SHIVAJI UNIVERSITY, KOLHAPUR

CENTRE FOR DISTANCE EDUCATION

Algebra-I

(Mathematics)

For

M. Sc. Part-I

First Edition 2008
Second Edition 2010

Prescribed for **M. Sc. Part-I**

Copies : 1,000

Published by:
Dr. D. V. Muley
Registrar,
Shivaji University,
Kolhapur-416 004

Printed by :

Shri. A. S. Mane,
I/c. Superintendent,
Shivaji University Press,
Kolhapur-416 004

ISBN-978-81-8486-080-1

★ Further information about the Centre for Distance Education & Shivaji University may be obtained from the University Office at Vidyanagar, Kolhapur-416 004, India.

★ This material has been produced with the developmental grant from DEC-IGNOU, New Delhi.

Centre for Distance Education
Shivaji University, Kolhapur

Centre for Distance Education
Shivaji University,
Kolhapur.

Algebra-I

Writing Team	Unit No.
Dr. Y. S. Powar Dept. of Mathematics, Shivaji University, Kolhapur.	**All**

■ Editor ■

Dr. Y. S. Powar
Department of Mathematics,
Shivaji University, Kolhapur.
Maharashtra.

Preface

This book in the form of "Notes of Algebra-I" is a natural outgrowth of the lectures delivered for M. Sc. Part-I students of Shivaji University. The primary purpose of this book is to facilitate the post graduate education in Algebra. The topics in the book will cover the syllabus of Algebra-I in detail for M. Sc. (Part-I) external students. For the basic ideas in Group theory and Ring theory students are advised to read in detail the other text books of Algebra.

First chapter deals with Group theory and it covers the following articles 1) Isomorphism theorems, 2) Soluable groups, 3) Series of Groups, 4) Sylow theorems.

The second Chapter is on Ring theory and it especially deals with polynomial rings.

In the third chapter we discuss Module theory, where modules are the generalization of vector spaces which students have studied in their B. Sc. course. The list of the articles in this chapter is as follows.

1) Modules 2) Sum and direct sum of submodules 3) Noetherian and Artenian Modules.

We owe a deep sense of gratitude to the Vice-Chancellor Dr. N. J. Pawar who has given impetus to go ahead with ambitious projects like the present one. Dr. L. N. Katkar, Head, Department of Mathematics, Shivaji University has to be profusely thanked for the ovation he has poured to prepare the SIM on Algebra. We also thank the Director of Distance Education Mode Mrs. Cima Yeole and Deputy Director Shri. S. S. Patil for their help and keen interest in completion of the SIM.

Prof. S. R. Bhosale
Chairman BOS in Mathematics
Shivaji University, Kolhapur-416004.

M. Sc. (Mathematics)

Algebra-I

Contents

CHAPTER I - GROUPS

Unit 1 : Isomorphism theorems :

1.1 Basic definitions and results

1.2 Isomorphism Theorems

1.1 Basic Definitions and Results :

Definition 1.1.1: A group $\langle G, *\rangle$ is a set G together with a binary operation $*$ defined on G, satisfying the following axioms.

(i) $a * (b * c) = (a * b) * c$

(ii) There exists an element $e \in G$ such that $e * a = a = a * e$.

(iii) For each $a \in G$, there is an element $a' \in G$ such that $a * a' = e = a' * a$.

for all $a, b \in G$.

The element e is called an identity element for $*$ in G and the element a' is called the inverse of a with respect to $*$ in G.

Generally, we use ‘ $\cdot$ ’ for a binary operation in a group G and $x \cdot y$ is denoted by xy simply.

Definition 1.1.2: A group G is abelian if its binary operation $*$ is commutative.

i.e. $ab = ba$ for all $a, b \in G$

Definition 1.1.3: Let H be a subset of a group G. If H is itself a group under the induced binary operation defined on G, then H is a sub group of G. We denote this by $H \leq G$.

G is the improper subgroup of G. All other subgroups of G are proper subgroups. Also $\{e\}$ is the trivial subgroup of G. All other subgroups are non trivial.

Definition 1.1.4: Let G be a group and let $a \in G$. Then the subgroup $H = \{a^n \,/\, n \in Z\}$ of G is called the cyclic subgroup of G generated by a and it is denoted by $< a >$.

(here $a^n = a \cdot a \cdot \ldots \cdot a$ n times)

Definition 1.1.5: An element a of group G generates G (or a is generator for G) if $< a > = G$.

A group G is cyclic if there is some element a in G that generates G.

Definition 1.1.6: A permutation of a set A is a function from A into A that is both one-one and onto.

Definition 1.1.7: If A is a finite set $\{1, 2, \dots, n\}$, then the group of all permutations of A is the symmetric group of n letters and is denoted by S_n. [Note that $|S_n| = n\,!$].

Definition 1.1.8: The subgroup of S_n consisting of even permutations of n letters is the alternating group A_n of n letters. [Note that, $|A_n| = \frac{n!}{2}$]

Definition 1.1.9: Let G_1 and G_2 be any groups. A mapping $\phi : G_1 \longrightarrow G_2$ is a homomorphism if

$$\phi(xy) = \phi(x) \cdot \phi(y) \qquad \text{for all } x, y \in G_1$$

An isomorphism of a group G_1 with a group G_2 is a one to one homomorphism of G_1 onto G_2.

Definition 1.1.10: Let H and K be subgroups of a group G. The join $H \vee K$ of H and K is the intersection of all subgroups of G containing $HK = \{hk \,/\, h \in H,\ k \in K\}$.

$H \vee K$ is the smallest subgroup of G containing both H and K.

Definition 1.1.11: Let H and K be subgroups of a group G. G is the internal direct product of the subgroups H and K if the mapping $\phi : H \times K \longrightarrow G$ defined by $\phi(h, k) = h \cdot k$ is an isomorphism.

In this case any $g \in G$ can be uniquely written as $g = h \cdot k,\ h \in H$ and $k \in K$. We can generalize this definition for any finite n.

Definition 1.1.12: Let G be group and let $a_i \in G$, for $i \in I$ (I is an indexing set). The smallest subgroup of G containing $\{a_i \,/\, i \in I\}$ is the subgroup generated by $\{a_i \,/\, i \in I\}$. If this subgroup is all of G, then we say $\{a_i \,/\, i \in I\}$ generates G and $a_i's$ are the generators of G. If there exists a finite set $\{a_i \,/\, i \in I\}$ that generates G, then we say G is finitely generated.

Definition 1.1.13: Let H be subgroup of G and let $a \in G$. The left coset aH of H is the set $\{ah \,/\, h \in H\}$. The right coset Ha is similarly defined.

Definition 1.1.14: Let H be subgroup of group G. The number of left cosets of H in G is the index of H in G and is denoted by $(G : H)$

If G is finite, then $(G : H)$ is finite and $(G : H) = \frac{|G|}{|H|}$.

Definition 1.1.15: A subgroup H of group G is a normal subgroup of G if $g^{-1}Hg = H$ for all $g \in G$. We denote this by $H \trianglelefteq G$.

Obviously, H is normal iff $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

Definition 1.1.16: Two subgroups H and K of a group G are conjugate of each other if $H = g^{-1}Kg,$ for some $g \in G$.

Definition 1.1.17: If N is a normal subgroup of a group G, the group of right/left cosets of N under induced operation is the factor (quotient) group of G modulo N and is denoted by $\frac{G}{N}$.

Definition 1.1.18: A group G is simple if it has no proper, nontrivial normal subgroups.

i.e. if $H \leq G$ then either $H = \{e\}$ or $H = G$.

Definition 1.1.19 : An element $aba^{-1}b^{-1}$ in a group G $(a, b \in G)$ is called a commutator of a and b in G.

Definition 1.1.20 : The kernel of a homomorphism ϕ of a group G into a group G' is the set of all elements of G mapped onto the identity element of G' by ϕ. This is denoted by $ker\ \phi$.

Thus, $ker\ \phi = \{x \in G / \phi(x) = e'\}$.

Definition 1.1.21: Let G be a group. S is any non empty subset of G. The normalizer of S in G is the set $N[S] = \{x \in G / xSx^{-1} = S\}$.

The normalizer of $\{a\}$ is denoted by $N[a]$.

Definition 1.1.22: Let G be a group and $a \in G$. The set $C(a) = \{xax^{-1} / x \in G\}$ is called the conjugate of a in G.

Theorem 1.1.23: If H and K are subgroup of a group G, then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof : Let $|H| = r$, $|K| = s$ and $|H \cap K| = t$.

$HK = \{h \cdot k \ / \ h \in H \text{ and } k \in K\}$

Then $|HK| \leq |H| \cdot |K| = r \cdot s$

(i) Let $h_1 k_1 = h_2 k_2$ for some $h_1 h_2 \in H$ and $k_1, k_2 \in K$.

Let $x = h_2^{-1} h_1 = k_2 k_1^{-1}$.

Then $x = h_2^{-1} h_1 \implies x \in H$ and $x = k_2 k_1^{-1} \implies x \in K$.

Thus $x \in H \cap K$ and further

$h_2 = h_1 x^{-1}$ and $k_2 = x k_1$

Thus $h_1 k_1 = h_2 k_2 \implies \exists\ x \in H \cap K$ such that $h_2 = h_1 x^{-1}$ and $k_2 = x k_1$.

(ii) Suppose $\exists\ y \in H \cap K$ such that

$h_3 = h_1 y^{-1}$ and $k_3 = y k_1$ for some $h_1 h_3 \in H$ and $k_1 k_3 \in K$.

But then $h_3 k_3 = h_1 y^{-1} \cdot y k_1 = h_1 k_1$.

Thus given $y \in H \cap K$, $h_1 y^{-1}$ and $y k_1$ in HK will produce the element $h_1 k_1$.

From (1) and (2), we get that there exists a one-one onto correspondence between the repeated elements in HK and the elements of $H \cap K$. Thus any element $hk \in HK$ can be represented in the form of $h_i k_i$ for $h_i \in H$ and $k_i \in K$ for all i, $1 \leq i \leq t$.

Hence

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

1.2 Isomorphism Theorems:

Theorem 1.2.1: A group G is the internal direct product of subgroups H and K if and only if

(i) $G = H \vee K$

(ii) $hk = kh$ for all $h \in H$ and $k \in K$.

(iii) $H \cap K = \{e\}$

Proof : <u>Only if part :</u>

Let G be internal direct product of H and K. Hence $\phi: H \times K \longrightarrow G$ defined by

$$\phi(h,k) = hk$$

is an isomorphism.

Define

$$\bar{H} = \{(h,e)/h \in H\} \quad \text{and} \quad \bar{K} = \{(e,k)/k \in K\}.$$

Then $\bar{H} \leq H \times K$ and $\bar{K} \leq H \times K$.

Further $\bar{H} \vee \bar{K} = H \times K$; $\bar{H} \cap \bar{K} = \{(e,e)\}$

$(h,e) \in \bar{H}$ and $(e,k) \in \bar{K} \implies (h,e)(e,k) = (h,k)$

and $(e,k)(h,e) = (h,k)$.

Hence, $(h,e)(e,k) = (e,k)(h,e)$.

Therefore we get

(i) $\bar{H} \vee \bar{K} = H \times K$

(ii) $(h,e)(e,k) = (e,k)(h,e)$, for all $(h,e) \in \bar{H}$ and $(e,k) \in \bar{K}$.

(iii) $\bar{H} \cap \bar{K} = \{(e,e)\}$

As $\phi : H \times K \longrightarrow G$ is an isomorphism we get $\phi(\bar{H}) = H$ and $\phi(\bar{K}) = K$ and $\phi(H \times K) = G$. Hence we get

(i) $G = H \vee K$.

(ii) $hk = kh$ for all $h \in H$ and $k \in K$.

(iii) $H \cap K = \{e\}$

<u>If part :</u>

Define $\phi : H \times K \longrightarrow G$ by

$$\phi(h,k) = h.k$$

To prove that ϕ is an isomorphism.

(i) ϕ is a well defined map.

$(h_1, k_1) = (h_2, k_2) \implies h_1 = h_2$ and $k_1 = k_2$

$\implies h_1k_1 = h_2k_2 \implies \phi(h_1, k_1) = \phi(h_2, k_2)$

(ii) ϕ is one one.

Let $\phi(h_1, k_1) = \phi(h_2, k_2)$

Then $h_1 k_1 = h_2 k_2$

and hence $h_2^{-1} h_1 = k_2 k_1^{-1}$

But $h_2^{-1} h_1 \in H$ and $k_2 k_1^{-1} \in K$

and hence $h_2^{-1} h_1 \in H \cap K = \{e\}$ and $k_2 k_1^{-1} \in H \cap K = \{e\}$.

Thus $h_2^{-1} h_1 = e$ and $k_2 k_1^{-1} = e$, proving that $h_1 = h_2$ and $k_1 = k_2$.

Hence $(h_1,\ k_1) = (h_2, k_2)$

This shows that ϕ is one-one.

(iii) ϕ is onto.

Let $g \in G$. As $hk = kh$ for all $h \in H$ and $k \in K$. We get HK is a subgroup of G and hence $H \vee K = HK$. But by (i) $H \vee K = G$. Therefore $G = HK$. Thus $g \in G$ can be expressed as $g = hk$ for some $h \in H$ and $k \in K$. And we get $\phi(h, k) = g$.

This shows that ϕ is onto.

(iv) ϕ is a homomorphism.

$$\begin{aligned}
\phi[(h_1,\ k_1)\ (h_2, k_2)] &= \phi(h_1 h_2,\ k_1 k_2) \\
&= h_1 h_2\ k_1 k_2 \\
&= h_1\ [\ k_1 h_2]\ k_2 && \dots \text{by (2)} \\
&= (h_1 . k_1)\ (h_2 . k_2) \\
&= \phi(h_1,\ k_1)\ \phi(h_2, k_2)
\end{aligned}$$

From (i), (ii), (iii) and (iv), we get ϕ is an isomorphism. Hence $G = H \times K$.

Theorem 1.2.2: Let N be a normal subgroup of G.

Then the map $f\ :\ G \longrightarrow \frac{G}{N}$ defined by

$$f(g) = N_g\ , \qquad \text{for } g \in G$$

is an onto homomorphism.

Proof : f is obviously onto.

Now $f(g_1 g_2) = N_{g_1 g_2} = \left(N_{g_1}\right)\left(N_{g_2}\right) = f(g_1) \cdot f(g_2)$, for all $g_1,\ g_2 \in G$

Shows that f is a homomorphism.

Hence f is an onto homomorphism.

Remark : This map f is called natural or canonical homomorphism.

Theorem 1.2.3: Let G and G' be any groups. For any homomorphism $\phi\ :\ G \longrightarrow G'$, kernel of ϕ is a normal subgroup of G.

Proof :

(i) $ker\ \phi = \{x \in G \mid \phi(x) = e'\}$. As $e \in ker\phi$; $ker\phi$ is non empty set.

(ii) Let $x, y \in ker\ \phi$.

$\phi(xy) = \phi(x) \cdot \phi(y)$ ….. $\because$ ϕ is homomorphism.

$= e' \cdot e'$ ..... $\because \quad x, y \in ker\ \phi$

$= e'$

Thus $\phi(xy) = e'$.

Hence $x.y \in ker\ \phi$.

(iii) Let $x \in ker\ \phi$. Then $\phi(x) = e'$.

As $\phi(x^{-1}) = [\phi(x)]^{-1} = [e']^{-1} = e'$ shows that $x^{-1} \in ker\ \phi$.

From (i), (ii) and (iii) we get $ker\phi$ is a subgroup of G.

(iv) Let $n \in ker\ \phi$ and $g \in G$. Then

$$\phi(g^{-1}ng) = \phi(g^{-1})\ \phi(n)\ \phi(g)$$
$$= [\phi(g)]^{-1} \cdot e' \cdot \phi(g)$$
$$= e'$$

Hence $g^{-1}ng \in ker\phi$, for all $g \in G$ and $n \in N$.

Thus shows that $ker\phi$ is a normal subgroup of G.

Theorem 1.2.4: Let G and G' be groups. $\phi : G \longrightarrow G'$ is a homomorphism.

(i) $H \leq G \implies \phi(H) \leq G'$

(ii) $H \trianglelefteq G \implies \phi(H) \trianglelefteq G'$

(iii) $K' \leq G' \implies \phi^{-1}(K') \leq G$

(iv) $K' \trianglelefteq G' \implies \phi^{-1}(K') \trianglelefteq G$

Proof : Proof is obvious and hence omitted.

- ***First Isomorphism Theorem :***

Theorem 1.2.5: Every homomorphic image of a group is isomorphic with its suitable quotient group.

OR Let G and G' be groups and let $\phi: G \longrightarrow G'$ be an onto homomorphism.

Then $G' \cong \frac{G}{ker\phi}$.

Proof : Let $\phi: G \longrightarrow G'$ be onto homomorphism. Then $G' = \phi(G) = \{\phi(x)/x \in G\}$.

Let $N = ker\phi$. Then $N \trianglelefteq G$ (Seer theorem 0.4).

Let $\psi : G \longrightarrow \frac{G}{N}$ be canonical mapping. Then ψ is an onto homomorphism. (See theorem 1.2.2).

Define $\gamma : \frac{G}{N} \longrightarrow G' = \phi(G)$ by

$$\gamma\left(N_g\right) = \phi(g)\,, \qquad \text{for } g \in G$$

Claim 1 : ϕ is well defined map.

Let $N_{g_1} = N_{g_2}$ for some $g_1,\ g_2 \in G$

$$\begin{aligned} N_{g_1} = N_{g_2} &\Longrightarrow\ g_1\, g_2^{-1} \in N \\ &\Longrightarrow\ g_1\, g_2^{-1} \in ker\phi \\ &\Longrightarrow\ \phi\,(g_1\, g_2^{-1}) = e' \\ &\Longrightarrow\ \phi\,(g_1)\cdot\phi(\,g_2^{-1}) = e' \\ &\Longrightarrow\ \phi\,(g_1)\cdot[\phi(\,g_2)]^{-1} = e' \\ &\Longrightarrow\ \phi\,(g_1) = \phi(\,g_2) \\ &\Longrightarrow\ \gamma\left(N_{g_1}\right) = \gamma\left(N_{g_2}\right) \end{aligned}$$

This shows that γ is well defined.

Claim 2 : γ is a homomorphism.

$$\begin{aligned} \gamma\left(N_{g_1}\cdot N_{g_2}\right) &= \gamma\left(N_{g_1 g_2}\right) \\ &= \phi(g_1\, g_2) \\ &= \phi(g_1)\,\phi(g_2) \\ &= \gamma\left(N_{g_1}\right)\cdot\gamma\left(N_{g_2}\right) \qquad \text{for any } N_{g_1},\ N_{g_2} \in \frac{G}{N} \end{aligned}$$

This shows that γ is a homomorphism.

Claim 3 : γ is onto.

Let $y \in G'$. ϕ being onto, there exists $x \in G$ such that $\phi(x) = y$. For this $x \in G$, $N_x \in \frac{G}{N}$ and $\gamma(N_x) = \phi(x) = y$. This shows that γ is onto.

Claim 4 : γ is one-one.

Let $\gamma(N_x) = \gamma\left(N_y\right)$ for some $x, y \in G$

$$\begin{aligned} \gamma(N_x) = \gamma\left(N_y\right) &\Longrightarrow\ \phi(x) = \phi(y) \\ &\Longrightarrow\ \phi\,(x)\cdot[\phi(\,y)]^{-1} = e' \\ &\Longrightarrow\ \phi\,(x)\cdot\phi(y^{-1}) = e' \\ &\Longrightarrow\ \phi\,(xy^{-1}) = e' \\ &\Longrightarrow\ xy^{-1} \in ker\phi = N \\ &\Longrightarrow\ N_x = N_y \end{aligned}$$

Thus $\gamma(N_x) = \gamma\left(N_y\right) \Longrightarrow N_x = N_y$.

Hence γ is one-one.

From claims (i) to (iv) it follows that γ is an isomorphism and hence $\frac{G}{ker\phi} \cong G'$.

Diagrammatically we represent the theorem as follows.

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, "\psi"'] & G' = \phi(G) \\ \dfrac{G}{N = ker\phi} \arrow[ur, "\gamma"'] & \end{tikzcd} \qquad \begin{tikzcd} g \arrow[r, "\phi"] \arrow[d, "\psi"'] & \phi(g) \\ N_g \arrow[ur, "\gamma"'] & \end{tikzcd}$$

$$(N = ker\phi)$$

- ***Second Isomorphism Theorem :***

Theorem 1.2.6: H is a subgroup of group G and N is a normal subgroup of a group G. Then $\frac{HN}{N} \cong \frac{H}{H \cap N}$

Proof : $H \leq G$ and $N \trianglelefteq G \Longrightarrow HN \leq G$

Further $N \leq HN$ and $N \trianglelefteq G \Longrightarrow N \trianglelefteq HN$

Hence $\frac{HN}{N}$ is defined.

$H \cap N \trianglelefteq H \Longrightarrow \frac{H}{H \cap N}$ is defined.

Define $\phi : HN \longrightarrow \frac{H}{H \cap N}$ by

$\phi(hn) = (H \cap N)\, h$ for $h \in H$ and $n \in N$

<u>Claim 1 :</u> ϕ is well defined.

Let $h_1n_1 = h_2n_2$ for $h_1, h_2 \in H$ and $n_1, n_2 \in N$.

$h_1n_1 = h_2n_2 \Longrightarrow h_2^{-1}\, h_1 = n_2n_1^{-1}$

$h_2^{-1}\, h_1 \in H$ and $n_2n_1^{-1} \in N$.

Hence $h_2^{-1}\, h_1 = n_2n_1^{-1} \Longrightarrow h_2^{-1}\, h_1 \in H \cap N$

$\Longrightarrow (H \cap N)\, h_1 = (H \cap N)\, h_2$

$\Longrightarrow \phi\,(h_1n_1) = \phi\,(h_2n_2)$

This shows that ϕ is well defined.

<u>Claim 2 :</u> ϕ is a homomorphism.

$\phi\,[(h_1n_1)(h_2n_2)]$ .... $h_1, h_2 \in H$ and $n_1, n_2 \in N$

$= \phi\,[h_1\,(n_1h_2)\,n_2]$ .... $N \trianglelefteq G \Longrightarrow hN = Nh$

$= \phi\,[h_1\,(h_2n_3)\,n_2]$ Hence $n_1h_2 = h_2n_3$ for some $n_3 \in N$

$= \phi\,[(h_1h_2)(n_3n_2)]$

$= (H \cap N)\, h_1 h_2$

$= [(H \cap N)\, h_1]\, [(H \cap N)\, h_2]$

$= \phi\, (h_1 n_1)\, \phi\, (h_2 n_2)$

This shows that ϕ is a homomorphism.

<u>Claim 3 :</u> ϕ is onto.

Let $(H \cap N)\, h \in \frac{H}{H \cap N}$. Then $h \in H$.

As $h \in H \implies h \cdot e \in HN$ and $\phi(he) = (H \cap N)\, h$.

This shows that ϕ is onto.

From claim 1, claim 2 and claim 3, ϕ is an onto homomorphism. Hence by 1st isomorphism theorem,

$$\frac{HN}{ker\phi} \cong \frac{H}{H \cap N} \qquad \text{. . . (1)}$$

Now,

$ker\phi = \{hn \in HN \ / \ \phi(hn) = (H \cap N)\}$

$= \{hn \in HN \ / \ (H \cap N)h = (H \cap N)\}$

$= \{hn \in HN \ / \ h \in (H \cap N)\}$

$= N$ ... $\because\ h \in H \cap N \implies h \in N$

$\implies h \cdot n \in N$ for $h \in H$ and $n \in N$

Thus $ker\phi = N$ . . . (2)

From (1) and (2) we get

$$\frac{HN}{N} \cong \frac{H}{H \cap N}$$

- ***Third Isomorphism Theorem :***

Theorem 1.2.7: Let H and K be normal subgroups of a group G with $K \leq H$. Then

$$\frac{G}{H} \cong \frac{G/K}{H/K}$$

Proof : Let H and K are normal in G and $K \leq H$. Therefore K is a normal subgroup of H.

Thus $\frac{G}{H}, \frac{G}{K}, \frac{H}{K}$ are all defined.

Define $\phi : G \longrightarrow \frac{G/K}{H/K}$ by

$$\phi(g) = \left(\frac{H}{K}\right) \cdot \left(K_g\right) \qquad \text{for each } g \in G.$$

Claim 1 : ϕ is well defined.

Let $g_1 = g_2$ in G.

$$g_1 = g_2 \implies K_{g_1} = K_{g_2}$$
$$\implies \left(\frac{H}{K}\right) \cdot K_{g_1} = \left(\frac{H}{K}\right) \cdot K_{g_2}$$
$$\implies \phi\,(g_1) = \phi\,(g_2)$$

Hence ϕ is well defined.

Claim 2 : ϕ is homomorphism..

Let $g_1, g_2 \in G$.

$$\phi(g_1\, g_2) = \left(\frac{H}{K}\right) \cdot K_{g_1\, g_2}$$
$$= \left(\frac{H}{K}\right) \cdot [K_{g_1} \cdot K_{g_2}]$$
$$= \left\{\left(\frac{H}{K}\right) \cdot K_{g_1}\right\}\left\{\left(\frac{H}{K}\right) \cdot K_{g_2}\right\}$$
$$= \phi(g_1) \cdot \phi(g_2)$$

This shows that ϕ is homomorphism.

Claim 3 : ϕ is onto.

Let $\left(\frac{H}{K}\right) \cdot K_a \in \left(\frac{G/K}{H/K}\right)$. Then $a \in G$. For this $a \in G$ we get $\phi(a) = \left(\frac{H}{K}\right) \cdot K_a$.

Therefore ϕ is onto.

From claim 1, claim 2 and claim 3, ϕ is an onto homomorphism. Hence by 1st isomorphism theorem,

$$\frac{G}{ker\phi} \cong \frac{G/K}{H/K} \qquad \ldots (1)$$

Now,

$$ker\phi = \{x \in G \;/\; \phi(x) = (H/K)\}$$
$$= \{x \in G \;/\; (H/K)(K_x) = (H/K)\}$$
$$= \{x \in G \;/\; K_x \in (H/K)\}$$
$$= \{x \in G \;/\; x \in H\}$$

Thus $ker\phi = H$ . . . (2)

From (1) and (2) we get

$$\frac{G}{H} \cong \frac{G/K}{H/K}$$

- ***Zassenhaus Lemma :***

Theorem 1.2.8: Let H and K be subgroups of group G. H^* and K^* be normal subgroups of H and K respecively. Then

(i) $H^*(H \cap K^*)$ is a normal subgroup of $H^*(H \cap K)$.

(ii) $K^*(H^* \cap K)$ is a normal subgroup of $K^*(H \cap K)$.

(iii) $\frac{H^*(H \cap K)}{H^*(H \cap K^*)} \cong \frac{K^*(H \cap K)}{K^*(H^* \cap K)} \cong \frac{H \cap K}{(H^* \cap K) \cdot (K^* \cap H)}$

Proof :

(i) $H \cap K \leq H, \quad H^* \trianglelefteq H \quad \Rightarrow \quad H^* \cdot (H \cap K) \leq H.$

(ii) $H \cap K \leq K, \quad K^* \trianglelefteq K \quad \Rightarrow \quad K^* \cdot (H \cap K) \leq K.$

(iii) $H^* \cap K \trianglelefteq H$ and $H^* \cap K \leq K$

Hence $H^* \cap K \trianglelefteq H \cap K.$

Similarly, $K^* \cap H \trianglelefteq H \cap K.$

Hence $(H^* \cap K) \cdot (K^* \cap H) \trianglelefteq (H \cap K).$

Therefore $\frac{H \cap K}{(H^* \cap K) \cdot (K^* \cap H)}$ is defined.

Put $L = (H^* \cap K) \cdot (K^* \cap H)$. Thus $L \trianglelefteq (H \cap K)$.

(iv) Define $\phi : H^*(H \cap K) \longrightarrow \frac{(H \cap K)}{L}$ by

$$\phi(hx) = Lx$$

where $h \in H^*$ and $x \in H \cap K$.

<u>Claim 1 :</u> ϕ is well defined.

Let $h_1 x_1 = h_2 x_2$ for $h_1, h_2 \in H^*$ and $x \in H \cap K$.

Then $h_2^{-1} h_1 = x_2 x_1^{-1}$ for $h_2^{-1} h_1 \in H^*$ and $x_2 x_1^{-1} \in H \cap K$.

Hence $h_2^{-1} h_1 = x_2 x_1^{-1} \Rightarrow h_2^{-1} h_1 \in H^* \cap (H \cap K)$

$\Rightarrow h_2^{-1} h_1 \in H^* \cap K \subseteq L$

$\Rightarrow h_2^{-1} h_1 \in L$

$\Rightarrow x_2 x_1^{-1} \in L$

$\Rightarrow L_{x_1} = L_{x_2}$

$\Rightarrow \phi\,(h_1 x_1) = \phi(h_2 x_2)$

This shows that ϕ is a well defined map.

<u>Claim 2 :</u> ϕ is homomorphism.

