M.Sc. MATHEMATICS - I YEAR

DKM11 : ADVANCED ABSTRACT ALGEBRA

SYLLABUS

Unit I :

Groups – A counting principle – Normal subgroups and Quotient groups – homomorphism – isomorphism – Cayley's theorem – permutation groups. [Sections 2.6-2.10]

Unit II :

Another counting principle – Sylow's Theorems – Direct products. [Sections 3.11-3.13]

Unit III :

Rings – homomorphism – Ideals and quotient rings – Field of quotients of an integral domain – Polynomial rings – Polynomial rings over rational field. [Sections 3.4-3.10]

Unit IV :

Vector spaces – Linear transformation and bases – Algebra of linear transformations – Characteristic roots – [Sections 4.1,4.2,6.1,6.2,6.3&6.8] – canonical form - triangular form – trace & tanspose.

Unit V:

Extension fields – roots of polynomials – more about roots. [Sections 5.1,5.3 & 5.5]

Text :

Topics in Algebra (Second Edition) By I.N. Herstein – Willey Indian Edition.

1. UNIT I

Groups

Definition 1.1 ***Group:*** *A non-empty set of elements G is said to form a group if in G there is defined a binary operation, called the product and denoted by $(\cdot)$ such that*

1. *$a, b \in G \Rightarrow a \cdot b \in G$ (closure axiom),*
2. *$a, b, c \in G \Rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (Associative axiom),*
3. *there exists an element $e \in G$ such that $a \cdot e = e \cdot a = a, \forall a \in G$ (Existence of identity),*
4. *$\forall a \in G$ there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$ (Existence of inverse).*

Definition 1.2 ***Abelian group:*** *A group G is said to abelian (or commutative) if $\forall a, b \in G \Rightarrow a \cdot b = b \cdot a$.*

Remark 1.3 *A group which is not abelian is called a non-abelian group.*

Example 1.4 *Let $G = \{0, \pm 1, \pm 2, ...\}$. Define $a \cdot b = a + b$. Then G is an abelian group. i.e., $(\mathbb{Z}, +)$ is an abilian group.*

Example 1.5 *Let $G = \{1, -1\}$. Then G is a group under multiplication. Here G is an abelian group of order 2.*

Example 1.6 *Let $S_3 = \{x_1, x_2, x_3\}$, consider*

$$e = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \phi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}, \quad \psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix} \text{ and } \quad \phi^2 = e$$

$$\phi{\cdot}\psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}, \psi{\cdot}\phi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix} \text{ and } \psi^2 = \psi{\cdot}\psi = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}$$

$G = \{e, \phi, \psi, \phi \cdot \psi, \psi \cdot \phi, \psi^2\} = S_3$.
G is a non-abelian group under composition of function and it is a symmetric group of order 3, and denoted by S_3.$O(S_3) = 3! = 6$.

$\cdot$	e	ϕ	ψ	$\phi \cdot \psi$	$\psi \cdot \phi$	ψ^2
e	e	ϕ	ψ	$\phi \cdot \psi$	$\psi \cdot \phi$	ψ^2
ϕ	ϕ	e	$\phi \cdot \psi$	ϕ	ψ^2	$\psi \cdot \phi$
ψ	ψ	$\psi \cdot \phi$	ψ^2	ϕ	$\phi \cdot \psi$	e
$\phi \cdot \psi$	$\phi \cdot \psi$	ψ^2	$\psi \cdot \phi$	e	ψ	ϕ
$\psi \cdot \phi$	$\psi \cdot \phi$	ψ	ϕ	ψ^2	e	$\phi \cdot \psi$
ψ^2	ψ^2	$\psi \cdot \phi$	e	$\psi \cdot \phi$	ϕ	ψ

Example 1.7 *Let S be a non-empty the set having finite number of elements then $A(s)$, the set of all permutations of S (i.e. the set of all $1-1$, onto functions from S onto itself). So, it is a non-abelian group under the composition of function.*

Example 1.8 *Let*

$$G = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in R \text{ and } ad - bc \neq 0\}$$

Then G is an infinite non-abelian group under matrix multiplication.

Lemma 1.9 *If G is a group, then*

1. *the identity element of G is unique,*
2. *every element $a \in G$ has unique inverse in G,*
3. *for any $a \in G, (a^{-1})^{-1} = a$,*
4. *for all $a, b \in G, (ab)^{-1} = b^{-1} \cdot a^{-1}$.*

Definition 1.10 ***subgroup:*** *A non-empty subset H of a group G is said to be subgroup of G, if under the product G, H itself form a group.*

Example 1.11
1. *$(2Z, +)$ is a subgroup of $(z, +)$,*
2. *$(3Z, +)$ is a subgroup of $(Z, +)$,*
3. *In general, $(nZ, +)$ is a subgroup of $(Z, +)$,*
4. *H={1,-1} is a subgroup of G={1,-1,i,-i} under usual multiplication.*

Remark 1.12 *If H is a subgroup of G, and G is a subgroup of K then H is a subgroup of K.*

Lemma 1.13 *A non-empty subset H of the group G is a subgroup of G iff*

1. *$a, b \in H \Rightarrow ab \in H$*
2. *$a \in H \Rightarrow a^{-1} \in H$*

Lemma 1.14 *If H is a non-empty finite subset of a group G and H is closed under multiplication then H is a subgroup of G.*

Example 1.15 *Let S be any non-empty set. Then $A(s)$ is a group under composition of mapping. Let $x_0 \in S$. Let $H(x_0) = \{\phi \in A(s) | \phi(x_0) = x_0\}$. Then $H(x_0)$ is a subgroup of $A(s)$.*

Example 1.16 $S = \{x_1, x_2, x_3\}$: $A(s) = s_3$ $[\because H(x_1) = \{e, \psi.\phi\}$
$H(x_1) = \{\phi \in A(s)/\phi(x_1) = x_1\}$ $H(x_2) = \{e, \phi.\psi\}$
$A(s) = \{e, \phi, \psi, \psi.\phi, \phi.\psi, \psi^2\}$ $H(x_3) = \{e, \phi\}]$
Here, $H(x_1), H(x_2)$ *and* $H(x_3)$ *are subgroups of* S_3

Remark 1.17 $H(x_1) \cap H(x_2) = H(x_2) \cap H(x_3) = H(x_3) \cap H(x_1) = \{e\}$.

Definition 1.18 Cyclic Group: *Let* G *be any group,* $a \in G$. *Let* $\langle a\rangle = \{a^i/i \in z\} = \{....a^{-2}, a^{-1}, a^0, a^1, a^2...\}$. *Then* $\langle a\rangle$ *is called as cyclic subgroup generated by* a. *If* $\langle a\rangle = G$ *for some* $a \in G$ *then* G *is said to be a cyclic group.*

Example 1.19 *Consider* $G = \{1, -1, i, -i\}$, *let* $a = i$. *Then* $\langle a\rangle = G$, G *is cyclic.*

Example 1.20 *Let* G *be the group of all real number addition* $(R, +)$ *and let* H *be the set of all integers under addition. Then* H *is a subgroup of* G.

Example 1.21 *Let*

$$G = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a, b, c, d \in R \text{ and } ad - bc \neq 0\} \text{is a group under multiplication}$$

$$H = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} | a, b, d \in Z\}$$

$$K = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} | b \in R\}$$

Then H *is a subgroup of* G *and* K *is a subgroup of* H.

Example 1.22 *Let* G *be a group of all non-zero complex number,(i.e.)* $G = C = \{a + ib$ *, both* a *and* b *are not zero*$\}$ *under multiplication. Let* $H = \{a + ib | a^2 + b^2 = 1\} = \{z \in \mathbb{C} |\ |z| = 1\}$. *Then* H *is a subgroup of* G.

Definition 1.23 *Let* G *be a group,* H *be a subgroup of* G*; for* $a, b \in G$ *we say* a *is congruent to* b *mod* H*,written as* $a \equiv b(mod H)$ *if* $ab^{-1} \in H$.

Lemma 1.24 *The relation* $'\equiv'$ *is an equivalence relation.*

Definition 1.25 Right Cosets: *If* H *is a subgroup of* G, $a \in G$ *then* $Ha = \{ha | h \in H\}$. Ha *is called a right cosets of* H *in* G.

Example 1.26 *Let* $G = \{J_{12}, \oplus\}, H = \{0, 4, 8\}$. *Then Distinct right cosets of* H *in* G *are* $H, H \oplus 1, H \oplus 2, H \oplus 3$.

Lemma 1.27 *For all* $a \in G, Ha = \{x \in G | a \equiv x(mod\ H)\}$

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*** *$\phi(n)$: $\phi(1) = 1, \phi(n) =$ number of positive integers less than n and relatively prime to n for $n > 1$.*
$\phi(8) = 4$ ($\because 1, 3, 5, 7$ are relatively prime to 8), $\phi(5) = 4, \phi(7) = 6, \phi(10) = 4, \phi(15) = 7$.

Corollary 1.41 *If n is a positive integer and a is relatively prime to n $((a,n)=1)$, then $a^{\phi(n)} \equiv 1(mod\ n)$.*

Corollary 1.42 *(i) If P is a finite prime number and a is any integer than $a^p \equiv a(mod\ p)$*
(ii) If G is a finite group of prime order then G is cyclic.

Counting principle: Let H,K be any two subgroups of a group G. Let $HK = \{hk/h \in H, K \in k\}$.

Example 1.43 *Consider the group $G = S_3 = \{e, \phi, \psi, \phi\cdot\psi, \psi\cdot\phi, \psi^2\}$. Let $H = \{e, \phi\}$ and $K = \{e, \phi\cdot\psi\}$. Then $HK = \{e\cdot e, e(\phi\cdot\psi), \phi\cdot e, \phi\cdot(\phi\cdot\psi)\} = \{e, \phi\cdot\psi, \phi, \psi\}$. Here HK is not a subgroup of G. Because, it is not closed under $(\cdot)$. $(\phi\cdot\psi, \phi \in HK$ but $(\phi\cdot\psi)\cdot\phi = \psi^2 \notin HK)$(i.e.) H and K are the subgroups of G but HK is not the subgroups of G. Since $O(HK)$ does not divides $O(G)$, by Lagrange's Theorem, HK need not be a subgroup of G.*

Lemma 1.44 *HK is a subgroup of G iff $HK = KH$.*

Corollary 1.45 *If H and K are subgroups of an abelian group G, then HK is a subgroup of G.*

Theorem 1.46 *If H and K are finite subgroups of orders $O(H)$ and $O(K)$ then $O(HK) = \frac{O(H)\ O(K)}{O(H\cap K)}$.*

Corollary 1.47 *Suppose H and K are the subgroup of a group G and order of H is greater than $\sqrt{O(G)}$ (i.e.) $O(H) > \sqrt{O(G)}$. Then $H \cap K \neq \{e\}$ (non-trivial).*

Normal Subgroups and Quotient groups:

Definition 1.48 *A subgroup N of a group G is said to be a normal subgroup of G if for every $g \in G$ and $n \in N, gng^{-1} \in N$.*

Result 1.49 *N is a normal subgroup of $G \Leftrightarrow gNg^{-1} = N$.*

Result 1.50 *A subgroup N of a group G is a normal subgroup of $G \Leftrightarrow$ every left cosets of N in G is a right cosets of N in G.*

Result 1.51 *A subgroup N of a group G is a normal subgroup of $G \Leftrightarrow$ the product of any two right cosets of N in G is again a right cosets of N in G.*

Theorem 1.52 *If G is a group and N is a normal subgroup of G, then $G/N = \{Na | a \in G\}$. Let $X = Na, Y = Nb \in G/N$. Define $X\cdot Y = Na\cdot Nb = Nab$. Under this product $(\cdot)$, G/N is a group which is called a quotient group (or) a factor group of G/N*

Example 1.53 *Let $G = (Z_{12}, \oplus_{12})$ and $N = \{0, 4, 8\}$.*
Then $G = \{N \oplus 0, N \oplus 1, N \oplus 2, N \oplus 3\}$.

Lemma 1.54 $O(G/N) = \frac{O(G)}{O(N)}$

Homomorphism:

Definition 1.55 *A mapping ϕ from a group G into a group $\bar{G}$ is said to be a homomorphism if for all $a, b \in G, \phi(ab) = \phi(a) \cdot \phi(b)$.*

Example 1.56

1. *Let G be any group. Define $\phi : G \to G$ by $\phi(x) = e \ \forall x \in G$, where e is the identity element of G. Then ϕ is a homomorphism of G into $\bar{G}$. Let $x, y \in G \Rightarrow xy \in G$, $\phi(x) = e, \phi(y) = e, \phi(xy) = e = e \cdot e = \phi(x) \cdot \phi(y)$.*

2. *Let G be a group. Define $\phi : G \to G$ by $\phi(x) = x \ \forall x \in G$. Then ϕ is a homomorphism. Let $a, b \in G \Rightarrow ab \in G, \phi(a) = a; \phi(b) = b, \phi(a \cdot b) = ab = a \cdot b = \phi(a) \cdot \phi(b) \ \forall a, b \in G$.*

3. *Let G be a group of all real numbers under addition and let $\bar{G}$ be group of non-zero real numbers with a product being ordinary multiplication of real numbers. (i.e.) $G = (R, +); \bar{G} = (R - \{0\}, \cdot)$. Define $\phi : G \to \bar{G}$ by $\phi(a) = 2^a$. Then ϕ is a homomorphism. Let $a, b \in G \Rightarrow a + b \in G$. Now, $\phi(a + b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b) \ \forall a, b \in G$.*

4. *Let $G = S_3 = \{e, \phi, \psi, \phi \cdot \psi, \psi \cdot \phi, \psi^2\}$ and $\bar{G} = \{e, \phi\}$. Define $f : G \to \bar{G}$ by $f(\phi^i \cdot \ \psi^j) = \phi^i$. $f(e) = e$; $f(\phi) = \phi$; $f(\psi) = e$; $f(\phi \cdot \psi) = \phi$; $f(\psi \cdot \phi) = f(\phi\psi^2) = \phi$; $f(\psi^2) = e$. Clearly, f is a homomorphism. Let $x = \phi^i \ \psi^j, y = \phi^r \ \psi^s$. $f(xy) = f(\phi^{i+r} \cdot \psi^{j+s}) = \phi^{i+r} = \phi^i \cdot \phi^r = f(\phi^i \ \psi^j) \cdot f(\phi^r \ \psi^s) = f(x) \cdot f(y)$.*

5. *Let G be the group of non-zero real numbers under multiplication. Let $\bar{G} = (\{1, -1\}, \cdot)$[(i.e.) $G = (R - \{0\}, \cdot)$]. Define $\phi : G \to \bar{G}$ by*

$$\phi(x) = \begin{cases} 1 & \text{if } x \text{ is positive} \\ -1 & \text{if } x \text{ is negative} \end{cases}$$

   (a) *Let $x, y \in G \Rightarrow x$ and y are positive and $\phi(x) = 1; \phi(y) = 1 \Rightarrow xy$ is positive. Then $\phi(xy) = 1 = 1 \cdot 1 = \phi(x) \cdot \phi(y)$,*

   (b) *x and y are negative $\Rightarrow \phi(x) = -1; \phi(y) = -1 \Rightarrow xy$ is positive. Then $\phi(xy) = 1 = -1 \cdot -1 = \phi(x) \cdot \phi(y)$,*

   (c) *x is positive and y is negative $\Rightarrow \phi(x) = 1$ and $\phi(y) = -1 \Rightarrow xy$ is negative. Then $\phi(xy) = -1 = 1 \cdot -1 = \phi(x) \cdot \phi(y)$,*

   (d) *x is negative and y is positive $\Rightarrow \phi(x) = -1$ and $\phi(y) = 1 \Rightarrow xy$ is negative. Then $\phi(xy) = -1 = -1 \cdot 1 = \phi(x) \cdot \phi(y)$.*

6. *Let G be a group of integers under addition,(i.e.) $G = (z, +)$ and $\bar{G}$ be the group of integers under addition modulo n. (i.e.) $\bar{G} = (Z_n, \oplus_n)$. Define $\phi : G \to \bar{G}$ by $\phi(x)$=Remainder of x on division by $n = r(mod\ n)$. Clearly, ϕ is a homomorphism.*

7. *Let G be a group of positive real number under multiplication and $\bar{G}$ be the group of all real numbers under addition. Define $\phi : G \to \bar{G}$ by $\phi(x) = log_{10}x$. Let $x, y \in G$. Then $\phi(xy) = log_{10}xy = log_{10}x + log_{10}y = \phi(x) + \phi(y)$. Then, ϕ is a homomorphism. ($\because$ the operation on the RHS in $\bar{G}$ is infact addition).*

Theorem 1.57 *Suppose G is a group, N a normal subgroup of G; define a mapping $\phi : G \to G/N$ by $\phi(x) = Nx\ \forall x \in G$. Then ϕ is a homomorphism of G onto G/N.*
Proof: Let $x, y \in G$. Then $\phi(x) = Nx, \phi(y) = Ny$. Now, $\phi(xy) = Nxy = Nx \cdot Ny = \phi(x) \cdot \phi(y)$. Hence, ϕ is a homomorphism. Let $X \in G/N$, then $X = Nx, x \in G$. Then $\phi(x) = Nx = X$. Therefore ϕ is onto. Thus, ϕ is a homomorphism of G onto G/N.

Remark 1.58 *It is true that a homomorphism need not be $1 - 1$.*

Definition 1.59 *If ϕ is a homomorphism of $G \times \bar{G}$, the kernal of ϕ (K_ϕ), defined by $K_\phi = \{x \in G | \phi(x) = \bar{e}, \bar{e}$ is the identity element of $\bar{G}\}$. Clearly K_ϕ is a subset of G.*

Example 1.60
1. *Define $\phi : G \to G$ by $\phi(x) = e\ \forall x \in G$. Then $K_\phi = \{x \in G | \phi(x) = e\} = G$.*

2. *Define $\phi : G \to G$ by $\phi(x) = x\ \forall x \in G$. Then $K_\phi = \{x \in G | \phi(x) = x\} = e$.*

3. *Define $\phi : G \to \bar{G}$ by $\phi(a) = 2^a\ \forall a \in G$. Then $K_\phi = \{a \in G | \phi(a) = 2^a\} = \{0\}$.*

4. *Define $f : G \to \bar{G}$ by $f(\phi^i\ \psi^i) = \phi^i$. Then $K_\phi = \{\phi \in G | f(\phi^i\ \psi^i) = \phi^i\} = \{e, \psi, \psi^2\}$.*

5. *Define $\phi : G \to \bar{G}$ by*

$$\phi(x) = \begin{cases} 1 & \text{if } x \text{ is positive} \\ -1 & \text{if } x \text{ is negative.} \end{cases}$$

Then $K_\phi = \{x \in G | \phi(x) = 1 = e$,if x is positive $\}$ =set of all positive numbers in G.

6. *Define $\phi : G \to \bar{G}$ by $\phi(x) = log_{10}x$. Then $K_\phi = \{x \in G | \phi(x) = log_{10}x\} = \{1\}$.*

Lemma 1.61 *If ϕ is a homomorphism of $G \times \bar{G}$,then*

1. *$\phi(e)$,the unit element in $\bar{G}$,*
2. *$\phi(x^{-1}) = (\phi(x))^{-1}, \forall x \in G$.*

Proof: 1. Let $x \in G, \phi(x) \in \bar{G}$. Now, $\phi(x) \cdot \bar{e} = \phi(x) = \phi(x \cdot e) = \phi(x) \cdot \phi(e) \Rightarrow \phi(e) = \bar{e}$ (By LCL)
2. By (1), we have $\phi(e) = \bar{e} \Rightarrow \bar{e} = \phi(e) = \phi(x \cdot x^{-1}) = \phi(x) \cdot \phi(x^{-1}) \Rightarrow \phi(x^{-1}) = [\phi(x)]^{-1}$

Remark 1.62 *Since e is the kernal of any homoomorphism, K_ϕ is not empty.*

Lemma 1.63 *If ϕ is the homoomorphism of G into $\bar{G}$ with kernal K, then K is a normal subgroup of G.*
Proof: Let $x, y \in K$. Then $\phi(x) = \bar{e}, \phi(y) = \bar{e}$. Now, $\phi(xy) = \phi(x) \cdot \phi(y) = \bar{e} \cdot \bar{e} = \bar{e} \Rightarrow xy \in K$ .....(i).
Now,$\phi(x^{-1}) = [\phi(x)]^{-1}$ (by (2) of Lemma 1.61) $\phi(x^{-1}) = (e^{-1})^{-1} = e \Rightarrow x^{-1} \in K$ .....(ii).
By (i) and (ii), K is a subgroup of G. Let $g \in G$ and $k \in K, \phi(k) = \bar{e}$. Now, $\phi(gkg^{-1}) = \phi(g)\ \phi(k)\ \phi(g^{-1}) = \phi(g)\ \phi(k)\ [\phi(g)]^{-1} = \phi(g)\ \bar{e}\ [\phi(g)]^{-1} = (\phi(g))\ [\phi(g)]^{-1} \Rightarrow \phi(gkg^{-1}) = \bar{e} \Rightarrow gkg^{-1} \in K, \forall g \in G, k \in K$. Therefore K is a normal subgroup of G.

Lemma 1.64 *If ϕ is a homomorphism of G onto $\bar{G}$ with kernal K,then the set of all inverse images of $\bar{g} \in \bar{G}$ under ϕ in G is group by K_x, where x is any particular inverse image of $\bar{g}$ in G.*
Proof: We have to prove $K_x = \{\phi^{-1}(\bar{g}), x \in G | \phi(x) = \bar{g}\}$ If $y \in K_x \Rightarrow y = k_x, k \in K$. (Since $k \in K, \phi(k) = \bar{e}$) Now, $\phi(y) = \phi(kx) = \phi(k) \cdot \phi(x) = \bar{e} \cdot \bar{g} = \bar{g} \Rightarrow y \in \phi^{-1}(\bar{g})$, Therefore $kx\ C\{\phi^{-1}(\bar{g})\}$.....(i)
Does all the elements of K_x are in the collection of inverse images of $\bar{G}$ whenever exists? Let us check can there be any other. Suppose that $Z = G\ \ni$: $\phi 9 = (Z) = \bar{g} = \phi(x) \Rightarrow \phi(Z) = \phi(x) \Rightarrow \phi(Z) \cdot [\phi(x)]^{-1} = \bar{e} \Rightarrow \phi(Z)\ \phi(x^{-1}) = \bar{e} \Rightarrow \phi(Z\ x^{-1}) = \bar{e} \Rightarrow Z\ x^{-1} \in K \Rightarrow Z \in Kx \Rightarrow \{\phi^{-1}\ (\bar{g})\}\ C\ k_x$.....(ii)
from (i) and (ii), $k_x = \{\phi^{-1}(\bar{g})\}$.

Result 1.65 *Let $\phi : G \to \bar{G}$ be a (function) homomorphism. $K_\phi = \{e\}$ iff ϕ is $1-1$.*
Proof: Suppose ϕ is $1-1$. Let $x, y \in G$. Let $x \in K_\phi \Rightarrow \phi(x) = \bar{e} = \phi(e)$ [By Lemma 1.61(1)] $\Rightarrow \phi(x) = \phi(e) \Rightarrow x = e$ [$\because \phi$ is $1-1$]. Conversely suppose that $K_\phi = \{e\}$. To prove: ϕ is $1-1$. Suppose, $\phi(x) = \phi(y) \Rightarrow \phi(x)[\phi(y)]^{-1} = \bar{e} \Rightarrow \phi(x)\ (\phi(y^{-1})) = \bar{e} \Rightarrow \phi(xy^{-1}) = \bar{e}$ [$\because \phi$ is homomorphism] $\Rightarrow xy^{-1} \in K_\phi = \{e\} \Rightarrow xy^{-1} = e \Rightarrow x = y \Rightarrow \phi$ is $1-1$.

Definition 1.66 *A homomorphism $\phi : G \to \bar{G}$ is said to be an isomorphism if ϕ is 1-1.*

Remark 1.67 *$\phi : G \to \bar{G}$ is an isomorphism $\Leftrightarrow K_\phi = \{e\}$.*

Definition 1.68 *Two groups G, G^* are said to be isomorphic if there is an isomorphism of G onto G^*. It is denoted by $G \cong G^*$. [(i.e.) $\phi : G \to G^*, \phi$ is $1-1$, onto and homomorphism if $G \cong G^*$].*

Result 1.69 *Isomorphic '$\cong$' is an equivalence relation.*
Proof:

1. Let $i_G : G \to G$ define by $i_G(x) = x \ \forall x \in G$, is a identity function on G. Clearly identity function is $1-1$, onto and homomorphism. So $G \cong G$ is reflexive.

2. Now, let $G \cong G^*$ and $f : G \to G^*$ be an isomorphism.
   $\Rightarrow f$ is $1-1$, onto and homomorphism.
   $\Rightarrow f^{-1} : G^* \to G$ is also $1-1$ and onto. [since $f(a) = (b) \Rightarrow f^{-1}(b) = a$]
   Now, let $x^*, y^* \in G^*$.
   Let $f^{-1}(x^*) = x$ and $f^{-1}(y^*) = y$.
   $\Rightarrow f(x) = x^*$ and $f(y) = y^*$.
   $f(xy) = f(x)f(y) = x^*y^*$
   $f^{-1}(x^*y^*) = xy = f^{-1}(x^*)f^{-1}(y^*)$.
   $\therefore f^{-1}$ is homomorphism.
   $\therefore f^{-1}$ is $1-1$,onto and homomorphism.
   $\Rightarrow G^* \cong G$ and hence symmetric.

3. Now let $G \cong G^*$ and $G^* \cong G^{**}$ with $f : G \to G^*$ and $g : G^* \to G^{**}$. Hence f and g are bijections and $g \circ f : G \to G^{**}$ is also a bijection.

   Now let $x, y \in G$.
   Then $(g \circ f)(xy) = g(f(xy))$
   $= g(f(x)f(y))$ ($\because f$ is homomorphism)
   $= g[f(x)]\ g[f(y)]$
   $= (g \circ f)(x)(g \circ f)(y)$
   $\therefore g \circ f$ is isomorphism.

   $\{\because$ Let $x, y \in G$.
   $\Rightarrow (g \circ f)(x) = (g \circ f)(y)$
   $\Rightarrow g(f(x)) = g(f(y))$
   $\Rightarrow f(x) = f(y)$ [$\because g$ in $1-1$]
   $\Rightarrow x = y$ ($\because f$ is $1-1$)
   $\therefore g \circ f$ is also $1-1$
   $g(y) = z$ ($\because g$ is onto)
   $f(x) = y$(f is onto)
   $g \circ f(x) = g[f(x)]$
   $= g(y) = z$.
   $\therefore g \circ f$ is onto.$\}$

   $\Rightarrow G \cong G^{**} \Rightarrow$ transitive. Thus $'\cong'$ is an equivalence relation.

Corollary 1.70 *A homomorphism $\phi : G$ into $\bar{G}$ with kernal K_ϕ is an isomorphism iff $K_\phi = \{e\}$.*
Proof: Suppose $\phi : G \to \bar{G}$ is an isomorphism with kernal K_ϕ.

To prove: $K_\phi = \{e\}$
Let $x \in K_\phi$.
$\Rightarrow \phi(x) = \bar{e} = \phi(e)$
$\Rightarrow x = e$
$\Rightarrow K_\phi = \{e\}$ [Since ϕ is $1-1$].
Conversely suppose $\phi : G \to \bar{G}$ is a homomorphism with kernal $K_\phi = \{e\}$.
To prove: ϕ is an isomorphism. It is enough to prove that ϕ is $1-1$.
Suppose $\phi(x) = \phi(y)$
$\Rightarrow \phi(x)[\phi(y)]^{-1} = e$
$\Rightarrow \phi(x)[\phi(y)^{-1}] = e$
$\Rightarrow \phi(xy^{-1}) = e$
$\Rightarrow xy^{-1} = e \Rightarrow x = y$. Therefore ϕ is $1-1$.

Theorem 1.71 *Let ϕ be a homomorphism of G onto $\bar{G}$ with kernal K. Then $G/K \cong \bar{G}$.*
Proof: Given: $\phi : G \to \bar{G}$ is an onto homomorphism and $K_\phi = K = \{x \in G | \phi(x) = \bar{e}$, identity in $\bar{G}\}$. Define a function $\sigma : G \to G/K$ by $\sigma(y) = K_y$ and $\psi : G/K \to \bar{G}$ by $\psi(Kg) = \phi(g)$. To prove:

1. ψ is well defined: Suppose, $Kg = Kg' \Rightarrow g \in Kg' \Rightarrow g = kg', k \in K \Rightarrow \phi(g) = \phi(kg') = \phi(k)\ \phi(g') = \bar{e}\phi(g') = \phi(g') \Rightarrow \psi(Kg) = \psi(Kg')$. Therefore ψ is well defined.

2. ψ is onto: Let $\bar{g} \in \bar{G}$. $\because \phi : G \to \bar{G}$ is onto, there exists an element $g \in G$ such that $\phi(g) = \bar{g} \Rightarrow \psi(Kg) = \bar{g}$ (i.e.) Every element $\bar{g} \in \bar{G}$ has inverse Kg under ψ. $\therefore \psi$ is onto.

3. ψ is a homomorphism: Let $x = Kg$ and $y = Kg' \in G/K$. Now, $\psi(xy) = \psi(Kg \cdot Kg') = \psi(Kgg') = \phi(gg')$ (by defn) $=\phi(g)\ \phi(g')[\because \phi$ is homomorphism$]=\psi(kg)\ \psi(kg') = \psi(x)\psi(y)$. $\therefore \psi$ is a homomorphism.

4. ψ is $1-1$: To prove: ψ is $1-1$. It is enough to prove that $K_\psi = \{e\} = \{x \in G/K | \psi(x) = \bar{e}\} = \{x = Kg, g \in G | \psi(Kg) = \bar{e}\} = \{g \in G | \phi(g) = \bar{e}\} = \{g \in G | g = \bar{e}\} = \{e\} \Rightarrow \psi$ is $1-1$. Thus $\psi : G/K \to \bar{G}$ is $1-1$, onto homomorphism. Hence $G/K \cong \bar{G}$.

Remark 1.72 *The above theorem tells that a group can be expected to arise from the homomorphic image of the general group must be expressible in the form of G/K where K is normal in G. (i.e.) For any normal subgroup N of G, G/N is a homomorphic image of G. Thus there is a $1-1$ correspondence between homomorphic images of G and normal subgroups of G.*

Definition 1.73 Simple: *A group G is said to be simple if it has no non-trivial normal subgroups.*

Theorem 1.74 ***Cauchy's Theorem for Abelian Groups:***
Suppose G is a finite abelian group and $p/O(G)$, where p is a prime number. Then there is an element $a \neq e \in G$ such that $a^p = e$.
Proof: We have to prove this theorem by induction over order of G $[O(G)]$. The theorem is clearly true for a group having single element. Assume that the theorem is true for all abelian groups having fewer elements than G.
case(i) If G has no subgroup $H \neq \{e\}$. Claim that G must be a cyclic group of prime order. Consider an element $a \in G, a \neq \{e\}$. Take $H = \langle a \rangle$. Then H is a subgroup of G and $H \neq \{e\}$. Therefore By hypothesis, $H = G = \langle a \rangle$. $\Rightarrow G = \langle a \rangle$, since G has no improper subgroup. Therefore G is a cyclic group. Any cyclic group is isomorphic to $(Z, +)$ or $(Z_n, \oplus)$. Since G is finite, $G \cong Z_n$, for some n. Claim that n is prime. Suppose not, (i.e) n is composite. Let $n = pq, 1 < p < n, 1 < q < n$ where p and q are primer. Now the subgroup generated by a, (i.e) $\langle a^p \rangle$ is a proper subgroup of G of order G. (i.e) G has a proper subgroup which is not equal to $\{e\}$, which is a contradiction. Therefore our assumption is wrong. Therefore n is prime. Hence G is a cyclic group of prime order. Then G has $p-1$ elements. By a corollary to Lagrange's theorem $a^p = a^{O(G)} = e$ and $a \neq e$.
case(ii) Suppose G has a improper subgroup $N \neq \{e\}$
subcase:(a)
If $p/O(N)$
Since $O(N) < O(G)$ and N is abelian, by induction hypothesis there is an element $b \in N, b \neq e$ such that $b^p = e$.[$\because$ $p/O(N)$ and N is abelian and $O(N) < O(G)$ By induction hypothesis] $b \in N \subset G \Rightarrow b \in G$. Thus there exists an element $b \in G$ such that $b^p = e$ and $b \neq \{e\}$.
subcase:(b)
Suppose G has a proper subgroup $N \neq \{e\}$ and p does not divides $O(N)$. Since G is a abelian and N is a normal subgroup of G, G/N is a group. [$\because$ subgroup of an abelian group is normal]. Moreover, $O(G/N) = \frac{O(G)}{O(N)}$, since $p/O(G)$ and p does not divides $O(N), p$ divides $\frac{O(G)}{O(N)}$. [If not,(i.e) if p does not divides $\frac{O(G)}{O(N)} \Rightarrow p$ does not divides $O(G/N)$ and $p/O(N) \Rightarrow p$ does not divides $O(G)$, which is a contradiction]. (i.e) $p/O(G/N)$ and $O(G/N) < O(G)$. Therefore by induction hypothesis there exists and element $x \in G/N, x \neq N$ such that $x^p = N$.....(1)
$\because$ $x \in G/N, x = N_b$ Where $b \in G$ and $N = N_e$. By (1), $x^p = N \Rightarrow (Nb)^p = N \Rightarrow Nb^p = N$ [$\because$ $Ha = H \Leftrightarrow a \in H$] $\Rightarrow b^p \in N$ and $b \notin N$ $\Rightarrow (b^p)^{O(N)} = e$ [$\because$ $a \in G, a^{O(G)} = e$] $\Rightarrow b^{pO(N)} = e \Rightarrow (b^{O(N)})^p = e$. Let $b^{O(N)} = c$. Therefore $c^p = e, c \in N \subset G$.
claim that $c \neq e$
Suppose $c = e$.
$\Rightarrow b^{O(N)} = e \Rightarrow Nb^{O(N)} = Ne = N \Rightarrow Nb^{O(N)} = N \Rightarrow Nb = N \Rightarrow b \in N$ $\Rightarrow\Leftarrow$ to $b \notin N$. Hence, $c \neq e$. Thus there exists an element $c \in G, c \neq e$ such that $c^p = e$. Hence, the theorem.

