)$.............. (2) where $a = dd_1$ and $b = mm_1$ are integers $\Rightarrow bf(x) = a\lambda(x)l_1(x)$.................... (3) $\Rightarrow c(bf(x)) = c(a\lambda(x)l_1(x)) \Rightarrow bc(f(x)) = ac(\lambda(x)l_1(x)) \Rightarrow b = a$......................... (4) [$\because f(x)$, $l_1(x)$, $\lambda(x)$ are primitive, their content is 1]. From (2) and (4), $f(x) = \lambda(x)l_1(x)$. $\therefore f(x)$ can be factored as a product of two polynomial havingtwo integer coefficient. [$\lambda(x)$ and $l_1(x)$ are polynomial having integer coefficient]. Hence the theorem.

Corollary 3.68 *If an integer monic polynomial factors as the product of two non-constant polynomials having rational coefficients then it factors as the product of two integer monic polynomials.*

Proof: $f(x)$ is an integer monic polynomial and factored as a product of two non-constant polynomials having rational coefficients. (i.e.) $f(x)$ is a primitive polynomial factored as the product of two polynomial having rational coefficients. By Theorem 3.67 $f(x)$ can be factored as product of two polynomials having integer coefficients. Let $f(x) = p(x) \cdot r(x)$, where $p(x)$, $r(x)$ are polynomial with integer coefficient. Let $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ and $r(x) = b_0 + b_1x + b_2x^2 + \ + b_mx^m$, where a_i's and b_j's are integers. $\because f(x)$ is monic, leading coefficient of $f(x)$ is 1. Then leading coefficient of $p(x) \cdot r(x) = 1 \Rightarrow a_n = b_m = 1 \Rightarrow$ either $a_n = b_m = 1$ (or) $a_n = b_m = -1$. $\therefore$ In either case, $p(x)$, $r(x)$ are integer monic polynomials. Hence $f(x)$ can be factoredastheproductoftwointegermonicpolynomials.

Example 4.27 *In the vector space* $F^{(n)} = V_n(F) = \{(\alpha_1, \alpha_2, ..., \alpha_n)\}$. *Then the vector space* $S = \{e_1, e_2, ..., e_n\}$ *where* $e_1 = \{1, 0, ..., 0\}$; $e_2 = \{0, 1, 0, ..., 0\}$; ...; $e_n = \{0, 0, ..., 1\}$ *is linearly independent. Let* $\lambda_1, \lambda_2, ..., \lambda_n \in F$. *Then*
$\lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n = 0 \Rightarrow \lambda_1(1, 0, ..., 0) + \lambda_2(0, 1, ..., 0) + ... + \lambda_n(0, 0, ..., 1) = 0 \Rightarrow (\lambda_1, 0, ..., 0) + (0, \lambda_2, ..., 0) + (0, 0, ..., \lambda_n) = 0 \Rightarrow (\lambda_1, \lambda_2, ..., \lambda_n) = 0 \Rightarrow$
$\lambda_1 = 0, \lambda_2 = 0, ..., \lambda_n = 0$.

Remark 4.28 *If the set of vector* $S = \{v_1, v_2 .... v_n\}$ *is linearly independent then none of the vector* $v_1, v_2, ..., v_n$ *be* $\dot{0}$.

Example 4.29 *Show that the set* $S = \{(1, 2, 4), (1, 0, 0), (0, 1, 0)(0, 0, 1)\}$ *is a linearly dependent subset of vector space* $R^{(3)}$ *where R is the field of Real numbers.*
Solution: Let $\lambda_1 = 1, \lambda_2 = -1, \lambda_3 = -2, \lambda_4 = -4$. Then $1(1, 2, 4) + (-1)(1, 0, 0) + (-2)(0, 1, 0) + (-4)(0, 0, 1) = (1, 2, 4) + (-1, 0, 0) + (0, -2, 0) + (0, 0, 4) = (0, 0, 0)$. $\therefore$ Given set is linearly dependent.

Lemma 4.30 *If* $v_1, v_2, ... , v_n$ *are linearly independent then every element in their linear span has a unique representation in the form,* $\lambda_1 v_1 + \lambda_2 v_2 + ... + \lambda_n v_n$ *with* $\lambda_i \in F$.

Result 4.31 *If* $v_1, v_2, ..., v_n \in V$ *then either they are linearly independent or some* v_k *is the linear combination of the preceding one's. If V is a finite dimensional vector space then it contains a finite set* $v_1, v_2, ..., v_n$ *of linearly independent elements whose linear span is V.*

Definition 4.32 ***Basis:*** *A subset S of a vector space V is called a basis of V if S consists of linearly independent elements and* $V = L(S)$. *Let set S consisting of vectors* $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$ *is a basis of* $F^{(3)}$.

Result 4.33

1. *If V is a finite dimensional vector space and if* $v_1, v_2, ... , v_m$ *is span V then some subsets of* $v_1, v_2, ..., v_m$ *forms a basis of V.*
2. *If* $v_1, v_2, ..., v_m$ *is a basis of V over F if* $w_1, w_2, ..., w_m$ *in V are linearly independent over F then* $m \leq n$.
3. *If V be a finite dimensional vector space over F then any two ba- sis of V have the same number of elements. For example,* $S_1 = \{(1, 0, 0), (0, 1, 0), (0, 1, 1)\}$ *and* $S_2 = \{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ *are two basis of the vector space* $F_{(3)}$.
4. $F^{(n)} \cong F^{(m)}$ *iff* $n = m$.
5. *If V be a finite dimensional vector space over a field F then* $V \cong F^{(n)}$ *for a unique integer n, infact n is the number of elements in any basis V over F.*

2. $dim(A(w)) = dim(V) - dim(W)$.