Let $h_1x_1,\ h_2x_2 \in H^*(H \cap K)$. Then $h_1, h_2 \in H^*$ and $x_1, x_2 \in H \cap K$.

As $H^* \trianglelefteq H$ and $x_1 \in H$ we get $x_1H^* = H^*x_1$. Thus $x_1h_2 \in x_1H^*$ implies $x_1h_2 \in H^*x_1$.

Hence $x_1h_2 = h_3x_1$ for some $h_3 \in H^*$. Hence we get

$\phi\ [(h_1x_1)(h_2x_2)] = \phi\ [h_1(x_1h_2)x_2]$ ... By associativity.

$= \phi\ [h_1(h_3x_1)x_2]$ ... $x_1h_2 = h_3x_1$.

$= \phi\ [(h_1\ h_3)\ (x_1\ x_2)]$ ... By associativity.

$= L_{x_1\,x_2}$ ... By definition of ϕ.

$= L_{x_1} \cdot L_{x_2}$

$= \phi\ (h_1x_1)\ \phi(h_2x_2)$

This shows that ϕ is a homomorphism.

Claim 3 : ϕ is onto.

Let $L_x \in \frac{H \cap K}{L}$. Then $x \in H \cap K$.

Hence, $e \cdot x \in H^* \cdot (H \cap K)$ and $\phi\ (ex) = L_x$. This shows that ϕ is onto.

Thus, from claim 1, claim 2 and claim 3 we get $\frac{H \cap K}{L}$ is a homomorphic image of $H^* \cdot (H \cap K)$.

Hence, by first isomorphism theorem,

$$\frac{H\cap K}{L} \cong \frac{H^*\cdot(H\cap K)}{ker\phi} \qquad \dots (1)$$

Now,

$$\begin{aligned}
ker\phi &= \{hx \in H^* \cdot (H \cap K)/\phi(hx) = L\} \\
&= \{hx \in H^* \cdot (H \cap K)/L_x = L\} \\
&= \{hx \in H^* \cdot (H \cap K)/x \in L\} \\
&= \{hx\ /\ h \in H^*\ and\ x \in (H \cap K) \cap L\} \\
&= \{hx\ /\ h \in H^*\ and\ x \in L\} \\
&= \{hx\ /\ hx \in H^* \cdot L\} \\
&= \{hx\ /\ hx \in H^* \cdot (H \cap K^*)\} \\
&= H^* \cdot (H \cap K^*) \qquad \dots (2)
\end{aligned}$$

[$H^*L = H^* \cdot (H^* \cap K) \cdot (H \cap K^*) = H^* \cdot (H \cap K^*)$ as $H^* \cap K \leq H^*$]

From (1) and (2), we get,

$$\frac{H \cap K}{L} \cong \frac{H^*\ (H \cap K)}{H^* \cdot (H \cap K^*)}$$

$ker\phi$ being a normal subgroup of $H^* \cdot (H \cap K^*)$, we get

$$H^* \cdot (H \cap K^*) \lhd \; H^* \cdot (H \cap K)$$

(v) As in (iv) we can prove

$$\frac{H \cap K}{L} \cong \frac{K^* \,(H \cap K)}{K^* \cdot (H^* \cap K)}$$

and $K^* \cdot (H^* \cap K)$ is a normal subgroup of $K^* \cdot (H \cap K)$.

This completes the proof of Zassenhaus Lemma.

Theorem 1.2.9: Let G be a group.

(i) For any non empty subset S of G, $N[S]$ is a subgroup of G.

Further, for any subgroup H of G.

(ii) $N[H]$ is the largest subgroup of G in which H is normal.

(iii) If K is a subgroup of $N[H]$, then H is a normal subgroup of KH.

Proof :

(i) $N[S] = \{x \in G / xSx^{-1} = S\}$. As $eSe^{-1} = S$ we get $e \in N[S]$.

Let $x, y \in N[S]$

$$\begin{aligned}(x^{-1}y)\; S\; (x^{-1}y)^{-1} &= (x^{-1}y)\; S\; (y^{-1}x)\\ &= x^{-1}\,(y\,S\,y^{-1})\,x\\ &= x^{-1}\,S\,x\\ &= S\end{aligned}$$

This shows that $x^{-1}y \in N[S]$ whenever $x, y \in N[S]$.

Hence N[S] is a subgroup of G.

(ii) Let H be a subgroup of G.

$H \subseteq N[H]$, as $hHh^{-1} = H$ for any $h \in H$

Let $H \lhd K$ where K is any subgroup of G. Then $kHk^{-1} = H$ for any $k \in K$.

Hence $K \subseteq N[H]$.

Now for any $g \in N[H]$ we get $gHg^{-1} = H$. This shows that $H \trianglelefteq N[H]$ and if $H \lhd K$ for some $K \leq G$, then $K \subseteq N[H]$.

Hence N [H] is the largest subgroup of G in which H is normal.

(iii) $K \leq N[H]$. Hence for all $k \in K$, $kHk^{-1} = H$. Hence HK = KH. This shows that HK is a subgroup of G.

$H \lhd N[H]$ and $K \leq N[H] \quad \Rightarrow \quad HK \leq N[H]$

$H \trianglelefteq N[H] \quad \Rightarrow \quad H \trianglelefteq KH$ as $H \leq HK$

Theorem 1.2.10: G is a group and H is a subgroup of G such that $(G{:}H) = 2$. Then H is a normal subgroup of G.

Proof : Select any $g \in G$ such that $g \notin H$.

Then, $\quad G = H \cup Hg \quad$ and $\quad H \cap Hg = \phi$.

Similarly, $G = H \cup gH \quad$ and $\quad H \cap gH = \phi$.

Hence, this is possible iff $Hg = gH$. Thus for any $g \notin H$ we get $Hg = gH$.

But, as for any $h \in H$, we have, $Hh = hH$. It follows that $Hg = gH$, for each $g \in G$.

Hence, $H \trianglelefteq G$.

Theorem 1.2.11 : Let G be a group. Then following statements are true.

(i) The set of conjugate classes of G is a partition of G.

(ii) $|c(a)| = [G{:}N(a)]$.

(iii) If G is finite, $|G| = \sum |G{:}N(a)|$, a is running over exactly one element from each conjugate class.

Proof :

(i) Define a relation '$\sim$' on G by $a \sim b$ iff $b = xax^{-1}$. Then '$\sim$' is an equivalence relation on G and the equivalence class containing a is $c(a)$. Hence, $G = \bigcup C(a)$ (disjoint union). Hence, $\{C(a) \,/\, a \in G\}$ forms a partition of G.

(ii) To prove $|c(a)| = (G{:}N(a))$.

Let $\mathfrak{R}$ denote the set of all right cosets of $N[a]$ in G.

Define a map $f : C(a) \longrightarrow \mathfrak{R}$ by

$$f(gag^{-1}) = N(a)g$$

(i) f is well defined (obviously true.)

(ii) f is one-one.

Let $(N_a)\, x = (N_a)\, y$, $\qquad$ for some $x, y \in G$

$$(N_a)\, x = (N_a)\, y \quad \Rightarrow \quad xy^{-1} \in N(a)$$
$$\Rightarrow \quad (xy^{-1})\, a\, (xy^{-1})^{-1} = a$$
$$\Rightarrow \quad xy^{-1}a = axy^{-1}$$
$$\Rightarrow \quad y^{-1}a\, y = x^{-1}ax$$

Thus , $\quad f(x^{-1}ax) = f(y^{-1}a\, y)$

$\Rightarrow \quad x^{-1}ax = y^{-1}a\, y$

Hence, f is one-one.

(iii) f is onto.

Let $(N_a)g \in \mathfrak{R}$. Then for this $g \in G,\ g^{-1}ag \in C(a)$ and $f(g^{-1}ag) = (N_a)g$. This shows that f is onto.

From (i), (ii) and (iii) we get $\exists$ a mapping $f : C(a) \longrightarrow \mathfrak{R}$ which is both one-one and onto. Hence $|c(a)| = |\mathfrak{R}| = [G: N(a)]$.

(iii) Let G be finite. As $G = \bigcup_a C(a)$ (disjoint union) we get $|G| = \sum_a |C(a)| = \sum_a (G : N(a))$ where a runs over exactly one element from each conjugate class.

Unit 2 : Solvable Groups :

2.1 Derived subgroup of a group G.

2.2 Isomorphism Theorems.

2.1 Derived subgroup of a group G :

Definition 2.1.1: Let G be a group. Define $U = \{aba^{-1}b^{-1} \ / \ a, b \in G\}$.

The subgroup generated by U i.e. $\langle U \rangle$ is called the derived subgroup of G and it is denoted by G'.

Remarks 2.1.2:

(i) U is the set of commutators in G.

(ii) $x \in G' \quad \Longrightarrow \quad x = y_1 y_2 \dots y_n$ where n is a finite integer and $y_i \in U$ for each i.

(iii) G' is also called commutator subgroup of G.

(iv) G is abelian iff $G' = \{e\}$.

Theorem 2.1.3: Let G be a group and let G' be the derived subgroup of G. Then

(i) $G' \lhd G$

(ii) $\frac{G}{G'}$ is abelian.

(iii) $N \trianglelefteq G$. $\frac{G}{N}$ is abelian iff $G' \leq N$.

Proof :

(1) By definition, G' is a subgroup of G only to prove G' is normal in G.

Let $g \in G$ and $x \in G'$.

Case I : $x \in G'$ and $x = aba^{-1}b^{-1}$.

Then $g^{-1}xg = g^{-1}(aba^{-1}b^{-1})g$

$$= (g^{-1}ag)\,(g^{-1}bg)\,(g^{-1}a^{-1}g)\,(g^{-1}b^{-1}g)$$

$$= (g^{-1}ag)\,(g^{-1}bg)\,(g^{-1}ag)^{-1}\,(g^{-1}bg)^{-1}$$

This shows that $gxg^{-1} \in U$ and hence $gxg^{-1} \in G'$.

Case II : Let $x \in G'$ and $x = y_1 y_2 \dots y_n$ where n is finite and $y_i \in U$ for each i and hence $g^{-1}xg$, being the finite product of elements of U. is in G'.

Thus, for $g \in G$ and $x \in G'$ we get $gxg^{-1} \in G'$ and hence G' is a normal subgroup of G.

(2) $G' \trianglelefteq G \quad \Longrightarrow \quad \frac{G}{G'}$ is defined.

To prove that $\frac{G}{G'}$ is abelian.

Let $G'_a, G'_b \in \frac{G}{G'}$. Then $a, b \in G$.

$[(G'_a)\ (G'_b)]\ [(G'_b)\ (G'_a)]^{-1} = [G'_{ab}]\ [G'_{ba}]^{-1}$ ... by the definition of $\cdot$ in $\frac{G}{G'}$.

$= [G'_{ab}]\ \left[G'_{(ba)^{-1}}\right]$

$= [G'_{ab}]\ \left[G'_{a^{-1}b^{-1}}\right]$

$= \left[G'_{aba^{-1}b^{-1}}\right]$

$= G'$ as $aba^{-1}b^{-1} \in G'$

$=$ identity element of $\frac{G}{G'}$.

But this shows that $(G'_a)\ (G'_b) = (G'_b)\ (G'_a)$.

Hence $\frac{G}{G'}$ is abelian.

(3)

Only if part :

$\frac{G}{N}$ is abelian $\Longrightarrow$ $(N_a)(N_b) = (N_b)(N_a)$ for all $a, b \in G$.

Hence $N_{ab} = N_{ba}$ for $a, b \in G$

$\Longrightarrow$ $(N_{ab})(N_{ba})^{-1} = N$ for $a, b \in G$

$\Longrightarrow$ $(N_{ab})\left(N_{(ba)^{-1}}\right) = N$ for $a, b \in G$

$\Longrightarrow$ $(N_{ab})(N_{a^{-1}b^{-1}}) = N$ for $a, b \in G$

$\Longrightarrow$ $N_{aba^{-1}b^{-1}} = N$ for $a, b \in G$

$\Longrightarrow$ $aba^{-1}b^{-1} \in N$ for $a, b \in G$

This shows that $U \subseteq N$. By the definition of subgroups generated by U, we get $\langle U \rangle \subseteq N$.

Therefore $G' \subseteq N$.

If part :

Let $N \trianglelefteq G$ and $G' \subseteq N$. To prove that $\frac{G}{N}$ is abelian.

As $G' \subseteq N$ we get we get $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.

Thus $N_{(aba^{-1}b^{-1})} = N$

i.e. $(N_{ab})\left(N_{(ba)^{-1}}\right) = N$

i.e. $(N_a)(N_b)[(N_b)(N_a)]^{-1} = N$

i.e. $(N_a)(N_b) = (N_b)(N_a)$

Thus, for all $a, b \in G$, we have $(N_a)(N_b) = (N_b)(N_a)$ and hence $\frac{G}{N}$ is abelian.

Example 2.1.4 : For any n, the derived subgroup S_n' of S_n is A_n.

Solution :

<u>Case I :</u> n = 1, 2

For n = 1, 2 we know $S_n' = \{e\}$ and $A_n = \{e\}$. Hence $S_n' = A_n$.

<u>Case II :</u> n > 2

We know $f = (1, 2) \in S_n$ and $g = (1, 2, 3) \in S_n$.

Hence, $fgf^{-1}g^{-1} \in S_n'$ $\forall$ n.

Thus, (1 2) (1 2 3) (2 1) (3 2 1) $\in S_n'$ for each <u>n</u>.

But $(1\ 2)(1\ 2\ 3)(2\ 1)(3\ 2\ 1) = (1\ 2\ 3)$

Hence, $(1\ 2\ 3) \in S_n'$.

As S_n' is normal subgroup of S_n for each n (See theorem 1.3), we get $g^{-1}xg \in S_n'$ for any $g \in S_n$ and $x \in S_n'$.

Hence, in particular

$g(1\ 2\ 3)g^{-1} \in S_n$ i.e. $g \in A_n$

As $g(1\ 2\ 3)g^{-1} = g$ for each $g \in A_n$, we get $A_n \subseteq S_n'$.

Now $fgf^{-1}g^{-1}$ is an even permutation for any $f, g \in S_n$, we get $S_n' \subseteq A_n$.

By combining both the inclusions, we get $S_n' = A_n$ and this completes the solution.

Example 2.1.5 : (i) $|G| = p$ (p is prime) $\Longrightarrow$ $G' = \{e\}$.

(ii) $|G| = p^2$ (p is prime) $\Longrightarrow$ $G' = \{e\}$.

Solution :

(i) $|G| = p$ $\Longrightarrow$ G is abelian.

Select any $a \in G$ such that $a \neq e$.

Then $\langle a \rangle$ is a subgroup of G and $O[\langle a \rangle] \mid O[G]$.

Hence $O[\langle a \rangle] \mid p$.

As $a \neq e$. We get $O[\langle a \rangle] = p$. i.e. $\langle a \rangle = G$.

Thus G is a cyclic and hence abelian.

$\Longrightarrow$ $G' = \{e\}$.

(ii) $|G| = p^2 \implies$ G is abelian. (See ex. 2.16, result 4)

$\implies G' = \{e\}$.

2.2 Solvable Groups :

Definition 2.2.1: Let G be any group. For any positive integer n, we define the n^{th} derived subgroup of G, written as $G^{(n)}$ as follows :

$$G^{(1)} = G', G^{(2)} = G^{(1)'}, \dots, G^{(n)} = \left[G^{(n-1)}\right]' \ \dots$$

where G' denotes the derived subgroup of G.

Definition 2.2.2: A group G is said to be solvable, if there exists some positive integer n such that $G^{(n)} = \{e\}$.

Example 2.2.3:

(i) Any abelian group G is solvable as $G^{(1)} = G' = \{e\}$

(ii) Let p be a prime number. The groups of order p, p^2 are solvable (See example 1.5)

(iii) Any finite group G with $|G| \leq 5$ is solvable. (Since any group G with $|G| \leq 5$ is abelian).

(iv) S_3 is solvable.

$S_3 = \langle \{(1)(1\ 2)(1\ 3)(2\ 3)(1\ 2\ 3)(1\ 3\ 2)\}, \circ \rangle$

Then, $S_3' = A_3 = \langle \{(1),\ (1\ 2\ 3),\ (1\ 3\ 2)\}, \circ \rangle$ … See example 2.1.4

As $(1\ 2\ 3)(1\ 3\ 2)(1\ 2\ 3)^{-1}(1\ 3\ 2)^{-1}$

$= (1\ 2\ 3)(1\ 3\ 2)(3\ 2\ 1)(2\ 3\ 1)$

$= (1\ )$

We get, $A_3' = \{e\} \longleftarrow$ an identity element of in S_3.

Hence, $S_3^{(2)} = A_3^{(1)} = \{e\}$. This shows that S_3 is solvable.

(v) S_n is not solvable for $n \geq 5$.

We need the following result.

<u>Result :</u> If $N \trianglelefteq S_n$ $(n \geq 5)$ then N contains each 3-cycles.

As $(S_n)'$ is a normal subgroup of S_n. $(S_n)'$ will contain all the 3-cycles in S_n.

Again $(S_n)'' = (S_n)^{(2)}$ is a normal subgroup of $(S_n)'$ and $(S_n)'$ contains all the 3-cycles in S_n. Hence, $(S_n)^{(2)}$ must contain each 3-cycles in S_n.

Continuing this process we will get that $(S_n)^{(k)}$ contains each 3-cycle in S_n and hence ∄ no k such that $(S_n)^{(k)} = \{e\}$.

Therefore S_n is not solvable for $n \geq 5$.

Theorem 2.2.4 : Every subgroup of a solvable group is solvable.

Proof : Let G be a solvable group and $H \leq G$. Then by the definition of the derived subgroup, we get $H' \leq G'$. In general $H^{(k)} \leq G^{(k)}$ for any positive integer k. As G is solvable, ∃ a positive integer n such that $G^{(n)} = \{e\}$. Hence

$H^{(n)} \leq G^{(n)} = \{e\} \qquad \Longrightarrow \qquad H^{(n)} = \{e\}$. Thus H is solvable.

Remark : Converse of theorem 2.2.4 need not be true.

Theorem 2.2.5 : Homomorphic image of a solvable group is solvable.

Proof : Let G_1 and G_2 be any two groups such that G_1 is solvable and G_2 is a homomorphic image of G_1. Hence ∃ a positive integer k such that $G_1^{(k)} = \{e_1\}$ where e_1 is the identity in G_1.

As G_2 is a homomorphic image of G_1, there exists an onto homomorphism $f: G_1 \longrightarrow G_2$.

Thus $G_2 = f(G_1) = \{f(x) \,/\, x \in G_1\}$.

Now $f(aba^{-1}b^{-1}) \;=\; f(a)f(b)[f(a)]^{-1}[f(b)]^{-1}$ for $a, b \in G_1$

Define

$U_1 = \{aba^{-1}b^{-1} \,/\; a, b \in G_1\}$ and

$U_2 = \{xyx^{-1}y^{-1} \,/\; x, y \in G_2\}$.

Then $U_2 = \{f(s)f(t)[f(s)]^{-1}[f(t)]^{-1} \,/\, s, t \in G_1\}$ as $G_2 = f(G_1)$

$= \{f(sts^{-1}t^{-1}) \,/\, s, t \in G_1\}$ . . . since f is a homomorphism.

$= f(U_1)$

But then we get $f(G_1') = G_2'$.

Continuing in this way we get

$$f\left(G_1^{(n)}\right) = [f(G_1)]^{(n)} \qquad \text{. . . for any positive integer n.}$$

As $G_1^{(k)} = \{e\}$ we get

$$f\left(G_1^{(k)}\right) = [f(G_1)]^{(k)}$$

$$\Longrightarrow \qquad f(\{e_1\}) = [f(G_1)]^{(k)}$$

$\Longrightarrow \quad \{e_2\} = {G_2}^{(k)}$ where e_2 is an identity element in G_2.

This shows that G_2 is solvable.

Corollary 2.2.6 : Any quotient group $\frac{G}{N}$ of a solvable group G is solvable.

Proof : As is a homomorphic image of G under the natural / canonical mapping $f : G \longrightarrow \frac{G}{N}$ defined by $f(g) = Ng$, the result follows by theorem 2.5.

Remark 2.2.7 : Converse of the corollary 2.2.6 need not be true.

For this consider the group S_n for $n \geq 5$. S_n is not solvable (See example 2.3 (5)).

$A_n \lhd S_n$ and hence $\frac{S_n}{A_n}$ is defined. As $\left|\frac{S_n}{A_n}\right| = 2$, we get $\frac{S_n}{A_n}$ is abelian and hence solvable.

Thus the quotient group $\frac{S_n}{A_n}$ is solvable but S_n is not solvable.

Theorem 2.2.8 : Let $N \trianglelefteq G$. If both N and $\frac{G}{N}$ are solvable, then G is solvable.

Proof : N is solvable $\Longrightarrow$ $\exists$ a positive integer k such that $N^{(k)} = \{e\}$.

$\frac{G}{N}$ is solvable $\Longrightarrow$ $\exists$ a positive integer l such that $\left[\frac{G}{N}\right]^{(l)} = \{N\}$.

(N is the identity element of $\frac{G}{N}$)

$$\text{Now } \left(\frac{G}{N}\right)' = \text{ the group generated by } \{N_a N_b N_{a^{-1}} N_{b^{-1}} \ / \ a, b \in G\}$$

$$= \text{ the group generated by } \{N_{aba^{-1}b^{-1}} \ / \ a, b \in G\} \qquad \ldots (1)$$

Now $G' \trianglelefteq G$ and $N \trianglelefteq G$ will imply $G'N$ is a normal subgroup of G and $N \trianglelefteq G'N$. Hence the quotient group $\frac{G'N}{N}$ is defined.

$$\frac{G'N}{N} = \{N_x \ / \ x \in G'N = NG'\} \qquad \ldots (2)$$

From (1) and (2), w get,

$$\left(\frac{G}{N}\right)' = \frac{G'N}{N}$$

Continuing in this way we get

$$\left(\frac{G}{N}\right)^{(n)} = \frac{G^{(n)}N}{N}, \qquad \text{for any positive integer n.}$$

Hence, $\left(\frac{G}{N}\right)^{(l)} = \frac{G^{(l)}N}{N} = \frac{N \cdot N}{N} = \{N\}$.

But then $G^{(l)} \subseteq N$ and hence $\left[G^{(l)}\right]^{(k)} \subseteq N^{(k)} = \{e\}$ implies $G^{(l+k)} = \{e\}$, establishing that G is solvable.

Combining the result of theorem 2.2.4, 2.2.8 and corollary 2.2.7 we get,

Corollary 2.2.9 : Let $N \lhd G$. G is solvable if and only if both N and $\frac{G}{N}$ are solvable.

Example 2.2.10 : A and B are solvable groups iff $A \times B$ is solvable.

Solution : **<u>Only if part :</u>**

Let A and B be solvable groups.

To prove that $A \times B$ is solvable.

We know, the mapping $f: A \times B \longrightarrow A$ defined by $f(a, b) = a$ is an onto homomorphism.

Hence, by fundamental theorem of homomorphism.

$$\frac{A \times B}{kerf} \cong A$$

where $kerf = \{e_1\} \times B$, e_1 denotes the identity element in A.

Thus,

$$\frac{A \times B}{\{e_1\} \times B} \cong A.$$

As A is solvable, by theorem 2.2.5, $\frac{A \times B}{\{e_1\} \times B}$ is solvable. . . . (1)

Further the mapping $g : \{e_1\} \times B \longrightarrow B$ defined by $g(e_1, b) = b$ for each $b \in B$ is isomorphism. Hence $\{e_1\} \times B \cong B$.

As B is solvable, by theorem 2.2.5 we get, $\{e_1\} \times B$ is a solvable group. . . . (2)

As both $\{e_1\} \times B$ and $\frac{A \times B}{\{e_1\} \times B}$ are solvable groups, by theorem 2.2.8, $A \times B$ is solvable.

<u>If part :</u>

Let $A \times B$ be a solvable group. As the mapping $f: A \times B \longrightarrow A$ defined by $f(a, b) = a$ is an onto homomorphism, we get A is a homomorphic image of a solvable group $A \times B$ and hence A is solvable.

Similarly, we can prove that B is solvable.

Example 2.2.11 : H and K be normal solvable subgroups of group G. Show that HK is solvable.

Solution : HK is a subgroup of G. By second isomorphism theorem,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}$$

Now, any quotient group of a solvable group being solvable, we get $\frac{H}{H \cap K}$ is a solvable. (Since H is solvable). Now isomorphic image of a solvable group is solvable. Hence $\frac{HK}{K}$ is solvable. Thus K and $\frac{HK}{K}$ both are solvable will imply HK is solvable. (See theorem 2.2.8).

Definition 2.2.12 : A finite sequence $\{N_0, N_1, \dots, N_r\}$ of subgroups of a group G is called a normal series of G if

$$\{e\} = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_r = G.$$

The quotient groups $\frac{N_i}{N_{i-1}}$ are called factors of the normal series. ($1 \leq i \leq r$).

For detail discussion of normal series see Unit 3.2.

Theorem 2.2.13 : A group G is solvable if and only if G has a normal series with abelian factors.

Proof : <u>Only f part :</u>

Let G be a solvable group. Hence $\exists$ a positive integer k such that $G^{(k)} = \{e\}$.

Consider $\{G^{(k)}, G^{(k-1)}, \dots, G^{(1)}, G\}$. By theorem 1.6, $G^{(i)}$ is a normal subgroup of G for each $i,\ 1 \leq i \leq k$. Further $G^{(i+1)} \lhd G^{(i)}$, by theorem 1.4 (1).

Hence the sequence $\{G^{(k)}, G^{(k-1)}, \dots, G^{(1)}, G\}$ forms a normal series

$$\{\mathrm{e}\} = G^{(k)} \lhd G^{(k-1)} \lhd \cdots \lhd G^{(1)} \lhd G\ .$$

Further the factors $\frac{G^{(i)}}{G^{(i+1)}}$ are abelian groups for each $i,\ 1 \leq i \leq k$ (See theorem 1.4 (2)).

Thus if G is solvable, G has a normal series,

$$\{\mathrm{e}\} = G^{(k)} \lhd G^{(k-1)} \lhd \cdots \lhd G^{(1)} \lhd G$$

with abelian factors.

<u>If part :</u>

Let G has a normal series. $\{H_0, H_1, \dots, H_n\}$ with $H_0 = \{e\}$ and $H_n = G$ and with abelian factors. Thus

$$\{e\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_n = G$$

and $\frac{H_{i+1}}{H_i}$ is an abelian group with $0 \le i \le n$.

Now $\frac{H_n}{H_{n-1}} = \frac{G}{H_{n-1}}$ is abelian.

$\Rightarrow \quad G' \subseteq H_{n-1} \quad \Rightarrow \quad G'' \subseteq (H_{n-1})'$

Hence by transitivity,

$$G'' \subseteq (H_{n-2}) \quad \text{i.e.} \quad G^{(2)} \subseteq H_{n-2}$$

Continuing in this way, we get

$$G^{(n)} \subseteq H_{n-n} = H_0 = \{e\}$$

Hence $G^{(n)} = \{e\}$, proving that G is Solvable.

Example 2.2.14 :

(i) In S_3 we have a normal series $\{e\} \lhd A_3 \lhd S_3$ such $\frac{S_3}{A_3}$ that is abelian and such $\frac{A_3}{\{e\}}$ that is abelian. Hence S_3 is solvable.

(ii) Consider the group S_4. $A_4 \lhd S_4$. Define

$$V_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Then $V_4 \lhd A_4$.

Consider the sequence $\{\{(1)\},\ V_4,\ A_4,\ S_4\}$. We have $\{(1)\} \lhd V_4 \lhd A_4 \lhd S_4$ . . . (1)

The factors of the normal series are

$$\frac{V_4}{\{e\}}, \frac{A_4}{V_4} \text{ and } \frac{S_4}{A_4}.$$

$\left|\frac{V_4}{\{e\}}\right| = \frac{|V_4|}{|\{e\}|} = \frac{4}{1} = 4 \quad \Rightarrow \quad \frac{V_4}{\{e\}}$ is abelian.

$\left|\frac{A_4}{V_4}\right| = \frac{|A_4|}{|V_4|} = \frac{12}{4} = 3 \quad \Rightarrow \quad \frac{A_4}{V_4}$ is abelian.

$\left|\frac{S_4}{A_4}\right| = \frac{|S_4|}{|A_4|} = \frac{24}{12} = 2 \quad \Rightarrow \quad \frac{S_4}{A_4}$ is abelian.

(Result used : G is abelian if $|G| \le 5$).

This shows that S_4 has a solvable series and hence S_4 is solvable.

Example 2.2.15 : Let G be a solvable group. Show that G contains at least one normal, abelian subgroup H.

Solution :

Case I : G is abelian. In this we take $H = G$.

Case II : G is non-abelian.

G is solvable $\Longrightarrow$ $\exists$ a positive integer k such that $G^{(k)} = \{e\}$.

Consider $H = G^{(k-1)}$.

Then $\{e\} = G^{(k)} \lhd G^{(k-1)}$. Hence $\left[G^{(k-1)}\right]' = \{e\}$.