Theorem 1.75 ***Sylow's theorem for finite abelian Groups:*** *If G is an abelian group of order, $O(G)$ and p is a prime number such that $p^\alpha/O(G)$ and $p^{\alpha+1}$ does not divides $O(G)$. Then G has a subgroup of order p^α.*
Proof: If $\alpha = 0$, then the subgroup $\{e\}$ satisfies the conclusion of the result. Suppose $\alpha \neq 0$. $[p^\alpha = p^0 = 1/O(G), p^{\alpha+1} = 2^1$ does not divides $O(G)]$.
Then $p/O(G)$, and G is abelian. $[\because p/p^\alpha/O(G) \Rightarrow p/O(G)]$. Therefore by Cauchy's theorem for finite abelian group there exists an element $a \neq e$ satisfying $a^p = e$. Let $S = \{x \in G | x^{p^n} = e$, for some integer $n\}$. $\because e \in G$ and $e^{p^n} = e$, $e \in S$. Therefore S is non-empty. $a \neq e, a^p = e \Rightarrow a^{p^1} = e \Rightarrow a \in S \Rightarrow S \neq \{e\}$.
Claim(i) S is a subgroup of G
Let $x, y \in S \Rightarrow x^{p^n} = e$ and $y^{p^m} = e$ for some intega n, m. Now $(xy)^{p^{mn}} = x^{p^{mn}} \cdot y^{p^{mn}} = (x^{p^n})^m \cdot (y^{p^m})^n = e^m \cdot e^n = e \Rightarrow xy \in S$. Therefore S is a subgroup of G [$\because S$ is finite]. Hence, the Claim(i).
Claim:(ii) $O(S) = p^\beta, O < \beta \leq \alpha$
Suppose $q \neq p$ and $q/O(S)$. Therefore by Cauchy's theorem, there exists an element $c \in S, c \neq e$ such that $c^q = e$. $\therefore c \in S$ there exists an integer $n \geq O$ such that $c^{p^n} = e$. Also, $(p^n, q) = 1$. Therefore integer λ and μ such that $\lambda p^n + \mu q = 1$. Now, $c = c^1 = c^{\lambda p^n + \mu q} = c^{\lambda p^n} \cdot c^{\mu q} = (c^{p^n})^\lambda \cdot (c^q)^\mu = e^\lambda \cdot e^\mu = e \cdot e \Rightarrow c = e \Rightarrow\Leftarrow$ to the fact that $c \neq e$. Thus there exists no prime number other than p which divides $O(S)$. $\because S$ is a subgroup of G, by Lagranges theorem $O(S)/O(G)$. Let $O(S) = p^\beta$, for some integer β, then we get $\beta \leq \alpha$. Suppose, $\beta < \alpha$. Consider the abelian group (G/S). Since $\beta < \alpha$, and $O(G/S) = \frac{O(G)}{O(S)}, p/O(G/S)$
$[\because p^\alpha/O(G) \Rightarrow O(G) = kp^\alpha$
$O(S) = p^\beta, \beta < \alpha, \alpha - \beta > 0, \alpha - \beta = \gamma > 0$
$O(G/S) = O(G)/O(S) = kp^\alpha/p^\beta = kp^{\alpha-\beta} = kp^\gamma$
$p/kp^\gamma \Rightarrow p/O(G/S)]$
$\because S$ is a normal subgroup of G and G is abelian, G/S is a group.
By Cauchy's theorem for finite abelian group there exists an element $Sx \in G/S, Sx \neq S$ such that $(sx)^{p^n} = S \Rightarrow Sx^{p^n} = S \Rightarrow x^{p^n} \in S[a \in G, a^{O(G)} = e] \Rightarrow (x^{p^n})^{O(S)} = e \Rightarrow (x^{p^n})^\beta = e \Rightarrow x^{p^{n+\beta}} = e$, $n + \beta > 0$, integer $\Rightarrow x \in S \Rightarrow Sx = S[a \in H \Leftrightarrow Ha = H] \Rightarrow\Leftarrow$to $Sx \neq S$. Therefore our assumption is wrong. (i.e) $\beta < \alpha$. Therefore $\beta = \alpha$. $\therefore O(S) = p^\beta = p^\alpha$. Hence,$G$ has a subgroup S such that $O(S) = p^\alpha$

Corollary 1.76 *If G is an abelian group of $O(G)$ and $p^\alpha/O(G)$, $p^{\alpha+1}$ does not divides $O(G)$ then there is a unique subgroup of G of order p^α.(p sylow subgroup)*
Proof: Suppose S and T are two subgroups of order p^α where $p^\alpha/O(G)$ and $p^{\alpha+1}$ does not divides $O(G)$
Suppose $S \neq T, O(S) = p^\alpha, O(T) = p^\alpha$. Now $O(ST) = O(S)O(T)/O(S \cap T) = p^\alpha p^\alpha/O(S \cap T) = p^{2\alpha}/O(S \cap T)$. $\because S \neq T$ and $S \cap T \subset S, O(S \cap T) <$

$O(S) = p^\alpha$. (i.e) $O(S \cap T) < p^\alpha$. Therefore $O(ST) = p^\gamma, \gamma > \alpha$. $\because G$ is abelian, $ST = TS$. Therefore ST is a subgroup of G, by Lagrange's Theorem $O(ST)/O(G)$. (i.e) $p^\gamma/O(G), \gamma > \alpha \Rightarrow p^{\alpha+1}/O(G) \Rightarrow\Leftarrow$ to $p^{\alpha+1}$ does not divides $O(G)$. This contradition shows that $S = T$. Therefore there exists a unique subgroup of G of order p^α

Lemma 1.77 *Let ϕ be a homomorphism of G onto $\bar{G}$ with kernal K. For $\bar{H}$ a subgroup of $\bar{G}$, let H be defined by $H = \{x \in G | \phi(x) \in \bar{H}\}$. Then*
(i) H is a subgroup of G
(ii) H contains K and
(iii) if $\bar{H}$ is normal in $\bar{G}$ then H is normal in G. Moreover this association sets up a $1-1$ mapping from the set of all subgroup of $\bar{G}$ onto the set of all subgroups of G which contains K.
Proof: Let $x, y \in H$. Then $\phi(x), \phi(y) \in H$. Now, $\phi(xy) = \phi(x) \cdot \phi(y) \in \bar{H}$ [$\because \bar{H}$ is a subgroup of $\bar{G}$]. Therefore $\phi(xy) \in \bar{H}$.....(i)
By definition, $xy \in H$. $\phi(x^{-1}) = [\phi(x)]^{-1}$ [$\because$ ϕ is homomorphism]$\Rightarrow$ $\phi(x^{-1}) \in \bar{H}$. Therefore $x^{-1} \in H$ (by definition).....(ii). By (i) and (ii), H is a subgroup of G
To prove: $H \supset K$
Let $x \in K \Rightarrow \phi(x) = \bar{e} \in \bar{G}$ [$\because \bar{H}$ is a subgroup of $\bar{G}$] $\Rightarrow \phi(x) = \bar{e} \in \bar{H}$ [$\because$ identity is unique in $\bar{G}$] $\Rightarrow x \in H$ (by definition) $\therefore K \subset H$
To prove: H is normal in G
Given:$\bar{H}$ is normal in $\bar{G}$. Let $g \in G$ and $h \in H$. Therefore $\phi(g) \in \bar{G}$ and $\phi(h) \in \bar{H}$ (by definition) and ϕ is onto map. Since $\bar{H}$ is normal in $\bar{G}$, $\phi(g)\phi(h)\phi(g^{-1}) \in \bar{H}$. (i.e) $\phi(ghg^{-1}) \in \bar{H} \Rightarrow ghg^{-1} \in H$. Therefore H is normal G. Hence given a subgroup $\bar{H}$ of $\bar{G}$, we have a subgroup of H of G such that $H \supset K$.
Conversely, suppose that L is a subgroup of G and $L \supset K$. Let $\bar{L} = \{\bar{x} \in \bar{G} | \bar{x} = \phi(x), x \in L\}$. Claim that $\bar{L}$ is a subgroup of $\bar{G}$. Let $\bar{x} \cdot \bar{y} \in \bar{L}$. Therefore $\bar{x} = \phi(x), \bar{y} = \phi(y) \Rightarrow \bar{x} \cdot \bar{y} = \phi(x) \cdot \phi(y), x, y \in L = \phi(x \cdot y), x, y \in L \Rightarrow \bar{x} \cdot \bar{y} \in \bar{L}$ (by definition) and $(\bar{x})^{-1} = [\phi(x)]^{-1}, x \in L = \phi(x^{-1}), x^{-1} \in L$. Therefore $x^{-1} \in \bar{L}$. Define: $T = \{x \in G | \phi(x) \in \bar{L}\}$. The correspondence is $1-1 \Leftrightarrow L = T$. $x \in L \Rightarrow \bar{x} = \phi(x) \in \bar{L}$ (by definition of $\bar{L}$) $\Rightarrow x \in T$. Therefore $L \subset T$.....(iii)
Conversely, let $t \in T$, $\phi(t) \in \bar{L} \Rightarrow \phi(t) = \phi(e), e \in L$. Therefore $\phi(te^{-1}) = \phi(t)\phi(e^{-1}) = \phi(t)[\phi(e)]^{-1} = \phi(t)[\phi(t)]^{-1} = \bar{e}$. Therefore $te^{-1} \in K \subset L \Rightarrow te^{-1} \in L \Rightarrow t \in Le \Rightarrow t \in L$. Therefore $T \subset L$.....(iv)
From (iii) and (iv), $T = L$
Therefore the correspondence is $1-1$.

Theorem 1.78 *Let ϕ be a homomorphism of G onto $\bar{G}$ with kernal K. Let $\bar{N}$ be a normal subgroup of $\bar{G}$, $N = \{x \in G | \phi(x) \in \bar{N}\}$. Then G/N*

isomorphic to $\bar{G}/\bar{N}$. *Equivalently* $G/N \cong (G/K)/(N/K)$
Proof: Let $\phi : G \to \bar{G}$ is a homomorphism. Then $\theta : \bar{G} \to \bar{G}/\bar{N}$ by $\theta(\bar{g}) = \bar{N}\bar{g}$ is a homomorphism of $\bar{G}$ onto $\bar{G}/\bar{N}$. Now, define $\psi : G \to \bar{G}/\bar{N}$ by $\psi(g) = \theta \cdot \phi(g)$. (i.e) $\psi(g) = \bar{N}\phi(g)$. $\because \theta$ and ϕ are onto mapping, ψ is also onto mapping.
ψ **is a homomorphism:**
Suppose $a, b \in \bar{G}$. Then $\psi(a) = \bar{N}\phi(a)$ and $\psi(b) = \bar{N}\phi(b)$. Now, $\psi(a \cdot b) = \bar{N}\phi(ab) = \bar{N}[\phi(a) \cdot \phi(b)] = \bar{N}\phi(a) \cdot \bar{N}\phi(b) = \psi(a) \cdot \psi(b)$. $\therefore \psi$ is a homomorphism. Let T be the kernal of ψ. (i.e) $T = \{g \in G | \psi(g) = \bar{N}\}, \bar{N}$ is identity in $\bar{G}/\bar{N}$.
Claim that $T = N$. Let $n \in N \Rightarrow \phi(n) \in \bar{N}[\because N = \{x \in G/O(x) \in \bar{N}\}] \Rightarrow \bar{N}\phi(n) = \bar{N} \Rightarrow \psi(n) = \bar{N} \Rightarrow n \in T$ [by the definition of T]. $\therefore N \subset T$.....(1)
Let $t \in T \Rightarrow \psi(t) = \bar{N} \Rightarrow \bar{N} \cdot \phi(t) = \bar{N} \Rightarrow \phi(t) \in \bar{N} \Rightarrow t \in N$ [by the definition of $\bar{N}$]. $\therefore T \subset N$.....(2)
From (1) and (2) $T = N$. Thus ψ is a homomorphism of G onto $\bar{G}/\bar{N}$ with kernal N. By the fundamental theorem of homomorphism, $G/N \cong \bar{G}/\bar{N}$.
$\because \bar{G} \cong G/K$ and $\bar{N} \cong N/K$
[$\because \phi : G$ onto $\bar{G}$ is a homomorphism with kernal K]
$\Rightarrow G/K \cong \bar{G}$
and $\phi/N : N$ onto N is a homomorphism with kernal $\bar{K}$
$\Rightarrow N/K \cong \bar{N}$
$\therefore G/N \cong \frac{G/K}{N/K}$ [$\because \bar{G}$ is isomorphic to G/K]
and $\bar{N} \cong N/K$
$\because \phi : G$ onto $\bar{G}$ is a homomorphism with kernal K.
$\phi/N : N$ onto $\bar{N}$ is a homomorphism with kernal K.
$\therefore G/N \cong \frac{G/K}{N/K}$ [by above theorem]
This theorem is known as first homomorphism theorem.

Theorem 1.79 ***CAYLEY'S THEOREM:*** *Every group is isomorphic to a subgroup of* $A(S)$ *for some appropriate* S, *Where* $A(S)$ *is the set of all* $1-1$ *mapping from* S *onto* S. *(i.e.) set if all bijection on* S.
Proof: Let G be a group, choose $S = G$. Define $T_g : S(G) \to S(G)$ by $xT_g = xg$. Clearly T_g is well defined.
T_g is onto:
For $y \in S$, choose $x = yg^{-1}$. Then $xT_g = (yg^{-1})T_g = yg^{-1}g = y$. (i.e.) every element $y \in G$ has pre-image $yg^{-1} \in G$ under T_g. $\therefore T_g$ is onto
T_g is $1-1$:
Let $x, y \in S$. Suppose $xT_g = yT_g \Rightarrow xg = yg \Rightarrow x = y$ (By RCL) $\Rightarrow T_g$ is $1-1$. $\therefore T_g \in A(S)$. Now, consider the map $\psi : G \to A(S)$,defined by $\psi(g) = T_g$. Suppose $g, h \in G$, then $(x)T_g \cdot T_h = ((x)T_g)T_h = (xg)T_h = xgh = (x)T_{gh}$ $\forall x$. $\therefore T_g \cdot T_h = T_{gh} \Rightarrow \psi(gh) = \psi(g) \cdot \psi(h)$. $\therefore \psi$ is a homomorphism. Let K be the kernal of ψ , then $K = \{g \in G | \psi(g) = \bar{e}, \bar{e}$ is the identity in $A(S)\} = \{g \in G | T_g = I$, Identity function $S \to S\} = \{g \in G | xT_g = x,$

Identity function $S \to S\} = \{g \in G | xg = x$, Identity function $S \to S\} = \{g \in G | g = e$, Identity in $G\} = \{e\}$. $\therefore \psi$ is an isomorphism of G into S. [By corollary to Lemma 1.64] A homomorphism $\phi : G \to \bar{G}$ with kernal K_ϕ is an isomorphism of G into $\bar{G} \Leftrightarrow K_\phi = \{e\}$.

Theorem 1.80 *If G is a group, H is a subgroup of G, and S is the set of all right cosets of H in G, then there is a homomorphism θ of G into $A(S)$, and the kernal of θ is the largest normal subgroup of G,which is contained in H.*
Proof: Let G be a group. Let H be a subgroup of G and $S = \{Hg | g \in G\}$. Define $t_g : S \to S$ by $(Hx)t_g = Hxg, \forall x \in G$. Clearly, t_g is well defined.
t_g is onto: Suppose, $Hy \in S$. Consider, $x = Hyg^{-1} \in S$. Now, $(x)t_g = (Hyg^{-1})t_g = (Hyg^{-1})g = Hy$. $\therefore t_g$ is onto.
t_g is 1-1:
Let $Hx, Hy \in S$. Suppose $(Hx)t_g = (Hy)t_g \Rightarrow Hxg = Hyg \Rightarrow Hx = Hy$. $\therefore t_g$ is $1-1$. $\therefore t_g$ is $1-1$ and onto, $\Rightarrow t_g n \in A(S)$. Define a function $\theta : G \to A(S)$ by $\theta(g) = t_g$. Clearly θ is well defined.
θ is a homomorphism:
For every $Hx \in A(S), (Hx)t_{gh} = Hxgh = (Hxg)t_h = ((Hx)t_g)t_h \Rightarrow (Hx)t_{gh} = ((Hx)t_g)t_h \quad \forall Hx \in S$. This is true for every $Hx \in S$. $\therefore t_{gh} = t_g \cdot t_h \Rightarrow \theta(gh) = \theta(g) \cdot \theta(h)$. $\therefore \theta$ is a homomorphism. Let K be the kernal of θ. $K = \{g \in G | \theta(g) = \bar{e}, \bar{e}$ is identity in $A(S)\} = \{g \in G | t_g = I, I : S \to S$ is identity$\} = \{g \in G | (Hx)t_g = (Hx)I, I : S \to S$ is identity$\} = \{g \in G | Hxg = HxI, I : S \to S$ is identity$\} = \{g \in G | Hxg = Hx\}$.....(1)
$= \{g \in G | xgx^{-1} \in H, \forall x \in G\} =$Normal subgroup of G. $\therefore$ kernal of a homomorphism is a normal subgroup of G.
To prove: $K \subset H$
Suppose let $b \in K$. $\therefore Hxb = Hx$ [by(1)] $\forall x \in G$. Put $x = e \Rightarrow Heb = He \Rightarrow Hb = H \Rightarrow b \in H \quad [\because Ha = H \Leftrightarrow a \in H]$. $\Rightarrow K \subset H$. $\therefore K$ is a normal subgroup of G contained in H.
To prove: K is the largest normal subgroup of G.
Suppose N is a normal subgroup of G which is contained in H. Let $n \in N$. $\because N$ is normal in $G, xnx^{-1} \in N \quad \forall x \in G \Rightarrow xnx^{-1} \in H \ [\because N \subseteq H] \Rightarrow Hxn = Hx \quad \forall x \in G [\because Ha = Hb \Leftrightarrow ab^{-1} \in H] \Rightarrow n \in K$ [by(1)] $\Rightarrow N \subset K$. $\therefore K$ is the largest normal subgroup of G contained in H.

Lemma 1.81 *If G is a finite group and $H \neq G$ is subgroup of G such that $O(G)$ does not divides $i(H)!$. Then H must contain a non trivial normal subgroup of G. In particular G cannot be simple.*
Proof: By above theorem, there is a homomorphism $\theta : G \to A(S)$ where S is the set of all right cosets of H in G. $\therefore O(S) = i(H)$, index of H. $\therefore O(A(S)) = i(H)!$. If $O(G)$ does not divides $i(H)! = O(A(S)) \Rightarrow O(G)$ does not divides $O(A(S))$. Then by Lagrange's theorem, we have A(S) can have no subgroup of order $O(G)$. Hence no subgroup is isomorphic to G. However, $A(S)$ does not contain $\theta(G) \subset A(S)$. Hence, $\theta(G)$ cannot be

isomorphic to G. (i.e.) θ cannot be an isomorphism but then kernal of θ is non-trivial normal subgroup of H. (i.e.) Here G has a non-trivial normal subgroup kernal of θ. Hence G cannot be simple.

Example 1.82 *If G is a group of order 36 and H is a subgroup of order 9. Then prove that, H contains a normal subgroup of order 3.*
Proof: $O(G) = 36; O(H) = 9; i(H) = \frac{O(G)}{O(H)} = 36/9 = 4; i(H)! = 4! = 24 \Rightarrow i(H)! < O(G)$. $\therefore$ By above theorem, H contains non-trivial normal subgroup N. (i.e.) N is a normal subgroup of H. $\therefore$ By Lagrange's Theorem, $O(N)/O(H)$. $\therefore O(N)/9 \Rightarrow O(N) = 1$ (or) $O(N) = 3$ (or) $O(N) = 9$. If $O(N) = 1$, then $N = \{e\} \Rightarrow\Leftarrow N \neq \{e\}$. If $O(N) = 9 \Rightarrow N = H \Rightarrow\Leftarrow N \neq H$. $\therefore O(N) = 3$.

Example 1.83 *Suppose G is a group of order 99 and H is a subgroup of G order 11. Then H is a normal subgroup of G.*
Proof: $O(G) = 99; O(H) = 11; i(H) = \frac{O(G)}{O(H)} = \frac{99}{11} = 9; i(H)! = 9!$. $\therefore$ By previous Lemma, H must contain a non-trivial normal subgroup N of $G \Rightarrow O(N)/O(H) = O(N)/11 \Rightarrow O(N) = 1$ (or) $O(N) = 11$ but $O(N) \neq 1$, since non-trivial. $\therefore O(N) = 11 = O(H) \Rightarrow N = H$. $\therefore H$ is a normal subgroup of G.

Permutation Group:

Suppose S_n is a finite set, having n elements, $S = \{x_1, x_2, ...x_n\}$. Then the set of all $1-1$ mapping of S onto itself, written as $A(S) = S_n$.

Definition 1.84 *Let S be a set and $\theta \in A(S)$. Given two elements $a, b \in S$ we define $a \equiv \theta^b \Leftrightarrow b = a\theta^i$ for some integer i. [i can be $+ve, -ve$ or zero]*

Result 1.85 *Congruence θ is an equivalence relation.*
Proof: (i) $\equiv \theta$ reflexive: $a = a\theta^0 = ae \Rightarrow a \equiv \theta^a \ \forall a \in S$. $\therefore \equiv \theta$ is reflexive.
(ii) $\equiv \theta$ is symmetric: Suppose $a \equiv \theta^b$ then $b = a\theta^i$ for some integer $i \Rightarrow a = b\theta^{-i} \Rightarrow b \equiv \theta^a$. $\therefore \equiv \theta$ is symmetric.
(iii) $\equiv \theta$ is transitive: Suppose $a \equiv \theta^b$ and $b \equiv \theta^c \Rightarrow b = a\theta^i$ and $c = b\theta^j$ for some integer i and j. Now, $c = b \cdot \theta^j = (a\theta^i)\theta^j = a(\theta^{i+j}) \Rightarrow a \equiv \theta^c$,for some integer $c = i + j$. $\therefore \equiv \theta$ is transitive.
Hence $\equiv \theta$ is an equivalence relation.

Let S be a set and $\theta \in A(S)$. Given two elements $a, b \in S$ we define $a \equiv \theta^b$ iff $b = a\theta^i$. $\equiv \theta$ is an equivalence relation which induces a decomposition of S into disjoint subsets namely the equivalence classes.
Let $s \in S$, the equivalence classes of s is called the orbit of s under θ; thus the orbit of s under θ consists of the elements $s\theta^i, i = 0, \pm 1, \pm 2, ...$
If S is a finite set and $s \in S$, there is a smallest positive integer $l = l(s)$,

depending on s such that $s\theta^l = s$. The orbit of s under θ then consists of an element $\{s, s\theta, s\theta^2, s\theta^3, ...s\theta^{l-1}\}$. A cycle of θ is the ordered set of $\{s, s\theta, s\theta^2, s\theta^3, ...s\theta^{l-1}\}$.

Example 1.86 *Let* $S = \{1, 2, 3, 4\}$.

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\theta \cdot \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\theta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Example 1.87 *Find the orbit and cycles of the following permutations,*

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$$

Solution: $S = \{1, 2, 3, 4, 5, 6\}$
Orbit of 1:
$1\theta^0, 1\theta^1, 1\theta^2, 1\theta^3, ...$
$1\theta^0 = 1$
$1\theta^1 = 1 \cdot \theta = 2$
$1\theta^2 = (1\theta) \cdot \theta = 2 \cdot \theta = 1$
$1\theta^3 = (1\theta^2) \cdot \theta = 1 \cdot \theta = 2$
$1\theta^4 = (1\theta^3) \cdot \theta = 2 \cdot \theta = 1$
$1\theta^5 = (1\theta^4) \cdot \theta = 1 \cdot \theta = 2$
$\therefore$ Orbit of 1 consists of the element $\{1, 2\}$
Orbit of 2:
$2\theta^0, 2\theta^1, 2\theta^2, ...$
$2\theta^0 = 2$
$2\theta^1 = 2 \cdot \theta = 1$
$2\theta^2 = (2 \cdot \theta) \cdot \theta = 1 \cdot \theta = 2$
$2\theta^3 = (2 \cdot \theta^2) \cdot \theta = 2 \cdot \theta = 1$
$\therefore$ Orbit of 2 consists of the element $\{1, 2\}$
Orbit of 3:
$3\theta^0, 3\theta^1, 3\theta^2, ...$
$3\theta^0 = 3$
$3\theta^1 = 3 \cdot \theta = 3$
$3\theta^2 = (3\theta) \cdot \theta = 3 \cdot \theta = 3$

$\therefore$ Orbit of 3 consist of the element $\{3\}$
Orbit of 4:
$4\theta^0, 4\theta^1, 4\theta^2, ...$
$4\theta^0 = 4$
$4\theta^1 = 4 \cdot \theta = 5$
$4\theta^2 = (4\theta) \cdot \theta = 5 \cdot \theta = 6$
$4\theta^3 = (4\theta^2) \cdot \theta = 6 \cdot \theta = 4$
$4\theta^4 = (4\theta^3) \cdot \theta = 4 \cdot \theta = 5$
$\therefore$ Orbit of 4 consists of the element $\{4, 5, 6\}$
Orbit of 5:
$5\theta^0, 5\theta^1, 5\theta^2, ...$
$5\theta^0 = 5$
$5\theta^1 = 5\theta = 6$
$5\theta^2 = (5 \cdot \theta) \cdot \theta = 6 \cdot \theta = 4$
$5\theta^3 = (5 \cdot \theta^2) \cdot \theta = 4 \cdot \theta = 5$
$\therefore$ Orbit of 5 consists of the element $\{6, 5, 4\}$
Orbit of 6:
$6\theta^0, 6\theta^1, 6\theta^2, ...$
$6\theta^0 = 6$
$6\theta^1 = 6 \cdot \theta = 4$
$6\theta^2 = (6\theta) \cdot \theta = 4 \cdot \theta = 5$
$6\theta^3 = (6\theta^2) \cdot \theta = 5 \cdot \theta = 6$
$\therefore$ Orbit of 6 consists of the element $\{4, 5, 6\}$
Cycles are the ordered set of orbits
$\therefore$ Cycles is (1 2) (3) (4 5 6)

Example 1.88 *Find the orbit cycle of the following permutation*

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

Solution: *Orbit of* 1*:* $1\theta^0, 1\theta^1, 1\theta^2$
$1\theta^0 = 1$
$1\theta^1 = 1\theta = 2$
$1\theta^2 = (1\theta)\theta = 2 \cdot \theta = 3$
Orbit of $1 = \{1, 2, 3, 8, 5, 6, 4\}$
Orbit of $2 = \{2, 3, 8, 5, 6, 4, 1\}$
Orbit of $3 = \{3, 8, 5, 6, 4, 1, 2\}$
Orbit of $4 = \{4, 1, 2, 3, 8, 5, 6\}$
Orbit of $5 = \{5, 6, 4, 1, 2, 3, 8\}$
Orbit of $6 = \{6, 4, 1, 2, 3, 8, 5\}$
Orbit of $7 = \{7\}$
Orbit of $8 = \{8, 5, 6, 4, 1, 2, 3\}$
Orbit of $9 = \{9\}$

Cycles are (1 2 3 8 5 6 4) (7) (9)
Product of all the cycles, C_1, C_2, C_3

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 8 & 1 & 6 & 4 & 7 & 5 & 9 \end{pmatrix}$$

Theorem 1.89 *Every permutation is the Product of its cycles.*
Proof: Let θ be a permutation on the set S. Then its cycles are of the form $(s, s\theta, ...s\theta^{l-1})$, where l is the least positive integer such that $S\theta^l = S, s \in S$. Let ψ be the product of all distinct cycles of θ.
claim that $\theta = \psi$
By multiplication of cycles and since the cycles and since the cycle of θ are disjoint, the image of $s' \in S$ under θ which is $s\theta'$ is same as the image of S' under ψ. So, θ, ψ have the same effect on every element of S. Hence, $\theta = \psi$
$\therefore$ Every permutation is the product of disjoint cycles.

Example 1.90 *Let*

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 5 & 2 & 1 & 8 & 4 & 6 & 9 \end{pmatrix}$$

The cycles are of the form
$\theta_1 = (1\ \theta\ \theta^2) = (1\ 3\ 5)$*;* $\theta_2 = (2\ 2\theta\ 2\theta^2) = (2\ 7\ 4)$*;* $\theta_3 = (6\ 8)$*;* $\theta_4 = (9)$
$\psi = \theta_1 \cdot \theta_2 \cdot \theta_3 \cdot \theta_4 = (1\ 3\ 5)\ (2\ 7\ 4)\ (6\ 8)\ (9)$

Lemma 1.91 *Every permutation is the product of 2 cycles.*
Proof: Let θ be the permutation on $S = \{a_1, a_2, ..., a_n\}$. By above lemma, θ can be written as the product of its cycles. Let $(a_1, a_2, ..., a_m)$ be any cycle θ of length $m(m < n)$. This can be decomposed as $(a_1, a_2, ..., a_m) = (a_1, a_2)\ (a_1, a_3)...(a_1, a_m)$. $\therefore$ A_n m-cycle can be written as the product of 2-cycles. Any permutation can be expressed as a product of transpositions. Since every permutation is the product of its disjoint cycles and every cycle is a product of 2-cycles, it follows that every permutation is a product of 2-cycles.

Note 1.92 *We shall refer to 2-cycles as transpositions.*

Definition 1.93 *A permutation $\theta \in S_n$ is said to be an even permutation if it can be represented as a product of an even number of transpositions and is said to be an odd permutation if it can be represented as a product of an odd number of transpositions.*

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 $\theta \in S_n$

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

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

It is clear that $\theta : P(x_1, x_2, ..., x_n) \to \pm P(x_1, x_2, ..., x_n)$. For example, consider $\theta = (1\ 3\ 4)\ (2\ 5) \in S_5$. Then $P(x_1, x_2, ..., x_5) = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)$; $\theta(P(x_1, x_2, ..., x_5)) = (x_3 - x_5)(x_3 - x_4)(x_3 - x_1)(x_3 - x_2)(x_5 - x_4)(x_5 - x_1)(x_5 - x_2)(x_4 - x_1)(x_4 - x_2)(x_1 - x_2) = -[(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_1 - x_5)(x_2 - x_3)(x_2 - x_4)(x_2 - x_5)(x_3 - x_4)(x_3 - x_5)(x_4 - x_5)] = -P(x_1, x_2, ..., x_5)$. Suppose $\theta = (1, 2) \in S_2$; $P(x_1, x_2) = (x_1 - x_2)$; $\theta(P(x_1, x_2)) = (x_2 - x_1) = -(x_1 - x_2) = -P(x_1, x_2)$. (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 unchanged

(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

P. (i.e) P operated upon by a transposition becomes $-P$. If the permutation θ can be expressed as a product of x transposition then,
$\theta P = [(-1)(-1)...(-1)]P \quad (x \text{ times})$
$= (-1)^x \cdot P$.....(1)
Also if θ can be expressed as a product of y transpositions then,
$\theta P = [(-1)(-1)...(-1)]P \quad (y \text{ times})$
$= (-1)^y \cdot P$.....(2)
from (1) and (2), $(-1)^x \cdot P = (-1)^y \cdot P \Rightarrow (-1)^x = (-1)^y$
$\Rightarrow x$ and y are both odd (or) x and y are both even.

Lemma 1.96 *S_n has a normal subset of index 2, the alternating group A_n consisting of all even permutations.*
Proof: We know that S_n is group. A_n is the subset of S_n consisting of all even permutations.
A_n is a subgroup of S_n:
Let $\theta_1, \theta_2 \in A_n$. $\Rightarrow \theta_1$ and θ_2 are even permutations. $\Rightarrow \theta_1 \cdot \theta_2$ is an even permutation. $\Rightarrow \theta_1 \cdot \theta_2 \in A_n$ [$\because$ product of any two even permutation is even]. $\therefore A_n$ is a subgroup of S_n.
Claim that A_n is normal in S_n:
Let $W = \{1, -1\}$ is a group under multiplication. Define $\psi : S_n \to W$ by

$$\psi(s) = \begin{cases} 1 & \text{if } s \text{ is an even permutation} \\ -1 & \text{if } s \text{ is an odd permutation} \end{cases}$$

Claim that ψ is a homomorphism onto W. Let $s, t \in S_n$.
Case(i) If s, t are even, then st is even. $\therefore \psi(st) = 1 = 1 \cdot 1 = \psi(s) \cdot \psi(t)$
Case(ii) If s, t are odd, then st is even. $\therefore \psi(st) = 1 = -1 \times -1 = \psi(s) \cdot \psi(t)$
Case(iii) If s is odd and t is even, then st is odd. $\therefore \psi(st) = -1 = -1 \times 1 = \psi(s) \cdot \psi(t)$
Case(iv) Le t s is even and t is odd. (i.e) $\psi(s) = 1$ and $\psi(t) = -1 \Rightarrow st$ is odd. $\therefore \psi(st) = -1 = 1 \times -1 = \psi(s) \cdot \psi(t) \Rightarrow \psi$ is a homomorphism. Clearly ψ is onto.
Now, to prove A_n is normal in S_n. kernal $\psi = \{s \in S_n | \psi(s) = \text{identity in } W\} = \{s \in S_n | \psi(s) = 1\} = A_n$. Thus ψ is a homomorphism of S_n onto W with kernal A_n. $\therefore$ By Lemma 1.63, A_n = kernal ψ is normal in S_n. By Theorem 1.71 $S_n/A_n \cong W$. $\Rightarrow O(W) = O(\frac{S_n}{A_n}) \Rightarrow O(\frac{S_n}{A_n}) = 2$ [$\because O(G/H) = \frac{O(G)}{O(H)} = i_G(H)$] $\Rightarrow i_{s_n}(A_n) = 2$. Also, $O(A_n) = \frac{O(S_n)}{2} = \frac{n!}{2}$.

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 *$C(a) = \{x \in G | x \sim a\} = \{x \in G | x \sim a\} = \{x \in G | x = y^{-1}ay, y \in G\} = \{y^{-1}ay | y \in G\}$. If consists of the set of all distinct elements 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,*

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

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

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) $G = S_3 = \{e, \phi, \psi, \phi \cdot \psi, \psi \cdot \phi, \psi^2\}$. $N(\phi) = \{e, \phi\}$; $N(\psi) = \{e, \psi, \psi^2\}$; $N(\psi^2) = \{e, \psi^2, \psi\}$.

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 $G = S_3 = \{e, \phi, \psi, \phi \cdot \psi, \psi \cdot \phi, \psi^2\}$. $C(\phi) = \{x^{-1}\phi x | x \in S_3\} = \{e^{-1}\phi e, \phi^{-1}\phi\phi, \psi^{-1}\phi\psi, (\phi \cdot \psi)^{-1}\phi(\phi \cdot \psi), (\psi \cdot \phi)^{-1}\phi(\psi \cdot \phi), (\psi^2)^{-1}\phi\psi^2\}$
$C(1,2) = \{e^{-1}(1,2)e, (1,2)^{-1}(1,2)(1,2), \psi^{-1}(1,2)\psi, (\phi\cdot\psi)^{-1}(1,2)(\phi\cdot\psi), (\psi\cdot\phi)^{-1}(1,2)(\psi\cdot\phi), (\psi^2)^{-1}(1,2)\psi^2\} = \{(1\ 2\ 3)\ (1\ 2)\ (1\ 2\ 3), (1\ 2)\ (1\ 2)\ (1\ 2), (1\ 3\ 2)\ (1\ 2)\ (1\ 3\ 2), (1\ 3)\ (1\ 2)\ (1\ 3), (2\ 3)\ (1\ 2)\ (2\ 3), (2\ 3\ 1)\ (1\ 2)\ (1\ 3\ 2)\} = \{(1\ 2), (1\ 2), (2\ 3)\}$. $\therefore C(\phi) = \{\phi, \phi \cdot \psi, \psi \cdot \phi\}$
$C_{(1,2)} = O(C(1,2)) = 3$. $\frac{O(G)}{O(N(1,2))} = \frac{6}{3} = 3$. $\therefore C_{(1,2)} = \frac{O(S_3)}{O(N(1,2))}$.

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, yields 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 $n \in N(a), [\because y \in N(a) \cdot x, y = nx] \Rightarrow y^{-1} = (nx)^{-1} = x^{-1}n^{-1}$; $y^{-1}ay = x^{-1}n^{-1}ay = x^{-1}n^{-1}anx = x^{-1}(n^{-1}an)x = x^{-1}ax = x^{-1}ax$. 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 $x^{-1}ax \neq y^{-1}ay$. 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

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

Proof: By previous theorem,

$$O(G) = \sum_{a \in G} C_a = \sum_{a \in G} \frac{O(G)}{O(N(a))}$$

Where the sum runs over one element a from in each conjugate class. This is known as class equation of G.

Example 2.10 *State and Prove class equation of a group G.*
Proof: The proof is obvious from above theorem and its corollary.

Definition 2.11 ***Centre of** a **group** G: The centre Z (or) $Z(G)$ of a group G is defined by $Z = \{z \in G | xz = zx \ \forall x \in G\}$.*

Example 2.12 *(i) $G = \{1, -1, i, -i\}$ and $Z = G$.*
(ii) $G = S_3$ and $Z(G) = Z(S_3) = \{e\}$.

Lemma 2.13 *$a \in Z(G) \Leftrightarrow N(a) = G$; if G is finite, $a \in Z(G) \Leftrightarrow O(N(a)) = O(G)$*
Proof: Suppose $a \in Z(G) \Rightarrow ax = xa \ \forall x \in G \Rightarrow x \in N(a) \ \forall x \in G \Rightarrow G \subseteq N(a)$. But $N(a) \subseteq G$. $\therefore N(a) = G$. Conversely suppose $N(a) = G \Rightarrow x \in N(a) \ \forall x \in G \Rightarrow ax = xa \ \forall x \in G \Rightarrow a \in Z(G)$. If G is finite, and $a \in Z \Leftrightarrow N(a) = G \Leftrightarrow O(N(a)) = O(G)$.

Theorem 2.14 ***Application-1:** If $O(G) = p^n$, where p is a prime number then centre of $G, Z(G) \neq \{e\}$. [Z is non-trival]*
Proof: If $a \in G$, Since $N(a)$ is a subgroup of G by Lagrange's theorem $\frac{O(N(a))}{O(G)} = p^n \Rightarrow O(N(a))/p^n$. Let $O(N(a))/p^{n\alpha}$, $n\alpha \leq n$. $a \in Z(G) \Leftrightarrow O(G) = O(N(a)) \Leftrightarrow p^n = p^{n\alpha} \Leftrightarrow n = n\alpha$. By class equation, $O(G) = \sum \frac{O(G)}{O(N(a))}$, where the sum runs over the set of elements $a \in G$. Using one a, from each conjugate class.

$$\begin{aligned}
O(G) &= \sum_{a \in Z(G)} \frac{O(G)}{O(N(a))} + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))} \\
&= \sum_{O(N(a)) = O(G)} \frac{O(G)}{O(N(a))} + \sum_{O(N(a)) \neq O(G)} \frac{O(G)}{O(N(a))} \\
&= \sum_{a \in Z} \frac{O(G)}{O(G)} + \sum_{O(N(a)) \neq O(G)} \frac{O(G)}{O(N(a))} \\
&= \sum_{a \in G} 1 + \sum_{O(N(a)) \neq O(G)} \frac{O(G)}{O(N(a))} \\
&= O(Z) + \sum_{O(N(a)) \neq O(G)} \frac{O(G)}{O(N(a))}
\end{aligned}$$

Let O(Z) = Z.

$$\begin{aligned} O(G) &= Z + \sum_{n \neq n_\alpha} \frac{O(G)}{O(N(a))} \\ &= Z + \sum_{n \neq n_\alpha} \frac{p^n}{p^{n_\alpha}} \\ &= Z + \sum_{n \neq n_\alpha} p^{n-n_\alpha} \end{aligned}$$

$$\therefore p^n = Z + \sum_{n_\alpha < n} p^k, k = n - n_\alpha > 0 \text{.....(1)}$$

$$Since\ p/p^n\ and\ p/\sum_{n_\alpha < n} p^k,$$

$$from\ (1)\ p/(p^n - \sum_{n_\alpha < n} p^k) \Rightarrow p/Z \Rightarrow p/O(Z)$$

$\because e \in Z, O(Z) \neq op/O(Z), O(Z) \neq 0$ and p is prime. $\therefore O(Z) > 1$. $\therefore Z(G) \neq \{e\}$. Hence, Z is non-trivial and the theorem.