3. $\hat{V}/A(W) \cong \hat{W}$.

4. $A(A(W)) = W$.

Linear Transformation:

We know that $Hom(V, W)$, the set of all vector space homomorphisms of V into W is a vector space over the field F. In this section we are very much interested on $Hom(V, V)$.

Definition 4.45 *An associative ring A is said to be an algebra over F if A is a vector space over a field F such that $a, b \in A$ and $\alpha \in F$, $\alpha(ab) = (\alpha a)b$.*

Remark 4.46 *Every algebra A over a field F is a vector space over a field F. Is the converse true?*

Result 4.47 *$Hom(V, V)$ is an algebra over F.*

Proof: Let $T_1, T_2 \in Hom(V, V)$. Define $+$ and $\cdot$ as follows, $T_1+T_2 : V \to V$ by $v(T_1+T_2) = vT_1+vT_2$ and $T_1 \cdot T_2 : V \to V$ by $v(T_1 \cdot T_2) = (vT_1)T_2 \ \forall v \in V$. We shall first prove that $Hom(V, V)$ is a ring. Let $\alpha, \beta \in F$ and $v_1, v_2 \in V$,

$$\begin{aligned}
(\alpha v_1 + \beta v_2)(T_1 + T_2) &= (\alpha v_1 + \beta v_2)T_1 + (\alpha v_1 + \beta v_2)T_2 \\
&= (\alpha v_1)T_1 + (\beta v_2)T_1 + (\alpha v_1)T_2 + (\beta v_2)T_2 \\
&= \alpha(v_1T_1) + \beta(v_2T_1) + \alpha(v_1T_2) + \beta(v_2T_2) \\
&= \alpha(v_1T_1 + v_1T_2) + \beta(v_2T_1 + v_2T_2) \\
&= \alpha(v_1(T_1 + T_2)) + \beta(v_2(T_1 + T_2))
\end{aligned}$$

$\therefore T_1 + T_2 \in Hom(V, V) \Rightarrow +$ is closed.

Let $T_1, T_2, T_3 \in Hom(V, V)$. Then $T_1+(T_2+T_3) = (T_1+T_2)+T_3 \ \forall T_1, T_2, T_3 \in Hom(V, V) \Rightarrow +$ is Associative.

$0 : V \to V$ defined by $v_0 = 0 \ \forall v \in V$ serve as additive identity element. For $0 + T_1 = T_1 + 0 = T_1 \ \forall T_1 \in Hom(V, V)$.

Inverse of T_1 is $-T_1$ defined by, $v(-T_1) = -(vT_1) \ \forall v \in V$. Since $T_1+(-T_1) = (-T_1 + T_1) = 0$ for $v(T_1 + (-T_1)) = vT_1 + v(-T_1) = vT_1 + (-vT_1) = 0$. Similarly $v(-T_1 + T_1) = 0 \Rightarrow T_1 + (-T_1) = (-T_1) + T_1 = 0$.

$v(T_1 + T_2) = vT_1 + vT_2$ [$vT_1, vT_2 \in V$ and $(V, +)$ is abelian] $= vT_2 + vT_1 = v(T_2 + T_1) \Rightarrow T_1 + T_2 = T_2 + T_1$. $\therefore +$ is commutative. Hence $(Hom(V, V), +)$ is abelian group. Now,

$$\begin{aligned}
(v_1 + v_2)(T_1 \cdot T_2) &= ((v_1 + v_2)T_1) \cdot T_2 \\
&= (v_1T_1 + v_2T_1) \cdot T_2 \\
&= (v_1T_1)T_2 + (v_2T_1)T_2 \\
&= v_1(T_1 \cdot T_2) + v_2(T_1 \cdot T_2)
\end{aligned}$$

Remark 4.64 *If V is finite dimensional over F then an element in $A(V)$ which is right invertible is invertible.*

Theorem 4.65 *If V is finite dimensional over F, then $T \in A(V)$ is invert- ible iff the constant terms of the minimal polynomial for T is not zero.*

Proof: Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_k x^k$ be the minimal polynomial for T. Assume that $\alpha_0 \neq 0$ and $p(T) = 0$. To prove: T is invertible. Since $p(x)$ is a minimal polynomial for T.

$$p(T) = 0 \Rightarrow \alpha_0 + \alpha_1 T + \dots + \alpha_k T^k = 0 \quad \dots\dots\dots (1)$$

$$\alpha_0 = -(\alpha_1 T + \dots + \alpha_k T^k)$$

$$\alpha_0 = -(\alpha_1 + \alpha_2 T + \dots + \alpha_k T^{k-1})T \quad \alpha = T(-\alpha_1 - \alpha_2 T + \dots - \alpha_k T^{k-1})$$

$$\Rightarrow 1 = T\left(\frac{1}{\alpha_0}(-\alpha_1 - \alpha_2 T - \dots - \alpha_k T^{k-1})\right)$$

$$1 = T\left(-\frac{1}{\alpha_0}(\alpha_1 + \alpha_2 T + \dots + \alpha_k T^{k-1})\right)$$