$\Longrightarrow$ $G^{(k-1)}$ is abelian. (See remark 1.2 (iv))

$G^{(1)} \lhd G \Longrightarrow G^{(2)} \lhd G$ (See example 1.6)

$G^{(2)} \lhd G \Longrightarrow G^{(3)} \lhd G$

Continuing in this way we get

$$H = G^{(k-1)} \lhd G$$

Thus G contains a normal, abelian subgroup H.

Example 2.2.16 : Let G be a non-abelian group such that $|G| = p^3$, where p is any prime number. Show that $G' = Z(G)$.

Solution : To solve this problem we mainly use the following result.

Let p be a prime.

Result 1 : $|G| = p^n \ (n > 0) \Longrightarrow Z(G) \neq \{e\}$.

Result 2 : $|G| = p \Longrightarrow$ G is cyclic.

Result 3 : $\frac{G}{Z(G)}$ is cyclic $\Longrightarrow$ G is abelian.

Result 4 : Any group of order p^2 is abelian.

Result 5 : $\frac{G}{N}$ is abelian $\Longrightarrow G' \subseteq N$.

Result 6 : G is abelian $\Longleftrightarrow G' = \{e\}$.

Solution of the problem :

(i) $|G| = p^3 \Longrightarrow Z(G) \neq \{e\} \Longrightarrow |Z(G)| \neq 1$.

(ii) G is non-abelian $\Longrightarrow Z(G) \neq G \Longrightarrow |Z(G)| \neq p^3$.

(iii) As $Z(G) \lhd G$, $|Z(G)| \,\Big|\, |G| = p^3$.

Hence, $|Z(G)| = 1,\ p,\ p^2,\ p^3$.

From (i) and (ii),

$$|Z(G)| = p^2 \text{ or } p$$

(iv) $|Z(G)| = p^2 \quad \Rightarrow \quad \left|\frac{G}{Z(G)}\right| = \frac{|G|}{|Z(G)|} = \frac{p^3}{p^2} = p.$

Thus $\left|\frac{G}{Z(G)}\right| = p$ and hence $\frac{G}{Z(G)}$ is a cyclic group. Hence G must be abelian.

As this is not true we get $|Z(G)| \neq p^2$.

(v) Hence, only possible value of $|Z(G)|$ is p. But in this case

$$\left|\frac{G}{Z(G)}\right| = \frac{|G|}{|Z(G)|} = \frac{p^3}{p} = p^2.$$

This shows that $\frac{G}{Z(G)}$ is an abelian group. But then $G' \subseteq Z(G)$.

As $G' \leq Z(G)$ we get $|G'| \,\Big|\, |Z(G)| = p$ As G is non-abelian, $|G'| \neq 1$.

Thus, $|G'| = p = |Z(G)|$. This in turn shows that $G' = Z(G)$.

Exercise

(i) Show that the groups of order $p,\ p^2,\ pq,\ ,\ p^2q$ where p and q are distinct primes are solvable.

(ii) Prove that any group of order pqr is solvable when p, q, r are primes and $r > pq$.

(iii) Show that a group of order 4p, where p is prime is solvable.

(iv) State whether the following statements are true or false.

1. Every finite group is solvable.
2. Every finite group of prime order is solvable.
3. S_7 is a solvable group.
4. G is solvable if G has a normal series.
5. The property of 'being a solvable group' is preserved under isomorphism.

(v) Prove or disprove : $S_3 \times S_3$ is solvable.

Theorem 2.2.17 : If $N \trianglelefteq G$, then the derived subgroup of N is also a normal subgroup of G.

Proof : $N \trianglelefteq G$. N'= derived subgroup of G.

N' = the subgroup generated by the set $\{n_1n_2n_1^{-1}n_2^{-1} / \ n_1, n_2 \in N\}$.

Let $x \in N'$ and $g \in G$. To prove that $g^{-1}xg \in N'$.

It is enough to prove that $g^{-1}xg \in N'$, when $x = n_1n_2n_1^{-1}n_2^{-1}$, for some $n_1, n_2 \in N$.

Now, $\quad g^{-1}(n_1n_2n_1^{-1}n_2^{-1})g$

$= \ (g^{-1}n_1g)\,(g^{-1}n_2g)\,(g^{-1}n_1^{-1}g)\,(g^{-1}n_2^{-1}g)$

$= \ (g^{-1}n_1g)\,(g^{-1}n_2g)\,(g^{-1}n_1g)^{-1}\,(g^{-1}n_2g)^{-1}$

Now, N being a normal subgroup of G, $g^{-1}(n_1n_2n_1^{-1}n_2^{-1})g$ is finite product of the type $aba^{-1}b^{-1}$ where $a, b \in N$.

Hence, $g^{-1}(n_1n_2n_1^{-1}n_2^{-1})g \in N'$.

Hence $N' \trianglelefteq G$.

Example 2.2.18 : True or false ? Justify.

If every proper subgroup of G is solvable, then G is solvable.

Solution : False. Let $G = A_5$.

Assume that A_5 is solvable.

Then $\frac{S_5}{A_5}$ is abelian. (Since $\left|\frac{S_5}{A_5}\right| = 2 \implies \frac{S_5}{A_5}$ is abelian).

Hence, by theorem 2.2.8, S_5 is solvable; which is not true.

Hence, $G = A_5$ is not solvable.

Claim : All proper subgroups of A_5 are solvable.

$O(A_5) = \frac{O(S_5)}{2} = 60 = 2^3 \cdot 3 \cdot 5$

(i) A_5 is simple $\Longrightarrow A_5$ does not have any subgroup of order 30.

(ii) A_5 may contain subgroups of order $2,\ 2^2,\ 3, 5,\ 6 = 2 \cdot 3,\ 10 = 2 \cdot 5,\ 15 = 3 \cdot 5,$ $20 = 2^2 \cdot 5.$

All these subgroups of A_5 are solvable by the following result.

Result : Let p and q be distinct primes. Then any groups of order pq or p^2q are solvable.

Example 2.2.19 : Show that the set G of all matrices of the type

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \qquad a,\ b,\ c \in Z_3$$

is non abelian and solvable under the multiplication.

Solution : It is easy to prove that $\langle G,\ \cdot\ \rangle$ is a group.

As $a,\ b,\ c \in Z_3 = \{0,\ 1,\ 2\},\ \ |G| = 27 = 3^3$. As any group of order power of a prime, is solvable, G is solvable.

Example 2.2.20 : Show that $S_n \supset A_n \supset \{e\}$ is a normal series in S_n for $n > 4$. Deduce that S_n is not solvable for $n > 4$.

Solution : We know that $A_n \lhd S_n$ and $\{e\} \lhd A_n$. Hence $\{\{e\},\ A_n,\ S_n\}$ forms a normal series in S_n. Let S_n be solvable for n > 4. Then subgroup of solvable group being solvable, A_n will be a solvable. But A_n is not solvable for > 4 as A_n is simple for n > 4 and a solvable group contains non-trivial normal subgroup (See theorem 2.13)

***Exercise* :** Prove that $S_3 \times S_3$ is solvable.

Unit 3: Series of A Group

3.1 Subnormal Series :

Definition 3.1.1 : Let G be a group. A subnormal series of a group G is a finite sequence $H_0, H_1, \dots, H_n$ of subgroups of G such that $H_i \lhd H_{i+1}$ for each $i,\ 0 \le i < n$ with $H_0 = \{e\}$ and $H_n = G$.

Remarks :

(i) Every group G has a subnormal series with $H_0 = \{e\}$ and $H_1 = G$.

(ii) The groups $\frac{H_{i+1}}{H_i}$ are called factor groups of the series $(0 \le i < n-1)$.

Examples 3.1.2 :

(i) In a group $\langle Z, +\rangle$, $\{0\} < 8Z < 4Z < Z$ is a subnormal series where

$$8Z = \{0,\ \pm 8,\ \pm 16,\ \pm 24,\ \dots\}$$

$$4Z = \{0,\ \pm 4,\ \pm 8,\ \pm 16,\ \pm 24,\ \dots\}$$

$$\{0\} \lhd 8Z,\ 8Z \lhd 4Z \text{ and } 4Z \lhd Z.$$

Hence, the finite sequence $\{\{e\},\ 8Z, 4Z, Z\}$ of subgroups of Z form a subnormal series.

(ii) Let $G = \langle a \rangle$ where $a^6 = e$.

Then $G = \{a,\ a^1, a^2, a^3, a^4, a^5, a^6\}$ with $a^6 = e$.

Define $H = \{e, a^3\}$. Then $\{\{e\},\ H, G\}$ will form a subnormal series in G.

(iii) In S_3, $\{(1), A_3, S_3\}$ will form a subnormal series in S_3.

(iv) Let $G = \langle a \rangle$, where $a^{12} = e$.

Then $S_1 = \{\{e\}, \langle a^4 \rangle, \langle a^2 \rangle, \mathrm{G}\}$

and $S_2 = \{\{e\}, \langle a^6 \rangle, \langle a^3 \rangle, \mathrm{G}\}$

will be two subnormal series in G.

Definition 3.1.3 : A subnormal series $\{K_j\}$ is a refinement of a subnormal series $\{H_i\}$ if $\{H_i\} \subseteq \{K_j\}$ that is each $H_i = K_j$ for some j.

Example 3.1.4 :

(i) The series in Z given by

$$\{0\} \lhd 72Z \lhd 24Z \lhd 8Z \lhd 4Z \lhd Z$$

is a refinement of the series

$$\{0\} \lhd 72Z \lhd 8Z \lhd Z$$

(ii) Let $G = \langle a \rangle$ where $a^{12} = e$.

The subnormal series

$$\{e\}, \langle a^4 \rangle, \langle a^2 \rangle, \mathrm{G}$$

is not a refinement of the series

$$\{e\}, \langle a^6 \rangle, \langle a^3 \rangle, \mathrm{G} \qquad \text{in } G.$$

Definition 3.1.5 : Two subnormal series $\{H_i\}$ and $\{K_j\}$ of the same group G are isomorphic if there is a one-one correspondence between the collection of factor groups $\left\{\frac{H_{i+1}}{H_i}\right\}$ and $\left\{\frac{K_{j+1}}{k_j}\right\}$ such that the corresponding factor groups are isomorphic.

Remark : The two isomorphic normal series must contain the same number of subgroups.

Example 3.1.6 : Let $G = Z_{15}$.

$$Z_{15} = \langle \{0, 1, 2, 3, \dots, 14\},\ \ \oplus_{15} \rangle$$

$< 5 >$ = the subgroup generated by 5 in Z_{15} = $\{0,\ 5,\ 10\}$

$< 3 >$ = the subgroup generated by 3 in Z_{15} = $\{0,\ 3,\ 6,\ 9,\ 12\}$

Consider the two subnormal series in Z_{15} given by

$$S_1 = \{\{0\},\ \langle 5\rangle,\ Z_{15}\}$$

and $$S_2 = \{\{0\},\ \langle 3\rangle,\ Z_{15}\}$$

The set of factor groups for S_1 is

$$T_1 = \left\{\frac{Z_{15}}{\langle 5\rangle},\ \frac{\langle 5\rangle}{\{0\}}\right\}$$

The set of factor groups for S_2 is

$$T_1 = \left\{\frac{Z_{15}}{\langle 3\rangle},\ \frac{\langle 3\rangle}{\{0\}}\right\}$$

Now, $\dfrac{Z_{15}}{\langle 5\rangle} \cong Z_5$ and $\dfrac{\langle 3\rangle}{\{0\}} \cong Z_5$

and $\dfrac{Z_{15}}{\langle 3\rangle} \cong Z_3$ and $\dfrac{\langle 5\rangle}{\{0\}} \cong Z_3$

We establish one-one, onto correspondence between T_1 and T_2 as

$$\frac{Z_{15}}{\langle 5\rangle} \longleftrightarrow \frac{\langle 3\rangle}{\{0\}} \qquad \text{and} \qquad \frac{\langle 5\rangle}{\{0\}} \longleftrightarrow \frac{Z_{15}}{\langle 3\rangle}$$

Then the corresponding factor group being isomorphic we get, the two series S_1 and S_2 of Z_{15} are isomorphic.

- ***Schreier's Theorem :***

Theorem 3.1.7 : Two subnormal series of a group G have isomorphic refinements.

Proof : Let G be a group and let

$$\{e\} = H_0 < H_1 < H_2 < \cdots < H_n = G \qquad \ldots (1)$$

and $$\{e\} = K_0 < K_1 < K_2 < \cdots < K_m = G \qquad \ldots (2)$$

be two subnormal series of G.

Define

$$H_{ij} = H_i \cdot (H_{i+1} \cap K_j)$$

As $H_i \lhd H_{i+1}$ we get $H_i \cdot (H_{i+1} \cap K_j)$ is a subgroup of G for each $i,\ 0 \le i \le n-1$ and each $j,\ o \le j < m$.

(i) $H_i \lhd H_{i+1}$ and $K_j \lhd K_{j+1}$. Hence by Zassenhaus Lemma,

$$H_i \cdot (H_{i+1} \cap K_j) \lhd H_i \cdot (H_{i+1} \cap K_{j+1})$$

i.e. $$H_{i,j} \trianglelefteq H_{i,j+1}$$

(ii) $H_{i,0} = H_i \cdot (H_{i+1} \cap K_0)$

$$= H_i \cdot (H_{i+1} \cap \{e\})$$

$$= H_i \cdot \{e\}$$

$= H_i$

(iii) $H_{i,m} = H_i \cdot (H_{i+1} \cap K_m)$

$= H_i \cdot (H_{i+1} \cap G)$

$= H_i \cdot H_{i+1}$

$= H_{i+1}$ as $H_i \subseteq H_{i+1}$

From (i), (ii) and (iii), we get a chain containing $nm + 1$ elements not necessarily distinct groups which is as follows.

$$\begin{aligned} \{e\} = H_0 = H_{0,0} \quad & \leq H_{0,1} \leq \cdots \leq H_{0,m} = H_{1,0} = H_1 \\ & \leq H_{1,1} \leq \cdots \leq H_{1,m} = H_{2,0} = H_2 \\ & \ldots \ldots \ldots \ldots \ldots \\ & \leq H_{n-1,1} \leq H_{n-1,2} \leq \cdots \leq H_{n-1,m} = H_n = G \end{aligned} \qquad \ldots (3)$$

This chain refines the chain in (1). The set of factor groups of the chain represented in (3) is

$$\left\{\frac{H_{i,j+1}}{H_{i,j}} \; / \; 1 \leq i \leq n, \;\; 1 \leq j \leq m-1\right\} \qquad \ldots (4)$$

Similarly, by defining

$$K_{j,i} = K_j \cdot \left(K_{j+1} \cap H_i\right) \qquad \text{for } 0 \leq j \leq m-1 \text{ and } 0 \leq i \leq n.$$

We obtain a subnormal chain containing $nm + 1$ element as follows.

$$\begin{aligned} \{e\} = K_0 = K_{0,0} \quad & \leq K_{0,1} \leq \cdots \leq K_{0,n} = K_{1,0} = K_1 \\ & \leq K_{1,1} \leq \cdots \leq K_{1,n} = K_{2,0} = K_2 \\ & \ldots \ldots \ldots \ldots \ldots \\ & \leq K_{m-1,1} \leq K_{m-1,2} \leq \cdots \leq K_{m-1,n} = K_m = G \end{aligned} \qquad \ldots (5)$$

Note that the two chains represented in (4) and (5) not necessarily contain distinct groups. The chain (5) refines the chain (2). The set of factor groups of the chain represented in (5) is

$$\left\{\frac{K_{j,i+1}}{K_{j,i}} \, / \, 0 \leq j \leq m, \;\; 0 \leq i < n-1\right\} \qquad \ldots (6)$$

Again as $H_i \lhd H_{i+1}$ and $K_j \lhd K_{j+1}$, by Zassenhaus Lemma,

$$\frac{H_i \cdot \left(H_{i+1} \cap K_{j+1}\right)}{H_i \cdot \left(H_{i+1} \cap K_j\right)} \;\cong\; \frac{K_j \cdot \left(K_{j+1} \cap H_{i+1}\right)}{K_j \cdot \left(K_{j+1} \cap H_i\right)}$$

i.e. $$\frac{H_{i,j+1}}{H_{i,j}} \;\cong\; \frac{K_{j,i+1}}{K_{j,i}} \qquad \text{for } 0 \leq i \leq n-1 \text{ and } \; 0 \leq j \leq m-1.$$

This isomorphism establishes one to one onto correspondence between the two sets represented in (4) and (6). Deleting the repeated groups from the chains represented in (3) and (5) we get subnormal series of distinct groups that are isomorphic refinements of the subnormal series represented in (1) and (2) respectively.

This establishes that any two subnormal series of a group G have isomorphic refinements.

Example 3.1.8 : Give the isomorphic refinements of the two subnormal series of $\langle Z, +\rangle$.

(i) $\{0\} \lhd 60Z \lhd 20Z \lhd Z$

(ii) $\{0\} \lhd 245Z \lhd 49Z \lhd Z$

Solution : Define $H_0 = \{0\}, \quad H_1 = 60Z, \quad H_2 = 20Z, \quad H_3 = Z$

$K_0 = \{0\}, \quad K_1 = 245Z, \quad K_2 = 49Z, \quad K_3 = Z$

Define $H_{i,j} = H_i \cdot \left(H_{i+1} \cap K_j\right) \qquad \forall \quad 0 \le i \le 2, \quad 0 \le j \le 3.$

Then,

$H_{0,0} = H_0 = \{0\}$

$H_{0,1} = H_0 \cdot (H_1 \cap K_1) = H_1 \cap K_1 = 60Z \cap 245Z$

$= 2940Z \qquad\qquad (\, 2940 = l.c.m.(60, 245)\,)$

$H_{0,2} = H_0 \cdot (H_1 \cap K_2) = H_1 \cap K_2 = 60Z \cap 49Z = 2940Z$

$H_{0,3} = H_0 \cdot (H_1 \cap K_3) = H_1 \cap K_3 = H_1 = 60Z$

$H_{1,0} = H_1 \cdot (H_2 \cap K_0) = 60Z \cdot \{0\} = 60Z$

$H_{1,1} = H_1 \cdot (H_2 \cap K_1) = 60Z \cdot (20Z \cap 245Z) = 60Z$

$H_{1,2} = H_1 \cdot (H_2 \cap K_2) = 60Z \cdot (20Z \cap 49Z) = 60Z$

$H_{1,3} = H_1 \cdot (H_2 \cap K_3) = H_1 \cdot H_2 = 60Z \cdot 20Z = 20Z = H_2$

$H_{2,0} = H_2 \cdot (H_3 \cap K_0) = H_2 \cdot \{0\} = H_2 = 20Z$

$H_{2,1} = H_2 \cdot (H_3 \cap K_1) = 20Z \cap 245Z = 5Z$

$H_{2,2} = H_2 \cdot (H_3 \cap K_2) = H_2 \cdot K_2 = 20Z \cdot 49Z = Z$

$H_{2,3} = H_2 \cdot (H_3 \cap K_3) = H_2 \cdot Z = Z$

Hence, the refinement of the series represented in (1) is

$$\begin{aligned}\{0\} = H_{0,0} \quad &\le H_{0,1} \le H_{0,2} \le H_{0,3} = H_1 = H_{1,0} \\ &\le H_{1,1} \le H_{1,2} \le H_{1,3} = H_2 = H_{2,0} \\ &\le H_{2,1} \le H_{2,2} \le H_{2,3} = H_3\end{aligned}$$

$$\{0\} \le 2940Z \le 2940Z \le 60Z \le 60Z \le 60Z \le 20Z \le 5Z \le Z \le Z\ .$$

Deleting the repeated factors, we get,

$$\{0\} \lhd 2940Z \lhd 60Z \lhd 20Z \lhd 5Z \lhd Z.$$

This is refinement of the series

$$\{0\} \lhd 60Z \lhd 60Z \lhd 20Z \lhd Z.$$

Similarly, defining $K_{i,j} = K_j(K_{j+1} \cap H_i)$, we can obtain the refinement of the series,

$$\{0\} = K_0 \lhd K_1 \lhd K_2 \lhd K_3 = Z$$

which is as follows.

$$\{0\} \lhd 2940Z \lhd 980Z \lhd 245Z \lhd 49Z \lhd Z.$$

Definition 3.1.9 : A subnormal series $\{H_i\} = \{H_0, \ldots, H_n\}$ of a group G is a composition series if all the factor groups $\frac{H_{i+1}}{H_i}$ are simple. ($H_0 = \{e\}$ and $H_n = G$)

Remark : In a composition series $\{H_i\}$, H_i will be a maximal normal subgroup of H_{i+1}.

Examples 3.1.10 :

(i) Consider the group S_n for $n \geq 5$.

The series $\{e\} < A_n < S_n$ is a composition series in S_n.

Here $\frac{A_n}{\{e\}} \cong A_n$ and $\left|\frac{S_n}{A_n}\right| = 2 \implies \frac{S_n}{A_n} \cong Z_2$

Now for $n \geq 5$, A_n is a simple (as any normal subgroup $N \neq \{e\}$ of A_n will contain each 3-cycle in S_n and hence $N = A_n$).

Hence $\frac{A_n}{\{e\}}$ is a simple group.

Similarly, Z_2 being simple we get $\frac{S_n}{A_n}$ is simple.

Hence $\{e\} \lhd A_n \lhd S_n$ is a composition series of S_n for $n \geq 5$.

(ii) Consider the group $G = Z_{15}$.

The series $\{0\} < \langle 5 \rangle < Z_{15}$ is a composition series in Z_{15}.

$\{0\} < \langle 5 \rangle < Z_{15}$ is a subnormal series.

$$\frac{\langle 5 \rangle}{\{0\}} \cong Z_5 \qquad \implies \frac{\langle 5 \rangle}{\{0\}} \text{ is a simple group.}$$

$$\frac{Z_{15}}{\langle 5 \rangle} \cong Z_3 \qquad \implies \frac{Z_{15}}{\langle 5 \rangle} \text{ is a simple group.}$$

Hence $\{0\} < \langle 5 \rangle < Z_{15}$ is a composition series in Z_{15}.

(iii) Consider the group $G = \langle a \rangle$ where $|G| = 6$. Hence $a^6 = e$.

Define $H_1 = \langle a^3 \rangle = \{e, a^3\}$ and

$H_2 = \langle a^2 \rangle = \{e, a^2, a^4\}$.

Then $\{\{e\},\ H_1,\ G\}$ and $\{\{e\},\ H_2,\ G\}$ will form two composition series in G.

(iv) Z has no composition series.

Let us assume that $\exists$ a composition series

$$\{0\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = Z \qquad \text{in } Z.$$

$$\{0\} < H_1 < Z \quad \Longrightarrow \quad H_1 = nZ \qquad \text{for some positive integer n.}$$

As $\frac{H_1}{H_0} \cong nZ$, we must have nZ is simple.

But this is not true as nZ contains many nontrivial proper normal subgroups. Hence our assumption is wrong.

Thus Z has no composition series.

- ***Existence of Composition series :***

Theorem 3.1.11 : Every finite group G has at least one composition series.

Proof : If G is a simple group, then $\{e\} \lhd G$ is a composition series in G.

If G is not simple group, then G has at least one proper normal subgroup $H \neq \{e\}$.

If H is a maximal normal subgroup then $\{e\}$ will be maximal subgroup of H.

Hence $\frac{G}{H}$ and $\frac{H}{\{e\}}$ are simple subgroups. This shows that $\{\{e\}, H, G\}$ will form a composition series in G.

Let H be not maximal in G. It means that there exists a maximal normal subgroup K such that $H \subset K \subset G$. Hence $\{\{e\}, H, K, G\}$ will form a composition series.

If H is maximal in G, but $\{e\}$ is not maximal in H then find a maximal normal subgroup L such that $\{e\} \subset L \subset H$. In this case $\{\{e\}, L, H, G\}$ will be the composition series of the group G.

Proceeding like this, we always find a composition series for G. Since G is a finite group, the number of its subgroups is also finite. Hence the composition series obtained finally contains a finite number of elements.

This proves that any finite group G has at least one composition series.

Remark : An infinite group may or may not have a composition series.

e.g. The group $\langle Z, +\rangle$ has no composition series. (See example 3.1.10 (4)).

- ***Jordan-Hölder Theorem :***

Theorem 3.1.12 : Any two composition series of a group G are isomorphic.

Proof : Let $\{H_i\}$ and $\{K_j\}$ be any two composition series of G.

Hence $\frac{H_{i+1}}{H_i}$ is a simple group for each i, $1 \le i \le n-1$ and

$\frac{K_{j+1}}{K_j}$ is a simple group for each j, $1 \le j \le m-1$.

But we know that $\frac{G}{N}$ is a simple group if and only if N is a maximal normal subgroup of G.

Hence,

$\frac{H_{i+1}}{H_i}$ is a simple implies H_i is a maximal normal subgroup of H_{i+1}, for $1 \le i \le n-1$.

Thus, intersection of any normal subgroups in between implies H_i and H_{i+1} is not possible.

Similarly, further refinement of the of the composition series $\{K_j\}$ is not possible.

Thus, $\{H_i\}$ and $\{K_j\}$ must be already isomorphic and $m = n$.

Theorem 3.1.13 : If a group G has a composition series and if N is a proper normal subgroup of G then there exist a composition series containing N.

Proof : Let $\{H_i\}$ be a composition series of G. Then

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G \qquad \ldots (1)$$

and $\frac{H_{i+1}}{H_i}$ is a simple group for each i, $1 \le i \le n-1$.

Consider the subnormal series of G given by,

$$\{e\} \lhd N \lhd G \qquad \ldots (2)$$

Define $K_0 = \{e\}$, $K_1 = N$, $K_2 = G$.

Define $K_{i,j} = K_i\left(K_{i+1} \cap H_j\right)$

for $0 \le i < 2$ and $0 \le j \le n$.

Then $\{0\} = K_0 = K_{0,0} < K_{0,1} < \cdots < K_{0,n} = K_1 = K_{1,0} = N$

$$< K_{1,1} < \cdots < K_{1,n} = K_2 = G \qquad \ldots (3)$$

The series in (3) is a refinement of the subnormal series (2). The refinement of (1) being impossible (as $\{H_i\}$ is a composition series) we get the two subnormal series represented by (1) and (3) must be isomorphic. As the isomorphic image of simple groups is a simple group, we get all the factor groups of the subnormal series (3) will be simple groups.

Hence, the subnormal series (3) containing N is a composition series.

Example 3.1.14 : Find the composition series for $S_3 \times S_3$.

Solution : $H_0 = \{e\} \times \{e\}$

$H_1 = A_3 \times \{e\}$

$H_2 = A_3 \times A_3$

$H_3 = S_3 \times A_3$

$H_4 = S_3 \times S_3$

Then $\{e\} \times \{e\} = H_0 \lhd H_1 \lhd H_2 \lhd H_3 \lhd H_4 = S_3 \times S_3$ is a composition series in $S_3 \times S_3$.

Example 3.1.15 : Show that if $\{e\} = H_0 < H_1 < H_2 < \cdots < H_n = G$ is a subnormal series of a group G and if $O\left(\frac{H_{i+1}}{H_i}\right) = S_{i+1}$ then G is of finite order $S_1 . S_2 . \ldots . S_n$.

Solution : By data

$$O\left(\frac{H_1}{H_0}\right) = S_1$$

Thus

$$\frac{O(H_1)}{O(H_0)} = S_1 \qquad \Rightarrow \qquad O(H_1) = S_1 \cdot O(H_0) = S_1 \cdot 1 = S_1$$

$$O\left(\frac{H_2}{H_1}\right) = \frac{O(H_2)}{O(H_1)} = S_2 \qquad \Rightarrow \qquad O(H_2) = S_2 \cdot O(H_1) = S_2 \cdot S_1$$

Continuing in this way, we get

$$\frac{O(H_n)}{O(H_{n-1})} = O\left(\frac{H_n}{H_{n-1}}\right) = S_n \qquad \Rightarrow \qquad O(H_n) = S_n \cdot O(H_{n-1})$$

$$\Rightarrow \qquad O(G) = S_n \cdot O(H_{n-1}) \qquad (\because \quad G = H_n)$$

$$= S_n \cdot S_{n-1} \cdot S_{n-2} \cdot \ldots \cdot S_1$$

$$= S_n \cdot S_{n-1} \cdot S_{n-2} \cdot \ldots \cdot S_1$$

Hence, G is a finite group and $O(G) = S_1 \cdot S_2 \cdot \ldots \cdot S_n$.

Example 3.1.16 : Show that an abelian group has a composition series iff it is finite.

Solution : **<u>Only if part :</u>**

Let G be an abelian group. Let $\{H_i\}$ be a composition series of G.

Then $\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$ and $\frac{H_{i+1}}{H_i}$ is a simple group for each $i, 1 \leq i \leq n-1$.

We know that if a group G is abelian then any subgroup of G is also abelian.

Hence $\frac{H_{i+1}}{H_i}$ is abelian for each $i, \quad 1 \leq i \leq n-1$.