Corollary 2.15 *If $O(G) = p^2$ where p is a prime number, then G is abelian.*
Proof: Suppose $O(G) = p^2$, to prove G is abelian, it is enough to prove that $Z(G) = G$. Since $O(G) = p^2$, by previous theorem $Z(G) \neq \{e\}$. Since $Z(G)$ is a subgroup of G, by Lagrange's theorem, $\frac{O(Z(G))}{O(G)} = p^2 \Rightarrow O(Z(G))/p^2 \Rightarrow O(Z(G)) = 1$ (or) p (or) p^2.
Case(i): $O(Z(G)) \neq 1$[$\because Z(G)$ is non-trival].
Case(ii): $O(Z(G)) = p^2 = O(G) \Rightarrow O(Z(G)) = O(G) \Rightarrow Z(G) = G \Rightarrow G$ is abelian.
Case(iii) Suppose, $O(Z(G)) = p$. Claim that there is an element $a \in G$ such that $a \notin Z$. Suppose not,(i.e.) if $a \in Z \Rightarrow O(N(a)) = O(G)$ (by Lemma 2.13). By class equation,

$$O(G) = \sum_{a \in Z} \frac{O(G)}{O(N(a))} = \sum_{O(N(a)) = O(G)} \frac{O(G)}{O(N(a))} = \sum_{a \in Z} 1$$

$\therefore O(G) = O(Z) \Rightarrow O(G) = p \Rightarrow\Leftarrow$ to the fact $O(G) = p^2$. Hence the claim, there is an element $a \in G$ such that $a \notin Z$. Consider the subgroup $N(a)$ in G, then $Z(G) \subset N(a) \subset G$ [$\because a \in N(a)$ and $a \notin Z$]. $\therefore O(N(a)) > O(Z(G)) = p$ .....(2)
By Lagrange's theorem $\frac{O(N(a))}{O(G)} = p^2 \Rightarrow O(N(a))/p^2$.....(3)
$\Rightarrow O(N(a)) = p^2$ [by (2) and (3)] $\Rightarrow O(N(a)) = p^2 = O(G) \Rightarrow O(N(a)) = O(G) \Rightarrow N(a) = G \Rightarrow a \in Z \Rightarrow\Leftarrow$ to $a \notin Z$ $\therefore O(Z(G)) \neq p$. $\therefore$ The only possibility of $O(Z(G)) = p^2 = O(G) \Rightarrow Z(G) = G$. Hence, G is abelian.

Theorem 2.16 ***Application-2: CAUCHY'S THEOREM*** *If p is a prime number and $p/O(G)$, then G has an element of order p.*

Proof: We have to find an element $a \neq e \in G$ such that it satisfier $a^p = e$. We prove this theorem by induction on $O(G)$. The result is clearly true for a group of order 1. We assume that the theorem is true, for all groups T such that $O(T) < O(G)$. Now, we have to prove the theorem for G.

Case(i): Suppose W be any subgroup of $G, W \neq G.$ such that $p/O(W)$ [p divides the order of any non-trivial subgroup of G]. $\therefore O(W) < O(G)$. By induction hypothesis, the theorem is true for W, then there exists an element $a \in W, a \neq e$ such that $a^p = e \Rightarrow a \neq e, a \in G$, such that $a^p = e$ ($\because a \in W \subset G$). $\therefore G$ has an element of order p.

Case(ii): Suppose we assume that p does not divide order of any proper subgroup of G. In particular, if $a \notin Z$ then $N(a) \neq G$ (by Lemma 2.13). (i.e.) $N(a)$ is a proper subgroup of G if $a \notin Z(a)$. By assumption p does not divide $O(N(a))$. Consider the class equation of G,

$$\begin{aligned} O(G) &= \sum \frac{O(G)}{O(N(a))} \\ &= \sum_{N(a)=G} \frac{O(G)}{O(N(a))} + \sum_{N(a)\neq G} \frac{O(G)}{O(N(a))} \\ &= \sum_{a\in G} \frac{O(G)}{O(N(a))} + \sum_{N(a)\neq Z(G)} \frac{O(G)}{O(N(a))} \\ &= \sum_{a\in G} 1 + \sum_{N(a)\neq Z(G)} \frac{O(G)}{O(N(a))} \\ &= O(Z(G)) + \sum_{N(a)\neq G} \frac{O(G)}{O(N(a))} \text{.....(1)} \end{aligned}$$

Since $p/O(G)$ and p does not divide $O(N(a)), p/\frac{O(G)}{O(N(a))}$

$$\Rightarrow \sum_{N(a)\neq G} \frac{O(G)}{O(N(a))}$$

Thus $p/O(G)$ and

$$\sum_{N(a)\neq G} \frac{O(G)}{O(N(a))}$$

$\Rightarrow p/O(Z(G))$ [from(1)], where $Z(G)$ is a proper subgroup of G. But we have assumed that p does not divide any proper subgroup of G. $\therefore Z(G)$ cannot be a proper subgroup of G. $\therefore Z(G) = G \Rightarrow G$ is abelian. Thus $p/O(G)$ and G is abelian. $\therefore$ By Cauchy's theorem for abelian group, there exists $a \neq e, a \in G$ such that $a^p = e$

Theorem 2.17 ***Sylow's Theorem for arbitrary groups:*** *If $p^m/O(G)$, p^{m+1} does not divides $O(G)$, then G has a subgroup of order p^m, where p is a prime number.*

Proof: We prove this theorem by induction on $O(G)$. If $O(G) = 1$, the theorem is vacuously true. If $O(G) = 2$, the theorem only relevant prime number is 2. $2^1/O(G), 2^2$ does not divides $O(G)$. Certainly G has a subgroup of order 2 namely itself. The result is true if $O(G) = 2$. Suppose, we assume that the theorem is true for all groups of order less than $O(G)$. We want to show that the result is true for group G. Suppose assume that $p^m/O(G)$, p^{m+1} does not divides $O(G)$, where p is a prime number, $m \geq 1$.
Case(i): Suppose there exists a proper subgroup $H(G)$ such that $p^m/O(H)$. $\because H$ is a proper subgroup of $G, O(H) < O(G)$. $\therefore$ By induction hypothesis, H would have a subgroup T of order p^m. Since T is a subgroup of H and H is a subgroup of G, T is a subgroup of G of order p^m.
Case(ii): Suppose we assume that p^m does not divides $O(H)$ for any subgroup $H(G)$ and $H \neq G$. [(i.e.) p^m does not divide any proper subgroup of $O(G)$]. If $a \in G$, then $N(a) = \{x \in G | ax = xa\}$ is a subgroup of G. If $a \notin Z(G)$ then $N(a) \neq G$. (i.e.) $N(a)$ is a proper subgroup of G. $\therefore$ By our assumption p^m does not divides $O(N(a))$. Consider the class equation, $O(G) = \sum C_a$, where the sum runs over one element a for each conjugate class.

$$\begin{aligned}
\Rightarrow O(G) &= \sum \frac{O(G)}{O(N(a))} \\
&= \sum_{a \in Z} \frac{O(G)}{O(N(a))} + \sum_{a \notin Z} \frac{O(G)}{O(N(a))} \\
&= \sum_{a \in Z} \frac{O(G)}{O(G)} + \sum_{a \notin Z} \frac{O(G)}{O(N(a))}
\end{aligned}$$

[$\because$ if $a \in Z \Rightarrow O(N(a)) = O(G)$]

$$\begin{aligned}
&= \sum_{a \in Z} 1 + \sum_{a \notin Z} \frac{O(G)}{O(N(a))} \\
&\Rightarrow O(G) = O(Z) + \sum_{a \notin Z} \frac{O(G)}{O(N(a))} \text{.....(1)}
\end{aligned}$$

Since $p^m/O(G)$ and p^m does not divides $O(N(a))$ we have $p^m/\frac{O(G)}{O(N(a))}$

$$\begin{aligned}
&\Rightarrow p^m / \sum_{a \notin Z} \frac{O(G)}{O(N(a))} \\
&\Rightarrow p^m / (O(G) - \sum_{a \notin Z} \frac{O(G)}{O(N(a))}) \\
&\Rightarrow p^m / O(Z).
\end{aligned}$$

Since $p^m/O(Z)$ by Cauchy's theorem, Z has an element $b \neq e$ such that $b^p = e$. B is a subgroup of G of order p. $\therefore B$ is normal in G [$\because$ Every subgroup of an abelian group is normal]. We can form he quotient group $\bar{G}, \bar{G} = G/B = \{Bx | x \in G\}$. Now, $O(\bar{G}) = O(G/B) = \frac{O(G)}{O(B)} = \frac{O(G)}{p} < O(G)$. Also, $p^{m-1}/O(G/B) = O(\bar{G})$ [$\because p^m/O(G) \Rightarrow O(G) = tp^m$,some integer t]. Now $O(\bar{G}) = \frac{O(G)}{O(B)} = \frac{tp^m}{p} = tp^{m-1} \Rightarrow p^{m-1}/O(\bar{G})$. Also, p^m does not divides $O(\bar{G})$ and $O(\bar{G}) < O(G)$ [$p^{m-1}/O(\bar{G})$ and p^m does not divides $O(\bar{G})$]. $\therefore$ By induction hypothesis $(\bar{G})$ has a subgroup $\bar{P}$ of order p^{m-1}. Let $P = \{x \in G | xB \in \bar{P}\}$, then P is a subgroup of G by fundamental theorem of homomorphism, $\bar{P} \cong P/B$. $\therefore p^{m-1} = O(\bar{P}) = \frac{O(P)}{O(B)} = \frac{O(P)}{p} \Rightarrow O(P) = p^m$. Thus P is a required p-Sylow subgroup of G of order p^m. Hence the theorem.

Direct Product:

Definition 2.18 ***External Direct Product:*** *Let A and B be any two groups.Consider the cartesian product of A and $B, G = A \times B = \{(a, b) | a \in A, b \in B\}$. Let $x = (a_1, b_1)/a_1 \in A, b_1 \in B$; $y = (a_2, b_2)/a_2 \in A, b_2 \in B$. Define $x \cdot y = (a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2)$.*

Result 2.19 *Under this operation $(\cdot), G$ is a group and this group G is called external direct product of A and B.*
Proof: (i) $(\cdot)$ is closed: Let $x = (a_1, b_1) \in G, y = (a_2, b_2) \in G$. Now, $x \cdot y = (a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2) \in G$ ($\because a_1a_2 \in A, b_1b_2 \in B$). $\therefore (\cdot)$ is closed
(ii) $(\cdot)$ is associative: Let $x = (a_1, b_1) \in G, y = (a_2, b_2) \in G$ and $z = (a_3, b_3) \in G$. Then $x \cdot (y \cdot z) = (a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] = (a_1, b_1) \cdot [(a_2b_2), (a_3b_3)] = (a_1 \cdot (a_2a_3), b_1 \cdot (b_2b_3)) = ((a_1a_2) \cdot a_3, (b_1b_2) \cdot b_3) = (a_1a_2, b_1(b_2) \cdot (a_3, b_3)) = (x \cdot y) \cdot z \ \forall x, y, z \in G$. $\therefore (\cdot)$ is associative.
(iii) Existence of identity: Consider $e = (e_1, e_2)$, where e_1 is the identity element in A and e_2 is the identity element in B. Now, $x \cdot e = (a_1, b_1) \cdot (e_1, e_2) = (a_1 \cdot e_1, b_1 \cdot e_2) = (a_1, b_1) = x$ and $e \cdot x = x \ \forall x \in G$. $\therefore e = (e_1, e_2)$ act as a identity element of G.
(iv)Existence of inverse: let $x = (a_1, b_1) \in G$; $x^{-1} = (a_1^{-1}, b_1^{-1}) \in G$, where $a_1^{-1} \in A, b_1^{-1} \in B$. Now, $x \cdot x^{-1} = (a_1, b_1) \cdot (a_1^{-1}, b_1^{-1}) = (a_1a_1^{-1}, b_1b_1^{-1}) = (e_1, e_2) \in G$, where e_1 is the identity element in A and e_2 is the identity element in B. $\therefore x \cdot x^{-1} = e$. $\therefore (a_1^{-1}, b_1^{-1})$ acts as the inverse of G.
$\therefore G$ is a group.

Definition 2.20 *Let $G_1, G_2, G_3 ... G_n$ be the n groups. Let $G = G_1 \times G_2 \times G_3 \times ... \times G_n = \{(g_1, g_2 ... g_n)/g_1 \in G_1, g_2 \in G_2 ... g_n \in G_n)\}$. Let $x = (g_1, g_2 ... g_n) \in G$; $y = (g_1', g_2' ... g_n') \in G$. Define $x \cdot y = (g_1, g_2 ... g_n) \cdot (g_1', g_2' ... g_n') = (g_1g_1' ... g_ng_n')$. Under this operation, G is a group and we called G as an external direct product of the group $G_1, G_2, G_3 ... G_n$*

Internal Direct Product: Let A and B be any two groups. Consider $G = A \times B$ and $\bar{A} = \{(a, f) \in G | a \in A, f$ is the identity element in $B\}$; $\bar{B} = \{(b, f) \in G | a \in B, e$ is the identity element in $A\}$. Clearly $\bar{A}$ and $\bar{B}$ are the subgroups of G. Define a map $\phi : A \to \bar{A}$ by $\phi(a) = (a, f), a \in A$. Suppose $\phi(a) = \phi(a) \Rightarrow (a, f) = (b, f) \Rightarrow a = b$. $\therefore \phi$ is $1 - 1$. $\phi(ab) = (ab, f) = (a, f) \cdot (b, f) = \phi(a) \cdot \phi(b)$. $\therefore \phi$ is a homomorphism. Let $(a, f) \in \bar{A}$ then there exists an element $a \in A$ such that $\phi(a) = (a, f)$. $\therefore \phi$ is onto. $\therefore \phi$ is an isomorphism of A onto $\bar{A}$. (i.e.) $A \cong \bar{A}$. Similarly Define $\psi : B \to \bar{B}$ by $\psi(b) = (e, b)$. Then ψ is a homomorphism of B onto $\bar{B}$. $\therefore B \cong \bar{B}$. To prove: $\bar{A}$ and $\bar{B}$ are normal subgroups of G. Let $x = (a_1, b_1) \in G$ where $a_1 \in A, b_1 \in B$; $x^{-1} = (a_1^{-1}, b_1^{-1}) \in G$ where $a_1^{-1} \in A, b_1^{-1} \in B$. Let $n = (a, f) \in \bar{A}$. Now,

$$\begin{aligned} xnx^{-1} &= (a_1, b_1)(a, f)(a_1^{-1}, b_1^{-1}) \\ &= (a_1 a, b_1 f)(a_1^{-1}, b_1^{-1}) \\ &= (a_1 a a_1^{-1}, b_1 f b_1^{-1})) \\ &= (a_1 a a_1^{-1}, b_1 b_1^{-1} f) \\ &= (a_1 a a_1^{-1}, f) \in \bar{A} \ [\because a_1 a a_1^{-1} \in A \text{ and } f \text{ is identity in } B] \\ &\Rightarrow xnx^{-1} \in \bar{A}, \forall x \in G, n \in \bar{A}. \end{aligned}$$

$\therefore \bar{A}$ is a normal subgroup of G. Similarly we can prove that $\bar{B}$ is the normal subgroup of G. Claim that $G = \bar{A}\bar{B}$ and for every $g \in G$, has unique decomposition in the form $g = \bar{a}\bar{b}; \bar{a} \in \bar{A}, \bar{b} \in \bar{B}$. Let $g \in G = A \times B = \{(a, b) | a \in A, b \in B\}$; $g = (a, b) = (a, f)(e, f) \Rightarrow g = \bar{a}\bar{b}, \bar{a} = (a, f) \in \bar{A}$; $\bar{b} = (e, b) \in \bar{B}$.
Uniqueness: Let $g \in G$ can be written as $g = \bar{x}\bar{y}, \bar{x} \in \bar{A}, \bar{y} \in \bar{B}, \bar{x} = (x, f), x \in A, f$ is the identity element in B and $\bar{y} = (e, y), y \in B, e$ is the identity element in A. $g = \bar{x}\bar{y} = (x, f)(e, y) = (x, y)$, but $g = (a, b)$. $\therefore (a, b) = (x, y) \Rightarrow a = x$ and $b = y$. $\therefore \bar{x} = (x, f) = (a, f) = \bar{a}$ and $\bar{y} = (e, y) = (e, b) = \bar{b}$. $\therefore g \in G$ can be uniquely written as $g = \bar{a} \cdot \bar{b}, \bar{a} \in \bar{A}, \bar{b} \in \bar{B}$. Since $g \in G$ is arbitrary chosen $G = \bar{A}\bar{B}$ is called the internal direct product of the group $\bar{A}$ and $\bar{B}$.

Definition 2.21 *Let G be a group and $\bar{A}, \bar{B}$ be a normal subgroup of G and $\bar{A} \cong A$ and $\bar{B} \cong B$ in such a way $g \in G$ has a unique representation of the form $g = \bar{a}\bar{b}, \bar{a} \in \bar{A}, \bar{b} \in \bar{B}$. Then G is called the internal direct product of $\bar{A}$ and $\bar{B}$*

Definition 2.22 *Let G be a group and $N_1, N_2, ..., N_n$ be normal subgroups of G such that*
(i) $G = N_1 N_2 \cdots N_n$
(ii) Given $g \in G$ then $g = m_1 m_2 \cdots m_n$, $m_i \in N_i$ is a unique representation. Then G is called the internal direct product of the groups $N_1, N_2, ..., N_n$.

Lemma 2.23 *Suppose G is the internal product of $N_1, N_2, ..., N_n$. Then for $i \neq j, N_i \cap N_j = \{e\}$ and if $a \in N_i, b \in N_j$ then $ab = ba$*
Proof: Let $x \in N_i \cap N_j \Rightarrow x \in N_i$ and $x \in N_j$. When $x \in N_i, x = e_1e_2 \cdots e_{i-1}xe_{i+1} \cdots e_n$ .....(1)
Here $e_1 = e_2 = ... = e_{i-1} = e_{i+1} = ... = e_n = e \in N_i$ where $e_i \in N_i, i = 1, 2, ..., n$ and $i \neq j$. Similarly $x \in N_j$ then, $x = e_1e_2 \cdots e_{i-1}e_ie_{i+1} \cdots e_{j-1}xe_{j+1} \cdots e_n$ .....(2)
Here $e_1 = e_2 = ... = e_{i-1} = e_{i+1} = ... = e_{j-1} = e_{j+1} = ... = e_n = e$. Since any element in G, in particular x has unique representation of the form $m_1m_2 \cdots m_n$ where $m_i \in N_i$. $\therefore$ The two composition [i.e.(1) and (2)] in this form of x must coincide and the entry from N_i in each must be equal. $e_1e_2 \cdots e_{i-1}xe_{i+1} \cdots e_n = e_1e_2 \cdots e_{i-1}e_ie_{i+1} \cdots e_{j-1}xe_{j+1} \cdots e_n$ for each $e_i = e \; \forall i$. $\therefore x = e$. $\therefore N_i \cap N_j = \{e\} \; \forall i \neq j$. To prove $ab = ba$, $\forall a \in N_i, b \in N_j$, it is enough to prove that $aba^{-1}b^{-1} \in N_i \cap N_j$. Let $a \in N_i \Rightarrow a^{-1} \in N_i$ and $b \in N_j \Rightarrow b \in G$ and $b^{-1} \in G$. (i.e.) $b \in G, a^{-1} \in N_i$. Since N_i is normal in G, $ba^{-1}b^{-1} \in N_i$ and $a \in N_i \Rightarrow aba^{-1}b^{-1} \in N_i$ .....(1)
Since $b \in N_j, b^{-1} \in N_j$. $a \in N_i \Rightarrow a \in G, a^{-1} \in G$. (i.e.) $a \in G, b^{-1} \in N_j$. Since N_j is normal in $G, ab^{-1}a^{-1} \in N_j$ and $b^{-1} \in N_j \Rightarrow aba^{-1}b^{-1} \in N_j$ .....(2)
From (1) and (2), $aba^{-1}b^{-1} \in N_i \cap N_j = \{e\} \Rightarrow aba^{-1}b^{-1} = e \Rightarrow ab = ba \; \forall a \in N_i, b \in N_j$

Remark 2.24 *Converse of the above lemma is not true.*

Theorem 2.25 *Let G be a group and suppose that G is the internal product of $N_1, N_2, ...N_n$. Let $T = N_1 \times N_2 \times \cdots \times N_n$. Then G and T are isomorphic.*
Proof: Suppose G is the internal direct product of $N_1, N_2, ..., N_n$. Let $x \in G$. Then x can be unique expressed as $x = a_1a_2 \cdots a_n, a_i \in N_i$. Define a map $\psi : T \to G$ by $\psi(a_1, a_2, ..., a_n) = a_1a_2 \cdots a_n$ where each $a_i \in N_i, i = 1, 2, ..., n$. Let $x = (a_1, a_2, ..., a_n), y = (b_1, b_2, ..., b_n)$. Suppose $\psi(x) = \psi(y) \Rightarrow (a_1 \cdot a_2 \cdots a_n), y = (b_1 \cdot b_2 \cdots b_n) \Rightarrow a_1 = b_1, a_2 = b_2, ..., a_n = b_n$ (By the uniqueness of the internal direct products) $\Rightarrow (a_1, a_2, ..., a_n) = (b_1, b_2, ..., b_n) \Rightarrow x = y$. $\therefore \psi$ is $1-1$. Since G is the internal direct products of $N_1, N_2, ..., N_n$ if $x \in G$, then $x = (a_1, a_2, ..., a_n)$ for $a_i \in N_i, a_2 \in N_2, ..., a_n \in N_n$. But then $\psi(a_1, a_2, ..., a_n) = a_1 \cdot a_2 \cdots a_n = x$. $\therefore \psi$ is onto. Now, $\psi(x \; y) = \psi((a_1, a_2, ..., a_n) \; (b_1, b_2, ..., b_n)) = \psi(a_1b_1, a_2b_2, ..., a_nb_n) = a_1b_1 \cdot a_2b_2 \cdots a_nb_n = a_1 \cdot a_2 \cdots a_n \cdot b_1 \cdot b_2 \cdots b_n$ [By lemma 2.23 $a_jb_j = b_ja_i$ for $i \neq j a_1b_1 \cdot a_2b_2 \cdots a_nb_n = a_1 \cdot a_2 \cdots a_n \cdot b_1 \cdot b_2 \cdots b_n$] $= \psi(a_1, a_2, ..., a_n)\psi(b_1, b_2, ..., b_n) = \psi(x) \cdot \psi(y)$. $\therefore \psi$ is a homomorphism. $\therefore \psi$ is an isomorphism. $\therefore G \cong T$.

3. UNIT III

Rings

Definition 3.1 ***Associative ring:*** *A non-empty set R is said to be an associative ring, If in R, there are defined two operations, denoted by $+$ and $\cdot$ respectively, such that $\forall a, b, c \in R$*

1. $a + b \in R$
2. $a + b = b + a$
3. $a + (b + c) = (a + b) + c$
4. *There is an element* 0 *in* $R \ni$: $a + 0 = a \forall a \in R$
5. *There is an element* $-a$ *in* $R \ni$: $a + (-a) = 0$
6. $a \cdot b \in R$
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
8. $a \cdot (b + c) = a \cdot b + a \cdot c$
9. $(b + c) \cdot a = b \cdot a + c \cdot a$

Example 3.2 *R is the set of all integers, positive, negative, zero; $(+)$ is the usual addition and $(\cdot)$ is the usual multiplication of integers $(R, +, \cdot)$is a ring.*

Definition 3.3 *If there is an element $1 \in R \ \ni$: $a \cdot 1 = 1 \cdot a = a, \forall a \in R$ then we say that R is a ring with unit element. If $a \cdot b = b \cdot a \ \forall a, b \in R$ then we call R is a commutative ring.*

Example 3.4 *$(\mathbb{J}, +, \cdot)$ is a commutative ring with unit element*

Example 3.5 *$(2\mathbb{J}, +, \cdot)$ is a commutative ring but it has no unit element. $(2Z, \oplus, \odot)$ is a commutative ring with unit element*

Definition 3.6 *A commutative ring R with unit element in which every non-zero elements has a multiplicative inverse is called a field.*

Example 3.7 *$(\mathbb{J}_7, \oplus, \odot)$ is a field and it is finite hence $(\mathbb{J}_7, \oplus, \odot)$ is a finite field. $(\mathbb{J}_6, \oplus, \odot)$ is a ring. Here $\bar{2} \cdot \bar{3} = 0$, yet $\bar{2} \neq 0$ and $\bar{3} \neq 0$. Thus it is*

possible in a ring R, that $a \cdot b$ with neither $a = 0$ nor $b = 0$. This cannot happen in a field. This is an example for a ring R which is not a field. Let

$R = \{\alpha_{11}e_{11} + \alpha_{12}e_{12} + \alpha_{21}e_{21} + \alpha_{22}e_{22} =$

$\sum_{i,j=1}^{2} \alpha_{ij}e_{ij}$ *where* α_{ij} *are rational numbers (i.e.)* $\alpha_{ij} \in \mathbb{Q}\}$.

$X = Y = \sum_{i,j=1}^{2} \alpha_{ij}e_{ij} = \sum_{i,j=1}^{2} \beta_{ij}e_{ij} \Leftrightarrow \alpha_{ij} = \beta_{ij}\ \forall i, j = 1, 2.$

$X + Y = \sum_{i,j=1}^{2} \alpha_{ij}e_{ij} + \sum_{i,j=1}^{2} \beta_{ij}e_{ij} = \sum_{i,j=1}^{2} (\alpha_{ij} + \beta_{ij})e_{ij}$

$X \cdot Y = (\sum_{i,j=1}^{2} \alpha_{ij}e_{ij})(\sum_{i,j=1}^{2} \beta_{ij}e_{ij}) = \sum_{i,j=1}^{2} \gamma_{ij}e_{ij}$

where $\gamma_{ij} = \sum_{i,j=1}^{2} \alpha_{ir}\beta_{rj} = \alpha_{i1}\beta_{1j} + \alpha_{i2}\beta_{2j}$ *and* $e_{ij} \cdot e_{ke} = 0$ *for* $j \neq k$

$e_{ij} \cdot e_{ke} = e_{ie}$ *for* $j = k$.

$a = e_{11} - e_{21} + e_{22} = 1 \cdot e_{11} + 0 \cdot e_{12} + (-1)e_{21} + 1 \cdot e_{22}$

$b = e_{22} + 3e_{12} = 0 \cdot e_{11} + 3 \cdot e_{12} + 0 \cdot e_{21} + 1 \cdot e_{22}$

$a \cdot b = (e_{11} + 0 \cdot e_{12} + (-1)e_{21} + e_{22})(0 \cdot e_{11} + 3 \cdot e_{12} + 0 \cdot e_{21} + 1 \cdot e_{22})$

$= 0 + 3 \cdot e_{12} + 0 + 0 + 0 + 0 + 0 + 0 + (-3)e_{22} + 0 + 0 + 0 + 0 + 0 + e_{22}$

$= 3 \cdot e_{12} - 3 \cdot e_{22} + e_{22} = 3 \cdot e_{12} - 2e_{22}$

$\therefore$ *R is a ring. It is called a ring of 2×2 rational matrices.*

Example 3.8 $\mathbb{C} = \alpha + i\beta, \alpha, \beta \in \mathbb{R}$. $(\mathbb{C}, +, \cdot)$ *is a field.*

Example 3.9 *Let* $Q = \{\alpha_0 + \alpha_1\vec{i} + \alpha_2\vec{j} + \alpha_3\vec{k}/\alpha_0, \alpha_1, \alpha_2\alpha_3 \in \mathbb{R}\}$ *and* $X = \alpha_0 + \alpha_1\vec{i} + \alpha_2\vec{j} + \alpha_3\vec{k}$; $Y = \beta_0 + \beta_1\vec{i} + \beta_2\vec{j} + \beta_3\vec{k}$. $X = Y \Leftrightarrow \alpha_i = \beta_i\ \forall i = 0, 1, 2, 3$. *Define*

$$\begin{aligned} X + Y &= (\alpha_0 + \alpha_1\vec{i} + \alpha_2\vec{j} + \alpha_3\vec{k}) + (\beta_0 + \beta_1\vec{i} + \beta_2\vec{j} + \beta_3\vec{k}) \\ &= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)\vec{i} + (\alpha_2 + \beta_2)\vec{j} + (\alpha_3 + \beta_3)\vec{k} \end{aligned}$$

$$\begin{aligned} X \cdot Y &= (\alpha_0 + \alpha_1\vec{i} + \alpha_2\vec{j} + \alpha_3\vec{k})(\beta_0 + \beta_1\vec{i} + \beta_2\vec{j} + \beta_3\vec{k}) \\ &= \alpha_0\beta_0 + \alpha_0\beta_1\vec{i} + \alpha_0\beta_2\vec{j} + \alpha_0\beta_3\vec{k} + \alpha_1\beta_0\vec{i} - \alpha_1\beta_1 + \alpha_1\beta_2\vec{k} \\ &\quad + \alpha_1\beta_3(-\vec{j}) + \alpha_2\beta_0\vec{j} + \alpha_2\beta_1(-\vec{k}) - \alpha_2\beta_2 + \alpha_2\beta_3\vec{i} + \alpha_3\beta_0\vec{k} \\ &\quad + \alpha_3\beta_1\vec{j} + \alpha_3\beta_2(-\vec{i}) + \alpha_3\beta_3(-1) \\ &= (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)\vec{i} \\ &\quad + (\alpha_0\beta_2 + \alpha_2\beta_0 - \alpha_1\beta_3 + \alpha_3\beta_1)\vec{j} + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)\vec{k} \end{aligned}$$

It is a non-commutative ring (i.e) $(R, +, \cdot)$ *with multiplicative unit element is called a Ring of Real Quaternions.*

Some special classes of Ring: If R is a commutative ring, then $a \neq 0 \in R$ is said to be a zero divisor, if there exists an element $b \in R, b \neq 0 \ni: ab = 0$.

Example 3.10 *In* $(\mathbb{Z}_6, \oplus, \odot), \bar{2}$ *is a zero divisor because* $\bar{3} = 0$ *such that* $\bar{2} \cdot \bar{3} = 0$. *Also,* $\bar{3}$ *is also a zero divisor.*

Definition 3.11 *A commutation ring is an Integral Domain if it has no zero divisor.*

Example 3.12 $(\mathbb{Z}, +, \cdot)$ *us a commutation ring and it has no zero divisor.*

Definition 3.13 *A ring is said to be divison ring if its non-zero elements form a group under multiplication.*

Example 3.14 $(\mathbb{R}, +, \cdot)$ *is a division ring.*

Definition 3.15 *A field is a commutative division ring.*

Example 3.16 $(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{J}_7, \oplus, \odot)$

Lemma 3.17 *If* R *is a ring, then* $\forall a, b \in R$

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a) \cdot b = -ab$
3. $-a \times -b = +ab$
4. *If in addition,* R *has unit element* 1, *then* $(-1)a = a$
5. $(-1)(-1) = 1$

Homomorphism

Definition 3.18 *A mapping* ϕ *from the ring* R *into the ring* R *is said to a homomorphism if,*

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a) \cdot \phi(b)\ \forall a, b \in R$

Example 3.19 *Let* R' *and* R' *be any two rings. Define* $\phi : R \to R'$ *by* $\phi(a) = 0', \forall a \in R, 0'$ *is the identity element in* R' *is clearly a homomorphism and is called a trivial homomorphism. Define* $\phi : R \to R'$ *by* $\phi(a) = a, \forall a \in R$ *is also a homomorphism.*

Lemma 3.20 *If ϕ is a homomorphism of R into R' then*

1. $\phi(0) = 0$
2. $\phi(-a) = -\phi(a)\ \forall a \in R$

Remark 3.21 *It need not be true that $\phi(1) = 1'$ where 1 and $1'$ are unit elements of R and R' respectively. However if R' is an integral domain (or) if R' is an arbitrary but ϕ is onto then $\phi(1) = 1'$.*

Definition 3.22 ***Kernal of a homomorphism:*** *If ϕ is a homomorphism of R into R', then the kernal of ϕ devoted by $I(\phi)$ is defined as, $I(\phi) = \{a \in R | \phi(a) = 0', 0'$ is the identity in $R'\}$. $I(\phi)$ is a subset of R.*

Example 3.23 *(i) $\phi : R \to R'$, defined by $\phi(a) = 0'\ \forall a \in R$. Then $I(\phi) = \{a \in R | \phi(a) = 0'\} = R$.*
(ii)$\phi' : R \to R$, by $\phi(a) = a\ \forall a \in R$. Then $I(\phi) = \{a \in R | \phi(a) = 0', 0'$ is identity in $R\} = \{0\}$

Lemma 3.24 *If ϕ is a homomorphism of R into R' with kernal $I(\phi)$, then*

1. *$I(\phi)$ is a subgroup of R under addition,*
2. *If $a \in I(\phi)$ and $r \in R$ there both ar and ra are in $I(\phi)$.*

Example 3.25

1. *$J(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in J\}$ which is a ring under usual addition and multiplication. Define $\phi : J(\sqrt{2}) \to J(\sqrt{2})$ by $\phi(a + b\sqrt{2} = a - b\sqrt{2}$. Clearly, ϕ is a homomorphism. $I(\phi) = \{a \in R | \phi(a) = 0', 0'$ is the identity in $R'\} = \{0 + 0\sqrt{2}\} = \{0\}$.*
2. *Define $\phi : J \to J_n$ by $\phi(a) = r$ where $a = q^{n+r}, 0 \leq r < n$. Clearly,$\phi$ is a homomorphism of J onto J_n. $I(\phi) = \{a \in R | \phi(a) = 0', 0'$ is the identity in $R'\} = \{na / a \in J\}$.*
3. *Let $R = \{$continuous real valued function on close internal $[0, 1]\}$ under usual addition and multiplication of function. (i.e.) $R = \{f | f : [0, 1] \to R\}$. Let F be a ring of real numbers. Define $\phi : R \to F$ by $\phi(f(x)) = f(1/2)$. Then ϕ is a homomorphism of R onto F.*

Definition 3.26 *A homomorphism of R into R' is said to be an isomorphism if it is a $1 - 1$ mapping.*

Definition 3.27 *Two rings are said to be isomorphic if there is an isomorphism of one onto other.*

Lemma 3.28 *A homomorphism $\phi : R \to R'$ is an isomorphism iff $I(\phi) = \{0\}$*

Ideals and Quotient Rings

Definition 3.29 *A non-empty set U of a ring R is said to be a two sided ideal of R if*

1. *U is a subgroup of R with respect to addition,*
2. *For every, $u \in U, r \in R$ both ru and $ur \in U$.*

Example 3.30 *$(2J, +, \cdot)$ is ideal of $(J, +, \cdot)$.*

Example 3.31 *Let $\phi : R \to R'$ be a homomorphism then the kernal $I(\phi)$ is an ideal of R. Kernal of any homomorphism in a ring is an ideal of R.*

Definition 3.32 *Let U be an ideal of R, Define $R/U = \{a + U | a \in R\}$. Define $+$ and $\cdot$ as follows, let $X = a + U \in R/U$; $Y = b + U \in R/U$. Then $X + Y = (a + b) + U$ and $X \cdot Y = ab + U$. Under this operation $+$ and $\cdot$, R/U is a ring and this is called the quotient ring of R modulo U.*

Remark 3.33
1. *If R is commutative, then R/U is commutative. Converse need not be true.*
2. *If R is a ring with unit element, then R/U is also a ring with unit element.*

Lemma 3.34 *If U is an ideal of the ring R, then R/U is a ring and is a homomorphism image of R under the definition $\phi : R \to R/U$ by $\phi(a) = a + U, \ \forall a \in R$.*

Result 3.35
1. *If U is an ideal of R and $1 \in U$ then $U = R$.*
2. *If F is a field then its only ideals are $\{0\}$ and F itself.*

More Ideals and Quotient Rings:

Lemma 3.36 *Let R be a commutative ring with unit element whose only ideals are $\{0\}$ and R itself. Then R is a field*

Definition 3.37 *An ideal $M \neq R$ in a ring R is said to be a maximal ideal of R if whenever U is an ideal of R such that $M \subset U \subset R$ then either $M = U$ (or) $U = R$.*

Theorem 3.38 *If R is commutative ring and M is an ideal of R, then M is a maximal ideal of $R \Leftrightarrow R/M$ is a field.*

Example 3.39 *Let $R = J$ and U be an ideal of R. U consists of all multiples of a fixed integer $U = \{x | x = tn_0, n_0$ is fixed integer, $t \in J\} = (n_0)$. U is a maximal ideal of $R \Leftrightarrow n_0$ is prime $\Rightarrow U = (2), (3), (5)$ are maximal ideal in $(J, +, \cdot)$.*

Definition 3.40 *A ring R can be imbedded in a ring R' if there is an isomorphism R into R'. R' will be called an over ring (or) extension of R if R can be imbedded in R'.*

Field of Quotients of an Integral Domain

Theorem 3.41 *Every integral domain can be imbedded in a field*
Proof: This theorem can be proved in the following 4 steps,

1. Specify the elements of the field F.
2. Define $(+)$ and $(\cdot)$ in F.
3. Prove that F is a field.
4. D can be imbedded in F.

Step 1: Let D be an integral domain. Define $M = \{(a,b)|a,b \in D, b \neq 0\}$, where (a,b) represents the quotient elements a/b. In M, we define a relation $\sim$ as follows, $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Claim that $\sim$ is an equivalence relation
$\sim$ **is reflexive:**
Since $ab = ba, \forall a,b \in D[\because D$ is an integral domain and so it is a commutative ring$] \Rightarrow (a,b) \sim (a,b)\ \forall a,b \in M. \therefore \sim$ is reflexive.
$\sim$ **is symmetric:**
Let $(a,b) \sim (c,d) \Rightarrow ad = bc \Rightarrow da = cb \Rightarrow cb = da \Rightarrow (c,d) \sim (a,b). \therefore \sim$ is symmetric.
$\sim$ **is transitive:**
Let $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f) \Rightarrow ad = bc$ and $cf = de$. Now,

$$
\begin{aligned}
& cf = de \\
& \Rightarrow bcf = bde \\
& \Rightarrow adf = bde (\because bc = ad) \\
& \Rightarrow afd = bed \\
& \Rightarrow (af - be)d = 0 \\
& \Rightarrow af - be = 0 [\because d \neq 0 \text{ and } d, ad - bc \in D \text{ an integral domain}] \\
& \Rightarrow af = be \\
& \Rightarrow (a,b) \sim (e,f)
\end{aligned}
$$

$\therefore \sim$ is transitive. Hence, $\sim$ is an equivalence relation. Let $[a,b]$ be the equivalence class in M of (a,b). Let $F = \{[a,b]|(a,b) \in M, a,b \in D, b \neq 0\}$
Step 2:
Define $+$ and $\cdot$ in F as follows: Let $[a,b],[c,d] \in F$. Define $[a,b] + [c,d] = [ad + bc, bd]$ and $[a,b] \cdot [c,d] = [ac, bd]$.
Step 3:

+ 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)

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

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

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

$\therefore$ + 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:
$[a,b]+[c,d]=[ad+bc,bd]=[bc+ad,bd]=[cb+da,bd]=[c,d]+[a,b]$ $\forall[a,b]+[c,d]\in F$. $\therefore$ + is commutative.
$\therefore$ $(F,+)$ 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 $(ac)(b'd')=$

$(bd)(a'c')$. Now,

$$\begin{aligned}(ac)(b'd') &= acb'd' \\ &= ba'cd' \ [\because [a,b] = [a',b']] \\ &= ba'dc' \ [\because ab' = ba'] \\ &= (bd)(a'c') \ [\because [c,d] = [c',d'], cd' = dc'].\end{aligned}$$

$\therefore \cdot$ is well defined.