Let $S = -\frac{1}{\alpha_0}(\alpha_1 + \alpha_2 + \dots + \alpha_k T^{k-1})$. Clearly, $S \neq 0$ and $TS = 1$. Similarly $ST = 1$. Thus $ST = TS = 1$. T is invertible. Conversely, Suppose that T is invertible. To prove: $\alpha_0 \neq 0$. Suppose not, $\alpha = 0$. From(1),

$$\alpha_1 T + \alpha_2 T^2 + \dots + \alpha_k T^k = 0$$

$$(\alpha_1 + \alpha_2 T + \dots + \alpha_k T^{k-1})T = 0.$$

Since T is invertible, T^{-1} exist. Multiplying the above relation t^{-1},

$$\Rightarrow ((\alpha_1 T + \alpha_2 T^2 + \dots + \alpha_k T^k)T)T^{-1} = 0T^{-1} = 0$$

$$\Rightarrow \alpha_1 T + \alpha_2 T^2 + \dots + \alpha_k T^{k-1} = 0 \quad \dots\dots\dots (2)$$

Let $q(x) = \alpha_1 x + \dots + \alpha_k x^{k-1}$. By(2), $q(T) = 0$. (i.e.) T satisfy the polynomial $q(x)$ of degree $k - 1$, which is a contradiction to the degree of minimal polynomial for T, which is $k \Rightarrow\Leftarrow$ shows that $\alpha_0 \neq 0$.

Corollary 4.66 *If V is finite dimensional over F and if $T \in A(V)$ is in- vertible then T^{-1} is a polynomial expression in T over F.*

Proof: Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_k x^k$ with $\alpha_k \neq 0$ be the minimal polynomial of T.

$$p(T) = 0 \Rightarrow \alpha_0 + \alpha_1 T + \alpha_2 T^2 + \ldots + \alpha_k T^k = 0$$
$$\Rightarrow \alpha_0 = -(\alpha_1 T + \alpha_2 T^2 + \ldots + \alpha_k T^k)$$
$$\alpha_0 = (-\alpha_1)T + (-\alpha_2)T^2 + \ldots + (-\alpha_k)T^k$$
$$1 = \left(-\frac{\alpha_1}{\alpha_0}\right)T + \left(-\frac{\alpha_2}{\alpha_0}\right)T^2 + \ldots + \left(-\frac{\alpha_k}{\alpha_0}\right)T^k$$
$$1 = \left(\left(-\frac{\alpha_1}{\alpha_0}\right) + \left(-\frac{\alpha_2}{\alpha_0}\right)T + \ldots + \left(-\frac{\alpha_k}{\alpha_0}\right)T^{k-1}\right)T$$
$$1 \cdot T^{-1} = \left(\left(-\frac{\alpha_1}{\alpha_0}\right) + (-\alpha_2/\alpha_0)T + \ldots + \left(-\frac{\alpha_k}{\alpha_0}\right)T^{k-1}\right)T \cdot T^{-1}$$
$$T^{-1} = \beta_1 + \beta_2 T + \ldots + \beta_k T^{k-1}$$

where $\beta_1 = (-\frac{\alpha_1}{\alpha_0}), \ldots, \beta_k = (-\frac{\alpha_k}{\alpha_0})$. $\therefore$ T^{-1} is a polynomial expression in T over F.

Corollary 4.67 *If V is a finite dimensional vector space over a field F and if $T \in A(V)$ is singular then there exists $S \neq 0$ in $A(V)$ such that $ST = TS = 0$.*

Proof: Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k$ be a minimal polynomial of T over F. (i.e.) $p(T) = 0 \Rightarrow \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k = 0$. Since T is singular (i.e.) T is non-invertible by Theorem 4.65, $\alpha_0 = 0$. $\therefore$ $\alpha_1 T + \alpha_2 T^2 + \ldots + \alpha_k T^k = 0 \Rightarrow (\alpha_1 + \alpha_2 T + \ldots + \alpha_k T^{k-1})T = 0$ (1)
Let $S = \alpha_1 + \alpha_2 T + \ldots + \alpha_k T^{k-1}$ then $S \neq 0$ ($\because \alpha_1 + \alpha_2 x + \alpha_3 x^2 + \ldots + \alpha_k x^{k-1}$ is of lower degree than $p(x)$). From (1), $ST = 0$. Similarly $TS = 0$ $\therefore ST = TS = 0$, where $S \neq 0$.

Corollary 4.68 *If V is a finite dimensional over F and if $T \in A(V)$ is right invertible then it is invertible.*

Proof: Given $T \in A(V)$ is right invertible. Then there exists $U \in A(V)$ such that $TU = 1$ (1)
To prove: T is invertible. Suppose T is not invertible. (i.e.) T is sin- gular, then by Corollary 4.67, there exists $S \neq 0$ in $A(V)$ such that $ST = TS = 0$ (2)
From (1), $TU = 0$

$$\Rightarrow S(TU) = S \cdot 1$$
$$\Rightarrow (ST)U = S$$
$$\Rightarrow 0 \cdot U = S \quad by(2)$$
$$\Rightarrow S = 0$$
$$\Rightarrow\Leftarrow S \neq 0$$

This contradiction shows that T is invertible.