Thus $\frac{H_{i+1}}{H_i}$ is abelian and simple group for each $i, \quad 1 \leq i \leq n-1$.

Hence $\frac{H_{i+1}}{H_i}$ is a cyclic group of prime order say p_{i+1}.

By example 3.1.15, we get $|G| = p_1.p_2.\ldots.p_n$ and hence G is a finite group.

<u>If part :</u>

Let G be a finite group.

By theorem 3.1.11, G has a composition series.

Example 3.1.17 : Show that infinite abelian group can have no composition series.

Solution : By an example 3.1.16, if an abelian group G contains a composition series, then G must be finite. Hence no infinite abelian group will contain a composition series.

3.2. Normal Series :

Definition 3.2.1 : Let G be a group. A normal series of G is a finite sequence $N_0, N_1, \ldots, N_k$ of normal subgroups of G such that $N_i < N_{i+1}$, $N_0 = \{e\}$ and $N_k = G$.

Remark 3.2.2 : Every normal series of a group G is a subnormal series but not conversely.

For this consider the group $G = D_4$ where $D_4 = \langle \{\varrho_0, \varrho_1, \varrho_2, \varrho_3, \mu_1, \mu_2, \delta_1, \delta_2\}, \ \ 0\rangle$ and

$$\varrho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\varrho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\varrho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \qquad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\varrho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \qquad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

This group D_4 is called the group of symmetries of a square.

The series D_4 given by

$$\{\varrho_0\} < \{\varrho_1, \mu_1\} < \{\varrho_0, \varrho_2, \mu_1, \mu_2\} < D_4$$

is a subnormal series but it is not a normal series as $\{\varrho_1, \mu_1\}$ is not a normal subgroup of D_4.

Remark 3.2.3 : As every subgroup of an abelian group is normal, every subnormal series in an abelian group will be a normal series. Thus the two concepts of normal and subnormal series coincide in an abelian group.

Example 3.2.4 : $\{0\} < 26Z < 13Z < Z$

and $\{0\} < 14Z < 7Z < Z$ are normal series in a group $\langle Z, +\rangle$.

Definition 3.2.5 : Let $\{N_i\}$ be a normal series of a group G. The normal series $\{K_j\}$ of a group G is a refinement of the normal series $\{N_i\}$ if $\{N_i\} \subseteq \{K_j\}$. i.e. $N_i = K_j$ for each i.

Example 3.2.6 : The normal series

$$\{0\} < 72Z < 24Z < 8Z < 4Z < Z$$

is a refinement of the normal series

$$\{0\} < 72Z < 8Z < Z$$

in an abelian group $\langle Z, +\rangle$.

Definition 3.2.7 : Two normal series $\{N_i\}$ and $\{K_j\}$ of a group G are said to be isomorphic if there exists a one to one, onto correspondence between the collection of factor groups $\left\{\frac{H_{i+1}}{H_i}\right\}$ and $\left\{\frac{K_{j+1}}{K_j}\right\}$. So that the corresponding factor groups are abelian.

Example 3.2.8 : The two normal series

$$\{0\} < \langle 5\rangle < Z_{15}$$

and $\{0\} < \langle 3\rangle < Z_{15}$

in a group Z_{15} are isomorphic.

Definition 3.2.9 : A normal series $\{N_i\}$ of a group G is principal if all the factor groups $\frac{N_{i+1}}{N_i}$ are simple.

Now we list the properties of normal series, the proofs of which are similar to those for subnormal series.

3.2.10 Properties of Normal Series :

(i) Two normal series of a group G are isomorphic (Schreier's Theorem).

(ii) Every finite group G has at least one principal series.

(iii) Any two principal series of a group G are isomorphic. (Jordan Hölder Theorem)

(iv) If a group G has a principal series and if N is a proper normal subgroup of G, then there exists a principal series in G containing N.

Exercise

(1) State whether the following statements are true or false.

- (i) Every normal series is a principal series.
- (ii) Every principal series is a composition series.
- (iii) Every composition series is a principal series.
- (iv) Every normal series is a subnormal series.
- (v) Every subnormal series is a normal series.
- (vi) Every group has a composition series.
- (vii) Every group has a principal series.
- (viii) Any two subnormal / normal series of the same group G are always isomorphic.
- (ix) Given any two normal series we can obtain the refinements for both the series.
- (x) Every abelian group has a composition series.

(2) Find all composition series for Z_{60}.

3.3 Ascending Central Series :

Definition 3.3.1 : The center of a group G is the set $\{x \in G \ / \ xg = gx \ \forall \ \ g \in G\}$.

Remark 3.3.2 :

(i) The center of a group G is generally denoted by Z or Z(G).

(ii) As $e \in Z(G)$, $Z(G) \neq \phi$ or $|Z(G)| \geq 1$.

(iii) G is abelian $\Leftrightarrow$ $Z(G) = G$.

(iv) $Z(G)$ is always a normal subgroup of G.

3.3.3 Ascending Central Series :

Let $Z(G)$ denote the center of a group G. As $Z(G) \trianglelefteq G$, the quotient group $\frac{G}{Z(G)}$ is defined. Consider the canonical / natural map $f: G \longrightarrow \frac{G}{Z(G)}$. Then f is an onto homomorphism.

Consider $Z\left[\frac{G}{Z(G)}\right]$. $Z\left[\frac{G}{Z(G)}\right]$ is a normal subgroup of the group $\frac{G}{Z(G)}$.

Hence, $f^{-1}\left[Z\left[\frac{G}{Z(G)}\right]\right]$ is a normal subgroup of G containing $Z(G)$. Denote this by $Z_1(G)$.

Thus we have,

$$\{e\} < Z(G) < Z_1(G) < G \qquad \ldots (1)$$

Now $Z_1(G) \triangleleft G$ and hence the quotient group $\frac{G}{Z_1(G)}$ is defined.

Consider the canonical/natural map $f_1 : G \longrightarrow \frac{G}{Z_1(G)}$. Surely f_1 is an onto homomorphism.

As $Z\left[\frac{G}{Z_1(G)}\right] \trianglelefteq \frac{G}{Z_1(G)}$, $f^{-1}\left[Z\left[\frac{G}{Z_1(G)}\right]\right]$ is a normal subgroup of G. Denote it by $Z_2(G)$.

Thus, continuing in this process, we can construct a sequence of normal subgroups of G i.e. $Z(G), Z_1(G), Z_2(G), \ldots$ such that $\{e\} \leq Z(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots$.

This series is called the ascending central series of the group G.

Example 3.3.4 : Find the ascending central series for (i) S_3 and (ii) D_4.

Solution :

(i) $G = S_3 \quad \Longrightarrow \quad Z(G) = \{i\}$ where i is the identity map.

Hence the ascending central series of S_3 is

$$\{i\} \leq \{i\} \leq \cdots \leq \{i\} \leq \cdots$$

(ii) $G = D_4 \quad \Longrightarrow \quad Z(G) = \{\rho_0, \rho_2\}$

where

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Now, $\left|\frac{D_4}{Z(D_4)}\right| = \frac{8}{2} = 4$

As $\left|\frac{D_4}{Z(D_4)}\right| \leq 5$

we get, $\frac{D_4}{Z(D_4)}$ is abelian and hence $Z\left[\frac{D_4}{Z(D_4)}\right] = \frac{D_4}{Z(D_4)}$.

$f: D_4 \longrightarrow \frac{D_4}{Z(D_4)}$ be a canonical mapping.

f being onto, $f^{-1}\left[\frac{D_4}{Z(D_4)}\right] = D_4$

Thus, the ascending central series in D_4 is

$$\{\rho_0\} \leq \{\rho_0, \rho_2\} \leq D_4 \leq D_4 \leq \cdots$$

3.4 Nilpotent Groups:

Thus we obtain normal subgroups $Z_1(G), Z_2(G), \ldots, Z_n(G), \ldots$ of G such that

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z\left[\frac{G}{Z_{n-1}(G)}\right], \qquad \text{for every positive integer n > 1.}$$

$Z_n(G)$ is called the n^{th} center of G.

Define $Z_0(G) = \{e\}$. Then

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z\left[\frac{G}{Z_{n-1}(G)}\right], \qquad \text{for all positive integers n.}$$

Again by definition,

$$Z_n(G) = \{x \in G \ \ xyx^{-1}y^{-1} \in Z_{n-1}(G) \ / \ \text{ for all } y \in G\}$$

Hence,

$$[Z_n(G)]' \subseteq Z_{n-1}(G).$$

Definition 3.4.1: A group G is said to be nilpotent if $Z_m(G) = G$ for some m. The smallest m such that $Z_m(G) = G$ is called the class of nilpotency of G.

Remark : Every abelian group is nilpotent. If G is abelian, then $Z_1(G) = Z(G)$. Hence G is nilpotent.

Theorem 3.4.2: Subgroup of a nilpotent group is nilpotent.

Proof : Let G be a nilpotent group.

Hence, $\exists$ a positive integer m such that $Z_m(G) = G$. Let $H \leq G$.

To prove that H is nilpotent.

When $H = \{e\}$ or $H = G$. The result is obviously true.

Let $\{e\} < H < G$.

Now let $x \in H \cap Z(G)$. Then $gx = xg$ for all $g \in G$ will imply $hx = xh$ for all $h \in H$. Hence $x \in Z(H)$. Thus ,

$$H \cap Z(G) \subseteq Z(H)$$

As $Z(G) = Z_1(G)$ and $Z(H) \leq H$ we get

$$H \cap Z(G) \leq Z_1(H) \qquad \ldots (1)$$

Now, let $x \in H \cap Z_2(G)$.

Then $\quad x \in Z_2(G)$ will imply $xyx^{-1}y^{-1} \in Z_1(G) \quad$ for all $y \in G$

But then $\quad xyx^{-1}y^{-1} \in Z_1(G) \quad$ for all $y \in H$

As $x \in H$ and $y \in H$ we get $xyx^{-1}y^{-1} \in Z_1(G) \quad$ for all $y \in H$.

But this in turn will imply $x \in Z_2(H)$. This shows that

$$H \cap Z_2(G) \leq Z_2(H) \qquad \ldots (2)$$

Continuing in this way, we get

$$H \cap Z_n(G) \subseteq Z_n(H) \qquad \text{for all n.}$$

Hence in particular,

$$H \cap Z_m(G) \subseteq Z_m(H)$$

i.e. $\quad H \cap G \subseteq Z_m(H)$

i.e. $\quad H \subseteq Z_m(H)$

But as always, $Z_m(H) \subseteq H$, we get $Z_m(H) = H$.

This proves that H is nilpotent.

Theorem 3.4.3: Every homomorphic image of a nilpotent group is nilpotent.

Proof : Let G be a nilpotent group. Let $\phi : G \longrightarrow G_1$ be an onto homomorphism. To prove that the group G_1 is nilpotent.

As G is nilpotent, ∃ a positive integer m such that $Z_m(G) = G$.

(i) $Z(G) = \{x \in G \ / \ xg = gx \ \ \forall \ \ g \in G\}$

$Z(G_1) = \{x \in G_1 \ / \ xg = gx \ \ \forall \ \ g \in G_1\}$

$= \{\phi(x) \in G_1 \ / \ \phi(x) \cdot \phi(g) = \phi(g) \cdot \phi(x) \ \ \forall \ \ \phi(g) \in G_1\} \quad \ldots \because \ \phi$ in onto.

But this shows that

$$\phi[Z(G)] \subseteq Z(G_1) \qquad \ldots (1)$$

Let $x \in Z_2(G)$. $\quad$ Then $\quad xyx^{-1}y^{-1} \in Z_1(G) \quad$ for all $y \in G$.

Hence,

$$\phi\,(xyx^{-1}y^{-1}) \in \phi[Z_1(G)] \qquad \text{for all } y \in G.$$

i.e. $\quad \phi(x)\,\phi(y)\,[\phi(x)]^{-1}\,[\phi(y)]^{-1} \in \phi[Z_1(G)] \qquad$ for all $\phi(y) \in G_1$.

But this in turn will imply $\phi(x) \in Z_2(G_1)$.

Thus, $\quad x \in Z_2(G) \quad \Longrightarrow \quad \phi(x) \in Z_2(G_1)$.

Therefore,

$$\phi\,[Z_2(G)] \subseteq Z_2(G_1) \qquad \ldots (2)$$

Continuing in this way, we get for all n

$$\phi\,[Z_n(G)] \subseteq Z_n(G_1) \qquad \ldots (3)$$

Hence in particular, $\quad \phi\,[Z_m(G)] \subseteq Z_m(G_1)$

Hence, $\quad \phi\,(G) \subseteq Z_m(G_1)$

But ϕ being onto, $\quad \phi\,(G) = G_1$

Hence , $\quad G_1 \subseteq Z_m(G_1) \subseteq G_1$

$\Longrightarrow \quad Z_m(G_1) = G_1$

Hence, the group G_1 in nilpotent.

Theorem 3.4.4: Any group of order p^n is nilpotent. OR Any p-group is nilpotent.

Proof : Let G be a group with $|G| = p^n$.

To prove that G is nilpotent.

If $G = Z(G)$ then we are through. Assume that $G \neq Z(G)$.

Then as $p \,\big|\, |G|$ we get $Z(G) \neq \{e\}$. Hence $|Z(G)| \neq 1$.

Further $|Z(G)| \,\big|\, |G|$ as $Z(G) \leq G$ we have $|Z(G)| = p^r$ for some $r < n$.

But then

$$\left|\frac{G}{Z(G)}\right| = \frac{|G|}{|Z(G)|} = p^{n-r}$$

will imply $p \,\Big|\, \left|\frac{G}{Z(G)}\right|$.

Hence, $Z\left[\frac{G}{Z(G)}\right]$ is non trivial. $\qquad$ i.e. $Z\left[\frac{G}{Z(G)}\right] \neq Z(G)$.

Hence, by definition of $Z_2(G)$ we get $Z(G) \subset Z_2(G)$.

i.e. $\quad |Z_1(G)| < |Z_2(G)|$.

Continuing in this way we get,

$$|Z_1(G)| < |Z_2(G)| < \cdots \leq |G| = p^n$$

Hence, there must exists some positive integer m such that $|Z_m(G)| = p^n$.

This shows that G is nilpotent.

Theorem 3.4.5: A group G is nilpotent iff G has a normal series.

$$\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$$

such that

$$\frac{N_{i+1}}{N_i} \subseteq Z\left[\frac{G}{N_i}\right]$$

for all i, $1 \leq i \leq k-1$.

Proof : <u>Only if part :</u>

Let G be nilpotent then $\exists$ a positive integer m such that $Z_m(G) = G$.

Consider the series

$$Z_0(G) = \{e\} < Z_1(G) < Z_2(G) < \cdots \leq Z_m(G) = G$$

Then

(i) $Z_i(G)$ is a normal subgroup of G for each i.

(ii) $\frac{Z_{i+1}}{Z_i} \subseteq Z\left[\frac{G}{Z_i}\right]$ for each i, $0 \leq i \leq m-1$.

(iii) $Z_i \lhd Z_{i+1}$ for each i, $0 \leq i \leq m-1$.

Hence

$$Z_0(G) = \{e\} < Z_1(G) < Z_2(G) < \cdots \leq Z_m(G) = G$$

will form the required series.

<u>If part :</u>

Let G be group and let G have a normal series

$$\{e\} = G_0 < G_1 < G_2 < \cdots \leq G_k = G$$

such that

$$\frac{G_{i+1}}{G_i} \subseteq Z\left[\frac{G}{G_i}\right]$$

To prove that G is nilpotent.

As $\frac{G_{i+1}}{G_i} \subseteq Z\left[\frac{G}{G_i}\right]$ we get $\frac{G_1}{\{e\}} \subseteq Z\left[\frac{G}{\{e\}}\right]$.

Thus, $G_1 \subseteq Z[G]$

i.e. $G_1 \subseteq Z_1[G]$ . . . (1)

Again by assumption, $\frac{G_2}{G_1} \subseteq Z\left[\frac{G}{G_1}\right]$.

Now, for any $x \in G$ we get $G_1 x \in \frac{G_2}{G_1}$. Hence $G_1 x \in Z\left[\frac{G}{G_1}\right]$.

Hence, $[G_1 x]\,[G_1 y] = [G_1 y]\,[G_1 x]$ for all $G_1, y \in \frac{G}{G_1}$

i.e. $xyx^{-1}y^{-1} \in G_1$ for all $y \in G$.

i.e. $xyx^{-1}y^{-1} \in Z_1[G]$ … by (1)

Thus, $x \in G_2 \implies xyx^{-1}y^{-1} \in Z_1[G]$

$\implies x \in Z_2[G]$

Hence, $G_2 \subseteq Z_2[G]$ . . . (2)

Continuing in this way we get

$$G = G_k \subseteq Z_k(G) \subseteq G.$$

Hence, $Z_k(G) = G$

Hence G is nilpotent.

Worked Examples

Example 3.4.6 : $G = S_3$ is not nilpotent.

Solution: For S_3, $Z(S_3) = \{\varrho_0\}$ where ϱ_0 is the identity element of S_3.

Hence, $Z_1(S_3) = \{\varrho_0\}$.

$$Z\left[\frac{S_3}{\{\varrho_0\}}\right] = \left\{\{\varrho_0\}\right\}$$

Hence, $Z_2(S_3) = \{\varrho_0\}$.

Continuing in this way we get, $Z_m(S_3) = \{\varrho_0\}$ for any $m \geq 0$.

Hence, S_3 is not nilpotent.

Example 3.4.7: D_4 is nilpotent.

Solution : We know that $Z_1(D_4) = \{\varrho_0,\ \varrho_2\}$.

Hence $$\frac{D_4}{Z(D_4)} = \frac{D_4}{\{\varrho_0, \varrho_2\}}$$

As $$\left|\frac{D_4}{\{\varrho_0, \varrho_2\}}\right| = \frac{|D_4|}{|\{\varrho_0, \varrho_2\}|} = \frac{8}{2} = 4$$

Hence, $\frac{D_4}{Z(D_4)}$ is abelian. Therefore $Z\left[\frac{D_4}{Z(D_4)}\right] = \frac{D_4}{Z(D_4)}$

Hence, $Z_2(D_4) = D_4$. Hence, D_4 is nilpotent.

Example 3.4.8 : Show that S_n is not nilpotent for $n \geq 3$.

Solution : For $n \geq 3$, $Z[S_n] = \{e\}$ where e is the identity element in S_n.

Thus $Z_1(S_n) = \{e\}$. But then $Z_m(S_n) = \{e\}$ for all positive integers m.

Hence S_n is nilpotent for $n \geq 3$.

Remark : S_3 is solvable but S_3 is not nilpotent. This shows that every solvable group need not be nilpotent. But converse is always true. i.e. every nilpotent group is solvable.

Theorem 3.4.9: Every nilpotent group is solvable.

Proof : Let G be nilpotent group. Then by theorem 3.4.5, there exists a normal series

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

such that

$$\frac{H_{i+1}}{H_i} \subseteq Z\left[\frac{G}{H_i}\right]$$

As $Z\left[\frac{G}{H_i}\right]$ is abelian, we get $\frac{H_{i+1}}{H_i}$ is abelian.

Hence by theorem 2.2.13, G is solvable.

Worked Examples

Example 3.4.10 : Give an example of a group G such that G has a normal subgroup N with both N and $\frac{G}{N}$ nilpotent but G is non-nilpotent.

Solution: Consider $G = S_3$.

We know, S_3 is not nilpotent (See example3.4.8).

$N = \{(1), (1,2,3), (1,3,2)\}$ is a normal subgroup of S_3.

N is an abelian subgroup of S_3 ($\because \quad |N| = 3$)

Hence N is nilpotent.

Again $\left|\frac{S_3}{N}\right| = \frac{6}{3} = 2 \quad \Rightarrow \quad \frac{S_3}{N}$ is abelian. $\quad \Rightarrow \quad \frac{S_3}{N}$ is nilpotent.

Thus both N and $\frac{S_3}{N}$ are nilpotent but S_3 is not nilpotent.

Example 3.4.11 : Show that the product of two nilpotent groups is a nilpotent group.

Solution : Let H and K be any two nilpotent groups.

Then ∃ positive integers m and n such that $Z_m(H) = H$ and $Z_n(K) = K$.

Let $G = H \times K$.

$$x \in Z(G) \quad \Longrightarrow \quad xg = gx \quad \text{for all } g \in G.$$

$$x = (x_1,\ x_2) \text{ and } \quad g = (g_1,\ g_2)$$

Then $xg = (x_1 g_1,\ x_2 g_2)$

$$gx = (g_1 x_1,\ g_2 x_2)$$

Thus, $xg = gx \quad \Longrightarrow \quad x_1 g_1 = g_1 x_1$ and $x_2 g_2 = g_2 x_2$ for all $g_1 \in H,\ \ g_2 \in K$

But this will imply $x_1 \in Z(H)$ and $x_2 \in Z(K)$.

Thus, $x = (x_1,\ x_2) \in Z(G) = Z(H \times K) \quad \Longrightarrow \quad (x_1,\ x_2) \in Z(H) \times Z(K)$

Similarly, we can prove that

$$(x_1,\ x_2) \in Z(H) \times Z(K) \quad \Longrightarrow \quad x = (x_1,\ x_2) \in Z(G) = Z(H \times K)$$

Hence,

$$Z(H \times K) = Z(H) \times Z(K).$$

By iteration,

$$Z_i(H \times K) = Z_i(H) \times Z_i(K) \qquad \text{for each positive integer } i.$$

Hence, if $m > n$ then $Z_n(K) = K \quad \Longrightarrow \quad Z_m(K) = K$.

Thus, $Z_m(H \times K) = Z_m(H) \times Z_m(K) = H \times K$.

This shows that $Z_m(G) = G$ and $G = H \times K$ is nilpotent.

Unit 4 : Sylow Theorems :

4.1 Group action on a set.

4.2 Class equation of a group.

4.3 p-groups

4.4 Three Sylow theorems.

4.1 Group action on a set :

Definition 4.1.1: Let G be any group and let X be any non-empty set. An action of G on X is a mapping $f: X \times G \longrightarrow X$ satisfying the following conditions

(i) $f(x, e) = x$ for all $x \in G$

(ii) $f(x, g_1 g_2) = f(f(x, g_1), g_2)$ for all $x \in G$ and $g_1,\ g_2 \in G$

Under these conditions we say X is a G-set. Note that every G-set need not be a group.

Examples 4.1.2 :

(i) Let $X = \{1, 2, \dots, n\}$ and $G = \langle S_n,\ 0\rangle$. Define $f : X \times G \longrightarrow X$ by

$$f(x, \sigma) = \sigma(x) \qquad \text{for } x \in X \text{ and } \sigma \in S_n.$$

Then

(1) $f(x,\ i) = i(x) = x$ where i = identity map defined on X.

(2) $f(x,\ \sigma_1 \circ \sigma_2) = (\sigma_1 \circ \sigma_2)(x) = \sigma_2[\sigma_1(x)]$

$= f[f(x, \sigma_1),\ \sigma_2]$

From (1) and (2) we get X is a G-set.

(ii) Let G be any group and let $H \leq G$. $\mathfrak{R}$ denotes the set of all right cosets of H in G.

Define $f : \mathfrak{R} \times H \longrightarrow \mathfrak{R}$ by

$$f(H_x, h) = H_{xh} \qquad \text{for } H_x \in \mathfrak{R} \text{ and } h \in H.$$

Then

(1) $f(H_x,\ e) = H_{xe} = H_x$ where i = identity map defined on X.

(2) $f(H_x,\ h_1 h_2) = H_{x(h_1 h_2)} = H_{(xh_1)h_2}$

$= f[f(H_x, h_1),\ h_2]$

From (1) and (2) we get $\mathfrak{R}$ is a H-set.

(iii) Let G be any group and X be the set of all subgroups of G. Define $f : X \times G \longrightarrow G$ by

$$f(T, g) = g^{-1}Tg \qquad \text{for } T \in X \text{ and } g \in G.$$

Then

(1) $f(T, e) = e^{-1}Te = T$

(2) $f(T,\ g_1 g_2) = (g_1 g_2)^{-1} T (g_1 g_2)$

$= g_2^{-1}\,[g_1^{-1} T g_1]\, g_2$

$= f[f(T, g_1),\ g_2]$

Hence X is a G - set.

(iv) Let G be a group and $H \leq G$. Define $f : G \times H \longrightarrow G$ by

$$f(g, h) = h^{-1}gh \qquad \text{for } g \in G \text{ and } h \in H.$$

Then

(1) $f(g, e) = e^{-1}ge = g$

(2) $f(g, h_1 h_2) = (h_1 h_2)^{-1}\, g\, (h_1 h_2)$

$= h_2^{-1}\,[h_1^{-1}\, g\, h_1]\, h_2$

$= f[f(g, h_1),\ h_2]$

Hence G is a H - set.

(v) Any group G is a G – set under the action $f: G \times G \longrightarrow G$ defined by

$$f(g_1, g_2) = g_1 \cdot g_2\ , \qquad \text{for all } g_1, g_2 \in G.$$

Remark : Let X be a G – set. Then by definition 4.1.1, there exists $f : X \times G \longrightarrow X$ satisfying the conditions,

(1) $f(x, e) = x$ and

(2) $f(x, g_1 g_2) = f[f(x, g_1),\ g_2]$.

Here onwards we write $f(x, g) = xg$, for all $x \in X$ and $g \in G$.

Thus, $xe = x$ and $x(g_1 g_2) = (xg_1)g_2$, for all $x \in X$ and $g_1, g_2 \in G$.

Let X be a G – set. For a fixed $x \in X$, define

$$G_x = \{g \in G\ /\ xg = x\}$$

and for a fixed $g \in G$, define

$$X_g = \{x \in X\ /\ xg = x\}.$$

As an important property of the set G_x, we prove

Theorem 4.1.3 : Let X be a G – set. for any $x \in X$, $G_x \leq G$.

Proof :

(i) $xe = x \implies e \in G_x \implies G_x \neq \phi$.

(ii) $g_1,\ g_2 \in G \implies xg_1 = x$ and $xg_2 = x$.

Hence, $x(g_1\ g_2) = (xg_1)g_2 = xg_2 = x$.

This shows that $g_1 g_2 \in G_x$.

(iii) Let $g \in G_x$. Then $xg = x \implies (xg)g^{-1} = xg^{-1}$

$\implies x(gg^{-1}) = xg^{-1}$

$\implies x \cdot e = xg^{-1}$

$\implies x = xg^{-1}$

Hence $g \in G_x \implies g^{-1} \in G_x$

From (i), (ii) and (iii) we get G_x is a sub group of G.

Definition 4.1.4 : Let X be a G – set. For any $x \in X$, the subgroup G_x of G is called the isotropy subgroup of G.

Example 4.1.5 : Let $X = \{1, 2, 3\}$. Then X is a S_3 - set. (See example 4.1.2 (1)). We have

$$S_3 = \{(1), (1\ \ 2), (1\ \ 3), (2\ \ 3), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$$

The isotropy subgroup of 2 is $\{(1), (1\ \ 3)\}$.

On each G-set X, the group G induces an equivalence relation. This we prove in the following theorem.

Theorem 4.1.6 : Let X be a G – set. Define a relation '~' on X by

$$x \sim y \quad \Rightarrow \quad x = y \cdot g, \qquad \text{for some } g \in G.$$

Then the relation '~' is an equivalence relation on X.

Proof :

(i) $xe = x$ for all $x \in X$ $\quad\Rightarrow\quad x \sim x$, for all $x \in X$.

$\Rightarrow$ the relation '~' is reflexive.

(ii) Let $x \sim y$. Hence $x = yg$, for some $g \in G$.

$xg^{-1} = (yg)\, g^{-1} = y(gg^{-1}) = ye = y$

This shows that $x \sim y \quad\Rightarrow\quad y \sim x$, for x, $y \in X$.

Hence the relation '~' is symmetric.

(iii) Let $x \sim y$ and $y \sim z$.

Then $x = yg_1$ and $y = zg_2$ for some $g_1,\ g_2 \in G$.

Thus, $x = yg_1 = (zg_2)g_1 = z(g_2g_1)$.

As $g_2,\ g_1 \in G$, we get $x \sim z$.

This shows that $x \sim y,\ y \sim z \ \Rightarrow\ x \sim z$ for $x, y, z \in X$.

Hence the relation '~' is transitive.

From (i), (ii) and (iii) we get '~' is an equivalence relation on X.

Definition 4.1.7 : Let X be a G – set. Each equivalence class produced by the equivalence relation '~' defined on X, described in Theorem 4.1.6, is called an orbit in X under G.

The equivalence class containing $x \in X$ is orbit of x and we denote it by xG.

Thus, $xG = \{y \in X \,/\, x \sim y\}$

$= \{y \in X \,/\, x = yg \ \ for\ some\ g \in G\}$

A relation between the orbit xG and the subgroup G_x in a G – set X is as follows.

Theorem 4.1.8 : Let X be any G – set. Then $|xG| = (G : G_x)$, for any $x \in X$.

Proof : Fix up any $x \in X$. Let $\mathfrak{R}$ denote the collection of all right cosets of the subgroup G_x in G. We will show that $\mathfrak{R}$ is equipotent with the set xG.