$\cdot$ **is closed:**

Let $[a,b],[c,d] \in F \ [b,d \in D, b \neq 0, d \neq 0 \therefore bd \neq 0]$. Now, $[a,b] \cdot [c,d] = [ac,bd] \in F[\because bd \neq 0]$. $\therefore \cdot$ is closed.

$\cdot$ **is associative:**

$$\begin{aligned}([a,b] \cdot [c,d]) \cdot (e,f) &= [(ac)e,(bd)f] \\ &= [a(ce),b(df)] \\ &= [a,b][ce,df] \\ &= [a,b]([c,d],[e,f])\end{aligned}$$

$\therefore \cdot$ is associative.

Existence of Multiplicative Identity:

Let $[a,a] \in F, a \neq 0$ be the multiplicative identity. For, $[a,b] \cdot [a,a] = [a^2,ab] = [a,b]$ and for,$[a,a] \cdot [a,b] = [a^2,ab] = [a,b]$. (i.e.) $[a,b] \cdot [a,a] = [a,a] \cdot [a,b] = [a,b]$.

Existence of Multiplicative inverse:

Let $[a,b] \in F, b \neq 0$. Then $[b,a] \in F, a \neq 0$ is the multiplicative inverse. For, $[a,b] \cdot [b,a] = [ab,ba] = [ab,ab] = [a,a] \ [\because (ab,ba) \sim (a,b)]$.

$\cdot$ **is commutative:**

Let $[a,b],[c,d] \in F$. $[a,b] \cdot [c,d] = [ac,bd] = [ca,db] = [c,d] \cdot [a,b]$. $\therefore \cdot$ is commutative.

$\therefore (F\backslash\{0\},\cdot)$ is abelian group.

$\cdot$ **is distributive over addition:**

$$\begin{aligned}[a,b] \cdot ([c,d] + [e,f]) &= [a,b] \cdot [cf + de, df] \\ &= [a(cf + de), b(df)] \\ &= [(acf + ade), bdf] \\ &= [(ac)f + (ae)d, (bd)f] \\ &= [(ac)(bf) + (ae)(bd), (bd)(bf)] \\ &= [ac,bd] + [ae,bf] \\ &= [a,b] \cdot [c,d] + [a,b] \cdot [e,f]\end{aligned}$$

and

$$\begin{aligned}([c,d]+[e,f])\cdot[a,b] &= [cf+de,df]\cdot[a,b]\\ &= [(cf+de)a,(df)b]\\ &= [cfa+dea,dfb]\\ &= [(ca)f+d(ea),d(fb)]\\ &= [(ca)(fb)+(db)(ea),(db)(fb)]\\ &= [ca,db]+[ea,fb]\\ &= [c,d]\cdot[a,b]+[e,f]\cdot[a,b].\end{aligned}$$

Hence F is a field.

Step 4:

We have to prove D can be imbedded in F. (i.e.) We shall find an isomorphism of $D \to F$. We first notice that $x \neq 0, y \neq 0$ in $D, [ax,x] = [ay,y]$ [$\because (ax,x) \sim (ay,y) \because axy = axy$]. Denote $[ax,x]$ by $[a,1]$. Define $\phi : D \to F$ by $\phi(a) = [a,1]\ \forall a$ in D.

ϕ is $1-1$:

Suppose $\phi(a) = \phi(b), a, b \in D$. $[a,1] = [b,1] \Rightarrow (a,1) \sim (b,1) \Rightarrow a \cdot 1 = b \cdot 1 \Rightarrow a = b$. $\therefore$ ϕ is $1-1$.

ϕ is homomorphism:

$\phi(a+b) = [a+b,1] = [a,1] + [b,1] = \phi(a) + \phi(b)$ and $\phi(ab) = [ab,1] = [a,1]\cdot[b,1] = \phi(a)\cdot\phi(b)$. $\therefore$ ϕ is an isomorphism of D into F. If D has the unit element 1, then $\phi(1)$ is the unit element of F. Hence D can be imbedded into F. Hence the theorem.

Note: Usually, the above field F is called field of quotients of D.

Polynomial Rings

Definition 3.42 *Let F be a field. The Ring of polynomials in the indeterminate x, written as $F(x)$, defined as $\{a_0 + a_1x + a_2x^2 + ... + a_nx^n\}$ where $n \in \mathbb{Z}^+ \cup \{0\}$ and the coefficient $a_0, a_1, a_2, ..., a_n$ are all in F. (i.e.) $F(x) = \{a_0 + a_1x + a_2x^2 + ... + a_nx^n | a_0, a_1, a_2, ..., a_n \in F, n \in \mathbb{Z}^+ \cup \{0\}\}$.*

Definition 3.43 *If $p(x) = a_0 + a_1x + a_2x^2 + ... + a_mx^m$ and $q(x) = b_0 + b_1x + ... + b_nx^n$ are in $F[x]$. Then,*

1. *$p(x) = q(x) \Leftrightarrow a_i = b_i \ \ \forall i \geq 0$,*
2. *$p(x) + q(x) = c_0 + c_1x + 2x^2 + ... + c_tx^t$ where $a_i + b_i = c_i \forall i$,*
3. *$p(x)\cdot q(x) = c_0 + c_1x + 2x^2 + ... + c_tx^t$ where $c_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + ... + a_0b_t$.*

Note 3.44 $c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0, c_2 = a_0b_2 + a_1b_1 + a_2b_2$.

Remark 3.45 *$F[x]$ is a commutative ring with unit element under addition and multiplication of polynomials defined above.*

Definition 3.46 ***Degree of a polynomial*** *If $f(x) = a_n x^n + .. + a_1 x + a_0 \neq 0$ in $F[x]$ and $a_n \neq 0$ ((i.e.) $a_i = 0\ \forall i \geq 0$), then degree of $f(x)$, denoted by $deg(f(x))$ is n. (i.e.) $deg(f(x))$ is the largest integer i for which i^{th} coefficient of $f(x) \neq 0$.*

Remark 3.47 *we do not define the degree of the zero polynomial. We say a polynomial is constant if its degree is zero.*

Lemma 3.48 *If $f(x)$ and $g(x)$ are non-zero elements of $F[x]$. Then degree of $deg(f(x)g(x)) = def(f(x)) + deg(g(x))$*
Proof: Let $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_m x^m, a_m \neq 0$ $[a_i = 0, \forall_i > m]$ in $F[x]$..... (1)
Let $g(x) = b_0 + b_1 x + ... + b_n x_n, b_n \neq 0$ $[b_j = 0 \forall j \geq n]$in $F(x)$.....(2)
Then $\deg(f(x)) = m$ and $\deg(g(x)) = n$. By definition, $f(x)g(x) = c_0 + c_1 x + c_2 x^2 + ... + c_k x^k$, where $c_t = a_t b_0 + a_{t-1} b_1 + ... + a_0 b_t$. Claim that $c_{m+n} \neq 0$ and $\forall i > m + n, c_i = 0$. Now, $c_{m+n} = a_{m+n} b_0 + a_{m+n-1} b_1 + a_{m+n-2} b_2 + ... + a_{m+2} b_{n-2} + a_{m+1} b_{n-1} + a_m b_n + a_{m-1} b_{n+1} + ... + a_0 b_{m+n} = a_m b_n \neq 0 \Rightarrow c_{m+n} \neq 0$..... (3)$[\because a_m \neq 0$ and $b_m \neq 0$ and $a_m b_m \in F]$.
For every $i > m+n \Rightarrow i-j+j > m+n \Rightarrow$ either $j > m$ (or) $i-j > n$. Then one of a_j or b_{i-j} is zero, so that $a_j b_{i-j} = 0 \Rightarrow c_i = a_i b_0 + a_{i-1} b_1 + ... + a_0 b_i = \sum a_j b_{i-j} = 0$. For every $i > m + n, c_i = 0$.....(4)
Hence the claim follows from (3) and (4). $\therefore$ $deg(f(x) \cdot g(x)) = m + n = deg(f(x)) + deg(g(x))$. Hence, the lemma.

Corollary 3.49 *(1) If $f(x)$ and $g(x)$ are non-zero elements in $F[x]$ then $deg(f(x)) \leq deg(f(x) \cdot g(x))$. By the above lemma, $deg(f(x) \cdot g(x)) = deg(f(x)) + deg(g(x)) \geq degf((x))[\because deg(g(x)) \geq 0]$.*
(2) $F[x]$ is integral domain.
Proof: Clearly $F[x]$ is a common ring with unit element. To prove $F[x]$ is an integral domain, it is enough to prove that $F[x]$ has no zero divisor, (i.e)product of any two non- zero elements in $F[x]$ is again a non-zero element in $F[x]$. Let $f(x) = a_0 + a_1 x + ... + a_m x^m, a_m \neq 0$ in $F[x]$ and $g(x) = b_0 + b_1 x + ... + b_n x^n, b_n \neq 0$ in $F[x]$. $\because a_m \neq 0, b_n \neq 0$ and a_m, b_n are in $F[x], a_m \cdot b_n \neq 0$. (i.e) the coefficient of x^{m+n} in $f(x) \cdot g(x)$ is non-zero. $\therefore$ $f(x) \cdot g(x) \neq 0$ in $F[x]$. Hence $F[x]$ is an integral domain.

Lemma 3.50 ***Existence of division algorithm in*** *$F[x]$: Given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$. Then there exists two polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x) \cdot g(x) + r(x)$, where either $r(x) = 0$ (or) $deg(r(x)) < deg(g(x))$.*
Proof: Let $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_m x^m, a_m \neq 0$ in $F[x]$ and $g(x) = b_0 + b_1 x + b_2 x^2 + ... + b_n x^n, b_n \neq 0$ in $F[x] \Rightarrow deg(f(x)) = m$ and

$deg(g(x)) = n$.
Case(i): If $m = 0$ (or) $m < n$, nothing to prove. For put $t(x) = 0$ and $r(x) = f(x)$, where $f(x)$, $deg(f(x)) < deg(g(x))$.
Case(ii): Assume that $m \geq n$. we shall prove the theorem by induction on degree of $f(x)$. If $m = 0$ and $n = 0 \Rightarrow f(x)$and $g(x)$are non-zero constant polynomial. Let $f(x) = a \neq 0, g(x) = b \neq 0, a, b \in F[x]$. Let $ab^{-1} = t(x)$. Now, $a = (ab^{-1})b \neq 0 \Rightarrow f(x) = t(x) \cdot g(x) + r(x)$, where $r(x) = 0$. $\therefore$ The result is true clearly. Assume that the result is true $\forall$ polynomial of degree $< m$. Consider the polynomial,

$$\begin{aligned} f_1(x) &= f(x) - a_m b_n^{-1} x^{m-1} g(x) \text{.....(1)} \\ &= a_0 + a_1 x + ... + a_m x^m - a_m b_n^{-1} x^{m-n}(b_0 + b_1 x + b_2 x^2 + ... + b_n x^n) \\ &= a_0 + a_1 x + ... + a_m x^m - a_m b_n^{-1} x^{m-n} b_0 - a_m b_n^{-1} x^{m-n} b_1 - .... - a_m x^m \\ &\Rightarrow deg(f_1(x)) \leq m - 1 < m \Rightarrow deg(f_1(x)) < m. \end{aligned}$$

$\therefore$ By induction hypothesis, there exists a polynomial $t_1(x), r(x) \in F[x]$ such that $f_1(x) = t_1(x)g(x) + r(x)$ where $r(x) = 0$ (or)deg $(r(x))$ <deg $(g(x))$. From (1),

$$\begin{aligned} f(x) &= f_1(x) + a_m b_n^{-1} x^{m-n} g(x) \\ &= t_1(x)g(x) + r(x) + a_m b_n^{-1} x^{m-n} g(x) \\ &= (t_1(x) + a_m b_n^{-1} x^{m-n}) g(x) + r(x), \end{aligned}$$

where $r(x) = 0$ (or) deg $r(x) <$ deg $g(x)$. This proves the existence of polynomial $t(x)$ and $r(x)$
To Prove: Uniqueness
Suppose, $f(x) = t_1(x)g(x)+r_1(x)$ and $f(x) = t(x)g(x)+r(x)$, where $r_1(x) = 0$ and $deg(r_1(x)) < deg(g(x)) \Rightarrow t_1(x)g(x) + r_1(x) = t(x)g(x) + r(x) \Rightarrow [t_1(x) - t(x)]g(x) = r(x) - r_1(x)$.....(2)
If $r(x) = 0$ and $r_1(x) = 0 \Rightarrow t(x) = t_1(x)$. If $deg(r(x)) < deg(g(x))$ and $deg(r_1(x)) < deg(g(x))$. Then (2) $\Rightarrow deg([t_1(x) - t(x)]g(x)) = deg(r(x) - r_1(x))$. This is possible only if $t_1(x) - t(x) = 0$. $\therefore$ $r_1(x) - r(x) = 0 \Rightarrow r(x) = r_1(x)$. Hence the uniqueness.

Theorem 3.51 *$F[x]$ is euclidean ring.*
Proof: $F[x]$ is an Integral Domain with unit element. Define a function d on a non-zero polynomial $f(x)$ in $F[x]$ as $d(f(x)) = deg(f(x))$. $\therefore$ $d(f(x)) \geq 0[\because deg(f(x) \geq 0]$. (i.e)$d(f(x))$ is non negative.....(1)
By Corollary 3.49, we have proved that if $g(x)$ and $f(x)$ are non-zero elements in $F[x]$, then $d(f(x)) \leq$ deg $(f(x) \cdot g(x))$. (i.e) $d(f(x)) \leq d(f(x) \cdot g(x))$.....(2)
By the above lemma, given two polynomials $f(x)$ and $g(x) \neq 0$ in $F[x]$, then there exists two polynomials $t(x)$ and $r(x)$ in $F[x], \ni$: $f(x) = t(x) \cdot g(x) + r(x)$, where $r(x) = 0$ (or) $deg(r(x)) < deg(g(x))$.....(3)
From (1),(2) and (3) $F[x]$ is euclidean ring.

Lemma 3.52 *$F(x)$ is a principal ideal ring.*
Proof: Clearly, $F(x)$ is an integral domain with unit element. Let U be the ideal of $F(x)$. Suppose $u = (0)$. (i.e.) U is an ideal generated by zero. Then $F(x)$is principle ideal ring. Then nothing to prove. Suppose $u \neq 0$. Then there exists an element $f(x) \in F[x]$ such that $0 \neq f(x)$ in $U \subset F[x]$. Claim that $U = (g(x))$. Let $g(x)$ be a polynomial of least degree in U. By division algorithm, there exists $t(x), r(x) \in F[x] \ \ni$: $f(x) = t(x) \cdot g(x) + r(x)$
where $r(x) = 0$ (or) $deg(r(x)) < deg(g(x))$.....(1)
Since U is an ideal and $t(x) \in F[x]$ and $g(x) \in U, t(x) \cdot g(x) \in U$ and also $f(x) \in U \Rightarrow t(x) \cdot g(x) - f(x) \in U \Rightarrow r(x) \in U$. $\because g(x)$ is a least degree polynomial in $U, deg(r(x))$ cannot be less than $deg(g(x))$. $\therefore \ r(x) = 0$. $\therefore \ f(x) = t(x) \cdot g(x) \in U$. Every polynomial of $F[x]$ can be written as a multiple of $g(x) \Rightarrow f(x) \in (g(x))$. $\therefore \ U = (g(x))$. Hence the claim. $\therefore \ U$ is a principle ideal in $F[x]$ and U is arbitrary. $\therefore \ F[x]$ is a principle ideal ring.

Lemma 3.53 *Given two polynomials $f(x), g(x)$ in $F[x]$ they have a greatest common divisor which can be realised as $d(x) = \lambda(x)f(x) + l_1(x)g(x)$ for some polynomial $\lambda(x), l_1(x)$*
Proof: Let $S = \{s(x)f(x) + t(x)g(x) | s(x)$ and $t(x) \in F[x]\}$. Then $F[x]$ is a ring with unit element. Let $s(x) = 1; t(x) = 0$. Then $f(x) \in S$. Similarly $g(x) \in S$. So, $S \neq \phi$. Let $h_1(x), h_2(x) \in S$. Then, $h_1(x) = s_1(x)f(x) + t_1(x) \cdot g(x)$; $h_2(x) = s_2(x)f(x) + t_2(x)g(x)$, where $s_1(x), s_2(x), t_1(x), t_2(x) \in F[x]$. Now,

$$\begin{aligned} h_1(x) - h_2(x) &= [s_1(x)f(x) + t_1(x)g(x)] - [s_2(x)f(x) + t_2(x)g(x)] \\ &= [s_1(x) - s_2(x)]f(x) + [t_1(x) - t_2(x)]g(x), \\ &\quad where\ s_1(x) - s_2(x), t_1(x) - t_2(x) \in F[x] \\ &= s(x)f(x) - t(x)g(x), \\ &\quad where\ s(x) = s_1(x) - s_2(x), t(x) = t_1(x) - t_2(x) \end{aligned}$$

$\therefore \ h_1(x) - h_2(x) \in S$.....(1)
Let $p(x) \in F[x]$ and $h(x) \in S$. Then,

$$\begin{aligned} p(x) \cdot h(x) &= p(x)[s(x)f(x) + t(x)g(x)] \\ &= (p(x)s(x))f(x) + (p(x)t(x))g(x), \\ &\quad where\ p(x)s(x) \in F(x)\ and\ p(x)t(x) \in F(x) \end{aligned}$$

$\therefore p(x) \cdot h(x) \in S$.....(2)
From (1) and (2), S is an ideal. $\because \ F[x]$ is an euclidean ring. $\therefore \ S$ is a principle ideal. $S = (m(x))$ for some $m(x) \in S$. $m(x) = s_0(x)f(x) + t_0(x)g(x)$, where $s_0(x)$ and $t_0(x) \in F[x]$.....(*)
Since $f(x) \cdot g(x) \in S, f(x) = a(x) \cdot m(x) \Rightarrow m(x)/f(x)$ and $g(x) = b(x) \cdot m(x) \Rightarrow m(x)/g(x)$.

Remark 3.54 *A polynomial over an arbitrary ring is not a principle ideal ring.*
Proof: The ring polynomial $J[x]$ over ring of integers is not a principle ideal ring.
Claim 1: The ideal $(2, x)$ of $J[x]$ generated by $(2, x)$ of $J[x]$ is not a principle ideal ring. Suppose $(2, x)$ is principle ideal in $J[x]$, there exists $g(x) \in J(x) \ \ni: (2, x) = g(x)$ [$\because 2 \in (2, x) \Rightarrow 2 \in (g(x))$]. $\therefore$ There exists $\phi(x) \in J[x]$ such that $2 = \phi(x) \cdot g(x)$.....(1)
$\because x \in (g(x))$, there exists $\phi'(x) \in J[x] \ni: x = \phi'(x) \cdot g(x)$.....(2)
From (1) and (2),

$$
\begin{aligned}
&(1) \Rightarrow 2x = x \cdot \phi(x) \cdot g(x) \\
&(2) \Rightarrow 2x = 2 \cdot \phi'(x) g(x) \\
&\Rightarrow x \cdot \phi(x) \cdot g(x) = 2 \cdot \phi'(x) g(x) \\
&\Rightarrow (x \cdot \phi(x) - 2 \cdot \phi'(x)) g(x) = 0 \\
&\Rightarrow x\phi(x) = 2\phi'(x) \ [\because g(x) \neq 0 \textit{ and } J[x] \textit{ is integral domain}]
\end{aligned}
$$

$\Rightarrow$ coefficient of $\phi(x)$ must be an even integer. $\therefore \phi(x) = 2h(x) \Rightarrow h(x) \in J[x]$.....(3)
From (1) and (3), $2 = 2h(x) \cdot g(x) \Rightarrow 1 = h(x) \cdot g(x) \Rightarrow 1 \in (g(x)) \Rightarrow J[x] = (g(x)) = (2, x)$ [$\because 1 \in U \Rightarrow U = R$]. $\therefore$ Every element of $J[x]$ belong to $(2, x)$ .....(A)
Claim 2: $1 \notin (2, x)$
Suppose $1 \in (2, x)$ then by Lemma 3.53, $[d(x) = \lambda(x) f(x) + l_1(x) g(x)] \Rightarrow 1 = 2p(x) + xq(x), p(x), q(x) \in J[x]$. Let $p(x) = a_0 + a_1 x + a_2 x^2 + ...; q(x) = b_0 + b_1 x + b_2 x^2 + ...$ Now, $1 = 2[a_0 + a_1 x + a_2 x^2 + ...] + x[b_0 + b_1 x + b_2 x^2 + ...] \Rightarrow 1 = 2a_0 \Rightarrow a_0 = 1/2 \notin J \Rightarrow\Leftarrow$ Hence, the claim(2). $1 \notin (2, x)$ which is a $\Rightarrow\Leftarrow$ to (A). $\therefore$ $(2, x)$ is not a principle ideal of $J[x]$. $\therefore J[x]$ is not a principle ideal ring

Definition 3.55 *A polynomial $p(x) \in F[x]$ is said to be irreducible over $F[x]$ if whenever $p(x) = a(x)b(x)$ with $a(x), b(x) \in F[x]$. Then one of $a(x)$ or $b(x)$ has degree 0. (i.e.) a constant.*

Example 3.56 *Let $f(x) = x^2 + 1 = (x + i)(x - i)$ is irreducible over real field but not over complex.*

Lemma 3.57 *Any polynomial in $F[x]$ can be written in a unique manner as a product of irreducible polynomial in $F[x]$*
Proof: Let $f(x)$ be a non-zero polynomial in $F[x]$. Then clearly, $deg(f(x)) > 0$. Let a be the coefficients of the leading terms of $f(x)$. Now, when $f(x)$ is of degree 1, it is of the form $a_0 + ax$, where $a_0, a \in F$ and $a \neq 0$. We may also write it in the form $f(x) = a(a^{-1}a_0 + x)$. Clearly, $a^{-1}a_0 + x$ is a monic irreducible polynomial in $F[x]$ and a is an element of F. So, when $f(x)$ is

a polynomial of degree 1, the theorem follows. Let us assume the theorem to be true $\forall$ polynomials of degree less than that of $f(x)$ and by induction we must show it to be true for $f(x)$. Since the coefficient of the leading term of $f(x)$ is a, we may write $f(x) = af_1(x)$, where $f_1(x) = a^{-1}f(x)$ and therefore $f_1(x)$ is a monic polynomial. Now, if $f(x)$ is irreducible, then so is $f_1(x)$ and so in this case the theorem will follow. On the other hand, if $f(x)$ is reducible we have, $f(x) = g(x) \cdot h(x)$, where $g(x)$ and $h(x)$ are non-unit, non-zero polynomials in $F[x]$. $\because F[x]$ is a polynomial over the field F, $deg[g(x) \cdot h(x)] = deg(g(x)) + deg(h(x))$ and since each one of $g(x)$ and $h(x)$ is a non-zero, non-unit polynomial in $F[x]$. $deg(g(x)) > 0$ and $degh(x) > 0$ and therefore, $deg(g(x)) < deg[g(x) \cdot h(x)] = deg(f(x))$ and $deg(h(x)) < deg[g(x) \cdot h(x)] = deg(f(x))$ [By Corollary 3.49]. So by assumed hypothesis, we can write $g(x) = a_1p_1(x)p_2(x) \cdots p_n(x)$, where each $p_i(x)$ is monic irreducible in $F[x]$ and $h(x) = a_2q_1(x)q_2(x) \cdots q_m(x)$, where each $q_j(x)$ is monic irreducible in $F[x]$. $\therefore$ $f(x) = g(x) \cdot h(x) = a_1a_2p_1(x)p_2(x) \cdots p_n(x)q_1(x) \cdots q_m(x)$ =product of finite no of irreducible polynomial in $F[x]$, where each $p_i(x)$ and $q_j(x)$ are monic irreducible in $F[x]$. Thus the theorem holds for $f(x)$ and therefore by induction hypothesis $\forall$ polynomials in $F[x]$. Now in order to show that this decomposition is unique, let $f(x) = ap_1(x)p_2(x) \cdots p_m(x) = aq_1(x)q_2(x) \cdots q_n(x)$, where each $p_i(x)$ and $q_j(x)$ are the monic irreducible polynomials in $F[x]$. Then $p_1(x)p_2(x) \cdots p_m(x) = q_1(x)q_2(x) \cdots q_n(x)$.....(1).
It is clear that $p_1(x)/p_1(x)p_2(x) \cdots p_m(x)$ and so from (1) we have, $p_1(x)/q_1(x)q_2(x) \cdots q_n(x)$. But this means that $p_1(x)$ must divide atleast one of $q_1(x)q_2(x) \cdots q_n(x)$. $\because F[x]$ is commutative ring, we may assume that $p_1(x)/q_1(x)$. Now, $p_1(x)/q_1(x)$and $p_1(x), q_1(x)$ are irreducible polynomials in $F[x]$. $\Rightarrow$ $p_1(x)$ and $q_1(x)$ are associates. $\Rightarrow$ $q_1(x)$ is unit times $p_1(x)$. $\Rightarrow q_1(x) = up_1(x)$ where u is a unit in $F[x]$. [$\because$ units in $F[x]$ are constant polynomial] $\Rightarrow q_1(x) = p_1(x)$ [$\because q_1(x)$ and $p_1(x)$ being monic, we must have $u = 1$]. Consequently, $p_1(x)p_2(x) \cdots p_m(x) = q_1(x)q_2(x) \cdots q_n(x)$ [$\because p_1 = q_1$] and therefore, $p_2(x)p_3(x) \cdots p_m(x) = q_2(x)q_3(x) \cdots q_n(x)$ [canceling $p_1(x)$]. Now, we can repeat the above argument on this relation with $p_2(x)$.
We continue the above process. Now, if $n > m$ then after m steps the LHS of (1) will become 1 and the RHS of (1) will reduce to a product of a certain number of $q(x)'s$ (the excess of n over m). But each $q_i(x)$ being irreducible polynomial, the product of there $q(x)$'s will therefore be a polynomial of degree not less than 1 and therefore, this product can never be 1. Thus, a $\Rightarrow\Leftarrow$ consequently n and m. Similarly, by changing the rules of $p(x)$ and $q(x)$ we have m and n. Hence $m = n$. Also in the above process, we have shown that every $p(x)$ is equal to $q(x)$. Hence the decomposition is unique except for the order in which the factors occur.

Lemma 3.58 *The ideal $A = (p(x))$ in $F[x]$ is a maximal ideal $\Leftrightarrow$ $p(x)$ is irreducible over F.*

Proof: Suppose $A = (p(x))$ is a maximal ideal $F[x]$. (i.e.) $0 \neq p(x)$ is maximal in $F[x]$. To Prove: $p(x)$ is irreducible over F. Since the ideal generated by $p(x)$ is maximal, $(p(x)) \neq F[x]$ and $p(x)$ is prime ($\because$ Every maximal ideal is prime). Consider the polynomial $f(x), g(x) \in F[x] \ni: f(x) \cdot g(x) \in (p(x)) \Rightarrow f(x) \in p(x)$ (or) $g(x) \in p(x) \Rightarrow f(x) = t(x)p(x)$ (or) $g(x) = r(x)p(x) \Rightarrow p(x)/f(x)$ (or) $p(x)/f(x)$. Thus, $p(x)/f(x) \cdot g(x) \Rightarrow p(x)/f(x)$ (or) $p(x)/g(x) \Rightarrow p(x)$ is irreducible over F. Conversely, suppose that $p(x)$ is a maximal ideal in $F[x]$. To Prove:$A = (p(x))$ is a maximal ideal in $F[x]$. Suppose there exists an ideal N of $F[x] \ni: (p(x)) \subset N \subset F[x]$.....(1)
Since N is in $F[x]$, which is a principal ideal ring, $N = (g(x)), g(x) \in F[x]$. From (1), $(p(x)) \subset (g(x)) \subset F[x] \Rightarrow (p(x)) \subset (g(x)) \Rightarrow (p(x)) \in (g(x)) \Rightarrow (p(x)) = t(x) \cdot g(x), t(x) \in F[x]$ $\because p(x)$ is irreducible either $deg(t(x)) = 0$ or $deg(g(x)) = 0$. Suppose $deg(g(x)) = 0$. Then $g(x)$ is a non-zero constant, say $g(x) = a, a \neq 0$ in F. $\because F$ is a field, $a = g(x)$ is a unit in $F[x]$. Then, $N = F[x]$ [$\because g(x) = F[x]$].....(2).
Suppose $deg(t(x)) = 0$. Let $t(x) = b$, a non-zero element in F. $\therefore g(x) = \frac{1}{b}p(x) \Rightarrow g(x) \in (p(x)) \Rightarrow N \subseteq (p(x))$. But $(p(x)) \subseteq N$
$\therefore N = (p(x))$. Thus, $p(x) \subseteq N \subseteq F[x] \Rightarrow$ either $(p(x)) = N$ (or) $N = F[x]$. $\therefore (p(x))$ is maximal in $F[x]$.

Polynomials over the Rational Field:

Definition 3.59 *The polynomial $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, where $a_0, a_1, ..., a_n$ are integers is said to be primitive if the GCD of $a_0, a_1, ..., a_n$ is 1. For example, $f(x) = 3 + 5x + 7x^2$ is primitive.*

Definition 3.60 *A polynomial in which the leading coefficient is 1 is called as monic polynomial. For example, $f(x) = 2 + 3x + 4x^2 + x^3$ is monic polynomial.*

Definition 3.61 *A polynomial is said to an integer monic if all the coefficients are integers and the leading coefficient is 1. For example, $f(x) = 5 - 6x + 12x^2 + x^3$ is integer monic polynomial.*

Lemma 3.62 *If $f(x)$ and $g(x)$ are primitive polynomials, then $f(x) \cdot g(x)$ is a primitive polynomial.[product of any two primitive polynomial is again primitive].*
Proof: Let $f(x) = a_0 + a_1(x) + ... + a_nx^n$ and $g(x) = b_0 + b_1(x) + ... + b_mx^m$ be primitive polynomials. To Prove: $f(x) \cdot g(x)$ is primitive. Suppose not, (i.e) $f(x) \cdot g(x)$ is not primitive. Then all the coefficient of $f(x) \cdot g(x)$ would be divisible by some integer > 1. Hence some prime number p, p divides all the coefficient of $f(x) \cdot g(x)$. $\because f(x)$is primitive, p does not divides all the coefficients of $f(x)$. Let a_j be the first coefficient of $f(x)$ such that p does not divides a_j. [$(i.e) p/a_0, p/a_1, ..., p/a_{j-1}$].....(1)
Similarly, $\because$ $g(x)$ is primitive, p does not divides all the coefficients of

$g(x)$. Let b_k be the first coefficient of $g(x)$ such that does not divides b_k. $[(i.e.)p/b_0, p/b_1, ..., p/b_{k-1}]$ .....(2)
$c_{j+k} = (a_{j+k}b_0 + a_{j+k-1}b_1 + ... + a_{j+1}b_{k-1}) + a_jb_k$
$+(a_{j-1}b_{k+1} + ... + a_1b_{j+k-1} + a_0b_{j+k})$..... (3)
By our choice of $a_j, p/a_0, p/a_1, ..., p/a_{j-1}$
$\Rightarrow p/a_0b_{j+k} + a_1b_{j+k+1} + .. + a_{j-1}b_{k+1}$..... (4)
By our choice of $b_k, p/b_0, p/b_1, ..., p/b_{k-1}$
$\Rightarrow p/a_{j+k}b_0 + a_{j+k+1}b_1 + .. + a_{j+1}b_{k-1}$..... (5)
But $p/c_{j+k} \Rightarrow p/(c_{j+k}) - (a_0b_{j+k} + a_1b_{j+k-1} + ... + a_{j-1}b_{k+1})$
$-(a_{j+k}b_0 + a_{j+k+1}b_1 + ... + a_{j+1}b_{k-1})$
$\Rightarrow p/a_jb_k$ [by (3)] $\Rightarrow p/a_j$ (or) $p/b_k[\because p$ is prime]
$\Rightarrow\Leftarrow$ to p does not divides a_j and p does not divides b_k. $\therefore$ Our assumption is wrong. Hence, $f(x) \cdot g(x)$ is primitive. Hence, the lemma.

Definition 3.63 ***Content of the Polynomial*** *Let $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, where a_i's are integers. The content of the polynomial is the GCD of $a_0, a_1, a_2, ..., a_n$ and it is denoted by $c(f)$. (i.e.) $c(f) = (a_0, a_1, a_2, ...a_n)$.*

Example 3.64 *Let $p(x) = 5+10x+25x^2+30x^3$. Then $c(f) = (5, 10, 25, 30) = 5$.*

Remark 3.65
1. *Any polynomial with integer coefficient is said to be integer monic if the content of $f(x) = 1$.*
2. *Any polynomial $p(x)$ with integer coefficient can be written as $p(x) = d(g(x))$, where d is the content of $p(x)$, and $g(x)$ is primitive.*

Example 3.66 *$p(x) = 3 + 6x + 9x^2 - 12x^3 = 3(1 + 2x + 3x^2 - 4x^3) = c(p(x))g(x)$, where $c(p(x)) = 3$ and $g(x) = 1 + 2x + 3x^2 - 4x^3$, primitive.*

Theorem 3.67 ***Gauss Lemma*** *If the primitive polynomial $f(x)$ can be factored as the product of two polynomials having rational coefficient, it can be factored as the product of two polynomials having integer coefficients.*
Proof: Suppose $f(x) = u(x) \cdot v(x)$, where $u(x)$ and $v(x)$ are polynomial having rational coefficients. Let $u(x) = \frac{a_0}{b_0} + (\frac{a_1}{b_1})x + (\frac{a_2}{b_2})x^2 + ... + (\frac{a_n}{b_n})x^n$, where a_i's and b_j's are integers and b_j's $\neq 0$, $\forall j$. Claim that $f(x) = \frac{a}{b}\lambda(x) \cdot l_1(x)$, where a, b are integer and $\lambda(x), l_1(x)$ are primitive polynomial with integer coefficients.
$u(x) = \frac{1}{b_0b_1b_2\cdots b_n}[a_0(b_1b_2 \cdots b_n) + a_1(b_0b_2b_3 \cdots b_n)x + a_2(b_0b_1b_2 \cdots b_n)x^2 + ... + a_n(b_0b_1b_2 \cdots b_{n-1})x^n] = \frac{1}{m}[c_0 + c_1x + c_2x^2 + .. + c_nx^n]$..... (1)
where $m = b_0b_1b_2 \cdots b_n$; $c_0 = a_0(b_1b_2 \cdots b_n)$; $c_1 = a_1(b_0b_2b_3 \cdots b_n); \cdots; c_n = a_n(b_0b_1b_2 \cdots b_{n-1})$. $\because$ any polynomial $f(x)$ can be written as $f(x) = d \cdot g(x)$ where d is content of $f(x)$ and $g(x)$ is primitive. $c_0+c_1x+c_2x^2+...+c_nx^n = d\lambda(x)$, where $d = (c_0, c_1, c_2, ..., c_n)$ and $\lambda(x)$ is primitive. $\therefore$ From (1), $u(x) =$

$\frac{d}{m}\lambda(x)$, where $d = (c_0, c_1, c_2, ..., c_n)$, $\lambda(x)$ 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. $\therefore$ $f(x) = u(x) \cdot v(x) = \frac{d}{m} \cdot \frac{d_1}{m_1} \cdot \lambda(x) l_1(x) = \frac{a}{b}\lambda(x) l_1(x)$.....(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 having two 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 $p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$ and $r(x) = b_0 + b_1 x + b_2 x^2 + ... + b_m x^m$, 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 factored as the product of two integer monic polynomials.

4. UNIT IV

Vector Spaces

Definition 4.1 ***Vector Space:*** *A non empty set V is said to be a vector space over a field F if V is an abelian group under(addition) and if for every $\alpha \in F, v \in V$, there is defined an element αv in V subject to*

1. $\alpha(v+w) = \alpha v + \alpha w$
2. $(\alpha+\beta) = \alpha v + \beta v$
3. $\alpha(\beta v) = (\alpha\beta)v$
4. $1 \cdot v = v \ \forall \alpha, \beta \in F, \ v, w \in V$

where 1 represents the unit element of V under usual multiplication.

Remark 4.2 *Axiom 1 states the fact that the multiplication element of V for fixed scalar α defined homomorphism of abelian group V into itself if $\alpha \neq 0$ this homomorphism can be shown to be an isomorphism.*

Example 4.3 *(i) Let F be a given field. Let K be a field which contains F as a subfield. We consider K as a vector space over F. For $(K,+)$ is an abelian group, for $\alpha \in F, v \in K, \alpha v \in K$. Axioms $1,2$ and 3 for K as a vector space over F are the consequences of right distributive law, left distributive law, and associative law respectively which holds for K as a ring . Since 1 is the identity element in K, the Axiom 4 follows from it.*
(ii) Let F be a field Let $V = \{(\alpha_1, \alpha_2....\alpha_n)|\alpha_i \in F\}$= all order of n tuples $= F^{(n)}$.