Theorem 4.69 *If V is finite dimensional over F, $T \in A(V)$ is singular iff $v \neq 0$ in V such that $vT = 0$.*

Proof: Assume that T is singular. By Corollary 4.67 there exists $S \neq 0 \in A(V)$ such that $ST = TS = 0$................(1)

Since $S \neq 0$ in $A(V)$, there exists $w \in V$ such that $wS \neq 0$. Let $v = wS$ then $v \neq 0$ in V, $vT = (wS)T = w(ST) = w\bar{0} = 0$ by(1) $\Rightarrow vT = 0$, $v \neq 0$. $\therefore$ There exists $v \neq 0$ in V such that $vT = 0$. Conversely, suppose that there exists $v \neq 0$ in V such that $vT = 0$. To prove: T is singular. Suppose not, T is invertible. Then there exists $U \in A(V)$ such that $UT = TU = 1$. Now, $TU = 1 \Rightarrow v(TU) = v \cdot 1$ (2)

$v(TU) = (vT)U = 0 \cdot U = 0 \rightarrow$ (3)

From (2) and (3), $v = 0 \Rightarrow\Leftarrow$ to $v \neq 0$. $\therefore$ T is singular.

Definition 4.70 *Let $T \in A(V)$, then (range of the linear transformation T) Range of $T = \{vT/v \in V\} = VT$*

Remark 4.71 *(1) Range of T is a subspace of V*

Proof: Let $u, v \in VT$, $\alpha, \beta \in F$. Now $(\alpha u + \beta v)T = (\alpha u)T + (\beta v)T = \alpha(uT) + \beta(vT) \in VT \Rightarrow \alpha u + \beta v \in VT$. $\therefore$ VT is a subspace of V. $\therefore$ Range of T is a subspace of V.

(2) If $VT = V$ then T is onto.

Theorem 4.72 *If V is finite dimensional over F, then $T \in A(V)$ is regular iff T maps V onto V.*

Proof: Suppose T is regular. To prove: T is onto. Let $v \in V$ consider vT^{-1}. Now, $(vT^{-1})T = v(t^{-1}T) = v \cdot 1 = v \Rightarrow v = (vT^{-1})T$, $v \in V$. (i.e.) every element $v \in V$ has pre-image vT^{-1} under T in V. $\therefore$ T is onto. Conversely, suppose that T is onto. To prove: T is regular. Suppose not, T is singular, we must show that T is not onto. Since T is singular, by Theorem 4.69, there exists $v_1 \neq 0$ in V such that $v_1T = \dot{0}$ ($\dot{0} : V \rightarrow V$). Suppose $\alpha_1 v_1 = 0 \Rightarrow \alpha_1 = 0 \Rightarrow v_1$ is linearly independent. Since $\{v_1\}$ is linearly independent in the finite dimensional vector space. Since V is finite dimensional, we can find vectors $v_2, v_3, ..., v_n$ such that $\{v_1, v_2, v_3, , v_n\}$ form a basis of V where $dim(V) = n$. $\therefore$ VT is generated by $w_1 = v_1T$, $w_2 = v_2T$, ..., $w_n = v_nT$. Since $w_1 = v_1T = 0$, VT is spanned by $v_2T, v_3T, , v_nT$. (i.e.) VT is spanned by $w_2, w_3, ..., w_n$ $\therefore$ $dim(VT) \leq (n-1) < n = dim(V) \Rightarrow dim(VT) < dim(V) \Rightarrow VT \subset V \Rightarrow VT \neq V \Rightarrow T$ is not onto.

Note 4.73 *The above theorem can be replaced as T is regular $\Leftrightarrow dim(VT) = dim(V)$ (i.e.) $VT = V$.*

Remark 4.74 *The above theorem suggest that we could use $dim(VT)$ not only as a test for regularity but even as a measure of degree of singularity for a given $T \in A(V)$.*

Consequently, $p(x)$ is the minimal polynomial of STS^{-1} also let $g(x)$ be the minimal polynomial of STS^{-1} (i.e.)$Sg(T)S^{-1} = 0 \Rightarrow Sg(T)S^{-1} = 0 \Rightarrow g(T) = 0$. (i.e) T satisfies the polynomial of $g(x)$. Let $h(x)$ be the polynomial of degree less than the degree of $g(x)$ and $h(x) = 0$. Again $h(STS^{-1}) = Sh(T)S^{-1} = 0$. (i.e.) STS^{-1} satisfies the polynomial $h(x)$ and $deg(h(x)) < deg(g(x))$, which is contradiction. Consequently, $g(x)$ is a minimal polynomial of T also. Hence the theorem.

Definition 4.85 *Let λ be a characteristic root of $T \in A(V)$ the element $v \neq 0$ in V is called characteristic vector of T belonging to λ if $vT = \lambda v$. (Theorem 4.81 guarantees the existence of such a characteristic vectors in V corresponding to λ*

Theorem 4.86 *If $\lambda_1, \lambda_2, ..., \lambda_k$ are distinct characteristic roots of $T \in A(V)$ and $v_1, v_2, ..., v_k$ are characteristics vectors of T belonging $\lambda_1, \lambda_2, ..., \lambda_k$ re- spectively then $v_1, v_2, ..., v_k$ are linearly independent over F.*

Proof: Case(i): If $k = 1$ then there is only one characteristic vector $v_1 \neq 0$ in V which is linearly independent.