Now $y \in xG \implies y \sim x \implies y = xg$ for some $g \in G$.

Define $\phi : xG \longrightarrow \mathfrak{R}$ by

$$\phi(y) = G_x\, g \qquad \text{where } y = xg, \quad g \in G.$$

(i) ϕ is well defined.

Let $y_1 = y_2$ in xG.

Then $y_1 = xg_1$ and $y_2 = xg_2$ for some $g_1, g_2 \in G$.

Thus $y_1 = y_2$

$$\begin{aligned} &\implies xg_1 = xg_2 \\ &\implies (xg_1)\, g_1^{-1} = (xg_2)\, g_1^{-1} \\ &\implies x(g_1g_1^{-1}) = x(g_2g_1^{-1}) \\ &\implies xe = x(g_2g_1^{-1}) \\ &\implies x = x(g_2g_1^{-1}) \\ &\implies g_2g_1^{-1} \in G_x \\ &\implies (G_x)g_1 = (G_x)g_2 \\ &\implies \phi(y_1) = \phi(y_2) \end{aligned}$$

This shows that ϕ is well defined map.

(ii) ϕ is one-one.

Let $\phi(y_1) = \phi(y_2)$, for some $y_1,\ y_2 \in X$.

Let $\phi(y_1) = (G_x)g_1$, where $y_1 = x\, g_1$

and $\phi(y_2) = (G_x)g_2$, where $y_2 = x\, g_2$.

Thus,

$$\begin{aligned} &\phi(y_1) = \phi(y_2) \\ \implies &(G_x)g_1 = (G_x)g_2 \\ \implies &g_1g_2^{-1} \in G_x \\ \implies &x\,(g_1g_2^{-1}) = x \\ \implies &(xg_1)\, g_2^{-1} = x \\ \implies &xg_1 = xg_2 \\ \implies &y_1 = y_2 \end{aligned}$$

This shows that ϕ is one-one.

(iii) ϕ is onto.

Let $(G_x)g \in \mathfrak{R}$. Then $g \in G$ and for this g, consider the element $y \in X$ defined by $y = xg$.

Then $\phi(y) = (G_x)g$ shows that ϕ is onto.

From (i), (ii) and (iii) we get ϕ is an one-one, onto mapping. Hence ,

$$|xG| = |\Re|$$

But $|\Re|$= Number of right cosets of G_x in G = $(G : G_x)$.

Hence, $|xG| = (G : G_x), \quad \forall \ x \in X.$

Corollary 4.1.9 : Let G be a finite group and let X be a finite G-set. Then

(i) $|G| = |xG| \cdot |G_x|$, for any $x \in X$.

(ii) $|X| = \sum_{x \in C} (G : G_x)$, where C denotes the subset of X containing exactly one element from each orbit.

Proof :

(i) From theorem 4.1.8, we have,

$$|xG| = (G : G_x) , \qquad \text{for any } x \in X.$$

Hence $|xG| = \frac{|G|}{|G_x|}$ … Since G is a finite group.

Hence $|G| = |xG| \cdot |G_x|$

(ii) Let C denote the subset of X containing exactly one element from each orbit of X under G.

Then

$$|X| = \sum_{x \in C} xG$$

Since

$$X = \bigcup_{x \in C} xG$$

and this union is a disjoint union.

As by theorem 4.1.8,

$$|xG| = (G : G_x)$$

we get,

$$|X| = \sum_{x \in C} (G : G_x)$$

The following theorem gives a tool for determining the number of orbits in a G-set X under G.

- ***Burnside Theorem :***

Theorem 4.1.10 : Let G be a finite group and let X be a finite G-set. If r is the number of orbits in X under G, then

$$r.|G| = \sum_{g \in G} |X_g|$$

Proof : Let N = number of ordered pairs $(x, g) \in X \times G$ for which $xg = x$. Then for a fixed $g \in G$, there are $|X_g|$ with pairs with g as a second member and $xg = x$. Hence

$$N = \sum_{g \in G} |X_g| \qquad \ldots (1)$$

Similarly, for a fixed $x \in X$, there are $|G_x|$ pairs with x as a first member and $xg = x$. Hence,

$$N = \sum_{x \in X} |G_x| \qquad \ldots (2)$$

From (1) and (2) we get,

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$$

$$= \sum_{x \in X} \frac{|G|}{|xG|} \qquad \because \quad |xG| = (G : G_x) = \frac{|G|}{|G_x|}$$

$$= |G| \sum_{x \in X} \frac{1}{|xG|} \qquad \ldots (3)$$

Now, let $O_1, O_2, O_3, \ldots, O_r$ be r orbits of X under G. Then $X = \bigcup_{i=1}^{r} O_i$ and this union is disjoint. Hence we get,

$$\sum_{x \in X} \frac{1}{|xG|} = \sum_{x \in \bigcup_{i=1}^{r} O_i} \frac{1}{|xG|}$$

$$= \sum_{x \in O_1} \frac{1}{|xG|} + \sum_{x \in O_2} \frac{1}{|xG|} + \cdots + \sum_{x \in O_r} \frac{1}{|xG|}$$

Now consider $\sum_{x \in O_1} \frac{1}{xG}$.

Let $O_1 = \{t_1, t_2, t_3, \ldots, t_n\}$ (O_i is finite as X is finite)

Hence,

$$\sum_{x \in O_1} \frac{1}{|xG|} = \frac{1}{|t_1 G|} + \frac{1}{|t_2 G|} + \cdots + \frac{1}{|t_n G|}$$

$$= \frac{1}{|O_1|} + \frac{1}{|O_1|} + \cdots$$

$$+ \frac{1}{|O_1|} \qquad (n \text{ times}) \ \ldots \text{by the definition of orbit}$$

$$= \frac{1}{n} + \frac{1}{n} + \cdots + \frac{1}{n} \qquad \ldots n \text{ times}$$

$$= \frac{n}{n} = 1$$

Generalizing this result we get,

$$\sum_{x \in O_i} \frac{1}{|xG|} = 1 \qquad \text{for each } i, \ \ 1 \leq i \leq r$$

Hence,

$$\sum_{x \in X} \frac{1}{|xG|} = 1 + 1 + \cdots + 1 \qquad (r \text{ times})$$

$$= r \qquad \ldots (4)$$

From (3) and (4) we get,

$$\sum_{g \in G} |X_g| = |G| \cdot r$$

i.e. $\quad r \cdot |G| = \sum_{g \in G} |X_g|$

This completes the proof.

4.2 Class Equation of a Group :

As an application of the Burnside theorem, we derive an equation which is called class equation of a group.

Let G be a finite group and let X be a finite G set. Let $O_1, O_2, O_3, \ldots, O_r$ be different r-orbits in X by G. Select $x_i \in O_i$ for each i. Then X being the disjoint union of $O_1, O_2, O_3, \ldots, O_r$, we get

$$|X| = \sum_{i=1}^{r} |O_i|$$

$$= \sum_{i=1}^{r} |x_i G| \qquad \dots (1)$$

Define $X_G = \{x \in X \ / \ xg = g, \quad \text{for all } g \in G\}$

Let O_i denote an one element orbit i.e. $O_i = \{x_i\}$. Then

$$\begin{aligned} O_i &= \{y \in X \ / \ y \sim x_i\} \\ &= \{y \in X \ / \ y = x_i\, g \quad \text{for some } g \in G\} \\ &= \{x_i\, g \ / \ g \in G\} \\ &= \{x_i\} \qquad \dots \text{by assumption.} \end{aligned}$$

Thus, $O_i = \{x_i\}$ if and only if $x_i = x_i\, g$ for all $g \in G$. Hence the set X_G is precisely the union of one element orbit in X. Assume that there are 's' one element orbits in X under G.

Then,

$$|X| = s + \sum_{i=s+1}^{r} |x_i G|$$

i.e.
$$|X| = |X_G| + \sum_{i=s+1}^{r} |x_i G| \qquad \dots (2)$$

Again, $|x_i G| = (G : G_{x_i})$ … by Burnside theorem.

Hence, from (2) we get,

$$|X| = |X_G| + \sum_{i=s+1}^{r} \left(G : G_{x_i}\right) \qquad \dots (3)$$

Now, for a finite group G we can consider G as a G set under conjugation.

i.e. $xg = g^{-1}xg \qquad$ for $x, g \in G$.

Then by (2) we get,

$$|G| = |X_G| + \sum_{i=s+1}^{r} x_i G \qquad \dots (4)$$

Consider the set X_G in (4)

$$\begin{aligned} X_G &= \{x \in X \ / \ xg = x, \ \forall \ \ g \in G\} \\ &= \{x \in X \ / \ g^{-1}xg = x, \ \forall \ \ g \in G\} \qquad (\because \ \ xg = g^{-1}xg) \\ &= \{x \in X \ / \ xg = gx, \ \forall \ \ g \in G\} \\ &= Z(G) \qquad Z(G) = \text{center of } G \end{aligned}$$

Substituting $|X_G| = |Z(G)|$ in (4) we get

$$|G| = |Z(G)| + \sum_{i=s+1}^{r} |x_i G|$$

$$= |Z(G)| + \sum_{i=s+1}^{r} \left(G : G_{x_i}\right)$$

Let $\quad n_i = \left(G : G_{x_i}\right) \quad$ for each i.

Then $\quad n_i \,\Big|\, |G| \quad$ for each i.

Hence,

$$|G| = |Z(G)| + n_{s+1} + n_{s+2} + \ldots + n_r$$

i.e. $\quad |G| = C + n_{s+1} + n_{s+2} + \ldots + n_r \qquad \ldots (5)$

where $C = |Z(G)|$

The equation (5) is called the class equation of the group G.

Recall that, for any $x \in G$ the set

$$C(x) = \{g^{-1}xg \ / \ g \in G\}$$

is called the conjugate class of x in G and the set

$$N(x) = \{g \in G \ / \ g^{-1}xg = x\}$$

is a normalizer of x in G. $N(x)$ is a subgroup of G and $|C(x)| = \left(G : N(x)\right)$. If xG denote the orbit of G under conjugation of G containing the element x; then

$$\begin{aligned} xG &= \{y \in X \ / \ y \sim x\} \\ &= \{y \in G \ / \ y = xg, \text{ for some } g \in G\} \\ &= \{y \in G \ / \ y = g^{-1}xg, \text{ for } g \in G\} \\ &= C(x) \end{aligned}$$

Thus $|xG| = |C(x)| = (G : N(x)) \qquad \ldots (6)$

From the equation (5) we get,

$$|G| = |Z(G)| + \sum_{i=s+1}^{r} |x_i G|$$

Where $x_i G$ represents the orbit in G under conjugation by G, containing more than one element.

Hence, from (5) and (6) we get

$$|G| = |Z(G)| + \sum_{x \in C}^{r} (G : N(x))$$

where C contains exactly one element from each conjugate class with more than one element.

Example : Consider the group $G = S_3$. The centre of the group S_3 contains only one element and the class equation of S_3 is 6 = 1 + 2 + 3.

With the help of class equation we derive the following important property of $|Z(G)|$.

Theorem 4.2.1 : Let G be a finite group with $|G| = p^n$ where p is a prime number. Then the centre of G is non trivial.

Proof : $|G| = p^n$. to prove that $Z(G) \neq \{e\}$.

We know that the class equation of G is

$$|G| = C + n_{c+1} + n_{c+2} + \ldots + n_r \qquad \ldots (1)$$

where $n_i \Big| \, |G|$ for each i and

n_i = cardinality of the conjugate class in G and $C = |Z(G)|$.

Now,

$$n_i \Big| \, |G| \implies n_i \Big| \, p^n \implies p \Big| \, n_i, \qquad \text{for each } i,\ c+1 \leq i \leq r.$$

Hence, $p \Big| \, n_{c+1} + n_{c+2} + \ldots + n_r$.

Again $p \Big| \, |G| = p^n$.

Hence, $p \Big| \, [|G| - (n_{c+1} + n_{c+2} + \ldots + n_r)]$

From (1) we get, $p \Big| \, c$.

i.e. $p \Big| \, |Z(G)|$.

Hence, $|Z(G)| > 1$.

i.e. $Z(G) \neq \{e\}$

We know that if $|G| = p$, (p is prime) then G is cyclic and hence abelian. In the next theorem we prove that if $|G| = p^2$ then also G is abelian.

Theorem 4.2.2 : If $O(G) = p^2$, (p is prime), then G is an abelian group.

Proof : Let G be a non abelian group. Then $G \neq Z(G)$.

Hence, $|Z(G)| \neq p^2$.

As $|G| = p^2$, by the theorem 2.1, $Z(G) \neq \{e\}$ and hence $|Z(G)| \neq 1$.

As $Z(G) \,\Big|\, |G|$, (G being finite) we get $|Z(G)| = 1,\ p,\ p^2$.

Hence, the only possible value is $|Z(G)| = p$.

Select any $a \in G$ such that $a \notin Z(G)$. (Such a exists as $Z(G) \subset G$).

Consider $N(a) = \{x \in G \,/\, xax^{-1} = a\}$.

Then $N(a) \leq G$. Further $x \in Z(G)$.

$\Longrightarrow \quad xg = gx \qquad$ for all $g \in G$.

$\Longrightarrow \quad xa = ax \qquad$ as $a \in G$.

$\Longrightarrow \quad xax^{-1} = a$

$\Longrightarrow \quad x \in N(a)$

Thus, $Z(G) \leq N(a)$.

But $a \in N(a)$ and $a \notin Z(G)$ gives $Z(G) \subset N(a)$.

Thus, we have $Z(G) < N(a) \leq G$.

As $N(a) \leq G$ and $|G| = p^2$, we must have $|N(a)| = p^2$.

But then $N(a) = G$. Then by definition of $N(a)$, $ax = xa$ for all $x \in G$.

But this in turn will imply $a \in Z(G)$, a contradiction.

Hence G must be abelian.

An important property of a finite G – set is proved in the following theorem.

Theorem 4.2.3 : Let G be a finite group and X is a finite G – set. If $|G| = p^n$ (n > 0), (or if $p \,\Big|\, |G|$) then $|X| \equiv |X_G|$ (mod p).

Proof : Let X be a G - set. X and G both are finite. We know that

$$|X| = |X_G| + \sum_{i=s+1}^{r} |x_i G| \qquad \ldots (1)$$

where $\quad X_G = \{x \in X \,/\, xg = gx \ \ for\ each\ g \in G\}$

and $\quad |X_G| = s$.

$x_i G$ denotes the orbit in X under the action of G containing more than one element.

r = number of orbits in X.

By theorem 4.1.8,

$$|x_i G| = (G : G_x)$$

Hence G being a finite group

$$(G : G_x) \,\Big|\, |G| \qquad \text{for each } i.$$

Thus, $\quad |x_i G| \,\Big|\, |G| \qquad$ for each i.

As $|G| = p^n$ we get $p \,\Big|\, |x_i G|$ for each i. Hence

$$p \,\Big|\, \sum_{i=s+1}^{r} |x_i G| \qquad \ldots (2)$$

From (1) we get,

$$\sum_{i=s+1}^{r} |x_i G| = |X| - |X_G|$$

Hence, by (2) we get $p \,\Big|\, |X| - |X_G|$.

i.e. $\quad |X| \equiv |X_G| \pmod{p}$

We know that converse of Lagrange's theorem need not be true.

i.e. if G is a finite group and if $m/O(G)$ then G not necessarily contains a subgroup of order m. But if m is a prime number then surely G contains a subgroup of order m if $m/|G|$. This is proved by Cauchy in the following theorem.

- **Cauchy theorem :**

Theorem 4.2.4 : Let G be a finite group and p be a prime number such that $p \,\Big|\, |G|$. Then there exists an element $a \in G$ such that $a^p = e$.

Proof :

(i) Define $X = \{(g_1, g_2, \ldots, g_p) \,/\, g_1 \cdot g_2 \cdot \ldots \cdot g_p = e \;\; and \;\; g_i \in G\}$

$g_1 \cdot g_2 \cdot \ldots \cdot g_p = e \;\; \Longrightarrow \;\; g_p^{-1} = g_1\, g_2 \ldots g_{p-1}$.

Hence in p-tuple $(g_1, g_2, \ldots, g_p)$ we have a freedom to select only $p-1$ elements $g_1, g_2, \ldots, g_{p-1}$. Therefore $|X| = |G|^{p-1}$.

As $p \,\Big|\, |G| \quad$ we get $\quad p \,\Big|\, |X|$.

(ii) Let $\sigma \in S_p$ given by $\sigma = (1,2,\dots,p)$.

Define $H = \langle\sigma\rangle$. Then H is subgroup in S_p.

Define $f : X \times H \longrightarrow X$ by

$$f\left((g_1, g_2, \dots, g_p),\ \sigma^k\right) = \left(g_{\sigma^k(1)}, g_{\sigma^k(2)}, \dots, g_{\sigma^k(p)}\right)$$

Then

(i) $f\left((g_1, g_2, \dots, g_p),\ i\right) = \left(g_{i(1)}, g_{i(2)}, \dots, g_{i(p)}\right)$

$$= \left(g_1, g_2, \dots, g_p\right)$$

(ii) $f\left((g_1, g_2, \dots, g_p),\ \sigma^k \circ \sigma^l\right) = \left(g_{\sigma^k\circ\sigma^l(1)}, g_{\sigma^k\circ\sigma^l(2)}, \dots, g_{\sigma^k\circ\sigma^l(p)}\right)$

$$= \left(g_{\sigma^l[\sigma^k(1)]}, g_{\sigma^l[\sigma^k(2)]}, \dots, g_{\sigma^l[\sigma^k(p)]}\right)$$

$$= f\left[f\left((g_1, g_2, \dots, g_p),\ \sigma^l\right),\ \sigma^k\right]$$

Hence, from (1) and (2) we get X is a H – set.

Hence, by theorem 2.3, we get,

$$|X| \equiv |X_H| \pmod p$$

Since $O(H) = p$.

(iii) As $p \,\big|\, |X|$ $\quad (\because \ |X| = |G|^{p-1})$

and $p \,\big|\, |X| - |X_H|$ we must have $p \,\big|\, |X_H|$.

Now $X_H = \left\{(g_1, g_2, \dots, g_p) \,/\, f\left((g_1, g_2, \dots, g_p),\ \sigma^l\right) = (g_1, g_2, \dots, g_p) \ \ \forall \ \ \sigma^l \in H\right\}$

Hence $(g_1, g_2, \dots, g_p) \in X_H$

$\Longrightarrow \quad f[(g_1, g_2, \dots, g_p),\ \sigma] = (g_1, g_2, \dots, g_p)$ as $\sigma \in H$

$\Longrightarrow \quad (g_{\sigma(1)}, g_{\sigma(2)}, \dots, g_{\sigma(p)}) = (g_1, g_2, \dots, g_p)$

$\Longrightarrow \quad (g_2, g_3, \dots, g_1) = (g_1, g_2, \dots, g_p)$

But then $g_1 = g_2 = \cdots = g_p$.

This shows that an element of the type $(a, a, \dots, a) \in X_H$ i.e. $a^p = e$.

As $p \,\big|\, |X_H|$ we must have $|X_H| > 1$.

Hence, $\exists$ $a \in G$ such that $a \neq e$ and $(a, a, \dots, a) \in X_H$.

But then we have an element $a \in G,\ a \neq e$ such that $a^p = e$.

This completes the proof.

An immediate application of Cauchy's theorem is

Theorem 4.2.5 : Let G be a finite group and let p be any prime number. If $p \mid |G|$, then there exists a subgroup of order p in G.

Proof : By Cauchy's theorem, $\exists\ a \in G$ such that $a \neq e$ and $a^p = e$.

Define $H = \langle a \rangle$.

Then H will be the subgroup of G of order p.

4.3. p – Groups :

Definition 4.3.1 : A group G is a p – group if every element in G has order a power of the prime p. A subgroup of a group G is a p-subgroup of G if the subgroup is itself a p-group.

The characterization of p-groups is given in the following theorem.

Theorem 4.3.1 : Let G be a finite group. Then G is a p-group if and only if $|G|$ is a power of prime p.

Proof : <u>Only if part :</u>

Let G be a p-group. Hence order of each element in G is a power of p. Let q be a prime number different from p. If $q \mid |G|$, then by Cauchy's theorem, there exists an element $a \in G$ such that $O(a) = q$.

By assumption, $O(a) = p^k$ for some k.

Thus, $q = p^r$; which is impossible. Hence no prime number other than p will be a divisor of $|G|$.

Hence, $|G| = p^n$ for some n.

<u>If part :</u>

Let $|G| = p^n$ for some n.

For any $a \in G$, we know $O(a) \mid O(G)$.

Hence, $O(a) \mid p^n$ implies $O(a)$ must be p^k for some k.

Hence, G is a p – group.

Theorem 4.3.2 : Let G be a finite group. Let H be a p – subgroup of G. Then

$$(N[H] : H) \equiv (G : H) \bmod p$$

Proof : $N[H] = \{g \in G \ / \ gHg^{-1} = H\}$

We know that $N[H]$ is a subgroup of G containing H.

Let $\Re$ denote the set of all right cosets of H in G.

Define $f : \Re \times H \longrightarrow \Re$ by

$$f(H_x, h) = H_{xh}$$

Then, $\Re$ is a H – set (See example 4.1.2 (2)).

As H is a p – subgroup $|H| = p^n$, for some n

As $p \,\big|\, |H|$ we get

$$|\Re| \equiv |\Re_H| \ (\mathrm{mod}\ p), \qquad \text{(See theorem 4.2.3)}$$

But $|\Re| = (G : H)$

Hence, $(G : H) = |\Re_H| \ (\mathrm{mod}\ p)$ . . . (1)

Now, $\Re_H = \{H_x \in \Re \ / \ f(H_x, h) = H_x \ \text{ for each } \ h \in H\}$

$= \{H_x \in \Re \ / \ H_{xh} = H_x \ \text{ for each } \ h \in H\}$

$= \{H_x \in \Re \ / \ x^{-1}hx \in H \ \text{ for each } \ h \in H\}$

$= \left\{H_x \in \Re - x^{-1}Hx = H\right\}$

$= \{H_x \in \Re \ / \ x \in N[H]\}$

= the set of all right cosets of H in $N[H]$.

Hence, $|\Re_H| = (N[H] : H)$ . . . (2)

From (1) and (2), we get,

$$(G : H) \equiv (N[H] : H) \ (\mathrm{mod}\ p)$$

Corollary 4.3.3 : Let H be a p – subgroup of a group G. If $p \,\big|\, (G : H)$, then $N[H] \neq H$.

Proof : By theorem 4.3.2, we get

$$(G : H) \equiv (N[H] : H) \ (\mathrm{mod}\ p)$$

As $p \,\big|\, (G : H)$ we get $p \,\big|\, (N[H] : H)$.

Hence, $(N[H] : H) \neq 1$.

i.e. $H \neq N[H]$

4.4. Sylow Theorems :

- ***First Sylow Theorem :***

Theorem 4.4.1 : Let G be a finite group with $|G| = p^n \cdot m$ where p is a prime number and $p \nmid m$. Then

(i) G contains a subgroup of order p^i for each i, $1 \leq i \leq n$.

(ii) Every subgroup of order p^i is a normal subgroup of a subgroup of order p^{i+1} for

$1 \leq i \leq n-1.$

Proof :

(i) By Cauchy's theorem (see theorem 4.2.4) there exists a subgroup of order p in G as $p \,\Big|\, |G|$. Assume that there exists a subgroup of order p^i for each $i < n$.

Let H be a subgroup of order p^i.

Now $\quad (G : H) = \frac{O(G)}{O(H)} = \frac{p^n \cdot m}{p^i} = p^{n-i} \cdot m.$

As $i < n$ we get $p \,\Big|\, (G : H)$.

Hence, by theorem 4.3.2,

$$(G{:}H) \equiv (N[H] : H) \ (\text{mod}\, p)$$

As $p \,\Big|\, (G{:}H)$ we get $\quad p \,\Big|\, (N[H] : H)$.

Hence, $p \,\Big|\, \frac{|N[H]|}{|H|}$ $\quad$ i.e. $\quad p \,\Big|\, O\left[\frac{N[H]}{H}\right]$.

Hence, by Cauchy's theorem, $\frac{N[H]}{H}$ contains a subgroup of order p. Let it be k.

Let $\gamma : N[H] \longrightarrow \frac{N[H]}{H}$ be the canonical mapping.

Then γ is an onto homomorphism.

$\gamma^{-1}(k) = \{x \in N[H] \,/\, \gamma(x) \in k\}$ is the subgroup of $N[H]$ of order p^{i+1}.

This shows that there exists a subgroup of order p^{i+1} in G.

By induction on n, the result follows.

(ii) By the construction explained in (i) we get,

$$H < \gamma^{-1}(k) \leq N[H]$$

where $O(H) = p^i$ and $O\big(\gamma^{-1}(k)\big) = p^{i+1}$.

As $H \lhd N[H]$. We must get $H \lhd \gamma^{-1}(k)$.

This shows that the subgroup of order p^i is normal in a subgroup of a subgroup of order p^{i+1}.

Example 4.4.2 : If $O(G) = 2^4 \cdot 3 \cdot 7$ then G contains subgroup H_1, H_2, H_3 and H_4 such that $O(H_1) = 2, O(H_2) = 2^2, O(H_3) = 2^3$ and $O(H_4) = 2^4$ and $H_1 \lhd H_2, H_2 \lhd H_3, H_3 \lhd H_4$. There also exists a subgroup K of order 3 and a subgroup T of order 7 in G.

Definition 4.4.3 : A Sylow p – subgroup of a group G is a maximal p – subgroup of G.

Example 4.4.4 : In example 4.4.2,

H_4 is a Sylow 2 – subgroup.

K is a Sylow 3 – subgroup.

T is a Sylow 7 – subgroup.

Remarks 4.4.5 :

(i) If $|G| = p^n \cdot m$ and $p \nmid m$ then the subgroup of order p^n will be a Sylow p – subgroup in G.

(ii) If P is a Sylow p – subgroup in G, then $O(g^{-1}Pg) = O(P)$ will imply $g^{-1}Pg$ is also Sylow p – subgroup of G, for any $g \in G$. i. e. any conjugate of a Sylow p – subgroup of G is also a Sylow p – subgroup of G.

Conjugate of a Sylow p – subgroup is a Sylow p – subgroup in a finite group G. But any two Sylow p – subgroups of G must be conjugates of each other. This we prove in the following theorem.

- ***Second Sylow Theorem :***

Theorem 4.4.6 : Let G be a finite group with $|G| = p^n \cdot m$ where p is a prime number and $p \nmid m$. Let P_1 and P_2 be any two Sylow p – subgroups of G. Then P_1 and P_2 are conjugate subgroups of G.

Proof : Let $\mathfrak{R}$ denote the set of all right cosets of P_1 in G.

Define $f : \mathfrak{R} \times P_2 \longrightarrow \mathfrak{R}$ by

$$f(P_{1x}, y) = P_1 xy.$$

Then

(i) $f(P_{1x}, e) = P_1 xe = P_1 x$

and (ii) $f(P_{1x}, gh) = P_1 xgh = P_1(xg)h = f(f(P_{1x}, g),\ h)$ for $g, h \in P_2$.

Hence $\mathfrak{R}$ is a P_2 set.

As P_2 is a Sylow p – subgroup, $p \,\Big|\, |p_2|$.

Hence, by theorem 4.2.3

$$|\mathfrak{R}| \equiv \left|\mathfrak{R}_{P_2}\right| (\text{mod}\, p) \qquad \ldots (1)$$

Now $\mathfrak{R}$ = the set of all right cosets of P_1 in G.

Hence, $|\mathfrak{R}| = (G : P_1)$.

Therefore, $|\mathfrak{R}| = (G : P_1) = \frac{|G|}{|P_1|} = \frac{p^n \cdot m}{p^n} = m$ and $p \nmid m$.

Hence, $\left|\Re_{P_2}\right| \neq 0$ … by (1)

Hence $\left|\Re_{P_2}\right| \geq 1$ … (2)

Now, $\Re_{P_2} = \{P_1x \in \Re \,/\, f(P_1x,\ g) = P_1x \quad \text{for all } g \in P_2\}$

$= \{P_1x \in \Re \,/\, P_1xg = P_1x \quad \text{for all } g \in P_2\}$

$= \{P_1x \in \Re \,/\, x^{-1}gx \in P_1 \quad \text{for all } g \in P_2\}$

$= \{P_1x \in \Re \,/\, x^{-1}P_2x \subseteq P_1\}$

$= \{P_1x \in \Re / x^{-1}P_2x = P_1\}$ (As $|x^{-1}P_2x| = |P_2| = |P_1| = p^n$)

By (2), $\left|\Re_{P_2}\right| \geq 1.$

Hence, there exists $x \in G$ such that $x^{-1}P_2x = P_1$. Hence the proof.

The existence and the nature of Sylow p – subgroups is proved in the First Sylow theorem and the Second Sylow theorem respectively. The third Sylow theorem deals with the number of Sylow p – subgroups in a group G.

- ***Third Sylow Theorem :***

Theorem 4.4.7 : Let G be a finite group and $p/|G|$ (p is any prime number).