Example 4.4 *$(R,+,\cdot)$ is a field. $V = \{(\alpha_1,\alpha_2)|\alpha_i \in R^*\} = R^{(2)}$, $V = \{(\alpha_1,\alpha_2,\alpha_3)|\alpha_i \in R^*\} = R^{(3)}$.*

Example 4.5 *$(Q^*,+,\cdot)$ is a field. $V = \{(\alpha_1,\alpha_2)|\alpha_i \in Q^*\} = Q^{(2)}$ and $V = \{(\alpha_1,\alpha_2,\alpha_3)|\alpha_i \in Q^* = Q^{(3)}$.*

Example 4.6 *Let F be a field $V = F[x]$= set of all of polynomial x over $F = \{\alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n | \alpha_i \in F\}$. Then V is a vector space over F.*

Definition 4.7 ***Subspace:*** *Let V be a vector space over a field F and if W is a subset of V. Then W is a subspace of V, if under the operations of V, W itself forms a vector space over F. Equivalently W subspace of V whenever $w_1, w_2 \in W, \alpha, \beta \in F$ implies $\alpha w_1 + \beta w_2 \in W$.*

Example 4.8 *Let F be a field. Let V_n be the set of all polynomials of degree less than n. Under natural operations for polynomials of addition and multiplication. V_n be the vector space over F, which is a subspace of $V = F[x] = \{\alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_n x^n + ... | \alpha_i \in F\}$.*

Definition 4.9 *If U and V are the vector spaces over F then the mapping T of U into V is said to be a homomorphism if*
(i) $(u_1 + u_2)T = u_1T + u_2T, \forall u_1, u_2 \in U$ *and* $\alpha \in F$
(ii) $(\alpha u_1)T = \alpha(u_1T)$
if T, in addition is $1-1$ we call it an isomorphism. $Ker\ T = \{u \in U | uT = 0$, identity element of addition in $V\}$.

Remark 4.10 *T is an isomorphism iff $Ker\ T = \{0\}$*

Definition 4.11 *Two vector spaces are said to be isomorphic if there is an isomorphism of one onto the other.*

Lemma 4.12 *Let V is a vector space over F*

1. $\alpha(0) = 0$ *for* $\alpha \in F$,
2. $0 \cdot v = 0$ *for* $v \in V$,
3. $(-\alpha)v = -\alpha v$, *for* $\alpha \in F, v \in V$,
4. *if* $v \neq 0$ *then* $\alpha \cdot v = 0 \Rightarrow \alpha = 0$.

Lemma 4.13 *If V is a vector space over F and W is a Subspace of V. Then $V/W = \{v + W | v \in V\}$. Let $v_1 + W, v_2 + W \in V/W$ and $\alpha \in F$. Define* (i) $(v_1 + W) + (v_2 + W) = v_1 + v_2 + W$,
(ii) $(v_1 + W) = \alpha v_1 + W$.
Under the operation defined above under the operation V/W is a vector space and is called quotient space of V/W.

Theorem 4.14 ***Fundamental theorem for vector homomorphism:*** *If T is a homomorphism of U onto V with kernal W. Then V is isomorphic to U/W conversely if U is a vector space and W is a subspace of U. Then there is a homomorphism of U onto U/W.*

Definition 4.15 *Let V be a vector space over F and let $U_1, U_2, ..., U_n$ be subspace of V. Then V is said to be the internal direct sum of $U_1, U_2, ..., U_n$ if every element $v \in V$ can be written in the unique way as $v = u_1 + u_2 + ... + u_n, u_i \in U_i$.*

Remark 4.16 *Let V be any vector space over field F. Then V itself and subset of V consisting of $\bar{0}$ vector only are the trivial subspace of V. They are improper subspace. For example let $V = \{(\alpha_1, \alpha_2, \alpha_3) | \alpha_1, \alpha_2, \alpha_3 \in F\}$ and $W = \{(\alpha_1, \alpha_2, 0) | \alpha_1, \alpha_2 \in F\}$. Then W is a subspace of V*

Linear Independent and Spaces:

Definition 4.17 *Let V be a vector space over F and if $v_1, v_2, ..., v_n$. Then any element of the form $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n$ where $\alpha_i \in F$ is a linear combination over F of $v_1, v_2, ..., v_n$.*

Definition 4.18 *Let V be a vector space over F and S be any non-empty subset of V. Then the linear span of S, $L(S)$ is the set of all linear combination of finite sets of element of S. (i.e.) $L(S) = \{\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n | v_1, v_2, ..., v_n$ is an arbitrary finite subset of S and $\alpha_1, \alpha_2, ..., \alpha_n$ is any arbitrary finite subset of $F\}$.*

Lemma 4.19 *$L(S)$ is a subspace of V.*

Lemma 4.20 *If S, T are the subset of V then,*

1. *$S \subset T \Rightarrow L(S) \subset L(T)$,*
2. *$L(S \cup T) = L(S) \cup L(T)$,*
3. *$L(L(S)) = L(S)$.*

The vector space V is said to be finite dimensional over F if there is a finite subset S in V such that $V = L(S)$.

Example 4.21 *Let $V = F^{(3)} = V_3(f) = \{(\alpha_1, \alpha_2, \alpha_3) | \alpha_1, \alpha_2, \alpha_3 \in F\}$. Let $S = \{(1, 0, 0)\}$; $L(S) = \{(\alpha, 0, 0) | \alpha \in F\} \subset V$.*

Example 4.22 *$V = F^{(3)}$; $S = \{(1, 0, 0), (0, 1, 0)\}$. $L(S) = \{(\alpha_1, \alpha_2, 0) | \alpha_1, \alpha_2 \in F\}$.*

Example 4.23 *Let $V = F^{(3)}$ and $S = \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$. Then $L(S) = V$.*

Example 4.24 *$V = \alpha_1 v_1 + ... + \alpha_n v_n$. Let $v = (a, b, c) \in F^{(3)} = V$. $(a, b, c) = a(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1) \Rightarrow (a, b, c) \in L(S) \Rightarrow V \subset L(S)$, but $L(S) \subset V$. $\therefore L(S) = V$.*

Definition 4.25 *If V is a vector space and if $v_1, v_2, ..., v_n$ are in V. We say that they are linearly dependent over F if there exist element $\lambda_1, \lambda_2, ..., \lambda_n$ in F not all of them zero(0) such that $\lambda_1 v_1 + ... + \lambda_n v_n = 0$. If the vectors are not linearly dependent over F they are said to be linearly independent.*

Remark 4.26 *Two vectors are linearly dependent one of them will be the scalar multiple of other.*

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* $\vec{0}$.

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 basis 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.

Definition 4.34 ***Dimension:*** *The dimension of V over F is the number of elements in any basis of V over F. For example, $dim(F_{(3)}) = 3$ and $dim(F_{(4)}) = 4$.*

Result 4.35 *Any two finite dimensional vector space over F of the same dimension are isomorphic. $dim_F(V_1) = dim(V_1) = n$ and $dim_F(V_2) = dim(V_2) = n \Rightarrow V_1 \cong V_2$.*

Definition 4.36 ***Dual space:*** *The set of all homomorphism of U into V will be written as $Hom(U, V)$.*

Lemma 4.37 *Let V, W be any two vector space over the field F. $Hom(V, W)$ be the set of all vector space homomorphisms of V into W. Then $Hom(V, W)$ is a vector space over F. Let $S, T \in Hom(V, W)$. Define $V(S + T) = VS + VT$ under this operation $Hom(V, W)$ is a vector space.*

Result 4.38

1. *If V and W are of dimensions m and n respectively over F then $Hom(V, W)$ is of dimension mn over F. If $dim_F(V) = m$ then $dim_F(Hom(V, V)) = dim_F(V)dim_F(V) = m \cdot m = m^2$.*
2. *$dim_F(Hom(V, F)) = dim_F(V) \times dim_F(V) = m \times 1 = m$.*
3. *$dim_F(Hom(Hom(V, F), F)) = dim_F(Hom(m, F)) = m$.*

Definition 4.39 *If V is a vector space, then its dual space is $Hom(V, F)$, We shall denote this as by $\widehat{V}$.*

Definition 4.40 *Any elements of $\widehat{V}$ is called a linear functional on V into F*

Remark 4.41 *if V is not finite dimensional $\widehat{V}$ is usually too large and would be of.*
Note: *$\widehat{\widehat{V}} = Hom(\widehat{V}, F)$.*

Result 4.42

1. *If V is a finite dimensional an $v \neq 0$ in V then there is an element $F \in \widehat{V}$ such that $F(v) = 0$.*
2. *If V is a finite dimensional vector space then there is an isomorphism of V onto $\widehat{\widehat{V}}$.*

Definition 4.43 *if W is a subspace of $\widehat{V}$ then annihilator of $W, A(W) = \{f \in \widehat{V} / f(W) = 0 \ \forall w \in W\}$.*

Result 4.44

1. *$A(w)$ is a subspace of $\widehat{V}$.*

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

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

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 $v_1, v_2 \in V$,

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

$\therefore \; T_1 + T_2 \in Hom(V, V) \Rightarrow +$ 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,

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

$$\begin{aligned}(\alpha v_1)(T_1 \cdot T_2) &= ((\alpha v_1)T_1) \cdot T_2 \\ &= \alpha(v_1 T_1) \cdot T_2 = \alpha((v_1 T_1)T_2) \\ &= \alpha(v_1(T_1 \cdot T_2))\end{aligned}$$

$\therefore\ T_1 \cdot T_2 \in Hom(V,V)$. Clearly $T_1(T_2 \cdot T_3) = (T_1 \cdot T_2)T_3\ \forall T_1, T_2, T_3 \in Hom(V,V)$. $\therefore\ \cdot$ is associative.
$T_1 \cdot (T_2 + T_3) = T_1 \cdot T_2 + T_1 \cdot T_3;\ (T_1 + T_2) \cdot T_3 = T_1 \cdot T_3 + T_2 \cdot T_3\ \forall T_1, T_2, T_3 \in Hom(V,V)$. $\cdot$ is distributive over F. $\therefore\ (Hom(V,V), +, \cdot)$ is a Ring.
Now, let $T_1 \cdot T_2 \in Hom(V,V)$. To Prove: $\alpha(T_1 + T_2) = \alpha T_1 + \alpha T_2$.

$$\begin{aligned}v(\alpha(T_1 + T_2)) &= \alpha(v(T_1 + T_2)) \\ &= \alpha(vT_1 + vT_2) \\ &= \alpha(vT_1) + \alpha(vT_2) \\ &= v(\alpha T_1) + v(\alpha T_2) \\ &= v(\alpha T_1) + v(\alpha T_2), \forall v \in V \\ &\Rightarrow \alpha(T_1 + T_2) = \alpha T_1 + \alpha T_2,\ \forall \alpha \in F\ and\ T_1, T_2 \in Hom(V,V).\end{aligned}$$

To prove:$(\alpha + \beta)T_1 = \alpha T_1 + \beta T_1$.

$$\begin{aligned}Let\ v \in V, v((\alpha + \beta)T_1) &= (\alpha + \beta)(vT_1) \\ &= v(\alpha T_1) + \beta(vT_1) \\ &= v(\alpha T_1) + v(\beta T_1) \\ &= v(\alpha T_1 + \beta T_1) \\ &\Rightarrow (\alpha + \beta)T_1 = \alpha T_1 + \beta T_1,\ \forall \alpha, \beta \in F\ and\ T_1 \in Hom(V,V).\end{aligned}$$

To Prove: $\alpha(\beta T_1) = (\alpha\beta)T_1$.

$$\begin{aligned}v(\alpha(\beta T_1)) &= \alpha(v(\beta T_1)) \\ &= \alpha(\beta(vT_1)) \\ &= \alpha\beta(vT_1) \\ &= v(\alpha\beta)T_1 \\ &\Rightarrow \alpha(\beta T_1) = (\alpha\beta)T_1\ \forall \alpha, \beta \in F and T_1 \in Hom(V,V).\end{aligned}$$

$v(1 \cdot T_1) = 1 \cdot (vT_1) = vT_1 \Rightarrow 1 \cdot T_1 = T_1\ \forall T_1 \in Hom(V,V)$. Hence $Hom(V,V)$ is a vector space over a field F. Let $v \in V$,

$$\begin{aligned}v(\alpha(T_1 T_2)) &= \alpha(v(T_1 T_2)) \\ &= \alpha((vT_1)T_2) \\ &= (vT_1)(\alpha T_2) \\ &= (vT_1)(\alpha T_2) \\ &\Rightarrow \alpha(T_1 T_2) = T_1(\alpha T_2).\end{aligned}$$

Now,

$$\begin{aligned} v((\alpha T_1)T_2) &= (v(\alpha T_1))T_2 \\ &= \alpha((vT_1))T_2 \\ &= \alpha(vT_1T_2) \\ &= v(\alpha(vT_1T_2)) \\ &\Rightarrow (\alpha T_1)T_2 = \alpha(T_1T_2) \\ \alpha(T_1T_2) &= (\alpha T_1)T_2 = T_1(\alpha T_2), \alpha \in F \text{ and } T_1, T_2 \in Hom(V,V). \end{aligned}$$

$\therefore$ $Hom(V,V)$ is an algebra over F.

Remark 4.48 *For convenient we shall write $Hom(V,V)$ as $A(V)$. Whenever we want to emphasis the role of field. We shall denote it by $A_F(V)$.*

Definition 4.49 *A linear transformations on V over F is an element of $A_F(V)$. (i.e.) A linear transformations is a vector space homomorphism of V onto itself.*

Remark 4.50 *We shall refer $A(V)$ as a ring or algebra of linear transformation on V.*

Lemma 4.51 *If A is an algebra with unit element over a field F. Then A is isomorphic to a sub-algebra of $A(V)$ for some vector space V over F.(Analogue of Cayley's theorem for algebra)*
Proof: Since A is an algebra over F. It must be a vector space over F. To prove: A is isomorphic to sub-algebra of $A(V)$, for some vector space V. Since A is a ring as well as a vector space, we choose $V = A$. Let $a \in A$, define $T_a : V(A) \to V(A)$ by $vT_a = va$ $\forall v \in V$. Claim T_a is a linear transformation on V. (i.e.) T_a is a vector homomorphism. Let $v_1, v_2 \in V$ and $\alpha \in F$
Now, $(v_1 + v_2)T_a = v_1 = v_1a + v_2a = v_1T_a + v_2T_a$..... (1)
$(\alpha v_1)T_a = (\alpha v_1)a = \alpha(v_1a) = \alpha(v_1T_a)$.....(2)
From (1)and (2), $T_a \in Hom(V,V) = A(V)$. (i.e.) T_a is a linear transformation on V. Hence the claim.
Define a mapping $\psi : A \to A(V)$ by $a\psi = T_a$ $\forall a \in A$. Let $a, b \in A$ and $\alpha \in F$. First, to prove that $T_{a+b} = T_a + T_b$. For $v \in V, vT_{a+b} = v(a + b) = va+vb = vT_a+vT_b$ $\forall v \in V \Rightarrow T_{a+b} = T_a+T_b$. Next, to prove that $T_{\alpha a} = \alpha T_a$. For any $v \in V, vT_{\alpha a} = v(\alpha a) = \alpha(va) = \alpha(vT_a)$ $\forall v \in V \Rightarrow T_{\alpha a} = \alpha T_a$. From $T_{a+b} = T_a + T_b$ we have, $\Rightarrow (a + b)\psi = a\psi + b\psi$.....(3)
From $T_{\alpha a} = \alpha T_a \Rightarrow (\alpha a)\psi = \alpha(a\psi)$..... (4)
From (3) and (4), ψ is a homomorphism of A into $A(V)$.
To prove ψ is $1-1$, it is enough to prove that $Ker\psi = \{0\}$ where 0 is the identity element in $A(V)$. Let $a \in Ker\psi$

$\Rightarrow a\psi = 0 \ \forall a \in A$
$\Rightarrow T_a = 0 \ \forall a \in A$
$\Rightarrow vT_a = 0 \ \forall a \in A$
$\Rightarrow va = 0, \ \forall a \in A, \forall v \in V$
$\Rightarrow ea = 0$ [$\because V = A(V)$ *contains the unit element*]
$\Rightarrow a = 0$
$\therefore Ker\psi = \{0\}$

$\therefore \psi$ is $1-1$, clearly ψ is onto. Hence ψ is an isomorphism of A onto $A(V)$. Hence A is isomorphic to some algebra of $A(V)$.

Lemma 4.52 *Let A be an algebra with element over F and suppose that A is of dimension of m over F then every element in A satisfies some non-trivial polynomials $f(x)$ of degree almost m.*
Proof: Given dim $A = m$. $\therefore$ Any set of $m+1$ elements in A is linearly dependent. Let $a \in A$. Then $e, a, a^2, a^3, ..., a^m$ are linearly dependent. $\therefore$ there exists scalar $\alpha_0, \alpha_1, ..., \alpha_m \in F$, not all zero such that $\alpha_0 e + \alpha_1 a + \alpha_2 a^2 + ... + \alpha_m a^m = 0 (i.e.) \alpha_0 + \alpha_1 a + \alpha_2 a^2 + ... + \alpha_m a^m = 0$..... (1)
Let $f(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_m x^m \in F[x]$. $\therefore$ By (1) a satisfies the polynomials $f(x) \in F[x]$ of degree almost m. Since a is arbitrary in A, every element in A satisfy the polynomial of degree at most m.

Theorem 4.53 *If V be an n dimensional vector space over a field F, given any element T in $A(V)$ there exists a non-trivial polynomial $q(x)$ of degree almost n^2 such that $q(T) = 0$.*
Proof: Given $T \in Hom(V,V) = A(V)$. But $dim(A(V)) = dim(Hom(V,V)) = dim(V) \cdot dim(V) = n \times n = n^2$. Since $A(V) = Hom(V,V)$ is an algebra of dimension n^2, let $T \in A(V)$. By the above lemma, there exists a non-trivial polynomial $q(x) \in F[x]$ of degree at most n^2. Hence $q(T) = 0$.

Definition 4.54 *A non trivial polynomial of lowest degree satisfied by T in $A(V)$ is called a minimal polynomial of T.*

Remark 4.55 *If $p(x)$ is a minimal polynomial of T and if T satisfies $h(x)$ also then $p(x)/h(x)$ (or) Show that the minimal polynomial of $T \in A(V)$ divides all other polynomial satisfied by T.*
Proof: Let $p(x)$ be the minimal polynomial for T then $p(T) = 0$ and $p(x)$ is of least degree. Given T also satisfies $h(x)$, then $h(T) = 0$..... (1)
By applying division algorithm to $p(x)$ and $h(x)$, $h(x) = p(x) \cdot q(x) + r(x)$, either $r(x) = 0$ or $deg(r(x)) < deg(p(x))$..... (2)
From (1), $0 = h(T) \Rightarrow p(T)q(T) + r(T) = 0 \Rightarrow r(T) = 0$[$\because p(T) = 0$]. If $deg(r(x)) < deg(p(x))$, we can come to a conclusion that $r(x)$ satisfies T whose degree is less than degree of $p(x)$. $\therefore$ $r(x) = 0$. From (2), $h(x) = p(x)q(x)(\because r(x) = 0) \Rightarrow p(x)/h(x)$. Hence the remark.

Definition 4.56 *Let A, B be any algebra's over F. A map $T : A \to B$ is called a homomorphism if,*

1. $(a_1 + a_2)T = a_1T + a_2T$,
2. $(a_1a_2)T = a_1Ta_2T$,
3. $(\alpha a_1)T = \alpha(a_1T)$.

If this T is $1-1$, we say that T is an isomorphism.
$Ker\ T = \{a \in A | aT = 0$, identity element in $B\}$.

Definition 4.57 *An element $T \in A(V)$ is called a right invertible if there exists an element $S \in A(V)$ such that TS=1. (1 is the unit element of $A(V)$)*

Definition 4.58 *An element $T \in A(V)$ is called a left invertible if there exists an element $S \in A(V)$ such that $ST = 1$.*

Definition 4.59 *An element $T \in A(V)$ is said to be invertible (or) regular if it is both right and left invertible (i.e.) there exists an element $S \in A(V)$ such that $TS = ST = 1$. We write S as T^{-1}.*

Remark 4.60 *If T is both right and left invertible and if $TS = UT = 1$, then S and U are unique.*

Definition 4.61 *An element $T \in A(V)$ which not regular is called singular.*

Remark 4.62 *It is quite possible that an element in $A(V)$ is right invertible but not invertible.*

Example 4.63 *Let F be the field of real numbers. Let $V = F[x]$ be the set of all polynomials in x. Define $S \in A(V)$ as $q(x)T = \frac{d}{dx}q(x)$. Let $T \in A(V)$ as $q(x)T = \int_1^x q(x)dx$. Here $TS = 1$ but $ST \neq 1$. Now,*

$$\begin{aligned} q(x)TS &= (q(x)T)S \\ &= (\int_1^x)S \\ &= \frac{d}{dx}(\int_1^x q(x)dx) \\ &= (q(x)) \cdot 1 \\ &= q(x) \\ &\Rightarrow TS = 1 \end{aligned}$$

$\therefore T$ is right invertible but not invertible.

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 invertible iff the constant terms of the minimal polynomial for T is not zero.*
Proof: Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_k x^k$ 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.

$$\begin{aligned} p(T) = 0 \Rightarrow \alpha_0 + \alpha_1 T + ... + \alpha_k T^k = 0 .....(1) \\ \alpha_0 = -(\alpha_1 T + ... + \alpha_k T^k) \\ \alpha_0 = -(\alpha_1 + \alpha_2 T + ... + \alpha_k T^{k-1})T \\ \alpha_0 = T(-\alpha_1 - \alpha_2 T + ... - \alpha_k T^{k-1}) \\ \Rightarrow 1 = T(\frac{1}{\alpha_0}(-\alpha_1 - \alpha_2 - ... - \alpha_k T^{k-1})) \\ 1 = T(-\frac{1}{\alpha_0}(\alpha_1 + \alpha_2 + ... + \alpha_k T^{k-1})) \end{aligned}$$

Let $S = -\frac{1}{\alpha_0}(\alpha_1 + \alpha_2 + ... + \alpha_k T^{k-1})$. 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),

$$\begin{aligned} \alpha_1 T + \alpha_2 T^2 + ... + \alpha_k T^k = 0 \\ (\alpha_1 + \alpha_2 T + ... + \alpha_k T^{k-1})T = 0. \end{aligned}$$

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

$$\begin{aligned} \Rightarrow ((\alpha_1 T + \alpha_2 T^2 + ... + \alpha_k T^k)T)T^{-1} = 0T^{-1} = 0 \\ \Rightarrow \alpha_1 T + \alpha_2 T^2 + ... + \alpha_k T^{k-1} = 0 .....(2) \end{aligned}$$

Let $q(x) = \alpha_1 x + ... + \alpha_k x^{k-1}$. 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 invertible then T^{-1} is a polynomial expression in T over F.*
Proof: Let $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_k x^k$ with $\alpha_k \neq 0$ be the minimal

polynomial of T.

$$\begin{aligned}
p(T) = 0 &\Rightarrow \alpha_0 + \alpha_1 T + \alpha_2 T^2 + ... + \alpha_k T^k = 0 \\
\Rightarrow \alpha_0 &= -(\alpha_1 T + \alpha_2 T^2 + ... + \alpha_k T^k) \\
\alpha_0 &= (-\alpha_1)T + (-\alpha_2)T^2 + ... + (-\alpha_k)T^k \\
1 &= (-\frac{\alpha_1}{\alpha_0})T + (-\frac{\alpha_2}{\alpha_0})T^2 + ... + (-\frac{\alpha_k}{\alpha_0})T^k \\
1 &= ((-\frac{\alpha_1}{\alpha_0}) + (-\frac{\alpha_2}{\alpha_0})T + ... + (-\frac{\alpha_k}{\alpha_0})T^{k-1})T \\
1 \cdot T^{-1} &= ((-\frac{\alpha_1}{\alpha_0}) + (-\alpha_2/\alpha_0)T + ... + (-\frac{\alpha_k}{\alpha_0})T^{k-1})T \cdot T^{-1} \\
T^{-1} &= \beta_1 + \beta_2 T + ... + \beta_k T^{k-1}
\end{aligned}$$

where $\beta_1 = (-\frac{\alpha_1}{\alpha_0}), ..., \beta_k = (-\frac{\alpha_k}{\alpha_0})$. $\therefore$ 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 $p(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_k x^k$ be a minimal polynomial of T over F. (i.e.) $p(T) = 0 \Rightarrow \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_k x^k = 0$. Since T is singular (i.e.) T is non-invertible by Theorem 4.65, $\alpha_0 = 0$. $\therefore$ $\alpha_1 T + \alpha_2 T^2 + ... + \alpha_k T^k = 0 \Rightarrow \therefore (\alpha_1 + \alpha_2 T + ... + \alpha_k T^{k-1})T = 0$.....(1)
Let $S = \alpha_1 + \alpha_2 T + ... + \alpha_k T^{k-1} then S \neq 0$ ($\because \alpha_1 + \alpha_2 x + \alpha_3 x^2 + ... + \alpha_k x^{k-1}$ 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 dimension 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 singular, then by Corollary 4.67, there exists $S \neq 0$ in $A(V)$ such that $ST = TS = 0$.....(2)
From (1), $TU = 0$

$$\begin{aligned}
&\Rightarrow S(TU) = S \cdot 1 \\
&\Rightarrow (ST)U = S \\
&\Rightarrow 0 \cdot U = S \quad by(2) \\
&\Rightarrow S = 0 \\
&\Rightarrow\Leftarrow S \neq 0
\end{aligned}$$

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 $v_1T = \vec{0}$ ($\vec{0} : V \rightarrow V$). 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 $T \in A(V)$.*

Definition 4.75 ***Rank of*** T*: If* V *is finite dimensional over* F*. The rank of* T *is dimensional of* VT*. The rank of* T *over* F*, it is denoted by* $r(T)$ *(i.e.)* $dim(VT)$*=Rank of* $T = r(T)$*.*

Remark 4.76 *1. If* $r(T) = dimV$*. Then* T *is regular,*

2. If $r(T) = 0$*. Then* $T = 0$*.*

Proof: (1) Given $r(T) = dim(V) \Rightarrow dim(VT) = dim(V) \Rightarrow VT = V \Rightarrow T$ is onto $\Rightarrow T$ is regular.
(2) Suppose $r(T) = 0 \Rightarrow dim(VT) = 0 \Rightarrow VT = \{0\} \Rightarrow \{vT | v \in V\} = \{0\} \Rightarrow \{vT = 0, \forall v \in V\} = 0 \Rightarrow T = \vec{0}$.

Lemma 4.77 *If* V *is finite dimensional vector space over* F*. Then* $S, T \in A(V)$

1. $r(ST) \leq r(T)$

2. $r(TS) \leq r(T)$ *and*

3. $r(ST) = r(TS) = r(T)$ *for* S *regular in* V*.*

Proof: $(1)VS \subset V \Rightarrow (VS)T \subset (V)T \Rightarrow V(ST) \subset VTdim(V(ST)) \leq dim(VT) \Rightarrow r(ST) \leq r(T)$.
$(2)r(T) = m = dim(VT)$, where VT is a subspace of V. Let$\{w_1, w_2, ..., w_m\}$ be basis of $VT \Rightarrow dim(VT) = m$. Now, $w_1S, w_2S, ..., w_mS$ generate $(VT)S \Rightarrow dim(V(TS)) \leq m = r(T)$. (i.e.) $r(TS) \leq r(T)$. From (1) and (2), $r(ST) \leq r(T) and r(TS) \leq r(S) \Rightarrow r(ST) \leq min\{r(T), r(S)\}$.
(3) Given S is regular

$$\begin{aligned} S \text{ is onto } &\Rightarrow VS = V \\ &(VS)T = VT \\ &V(ST) = VT \\ &\Rightarrow dim(V(ST)) = dimVT \\ &\Rightarrow r(ST) = r(T).....(i) \end{aligned}$$

Let $r(T) = m$, $VT = m$. Let $\{w_1, w_2, ..., w_m\}$ be a basis of VT. Now, $\{w_1S, w_2S, ..., w_mS\}$ generate $(VT)S = V(TS)$. Claim: $\{w_1S, w_2S, ..., w_mS\}$ is linearly independent for if $\alpha_1(w_1S) + \alpha_2(w_2S) + ... + \alpha_m(w_mS) = 0$ where $\alpha_i \in F$. Then,

$$\begin{aligned} &\alpha_1w_1S + \alpha_2w_2S + ... + \alpha_mw_mS = 0 \\ \Rightarrow &(\alpha_1w_1 + \alpha_2w_2 + ... + \alpha_mw_m)S = 0. \end{aligned}$$

Since S is regular, S^{-1} exists. Now,

$$\begin{aligned} (\alpha_1w_1 + \alpha_2w_2 + ... + \alpha_mw_m)S \cdot S^{-1} &= 0 \\ \alpha_1w_1 + \alpha_2w_2 + ... + \alpha_mw_m &= 0. \end{aligned}$$

$\Rightarrow \alpha_i = 0 \; \forall \; i$ [$\because \{w_1, w_2, ..., w_m\}$ are linearly independent]. Hence the claim.
(i.e.) $\{w1S, w_2S, ..., w_mS\}$ is a basis of $V(TS) \Rightarrow dim(V(TS)) = m \Rightarrow r(T) \Rightarrow r(TS) = r(T)$..... (ii)
From (i) and (ii) $r(ST) = r(TS) = r(T)$ for S regular in V.

Corollary 4.78 *if $T \in A(V)$ and if $S \in A(V)$ is regular then $r(T) = r(STS^{-1})$.*
Proof: $r(STS^{-1}) = r((ST)(S^{-1})) = r(S^{-1}(ST)) = r((S^{-1}S)T) = r(T)$.

Remark 4.79 *$S, T \in A(V)$ and if S is regular then STS^{-1} and T have same minimal polynomial.*

Characteristic roots:

Definition 4.80 *If $T \in A(V)$, then $\lambda \in F$ is called characteristics roots (or Eigen value of T) if $\lambda - T$ is singular.*

Theorem 4.81 *The element $\lambda \in F$ is a characteristics roots of $T \in A(V)$ iff for some $v \neq 0$ in $V, vT = \lambda v$.*
Proof: Suppose λ is a characteristic root of T. Then $\lambda - T$ is singular. By Theorem 4.69, there exists a $v \neq 0$ in V such that $v(\lambda - T) = 0 \Rightarrow \lambda v - vT = 0 \Rightarrow \lambda v = vT$. Conversely, assume that there is a vector $v \neq 0$ in V such that $vT = \lambda v \Rightarrow \lambda v - vT = 0 \Rightarrow v(\lambda - T) = 0$. By Theorem 4.69, $\lambda - T$ is singular. $\therefore$ λ is the characteristic root of T.

Lemma 4.82 *If $\lambda \in F$ is a characteristic root of $T \in A(V)$, then for any polynomial $q(x) \in F[x]$, $q(\lambda)$ is a characteristic root of $q(T)$.*
Proof: Let $q(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + ... + \alpha_m$. Suppose $\lambda \in F$ is a characteristic root of $T \in A(V)$. Then by Theorem 4.81, there is a non-zero vector $v \in V$ such that $vT = \lambda v$ .....(1)
To Prove: $q(\lambda)$ is characteristic root of $q(r)$, it is enough to prove that $vq(T) = q(\lambda)v, v \neq 0$ in V. Now $vT^2 = (vT)T = (\lambda v)T = \lambda(vT) = \lambda(\lambda v) = \lambda^2 v$. Similarly, $vT^3 = \lambda^3 v$. In general, $vT^k = \lambda^k v$ for all positive integer k. Now,

$$\begin{aligned} v(q(T)) &= v(\alpha_0 T^m + \alpha_1 T^{m-1} + ... + \alpha_m) \\ &= v(\alpha_0 T^m) + v(\alpha_1 T^{m-1}) + ... + v(\alpha_m) \\ &= \alpha_0(vT^m) + \alpha_1(vT^{m-1}) + ... + \alpha_m v \\ &= \alpha_0(\lambda^m v) + \alpha_1(\lambda^{m-1} v) + ... + \alpha_m v \\ &= (\alpha_0 \lambda^m + \alpha_1 \lambda^{m-1} + ... + \alpha_m)v \\ &= (q(\lambda))v. \end{aligned}$$

$v(q(T)) = (q(\lambda))v \; \forall v \neq 0$ in V. $\therefore$ $q(\lambda)$ is a characteristic root of $q(T)$.

Theorem 4.83 *If $\lambda \in F$ is a characteristic root of $T \in A(V)$, then λ is a root of minimal polynomial of T. In particular, T only has a finite number of characteristic root in F.*
Proof: Let $p(x) = \alpha_0 x^m + \alpha_1 x^{m-1} + ... + \alpha_m$ be the minimal polynomial of T over F. Then $p(T) = 0$ (i.e.) $\alpha_0 T^m + \alpha_1 T^{m-1} + ... + \alpha_m$.....(*)
Since λ is a characteristic root of T. Then by Theorem 4.81, there is $v \neq 0$ in V such that $vT = \lambda v$..... (1)
We have to show that $p(\lambda)v = vp(T)$. Now, $vT^2 = (vT)T = (\lambda v)T = \lambda(vT) = \lambda(\lambda v) = \lambda^2 v$. Similarly $vT^3 = \lambda^3 v$. In general $vT^k = \lambda^k v$ (2) for all positive integer k.....(2)

$$\begin{aligned} v(p(T)) &= v(\alpha_0 T^m + \alpha_1 T^{m-1} + ... + \alpha_m) \\ &= v(\alpha_0 T^m) + v(\alpha_1 T^{m-1}) + ... + v(\alpha_m) \\ &= \alpha_0(vT^m) + \alpha_1(vT^{m-1}) + ... + \alpha_m v \\ &= \alpha_0(\lambda^m v) + \alpha_1(\lambda^{m-1} v) + ... + \alpha_m v \\ &= (\alpha_0\lambda^m + \alpha_1\lambda^{m-1} + ... + \alpha_m)v \\ &= (p(\lambda))v.....(3) \end{aligned}$$

$p(\lambda)$is a characteristic root of $p(T)$. (3) $\Rightarrow v \cdot 0 = p(\lambda)v$ (by *) $\Rightarrow p(\lambda) = 0$. $\therefore$ λ is the root of the minimal polynomial of T and degree of $p(x) \leq n^2$ (by Theorem 4.53) where $n = dim_F(V)$. $\therefore$ T has only a finite number of characteristic root in F.

Lemma 4.84 *If $T, S \in A(V)$ and if S is regular, then T and STS^{-1} has the same minimal polynomial.*
Proof: First we shall show that for any polynomial $q(x) \in F[x], q(STS^{-1}) = S(q(T))S^{-1}$..... (1)
For let $q(x) = \alpha_0 + \alpha_1 x^1 + \alpha_2 x^2 + ... + \alpha_m x^m$. Now, $(STS^{-1})^2 = (STS^{-1})(STS^{-1}) = (ST)(S^{-1}S)(TS^{-1}) = (ST)(1)(TS^{-1}) = STTS^{-1} = ST^2S^{-1}$. Similarly we get $(STS^{-1})^k = ST^kS^{-1}$, for every k=1,2,3..... .....(2)

$$\begin{aligned} q(STS^{-1}) &= \alpha_0 + \alpha_1(STS^{-1}) + \alpha_2(STS^{-1})^2 + ... + \alpha_m(STS^{-1})^m \\ &= \alpha_0 + \alpha_1(STS^{-1}) + \alpha_2(ST^2S^{-1}) + ... + \alpha_m(ST^mS^{-1}) \\ &= S(\alpha_0 + \alpha_1 T + \alpha_2 T^2 + ... + \alpha_m T^m)S^{-1} \\ q(STS^{-1}) &= Sq(T)S^{-1}.....(3) \end{aligned}$$

Let $p(x)$ be the minimal polynomial of T over F. Then $p(T) = 0$..... (4)
Now by equation (3), $p(STS^{-1}) = Sp(T)S^{-1} = S(0)S^{-1} = 0 \Rightarrow STS^{-1}$ satisfies the minimal polynomial $p(x)$ of T. Suppose Let $f(x)$be the polynomial of T such that $deg(f(x)) < deg(p(x))$ and $f(STS^{-1}) = 0$. Again by eqn (3), $Sf(T)S^{-1} = f(STS^{-1}) = f(0) = 0 \Rightarrow Sf(T)S^{-1} = 0 \Rightarrow f(T) = 0$ [pre and post multiply by S and S^{-1}]. T satisfy the polynomial $f(x)$ and $deg(f(x)) < deg(p(x))$, which is contradiction to the minimality of $p(x)$.

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 $\lambda_1, \lambda_2, ..., \lambda_k$ respectively 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 $\gamma_2 = \lambda_2 - \lambda_1 \neq 0, \gamma_3 = \lambda_3 - \lambda_1 \neq 0, ..., \gamma_j = (\lambda_j - \lambda_1) \neq 0 \Rightarrow$ $v_2, v_3, ..., v_j$ 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 $T \leq 3$.

Corollary 4.87 *If $T \in A(V)$ and if $dim(V) = n$ then T can have at most n distinct characteristic root in F.*
Proof: Let$\lambda_1, \lambda_2, ..., \lambda_m$ be the distinct characteristic root of T. To prove: $m \leq n$. Let $v_1, v_2, ..., v_m$ be the characteristic vector T belonging to the characteristic roots $\lambda_1, \lambda_2, ..., \lambda_m$. By Theorem 4.86, $v_1, v_2, ..., v_m$ are linearly independent. Since the $dim(V) = n$, the number of elements in any linearly independent set in it will be less than or equal to n, $m \leq n$.