Case(ii): If $k > 1$, To prove: $v_1, v_2, ..., v_k$ are linearly independent. Suppose the characteristic vector $v_1, v_2, ..., v_k$ are linearly dependent over F. Then there exists scalars $\alpha_1, \alpha_2, ..., \alpha_k$ not all zero in F such that $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_k v_k = 0$. Without loss of generality, let us assume that the shortest relation with non-zero coefficients (by suitably renumbering)

$\beta_1 v_1 + \beta_2 v_2 + ... + \beta_j v_j = 0$

where $\beta_1 = \beta_2 = ... = \beta_j \neq 0$

Since λ_i's are characteristic roots we have

$v_i T = \lambda_i v_i, \forall i$

By equation(1),

$$(\beta_1 v_1 + \beta_2 v_2 + ... + \beta_j v_j)T = 0 \cdot T \; \beta_1 v_1 T + \beta_2 v_2 T + ... + \beta_j v_j T = 0$$

$$\beta_1(v_1 T) + \beta_2(v_2 T) + ... + \beta_j(v_j T) = 0$$

$$\beta_1\lambda_1 v_1 + \beta_2\lambda_2 v_2 + ... + \beta_j\lambda_j v_j = 0 \; (\beta_1\lambda_1)v_1 + (\beta_2\lambda_2)v_2 + ... + (\beta_j\lambda_j)v_j = 0 \; ....(2)$$

$$\lambda_1 \times (1) \Rightarrow \lambda_1\beta_1 v_1 + \lambda_2\beta_2 v_2 + ... + \lambda_1\beta_j v_j = 0$$

$$(2) - (3) \Rightarrow (\lambda_2 - \lambda_1)\beta_2 v_2 + (\lambda_3 - \lambda_1)\beta_3 v_3 + ... + (\lambda_j - \lambda_1)\beta_j v_j = 0 \; ....(4)$$

Now, $(\lambda_j - \lambda_1)\beta_j \neq 0, i = 2, 3, ..., j$ ($\because \lambda_j - \lambda_1 \neq 0, i > 1$ and $\beta_j \neq 0$). (i.e.)

$\gamma_2 v_2 + \gamma_3 v_3 + ... + \gamma_j v_j = 0 \; ....(5)$

where $\gamma_2 = \lambda_2 - \lambda_1 \neq 0, \gamma_3 = \lambda_3 - \lambda_1$ 0, ..., $\gamma_j = (\lambda_j - \lambda_1)$ 0 $\Rightarrow v_2, v_3, ..., v_j$ are linearly dependent. By relation (5) we have produced a shorter relation than that of equation (1) between $v_1, v_2, ..., v_k \Rightarrow\Leftarrow$. This contradiction proves that $v_1, v_2, ..., v_k$ are linearly independent. For example, $t \in V_3(F)$ number of characteristics root of $T \leq 3$.

triangular if

$$\begin{aligned}
v_1T &= \alpha_{11}v_1\\
v_2T &= \alpha_{21}v_1 + \alpha_{22}v_2\\
v_3T &= \alpha_{31}v_1 + \alpha_{32}v_2 + \alpha_{33}v_3\\
&\;\;\vdots\\
v_iT &= \alpha_{i1}v_1 + \alpha_{i2}v_2 + \alpha_{ii}v_i\\
&\;\;\vdots\\
v_nT &= \alpha_{n1}v_1 + \alpha_{n2}v_2 + \alpha_{nn}v_n.
\end{aligned}$$

(i.e.) if v_iT is a linear combination only if v_i and its predecessor in the basis.

Theorem 4.94 *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 prove this theorem by induction on the dimension of V over F. If $dim_F(V) = 1$. Then every matrix representation of $T \in A(V)$ is a scalar. (i.e.) A matrix of order 1×1 which is trivially a triangular matrix. Suppose the theorem is true for all vector spaces over F of dimension $(n-1)$. Let V be a vector spaces of dimension n over F. Since the Linear Transformation T on V has all its characteristic root in F. Let $\lambda_1 \in F$ be a characteristic root of T. Then there exists a non-zero vector $v_1 \in V$ such that $v_1T = \lambda_1 v_1$. Let $W = \{\alpha v_1 \mid \alpha \in F\}$ then W is a subspace of V of dimension 1. Then,

$$\begin{aligned}
WT &= \{(\alpha v_1)T \mid \alpha \in F, v_1 \in V\}\\
&= \{\alpha(v_1T) \mid \alpha \in F, v_1 \in V\}\\
&= \{\alpha w_1 \mid w_1 \in V, \alpha \in F\}
\end{aligned}$$

$\Rightarrow WT \subset W$. $\therefore$ W is a subspace of V of dimension 1 and invariant under T.

Let $\bar{V} = V/W$ then $dim(\bar{V}) = dim(V/W) = dim(V) - dim(W) = (n-1)$.