Let r = number of Sylow p – subgroups in G. Then

(i) $r \equiv 1(\text{mod } p)$ (ii) $r \,\Big|\, |G|$

Proof :

(i) Let r = number of Sylow p – subgroups in G.

Hence $r \neq 0$ (by First Sylow theorem)

Let $\mathcal{L}$ denote the set of all Sylow p – subgroups in G. Then $|\mathcal{L}| = r$.

Fix up any Sylow p – subgroup say P in G. Then for any $T \in \mathcal{L}$ we have

$T = g^{-1}Pg$ for some $g \in G$ (by Second Sylow theorem)

Define $f: \mathcal{L} \times P \longrightarrow \mathcal{L}$ by

$f(T,\ x) = x^{-1}Tx$ for any $g \in G$. (See remark 4.4.5 (2))

Now,

$f(T,\ e) = e^{-1}Te = T$ and

$f(T,\ xy) = (xy)^{-1}T(xy)$

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

$\Longrightarrow$ $f(T,\ xy) = f[f(T,x),y]$, for all $x,\ y \in P$

Hence, $\mathcal{L}$ is a P – set.

As P is a Sylow p – subgroup, $p/O(P)$.

Hence, by theorem 2.3, we have,

$$|\mathcal{L}| \equiv |\mathcal{L}_P| \pmod{p} \qquad \ldots (1)$$

Consider the set $\mathcal{L}_P$.

$\mathcal{L}_P = \{T \in \mathcal{L} \,/\, f(T,\ x) = T \quad \text{for all } x \in P\}$

$\quad = \{T \in \mathcal{L} \,/\, x^{-1}Tx = T \quad \text{for all } x \in P\}$

$\quad = \{T \in \mathcal{L} \,/\, x \in N[T] \quad \text{for all } x \in P\}$

Thus, $T \in \mathcal{L}_P$ iff $P \subseteq N[T]$.

Thus, $T \in \mathcal{L}_P$ iff $P \leq N[T]$.

Thus, P and T both are subgroup of $N[T]$ and hence they are p – subgroups of $N[T]$.

By Second Sylow theorem, P and T are conjugates.

Hence, for some $g \in N[T]$, $g^{-1}Tg = P$.

As $T \trianglelefteq N[T]$, $g^{-1}Tg = T$. Hence $P = T$.

Thus, $T \in \mathcal{L}_P$ iff $P = T$. This shows that $\mathcal{L}_P = \{P\}$.

Hence $\quad |\mathcal{L}_P| = 1 \qquad \ldots (2)$

From (1) and (2) we get

$$|\mathcal{L}| \equiv 1 \pmod{p}$$

i.e. $\quad r \equiv 1 \pmod{p}$

(ii) To prove $r \,\Big|\, |G|$.

Let $\mathcal{L}$ denote the set of all Sylow p – subgroups of G. As in (i) we can prove $\mathcal{L}$ is a G – set under the action $f : \mathcal{L} \times G \longrightarrow \mathcal{L}$ defined by

$$f(T,\ g) = g^{-1}Tg$$

By second Sylow theorem, elements of $\mathcal{L}$ are conjugates of each other.

Hence, $\mathcal{L}$ contains only one orbit.

Therefore

$|\mathcal{L}| = |$ orbit of P $|$ $\qquad (P \in \mathcal{L})$

$\Longrightarrow \quad |\mathcal{L}| = |\, P\mathcal{L} \,|$ $\qquad$ (orbit of $P = P\mathcal{L}$ under G)

$\Longrightarrow \quad r = (G : G_p)$ $\qquad$ (theorem 1.3)

But $\quad (G : G_p) \,\Big|\, |G|$ and hence $r \,\Big|\, |G|$.

Examples 4.4.8 :

(**1**) A Sylow 3 – subgroup of a group of order 12 has order 3 as $12 = 2^2 \times 3^1$.

(2) A Sylow 3 – subgroup of a group of order 54 has order $3^3 = 27$ as $54 = 2 \times 27 = 2 \times 3^3$.

(3) By third Sylow theorem, a group of order 24 must have either 1 or 3 Sylow 2 – subgroups.

Let r = number of Sylow 3 – subgroups.

(i) $r \,\big|\, |G| \quad \Rightarrow \quad r/24 \quad \Rightarrow \quad r = 1, 2, 3, 4, 6, 8, 12, 24$

(ii) $r \equiv 1(\text{mod } 2) \quad \Rightarrow \quad 2 \,\big|\, r - 1 \quad \Rightarrow \quad r = 1,\ 3$

(4) A group of order 255 must have either 1 or 85 Sylow 3 - subgroups.

$255 = 3 \times 5 \times 17$

Let r = number of Sylow 3 – subgroups.

(i) $r \,\big|\, |G| \quad \Rightarrow \quad r \,\big|\, 255 \quad \Rightarrow \quad r = 1, 3, 5, 15, 17, 51, 85, 255$

(ii) $r \equiv 1(\text{mod } 3) \quad \Rightarrow \quad 3 \,\big|\, r - 1 \quad \Rightarrow \quad r = 1$ or 85

(5) $|G| = 45$. Show that G contains only one Sylow 3 – subgroups. Is G simple ?

Solution : $|G| = 45 = 3^2 \times 5$.

By 1st Sylow theorem G contains Sylow 3 – subgroups each of order $3^2 = q$.

Let r = number of Sylow 3 – subgroups in G.

By 3rd Sylow theorem,

$$r \,\big|\, |G| \qquad \text{and} \qquad r \equiv 1(\text{mod } 3)$$

Hence

(i) $r \,\big|\, |G| \quad \Rightarrow \quad r \,\big|\, 45 \quad \Rightarrow \quad r \in \{1, 3, 5, 9, 15, 45\}$

(ii) $r \equiv 1(\text{mod } 3) \quad \Rightarrow \quad r = 1$

This shows that there exists only one Sylow 3 – subgroups of order $3^2 = 9$ say H.

By Second Sylow theorem,

$$H = g^{-1}Hg \qquad \text{for any } g \in G$$

Hence, H is a proper normal subgroup of G.

Hence, G is not simple.

(6) Show that a group of order 255 is not simple.

Solution : Let G be a group of order 255.

$|G| = 255 \quad \Longrightarrow \quad |G| = 17 \times 5 \times 3 = 17 \times 15$ and $17 \nmid 15$.

Hence, By 1st Sylow theorem there exists Sylow 17 – subgroups in G each of order 17.

Let r = number of Sylow 17 – subgroups.

Then, by 3rd Sylow theorem,

$$r \,\Big|\, |G| \qquad \text{and} \qquad r \equiv 1 (\text{mod } 17)$$

Hence,

(i) $r \,\Big|\, |G| \quad \Longrightarrow \quad r \in \{1, 3, 5, 15, 17, 51, 85, 255\}$

(ii) $r \equiv 1(\text{mod } 17) \quad \Longrightarrow \quad r = 1$

Thus, there exists only one Sylow 17 – subgroups in G say H.

Then, by Second Sylow theorem, H must be normal in G.

As $|H| = 17$, H is a proper normal subgroup of G.

Hence, G is not simple.

(7) Show that no group of order 30 is simple.

Solution : Let G be a group with $|G| = 30 = 5 \times 3 \times 2$.

(i) Hence, By 1st Sylow theorem, G contains Sylow 5 – subgroups each of order 5.

Let r = number of Sylow 5 – subgroups of G.

Then, by 3rd Sylow theorem,

$$r \,\Big|\, |G| \qquad \text{and} \qquad r \equiv 1 (\text{mod } 5)$$

Hence,

(i) $r \,\Big|\, |G| = 30 \quad \Longrightarrow \quad r \in \{1, 2, 3, 5, 6, 10, 15, 30\}$

(ii) $r \equiv 1(\text{mod } 5) \quad \Longrightarrow \quad 5 \,\Big|\, r - 1$. Hence $r = 1$ or 6.

Suppose G contains six Sylow 5 – subgroups. Let they be H_1, H_2, H_3, H_4, H_5 and H_6 be distinct Sylow 5 – subgroups.

Then, $O(H_i) = 5 \quad \forall \quad i,\ 1 \le i \le 6.$

$H_i \cap H_j = \{e\}$ for $i \neq j$

[If $x \in H_i \cap H_j$ and if $x \neq e$, then $\langle x \rangle = H_i = H_j$; #]

Hence, each H_i contains four elements each of order 5. Hence, there exists $6 \times 4 = 24$ elements in G each of order 5.

(ii) By 1st Sylow theorem G contains Sylow 3 – subgroups each of order 3.

Let r = number of Sylow 3 – subgroups of G.

Then, by 3rd Sylow theorem,

$$r \,\Big|\, |G| \qquad \text{and} \qquad r \equiv 1 (\text{mod } 3)$$

Hence,

(i) $r \,\Big|\, |G| = 30 \quad \Rightarrow \quad r \in \{1, 2, 3, 5, 6, 10, 15, 30\}$

(ii) $r \equiv 1(\text{mod } 3) \quad \Rightarrow \quad 3 \,\Big|\, r - 1$. Hence $r = 1$ or 10.

Suppose G contains ten Sylow 3 – subgroups each of order 3. Let $K_1, K_2, \dots, K_{10}$ denote distinct Sylow 3 – subgroups of G. As in (i) we can prove that G contains 20 distinct elements each of order 3.

(iii)Thus, from (i) and (ii), if G contains six Sylow 5 – subgroups and ten Sylow 3 – subgroups then G must contain 24 + 20 = 44 distinct elements which is not true as $|G| = 30$.

Hence, G must contain either only one Sylow 5 – subgroup or only one Sylow 3–subgroup. Thus in either the case, G contains a proper normal subgroup by 2nd Sylow theorem.

Hence, G is not simple.

(8) No group of order 36 is simple.

Solution : Let G be a group with $|G| = 36$.

$|G| = 36 = 3^2 \times 2^2$ and $3 \nmid 4$.

By 1st Sylow theorem, G contains Sylow 3 – subgroups each of order 9.

Let r = number of Sylow 3 – subgroups of G.

Then, by 3rd Sylow theorem,

$$r \,\Big|\, |G| \qquad \text{and} \qquad r \equiv 1 (\text{mod } 3)$$

Hence,

(i) $r \,\Big|\, |G| = 36 \quad \Rightarrow \quad r \in \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

(ii) $r \equiv 1(\text{mod } 3) \quad \Rightarrow \quad 3 \,\Big|\, r - 1$. Hence $r = 1$ or 4.

Suppose G contains four Sylow 3 – subgroups each of order 9. Let H, K be any two distinct Sylow 3 – subgroups. Then $|H| = 9$ and $|K| = 9$.

We know that,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Hence, $HK \subseteq G$ implies $|H \cap K| = 3$.

[$H \cap K \leq H \quad \Rightarrow \quad O(H \cap K) \Big| O(H) \quad \Rightarrow \quad O(H \cap K) \Big| 9$

$\Rightarrow \quad O(H \cap K) \in \{1, 3, 9\}$

But $O(H \cap K) = 1 \quad \Rightarrow \quad |HK| = 81$; impossible.

and $O(H \cap K) = 9 \quad \Rightarrow \quad H = K$; which is not true.]

Consider the group $N[H \cap K]$.

As $3 \Big| O(H \cap K),\ H \cap K < N[H \cap K]$ and hence $|N[H \cap K]| \in \{18,\ 36\}$ as

$|N[H \cap K]| \Big| |G| = 36$.

If $N(H \cap K) = 18$ then index of $N(H \cap K)$ in G is 2 and then $N(H \cap K)$ is a proper normal subgroup G, proving that G is not simple.

If $|N(H \cap K)| = 36$, then $N[H \cap K] = G$.

In this case, $H \cap K$ will be a proper normal subgroup of G.

Hence, G is not simple, in either the case.

(9) Show that Sylow p-subgroups of a finite group G is unique if and only if it is normal.

Solution :

<u>Only if part :</u>

Let G has a unique Sylow p-subgroup say H.

To prove that $H \lhd G$.

H is a Sylow p-subgroup $\Rightarrow$ gHg^{-1} is also a Sylow subgroup of G. By uniqueness we get,

$$H = g^{-1}Hg \qquad \text{for all } g \in G.$$

Hence, H is normal in G.

<u>If part :</u>

Let H be a Sylow p-subgroup in a group of G.

Let H be normal. If K is another Sylow p-subgroup of G then, by 2nd Sylow theorem,

$$K = gHg^{-1} \qquad \text{for some } g \in G.$$

But H being normal,

$$g^{-1}Hg = \text{H}$$

Thus, $K = H$. This shows that H is the unique Sylow p-subgroup.

(10) Let $H \lhd G$ such that index of H in G is prime to p. (p is any prime number). Show that H contains every Sylow p-subgroup of G.

Solution : Let $|G| = p^n \cdot m,\ p \nmid m$. i.e. $(p, m) = 1$.

By data, index of H in G is prime to p.

$\therefore \quad \frac{|G|}{|H|}$ is prime to p.

$\therefore \quad \frac{p^n \cdot m}{|H|}$ is prime to p and $|H| \,\Big|\, p^n \cdot m$

Assume that $|H| = p^n \cdot q$ where $(p, q) = 1$.

As $|H| = p^n \cdot q$, H contains a Sylow p-subgroup say K.

Then $|K| = p^n$, hence we get K is also a Sylow p-subgroup of G. If T is another Sylow p-subgroup of G we get $T = g^{-1}Kg$ for some $g \in G$. Hence

$$T = g^{-1}Kg \subseteq g^{-1}Hg = H \qquad (\text{as } H \lhd G)$$

shows that $T \subseteq H$.

Thus, H contains all the Sylow p-subgroups of G.

(11) $|G| = 108$. Show that G contains a normal subgroup of order 27 or 9.

Solution : $|G| = 108 = 3^3 \times 2^2 = 3^3 \cdot 4$ and $3 \nmid 4$.

Hence, by Sylow first theorem, ∃ Sylow 3-subgroups each of order 27.

Let $r =$ number of Sylow 3-subgroups in G.

Then $r \,\Big|\, |G|$ and $r \equiv 1 (\text{mod } 3)$.

Hence, $r \in \{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$

$3 \,\Big|\, r - 1 \quad \Rightarrow \quad r = 1$ or 4.

<u>Case I :</u> $r = 1$.

Then G contains only one Sylow subgroup of order 27 which is normal. (by second Sylow theorem).

<u>Case II :</u> $r = 4$.

Then G contains four Sylow 3-subgroups of order 27.

Let H and K denote any two distinct Sylow 3-subgroups. Then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

will imply $\quad |HK| = \frac{27 \times 27}{|H \cap K|}$ i.e. $\frac{27 \times 27}{108} < |H \cap K|$.

Further,

$$H \cap K \leq G \qquad \Rightarrow |H \cap K| \Big| |G| \qquad \Rightarrow |H \cap K| \Big| 108.$$

Hence, $|H \cap K| = 9$ or 27.

But $\quad |H \cap K| = 27 \quad \Rightarrow \quad H = K$, which is not true.

Hence, $|H \cap K| = 9$.

Now consider $N[H \cap K]$.

$$(H \cap K) \lhd H \quad \text{and} \quad (H \cap K) \lhd K$$

as $\quad O(H \cap K) = 3^2 \quad$ and $\quad O(H) = 3^3$.

[Any subgroup of order p^{n-1} is normal in a subgroup of group of order p^n]

Hence, $H \subset N[H \cap K] \quad$ and $\quad K \subset N[H \cap K]$.

Hence, the normal subgroup HK is properly contained in $N[H \cap K]$.

But then $|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{27 \times 27}{9} = 81$.

Therefore, $|N[H \cap K]| > |HK| = 81$

Hence, $|N[H \cap K]| = 108$ as $|N[H \cap K]| \Big| |G|$ and $|N[H \cap K]| > 81$.

Thus, $N[H \cap K] = G$. But this shows that $H \cap K$ is normal in G.

Theorem 4.4.9 : Let G be a finite group with $|G| = pq$ where p and q are distinct primes and $p < q$.

(i) G contains a normal subgroup of order q.

(ii) G is not simple.

(iii) If $p \nmid q - 1$, then G is cyclic and abelian.

Proof :

(i) $|G| = pq, \ \ q \nmid p$.

Hence, by 1st Sylow theorem G contains Sylow q-subgroups of order q.

Let r = number of Sylow q-subgroups . Then $r \Big| |G|$ and $r \equiv 1 (\text{mod } q)$

Hence, $r \in \{1, q, p, pq\}$

$$q \Big| r - 1 \quad \Rightarrow \quad r = 1.$$

Thus, there exists only one Sylow q-subgroups of G.

As G contains only one Sylow q-subgroup say H then $O(H) = q$ and $H \trianglelefteq G$ by 2nd Sylow theorem.

(ii) As G contains a proper subgroup normal subgroup H, G is not simple.

(iii) $|G| = pq$ and $p \nmid q$, by 1st Sylow theorem G contains Sylow p-subgroup of order p.

Let r = number of Sylow p-subgroups.

Then $r \Big| |G|$ and $r \equiv 1(\text{mod } p)$ by 3rd Sylow theorem

Hence, $r \in \{1, p, q, pq\}$. As $p \mid r-1$ we get $r = 1$. ($\because$ $p \nmid q-1$ by data)

Thus, there exists only one Sylow p-subgroups in G of order p.

Let H denote the Sylow q-subgroup and K denote the Sylow p-subgroup of G.

Then

(i) $H \cap K = \{e\}$.

If $x \in H \cap K$ and if $x \neq e$ then $\quad x \in H \implies O(x) = q$

$x \in K \implies O(x) = p$.

As $p \neq q$ we must have $H \cap K = \{e\}$.

(ii) $H \vee K \supseteq H$ and $H \vee K \supseteq K \quad \implies \quad H \vee K = G$

[$\because$ $O(H \vee K) \Big| pq$, $O(H) \Big| O(H \vee K)$, $O(K) \Big| O(H \vee K) \implies O(H \vee K) = pq$]

Hence, $G \cong H \times K \cong Z_q \times Z_p$.

Hence, G is cyclic and abelian.

Example 4.4.10 : $|G| = 15 \implies G$ is abelian and not simple.

Solution : $|G| = 15 = 5 \cdot 3$. 5 and 3 are distinct primes and $3 \nmid 5-1$.

Hence, by theorem 4.4.9, G is abelian and not simple.

Example 4.4.11 : Let G be a finite group. Prove that $\left|\frac{G}{Z(G)}\right| \neq 77$.

Solution: Assume that $\left|\frac{G}{Z(G)}\right| = 77$.

$\implies \quad \left|\frac{G}{Z(G)}\right| = 11 \cdot 7 \quad$ and $\quad 7 \nmid 11 - 1$.

Hence, by theorem, If $O(G) = p \cdot q$, where p, q are prime numbers such that $p \nmid q-1$ then G is cyclic, $\frac{G}{Z(G)}$ is cyclic.

But $\frac{G}{Z(G)}$ is cyclic $\quad \implies \quad$ G is abelian

$\implies \quad Z(G) = G$

$\implies \quad \left|\frac{G}{Z(G)}\right| = 1$

$\implies$ a contradiction.

Hence $\left|\frac{G}{Z(G)}\right| \neq 77$.

Example 4.12 : Prove that $\left|\frac{G}{Z(G)}\right| \neq 33$ for any finite group.

Solution : Let $\left|\frac{G}{Z(G)}\right| = 33 = 11 \cdot 3$ and $3 \nmid (11 - 1 = 10)$.

As $3 \nmid (11 - 1)$ by theorem 4.9, $\frac{G}{Z(G)}$ is abelian and Cyclic.

Hence, as $\frac{G}{Z(G)}$ is Cyclic, G is abelian.

But then $Z(G) = G$ and in this case $\left|\frac{G}{Z(G)}\right| = 1$, a contradiction.

Hence, $\left|\frac{G}{Z(G)}\right| \neq 33$ for any finite group G.

Example 4.4.13 : $|G| = 255 \implies G$ is abelian and not simple.

Solution : $|G| = 255 = 17 \times 5 \times 3 = 17 \times 15$ and $17 \nmid 15$.

(i) By 1st Sylow theorem, G contains Sylow 17 – subgroups each of order 17.

Let r = number of Sylow 17 – subgroups of G.

Then by 3rd Sylow theorem,

$$r \,\Big|\, |G| \quad \text{and} \quad r \equiv 1 (\text{mod } 17)$$

Hence, $r \in \{1, 3, 5, 15, 17, 51, 85, 255\}$.

$$17 \,\Big|\, r - 1 \implies r = 1.$$

Thus, there exists only one Sylow 17-subgroup in G of order 17.

Hence, by 2nd Sylow theorem, G is not simple.

Let us denote by H the Sylow 17 – subgroups of G. $\frac{G}{H}$ is defined.

$$\left|\frac{G}{H}\right| = \frac{|G|}{|H|} = \frac{255}{17} = 15.$$

Hence $\frac{G}{H}$ is abelian. (See theorem 4.4.10)

Hence, $G' \subseteq H$ (See theorem 2.1.5(iii))

Hence, $G' \leq H$.

By Lagrange's theorem, $|G'| \,\Big|\, |H| = 17 \implies |G'| = 1$ or 17.

(ii) By 1st Sylow theorem, G contains Sylow 3 – subgroups each of order 3.

Let r = number of Sylow 3 – subgroups in G.

By 3rd Sylow theorem,

$$r \,\Big|\, |G| \qquad \text{and} \qquad r \equiv 1 (\text{mod } 3)$$

Hence, $r = 1$ or 85.

(iii)By 1st Sylow theorem, G contains Sylow 5 – subgroups each of order 5.

Let r = number of Sylow 5 – subgroups in G.

By 3rd Sylow theorem,

$$r \,\Big|\, |G| \qquad \text{and} \qquad r \equiv 1 (\text{mod } 5)$$

Hence, $r = 1$ or 51.

(iv) $K \trianglelefteq G$ and hence $\frac{G}{K}$ is defined.

Now, if K is Sylow 3-subgroup then

$$\left|\frac{G}{K}\right| = \frac{|G|}{|K|} = \frac{17 \times 5 \times 3}{3} = 17 \times 5.$$

and if K is Sylow 5-subgroup then

$$\left|\frac{G}{K}\right| = \frac{|G|}{|K|} = \frac{17 \times 5 \times 3}{5} = 17 \times 3.$$

Thus, in either the case by theorem 4.4.9 $\frac{G}{K}$ is abelian.

Hence, $G' \subseteq K$.

Hence, $G' \leq K$ and $|G'| \,\Big|\, |K|$.

If K is Sylow 5-subgroup then $|G'| = 1$ or 5

and if K is Sylow 3-subgroup then $|G'| = 1$ or 3.

As $G' \trianglelefteq G$ we get $|G'| \in \{1, 3, 5, 17\}$.

Hence, $|G'| = 1$. i.e. $G' = \{e\}$.

But then G must be an abelian. ($|G'| = 1$ iff G is abelian).

Thus, the group of order 255 is abelian and not simple.

Example 4.4.14: Find all the Sylow 3-subgroups of S_4. Verify that they are all conjugate.

Solution : Let $G = S_4$. Then $|G| = 24 = 2^3 \times 3$.

By 1st Sylow theorem, G contains Sylow 3-subgroups of order 3.

Let r = number of Sylow 3-subgroups.

Then, by 3rd Sylow theorem,

$$r \,\Big|\, |G| \quad \text{and} \quad r \equiv 1 (\text{mod } 3)$$

$$r \,\Big|\, |G| = r \,\Big|\, 24 \quad \Longrightarrow \quad r \in \{1, 2, 3, 4, 6, 8, 12, 24\}$$

$$r \equiv 1 (\text{mod } 3) \quad \Longrightarrow \quad 3 \,\Big|\, r - 1. \text{ Hence } r = 1 \text{ or } 4.$$

Case I : $r = 1$.

Then G contains only one Sylow 3-subgroup. It must be normal by 2nd Sylow theorem.

Case II : $r = 4$.

Let G contains four Sylow 3-subgroups each of order 3 Hence each must be a cyclic group generated by the 3-cycles

(1, 2, 3), (1, 2, 4), (1, 3, 4) and (2, 4, 3)

These cyclic groups are conjugate to each other and they are distinct.

Example 4.4.15: $|G| = 2p$, p is prime, show that either G is cyclic or G is generated by $\{a, b\}$ with the relation $a^p = e = b^2$ and $bab = a^{-1}$.

Solution : $|G| = 2 \times p$ and $p \nmid 2$. Hence by 1st Sylow theorem, G contains Sylow p-subgroups, each of order p.

Let $r =$ number of Sylow p-subgroups.

Then by 3rd Sylow theorem,

$$r \,\Big|\, |G| \quad \text{and} \quad r \equiv 1 (\text{mod } p)$$

$$r \,\Big|\, |G| \quad \Longrightarrow \quad r \in \{1, 2, p, 2p\}$$

$$r \equiv 1 (\text{mod } p) \quad \Longrightarrow \quad p \,\Big|\, r - 1. \text{ Hence } r = 1.$$

Thus, G contains only one Sylow p-subgroup say H.

$$|H| = p \quad \Longrightarrow \quad H \text{ is cyclic.}$$

Let $H = \langle a \rangle$. Then $\left|\frac{G}{H}\right| = \frac{|G|}{|H|} = \frac{2p}{p} = 2$.

Hence, $\frac{G}{H}$ is Cyclic group of order 2.

$$O(H) = p \quad \Longrightarrow \quad H \subset G.$$

Select $b \in G$ such that $b \notin H$. Then $G = \{e, a, \dots, a^{p-1}, b, ba, \dots, ba^{p-1}\}$.

As $b \in G$, $O(b) \,\Big|\, O(G)$ and hence $O(b) = 2$ or p.

If $O(b) = p$, then $b \in \langle a \rangle = H$ as H is the only subgroup of G of order p; which is not true. Hence, $O(b) \neq p$.

Hence, $O(b) = 2$. Then $b^2 = e$.

Thus, $a^p = e = b^2$ . . . (1)

Now, consider the element bab^{-1}. As $\langle a \rangle$ is normal in G, $bab^{-1} \in H = \langle a \rangle$.

Thus, $bab^{-1} = a^k \implies b^{-1}(bab^{-1})b = b^{-1}a^k b$

$\implies (b^{-1}b)\, a\, (b^{-1}b) = b^{-1}a^k b$

$\implies e\, a\, e = b^{-1}a^k b$

$\implies a = b^{-1}a^k b$

$\implies a = (b^{-1}a\, b)^k$

$\implies a = (a^k)^k$

$\implies a^{k^2-1} = e$

$\implies p \mid k^2 - 1$

$\implies p \mid (k-1)(k+1)$

$\implies (k-1) = p$ or $(k+1) = p$

Case I : $p = k - 1 \implies k = 1 + p$

$bab^{-1} = a^k = a^{1+p} = a^1 \cdot a^p = a^1 \cdot e = a$

Case II : $p = k + 1 \implies k = p - 1$

$bab^{-1} = a^k = a^{p-1} = a^p \cdot a^{-1} = e \cdot a^{-1} = a^{-1}$

Thus, $bab^{-1} = a$ or $bab^{-1} = a^{-1}$

Thus, $ba = ab$ or $bab = a^{-1}$ $(\because \ b^2 = e \implies b^{-1} = b)$.

Thus, if $p = k - 1$ i.e. $k = 1 + p$, G is a non abelian group generated by $\{a, b\}$ with the relations $a^p = e = b^2$ and $bab = a^{-1}$.

If $p = k + 1$ then G is abelian and $O(ab) = 2p$. i.e. G is cyclic of order $2p$.

Example 4.4.16 : $O(G) = p^2$, p is a prime. Show that G is cyclic or G is isomorphic to direct product of two cyclic groups each of order p.

Solution : $O(G) = p^2 \implies G$ is abelian.

If G is cyclic then we are through.

Let G be not cyclic.

As $p \mid O(G)$, by Cauchy's theorem $\exists\ a \in G$ such that $O(a) = p$. Let $H = \langle a \rangle$.

Then $O(H) = p$. Hence, $H \neq G$.

Select $b \in G$ such that $b \notin H$. As $O(b) \mid O(G)$ we get, $O(b) = 1, p, p^2$.

As $b \notin H$ we get, $b \neq e$.

Hence $O(b) \neq 1$.

If $O(b) = p^2$, then G will be cyclic, not true.

Hence, $O(b) = p$. Let $K = \langle b \rangle$.

$$H \cap K \leq H \qquad \Longrightarrow \qquad O(H \cap K) \,\Big|\, O(H) = p.$$

Hence, $O(H \cap K) = 1$ or p.

If $O(H \cap K) = p$ will imply $H = K$, which is not true. Hence $O(H \cap K) = 1$.

Now, G is abelian $\Longrightarrow H \lhd G$ and $K \lhd G$. Hence $HK \lhd G$.

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{p \cdot p}{1} = p^2 = O(G) \qquad \text{(See theorem 1.2.6)}$$

But $HK = G$.

As H and K are normal subgroups of G with $H \cap K = \{e\}$ and $H \vee K = G$ we get $G \cong H \times K$. (see theorem 1.2.1)

This completes the proof.