Corollary 4.88 *If $T \in A(V)$ and if $dim_F(V) = n$ and if T has n distinct characteristic root in F, then there is a basis of V over F which consist of characteristic vector of T.*
Proof: Let $\lambda_1, \lambda_2, ..., \lambda_n$ be distinct characteristic roots of T. Let $v_1, v_2, ..., v_n$ be the characteristics roots $\lambda_1, \lambda_2, ..., \lambda_n$. We first claim that $v_1, v_2, ..., v_n$ are distinct for $1 \leq i, j \leq n$. Suppose $v_i = v_j \Rightarrow v_iT = v_jT \Rightarrow \lambda_i v_i = \lambda_j v_i \Rightarrow (\lambda_i - \lambda_j)v_i = 0 \Rightarrow \lambda_i - \lambda_j = 0 (\because v_i \neq 0) \Rightarrow \lambda_i = \lambda_j \Rightarrow\Leftarrow$ (Since $\lambda_1, \lambda_2, ..., \lambda_n$ distinct characteristic root). Hence $v_1, v_2, ..., v_n$ are distinct. By Theorem 4.86, $v_1, v_2, ..., v_n$ are linearly independent. Let $v \in V$, since $dim_F(V) = n$ any subset of $n + 1$ vectors are linearly dependent. (i.e.) $v_1, v_2, ..., v_n, v$ are linearly dependent. $\therefore$ there exists scalars $\alpha_1, \alpha_2, ..., \alpha_n, \alpha$ not all zero such that $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n + \alpha v = 0$. In particular $\alpha \neq 0$,

$$\begin{aligned}
\alpha v &= -(\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n) \\
v &= -\frac{1}{\alpha}(\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n) \\
\Rightarrow v &= (-(\alpha^{-1}\alpha_1)v_1 + (-\alpha^{-1}\alpha_2)v_2 + ... + (-\alpha^{-1}\alpha_n)v_n) \\
\Rightarrow v &= \beta_1 v_1 + \beta_2 v_2 + ... + \beta_n v_n \text{ where } \beta_i = -\alpha^{-1}\alpha_i, i = 1, 2, ..., n.
\end{aligned}$$

$\Rightarrow v \in L(S) \Rightarrow \{v_1, v_2, ..., v_n\}$ spans V. $\therefore$ $\{v_1, v_2, ..., v_n\}$ is a basis of V.

Canonical forms:
Triangular forms: Since the basis used at any time is completely at our choice for a given linear transformation T. It is natural for as to seek a basis in which the matrix of D will be a particular nice forms. Such nice forms of matrices as canonical forms. In this section we are going to see one such nice form called triangular form.

Definition 4.89 *The linear transformations $S, T \in A(V)$ are said to be similar if there exists an invertible element $C \in A(V)$ such that $T = CSC^{-1}$. The definition already defined interms of matrices as $m_2(T) = Cm_1C^{-1} \Rightarrow A = CBC^{-1}$. Two matrices $A, B \in F_n$ are similar if there exist an invertible element $C \in F_n$ such that $B = CAC^{-1}$.*

Remark 4.90 *(1) The relation of $A(V)$ defined by similarity is an equivalence relation. (i.e.) $S \sim T \Rightarrow S$ is similar to $T \Rightarrow T = CSC^{-1}$. $\sim$*

is reflexive, symmetric and transitive. $\therefore \sim$ is an equivalence relation. The equivalence class of an element in $A(V)$ under the relation similarity is called the similarity class and is denoted by $[S]$.
(2) For any two given linear transformations to determines whether on not similar is not an easy one. Instead, we try to establish some kind of landmark in each similarity classes of one of these to set if the other is in it, but this procedure is not feasible. To determine if two linear transformation are similar, we need but compute a particular canonical form for each and check if these are the same.

Definition 4.91 *Let W be a subspace of a vector space V. W is said to be invariant under $T \in A(V)$ if $WT \subset W$.*

Lemma 4.92 *If $W \subset V$ is a invariant under T then T induces a linear transformation $\bar{T}$ on V/W defined by $(v+w)\bar{T} = v + W$. If T satisfied the polynomial $q(x) \in F[x]$ then so does $\bar{T}$. If $p_1(x)$ is a minimal polynomial of $\bar{T}$ over F and if $p(x)$ is that for T then $p_1(x)/p(x)$.*
Proof: Part I: Given $T \in A(V) = Hom(V,V)$. (i.e.) $T : V \to V$ is a homomorphism. Let $\bar{V} = V/W = \{v+W | v \in V\}$. Define $\bar{v}\bar{T} = (v+W)\bar{T} = vT + W$. Suppose $\bar{v}_1 = \bar{v}_2, \bar{v}_1, \bar{v}_2 \in V/W$

$$\begin{aligned}
&\Rightarrow v_1 + W = v_2 + W \\
&\quad \Rightarrow v_1 = v_2 \in W [\because a + H = b + H \Rightarrow a - b \in H] \\
&\Rightarrow (v_1 - v_2)T \in WT \\
&\Rightarrow v_1T - v_2T \in WT \\
&\Rightarrow v_1T + W = v_2T + W \\
&\Rightarrow (v_1 + W)\bar{T} = (v_2 + W)\bar{T} \\
&\quad \Rightarrow \bar{v_1}\bar{T} = \bar{v_2}\bar{T}
\end{aligned}$$

$\therefore$ $\bar{T}$ is well defined.
Now,

$$\begin{aligned}
(\bar{v}_1 + \bar{v}_2)\bar{T} &= ((v_1 + W) + (v_2 + W))\bar{T} \\
&= (v_1 + v_2)T + W \\
&= v_1T + v_2T + W \\
&= (v_1T + W) + (v_2T + W) \\
&= (v_1 + W)\bar{T} + (v_2 + W)\bar{T} \\
&= \bar{v}_1\bar{T} + \bar{v}_2\bar{T}
\end{aligned}$$

$$\begin{aligned}(\alpha\bar{v_1})\bar{T} &= (\alpha(v_1)+W)\bar{T}\\ &= (\alpha v_1+W)\bar{T}\\ &= (\alpha v_1)T+W\\ &= \alpha(v_1T)+W\\ &= \alpha(v_1T+W)\\ &= \alpha((v_1+W)\bar{T})\\ &= \alpha(\bar{v}_1\bar{T})\end{aligned}$$

$\therefore$ $\bar{T}$ defines linear transformation on $\bar{V}$.
Part II: Suppose that T satisfies $q(x)=\alpha_0+\alpha_1x+\alpha_2x^2+...+\alpha_kx^k\in F[x]$. Then $q(T)=0$. (i.e.) $\alpha_0+\alpha_1T+\alpha_2T^2+.....+\alpha_kT^k=0.....$ (1)
Claim: $\overline{q(T)}=q(\bar{T})$ we prove that $q(\bar{T})=0$. Let $\bar{v}=v+W\in V/W=\bar{V}$

$$\begin{aligned}\bar{v}\overline{T^2} &= (v+w)\bar{T}^2\\ &= vT^2+W\\ &= (vT)T+W\\ &= (vT+W)\bar{T}\\ &= ((v+W)\bar{T})\bar{T}\\ &= (v+W)\bar{T}^2=(\bar{v})\bar{T}^2\\ \Rightarrow \overline{T^2} &= \bar{T}^2\end{aligned}$$

similarly $\overline{T^k}=\bar{T}^k$.....(2), for any $k>0$
Consequently for any polynomial $q(x)\in F[x], \overline{q(T)}=q(\bar{T})$, for

$$\begin{aligned}q(\bar{T}) &= \alpha_0+\alpha_1\bar{T}+\alpha_2\bar{T}^2+...+\alpha_k(\bar{T}^k)\\ &= \alpha_0+\alpha_1\bar{T}+\alpha_2\bar{T}^2+...+\alpha_k(\bar{T}^k)\\ &= \overline{\alpha_0+\alpha_1T+\alpha_2T^2+...+\alpha_kT^k}\\ &= \overline{q(T)}\\ q(\bar{T}) &= \overline{q(T)}\end{aligned}$$

for any $q(x)\in F[x]$ with $q(T)=0\Rightarrow q(\bar{T})=\overline{q(T)}=0$. $\therefore$ T satisfies $q(x)\in F[x]$.
Part III: Suppose $p_1(x)$ is minimal polynomial for $\bar{T}$ (i.e.) $p_1(x)=0$. Also given that $p(x)$ is minimal polynomial for T. (i.e.) $p(T)=0$. We have to show that $p_1(x)/p(x)$. Now $p(\bar{T})=\overline{p(T)}=\bar{0}\Rightarrow p(\bar{T})=\bar{0}=0$. $p(x)$ satisfies $\bar{T}$. By Remark 4.54, $p_1/p(x)$ (here $p(x)$ and $h(x)=p(x)=p_1(x)$).

Definition 4.93 ***Triangular matrix*** *A matrix M is called triangular if the entries above the main diagonal are zero (or) equivalently T is a linear transformation on V over F matrix of T in the basis $v_1,v_2,...,v_n$ are*

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 $W = \{\alpha v_1 | \alpha \in F\}$ then W is a subspace of V of dimension 1. Then,

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

$\Rightarrow WT \subset W$. $\therefore W$ 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 polynomial of 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 $\bar{v}_2, \bar{v}_3, ..., \bar{v}_n$ over $\bar{V}$ over F in which the matrix of $\bar{T}$ is triangular

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

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

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

(i.e.) the basis $v_1, v_2, ..., v_n$ 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 $\{v_1, v_2, ..., v_n\}$ is triangular.

Theorem 4.95 *If V is a dimensional over F and $T \in A(V)$ has matrix $m_1(T)$ in the basis $v_1, v_2, ..., v_n$ 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 $i = 1, 2, ..., n$ 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

transformation T on F^n whose matrix in the basis is precisely A.

$$\begin{aligned} v_1 &= (1, 0, ...0) \\ v_2 &= (0, 1, ...0) \\ &\cdot \\ &\cdot \\ &\cdot \\ v_n &= (0, 0, ...1) \end{aligned}$$

The characteristic root of T, being those of A are all in F. Hence by Theorem 4.94 there is a basis of F^n in which the matrix of T is triangular. However by Theorem 4.95 This changes of basis merely changes the matrix basis into CAC^{-1} for a suitable $C \in F_n$

Remark 4.97 *characteristic root of triangular matrix is diagonal matrix.*

Theorem 4.98 *If V is n dimensional over F and if $T \in A(V)$ has all its characteristic roots in F, then T satisfies a polynomial of degree n over F.*
Proof: Since V is n-dimensional over F and $T \in A(V)$ has all its root in F.
$\therefore$ By Theorem 4.94, we can find a basis $v_1, v_2, ..., v_n$ such that

$$\begin{aligned} v_1T &= \lambda_1 v_1 \\ v_2T &= \alpha_{21}v_1 + \lambda_2 v_2 \\ v_3T &= \alpha_{31}v_1 + \alpha_{32}v_2 + \lambda_3 v_3 \\ &\cdot \\ &\cdot \\ &\cdot \\ v_iT &= \alpha_{i1}v_1 + \alpha_{i2}v_2 + ... + \lambda_{ii-1}v_{i-1} + \lambda_i v_i \ for\ i = 1, 2, 3, ..., n. \end{aligned}$$

Equivalently,

$$\begin{aligned} v_1T - \lambda_1 v_1 &= 0 \\ (i.e.)\ v_1(T - \lambda_1) &= 0 \\ v_2T - \alpha_{21}v_1 + \lambda_2 v_2 &= 0 \\ (i.e.)\ v_2(T - \lambda_2) &= \alpha_{21}v_1 \\ v_3(T - \lambda_3) &= \alpha_{31}v_1 + \alpha_{32}v_2 \\ &\cdot \\ &\cdot \\ &\cdot \\ v_i(T - \lambda_i) &= \alpha_{i1}v_1 + \alpha_{i2}v_2 + ... + \alpha_{ii-1}v_{i-1} \ for\ i = 1, 2, ..., n \cdots (1) \end{aligned}$$

Now, $v_2(T-\lambda_2)(T-\lambda_1) = (v_2(T-\lambda_2))(T-\lambda_1) = \alpha_{21}v_1(T-\lambda_1) = \alpha_{21}(v_1(T-\lambda_1)) = \alpha_{21}(0) = 0$..... (2)

$$But\ (T-\lambda_2)(T-\lambda_1) = (T-\lambda_1)(T-\lambda_2)$$
$$v_1(T-\lambda_2)(T-\lambda_1) = v_1((T-\lambda_1)(T-\lambda_2)) = 0\ (by\ (1))$$
$$Similarly\ v_1((T-\lambda_3)(T-\lambda_2)(T-\lambda_1)) = 0$$

Continuing this type of computation fields,

$$v_1((T-\lambda_i)(T-\lambda_{i-1})\cdots(T-\lambda_2)(T-\lambda_1)) = 0$$
$$v_2((T-\lambda_i)(T-\lambda_{i-1})\cdots(T-\lambda_2)(T-\lambda_1)) = 0$$
$$\vdots$$
$$v_i((T-\lambda_i)(T-\lambda_{i-1})\cdots(T-\lambda_2)(T-\lambda_1)) = 0, i = 1,2,...,n$$
$$for\ i = n,\ let\ S = (T-\lambda_n)(T-\lambda_{n-1})\cdots(T-\lambda_2)(T-\lambda_1)$$
$$v_1S = v_1((T-\lambda_n)(T-\lambda_{n-1})\cdots(T-\lambda_2)(T-\lambda_1)) = 0$$
$$v_2S = v_2((T-\lambda_n)(T-\lambda_{n-1})\cdots(T-\lambda_2)(T-\lambda_1)) = 0$$
$$Similarly\ v_3S = 0, ..., v_nS = 0$$
$$v_2S = v_3S = ... = v_nS = 0$$

The matrix S satisfies $v_1S = 0, v_2S = 0, ..., v_nS = 0$. Since S anihilates a basis of V, S must anihilates all of V. $\therefore\ S = 0$.

$$(T-\lambda_n)(T-\lambda_{n-1})\cdots(T-\lambda_2)(T-\lambda_1) = 0 \text{.....(3)}$$
$$Let\ p(x) = (x-\lambda_n)(x-\lambda_{n-1})\cdots(x-\lambda_2)(x-\lambda_1)$$
$$p(T) = (T-\lambda_n)(T-\lambda_{n-1})\cdots(T-\lambda_2)(T-\lambda_1) = 0\ by(3)$$

Hence T satisfies the polynomial of degree n over F.

Canonical Form:

The relation on $A(V)$ defined by similarly is an equivalence relation. The equivalence class of the element of $A(V)$ will be called its similarity class. Given two linear transformation, by scanning the similarity class of one we could determine whether or not they are similar. But this procedure is not feasible one. Instead we try to establish some kind of land mark in each similarity class, and the way of going from any element in the class to this landmark. We shall prove the existence of linear transformation in each similarity class whose matrix in some basis of a particular nice form. These matrices will be called canonical forms. For example, triangular form is a canonical form.

Trace and Transpose

Definition 4.99 *The trace of a matrix A is the sum of the elements on the main diagonal of A we shall write trace of A as trA (i.e.) if $A = (\alpha_{ij})$ $i, j = 1, 2, ..., n$. Then*

$$trA = \sum_{i=1}^{n} \alpha_{ii}$$

Lemma 4.100 *For $A, B \in F_n$ and $\lambda \in F$,*

1. *Trace of $\lambda A = \lambda(trA)$.*

2. *$tr(A + B) = trA + trB$.*

3. *$tr(AB) = tr(BA)$.*

Proof: (1) Let

$$\begin{aligned} A &= (\alpha_{ij})\ i, j = 1, 2, ...n \\ \lambda A &= (\lambda\alpha_{ij})\ i, j = 1, 2, ...n \\ tr\lambda A &= \sum_{i=1}^{n} \lambda\alpha_{ij} \\ &= \lambda \sum_{i=1}^{n} \alpha_{ij} \\ &= \lambda(trA) \end{aligned}$$

(2) Let $(\alpha_{ij}) \in F_n, B = (\beta_{ij}) \in F_n$
Then $A + B = (\alpha_{ij}) + (\beta_{ij}) = (\gamma_{ij}),\ i, j = 1, 2, ..., n$ where $(\gamma_{ij}) = \alpha_{ij} + \beta_{ij},\ i, j = 1, 2, ..., n$.

$$\begin{aligned} tr(A + B) &= tr(\gamma_{ij}) \\ &= \sum_{i=1}^{n} \gamma_{ii} \\ &= \sum_{i=1}^{n} (\alpha_{ij} + \beta_{ii}) \\ &= \sum_{i=1}^{n} \alpha_{ii} + \sum_{i=1}^{n} \beta_{ii} \\ &= trA + trB \end{aligned}$$

(3) Let $A = (\alpha_{ij}) \in F_n, B = (\beta_{ij}) \in F_n$. Then, $AB = (\gamma_{ij})$, where

$$\begin{aligned}
\gamma_{ij} &= \sum_{i=1}^{n} \alpha_{ik}\beta_{kj} \\
tr(AB) &= tr(\gamma_{ij}) \\
&= \sum_{i=1}^{n} \gamma_{ii} \\
&= \sum_{i=1}^{n}(\sum_{k=1}^{n} \alpha_{ik}\beta_{ki}).....(i) \\
Let\ BA = (\lambda_{ij}),\ where\ \lambda_{ij} &= \sum_{k=1}^{n} \alpha_{ik}\beta_{kj} \\
tr(BA) &= tr(\lambda_{ij}) \\
&= \sum_{i=1}^{n} \lambda_{ii} \\
&= \sum_{i=1}^{n}(\sum_{k=1}^{n} \beta_{ik}\alpha_{ki}) \\
from\ (i)\ tr(AB) &= \sum_{i=1}^{n}(\sum_{k=1}^{n} \alpha_{ik}\beta_{ki}) \\
&= \sum_{k=1}^{n}(\sum_{i=1}^{n} \beta_{ki}\alpha_{ik}) \\
&= \sum_{k=1}^{n}(\lambda_{kk}) \\
&= \sum_{i=1}^{n}(\lambda_{ii}) \\
&= tr(BA)
\end{aligned}$$

Definition 4.101 *Let $T \in A(V)$ then the trace of T is the trace of the matrix $M_1(T)$ where $M_1(T)$ is the matrix of T in some basis of V*

Remark 4.102 *The above definition is meaningful and depends only on T and not on any particular basis of V.*

Corollary 4.103 *If A is invertible then $tr(ACA^{-1}) = trC$.*
Proof: Let $B = CA^{-1}$. Then, $tr(A(CA^{-1})) = tr(A(B)) = tr(BA) = tr(CA^{-1}A) = tr(C(AA^{-1})) = tr(C)$.

Lemma 4.104 *If $T \in A(V)$ then $tr(T)$ is the sum of the characteristic root of T.*
Proof: Let $p(x)$ be the minimal polynomial and K be the splitting field

of $p(x)$. In K_n, T can be brought to Jordon from say J, where $J = ATA^{-1}$; $trJ = tr(ATA^{-1}) = tr(AT)A^{-1} = trA^{-1}(AT) = trA^{-1}AT = trT$..... (1)
Since all the characteristic roots of T appears on the main diagonal of J (Jacobian). trJ=Sum of the characteristic root of T. $tr(T)$=Sum of the characteristic root of T. (by (1))

Corollary 4.105 $tr(BAB^{-1}) = trA$.

Remark 4.106 *If T is nilpotent $trT^i = 0\ \forall i \geq 1$.*
Proof: Given T is nilpotent $\Rightarrow$ there exist $k > 0$ such that $t^k = 0$. Let λ be the characteristic root of T then there exist $v \neq 0$ in V such that $vT = \lambda v$. Now, $vT^2 = (vT)T = (\lambda v)T = \lambda(VT) = \lambda(\lambda v) = \lambda^2 v$. Similarly $vT^k = \lambda^k v$ $\Rightarrow 0 = \lambda^k v$ ($\because T^k = 0$) $\Rightarrow \lambda^k = 0 \Rightarrow \lambda = 0$ (multiply by λ^{1-k}). Hence all the characteristic roots of T are 0 (since λ is only characteristic root). But trT = Sum of the characteristic root of $T = 0$. Since T is nilpotent, T^i, for $i \geq 1$ is nilpotent $\Rightarrow trT^i = 0\ \forall i \geq 1$.

Remark 4.107 *Converse of $trT^i = 0, \forall i \geq 1$ then T is nilpotent. The converse need not be true. In general T need not be nilpotent.*

Example 4.108 *Let*

$$T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

be a matrix over the field F of characteristic 2 $\Rightarrow 2a = 0\ \forall a \in F$..... (1) trT= Sum of diagonal element= 1+1=2(1)=0[$\because$ char F=2]. $T^i = T\ \forall i \geq 1$; $trT^i = trT = 0\ \forall i \geq 1$. But T is not nilpotent, since $T^k = T \neq 0\ \forall i$.

Lemma 4.109 *If F is a field of characteristic 0 and if $T \in A(V)$ is there exist $trT^i = 0\ \forall i \geq 1$, then T is nilpotent.*
Proof: Let $p(x) = x^m + \alpha_1 x^{m-1} + ... + \alpha_{m-1}T$ be the minimal polynomial of T. Then,

$$\begin{aligned} p(T) &= 0 \\ \Rightarrow T^m + \alpha_1 T^{m-1} + \alpha_2 T^{m-2} + ... + \alpha_m T^0 &= 0 \\ \Rightarrow tr(T^m + \alpha_1 T^{m-1} + \alpha_2 T^{m-2} + ... + \alpha_m T^0) &= tr(0) \\ \Rightarrow tr(\alpha_m I) &= 0\ [for\ i \geq 1, T^i = 0] \\ \Rightarrow \alpha_m (trI) &= 0 \\ \Rightarrow n\alpha_m = 0\ (where\ n = dim(V)\ and\ trI &= n) \\ \Rightarrow \alpha_m &= 0 (\because F\ is\ char\ 0) \end{aligned}$$

(i.e.) Independent term of minimal polynomial $p(x)$ is zero. $\therefore T$ is singular,by Theorem 4.65. Then there exists $v \neq 0$ in V such that $vT = 0$ (by

Theorem 4.65)$\Rightarrow vT = 0 \cdot v$. (i.e.) 0 is a characteristic root of T. Let K be an extension of F which contains all the characteristic root of T. Now in K_n, T can be brought to the triangular form (since 0 is the characteristic root if T). We have,

$$T = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \beta_2 & \alpha_2 & \cdots & 0 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ \beta_n & \cdot & \cdots & \alpha_n \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ * & T^2 \end{pmatrix}$$

where

$$T^2 = \begin{pmatrix} \alpha_2 & 0 & \cdots & 0 \\ * & \alpha_3 & \cdots & 0 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ * & * & \cdots & \alpha_n \end{pmatrix} is\ n-1 \times n-1\ matrix$$

$$T_2^K = \begin{pmatrix} 0 & 0 \\ * & T_2^k \end{pmatrix}$$

$\Rightarrow 0 = trT^k = trT_2^k \Rightarrow trT_2^k = 0\ \forall k \geq 1$. By using induction on dimension (or repeating the argument on T_2. We see that all the characteristic roots are zero)
$\alpha_2 = \alpha_3 = ... = \alpha_n = 0 \Rightarrow T$ is brought to the triangular form and all its diagonal elements are zero.

$$T = \begin{pmatrix} 0 & \cdot & \cdots & 0 \\ * & \cdot & \cdots & 0 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ * & \cdot & \cdots & 0 \end{pmatrix}$$

$\therefore T^n = 0$. Hence T is nilpotent.

Lemma 4.110 *If F is of characteristic 0 and if $S, T \in A(V)$ are such that $ST - TS$ commutes with S then $ST - TS$ is nilpotent.*

Proof: Given F is of characteristic 0 Let $k \geq 1$ then,

$$\begin{aligned}(ST-TS)^k &= (ST-TS)^{k-1}(ST-TS)\\ &= (ST-TS)^{k-1}(ST) - (ST-TS)^{k-1}(TS)\\ &= S((ST-TS)^{k-1}T) - ((ST-TS)^{k-1}T)S\\ &= SB - BS \text{ where } B = (ST-TS)^{k-1}T\\ \Rightarrow tr((ST-TS)^k) &= tr(SB-BS)\\ &= tr(SB) - tr(BS)\\ &= tr(BS-BS)\\ &= 0\end{aligned}$$

$\therefore tr((ST-TS)^k) = 0$ $k \geq 0$. $\therefore$ By Lemma 4.109 $ST-TS$ is nilpotent.

Definition 4.111 ***Transpose:*** *If $A = (\alpha_{ij}) \in F_n$ then the transpose of A, written as A', is the matrix $A' = (\gamma_{ij})$ where $\gamma_{ij} = \alpha_{ji}$ $\forall i$ and j.*

Lemma 4.112 *For all $A, B \in F_n$,*

1. $(A')' = A$
2. $(A+B)' = A' + B'$
3. $(AB)' = B'A'$

Proof: (1) Let $A = (\alpha_{ij}) \in F_n$. Then $A' = (\beta_{ij})$ where $\beta_{ij} = \alpha_{ji}$
$(A')' = (\gamma_{ij})$ where $\gamma_{ij} = \beta_{ji} \Rightarrow (A')' = (\beta_{ji}) = \alpha_{ij} = A$.
(2) Let $A = (\alpha_{ij}) \in F_n$; $B = (\beta_{ij}) \in F_n$

$$\begin{aligned}(A+B) &= (\alpha_{ij} + \beta_{ij}) = (\gamma_{ij})\\ (A+B)' &= (\delta_{ij}) \text{ where } \delta_{ij} = \gamma_{ji}\\ &= \gamma_{ji} = (\alpha_{ji} + \beta_{ji})\\ &= A' + B'\end{aligned}$$

(3) Let $A = (\alpha_{ij}) \in F_n$ and $B = (\beta_{ij}) \in F_n$

$$\begin{aligned}
A' = (\gamma_{ij}) \text{ where } \gamma_{ij} &= \alpha_{ji} \\
B' = (\delta_{ij}) \text{ where } \delta_{ij} &= \beta_{ji} \\
AB = (\lambda_{ij}) \text{ where } \lambda_{ij} &= \sum_{k-1}^{n} \alpha_{ik}\beta_{kj} \\
(AB)' = (\mu_{ij}) \text{ where } \mu_{ij} &= \lambda_{ji} \\
B'A' = (\xi_{ij}) \text{ where } \xi_{ij} &= \sum_{k-1}^{n} \delta_{ik}\gamma_{kj} \\
\xi_{ij} &= \sum_{k-1}^{n} \beta_{ki}\alpha_{jk} \\
&= \sum_{k-1}^{n} \alpha_{jk}\beta_{ki} \\
\xi_{ij} &= \lambda_{ji} \\
&= \mu_{ij} \\
B'A' &= (AB)'
\end{aligned}$$

Definition 4.113 *(i) A is said to be symmetric matrix if $A' = A$*
For example,

$$\begin{pmatrix} d & o & g \\ o & n & e \\ g & e & t \end{pmatrix}$$

(ii) A said to be skew symmetric matrix if $A' = -A$
For example,

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Definition 4.114 ***Adjoint Operator:*** *Let F be a field of complex number. Let $A = (\alpha_{ij}) \in F_n$. Then $A^* = (\gamma_{ij}$ where $\gamma_{ij} = \overline{\alpha_{ji}}$ the complex conjugate of α_{ji} so here $*$ is usually called the hermitian adjoint on F_n, denoted by A^* defined as $A^* = (\gamma_{ij})$ where $\gamma_{ij} = \overline{\alpha_{ji}}$. Let $A = (\alpha_{ij}) \in F$ the hermitian adjoint of A on F_n is defined as $A^* = \gamma_{ij}$ where $\gamma_{ij} = \overline{\alpha_{ji}}$.*

Remark 4.115 *Any matrix can be uniquely written as the sum of the symmetric an skew symmetric matrices for $A = \frac{1}{2}(A + A') + \frac{1}{2}(A - A')$.*

Definition 4.116 ***Adjoint mapping:*** *A mapping $*$ from F_n into F_n is called an adjoint if*

1. $(A^*)^* = A$

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

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

Example 4.120

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

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

corresponding to λ then,

$$\begin{aligned}
AX &= \lambda X \\
\Rightarrow \bar{X}'(AX) &= \bar{X}'(\lambda X) \\
\Rightarrow \bar{X}'AX &= \lambda \bar{X}'X \\
\Rightarrow (\bar{X}'AX)' &= \lambda \bar{X}'X \\
\Rightarrow X'A'\bar{X} &= \lambda \bar{X}'X \\
\Rightarrow \overline{(X'A'\bar{X})} &= \overline{(\lambda \bar{X}'X)} \\
\Rightarrow \bar{X}'\bar{A}'\bar{\bar{X}} &= \bar{\lambda}X'\bar{X} \\
\Rightarrow \bar{X}'\bar{A}'X &= \bar{\lambda}X'\bar{X} \\
\Rightarrow \bar{X}'AX &= \bar{\lambda}X'\bar{X} \ [\because \bar{A}' = A^* = A \text{ since hermitian}] \\
\Rightarrow \bar{X}'\lambda X &= \bar{\lambda}X'\bar{X} \\
\Rightarrow (\lambda \bar{X}'X) &= \bar{\lambda}(X'\bar{X}) \\
&= \bar{\lambda}(\bar{X}'X) \\
\Rightarrow (\lambda - \bar{\lambda})(\bar{X}'X) &= 0
\end{aligned}$$

$But\ \bar{X}'X = \bar{x_1}x_1 + \bar{x_2}x_2 + ... + \bar{x_n}x_n = \sum_{i=1}^{n} |x_i|^2 \neq 0$

$\Rightarrow (\lambda - \bar{\lambda}) = 0 \Rightarrow \lambda = \bar{\lambda}.\ \therefore\ \lambda$ is real.

Result 4.122 *If $A \in F_n$ then all the characteristic roots of AA^* are non-negative*

5. UNIT V

Extension Fields

Definition 5.1 *Let F be a field; a field K is said to be an extension of F if $K \supset F$. Equivalently, K is an extension of F if F is a subfield of K.*

Remark 5.2 *Throughout this chapter F will denote a given field and K an extension of F.*

Example 5.3 .

1. *$\mathbb{R}$ is an extension of $\mathbb{Q}$.*
2. *$\mathbb{C}$ is an extension of $\mathbb{R}$.*
3. *Any field is an extension of itself.*

Remark 5.4 .

1. *Extension field K can be regarded as a vector space over F. But a vector space over F cannot be considered as an extension.*
2. *If K is an extension of F, then under the ordinary field operation in K, K is a vector space over F. As a vector space we may talk about linear independence, dependence, dimensions, basis etc. in K relative to F.*

Definition 5.5 *Let F be a given field and K be an extension of F. The degree of K over F is the dimension of K as a vector space over F. (i.e.) degree of K over F=dimension of K over $F = dim_F(K)$.*

Note 5.6 *$[K : F]$ will denote the degree of K over F.*

Definition 5.7 *When K is finite dimensional as a vector space over F we say that $[K : F]$ is finite and we call K is finite extension of F.*

Example 5.8 .

1. *If F is an arbitrary field then clearly, F is a subfield of F. Every field F can be regarded as an extension of itself moreover, F can be regarded as a vector space over F. Here the set $S = \{1\}$ consisting of only the unity of F. S is linearly independent and $L(S) = F$. $\therefore$ S forms a basis of F over F. Then $dim_F(F)$=1 (i.e.) $[F : F]$=1. Here F is finite extension of F.*

2. *Since the field of complex numbers $\mathbb{C}$ contains the field of real numbers $\mathbb{R}$, $\mathbb{C}$ is an extension of $\mathbb{R}$. consider the set $S = 1, i$ of complex numbers. Claim: S is a bases of $\mathbb{C}$ over $\mathbb{R}$. Let $a, b \in \mathbb{R}$*
Now,

$$\begin{aligned} a + ib = a \cdot 1 + bi = 0 = 0 + i0 \\ \Rightarrow a \cdot 1 + b \cdot i = 0 \cdot 1 + 0 \cdot i \\ \Rightarrow a = 0, b = 0 \\ \Rightarrow S \text{ is Linearly independent.....(1)} \end{aligned}$$

Let $a + ib$ be an arbitrary element in $\mathbb{C}$. Now $a + ib = a \cdot 1 + bi$. (i.e.) Any element in $\mathbb{C}$ can be uniquely written as a linear combination of 1 and $i \Rightarrow L(S) = \mathbb{C}$..... (2)
From (1) and (2), S forms a basis of $\mathbb{C}$ over $\mathbb{R}$
$\Rightarrow dim_{\mathbb{R}}\mathbb{C} = 2 \Rightarrow [\mathbb{C} : \mathbb{R}] = 2$. $\therefore \mathbb{C}$ is an finite extension of $\mathbb{R}$.

3. *$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a field with respect to addition and multiplication. Also $\mathbb{Q}$ set of all rational numbers is a field with respect to addition and multiplication. Clearly $\mathbb{Q}$ is a subfield of $\mathbb{Q}\sqrt{2}$. (i.e.) $\mathbb{Q}(\sqrt{2})$ is an extension of $\mathbb{Q}$. Consider the set $S = \{1, \sqrt{2}\}$. Claim: S is Linearly Independent*

$$\begin{aligned} a + b\sqrt{2} = 0 \\ \Rightarrow a + b\sqrt{2} = 0 + 0\sqrt{2} \\ \Rightarrow a = 0, b = 0 \Rightarrow S \text{ is Linearly Independent.....(1)} \end{aligned}$$

Claim: S spans $\mathbb{Q}(\sqrt{2})$. Let $a + b\sqrt{2}$ be any element in $\mathbb{Q}(\sqrt{2})$ and $a + b\sqrt{2} = a \cdot 1 + b \cdot \sqrt{2}$. $\therefore L(S) = \mathbb{Q}(\sqrt{2})$.....(2)
From (1) and (2), S forms a basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ (i.e.) $dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}) = 2$. $\therefore$ $\mathbb{Q}(\sqrt{2})$ is a finite extension of $\mathbb{Q}$.

4. *Consider an indeterminate x over a field F. Let K be the field of Quotients of $F[x]$. Then K is an extension of F. For any $\alpha_0, \alpha_1 ..... \alpha_n \in F$ $\alpha_0 \cdot 1 + \alpha_1 \cdot x + ... + \alpha_n x^n + ... = 0 = 0 + 0 \cdot x + 0 \cdot x^2 + ... \Rightarrow \alpha_i = 0 \ \forall i$. The set $S = \{1, x, x^2, ..., x^n, x^{n+1}, ...\}$. It is an infinite subset of K which forms a basis of K over F. Consequently, $[K : F]$ is infinite.*

Theorem 5.9 *If L is a finite extension of K and K is a finite extension of F then L is a finite extension of F.*
Proof: Let $[L : K] = m$ and let $[K : F] = n$. Since $[L : K] = m, dim_K(L) = m$
Let $\{v_1, v_2, ..., v_m\}$ be a basis of L over K. Similarly, let $\{w_1, w_2 .... w_n\}$ be a basis of K over F. Let $S = \{v_i w_j | i = 1, 2, ..., m, j = 1, 2, ..., n\}$. To Prove: S forms a basis of L over F. First we must show that S generates L (i.e.) To Prove: $L(S) = L$. (i.e.) to show that every element in L can be written

as the linear combination of elements of S with the coefficients in F. Let $t \in L$ be any element. Since every element in L is a linear combination of $\{v_1, v_2, ..., v_m\}$ with coefficient in K, in particular $t = k_1v_1, k_2v_2, ..., k_mv_m$, where $k_i \in K$..... (1)
Since $[K : F] = n$ and $\{w_1, w_2, ..., w_n\}$ forms a basis of K over F, any element of K can be written as the linear combination of $\{w_1, w_2, ..., w_n\}$ with the coefficients in F

$$\begin{aligned} k_1 &= f_{11}w_1 + f_{12}w_2 + ... + f_{1n}w_n \\ k_2 &= f_{21}w_1 + f_{22}w_2 + ... + f_{2n}w_n \\ &\vdots \\ k_m &= f_{m1}w_1 + f_{m2}w_2 + ... + f_{mn}w_n, f_{ij} \in F.....(*) \end{aligned}$$

Substitute these values of $k_1, k_2, ..., k_n$ in (1)

$$\begin{aligned} t &= (f_{11}w_1 + f_{12}w_2 + ... + f_{1n}w_n)v_1 + (f_{21}w_1 + f_{22}w_2 + ... + f_{2n}w_n)v_2 + ... \\ &\quad + (f_{m1}w_1 + f_{m2}w_2 + ... + f_{mn}w_n)v_m, \ where \ f_{ij} \in F, i = 1, 2, ..., m; \\ &\quad j = 1, 2, ..., n \\ t &= f_{11}w_1v_1 + f_{12}w_2v_1 + ... + f_{1n}w_nv_1 + f_{21}w_1v_2 + f_{22}w_2v_2 + ... + f_{2n}w_nv_2 \\ &\quad + ... + f_{m1}w_1v_m + f_{m2}w_2v_m + ... + f_{mn}w_nv_m \\ t &= f_{11}(w_1v_1) + f_{12}(w_2v_1) + ... + f_{1n}(w_nv_1) + f_{21}(w_1v_2) + f_{22}(w_2v_2) + ... \\ &\quad + f_{2n}(w_nv_2) + ... + f_{m1}(w_1v_m) + f_{m2}(w_2v_m) + ... + f_{mn}(w_nv_m).....(A) \end{aligned}$$

(i.e.) t is a linear combination of $\{v_jw_j | i = 1, 2, ...m, j = 1, 2, ...n\}$ over F
$\therefore L(S) = L$.....(2)
Next we have to show that the elements of the set
$S = \{v_jw_j / i = 1, 2, ..., m, j = 1, 2, ..., n\}$ are linearly independent over F.
Suppose, $f_{11}(w_1v_1) + f_{12}(w_2v_1) + ...f_{1n}(w_nv_1) + f_{21}(w_1v_2) + f_{22}(w_2v_2) + ...f_{2n}(w_nv_2) + ... + f_{m1}(w_1v_m) + f_{m2}(w_2v_m) + ... + f_{mn}(w_nv_m) = 0$..... (3)
Claim that $f_{ij} = 0 \forall i = 1, 2, ...m, j = 1, 2, ...n$. Regrouping the (3) we get,
$(f_{11}w_1 + f_{12}w_2 + ... + f_{1n}w_n)v_1 + (f_{21}w_1 + f_{22}w_2 + ... + f_{2n}w_n)v_2 + ... + (f_{m1}w_1 + f_{m2}w_2 + ... + f_{mn}w_n)v_m = 0$..... (4)
(i.e.) $k_1v_1 + k_2v_2 + ... + k_mv_m = 0, k_i \in K$. But, by our assumption $\{v_1, v_2, ..., v_m\}$form the basis of L over K so $v_1, v_2, ..., v_n$ are linearly independent over K

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

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

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

(i.e.) $f_{ij} \forall i = 1, 2, ..., m, j = 1, 2, ..., n.$ $\therefore$ $S = \{v_i w_j | i = 1, 2, ..., m, j = 1, 2, ..., n\}$ 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. Clearly any element in L, linearly independent over K, linearly independent 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 $\alpha_0, \alpha_1, \alpha_2, ..., \alpha_n \in F$, not all zero such that $\alpha_0 a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0$.*

Remark 5.12 *if $p(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + ... + \alpha_n, \alpha_i \in F.$ $\therefore$ $\alpha_0 a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0 \Rightarrow p(a) = 0$. (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 $\mathbb{Q}$.