By Lemma 4.92, T induces the linear transformation $\bar{T}$ on $\bar{V}$. Also minimal polynomial of $\bar{T}$ over F divides minimal polynomial of T over F. $\therefore$ All the roots of minimal polynomial of $\bar{T}$ being the roots of minimal polynomialof T must be in F. Thus $\bar{V}$ and $\bar{T}$ satisfies the hypotheses of the theorem. Since $dim(\bar{V}) = n-1$, then by induction hypotheses there is a basis consists of the vector $\bar{v}_2, \bar{v}_3, \ldots, \bar{v}_n$ over $\bar{V}$ over F in which the matrix of $\bar{T}$ is triangular

$$\bar{v}_2\bar{T} = \alpha_{22}\bar{v}_2$$
$$\bar{v}_3\bar{T} = \alpha_{32}\bar{v}_2 + \alpha_{33}\bar{v}_3$$
$$\bar{v}_4\bar{T} = \alpha_{42}\bar{v}_2 + \alpha_{43}\bar{v}_3 + \alpha_{44}\bar{v}_4$$
$$\vdots$$
$$\bar{v}_n\bar{T} = \alpha_{n2}\bar{v}_2 + \alpha_{n3}\bar{v}_3 + \ldots + \alpha_{nn}\bar{v}_n$$

Let $v_2, v_3, \ldots, v_n$ be the elements of V mapping into $\bar{v}_2, \bar{v}_3, \ldots, \bar{v}_n$ of $\bar{V}$ respec- tively. (i.e.) $\bar{v}_2 = v_2+W$; $\bar{v}_3 = v_3+W$; ...; $\bar{v}_n = v_n+W$. Then $v_1, v_2, \ldots, v_n$ form a basis of V. Since $\bar{v}_2\bar{T} = \alpha_{22}(v_2+W) = \alpha_{22}v_2+W$

$$(v_2 + W) + \bar{T} = \alpha_{22}v_2 + W\ v_2T +$$
$$W = \alpha_{22}v_2 + W$$
$$\Rightarrow v_2T - \alpha_{22}v_2 \in W$$
$\Rightarrow v_2T - \alpha_{22}v_2$ *is a multiples of* v_1, *say* $\alpha_{21}v_1$
$$\Rightarrow v_2T - \alpha_{22}v_2 = \alpha_{21}v_1$$
$v_2T = \alpha_{21}v_1 + \alpha_{22}v_2$ *Similarly*
$$v_3T = \alpha_{31}v_1 + \alpha_{32}v_2 + \alpha_{33}v_3$$
$$\vdots$$
$$v_iT = \alpha_{i1}v_1 + \alpha_{i2}v_2 + \alpha_{ii}v_3 \ (i = 1, 2, \ldots, n)$$

(i.e.) the basis $v_1, v_2, \ldots, v_n$ of V over F provides us with a basis where every v_iT is a linear combination of v_i and its predecessors hence the matrix of T in the basis $\{v_1, v_2, \ldots, v_n\}$ istriangular.

Theorem 4.95 *If V is a dimensional over F and $T \in A(V)$ has matrix $m_1(T)$ in the basis $v_1, v_2, \ldots, v_n$ and $m_2(T) = Cm_1(T)C^{-1}$. In fact if S is the linear transformation of V defined by $v_iS = w_i$ for $i = 1, 2, \ldots, n$ then C can be chosen to be $m_1(S)$.*

Remark 4.96 *The above theorem can be restated as if there is a matrix $A \in F_n$ has all its characters root in F then there is matrix $C \in F_n$ such that CAC^1 is a triangular matrix.*

Proof: Let $A \in F_n$ has all its characteristic roots in F. A defines a linear

2. $(A + B)^* = A^* + B^*$

3. $(AB)^* = B^*A^*$ *for all* $A, B \in F_n$

Definition 4.117 *Suppose* F *be a field of complex numbers and that adjoint* $*$ *on* F_n *is the hermitian adjoint. The matrix* A *is called hermitian if* $A^* = A$.

Definition 4.118 *A is called skew hermitian if* $A^* = -A$

Remark 4.119 .

1. *Any square matrix A can be uniquely written as a sum of a hermitian and a skew hermitian matrices* $A = \frac{1}{2}(A + A^*) + \frac{1}{2}(A - A^*)$.

2. *If* $A \neq 0 \in F_n$ *then trace of* $AA^* > 0$

3. *If* $A_1, A_2, \ldots, A_k \in F_n$ *and if* $A_1A_1^* + A_2A_2^* + \ldots + A_kA_k^* = 0$ *then* $A_1 = A_2 = \ldots = A_k$.

4. *If* λ *is a scalar matrix then* $\lambda^* = \bar{\lambda}$

Example 4.120

$$\lambda = \begin{bmatrix} 3i & 0 \\ 0 & 3i \end{bmatrix}; \lambda^* = \begin{bmatrix} -3i & 0 \\ 0 & -3i \end{bmatrix}; \bar{\lambda} = \begin{bmatrix} -3i & 0 \\ 0 & -3i \end{bmatrix} \Rightarrow \lambda^* = \bar{\lambda}$$

Result 4.121 *The characteristics roots of a hermitian matrix are all real (i.e.) if a complex number* λ *is a characteristic roots of a hermitian matrix then* λ *must be real.*