Exercise

1. Show that a group of order 148 cannot be simple.
2. Show that a group of order 108 cannot be simple.
3 Show that a group of order 144 cannot be simple.

CHAPTER II : RING OF POLYNOMIALS

Unit 1 :

1.1 Ring of Polynomials R[x] :

Definition 1.1.1 : Let R be a ring. A polynomial $f(x)$ with coefficients in R and in an indeterminate x is an infinite formal sum

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

where, $a_i \in R$ and $a_i = 0$ for all but finite number of values of i. The a_i are called coefficients of $f(x)$. We simply write $f(x)$ as

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

when $a_{n+i} = 0$ for all $i \geq 1$.

Examples :

(i) $f(x) = x^2 + 2x + 5$ is a polynomial with coefficients in Z.

(ii) $f(x) = x^2 + 1$ is a polynomial with coefficients in Z_2.

(Here $f(x) = 1 \cdot x^2 + 0 \cdot x + 1$)

Definition 1.1.2: Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ be a polynomial with coefficients in a ring R. If there exists some $i > 0$ such that $a_i \neq 0$, then the largest value of such i is called the degree of the polynomial $f(x)$. If no such $i > 0$ exists, then we say that $f(x)$ is of zero degree.

Examples :

(i) The degree of the polynomial $f(x) = x^5 + 4x^4 + 3x^2 + 2x + 7$ with coefficients in Z is of degree 5.

(ii) $f(x) = \frac{2}{3} + 0 \cdot x + 0 \cdot x^2$. $f(x)$ is a polynomial with coefficients in Q. The degree of $f(x)$ is zero.

Definition 1.1.3: Let R be a ring and let $R[x]$ denote the set of polynomials with coefficients in R and in an indeterminate x. Let $f(x), g(x) \in R[x]$ where

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \qquad (a_i \in R)$$

and

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \qquad \left(b_j \in R\right)$$

We define $' + '$ and $' \cdot '$ of $f(x)$ and $g(x)$ as follows.

(i) $f(x) + g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n, \quad (m < n),$

where, $c_i = a_i + b_i, \ \forall \ i.$ [Here $b_{m+i} = 0$ for $i \geq 1$]

(ii) $f(x) \cdot g(x) = d_0 + d_1x + d_2x^2 + \cdots + d_{n+m}x^{n+m},$

where, $d_k = \sum_{i+j=k} a_ib_j \ , \ (1 \leq i \leq n, \ 1 \leq j \leq m)$

i.e. $d_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0.$

Obviously,

$$f(x) + g(x) \in R[x] \qquad \text{and} \qquad f(x) \cdot g(x) \in R[x].$$

Remark 1.1.4 : $\langle R[x], \ +, \ \cdot \rangle$ is a ring where $' + '$ and $' \cdot '$ are as defined in (i) and (ii) in the definition 1.1.3. This ring is called the polynomial ring over the ring R.

If R is a ring and x and y are two indeterminates, then we can form the ring $(R[x])(y)$, that is, the ring of polynomials in y, with coefficients that are polynomials in x.

As $(R[x])(y) \cong (R[y])(x)$, we denote this ring by $R[x, y]$, the ring of polynomials in two variables x and y with coefficients in R. We can similarly define the ring $R[x_1, x_2, \ldots, x_n]$ of polynomials in the $'n'$ indeterminate x_i with coefficients in R.

1.2 Properties of R[x] :

Theorem 1.2.1:

Let R be a ring. Then R is a sub-ring of the ring of polynomials $R[x]$.

Proof : Let $a \in R$, we write

$$f(x) = a + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^n \qquad (n \text{ finite})$$

Then $f(x) \in R[x]$ and is called a constant polynomial over the ring R.

Thus, if $a, b \in R$, then a, b are constant polynomials in $R[x]$ and as members of $R[x]$, their addition $a + b$ and multiplication $a \cdot b$ are again the constant polynomials in $R[x]$.

Hence, R is a subring of $R[x]$.

Theorem 1.2.2 : $R[x]$ is a ring of polynomials over a ring R. $R[x]$ is commutative iff R is commutative.

Proof : **<u>Only if part :</u>**

Let $R[x]$ be commutative. As, sub-ring of a commutative ring is commutative, we get R is commutative.

<u>If part :</u> Let R be commutative.

Let $f(x), g(x) \in R[x]$,

where, $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \qquad (a_i \in R)$

and $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m, \qquad \left(b_j \in R\right).$

Then,

$$f(x) \cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\, x + \cdots + \left[\sum_{i+j=k} a_i b_j\right] x^k + \cdots + a_n b_m x^{n+m}.$$

As R is commutative,

$a_0 b_0 = b_0 a_0$, $a_0 b_1 + a_1 b_0 = b_0 a_1 + b_1 a_0$, … , $\sum_{i+j=k} a_i b_j = \sum_{j+i=k} b_j a_i$, …,

$a_{1n} b_m = b_m a_n.$

Hence,

$$f(x) \cdot g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \cdots + \left[\sum_{i+j=k} a_i b_j\right] x^k + \cdots + a_n b_m x^{n+m}$$

$$= b_0 a_0 + (b_0 a_1 + b_1 a_0) x + \cdots + \left[\sum_{j+i=k} b_j a_i\right] x^k + \cdots + b_m a_n x^{n+m}$$

$$= g(x) \cdot f(x)$$

This shows that $R[x]$ is commutative.

Theorem 1.2.3 : Let R be a ring. $R[x]$ has unity iff R has unity.

Proof :

Only if part :

Let $R[x]$ be a ring with unity.

Define $\psi : R[x] \longrightarrow R$ by

$$\psi\, [a_0 + a_1x + a_2x^2 + \cdots + a_nx^n] = a_0$$

is an onto homomorphism, we get R has unity. [Since homomorphic image of a ring with unity contains the unity.]

If part :

Let the ring R contain the unity element say 1.

Then, consider the constant polynomial $1 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^n$ (n finite) will be the unity element of $R[x]$.

Definition 1.2.4 : Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a non zero polynomial in $R[x]$. We say that degree of $f(x)$ is n if $a_n \neq 0$ and $a_{n+i} = 0$ for $i \geq 1$.

We write, $\deg f(x) = n$.

Note that, the degree of a zero polynomial is not defined.

$\deg f(x) = 0$ if $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ with $a_i = 0$ for $i \geq 1$ and $a_0 \neq 0$.

i.e. $\deg f(x) = 0$ if $f(x)$ is a constant polynomial in $R[x]$.

Theorem 1.2.5 : Let R be a ring and $f(x), g(x)$ be non zero polynomials in $R[x]$, where $\deg f(x) = n$ and $\deg g(x) = m$. If $f(x) + g(x)$ and $f(x) \cdot g(x)$ are non zero polynomials in $R[x]$, then

(i) deg $[f(x) + g(x)] \leq \max(m, n)$

(ii) deg $[f(x) \cdot g(x)] \leq n + m$

(iii) If R is an integral domain, deg $[f(x) \cdot g(x)] = n + m$

Proof : Let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where $a_i \in R$ for $0 \leq i \leq n$ and $a_n \neq 0$ and $a_{n+i} = 0$, for each $i \geq 1$.

Let $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$

where $b_j \in R$ for $0 \leq j \leq m$ and $b_m \neq 0$ and $b_{m+i} = 0$ for each $i \geq 1$.

(i) $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + a_t x^t$, where $t = \max(n, m)$.

Hence, $\deg\ [f(x) + g(x)] \leq t = \max(m, n)$

(ii) $f(x) \cdot g(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + \cdots + (a_n b_m)x^{n+m}$.

This shows that

$$\deg\ [f(x) \cdot g(x)] \leq t = n + m$$

(iii) Let R be an integral domain.

Then, $\deg f(x) = n \quad \Longrightarrow \quad a_n \neq 0.$

$\deg g(x) = m \quad \Longrightarrow \quad b_m \neq 0.$

As R is an integral domain,

$$a_n \neq 0,\ b_m \neq 0 \quad \Longrightarrow \quad a_n b_m \neq 0.$$

Hence, $\deg\ [f(x) \cdot g(x)] = n + m.$ … See (ii)

Theorem 1.2.6 : R is an integral domain iff $R[x]$ is an integral domain.

Proof :

<u>Only if part :</u>

Let R be an integral domain.

To prove that $R[x]$ is an integral domain.

Let $f(x) \neq 0, g(x) \neq 0$ in $R[x]$ such that $f(x) \cdot g(x) = 0$.

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$

and $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$.

Let $f(x)$ and $g(x)$ both be constant polynomials.

Let $f(x) = a_0$ and $g(x) = b_0$.

Then, $f(x) \neq 0 \Longrightarrow a_n \neq 0$ and $g(x) \neq 0 \Longrightarrow b_0 \neq 0$.

As R is an integral domain, $a_0 b_0 \neq 0$.

i.e. $f(x) \cdot g(x) \neq 0$; which is not true.

Hence, one of $f(x), g(x)$ must be a non constant polynomial.

Let $f(x)$ be a non constant polynomial. Hence $\deg f(x) \geq 1$.

Hence, $\deg f(x) + \deg g(x) \geq 1$.

As R is an integral domain

$$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x) \geq 1$$

This leads to the contradiction as $f(x) \cdot g(x) = 0$.

Hence, $f(x) \cdot g(x) = 0 \quad \Longrightarrow \quad f(x) = 0$ or $g(x) = 0$.

i.e. $R[x]$ is an integral domain.

If part :

Let $R[x]$ be an integral domain. As the ring R is a subring of $R[x]$, R must be an integral domain.

Remark 1.2.7 : If F is a field then $F[x]$ may not be a field.

Proof : As F is a field, F is an integral domain. [Result : Every field is an integral domain.]

Hence, by theorem 1.2.6, $F[x]$ is an integral domain.

Consider the non-zero polynomial $f(x) \in F(x)$ given by

$$f(x) = 0 + 1 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^n.$$

We will prove that $f(x)$ has no multiplicative inverse in $F[x]$.

Let, if possible, $g(x) \in F[x]$ such that

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n$$

and $\quad f(x) \cdot g(x) =$ unity in $R[x]$.

$$= 1 + 0 \cdot x + 0 \cdot x^2 + \cdots + 0 \cdot x^n$$

Thus, by comparing the coefficients, we get

$$1 = 0; \quad \text{a contradiction.}$$

Hence, $f(x)$ does not have a multiplicative inverse in $F[x]$. Hence $F[x]$ is not a field.

Theorem 1.2.8 : Let F be a field then $F[x]$ is an Euclidian domain.

Proof :

(I) F is a field $\Rightarrow$ F is an integral domain.

$\Rightarrow$ $F[x]$ is an integral domain. … See theorem 1.2.6

(II) Let $f(x) \in F[x]$ be a non-zero polynomial. Define $d\big(f(x)\big) = \deg f(x)$.

Then, $d\big(f(x)\big)$ is a non-negative integer.

(i) For $f(x) \neq 0$ and $g(x) \neq 0$ in $F[x]$, we get

$$d\big(f(x) \cdot g(x)\big) = d\big(f(x)\big) + d\big(g(x)\big) \qquad \text{… See theorem 1.2.5}$$

Hence, $d\big(f(x)\big) \leq d\big(f(x) \cdot g(x)\big)$ as $d\big(g(x)\big) \geq 0$.

(ii) Let $f(x), g(x)$ be non zero polynomials in $F[x]$.

To prove that $\exists\ q(x), r(x) \in F[x]$ such that

$$f(x) = q(x) \cdot g(x) + r(x)$$

where $\quad r(x) = 0 \quad$ or $\quad d\big(r(x)\big) < d\big(g(x)\big)$.

Case I : $d(f(x)) < d(g(x))$. Then $f(x) = 0 \cdot g(x) + f(x)$

and the result follows in this case.

Case II : $d(g(x)) < d(f(x))$,

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, ($a_i \in F$ and $a_n \neq 0$)

and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$, ($b_i \in F$ and $b_m \neq 0$)

$d(g(x)) < d(f(x)) \quad \Rightarrow \quad m < n$.

Define $p(x) = f(x) - [a_n b_m^{-1} x^{n-m}]\, g(x)$.

Hence,

$$p(x) = [a_0 + a_1 x + \cdots + a_n x^n] - [b_0 + b_1 x + \cdots + b_m x^m]\ [a_n b_m^{-1} x^{n-m}]$$

shows that the coefficient of x^n in $p(x)$ is $a_n - (a_n b_m^{-1} \cdot b_m) = a_n - a_n = 0$.

Hence, $p(x) =$ zero polynomial or $d(p(x)) < \deg f(x) = n$.

Subcase I : $p(x)$ is a zero polynomial.

Then, $p(x) = f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$ will imply $0 = f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x)$.

Hence, $f(x) = a_n b_m^{-1} x^{n-m} \cdot g(x) + 0$.

Taking $q(x) = a_n b_m^{-1} x^{n-1}$ and $r(x) = 0$, the result follows.

Subcase II : $p_1(x) \neq 0$ and $\deg p(x) < \deg g(x)$.

Assume that the result is true for all the non zero polynomials in $F[x]$ of degree less than the degree of $g(x) = m$.

Then, by this assumption,

$$p(x) = q_1(x) \cdot g(x) + r(x),$$

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Hence, $f(x) - a_n b_m^{-1} x^{n-m} \cdot g(x) = q_1(x) \cdot g(x) + r(x)$.

Thus, $f(x) = [a_n b_m^{-1} x^{n-m} + q_1(x)]\, g(x) + r(x)$

i.e. $f(x) = q(x) \cdot g(x) + r(x)$

where $r(x) = 0$ or $\deg r(x) < \deg g(x)$

This shows that the result is true in this case also.

From (I) and (II), we get $F[x]$ is an Euclidean domain.

As every Euclidean domain is a principal ideal domain we get,

Corollary 1.2.9: For a field F, $F[x]$ is a P. I. D.

1.3 Division Algorithm in F[x]:

Theorem 1.3.1 : Let F be a field. Let

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

and $$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

be two polynomials in $F[x]$ with $a_n \neq 0$ and $b_m \neq 0$ with $m > 0$.

Then, there are two polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = q(x) \cdot g(x) + r(x) \qquad \text{with } \deg r(x) < \deg g(x).$$

These polynomials $q(x)$ and $r(x)$ are unique.

Proof : Define $S = \{f(x) - g(x) \cdot s(x) \,/\, s(x) \in F[x]\}$.

Then, $S \neq \phi$. (as $f(x) = f(x) - g(x) \cdot 0 \in S$)

Select $r(x) \in S$ such that $\deg r(x)$ is minimal.

Then, $r(x) \in S \quad \Rightarrow \quad r(x) = f(x) - g(x) \cdot q(x)$, for some $q(x) \in F[x]$.

Hence , $f(x) = g(x) \cdot q(x) + r(x)$.

If $r(x) = 0$ then we are through.

If $r(x) \neq 0$ then let

$$r(x) = c_tx^t + c_{t-1}x^{t-1} + \cdots + c_0 , \qquad \text{where } c_i \in F \text{ and } c_t \neq 0.$$

Hence, $\deg r(x) = t$.

We want to prove that $t < m$.

Let $t \nless m$. Then $t \geq m$.

Consider the following polynomial in $F[x]$.

$$f(x) - q(x) \cdot g(x) - [c_tb_m^{-1}]x^{t-m} \cdot g(x)$$

$$= f(x) - [q(x) + c_tb_m^{-1}x^{t-m}] \cdot g(x)$$

As $q(x) + c_tb_m^{-1}x^{t-m} \in F[x]$,

we get, $f(x) - q(x) \cdot g(x) - [c_tb_m^{-1}]x^{t-m} \cdot g(x) \in S$

But $f(x) - q(x) \cdot g(x) - c_tb_m^{-1}x^{t-m} \cdot g(x)$

$$= r(x) - c_tb_m^{-1}x^{t-m}[b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0]$$

$$= r(x) - [c_tx^t + \text{terms of lower degree}]$$

$$= [c_tx^t + c_{t-1}x^{t-1} + \cdots + c_0] - [c_tx^t + \text{terms of lower degree}]$$

Here, $f(x) - q(x) \cdot g(x) - c_tb_m^{-1}x^{t-m} \cdot g(x)$ is a polynomial of degree $< t = \deg r(x)$ and is a member of S.

This contradicts the fact that $r(x)$ is a polynomial in S of minimal degree.

Hence, our assumption that $t \geq m$ is wrong. Hence $t < m$. i.e. $\deg r(x) < \deg g(x)$.

Uniqueness :

Let $\quad f(x) = g(x) \cdot q_1(x) + r_1(x)$

and $\quad f(x) = g(x) \cdot q_2(x) + r_2(x)$

where $\quad \deg r_1(x) < m \quad$ and $\quad \deg r_2(x) < m,\ q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$.

Subtracting, we get,

$$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x) \qquad \ldots (1)$$

As $\quad \deg[r_2(x) - r_1(x)] < \deg g(x)$

we get (1) holds only when

$$q_1(x) - q_2(x) = 0 \qquad \Rightarrow \qquad q_1(x) = q_2(x).$$

and $\quad r_2(x) - r_1(x) = 0 \qquad \Rightarrow \qquad r_1(x) = r_2(x).$

This completes the proof.

1.3.2 Examples

Ex1 : Let $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = x^2 + 2x - 3$ be in $Z_7[x]$. Find $q(x)$ and $r(x)$ in $Z_7[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$ with $\deg r(x) < 2$.

Solution : Let $\quad f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$

and $\quad g(x) = x^2 + 2x - 3$

be in $Z_7[x]$.

g(x)	f(x)	q(x)
x^2+2x-3	$x^6+3x^5+0\cdot x^4+0\cdot x^3+4x^2-3x+2$	$x^4+x^3+x^2+x+5$
	$\underset{-}{x^6}\ \underset{-}{+}2x^5\ \underset{+}{-}3x^4$	
	$x^5+3x^4+0\cdot x^3$	
	$\underset{-}{x^5}\ \underset{-}{+}2x^4\ \underset{+}{-}3x^3$	
	$x^4+3x^3+4x^2$	
	$\underset{-}{x^4}\ \underset{-}{+}2x^3\ \underset{+}{-}3x^2$	
	$x^3+0\cdot x^2-3x$	
	$\underset{-}{x^3}\ \underset{-}{+}2x^2\ \underset{+}{-}3x$	
	$5x^2+0\cdot x+2$	
	$\underset{-}{5x^2}\ \underset{-}{+}3x\ \underset{+}{-}1$	
	$r(x)=4x+3$	

Thus, $\quad f(x) = g(x) \cdot q(x) + r(x)$

where $\quad q(x) = x^4 + x^3 + x^2 + x + 5$

$\qquad = x^4 + x^3 + x^2 + x - 2 \qquad \ldots \; (5 = -2 \text{ in } Z_7).$

and $\quad r(x) = 4x + 3$

Ex 2 : Let $f(x) = x^5 + x^3 + x$ and $g(x) = x^4 + 2x^3 + 2x$ in $Z_3[x]$. Find $q(x)$ and $r(x)$ in $Z_3[x]$ such that $f(x) = g(x) \cdot q(x) + r(x)$ with $\deg r(x) < 4$.

Solution :

g(x)	*f(x)*	*q(x)*
$x^4 + 2x^3 + 0 \cdot x^2 + 2x + 0$	$x^5 + 0 \cdot x^4 + x^3 + 0 \cdot x^2 + x + 0$	$x + 1$
	$\underline{-x^5 \pm 2 \cdot x^4 \pm 0 \cdot x^3 \pm 2 \cdot x^2 \pm 0 \cdot x}$	
	$x^4 + x^3 + x^2 + x + 0$	
	$\underline{-x^4 \pm 2x^3 \pm 0 \cdot x^2 \pm 2 \cdot x \pm 0}$	
	$r(x) = 2x^3 + x^2 + 2x$	

Thus, $\quad f(x) = g(x) \cdot q(x) + r(x)$,

where $\quad q(x) = x + 1$, $r(x) = 2x^3 + x^2 + 2x$ and $\deg r(x) < 4$.

Ex 3 : Let $f(x) = x^4 + 3x^3 + 3x^2 + x + 2$ and $g(x) = 4x^3 + 4x^2 + 3x + 3$ in $Z_5[x]$. Find $q(x)$ and $r(x)$ in $Z_5[x]$ so that $f(x) = g(x) \cdot q(x) + r(x)$ with $\deg r(x) < 3$.

Solution :

g(x)	*f(x)*	*q(x)*
$4x^3 + 4x^2 + 3x + 3$	$x^4 + 3x^3 + 3x^2 + x + 2$	$4x + 3$
	$\underline{-x^4 \pm x^3 \pm 2x^2 \pm 2x}$	
	$2x^3 + x^2 + 4x + 2$	
	$\underline{-2x^3 \pm 2x^2 \pm 4x \pm 4}$	
	$r(x) = 4x^2 + 3$	

Thus, $\quad f(x) = g(x) \cdot q(x) + r(x)$,

where $\quad q(x) = 4x + 3$, $\quad r(x) = 4x^2 + 3$ and $\deg r(x) < 3$.

1.4 Euclidean Domain And Unique Factorization Domain :

Definition 1.4.1 : An integral domain is a commutative ring R with unity containing no divisors of 0.

i.e. if $a \cdot b = 0$ for $a, b \in R$ then either $a = 0$ or $b = 0$.

Definition 1.4.2 : Let R be a commutative ring $a, b \in R, a \neq 0$. We say a divides b if $\exists$ $c \in R$ such that $b = ac$.

We write this by a/b. In this case a is called a factor of b.

Definition 1.4.3 : Let R be a commutative ring. Let $a, b \in R$. An element $d \in R$ is called the greatest common divisor of a and b if

(i) d/a and d/b.

(ii) If $\exists$ $c \in R$ such that c/a and c/b then c/d.

We denote this by $d = \gcd(a, b)$.

1.4.4 Remark :

(1) $\gcd(a, b)$ need not be unique in R.

For this consider $R = Z_8$. Then

$2 \otimes_8 3 = 6 \quad \Rightarrow \quad 2/6$

$2 \otimes_8 2 = 4 \quad \Rightarrow \quad 2/4$

Again, if $c/6$ and $c/4$ then $c/6 - 4$. i.e $c/2$.

Thus, $2 = \gcd(6, 4)$.

Again,

$1 \otimes_8 6 = 6$

$6 \otimes_8 6 = 4$

Hence, $6/6$ and $6/4$.

If $c/6$ and $c/4$ we get $c/6$.

Hence, $\gcd(6, 4) = 6$.

Hence, 2 and 6 are g.c.d. in Z_8 for the same pair (4, 6).

(2) Existence of g.c.d. for any pair a, b in a commutative ring R is not compulsory.

e.g. Consider the ring R of even integers.

$4, 6 \in R$. $2/4$ in R but $2 \nmid 6$ in R. As $2 \cdot 3 = 6$ but $3 \notin R$.

Thus, $\gcd(4, 6)$ does not exist in R.

Definition 1.4.5 : Let R be a commutative ring with unity. $a, b \in R$ are called associates if $a = ub$ for some unit u in R.

[u is a unit in R means multiplicative inverse u^{-1} of u exists in R]

Theorem 1.4.6 : Let R be an integral domain with unity. If $d_1 = \gcd(a, b)$ in R, then $d_2 = \gcd(a, b)$ in R, iff d_1 and d_2 are associates.

Proof :

Only if part :

Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(a, b)$.

Then, d_1/a and d_1/b.

d_2/a and d_2/b.

Hence, d_1/d_2 and d_2/d_1 … by the definition of gcd.

Hence, d_1 and d_2 are associates.

If part :

Let d_1 and d_2 be associates and $d_1 = \gcd(a, b)$.

$d_1 = u\, d_2$ for some unit u in R.

Hence, d_2/d_1.

But d_1/a and d_1/b.

Hence, d_2/a and d_2/b. . . . (1)

Let $x \in R$ such that x/a and x/b.

Then $d_1 = \gcd(a, b) \Rightarrow d_1/x$.

$\Rightarrow \quad x = d_1 t$, for some $t \in R$.

$= (u^{-1} d_2)\, t$

$= d_2 (u^{-1} t)$

But this shows that d_2/x.

Hence, $d_2 = gcd(a, b)$. . . . (2)

Definition 1.4.7 : Let D be UFD. A non constant polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

in $D[x]$ is primitive if the only common divisors of all the a_i are units of D.

1.4.8 Examples :

(i) $4x^2 + 7x + 3$ is primitive in $Z[x]$.

(ii) $3x^2 + 6x + 9$ is not primitive in $Z[x]$ as 3 is not a unit in Z.

(iii) Any non constant irreducible in $D[x]$, where D is UFD, is primitive.

Theorem 1.4.9 : Let D be a UFD. Let $f(x) \in D[x]$ be a non constant polynomial. Then, $f(x) = (c) \cdot g(x)$, where $g(x)$ is a primitive in $D[x]$. The element c is unique upto a unit factor in D and the polynomial $g(x)$ is unique up to a unit factor in D.

Proof : Let $f(x) = a_0 + +a_1 x + \cdots + a_n x^n$, $(a_n \neq 0)$ be a nonconstant polynomial in $D[x]$. The coefficients $a_0, a_1, \ldots, a_n$ in D can be factored into a finite product of irreducible in D, uniquely upto order and associates.

Assume that each coefficient of $f(x)$ is factorized in this way. Let p_i denote the irreducible in D appearing in the factorization of one coefficient. If P_i divides all coefficients, then p_i will be in the factorization of all coefficients. Assume that no other associates of p_i appears in the factorization of any coefficient of $f(x)$.

Define

$$c = \prod_i p_i^{\alpha_i}$$

where α_i is the greatest integer such that $p_i^{\alpha_i}$ divides all the coefficients of $f(x)$.

In this case $f(x) = (c)\, g(x)$ where $c \in D$ and $g(x) \in D[x]$ is primitive by construction.

<u>Uniqueness :</u>

Let if possible,

$$f(x) = (c)\, g(x) \qquad \text{and}$$
$$f(x) = (d)\, h(x) \qquad \text{in } D[x].$$

where $g(x)$ and $h(x)$ are primitive in $D[x]$ and $c, d \in D$.

Now, $(c)\, g(x) = (d)\, h(x)$ implies each irreducible factor in c must divide the irreducible factor in d and conversely.

By cancelling the irreducible factors from c and d, we get,

$$(u)\, g(x) = (v)\, h(x)$$

where u and v are units in D.

But this shows that c is unique up to the unit factors and the primitive polynomial $g(x)$ is also unique up to unit factors.

Theorem (Gauss) 1.4.10 : Let D be UFD. $f(x), g(x) \in D[x]$ be primitive polynomials. Then $f(x) \cdot g(x)$ is also primitive in $D[x]$.

Proof : Let $f(x) = a_0 + +a_1x + \cdots + a_nx^n,\ (a_n \neq 0)$ and

$g(x) = b_0 + +b_1x + \cdots + b_mx^m,\ (b_m \neq 0)$

be two primitive polynomials in $D[x]$.

Let $h(x) = f(x) \cdot g(x)$.

Then, $h(x) = (a_0b_0) + (a_1b_0 + a_0b_1)x + \cdots + \sum_{i+j=k} \left(a_i\, b_j\right) x^k + \cdots + (a_nb_n)x^{n+m}$

Select any irreducible p in D. $f(x)$ and $g(x)$ being primitive in $D[x]$, $p \nmid a_i$ for some i and $p \nmid b_j$ for some j.

Let a_r be the first coefficient in $f(x)$ such that $p \nmid a_r$. ie. $p/a_0, p/a_1, \ldots, p/a_{r-1}$.

Let b_s be the first coefficient in $g(x)$ such that $p \nmid b_s$. ie. $p/b_0, p/b_1, \ldots, p/b_{s-1}$.

The coefficient of x^{r+s} in $h(x) = f(x) \cdot g(x)$ is

$= (a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \cdots + a_{r+s}b_0)$

As $p/a_0, p/a_1, \ldots, p/a_{r-1}$ we get

$$p/(a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_{r-1}b_{s+1}).$$

Similarly, $p/b_0, p/b_1, \ldots, p/b_{s-1}$ will imply

$$p/(a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \cdots + a_{r+s}b_0).$$

But $p \nmid a_r$ and $p \nmid b_s$ imply $p \nmid a_rb_s$. (See result ****).

Hence, $p \nmid$ coefficient of x^{r+s} in $h(x)$.

Thus, we have proved that any irreducible $p \in D$ will not divide all the coefficients of $h(x) = f(x) \cdot g(x)$.

Hence, $h(x) = f(x) \cdot g(x)$ is a primitive polynomial in $D[x]$.

Generalization of the statement of Gauss's theorem is as follows.

Corollary 1.4.11: Let D be UFD. The finite product of primitive polynomials in $D[x]$ is again a primitive polynomial.

Proof : Let $f_1(x), f_2(x), \ldots, f_n(x) \in D[x]$ be primitive polynomials.

Let $f(x) = f_1(x) \cdot\ f_2(x) \cdot ... \cdot f_n(x)$.

Then, $f(x) \in D[x]$.

We will prove the result by induction on ‘n’.