Adjunctions to a in F is $F(a)$

The field obtained by adjointing a to F. Let K be an extension of F and $a \in K$. Let M be the collection of all subfields of K which contains both F and a, M is not empty because K is a subfield of K and K contains both F and a.

The intersection of all subfields of K which are members of M is also a subfield of K. Let $F(a)$ denote the intersection of those subfields of K which are members of M then $F(a)$ is a subfield of K. Obviously $F(a)$ contains both F and a because each members of M contains both F and a.

Thus $F(a)$ is a member of M function if E is any subfield of K containing then $F(a)$ is a subset of E (since $F(a)$ is the intersection of members of M and E is the members of M)

Thus $F(a)$ is a subfield of K containing both F and $'a'$ and itself and it is contained in any subfield of K containing both F and a. $\therefore$ $F(a)$ is the smallest subfield of K containing both F and a.

We call $F(a)$, the subfield of K obtained by adjoining $'a'$ in F. Our assumption of $F(a)$, so for has been purely an external one, we now give an alternative and more constructive description of $F(a)$

Suppose K is an extension field of F. Let $a \in K$ and

$$U = \{\frac{\alpha_0 a^n + \alpha_1 a^{n-1} + ... + \alpha_n}{\beta_0 a^m + \beta_1 a_{m-1} + ... + \beta_n} | \alpha_i \beta_j \in F, \beta_0 a^m + \beta_1 a^{m-1} + ... + \beta_n \neq 0\},$$

where m and n non-negative integer. Clearly U is a subfield of K. It can be easily seen that

$$(i)\ \alpha, \beta \in U \Rightarrow \alpha - \beta \in U$$
$$(ii)\ \alpha \in U, 0 \neq \beta \in U \Rightarrow \frac{\alpha}{\beta} \in U.$$

Then U is a subfield of K. Claim: $U = F(a)$. Clearly U contains both F and a. $\therefore$ U is a subfield of K containing both F and a. (i.e.) U contains $F(a)$..... (1) [Since $F(a)$ is the smallest subfield of K containing both F and a]. Further any subfield of K which contains both F and a by virtue of closure under addition and multiplication must contain all the elements $\alpha_0 a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0$
Since $F(a)$ is a subfield of K contain both F and a, $F(a)$ must contain all such elements being a subfield of K. $\therefore$ $F(a)$ must also contain U..... (2)
From (1) and (2), $F(a) = U$.

Theorem 5.13 *The element $a \in K$ is algebraic over F iff $F(a)$ is a finite extension of F. [(i.e.) $[F(a) : F]$ is finite iff $a \in K$ is algebraic over F]*
Proof: Suppose $F(a)$ is a finite extension of F. Let $[F(a) : F] = m$ where m is finite. To prove: $a \in K$ is algebraic over F. Since $F(a)$ is a field and $a \in F(a)$, the $(m+1)$ elements $1, a, a^2, ..., a_m$ are all in $F(a)$. Since the dim $F(a)$ as a vector space over F is m. [$\because [F(a) : F] = m$] $\therefore$ These $(m+1)$ elements

of $F(a)$ are linearly dependent over F. $\therefore$ there exists $\alpha_0, \alpha_1, \alpha_2, ..., \alpha_m \in F$, not all zero such that $\alpha_0 \cdot 1 + \alpha_1 a + \alpha_2 a^2 + ... + \alpha_m a^m = 0$..... (1)
Let$p(x) = \alpha_0 + \alpha_1 x + ... + \alpha_m x^m \in F[x]$. By (1) $p(a)$=0 (i.e.) a satisfies a non-zero polynomial in $F[x]$. Hence a is algebraic over F. Conversely, suppose that $a \in K$ is algebraic over F. Then a satisfies some non-zero polynomial in $F[x]$. Let $p(x)$ be a polynomial in $F[x]$ of smallest positive degree such that $p(a)$=0. Claim: $p(x)$ is irreducible over F. Suppose not, $p(x)$ is reducible over F. $p(x) = f(x)g(x), f(x), g(x) \in F[x]$, where $deg(f(x)) \neq 0$ and $deg(g(x)) \neq 0$. Now, $0 = p(a) = f(a)g(a) \Rightarrow g(a)f(a) = 0 \Rightarrow f(a) = 0$ (or) $g(a) = 0$ [$\because f(a), g(a) \in F$ and F is a field F is an integral domain and has no zero divisor]. Since $p(x)$ is the smallest positive degree polynomial such that $p(a)$=0. We have either $deg(f(x)) \geq deg(p(x))$ or $deg(g(x)) \geq deg(p(x))$. Thus $p(x) = f(x)g(x)$ where either $deg(f(x)) \geq deg(p(x))$ or $deg(g(x)) \geq deg(p(x))$. Which is a contradiction to the minimality of degree of $p(x)$. This contradiction shows that $p(x)$ is irreducible over F. Define a mapping $\psi : F[x] \to F(a)$ by $(h(x))\psi = h(a)$. To prove: ψ is a homomorphism. Let $h_1(x)$ and $h_2(x) \in F[x]$. Suppose $(h_1(x))\psi = h_1 a$ and $(h_2(x))\psi = h_2(a)$,

$$\begin{aligned}
(h_1(x) + h_2(x))\psi &= ((h_1 + h_2)x)\psi \\
&= (h_1 + h_2)(a) \\
&= h_1(a) + h_2(a) \\
&= (h_1(x))\psi + (h_2(x))\psi .....(1) \\
(h_1(x)h_2(x))\psi &= ((h_1 h_2)x)\psi \\
&= h_1 h_2(a) \\
&= h_1(a)h_2(a) \\
&= (h_1(x))\psi(h_2(x))\psi .....(2)
\end{aligned}$$

From (1) and (2), ψ is a homomorphism from $F[x]$ to $F(a)$. Let $V = Ker\psi = \{h(x) \in F[x] | (h(x))\psi = 0\}$ where 0 is identity element of $F(a)$. Claim: $V = Ker\psi$ is an ideal of $F[x]$. Let $h(x), g(x) \in V$, then $(h(x))\psi = 0$ and $(g(x))\psi = 0 \Rightarrow h(a) = 0$ and $g(a) = 0$. Let $S(x) = h(x) - g(x)$. $\therefore S(a) = h(a) - g(a) = 0 \Rightarrow S(x) \in V \Rightarrow h(x) - g(x) \in V$..... (3)
Let $h(x) \in V$ and $f(x) \in F[x]$, then $h(a) = 0$. Let $t(x) = h(x)f(x)$; $t(a) = h(a)f(a) = 0 \Rightarrow t(x) \in V \Rightarrow h(x)f(x) \in V, h(x) \in V, f(x) \in F[x]$. Similarly $f(x)h(x) \in V$..... (4)
From (3) and (4), V is an ideal of $F[x]$. Obviously $V \neq F[x]$ also $p(x)$ is an element of lower degree in the ideal V of $F[x]$. Since $p(x)$ is irreducible, V is a maximal ideal in $F(x)$. By a theorem, $F(x)/V$ is a field. By the general homomorphism $F[x]/V$ is isomorphic to the image of $F[x]$ we have shown that the image of $F[x]$ under ψ is a subfield of $F(a)$. This image contain $x\psi$ =0 and for every $\alpha \in F, \alpha\psi = \alpha$, thus the image of $F[x]$ under ψ is a subfield of $F(a)$ which contains both F and a. More clearly $F[x]/V$ is isomorphic

to $F(a)$. Let $V = (p(x))$ be the ideal generated by $p(x)$. The dimension of $F[x]/V$ as a vector space over F is precisely equal to the degree of $p(x)$. In view of this isomorphism we obtained between $F[x]/V$ and $F(a)$ we get that,

$$\begin{aligned}[F[x]/V : F] &= deg(p(x)) \\ deg_F(F(x)/V) &= deg(p(x)) \\ deg_F(F(a)) &= deg(p(x)) \\ [F(a) : F] &= deg(p(x))\end{aligned}$$

Hence $[F(a) : F]$ is finite.

Remark 5.14 *We have actually proved that more, namely that* $[F(a) : F]$ *= degree of the minimal polynomial satisfied by a over* F*.*

Example 5.15 *Let* F *be a field and Let* $F[x]$ *be a ring of polynomial in* x *over* F*. Let* $g(x)$ *of degree* n *be in* $F[x]$ *and* $V = (g(x))$ *in* $F[x]$*.Prove that* $F[x]/V$ *is* n *dimensional vector space over* F*.*
Solution: We have $V = \{f(x)g(x)|f(x) \in F[x]\}$; $F[x]/V = \{V+f(x)|f(x) \in F[x]\}$. Let $V + f_1(x), f_2(x) \in F[x]/V$. Then we define $(V + f_1(x)) + (V + f_2(x)) = V + f_1(x) + f_2(x)$. Also, we define scalar multiplication in $F[x]/V$ over F. Let $a \in F, V+f(x) \in F[x]/V$. Then we define, $a[V+f_x] = V+af_x$. Obviously $F[x]/V$ is an abelian group with respect to addition defined on it. The residue class V is the zero vector. Further let $a, b \in F$ and $f_1(x), f_2(x) \in F[x]$. Then,

$$\begin{aligned}(i)\ (a+b)[V + f_1(x)] &= V + (a+b)f_1(x) \\ &= V + af_1(x) + bf_1(x) \\ &= [V + af_1(x)] + [V + bf_1(x)] \\ &= a[V + f_1(x)] + b[V + f_1(x)] \\ (ii)\ a[\{V + f_1(x)\} + \{V + f_2(x)\}] &= a[V + f_1(x) + f_2(x)] \\ &= V + a(f_1(x) + f_2(x)) \\ &= V + af_1(x) + af_2(x) \\ &= [V + af_1(x)] + [V + af_2(x)] \\ &= a[V + f_1(x)] + a[V + f_2(x)] \\ (iii)\ a[b(V + f_1(x))] &= a[V + bf_1(x)] \\ &= V + (ab)f_1(x) \\ &= ab[V + f_1(x)] \\ (iv)\ [V + f_1(x)] &= V + 1 \cdot f_1(x) \\ &= V + f_1(x)\end{aligned}$$

Hence $F[x]/V$ is a vector space over F. Now, if $g(x)$ of degree n then to show that $F[x]$ is dimension n over F. We claim that $V+1, V+x, V+x^2, ..., V+x^n$

constitute the basis of $F[x]/V$ over F. First we shall show that these n elements of $F[x]/V$ are linearly independent over F. Now we have,

$$\begin{aligned} a_0(V+1)+a_1(V+x)+...+a_{n-1}(V+x^{n-1}) &= V \\ V+a_0+a_1x+...+a_{n-1}x^{n-1} &= V \\ a_0+a_1x+...+a_{n-1}x^{n-1} &\in V \\ \Rightarrow a_0+a_1x+...+a_{n-1}x^{n-1} &= f(x)g(x) \text{ for some } f(x)\in F[x] \end{aligned}$$

$f(x)=0$ [$\because$ $iff(x)\neq 0$ then $deg(f(x)g(x))\geq deg(g(x))=n$ and so we cannot have $f(x)\cdot g(x)=a_0+a_1x+...+a_{n-1}x^{n-1}$]
$a_0+a_1x+...+a_{n-1}x^{n-1}=0\Rightarrow a_0=a_1=...=a_{n-1}=0$
$V+1, V+x, V+x^2, ..., V+x^{n-1}$ are linearly independent over F. Let $V+f(x)$ be any element in $F[x]/V$. Then $f(x)\in F[x]$. By division algorithm there exists $q(x), r(x)\in F[x]$ such that $f(x)=q(x)g(x)+r(x)$ where either $r(x)=0$ or $deg(r(x))<deg(g(x))$. Now,

$$\begin{aligned} V+f(x) &= V+q(x)g(x)+r(x) \\ &= [V+q(x)g(x)]+(V+r(x)) \\ &= V+(V+r(x)) \\ &= V+r(x) \ (\because V \text{ is a zero vector}) \\ &= V+a_0+a_1x+...+a_{n-1}x^{n-1} \end{aligned}$$

where $a_0, a_1, ..., a_{n-1}\in F$ [$\because r(x)=0$ or $deg(r(x))<n$ (i.e.) $deg(g(x))$]
$V+f(x)=a_0(V+1)+a_1(V+x)+...+a_{n-1}(V+x^{n-1})$. Hence $V+1, V+x, ..., V+x^{n-1}$ forms a basis of $F[x]/V$ over F. $dim_F(F[x]/V)=n$ (i.e.) $[F[x]/V:F]=n$.

Definition 5.16 *A polynomial $p(x)$ over F of lowest positive degree satisfied by $a\in K$ is called a minimal polynomial for a over F.*

Remark 5.17 .

1. *We may assume that its coefficient of the highest power of x is 1, (i.e.) it is monic; in that case a monic polynomial of smallest degree over F satisfied by a is called the minimal polynomial of a over F.*

2. *$a\in K$ is said to be algebraic of degree n over F if it satisfies a minimal polynomial of degree n over F.*

Example 5.18 .

1. *Consider the polynomial x^2-3; $x^2-3=0\Rightarrow x=\pm\sqrt{3}$. $\therefore x^2-3$ is a minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}$. Clearly, it is monic and it satisfied by $\sqrt{3}$ as $\sqrt{3}$ is irrational it cannot satisfy the polynomial of degree 1 over $\mathbb{Q}$.*

2. $x^3 - 2$ *is a minimal polynomial of cubic root 2 over* $\mathbb{Q}$.

Result 5.19 *If* $p(x)$ *is a minimal polynomial of* a *over* F *of degree* n *then* $[F(a) : F] = n$

Proof: Suppose $p(x)$ is a minimal polynomial for a over F of degree n. Let $p(x) = x^n + \alpha_1 x^{n-1} + ... + \alpha_n, \alpha_i \in F$. $\therefore$ By our assumption,
$p(a) = a^n + \alpha_1 a^{n-1} + ... + \alpha_n = 0 \Rightarrow a_n = (-\alpha_1)a^{n-1} + ... + (-\alpha_n) \cdot 1$
(i.e.) a_n is a linear combinations of $1, a, a^2, ..., a^{n-1}$ and $\therefore a^n \in L(S)$ where $S = \{1, a, a^2, ..., a^{n-1}\}$..... (3)
$a^{n+1} = (-\alpha_1)a^n + (-\alpha_2)a^{n-1} + ... + (-\alpha_{n-1})a^2 - \alpha_n a$..... (2)
Sub (1) in (2) we get
$a^{n+1} = -[\alpha_1(-(\alpha_1 a^{n-1} + \alpha_2 a^{n-2} + ... + \alpha_n)) + \alpha_2 a^{n-1} + ... + \alpha_n a]$
$= -[(\alpha_2 - \alpha_1^2)a^{n-1} + (\alpha_3 - \alpha_1\alpha_2)a^{n-2} + ... + a(\alpha_n - \alpha_1\alpha_{n-1}) - \alpha_1\alpha_n]$
Showing that a^{n+1} is a linear combination of $1, a, ..., a^{n-1}$ over F. Continuing in this way we find that for each $k \geq 0, a^{n+k} \in L(S)$ (i.e.) a linear combination of $1, a, ..., a^{n-1}$.
Claim: $L(S) = F(a)$. $F(a)$ is the subfield of K generated by a over F. Then $F(a)$ being a field containing the field F. In order to show that $F(a)$ is a finite extension of F. We must show that $F(a)$ is a vector space over the field F is finite dimensional. Since $F(a)$ is the field containing a, $1, a, a^2, ..., a^{n-1}$ are the elements of $F(a)$. Let $L(S)$ denote the set of all linear combination of S. Then $F(a)$ being a vector space over F, each linear combination of elements of $F(a)$ over F will be contained in $F(a)$. Consequently $L(S) \subset F(a)$. Since $L(S)$ contains both F and a. It is clear that $L(S) = F(a)$. Since for each $k \geq 0, a^{n+k} \in L(S)$. It follows that the product of 2 elements of $L(S)$ is a linear combination of $1, a, a^2, ..., a^{n-1}$ and is therefore contained in $L(S)$. So $L(S)$ is closed for multiplication. Hence $L(S)$ is a subring of $F(a)$. Since $1 + 0 \cdot a + 0 \cdot a^2 + ... + 0 \cdot a_{n-1}$. (i.e.) as a linear combination of $1, a, a^2, ..., a^{n-1}$. $\therefore 1 \in L(S)$. (i.e.) $L(S)$ contains the unit element. Also the product of two non-zero elements of $L(S)$ is 0. Hence $L(S)$ is a ring with unit element and is without zero divisor. Let $T = F(a)$. Consider $T = \{\beta_0 + \beta_1 a + ... + \beta_{n-1}a^{n-1} / \beta_i \in F\}$. Clearly T is closed under addition and multiplication, T is a ring which contains both F and a. Claim: T is a field. Let $0 \neq u = \beta_0 + \beta_1 a + ... + \beta_{n-1}a^{n-1}$. Let $h(x) = \beta_0 + \beta_1 a + ... + \beta_{n-1}a^{n-1} \in F[x]$. Since $u \neq 0$ and $u = h(a)$ we have, $h(a) \neq 0$.(i.e.) a does not satisfy a polynomial $h(x)$ and $p(x)$ is the minimal polynomial satisfied by $a \Rightarrow p(x)$ does not divide $h(x)$ (i.e.) $p(x)$ and $h(x)$ are relatively prime polynomial in $F[x]$. Hence we can find polynomial $S(x)$

and $t(x)$ in $F[x]$

$$\begin{aligned} \Rightarrow p(x)S(x) + h(x)t(x) &= 1 \\ \text{But then } 1 &= p(a)S(a) + h(a)t(a) \\ &= h(a)t(a) \ [\because p(a) = 0] \\ &= ut(a) \ [\because h(a) = u] \\ u^{-1} &= t(a) \end{aligned}$$

Since $t(a)$ is the value of polynomials $t(x)$ at $x = a$ follows that $t(a)$ is a linear combination of $1, a, a^2, ..., a_{n-1}$. Also since a^{n+k} is a linear combination of $1, a, a^2, ..., a_{n-1}$ for each $k > 0$. It follows that $t(x)$ is a linear combination of $1, a, a^2, ..., a_{n-1}$; $t(a) \in L(S)$ (i.e.) $t(a) \in T$ (i.e.) Every non-zero element of T has its inverse in T. $\therefore$ T is a field. However T is a subset of $F(a)$, yet F and a are both contained in T which gives $T = F(a)$. We have identified $F(a)$ as the set of all expression $\beta_0 + \beta_1 a + ... + \beta_{n-1}a^{n-1}$. Hence $L(S)$ is a field containing F and a and itself contained in $F(a)$. Consequently $F(a) = L(S)$. Also the set S is linearly independent. Suppose if S is a linearly dependent. There exists elements $\alpha_0, \alpha_1, ..., \alpha_{n-1}$ not all zero such that $\alpha_0 \cdot 1 + \alpha_1 a + ... + \alpha_{n-1}a^{n-1} = 0 \Rightarrow a$ satisfy a polynomial, $\alpha_0 + \alpha_1 x + ... + \alpha_{n-1}x^{n-1}$ of deg $n - 1$ which is a contradiction to the minimality of $p(x)$. This contradiction shows that S is linearly independent. $\therefore S = \{1, a, a^2, ..., a^{n-1}\}$ is the basis of the vector space $F(a)$ over the field F. (i.e.) $[F(a) : F] = n$.

Theorem 5.20 *If $a \in K$ is algebraic of degree n over F then $[F(a) : F] = n$.*
Proof: Let K be a finite extension of the given field F. Suppose $a \in K$ is algebraic over F of degree n. $\therefore$ There exists a minimal polynomial $p(x)$ of degree n over F satisfies a. $\therefore$ By the above result, $[F(a) : F] = n$.

Theorem 5.21 *If a, b in K are algebraic over F then $a \pm b, ab$ and $\frac{a}{b}(b \neq 0)$ are all algebraic over F. In otherwords, the elements in K which are algebraic over F form a subfield of K.*
Proof: Let E be the set of all elements of K which are algebraic over F. $E = \{a \in K | a$ is algebraic over $F\}$. Since each element $\alpha \in F$ satisfies the monic polynomial $(x - \alpha)$ over F, It follows that $\alpha \in F$ is algebraic over F. $\therefore$ E is not empty and is a subset of K. Suppose a is algebraic of degree m over F. $\therefore$ $a \in E$ and $[F(a) : F] = m$ [by Theorem 5.20]. Let $T = F(a)$ the T is a subfield of K of degree m over F. Suppose b is algebraic of degree n over F then it is algebraic of degree almost n over T which contains F. (i.e.) $T(b)$ is a subfield of K and is of degree atmost n over T. Let $W = T(b)$ then $[W : T] \leq n$ (i.e.) $[T(b) : T] \leq n$ (i.e.) $[F(a, b) : T] \leq n \Rightarrow [F(a, b) : F(a)] \leq n$. By Theorem 5.9, $[W : F] = [W : T][T : F]$ (i.e.)$[W : T] = [F(a, b) : F] = [F(a, b) : F(a)][f(a) : F] =$

$mn \Rightarrow [F(a,b):F] = [W:F] = mn$. Hence $F(a,b)$ is a finite extension is an algebraic extension it follows that $F(a,b)$ is an algebraic extension of F. But $F(a,b)$, being a field $a, b \in F(a,b) \Rightarrow a \pm b, ab, \frac{a}{b}(b \neq 0) \in F(a,b)$ (Since each element of $F(a,b)$is algebraic over F) $\Rightarrow a \pm b, ab, \frac{a}{b}(b \neq 0) \in E$. Hence E is a subfield of K. (i.e.) the elements in K which are algebraic over F form a subfield of K.

Corollary 5.22 *If a and b in K are algebraic over F of degree m and n respectively then $a \pm b, ab, \frac{a}{b}(b \neq 0)$ are algebraic of degree atmost mn.*
Proof: Since $a \in K$ is algebraic over F of degree $m, [F(a):F] = m$. Since $b \in K$ is algebraic over F of degree $n, [F(b):F] = n$. Then the minimax polynomial over F of degree n satisfies b. But $F(a)$, being a subfield of F, the minimal polynomial over $F(a)$ satisfies b is of degree atmost n. Let $T = F(a)$ and $W = T(b)$ $\therefore$ $[W:T] \leq n$; $[F(a,b):F(a)] \leq n$. By Theorem 5.9, $[F(a,b):F] = [F(a,b):F(a)][F(a):F] \leq mn$ $\therefore$ $F(a,b)$ is finite under algebraic extension of F of degree not exceeding mn. Consequently each element of $F(a,b)$ is algebraic of degree not exceeding mn. Moreover $F(a,b)$, being a field, $a \pm b, ab, \frac{a}{b}$ (if $b \neq 0$) $\in F(a,b)$. Hence $a \pm b, ab, \frac{a}{b}(b \neq 0)$ are algebraic of degree at most mn over F.

Definition 5.23 *The extension K of F is called an algebraic extension of F if every element in K is algebraic over F.*

Theorem 5.24 *If L is an algebraic extension of K and if K is an algebraic extension of F, then L is an algebraic extension of F.*
Proof: Let u be an arbitrary element of L. To Prove: L is an algebraic extension of F, it is enough to prove that u is algebraic over F. (i.e.) To Prove: It satisfies some non trivial polynomial whose coefficients are in F. Since $u \in L$ and L is an algebraic extension of K, u satisfies a non trivial polynomial $x^n + \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + ... + \sigma_n$, where $\sigma_1, \sigma_2, ..., \sigma_n \in K$. But K is an algebraic extension of F $\therefore \sigma_1, \sigma_2, ..., \sigma_n$ are algebraic over F. By several uses of Theorem 5.20, $M = F(\sigma_1, \sigma_2, ..., \sigma_n)$ is a finite extension of F. Since u satisfy the polynomial $x^n + \sigma_1 x^{n-1} + ... + \sigma_n$, where coefficient $\sigma_1, \sigma_2, ..., \sigma_n$ are in $M = F(\sigma_1, \sigma_2, ..., \sigma_n)$. $\therefore$ u is algebraic over M using theorem 5.13, $M(u)$ is finite extension of M. By Theorem 5.9, $[M(u):F] = [M(u):M][M:F]$. $M(u)$ is a finite extension of F and u is an algebraic over F.

Definition 5.25 *A complex number is said to be algebraic number if it is an algebraic over the field of rational number.*

Example 5.26 *Let $a = 2 + 3i$ then $(a-2)^2 = (3i)^2 \Rightarrow a^2 + 4 - 4a = -9 \Rightarrow a^2 - 4a + 13 = 0$. Now, $p(x) = x^2 - 4x + 13$. $\therefore$ $a = 2 + 3i$ satisfies a polynomial over the field of rational numbers. $\therefore$ $2 + 3i$ is an algebraic number.*

Example 5.27 *(a) Let $\mathbb{R}$ be a field of real numbers and $\mathbb{Q}$ field of rational numbers in $\mathbb{R}$, $\sqrt{2}$ and $\sqrt{3}$ are both algebraic both algebraic over $\mathbb{Q}$ exhibit a polynomial of degree 4 over $\mathbb{Q}$ satisfied by $\sqrt{2}+\sqrt{3}$.*
(b) What is degree of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.
(c) What is the degree of $\sqrt{3}\sqrt{2}$ over $\mathbb{Q}$.
solution: (a) Given $\sqrt{2} \in \mathbb{R}$ algebraic over $\mathbb{Q}$ and the element $\sqrt{2} \in \mathbb{R}$ satisfy the polynomial, $x^2 - 2 = 0$ over $\mathbb{Q}$ and $x^2 - 2$ is an irreducible. The degree of algebraic of $\sqrt{2}$ over $\mathbb{Q} = deg(x^2 - 2)$. $\sqrt{2}$ is algebraic of degree 2 over $\mathbb{Q}$. $[\mathbb{Q}\sqrt{2} : \mathbb{Q}] = 2$. Similarly $\sqrt{3}$ is algebraic over $\mathbb{Q}$. $\sqrt{3} \in \mathbb{R}$ satisfies a polynomial $x^2 - 3$ over $\mathbb{Q}$. $\sqrt{3} \in \mathbb{R}$ is an algebraic of degree 2 over $\mathbb{Q}$.

$$
\begin{aligned}
[\mathbb{Q}\sqrt{3} : \mathbb{Q}] &= 2 \\
Let\ x &= \sqrt{3} + \sqrt{2} \\
\Rightarrow x - \sqrt{3} &= \sqrt{2} \\
\Rightarrow (x - \sqrt{3})^2 &= 2 \\
\Rightarrow x^2 - 2\sqrt{3}x + 3 &= 2 \\
\Rightarrow x^2 + 1 &= 2\sqrt{3}x \\
\Rightarrow (x^2 + 1)^2 &= 4 \cdot 3x^2 \\
\Rightarrow x^4 + 1 + 2x^2 &= 12x^2 \\
\Rightarrow x^4 - 10x^2 + 1 &= 0
\end{aligned}
$$

Let $p(x) = x^4 - 10x^2 + 1$
which is the required fourth degree polynomial satisfies $\sqrt{3} + \sqrt{2}$ over $\mathbb{Q}$.
(b) $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$:
We shall now prove the converse. Since $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ is field,

$$
\begin{aligned}
(\sqrt{2} + \sqrt{3})^3 &= 11\sqrt{2} + 9\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
\text{Also } -9(\sqrt{2} + \sqrt{3}) &\in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
1/2[(11\sqrt{2} + 9\sqrt{3}) - 9(\sqrt{2} + \sqrt{3})] &= \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
\sqrt{2} + \sqrt{3} - \sqrt{2} &= \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
\text{Thus } \sqrt{2}, \sqrt{3} &\in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
\mathbb{Q}(\sqrt{2}, \sqrt{3}) &\in \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
\text{Hence } \mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \mathbb{Q}(\sqrt{2} + \sqrt{3}).
\end{aligned}
$$

Let $L = \mathbb{Q}\sqrt{2}$ then $[L : \mathbb{Q}] = 2$. Also $x^2 - 3$ is an irreducible polynomial

over L satisfied by $\sqrt{3}$,

$$\begin{aligned}
[L\sqrt{3} : L] &= 2 \\
\text{Now } [L\sqrt{3} : \mathbb{Q}] &= [L\sqrt{3} : L][L : \mathbb{Q}] \\
&= 2 \cdot 2 = 4 \\
\text{Let } L(\sqrt{3}) &= (\mathbb{Q}\sqrt{2})\sqrt{3} = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\
&= \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] &= 4
\end{aligned}$$

$\Rightarrow \sqrt{2} + \sqrt{3}$ is of degree 4 over $\mathbb{Q}$.
(c) Let a denote the field of rational numbers. Let $K = \mathbb{Q}\sqrt{2}$; $L = K\sqrt{3}$. Now, $[L : K]$=2 and $[K : \mathbb{Q}]$=2. To find $[L : \mathbb{Q}]$,

$$\begin{aligned}
[L : \mathbb{Q}] &= [L : K][K : \mathbb{Q}] \\
L &= K\sqrt{3} \\
&= (\mathbb{Q}\sqrt{2})(\sqrt{3}) \\
&= \mathbb{Q}(\sqrt{2}\sqrt{3}) \\
[L : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2}\sqrt{3}) : \mathbb{Q}] \\
&= [L : K][K : \mathbb{Q}] = 2 \cdot 2 = 4.
\end{aligned}$$

Example 5.28 *With the same notation as in above problem. Show that* $\sqrt{2} + \sqrt[3]{5}$ *is algebraic over* $\mathbb{Q}$ *of degree 6.*
Solution: Let $\sqrt{2} + \sqrt[3]{5}$. To prove: $[\mathbb{Q}(a) : \mathbb{Q}]$=6. Given $\sqrt{2} \in \mathbb{R}$ algebraic over $\mathbb{Q}$ and the element $\sqrt{2} \in \mathbb{R}$ satisfies the polynomial $x^2-2 = 0$ over $\mathbb{Q}$ and x^2-2 is an irreducible. The degree of algebraic of $\sqrt{2}$ over $\mathbb{Q} = deg(x^2-2) =$ 2. (i.e.) $\sqrt{2}$ is algebraic of degree 2 over $\mathbb{Q}$. (i.e.) $[\mathbb{Q}\sqrt{2} : \mathbb{Q}]$=2. Similarly $\sqrt[3]{5}$ algebraic over $\mathbb{Q}$. $\sqrt[3]{5} \in \mathbb{R}$ satisfies a polynomial $x = \sqrt[3]{5} \Rightarrow x = 5^{1/3} \Rightarrow x^3 = 5 \Rightarrow x^3 - 5 = 0\}$ over $\mathbb{Q}$ and $x^3 - 5$ is an irreducible. The degree of algebraic of $\sqrt[3]{n}$ over $\mathbb{Q} = deg(x^3 - 5) = 3$.

$$\begin{aligned}
[\mathbb{Q}\sqrt[3]{5} : \mathbb{Q}] &= 3 \\
\text{Let } x &= \sqrt{2} + \sqrt[3]{5} \\
\Rightarrow x - \sqrt{2} &= \sqrt[3]{5} \\
(x - \sqrt{2})^3 &= 5 \\
\Rightarrow (x - \sqrt{2})(x^2 - 2x\sqrt{2} + 2) &= 2 \\
\Rightarrow x^3 - 2\sqrt{2}x^2 - \sqrt{2}x^2 + 2x + 4x - 2\sqrt{2} &= 5 \\
\Rightarrow x^3 - 3\sqrt{2}x^2 + 6x - 2\sqrt{2} &= 5
\end{aligned}$$

$$\Rightarrow x^3 + 6x = [5 + \sqrt{2}(2 + 3x^2)]$$
$$(x^3 + 6x - 5)^2 = [\sqrt{2}(2 + 3x^2)]^2$$
$$\Rightarrow x^6 + 36x^2 + 25 + 12x^4 - 60x - 10x^3 = 2(4 + 9x^4 + 12x^2)$$
$$\Rightarrow x^6 + 6x^4 - 10x^3 + 12x^2 - 60x - 8 + 25 = 0$$
$$\Rightarrow x^6 + 6x^4 - 10x^3 + 12x^2 - 60x + 17 = 0$$

Now, $p(x) = x^6 + 6x^4 - 10x^3 + 12x^2 - 60x + 17 = 0 \in \mathbb{Q}[x]$, which satisfies $(\sqrt{2} + \sqrt[3]{5})$. $[\mathbb{Q}(\sqrt{2} + \sqrt[3]{5}) : \mathbb{Q}]$ = degree of $p(x) = 6$. $(\sqrt{2} + \sqrt[3]{5})$ is algebraic over $\mathbb{Q}$ of degree 6.

Roots of Polynomials:

Definition 5.29 *If $p(x) \in F[x]$ then an element a lying in some extension field F is called a root of $p(x)$ if $p(a) = 0$.*

Lemma 5.30 ***Remainder theorem:*** *If $p(x) \in F[x]$ and if K is an extension of F then for any element $b \in K, p(x) = (x - b)q(x) + p(b)$ where $q(x) \in F[x]$ and $deg(q(x)) = deg(p(x)) - 1$.*
Proof: Since $F \subset K, F[x] \subset K[x]$; $p(x) \in F[x] \Rightarrow p(x) \in K[x]$. Since the polynomial $p(x)$ and $(x - b)$ are both in $K[x]$, we can apply division algorithm for this polynomial. $\therefore$ there exists polynomials $q(x)$ and $r(x)$ in $K[x]$ such that $p(x) = (x-b)q(x)+r(x), q(x) \in K[x]$, where either $r(x) = 0$ or $deg(r(x)) < deg(x - b)$. (i.e.) in either case $r(x)$ must be a constant in $K[x]$. Let $r(x) = r \in K$ (i.e.) r must be an element in K. Since $p(x) = (x - b)q(x) + r$, let $p(b) = r \Rightarrow p(x) = (x - b)q(x) + p(b)$.....(1)
Suppose $deg(p(x)) = n$ and $deg(q(x)) = m$. From (1) $deg(p(x)) = deg(p(x)) = deg(x - b)q(x) + deg(p(b)) \Rightarrow n = 1 + m + 0 \Rightarrow m = n - 1 \Rightarrow deg(q(x)) = deg(p(x)) - 1$.

Corollary 5.31 ***Factor Theorem:*** *If $a \in K$ is a root of $p(x) \in F[x]$ where $F \subset K$ then in $K[x], (x - a)/p(x)$.*
Proof: Let $p(x) \in F[x]$ and $a \in K$ where K is an extension of K. Then by Remainder theorem in $K[x]$, we have $p(x) = (x-a)q(x)+p(a) \Rightarrow p(x) = (x-a)q(x)+0$ ($\because$ a is a root of $p(x)$) $\Rightarrow p(x) = (x-a)q(x) \Rightarrow (x-a)/p(x) \in K[x]$.

Definition 5.32 *The element $a \in K$ is a root of $p(x) \in F[x]$ of multiplicity m if $(x - a)^m/p(x)$ where $(x - a)^{m+1}/p(x)$.*

Lemma 5.33 *A polynomial of degree n over a field can have at most n roots in any extension field.*
Proof: We prove this theorem by induction on n, the degree of the polynomial $p(x)$. Let $p(x)$ be a polynomial of degree 1 over any F. Let $p(x) = \alpha x + \beta, \alpha, \beta \in F$ and $\alpha \neq 0$. Let a be a root of $p(x)$ in some extension of F. Then $p(a) = \alpha a + \beta \Rightarrow 0 = \alpha a + \beta \Rightarrow a = -\beta/\alpha (\alpha \neq 0)$. In this case $p(x)$

has the unique root $-(\beta/\alpha)$ (i.e.) $p(x)$ has one and exactly one roots in any in any extension field of F. The theorem is true when $p(x)$ is of degree 1. Assuming that the result is true in any field for all polynomial of degree less than n. Let us suppose that $p(x)$ be a polynomial of degree n over F. Let K be any extension of F. If $p(x)$ has no roots in K ,then the theorem is obviously true, because the number of roots in K is zero which is definitely at most n. So, let us suppose that $p(x)$ has at least one root, say $a \in K$. Let a be the root of multiplicity m then in $K[x]$,
$(x-a)^m/p(x), m \leq n$..... (1)
$\Rightarrow deg((x-a)^m) \leq deg(p(x)) \Rightarrow m \leq n$. Since $(x-a)^m$, is a divisor of $p(x)$ in $K[x]$. We have $p(x) = (x-a)^m q(x)$ where $q(x) \in K[x] \Rightarrow deg(p(x)) = deg((x-a)^m) + deg(q(x))$; $deg(q(x)) = deg(p(x)) - deg((x-a)^m) = (n-m) \leq n$ $(1 \leq m \leq n)$. Now, a is a root of $p(x)$ of multiplicity m. we have, $(x-a)^{m+1}$ does not divides $p(x) = (x-a)^{m+1}q(x)$..... (2)
$\Rightarrow (x-a)^{m+1}$ does not divides $(x-a)^{m+1}q(x) \Rightarrow (x-a)$ does not divides $q(x)$ [if $(x-a)/q(x)$ then $(x-a)^{m+1}/p(x) \Rightarrow\Leftarrow$ to2]. $\therefore a$ is not a root of $q(x)$. If $b \neq a$ is a root of $p(x)$ in K then, $0 = p(b) = (b-a)^m q(b)$. Since K is a field and $0 \neq (b-a)^m \in K$ and $q(b) \in K$, we have $q(b) = 0 \Rightarrow b$ is a root of $q(x)$ in K. $\therefore$ Any root of $p(x)$ in K other than a must also be a root of $q(x)$ in K. Since $deg(q(x)) = n - m < n$, by our induction hypothesis, $q(x)$ has atmost $n-m$ roots in K other than a. $\therefore p(x)$ has atmost $(n-m)+m$ roots in K. (i.e.) $p(x)$ has atmost n roots in K. $\therefore$ The root a if $p(x)$ of $p(x)$ of multiplicity m being counted m times. $\therefore$ By induction hypothesis the lemma follows.