Proof: Let A be a hermitian matrix then $A = A^*$ (i.e.) $\bar{A}' = A$ and λ be a characteristic root of $T \in A(V)$. Let X be a characteristics vector

$$\therefore k_1 = k_2 = \ldots = k_m = 0$$

$$k_1 = 0 \Rightarrow f_{11}w_1 + f_{12}w_2 + \ldots + f_{1n}w_n = 0$$
$$k_2 = 0 \Rightarrow f_{21}w_1 + f_{22}w_2 + \ldots + f_{2n}w_n = 0$$
$$\vdots$$
$$k_m = 0 \Rightarrow f_{m1}w_1 + f_{m2}w_2 + \ldots + f_{mn}w_n = 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Since $\{w_1, w_2, \ldots, w_n\}$ forms the basis of K over F they are linearly indepen- dent over F.
from (5) we have,

$$f_{11} = f_{12} = \ldots = f_{1n} = 0$$
$$f_{21} = f_{22} = \ldots = f_{2n} = 0$$
$$\vdots$$
$$f_{m1} = f_{m2} = \ldots = f_{mn} = 0$$

(i.e.) $f_{ij} \forall i = 1, 2, \ldots, m, j = 1, 2, \ldots, n$. $\therefore$ $S = \{v_i w_j \mid i = 1, 2, \ldots, m, j = 1, 2, \ldots, n\}$ is linearly independent. (6)
From (2) and (3), the set S which contains mn elements forms the basis of L over F. $\therefore [L : F] = dim_F(L) = mn = [L : K][K : F]$. (7)
Since $[L : K]$ and $[K : F]$ are finite $\Rightarrow [L : F]$ is finite by (7). $\therefore$ L is a finite extension of F.

Corollary 5.10 *If L is a finite extension of F and K is a subfield of L which contains F, then $[K : F]/[L : F]$.*

Proof: Given L, K, F are fields, such that $L \supset K \supset F$ and $[L : F]$ is finite. Clearlyany elementin$L$,linearlyindependentover$K$,linearlyindependent over F. From the assumption $[L : F]$ is finite we come to conclusion that $[K : F]$ is finite. By previous theorem, $[L : F] = [L : K][K : F]$. Hence $[K : F]/[L : F]$.

Definition 5.11 *An element $a \in K$ is said to be algebraic over F if there exists elements $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n \in F$, not all zero such that $\alpha_0 a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0$.*

Remark 5.12 *if $p(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$, $\alpha_i \in F$. $\therefore$ $\alpha_0 a^n + \alpha_1 a^{n-1} + \ldots + \alpha_n = 0$ $\Rightarrow p(a) = 0$. (i.e.) $a \in K$ is algebraic over F if there is a non-zero polynomial $p(x) \in F[x]$ which satisfies a. (i.e.) $p(a)=0$.*
For example, $p(x) = x^3 + 3x^2 + 3x + 1 \Rightarrow p(-1) = 0 \Rightarrow -1$ is algebraic over $\mathbb{Q}$ and 1 is not algebraic over $\mathbb{Q}$.

Let $\alpha, \beta \in F$ such that $\alpha\psi = \beta\psi$,

$$V + \alpha = V + \beta$$
$$(\alpha - \beta) \in V = p(x)$$
$$(\alpha - \beta) = f(x)p(x) \text{ for some } f(x) \in F[x]$$
$$\Rightarrow f(x)=0$$
$$\Rightarrow (\alpha - \beta) = 0$$
$$\Rightarrow \alpha = \beta \ \psi$$

is 1 − 1.

(ii) ψ is homomorphism:

$$(\alpha + \beta)\psi = V + (\alpha + \beta)$$
$$= (V + \alpha) + (V + \beta)$$
$$= \alpha\psi + \beta\psi$$

$\therefore$ ψ is a homomorphism.

Thus ψ is an isomorphism from F into E. Let $\bar{F}$ be the image of F into E under ψ. Let $\bar{F} = \{\alpha + V \mid \alpha \in F\}$. Thus ψ is an isomorphism of F onto $\bar{F}$ and $\bar{F}$ is a subfield of E isomorphic to F by the mapping $\psi : F[x] \to E$, by $f(x)\psi = f(x)+V$ and the restriction of ψ to F induces an isomorphism of F onto $\bar{F}$. If we identify F and $\bar{F}$ under this isomorphism we can consider E to be an extension of F.
Claim: E is a finite extension of F of degree n equal to degree of $p(x)$. First we shall prove that the n elements $\{1+V, x+V, (x+V)^2 = x_2+V, (x+V)^3 = x^3+V, \ldots, (x + V)^{n-1} = x^{n-1} + V\}$ form a basis of E over F. $[E : F] = n$. Finally we shall show that $p(x)$ has a root in E. Let $p(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_k x^k$ where $\beta_0, \beta_1, \beta_2, \ldots, \beta_k \in F$. First Let us make $p(x)$ be a polynomial over E with help of the identification we have made between F
and $\bar{F}$. For convenience of notation Let us denote the element $x\psi = x + V$ in the field $\bar{F}$ as $\alpha\beta_k$ by β_k+V, $p(x) = (\beta_0+V)+(\beta_1+V)x+\ldots+(\beta_k+V)x^k$. We shall show that $x + V \in E$ satisfies $p(x)$.