Theorem 5.34 *If $p(x)$ is a polynomial in $F[x]$ of degree $n \geq 1$ and is irreducible over F, then there is an extension E of F such that $[E:F] = n$ in which $p(x)$ has a root.*

Proof: Let $F[x]$ be the ring of polynomial in x over F. Let $V = (p(x))$ be the ideal generated by $p(x) \in F[x]$. Then V is a maximal ideal of $F[x]$. Hence by Theorem 3.38. $\therefore F[x]/V = E(say)$ is a field. We shall show that the field E satisfies all the requirements of the theorem. First we shall show that E can be regarded as an extension of F. Even though E does not contain the the elements of F in their original form, for this, we shall show that the field F can be embedded in the field E. Let $\bar{F}$ be the image of F in E. Let $\psi : F \to E$ defined by $\alpha\psi = V + \alpha, \alpha \in F$.

(i) ψ is 1-1:

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

$$\begin{aligned} V + \alpha &= V + \beta \\ (\alpha - \beta) \in V &= p(x) \\ (\alpha - \beta) &= f(x)p(x) \text{ for some } f(x) \in F[x] \\ \Rightarrow f(x) &= 0 \\ \Rightarrow (\alpha - \beta) &= 0 \\ \Rightarrow \alpha &= \beta \\ \psi \text{ is } 1 - 1.& \end{aligned}$$

(ii) ψ is homomorphism:

$$\begin{aligned} (\alpha + \beta)\psi &= V + (\alpha + \beta) \\ &= (V + \alpha) + (V + \beta) \\ &= \alpha\psi + \beta\psi \end{aligned}$$

$\therefore \psi$ 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 $\bar{F} = \{\alpha + V | \alpha \in F\}$. 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 $\{1+V, x+V, (x+V)^2 = x_2+V, (x+V)^3 = x^3 + V, ..., (x+V)^{n-1} = x^{n-1} + V\}$ form a basis of E over F. $[E : F] = n$. Finally we shall show that $p(x)$ has a root in E. Let $p(x) = \beta_0 + \beta_1 x + \beta_2 x^2 + ... + \beta_k x^k$ where $\beta_0, \beta_1, \beta_2, ..., \beta_k \in F$. 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 E as $a\beta_k$ by $\beta_k + V, p(x) = (\beta_0 + V) + (\beta_1 + V)x + ... + (\beta_k + V)x^k$. We shall show that $x + V \in E$ satisfies $p(x)$.

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

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

properties required in the conclusion of the theorem.

Corollary 5.35 *If $f(x) \in F[x]$ the there is a finite extension E of F in which $f(x)$ has a root. Moreover $[E : F] \leq deg(f(x))$.*
Proof: Let $p(x)$ be an irreducible factor of $f(x)$. Let $f(x) = p(x)q(x)$. $\therefore$ $deg(p(x)) \leq deg(f(x))$. Let a be a root of $p(x)$ in some extension field K of F. Then $p(a) = 0 \Rightarrow f(a) = p(a)q(a) = 0 \Rightarrow f(a) = 0$. Thus any root of $p(x)$ in some extension field of F is also a root of $p(x)$ in that extension field. Since $p(x)$ is irreducible over F, by the above theorem, $[E : F] = deg(p(x)) \leq deg(f(x)) \Rightarrow [E : F] \leq deg(f(x))$.

Theorem 5.36 *let $f(x) \in F[x]$ be a polynomial of degree n greater than or equal to q then there is an extension of E of F of degree atmost $n!$ in which $f(x)$ has n roots.*
Proof: We shall prove this theorem by induction on n the degree of $f(x)$. Let $f(x) \in F[x]$ of degree 1. Let $f(x) = a_0x + a_0, a \in F, a_0 \neq 0$. Now F itself is an extension of F. $\therefore [F : F] = 1$ (i.e.) $[F : F] \leq 1!$. Now, $f(x) = a_0x + a_0 = 0 \Rightarrow x = -a/a_0 \in F, a_0 \neq 0$ is a root of $f(x) = a_0x + a$. Thus if degree of $f(x)$=1. There is a finite extension F of degree atmost 1=1!. $\therefore$ The result is true for n=1. Now assume by our induction hypothesis that the theorem is true in any field for all polynomials of degree less than n. Let $f(x)$ be a polynomial of degree n over a field F. By Corollary 5.35, there is an extension E_0 of F with $[E_0 : F] \leq deg(f(x))$ in which $f(x)$ has a root, α(say). $\therefore$ By remainder theorem, in $E_0[x], f(x)$ can be factored as $f(x) = (x - \alpha)q(x) + (\alpha)$ where deg of $q(x) = deg(f(x)) - 1 = (n - 1) < n$ (i.e.)$deg(q(x)) < n$ $\therefore$ By induction hypothesis there is an extension E of degree atmost $(n-1)!$ (i.e.) $[E : E_0] = (n-1)!$ in which $q(x)$ has n-1 roots. Since any root of $f(x)$ is either α or a root of $q(x)$. $\therefore$ In E we obtain all n roots of $f(x)$. Since E is an extension of E_0 and E_0 is an extension of F, we have, E is an extension F $\therefore [E : F] \leq [E : E_0][E_0 : E] = (n-1)!n = n! \Rightarrow [E : F] \leq n!$. Thus E is an extension of F of degree atmost $n!$ in which $f(x)$ has n roots.

Remark 5.37 *The above theorem asserts that the finite extension E of a given field F in which the given polynomial of degree n over F has n roots. Let $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n, a_0 \neq 0 \in F[x]$. Let $\alpha_1, \alpha_2, ..., \alpha_n$ be n roots of $f(x)$ in E. $\therefore$ By Corollary 5.31, $f(x)$ can be factored over E as $f(x) = a_0(x-\alpha_1)(x-\alpha_2 \cdots (x-\alpha_n)$. Thus $f(x)$ splits of completely over E as a product of linear factors such a finite extension of F of minimal degree in which $f(x)$ splits of completely over E as a product of linear factor exists for such minimal extension improper subfield has the property.*

Definition 5.38 *If $f(x) \in F[x]$, a finite extension E of F is said to be a splitting field over F for $f(x)$ if over $E[F(x)]$ but not over any proper subfield of E. $f(x)$ can be factored as a product of linear factors.*

Remark 5.39 *The above theorem guarantees the existence of splitting field.*
Equivalent definition of splitting field for $f(x)$ ***over*** F***:***
E is a splitting field of $f(x)$ over F if E is a minimal extension of F in which $f(x)$ has n roots where $n = deg(f(x))$.

Remark 5.40 *A minimal extension E of a field F is said to be splitting field of $f(x) \in F[x]$ if $f(x) \in F[x]$ is expressible as $f(x) = a_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n, \alpha_i \in F$ and $E = F(\alpha_1, \alpha_2, ..., \alpha_n),\ \alpha_0, ..., \alpha_n \in E$.*

Note 5.41 *Let E_1 and E_0 be two splitting fields of the same polynomial $f(x)$ in $F[x]$. We shall show that they are isomorphic by an isomorphism leaving every element of F fixed.*

An isomorphic mapping:
Let F and F' be two fields and let E and E' be the extension fields of F and F' respectively. An isomorphism $\sigma : E \to E'$ is called a continuation of an isomorphism $\psi : F \to F',\ (\alpha)\sigma = (\alpha)\psi\ \forall \alpha\tau = \alpha \in E$. Let τ be an isomorphism of F onto F' for convenience let us denote the image of any $\alpha \in F$ under τ by α' (i.e.) $\alpha\tau = \alpha'$.

Remark 5.42 *In the fallowing result we can make use of τ to set up an isomorphism between $F[x]$ and $F'[t]$.*

Lemma 5.43 *Let ψ be an isomorphism of a field F onto a field F' such that $(\alpha)\tau = \alpha'$. Show that there is an isomorphism τ^* of $F[x]$ onto $F'[t]$ with a property that $(\alpha)\tau^* = \alpha'\ \forall \alpha \in F[x]$.*
Proof: Given τ is a isomorphism of F onto F'. For any $\alpha \in F$ we write $(\alpha)\tau = \alpha'$. Let us define $\tau^* = F[x] \to F'[t]$ as follows, let $f(x) = \alpha_0x^n + \alpha_1x^{n-1} + ... + \alpha_n$. Define

$$\begin{aligned}(f(x))\tau^* &= (\alpha_0x^n + \alpha_1x^{n-1} + ... + \alpha_n)\tau^* \\ &= (\alpha_0\tau)t^n + (\alpha_1\tau)t^{n-1} + ... + (\alpha_n\tau) \\ &= \alpha_0't^n + \alpha_1'x^{n-1} + ... + \alpha_n' \\ &= f'(t)(\text{say})\end{aligned}$$

we shall show that τ^* is 1-1. Let $f(x) = \alpha_0x^n + \alpha_1x^{n-1} + ... + \alpha_n$ and $g(x) = \beta_0x^m + \beta_1x^{m-1} + ... + \beta_m$ be any two elements in $F[x]$. Suppose

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

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

$$
\begin{aligned}
&[f(x)+g(x)]\tau^* \\
&\quad = [\alpha_0 x^n + \alpha_1 x^{n-1} + ... + \alpha_n + \beta_0 x^m + \beta_1 x^{m-1} + ... + \beta_m] \\
&\quad = ((\alpha_0' x^n + \alpha_1' x^{n-1} + ... + \alpha_n') + (\beta_0' x^m + \beta_1' x^{m-1} + ... + \beta_m')) \\
&\quad = (\alpha_0 x^n + \alpha_1 x^{n-1} + ... + \alpha_n)\tau^* + (\beta_0 x^m + \beta_1 x^{m-1} + ... + \beta_m)\tau^* \\
&\quad = f(x)\tau^* + g(x)\tau^*
\end{aligned}
$$

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 $f(x) = (\alpha_0 x^n + \alpha_1 x^{n-1} + ...+\alpha_n) \in F[x]$. Let us define $f'(t) = \alpha_0' t^n + \alpha_1' x^{n-1} + ... + \alpha_n' \in F'[t]$. 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 $V + g(x) = V + h(x)$

then $[V+g(x)]\tau^{**} = [V+h(x)]\tau^{**},\ g(x), h(x) \in F[x]$. We have $V+g(x) = V+h(x) \Rightarrow g(x)-h(x) \in V \Rightarrow [g(x)-h(x)] = [k(x)f(x)]$ where $k(x) \in F[x]$

$$\begin{aligned}
[g(x)-h(x)]\tau^* &= [k(x)f(x)]\tau^* \\
\Rightarrow g(x)\tau^* - h(x)\tau^* &= (k(x))\tau^* \cdot (f(x))\tau^* \\
\Rightarrow g'(t) - h'(t) &= k'(t)f'(t) \\
\Rightarrow g'(t) - h'(t) &\in V' \\
\Rightarrow V' + g'(t) &= V' + h'(t) \\
\Rightarrow [V+g(x)]\tau^{**} &= [V+h(x)]\tau^{**}
\end{aligned}$$

$\therefore \tau^{**}$ is well defined.

τ^{**} **is 1-1:** Let $g(x), h(x) \in F[x]$.

$$\begin{aligned}
[V+g(x)]\tau^{**} &= [V+h(x)]\tau^{**} \\
V' + g'(t) &= V' + h'(t) \\
g'(t) - h'(t) &\in V' \\
g'(t) - h'(t) &= k'(t)f'(t) \quad \text{for some } k'(t) \in F'[t] \\
\Rightarrow g(x)\tau^* - h(x)\tau^* &= (k(x))\tau^*(f(x))\tau^* \\
(g(x) - h(x))\tau^* &= (k(x) \cdot f(x))\tau^* \\
\Rightarrow g(x) - h(x) &= k(x)f(x) \\
\Rightarrow g(x) - h(x) &\in V \\
\Rightarrow V + g(x) &= V + h(x)
\end{aligned}$$

$\Rightarrow \tau^{**}$ is $1-1$.

τ^{**} **is onto:**

Since the mapping τ^* is onto. $\therefore$ corresponding to any polynomial $g'(t) \in F'[t]$

we have a polynomial $g(x)$ in $F[x]$, $V' + g'(t) \in F'[t]/V' \Rightarrow V + g(x) \in F[x]/V$ such that $[V+g(x)]\tau^{**} = V' + g'(t) \Rightarrow \tau^{**}$ preserves addition and multiplication. Let $g(x), h(x) \in F[x]$, we have

$$\begin{aligned}
[(V+g(x)) + (V+h(x))]\tau^{**} &= (V + g(x) + h(x))\tau^{**} \\
&= V' + (g(x) + h(x))\tau^{**} \\
&= V' + (g(x))\tau^* + (h(x))\tau^* \\
&= V' + (g'(t) + h'(t)) \\
&= (V' + g'(t)) + (V + h'(t)) \\
&= (V+g(x))\tau^{**} + (V+h(x))\tau^{**} \\
\text{Also, } [(V+g(x)) + (V+h(x))]\tau^{**} &= [V + g(x)h(x)]\tau^{**} \\
&= V' + (g(x))\tau^* \cdot (h(x))\tau^* \\
&= V' + g'(t) \cdot h'(t) \\
&= [V' + g'(t)] \cdot [V + h'(t)] \\
&= [V+g(x)]\tau^{**}[V+h(x)]\tau^{**}
\end{aligned}$$

Thus τ^* is an isomorphism of $F[x]/V$ onto $F'[t]/V'$. In Theorem 5.34 we have shown that F can be imbedded in field $F[x]/V$ by identifying the element $\alpha \in F$ with the residue class (coset) $V+\alpha$ in $F[x]/V$. Similarly we can consider F' to be obtained in $F'[t]/V'$ with this identification for any $\alpha \in F$ we have $\alpha\tau^{**} = (V+\alpha)\tau^{**} = V' + (\alpha)\tau^* = V' + \alpha' = \alpha'$ (α' has been identified with $V+\alpha$).

Example 5.46 *Let F be any field and let $p(x) = x^2 + \alpha x + \beta . \alpha, \beta$ be in $F[x]$. Let K be any extension of F.*
By Lemma 5.33, $p(x)$ has a root in $K[x]$. $\therefore p(a) = 0$.

$$\begin{aligned} 0 = p(a) &= a^2 + \alpha a + \beta \\ \beta &= -a(a+\alpha) \\ \text{Let } b &= -\alpha - a \in K \\ \therefore \alpha &= -(a+b) \ldots\ldots (1) \\ p(b) &= b^2 + \alpha b + \beta \\ &= (\alpha + a)^2 - \alpha(a+\alpha) - a(a+\alpha) \\ &= \alpha^2 + a^2 + 2\alpha a - \alpha a - \alpha^2 - a^2 - a\alpha \\ &= 0 \end{aligned}$$

$\therefore b$ is root in K
Case(i): *Suppose $b = a$. Then, $p(x) = x^2 + \alpha x + \beta = x^2 - x(a+b) - a^2 - a\alpha = x^2 - x(a+b) + ab$. Since $b = a$, $p(x) = x^2 - 2ax + a^2 = (x-a)^2 = (x-a)(x-a)$. $\therefore$ both the roots of $p(x)$ are in K.*
Case (ii): *Suppose $b \neq 0$. Then,*

$$\begin{aligned} p(x) &= x^2 + (-a-b)x + a(a+b) - a^2 \\ &= x^2 + (-a-b)x + a(a+b-a) \\ &= x^2 + (-a-b)x + ab \\ &= (x-a)(x-b) \end{aligned}$$

$\therefore$ a and b are the roots of $p(x)$ consequently $p(x)$ can be splitted by an extension of degree 2 over F.

Remark 5.47 *We could also get this result directly by invoking Theorem 5.36.*

Example 5.48 *Let F be the field of rational numbers and $f(x) = x^3 - 2$. In the field of complex number. Determine the degree of the splitting field of this polynomial $f(x)$ over F.*
Solution: Given F is a field of rational number. Let $f(x) = x^3 - 2 \in F[x] =$

$Q[x]$. In the field of complex number we can find 3 roots of $f(x)$ as follows.

$$\begin{aligned} f(x) &= 0 \\ x^3 - 2 &= 0 \\ x^3 &= 2 \cdot 1 \\ x^3 &= 2[cos0 + isin0] \\ x^3 &= 2(cos2k\pi + isin2k\pi) \\ x &= 2^{\frac{1}{3}}(cos2k\pi + isin2k\pi)^{\frac{1}{3}} \\ x &= 2^{\frac{1}{3}}(cos(\frac{2k\pi}{3}) + isin(\frac{2k\pi}{3})) \end{aligned}$$

Put k=0,1,2..., then the roots are

$$\begin{aligned} k = 0 \Rightarrow x_1 &= 2^{\frac{1}{3}}(cos0 + isin0) = 2^{\frac{1}{3}} \\ k = 1 \Rightarrow x_2 &= 2^{\frac{1}{3}}(cos(\frac{2\pi}{3}) + isin(\frac{2\pi}{3})) \\ &= 2^{\frac{1}{3}}[-1 + \frac{\sqrt{3}i}{2}] \\ &= 2^{\frac{1}{3}}\omega \\ k = 2 \Rightarrow x_3 &= 2^{\frac{1}{3}}(cos(\frac{4\pi}{3}) + isin(\frac{4\pi}{3})) \\ &= 2^{\frac{1}{3}}(cos(240^\circ) + isin(240^\circ)) \\ &= 2^{\frac{1}{3}}(cos(270^\circ - 30^\circ) + isin(240^\circ - 30^\circ)) \\ &= 2^{\frac{1}{3}}(-sin(30^\circ) + i(-cos30^\circ)) \\ &= 2^{\frac{1}{3}}(-\frac{1}{2} - \frac{\sqrt{3}i}{2}) \\ &= 2^{\frac{1}{3}}(-1 - \frac{\sqrt{3}i}{2}) \\ &= 2^{\frac{1}{3}}\omega^2 \end{aligned}$$

$\therefore$ The roots are $2^{\frac{1}{3}}, 2^{\frac{1}{3}}\omega, 2^{\frac{1}{3}}\omega^2$, where $\omega = -1 + \frac{\sqrt{3}i}{2}$ and $\omega^2 = -1 - \frac{\sqrt{3}i}{2}$ and $2^{\frac{1}{3}}$ is a real cubic root of 2. The polynomial $f(x)$ is irreducible over Q by Eisentien criterion. Since $2^{\frac{1}{3}}$ is root of $f(x), 2^{\frac{1}{3}}$ is algebraic over F of degree 3. $\therefore [F(2^{1/3}) : F]$=3 by Theorem 5.20. Let F be the splitting field of $f(x)$ over F the field F of $2^{1/3}$ cannot splits $f(x)$ because as a subfield of real field it cannot contain the complex number but not real number $w \cdot 2^{\frac{1}{3}}$. $\therefore f(2^{\frac{1}{3}})$ will be a proper subfield of E so we have $[E : F] > [F(2^{\frac{1}{3}}) : F]$=3. Also by Theorem 5.36, $[E : F] \leq 3!$=6 $\Rightarrow [E : F] = [E : F(2^{\frac{1}{3}})][F(2^{\frac{1}{3}}) : F]$ (by Theorem 5.9) $\Rightarrow [F(2^{\frac{1}{3}}) : F]/[E : F] \Rightarrow 3/6$. $\therefore$ We must have $[E : F] = 6$. $\therefore E$ is the splitting field of $f(x)$ over F of degree 6.

Example 5.49 *Let F be the field of rational numbers and let $f(x) = x^4 + x^2 + 1 \in F[x]$ prove that $E = F(w), w = -1 + \frac{\sqrt{3}i}{2}$ is a splitting field of $f(x)$ over F and prove that $[E : F]$=2.*

More about roots

Definition 5.50 *If $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + ... + \alpha_i x^{n-i} + ... + \alpha_{n-1}x + \alpha_n$ in $F[x]$, then the derivative of $f(x)$, written as $f'(x)$, is the polynomial $f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + ... + (n-i)\alpha_i x^{n-i+1} + ... + \alpha_{n-1}$ in $F[x]$.*

Definition 5.51 *A field F is said to be characteristic zero if $ma \neq 0$ for $a \neq 0$ in F and $m > 0$ an integer. If $ma = 0$ for some $m > 0$ and some $a \neq 0 \in F$ then F is said to be of finite characteristic. If there exists a smallest positive integer p such that $pa = 0$ for all $a \in F$ then the characteristic of F is p.*

Remark 5.52 .

1. *If F is of finite characteristic then its characteristic, p is a prime number.*

2. *If F be a field of characteristic $p \neq 0$, in this case the derivative of a polynomial $x^p, px^{p-1} = 0$ thus the usual result from the calculus that a polynomial whose derivative is zero must be a constant no longer need hold true.*

3. *However if the characteristic of F is zero and if $F'(x) = 0$ for $f(x) \in F$, it is indeed true that $f(x)$=constant (i.e.) $f(x) = \alpha \in F$. Even when the characteristic of F is $p \neq 0$ we can still describe the polynomial with zero derivative. If $f'(x)$=0 then $f(x)$ is a polynomial in x^p.*

Lemma 5.53 *For any polynomials $f(x), g(x) \in F[x]$ and only $\alpha \in F$.*

1. $(f(x) + g(x))' = f'(x) + g'(x)$.

2. $(\alpha(f(x)))' = \alpha f'(x)$.

3. $(f(x) + g(x))' = f'(x)g(x) + f(x)g'(x)$.

Proof: (1) Let

$$f(x) = \alpha_n + \alpha_{n-1}x + ... + \alpha_{n-(m-1)}x^{m-1} + ... + \alpha_{n-m}x^m + \alpha_{n-(m+1)}x^{m+1} + ... + \alpha_0 x^n \text{ and}$$

$$g(x) = \beta_m + \beta_{m-1}x + \beta_{m-2}x^2 + ... + \beta_2 x^{m-2} + \beta_1 x^{m-1} + \beta_0 x^m$$

Assume that $n > m$

$$
\begin{aligned}
&f(x)+g(x)\\
&\quad=(\alpha_n+\beta_m)+(\alpha_{n-1}+\beta_{m-1})x+...+(\alpha_{n-m+1}+\beta_1)x^{m-1}\\
&\qquad+(\alpha_{n-m}+\beta_0)x^m+\alpha_{n-m-1}x^{m+1}+...+\alpha_1x^{n-1}+\alpha_0x^n\\
&(f(x)+g(x))'\\
&\quad=(\alpha_{n-1}+\beta_{m-1})+2(\alpha_{n-2}+\beta_{m-2})x+...+(m-1)(\alpha_{n-m+1}+\beta_1)x^{m-2}\\
&\qquad+m(\alpha_{n-m}+\beta_0)x^{m-1}+(m+1)\alpha_{n-m-1}x^m+...+(n-1)\alpha_1x^{n-2}\\
&\qquad+n\alpha_0x^{n-1}\\
&\quad=(\alpha_{n-1}+2\alpha_{n-2}x+...+(m-1)\alpha_{n-(m-1)}x^{m-2}+m\alpha_{n-m}x^{m-1}\\
&\qquad+(m+1)\alpha_{n-m-1}x^m+...+(n-1)\alpha_1x^{n-2}+n\alpha_0x^{n-1})\\
&\qquad+(\beta_{m-1}+2\beta_{m-2}x+(m-1)\beta_1x^{m-2}+m\beta_0x^{m-1})\text{ where } n=m\\
&\quad=f'(x)+g'(x)
\end{aligned}
$$

(2)

$$
\begin{aligned}
\alpha(f(x))&=\alpha\alpha_n+\alpha\alpha_{n-1}x+...+\alpha\alpha_{n-m+1}x^{m-1}+\alpha\alpha_{n-m}x^m\\
&\qquad+\alpha\alpha_{n-m-1}x^{m+1}+...+\alpha\alpha_0x^n\\
(\alpha(f(x)))'&=\alpha\alpha_{n-1}+2\alpha\alpha_{n-2}x+...+(m-1)\alpha\alpha_{n-m+1}x^{m-2}\\
&\qquad+m\alpha\alpha_{n-m}x^{m-1}+(m+1)\alpha\alpha_{n-m-1}x^m+...+n\alpha\alpha_0x^{n-1}\\
&=\alpha(\alpha_{n-1}+2\alpha_{n-2}x+...+(m-1)\alpha_{n-(m-1)}x^{m-2}+m\alpha_{n-m}x^{m-1}\\
&\qquad+(m+1)\alpha_{n-m-1}x^m+...+n\alpha_0x^{n-1})\\
&=\alpha f'(x)
\end{aligned}
$$

(3) To Prove this part it is enough to prove it in the highly special case, $f(x)=x^i$ and $g(x)=x^j$ where i and j are positive. $g(x)f(x)=x^{i+j}$. Then,

$$
\begin{aligned}
(f(x)g(x))'&=ix^{i-1}x^j=(i+j)x^{i+j-1}.....(1)\\
f'(x)g(x)&=ix^{i-1}x^j.....(2)\\
f(x)g'(x)&=jx^ix^{j-1}.....(3)
\end{aligned}
$$

$(2)+(3)\Rightarrow f(x)g'(x)+f'(x)g(x)=(i+j)x^{i+j-1}=(f(x)g(x))$.

Remark 5.54 *If $f(x)$ and $g(x)$ in $F[x]$ have a non trivial common factor in $K[x]$, for K an extension of F then they have a non-trivial common factor in $F[x]$. For where they relatively prime as elements in $F[x]$, then they would be able to find two polynomials $a(x)$ and $b(x)$ in $F[x]$ such that $a(x)f(x)+b(x)g(x)$=1. Since this relation holds for those elements viewed as elements of $K[x]$, in $K[x]$ they would have to be relatively prime*

Lemma 5.55 *The polynomial $f(x)\in F[x]$ has a multiple root iff $f(x)$ and $f'(x)$ have a non-trivial (i.e. of positive degree) common factors.*

Proof: From the above remark, just may, we may assume without loss of generality, the roots of $f(x)$ are all lie in F (otherwise extend F to K, the splitting field of F). Suppose $f(x)$ has a multiple root α of multiplicity $m \geq 2$. Then $f(x) = (x-\alpha)^m q(x)$ and $q(\alpha) \neq 0,\ q(x) \in K[x]$.

$$\begin{aligned}\therefore f'(x) &= m(x-\alpha)^{m-1}q(x) + (x-\alpha)^m q'(x)\\ &= (x-\alpha)((x-\alpha)^{m-2}mq(x) + (x-\alpha)^{m-1}q'(x))\\ &= (x-\alpha)\cdot r(x)\ (\because m > 1)\\ &\quad \text{where } r(x) = (x-\alpha)^{m-2}mq(x) + (x-\alpha)^{m-1}q'(x).\end{aligned}$$

Also $f'(\alpha)$=0 (i.e.) α is a root of $f'(x)$. $\therefore f(x)$ and $f'(x)$ have the common factor $x-\alpha$. Conversely, suppose that $f(x)$ and $f'(x)$ have a non trivial common factor. To Prove: $f(x)$ has a multiple root. Suppose not, (i.e.) $f(x)$ has no multiple root. Then $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where α_i's are all distinct (We assume that $f(x)$ to be monic)

$$\begin{aligned}f'(x) &= (x \tilde{-} \alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) + (x-\alpha_1)(x \tilde{-} \alpha_2)\cdots(x-\alpha_n)\\ &\quad + (x-\alpha_1)(x-\alpha_2)\cdots(x \tilde{-} \alpha_n)\\ &= \sum_{i=1}^{n}(x-\alpha_1)(x-\alpha_2)\cdots(x \tilde{-} \alpha_i)\cdots(x-\alpha_n),\end{aligned}$$

where $\sim$ denote the term is omitted. Claim: No root of $f(x)$ is a root of $f'(x)$ (i.e. $f(x)$ and $f'(x)$ have no common factor)

$$\begin{aligned}&f'(\alpha i)\\ &= (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\cdots(\alpha_1-\alpha_n) + (\alpha_2-\alpha_1)(\alpha_2-\alpha_3)\cdots(\alpha_2-\alpha_n) +\\ &\ (\alpha_3-\alpha_1)(\alpha_3-\alpha_2)\cdots(\alpha_3-\alpha_n) + (\alpha_n-\alpha_1)(\alpha_n-\alpha_2)\cdots(\alpha_n-\alpha_{n-1})\\ &= \prod_{j\neq i}(\alpha_i-\alpha_j) \neq 0\ (\because \alpha_i \neq \alpha_j \text{ for } i \neq j)\end{aligned}$$

This show that $f'(x)$ =0 holds if one of the roots $\alpha_1, \alpha_2, ..., \alpha_n$ is a multiple root of $f(x)$. However if $f(x)$ and $f'(x)$ have a non trivial common factor, they have common root, namely, any root of this common that $f(x)$ has a multiple root.

Corollary 5.56 *If $f(x) \in F[x]$ is irreducible, then*

1. *if the characteristic of F is zero, $f(x)$ has no multiple root,*
2. *if the characteristic of F is $p \neq 0$, $f(x)$ has a multiple root only if it is of the form $f(x) = g(x^p)$.*

Proof: (1) Let $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + ... + \alpha_{n-1}x + \alpha_n, \alpha_0 \neq 0$ be an irreducible polynomial of degree $n \geq 1$ over a field F of characteristic zero.

Then $f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + ... + \alpha_{n-1}$. Since F is of characteristic zero and $\alpha_0 \neq 0$, then $n\alpha_0 \neq 0$. $\therefore f'(x) \neq 0$, also $deg(f'(x)) < deg(f(x))$. To Prove: $f(x)$ has no multiple root. Suppose if possible $f(x)$ has a multiple root (say α). Then by above lemma, $f(x)$ and $f'(x)$ have a non-trivial common factor and hence $f(x)/f'(x)$. But $f'(x) \neq 0$ and $f(x)$ and $f'(x)$ both being irreducible with deg $f'(x) < degf(x)$. This shows that $f(x)$ does not divides $f'(x)$
$\Rightarrow\Leftarrow$ to $f(x)/f'(x)$ (i.e.) if α is not a root $f(x)$ then α is not a multiple root of $f(x)$ hence $f(x)$ has no multiple root.
(2) In this case characteristic of F is $p \neq 0$. Suppose α is a multiple root of $f(x)$. Let $f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n, \alpha_n \neq 0$. Let $f'(x) = \alpha_1 + 2\alpha_2 x + ... + n\alpha_n x^{n-1}$. Now, since $f(x)$ has a multiple root, $f'(x) = 0$ (i.e.) $\alpha_1 + 2\alpha_2 x + ... + n\alpha_n x^{n-1} = 0 = 0 + 0x + 0x^2 + ... + 0x^{n-1} \Rightarrow \alpha_1 = 2\alpha_2 = 3\alpha_3 = ... = n\alpha_n = 0$ (i.e.) for any $k, 1 \leq k \leq n, k\alpha_k = 0$. Since F is of characteristic $p \geq 0, p/k$ or $\alpha_k = 0$. Thus when $f'(x) = 0$ we see that if for any $k.\alpha_k \neq 0$ then $p/k \Rightarrow k = k_1 p$. That means $f(x)$, if any term $\alpha_k x^k$ has $\alpha_k \neq 0$ then it is of the form $\alpha_{k_1 p} x^{k_1 p} = \alpha_{k_1 p}(x^p)^{k_1}$ so that $f(x)$ is of the form $\beta_0 + \beta_1 x^p + \beta_2 (x^p)^2 + ... + \beta_n (x^p)^n$ for some positive integer n then $f(x) \in F[x^p]$. $f(x)$ is of the form $g(x^p)$.

Corollary 5.57 *If F is a field of characteristic $p \neq 0$ then the polynomial $x^{p^n} - x \in F[x]$ for $n \geq 1$ has distinct roots.*
Proof: Let $f(x) = x^{p^n} - x$. Then $f'(x) = p^n x^{p^n - 1} - 1$..... (1)
Now $p \in F$, we mean 1+1+...+1 (p times). Since F is of characteristic p, the order of element of the additive group of F is p, p=1+1+...+1 (p times). Hence $p^n = 0 \Rightarrow f(x) = -1$. Now we see that $f(x)$ and $f'(x)$ have non trivial common factor. By Lemma 5.55, $f(x)$ has no multiple roots. Hence $f(x)$ has distinct roots.

Definition 5.58 *The extension K of a field F is called a simple extension of F if $K = F(\alpha)$ for some $\alpha \in K$.*

Theorem 5.59 *If F is of characteristic zero and if a, b are algebraic over F then there exists an element $c \in F(a, b)$ such that $F(a, b) = F(c)$.*
Proof: Given, F is of characteristic zero. Let $f(x), g(x)$ be the irreducible polynomial over F of a and b respectively and let m, n be their respective degrees. Let K be an extension of F in which both $f(x)$ and $g(x)$ splits completely (i.e.) K is the splitting field of $f(x)$ and $g(x)$ over F then $a, b \in K$. Clearly, every root of $f(x)$ is a root of $f(x)g(x)$ and K contains the splitting field of $f(x)$. Since the characteristic of F is zero all roots of $f(x)$ and $g(x)$ are distinct (by Corollary 5.56). Let $f(x)$ has m distinct roots say $a = a_1, a_2, ..., a_m$ in K and $g(x)$ has n distinct roots say $b = b_1, b_2, ..., b_n$ in K. If $j \neq 1$ then $b_j \neq b_1 = b$ (i.e.) $b - b_j \neq 0$. We can solve the equation $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$ has only one solution λ in K namely,

$\lambda = \frac{a_i - a}{b - b_j} \in K$. These λ's are finite numbers. As F is of characteristic zero. F has infinite number of elements. So we can find an element $r \in F$ such that $a_i + rb_j = a + rb \ \forall i$ and $\forall j \neq$ (i.e.) $i, j \geq 2$. Let $c = a + \sqrt{b} \in F(a, b)$. Claim: $F(c) = F(a, b)$. Since $a, b \in F(a, b)$, $a + \sqrt{b} \in F(a, b) \Rightarrow c \in F(a, b) \Rightarrow F(c) = F(a, b)$..... (1)
Let $K = F(c)$. Since b is a root of $g(x), (x - b)$ is a factor of $g(x)$. Let $h(x) = f(c - rx)$. Then $h(b) = 0 \Rightarrow b$ is a root of $h(x) \Rightarrow (x - b)$ is a factor of $h(x)$. (i.e.) $(x - b)$ is a common factor of $h(x)$ and $g(x)$. If $j \neq 1, h(b_j) = f(c - rb_j) \neq f(a) \neq 0 \Rightarrow f(c - rb_j) \neq 0$ (i.e.) $(x - b_j)$ is not a factor of $h(x)$. Also $(x - b)^2$ does not divides $g(x), (x - b)^2$ cannot divide the gcd of $h(x)$ and $g(x)$. Thus, $(x - b)$ is a gcd of $h(x)$ and $g(x)$ over F of K. But then they have a non trivial gcd over K which must be divisor of $(x - b)$. Since $deg(x - b) = 1$ we see that the gcd of $g(x)$ and $h(x)$ in $K[x]$ is exactly $x - b$. Thus $x - b \in K[x]$. Hence $b \in K = F(c) \Rightarrow b \in F(c)$. Since $b, c \in F(c)$ and $r \in F(c) \supset F \Rightarrow c - rb \in F(c) \Rightarrow a = c - rb \in F(c) \Rightarrow a, b \in F(c) \Rightarrow F(a, b) \subset F(c)$..... (2)
From (1) and (2), $\Rightarrow F(a, b) = F(c)$.

Corollary 5.60 *Any finite extension of a field of characteristic zero is a simple extension.*
Proof: Let $\alpha_1, \alpha_2, ..., \alpha_n$ be algebraic over F of characteristic zero. Then by repeated use of the preceding theorem we have,

$$\begin{aligned} F(\alpha_1, \alpha_2, ..., \alpha_n) &= K \\ &= F(\alpha_1, \alpha_2), (\alpha_3, \alpha_4, ..., \alpha_n) \\ &= F(\gamma_1), (\alpha_3, \alpha_4, ..., \alpha_n) \ \ \because F(\alpha_1, \alpha_2) = F(\gamma_1) \\ &= F(\gamma_1, \alpha_3), (\alpha_4, ..., \alpha_n) \\ &= F(\gamma_2), (\alpha_4, \alpha_5, ..., \alpha_n) \\ &\ \ . \\ &\ \ . \\ &\ \ . \\ &= F(\gamma_{n-2}), \alpha_n \\ &= F(\gamma_{n-1}) \end{aligned}$$

$F(\alpha_1, \alpha_2, ..., \alpha_n)$ is a simple extension of F.

Course Material Prepared by
Dr. S. PIOUS MISSIER
Associate Professor, P.G. and Research Department of Mathematics
V. O. Chidambaram College, Tuticorin - 628 008.