$$p(x + V) = (\beta_0 + V) + (\beta_1 + V)(x + V) + \ldots + (\beta_k + V)(x + V)^k$$
$$= (\beta_0 + V) + (\beta_1 + V)(x + V) + (\beta_2 + V)(x^2 + V) + \ldots$$
$$+ (\beta_k + V)(x^k + V)$$
$$= (\beta_0 + \beta_1 x + \beta_2 x^2 + \ldots + \beta_k x^k) + V$$
$$= p(x) + V$$
$$= v \ (\because p(x) \in V)$$
$$= \text{zero element of } E.$$

Thus $(x + V)$ satisfies $p(x)$. $\therefore$ An element $x + V$ in the extension E satisfies the polynomial $p(x) \in F[x]$. The field E has been shown to satisfy all the

$$(f(x))\tau^* = g(x)\tau^*$$
$$\Rightarrow (\alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n)\tau^* = (\beta_0 x^m + \beta_1 x^{m-1} + \ldots + \beta_m)\tau^*$$
$$\Rightarrow \alpha_0' t^n + \alpha_1' x^{n-1} + \ldots + \alpha_n' = \beta_0' t^m + \beta_1' x^{m-1} + \ldots\ldots\ldots\ldots + \beta_m'$$
$$\Rightarrow n = m \text{ and } \alpha_i' = \beta_i', i = 0, 1, \ldots\ldots\ldots n$$
$$\Rightarrow n = m \text{ and } (\alpha_i)\tau = (\beta_i)\tau, i = 0, 1, 2 \ldots\ldots\ldots n$$
$$\Rightarrow n = m \text{ and } \alpha_i = \beta_i,\ i = 0,\ 1,\ 2\ldots n\ (\because \tau \text{ is 1-1})$$
$$f(x) = g(x)$$

$\tau*$ **is onto:** Let $\gamma_0' t^n + \gamma_1' x^{n-1} + \ldots + \gamma_n'$ be any element of $F'[t], \gamma_i' \in F'$ since τ is onto, there exists $\gamma_0, \gamma_1, \ldots, \gamma_n \in F$ such that $(\gamma_0)\tau = \gamma_0', (\gamma_1)\tau = \gamma_1', \ldots, (\gamma_n)\tau = \gamma_n'$. Now $\gamma_0 x^n, \gamma_1 x^{n-1}, \ldots, \gamma_n \in F[x]$ and $(\gamma_0 x^n, \gamma_1 x^{n-1}, \ldots, \gamma_n)\tau^* = (\gamma_0' t^n + \gamma_1' x^{n-1} + \ldots + \gamma_n')$. $\therefore \tau^*$ is onto.

τ^* **is a homomorphism:** To Prove: $(f(x) + g(x))\tau^* = f(x)\tau^* + g(x)\tau^*$

$$[f(x)+g(x)]\tau^*$$
$$= [\alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n + \beta_0 x^m + \beta_1 x^{m-1} + \ldots + \beta_m]$$
$$= ((\alpha_0' x^n + \alpha_1' x^{n-1} + \ldots + \alpha_n') + (\beta_0' x^m + \beta_1' x^{m-1} + \ldots + \beta_m'))$$
$$= (\alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n)\tau^* + (\beta_0 x^m + \beta_1 x^{m-1} + \ldots + \beta_m)\tau^*$$
$$= f(x)\tau^* + g(x)\tau^*$$

Hence τ^* is an isomorphism of $F[x]$ onto $F'[t]$.

Remark 5.44

1. *Further if $f(x) \in F[x]$ be simply taken as α where $\alpha \in F$ then $(f(x))\tau^* = \alpha\tau^* = \alpha\tau = \alpha'$.*

2. *From the above theorem we conclude that factorisation of $f(x)$ in $F[x]$ result in like factorisation of $f(x)\tau^* = f'(t)$ in $F'[t]$ and vice versa. In particular $f(x)$ is irreducible in $F[x]$ iff $f'(t)$ is irreducible in $F'[t]$.*

Lemma 5.45 *Let τ be an isomorphism of a field F onto a field F' defined by $(\alpha)\tau = \alpha'$ $\forall\alpha \in F$ for an arbitrary polynomial $f(x) = (\alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n) \in F[x]$. Let us define $f'(t) = \alpha_0' t^n + \alpha_1' x^{n-1} + \ldots + \alpha_n' \in F'[t]$. If $f(x)$ is irreducible in $F[x]$, show that there is an isomorphism τ^{**} of $F[x]/f(x)$ onto $F'[t]/f'[t]$ with the property that $\alpha\tau^{**} = \alpha'(x + f(x))\tau^{**} = t + f'(t)$.*

Proof: Let $\tau^* : F[x] \to F'[t]$ defined by $f(x)\tau^* = f'(t)$. Then by Lemma 5.43 τ^* is an isomorphism of $F[x]$ onto $F'[t]$. Let $f(x)$ be irreducible in $F[x]$ then $f'(t)$ will be irreducible in $F'[t]$. $V = (f(x))$ ideal generated by $f(x)$ in $F[x]$ and $V' = (f'(t))$ ideal in $F'[t]$. Now, $f(x)$ and $f'(t)$ are irreducible both V and v' are maximal ideal. $F[x]/V$ and $F'[t]/V$ are fields. Define $\tau^{**} : F[x]/V \to F'[t]/V'$ by $(g(x) + V)\tau^{**} = g(x)\tau^* + V' = g'(t) + V'$.

τ^{**} **is well defined:** For this we have to show that if $V + g(x) = V + h(x)$