The result is true for $n = 2$ by Gauss’s theorem.

Let the result be true for $n = r$ say.

i.e. $f_1(x) \cdot\ f_2(x) \cdot ... \cdot f_r(x)$ is a primitive polynomials.

Consider $f_1(x) \cdot\ f_2(x) \cdot ... \cdot f_r(x) \cdot f_{r+1}(x)$ then this will be the product of two primitive polynomials $\left(f_1(x) \cdot\ f_2(x) \cdot ... \cdot f_r(x)\right)$ and $f_{r+1}(x)$, and hence a primitive polynomial in $D[x]$ by Gauss’s theorem.

By principle of mathematical induction, the result follows.

1.5 Zero of the Polynomials :

Definition 1.5.1 : Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be in $F[x]$ where F is a field. If $a \in F$ such that $f(a) = a_0 + a_1a + a_2a^2 + \cdots + a_na^n = 0$ (zero in F) then a is called a zero of $f(x)$ in F.

Example 1.5.2 : Find all zeros of $x^5 + 3x^3 + x^2 + 2x$ in $Z_5[x]$.

Solution : Let $f(x) = x^5 + 3x^3 + x^2 + 2x$ and $Z_5 = \{0, 1, 2, 3, 4\}$.

(i) $f(0) = 0$ $\Longrightarrow$ 0 is a zero of $f(x)$.

(ii) $f(1) = 1 + 3 + 1 + 2 = 1 \neq 0$ $\Longrightarrow$ 1 is not a zero of $f(x)$ in Z_5.

(iii) $f(2) = 4 \neq 0$ $\Longrightarrow$ 2 is not a root of $f(x)$ in Z_5.

(iv) $f(3) = f(-2) \neq 0$

(v) $f(4) = f(-1) = -1 - 3 + 1 - 2 = 0$. Hence 4 is root of $f(x)$ in Z_5.

Thus, $x = 0$ and $x = 4(= -1)$ are roots of $f(x)$ in Z_5.

Definition 1.5.3 : Let $f(x), g(x) \in F[x]$ where F is a field. We say $g(x)$ is a factor of $f(x)$ if $f(x) = g(x) \cdot q(x)$ for some $q(x) \in F[x]$.

In this case we also say that $g(x)$ divides $f(x)$ in $F[x]$.

Example : $x + 1$ is a factor of $x^2 + 1$ in $Z_2[x]$.

Solution :

$g(x)$	$f(x)$	$q(x)$
$x+1$	x^2+1	$x+1$
	$\underset{-}{x^2} \underset{-}{+x}$	
	$-x+1$	
	$\underset{-}{x} \underset{-}{+1}$	
	$r(x)=0$	

Thus,

$$f(x) = g(x) \cdot q(x) , \qquad \text{where } q(x) = x + 1 \in Z_2[x] .$$

Hence, $x + 1$ is a factor of $x^2 + 1$ in $Z_2[x]$.

Theorem 1.5.4 : Let F be a field. An element $a \in F$ is a zero of $f(x) \in F[x]$ iff $x - a$ is a factor of $f(x)$ in $F[x]$.

Proof :

<u>Only if part :</u>

Let $a \in F$ be a zero of $f(x) \in F[x]$.

Hence, by definition $f(a) = 0$. By division algorithm, $\exists\ q(x), r(x) \in F[x]$ such that

$$f(x) = (x - a) \cdot q(x) + r(x) , \qquad \text{where } \deg r(x) < 1.$$

Hence, $r(x)$ must be a constant polynomial in $F[x]$. Let $r(x) = c, c \in F$.

Thus , $\quad f(x) = (x - a) \cdot q(x) + c.$

Therefore, $\quad f(a) = (a - a) \cdot q(a) + c.$

$\Rightarrow \quad 0 = 0 + c \quad \Rightarrow \quad c = 0$

Hence, $\quad f(x) = (x - a) \cdot q(x), \qquad q(x) \in F[x].$

This shows that $(x - a)$ is a factor of $f(x)$.

<u>If part :</u>

Let $f(x) = (x - a) \cdot q(x)$ for some $q(x) \in F[x]$.

Then, $f(a) = (a - a) \cdot q(a)$.

$\Rightarrow \quad f(a) = 0.$

Hence, a is a zero of $f(x)$.

Theorem 1.5.5 : Let F be a field and let $f(x) \in F[x]$ be a non zero polynomial of degree n. $f(x)$ has at most n roots in F.

Proof : If $f(x)$ has no zero in F then the result is obviously true.

Let $a_1 \in F$ be a zero of $f(x)$. Then by theorem 1.5.4,

$$f(x) = (x - a_1)\, q_1(x)\ , \qquad \text{where } \deg q_1(x) = n - 1.$$

If $q_1(x)$ has no zeros in F, then $f(x)$ has only one one zero in F and in this case the result is true.

If $a_2 \in F$ is a zero of $q_1(x)$, then

$$q_1(x) = (x - a_2)\, q_2(x)\ , \qquad \text{where } \deg q_2(x) = n - 2.$$

Continuing in this way, we get,

$$f(x) = (x - a_1)(x - a_2) \dots (x - a_r)\ q_r(x),$$

where $q_r(x) \in F[x]$ such that $q_r(x)$ has no zeros in F.

Clearly, $r \leq n$.

Claim : $b \in F$ such that $b \neq a_i \quad \forall \quad i,\ 1 \leq i \leq n$ will not be a zero of $f(x)$.

i.e. no element of F other than a_i will be a zero of $f(x)$.

$$f(b) = (b - a_1)(b - a_2) \dots (b - a_r)\ q_r(b),$$

As $b \neq a_i$ we get $b - a_i \neq 0 \quad \forall \quad i,\ 1 \leq i \leq r$.

$q_r(b) \neq 0$ as $q_r(x)$ has no zero in F.

As F is an integral domain (F being a field) we get,

$$(b - a_1)(b - a_2) \dots (b - a_r)\ q_r(b) \neq 0$$

i.e. $f(b) \neq 0$.

Hence, no element $b \in F$ other than a_i will be a zero of $f(x)$.

Thus, $a_1, a_2, \dots, a_r\ (r \leq n)$ are the only zeros of $f(x)$.

Hence $f(x)$ has at most n zeros in F.

1.5.6 Example

Ex 1 : Consider the polynomial

$$f(x) = x^4 + 3x^3 + 2x + 4$$

in $Z_5[x]$.

As $f(1) = 1 \oplus_5 3 \oplus_5 2 \oplus_5 4 = 0$ in Z_5,

we get, $1 \in Z_5$ is a root of $f(x)$.

Hence, $f(x) = (x - 1) \cdot q_1(x)$ . . . (1)

To find $q_1(x)$:

$$
\begin{array}{c|l|l}
 & \qquad f(x) & q_1(x) \\
\hline
x-1 & x^4 + 3x^3 + 0\cdot x^2 + 2x + 4 & x^3 + 4x^2 + 4x + 1 \\
 & \underline{\underset{-}{}x^4 \underset{+}{-} x^3} & \\
 & \quad 4x^3 + 0\cdot x^2 & \\
 & \quad \underline{\underset{-}{}4x^3 \underset{+}{-} 4x^2} & \\
 & \qquad 4x^2 + 2x & \\
 & \qquad \underline{\underset{-}{}4x^2 \underset{+}{-} 4x} & \\
 & \qquad\quad 6x + 4 & \\
 & \qquad\quad \underline{\underset{-}{}x \underset{+}{-} 1} & \\
 & \qquad\qquad 0 &
\end{array}
$$

Hence, $\quad q_1(x) = x^3 + 4x^2 + 4x + 1$

Again $\quad q_1(1) = 0$ in Z_5.

Hence, 1 is a zero of $q_1(x) \in Z_5(x)$.

Hence, $\qquad q_1(x) = (x-1)\, q_2(x)$ . . . (2)

To find $q_2(x)$:

$$
\begin{array}{c|l|l}
 & \qquad q_1(x) & q_2(x) \\
\hline
x-1 & x^3 + 4x^2 + 4x + 1 & x^2 + 4 \\
 & \underline{\underset{-}{}x^3 \underset{+}{-} x^2} & \\
 & \quad 4x + 1 & \\
 & \quad \underline{\underset{-}{}4x \underset{+}{-} 4} & \\
 & \qquad 0 &
\end{array}
$$

Thus, $\quad q_2(x) = x^2 + 4$

Again $\quad q_2(1) = 0$.

Hence, $1 \in Z_5$ is a zero of $q_2(x) \in Z_5(x)$.

Hence, $\qquad q_2(x) = (x-1)\, q_3(x)$ . . . (3)

To find $q_3(x)$:

$$
\begin{array}{c|c|c}
 & q_2(x) & q_3(x) \\
\hline
x-1 & x^2+0x+4 & x+1 \\
 & \underset{-}{} x^2 \underset{+}{-} x & \\
\cline{2-2}
 & x+4 & \\
 & \underset{-}{} x \underset{+}{-} 1 & \\
\cline{2-2}
 & 0 &
\end{array}
$$

Thus, $\quad q_3(x) = x + 1$

Thus, from (1), (2) and (3), we get

$$f(x) = (x-1)(x-1)(x-1)(x+1)$$

$$= (x-1)^3 \cdot (x+1).$$

Ex 2 : Let $f(x)$ and $g(x)$ be in $Z_5[x]$, where

$$f(x) = 4x^3 + 4x^2 + 3x + 3 \qquad \text{and}$$

$$g(x) = 4x^2 + 3.$$

Show that $g(x)$ is a factor of $f(x)$ in $Z_5[x]$ (or $g(x)$ divides $f(x)$ in $Z_5[x]$).

Solution :

$$
\begin{array}{c|c|c}
g(x) & f(x) & q(x) \\
\hline
4x^2+3 & 4x^3+4x^2+3x+3 & x+1 \\
 & \underset{-}{} 4x^3 \underset{-}{+} 0x^2 \underset{-}{+} 3x & \\
\cline{2-2}
 & 4x^2+3 & \\
 & \underset{-}{} 4x^2 \underset{-}{+} 3 & \\
\cline{2-2}
 & 0 &
\end{array}
$$

Thus, $\quad f(x) = g(x) \cdot (x+1)$

This shows that $g(x)$ is a factor of $f(x)$.

Ex 3 : Find all the zeros of the following polynomial $f(x) = x^3 + 2x + 3$ in $Z_5[x]$.

Solution : $f(1) \neq 0$. Hence 1 is not a zero of $f(x)$.

$f(-1) = 0$. Hence -1 is a zero of $f(x)$ in Z_5.

i.e. $\quad$ 4 is a zero of $f(x)$.

$\therefore$ $(x-4)$ is a factor of $f(x)$ in $Z_5[x]$.

$$
\begin{array}{r|l|l}
 & & q_1(x) \\
\hline
x+1 & x^3 + 2x + 3 & x^2 + 4x + 3 \\
 & \underset{-}{}x^3 \underset{-}{+} 4x^2 & \\
\cline{2-2}
 & \qquad 4x^2 + 2x & \\
 & \qquad \underset{-}{}4x^2 \underset{-}{+} 4x & \\
\cline{2-2}
 & \qquad\qquad 3x + 3 & \\
 & \qquad\qquad \underset{-}{}3x \underset{-}{+} 3 & \\
\cline{2-2}
 & \qquad\qquad\qquad 0 &
\end{array}
$$

$\therefore \qquad f(x) = (x+1) \cdot (x^2 + 4x + 3).$

Let $q_1(x) = x^2 + 4x + 3$.

Again $q_1(-1) = 0$. Hence -1 is a root of $q_1(x)$ and hence $f(x)$ in $Z_5[x]$.

$$
\begin{array}{r|l|l}
 & & q_2(x) \\
\hline
x+1 & x^2 + 4x + 3 & x + 3 \\
 & \underset{-}{}x^2 \underset{-}{+} x & \\
\cline{2-2}
 & \qquad 3x + 3 & \\
 & \qquad \underset{-}{}3x \underset{-}{+} 3 & \\
\cline{2-2}
 & \qquad\qquad 0 &
\end{array}
$$

Thus, $f(x) = (x+1)(x+1) \cdot (x+3)$.

Hence, -1 and -3 are zeros of $f(x)$ in Z_5.

i.e. 4 and 2 are zeros of $f(x)$ in Z_5.

[Since additive inverse of 1 in Z_5 is 4 and additive inverse of 3 in Z_5 is 2].

Ex 4 : Show that the polynomial $f(x) = x^4 + 4$ can be factorized into linear factors in $Z_5[x]$.

Solution : Let $f(x) = x^4 + 4$. Then $f(1) = 0$ in Z_5.

Hence, $1 \in Z_5$ is a zero of $f(x)$.

$$
\begin{array}{r|l|l}
x-1 & x^4+4 & x^3+x^2+x+1 \\
 & \underline{\underset{-}{x^4}\underset{+}{-}x^3} & \\
 & \quad x^3+0x^2 & \\
 & \quad \underline{\underset{-}{x^3}\underset{+}{-}x^2} & \\
 & \qquad x^2+0x & \\
 & \qquad \underline{\underset{-}{x^2}\underset{+}{-}x} & \\
 & \qquad\quad x+4 & \\
 & \qquad\quad \underline{\underset{-}{x}\underset{+}{-}1} & \\
 & \qquad\qquad 0 &
\end{array}
$$

Thus, $\quad f(x) = (x-1)(x^3+x^2+x+1)$ ... (1)

Let $q_1(x) = x^3+x^2+x+1$.

Then, $q_1(x) \in Z_5[x]$ and $q_1(-1) = 0$ i.e. $q(4) = 0$.

Hence, $(x-4) = (x+1) \in Z_5[x]$ is a factor of $q_1(x)$.

$$
\begin{array}{r|l|l}
x+1 & x^3+x^2+x+1 & x^2+1 \\
 & \underline{\underset{-}{x^3}\underset{-}{+}x^2} & \\
 & \quad x+1 & \\
 & \quad \underline{\underset{-}{x}\underset{-}{+}1} & \\
 & \qquad 0 &
\end{array}
$$

Thus, $f(x) = (x-1)(x+1)\cdot(x^2+1)$.

Let $q_2(x) = x^2+1$, $\quad q_2(x) \in Z_5[x] \quad$ and $\quad q_2(2) = 0$.

Hence, 2 is a zero of $q_2(x)$.

$$
\begin{array}{r|l|l}
x-2 & x^2+1 & x+2 \\
 & \underline{\underset{-}{x^2}\underset{+}{-}2x} & \\
 & \quad 2x+1 & \\
 & \quad \underline{\underset{-}{2x}\underset{+}{-}4} & \\
 & \qquad 0 &
\end{array}
$$

Thus, $f(x) = (x-1)(x+1)(x-2)(x+2)$.

1.6 Irreducible Polynomials in R[x] :

Throughout R denotes an integral domain with unity.

Definition 1.6.1: Let $f(x) \in R[x]$ and $\deg f(x) \geq 1$. $f(x)$ is said to be irreducible polynomial over R, if it cannot be expressed as a product of two polynomials $g(x)$ and $h(x) \in R[x]$ such that

$$0 < \deg g(x) < \deg f(x) \quad \text{and} \quad 0 < \deg h(x) < \deg f(x).$$

1.6.2 Remarks:

(i) If $f(x) = g(x) \cdot h(x)$ and if $f(x) \in R[x]$ is irreducible, then $\deg f(x) = 0$ or $\deg h(x) = 0$.

(ii) A polynomial of positive degree which is not irreducible is said to be reducible.

(iii) The polynomial $(x^2 + 1) \in Z[x]$ is irreducible over Z but it is reducible over $\mathbb{C}$ as $(x^2 + 1) \in \mathbb{C}[x]$ and $(x^2 + 1) = (x + i)(x - i)$.

(iv) Any polynomial of degree 1 over R is irreducible over R.

(v) The units in R and $R[x]$ are the same.

Theorem 1.6.3 : Every irreducible polynomial in $R[x]$ is an irreducible element in $R[x]$.

Proof : Let $f(x) \in R[x]$ be an irreducible element in $R[x]$.

To prove that $f(x)$ is an irreducible polynomial in $R[x]$.

Let, if possible, $f(x)$ be reducible over R.

Let $f(x) = g(x) \cdot h(x)$, where $g(x), h(x) \in R[x]$

with $0 < \deg g(x) < \deg f(x)$ and

$0 < \deg h(x) < \deg f(x)$.

As $\deg g(x) > 0$ and $\deg h(x) > 0$, $g(x)$ and $h(x)$ are not constant polynomials and $g(x), h(x) \notin R$. Hence they are not units in R.

By lemma, $f(x)$ and $g(x)$ are not units in $R[x]$. Hence $f(x)$ is not an irreducible element in $R[x]$.

Thus, $f(x)$ is not an irreducible polynomial.

$\Longrightarrow$ $f(x)$ is not an irreducible element.

This shows that irreducible element in $R[x]$ is an irreducible polynomial in $R[x]$.

Remark 1.6.4 : Converse of the above theorem need not be true.

i.e. Irreducible polynomial in $R[x]$ need not be an irreducible element in $R[x]$.

Consider, the polynomial $3x^2 + 3 \in Z[x]$.

Then $3x^2 + 3$ is an irreducible polynomial in $Z[x]$.

But $3x^2 + 3 = 3(x^2 + 1)$

= Product of two polynomials in $Z[x]$ which are non units in $Z[x]$.

(Since the units in $Z[x]$ are the units in Z which are 1 and -1).

Thus, $3x^2 + 3$ is expressed as a product of two non zero, non unit polynomials in $Z[x]$.

Hence, $3x^2 + 3$ is not an irreducible element in $Z[x]$.

Remark 1.6.5 : Primitive polynomial $f(x) \in R[x]$ may be reducible or irreducible over R.

Example : $f(x) = x^2 - 3x + 2 \in Z[x]$ is a primitive and reducible as

$x^2 - 3x + 2 = (x - 2)(x - 1)$ but $f(x) = x^2 - 2 \in Z[x]$ is a primitive and irreducible over Z.

Theorem 1.6.6 : Let R be UFD and $f(x) \in R[x]$. $f(x)$ is an irreducible element in $R[x]$ iff either f is an irreducible element of R or f is an irreducible primitive polynomial in $R[x]$.

Proof :

<u>Only if part :</u>

Let $f(x) \in R[x]$ be an irreducible element of $R[x]$. If $f \in R$, then f will be a constant polynomial and it will be an irreducible element in R.

Hence, if $f \notin R$, we have to prove that $f(x)$ is irreducible over R and $f(x)$ is a primitive polynomial.

(i) To prove $f(x)$ is irreducible over R.

Let $f(x)$ be reducible over R.

Let $f(x) = g(x) \cdot h(x)$; $g(x), h(x) \in R[x]$.

As $f(x)$ is an irreducible element in $R[x]$ either $g(x)$ or $h(x)$ must be unit in $R[x]$.

As units in R and $R[x]$ are the same, either $g(x)$ or $h(x)$ is a unit in R.

Hence, $\deg g(x) = 0$ or $\deg h(x) = 0$ (being constant polynomial in $R[x]$).

But this in turn shows that $f(x)$ is an irreducible polynomial in $R[x]$.

(ii) Let $f(x) = c\, f_1(x)$ where $c =$ content of $f(x)$ and $f_1(x)$ is a primitive polynomial in $R[x]$.

As $\deg f(x) = \deg f_1(x)$, we get $\deg f_1(x) \geq 1$ and hence $f_1(x) \notin R$.

Hence, $f_1(x)$ is not a unit in $R[x]$ and c is a unit in R.

Hence, $f(x)$ is a primitive polynomial in $R[x]$.

Thus, if a non constant polynomial $f(x) \in R[x]$ is an irreducible element in $R[x]$ then it is an irreducible, primitive polynomial in $R[x]$.

If part :

Let $f(x) \in R[x]$.

If $f(x)$ is an irreducible element in $R[x]$ then $f(x)$ is an irreducible polynomial in $R[x]$ (See theorem 1.6.3).

Let $f(x) \in R[x]$ be primitive irreducible polynomial in $R[x]$.

To prove that $f(x)$ is an irreducible element in $R[x]$.

Let $\quad f(x) = g(x) \cdot h(x) \quad$ for some $g(x),\ h(x) \in R[x]$.

As $f(x)$ is an irreducible polynomial,

$$\deg g(x) = 0 \qquad \text{or} \qquad \deg h(x) = 0$$

Let $\deg g(x) = 0$. Then $g(x)$ is a constant polynomial in $R[x]$. Let $g(x) = b_0$.

Hence, $g(x) \in R$.

Now, $c\,(f) = c\,(gh) = c(g) \cdot c(h)$.

f is primitive $\quad\Longrightarrow\quad c\,(f) =$ unit in R.

Hence, $g(x)$ is unit in $R[x]$.

Thus ,

$$f(x) = g(x) \cdot h(x) \quad \Longrightarrow \quad g(x) \text{ is unit in } R[x].$$

This in turn shows that $f(x)$ is an irreducible element in $R[x]$.

Theorem 1.6.7 : Let R be UFD. Let $p(x) \in R[x]$ be a primitive polynomial in $R[x]$. $p(x)$ can be factored in a unique way as a product of irreducible elements in $R[x]$.

Proof : Let F be a field of quotients of R. Then $F[x]$ is an Euclidean domain.

Hence, $F[x]$ is a PID and therefore $F[x]$ is UFD .

(i) To prove that $p(x) \in R[x]$ can be factored as a product of irreducible elements in $R[x]$.

$p(x) \in R[x] \implies p(x) \in F[x]$.

As $F[x]$ is UFD, we can write

$$p(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_n(x)$$

where $p_i(x) \in F[x]$ and $p_i(x)$ is an irreducible polynomial in $F[x]$ for each $i,\ 1 \le i \le n$.

$$p_i(x) \in F[x] \quad \Rightarrow \quad p_i(x) = \frac{1}{a_i}\ f_i[x], \qquad \text{where } a_i \in R \text{ and } f_i(x) \in R[x].$$

Further, $p_i(x)$ is an irreducible polynomial in $F[x] \Rightarrow p_i(x)$ is an irreducible element in $F[x]$.

$\Rightarrow$ $f_i(x)$ is an irreducible element in $F[x]$ for each $i,\ 1 \le i \le n$.

Now,

$$\begin{aligned} p_i(x) &= \frac{1}{a_i}\ f_i[x] \\ &= \frac{1}{a_i}\ [c_i\, f_i^*(x)] \end{aligned}$$

where $c_i = c(f_i) =$ constant of f_i and $f_i^*(x)$ is a primitive polynomial in $R[x]$.

$$p_i(x) = \frac{c_i}{a_i}\ f_i^*(x), \qquad \forall \quad i,\ 1 \le i \le n.$$

Thus, $p(x) = \dfrac{c_1\, c_2\, \ldots\, c_n}{a_1\, a_2\, \ldots\, a_n}\ f_1^*(x)\, f_2^*(x)\ \ldots\ f_n^*(x)$

Hence, $(a_1\, a_2\ \ldots\ a_n)\, p(x) = (c_1\, c_2\ \ldots\ c_n)\, f_1^*(x)\, f_2^*(x)\ \ldots\ f_n^*(x)$.

As each $p_i(x)$ is an irreducible polynomial in $F[x]$, we get $f_i^*(x)$ is also an irreducible polynomial and hence irreducible element in $F[x]$.

Thus, $f_i^*(x)$ is an irreducible element in $R[x]$.

Equating the content on both sides, we get, $a_1\, a_2\ \ldots\ a_n = (c_1\, c_2\ \ldots\ c_n)\, u$, where u is a unit in R.

Hence,

$$\begin{aligned} p(x) &= u^{-1}[f_1^*(x)\, f_2^*(x)\ \ldots\ f_n^*(x)] \\ &= [u^{-1} f_1^*(x)]\, f_2^*(x)\ \ldots\ f_n^*(x) \\ &= \text{Product of irreducible elements in } R[x]. \end{aligned}$$

This shows that $p(x) \in R[x]$ is factored into a product of irreducible elements in $R[x]$.

(ii) Uniqueness :

Let $p(x) = f_1^*(x)\, f_2^*(x)\ \ldots\ f_n^*(x)$

and $p(x) = r_1(x)\, r_2(x)\ \ldots\ r_n(x)$

be two factorization of $p(x)$ as a product of irreducible elements in $R[x]$.

As R is a UFD, the number n will remain the same as $F[x]$ is a UFD, $r_i(x)$ is uniquely determined upto associates in $F[x]$.

Hence, $\quad r_i(x) = u_i\, f_i^*(x), \qquad$ where u_i is a unit in F.

Hence, $\quad u_i = \frac{a_i}{b_i}, \qquad$ for some $a_i, b_i \in R, \qquad \forall \quad i,\ 1 \le i \le n.$

Thus,

$$r_i(x) = \frac{a_i}{b_i}\, f_i^*(x) \qquad \forall \quad i,\ 1 \le i \le n.$$

Hence, $\quad b_i\, r_i(x) = a_i\, f_i^*(x) \qquad \forall \quad i,\ 1 \le i \le n.$

As $r_i(x)$ and $f_i^*(x)$ are primitive polynomials, equating the contents on both sides we get $b_i = v_i\, a_i$ where v_i is a unit in R.

Hence, $r_i(x)$ is associate of $f_1^*(x)$ in $R[x]$.

Thus the uniqueness follows.

Theorem 1.6.8 : R is UFD $\Rightarrow R[x]$ is UFD.

Proof : Let $f(x) \in R[x]$ be a non zero non unit element in $R[x]$.

Let $f(x) = c\, p(x)$ where $c =$ content of f and $p(x)$ is a primitive polynomial in x.

By theorem 1.6.7,

$$p(x) = f_1^*(x)\, f_2^*(x)\ \dots\ f_n^*(x)$$

where $f_i^*(x)$ is an irreducible element in $R[x]$ and this representation is unique up to associates.

Also $c \in R$ and R is UFD imply

(i) c is unit in R or

(ii) c can be expressed as $c = c_1\, c_2 \dots c_k$ where c_r are irreducible elements in R, $\forall\, r$, $1 \le r \le k$

<u>Case (i) :</u> c is a unit in R.

Then, $f(x) = c\, p(x)$

$= c\, [f_1^*(x)\, f_2^*(x)\ \dots\ f_n^*(x)]$

$= c\, [f_1^*(x)][\, f_2^*(x)\ \dots\ f_n^*(x)]$

= Finite product of irreducible elements in $R[x]$ and the representation is unique upto associates.

<u>Case (ii) :</u> c is non unit.

Then $c = c_1\, c_2 \dots c_k$ where each c_i is an irreducible elements in R.

As c_i is an irreducible element in R, c_i is an irreducible element in $R[x]$.

Thus, $f(x) = c_1\, c_2 \ldots c_k\, f_1^*(x)\, f_2^*(x)\ \ldots\ f_n^*(x)$

= Finite product of irreducible elements in $R[x]$ and the representation is unique upto associates.

Thus, from case (i) and case (ii), we get $R[x]$ is UFD.

1.6.9 Example : $Z[x]$ is UFD as Z is UFD. $Z[x]$ is UFD but not PID.

[If $Z[x]$ is PID then Z must be a field which is not so.]

Now onwards F denotes a field.

1.6.10 Remarks :

(i) Let $f(x) \in F[x]$ be irreducible over F. But note that, at the same time it may be reducible over the field E. ($E \supseteq F$).

(ii) Any polynomial of degree 1 in $F[x]$ is irreducible over F.

Example 1.6.11 : $x^3 - 3 \in Q[x]$ is irreducible over Q.

But it is reducible over $\mathbb{R}$ where $Q =$ the field of quotients and $\mathbb{R} =$ the field of reals.

For the polynomials of degree 2 or 3 particularly we have

Theorem 1.6.12 : Let F be a field and $f(x) \in F[x]$. Let $\deg f(x) = 2 \text{ or } 3$. Then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F.

Proof :

Only if part :

Let f be reducible over F.

Then $\quad f(x) = g(x) \cdot h(x)$

where $\quad g(x), h(x) \in F[x]$, $\deg g(x) < \deg f(x)$ and $\deg h(x) < \deg f(x)$.

$$f(x) = g(x) \cdot h(x)$$

$\Longrightarrow \quad \deg f(x) = \deg g(x) + \deg h(x) \qquad$ [$\because$ F is an integral domain]

As $\quad \deg f(x) = 2/3$, the $\deg g(x) = 1$ or $\deg h(x) = 1$.

Thus, let us assume that $\deg g(x) = 1$.

Then, $g(x) = x - a$ say, for some $a \in F$.

But then $f(x) = (x-a) \cdot h(x) \quad \Longrightarrow \quad f(a) = 0$ and hence $a \in F$ will be a zero of $f(x) \in F[x]$.

<u>If part :</u>

Let $f(x) \in F[x]$ has a zero in F say $'a'$. Then $(x-a)$ is a factor of $f(x)$.

Hence, $\quad f(x) = (x-a) \cdot g(x)$.

Hence, $\deg f = \deg(x-a) + \deg g(x)$

where $\quad \deg g(x) = 2 < \deg f(x) = 1 + \deg g(x)$, $\quad$ if $\deg f(x) = 3$

or $\quad \deg g(x) = 1 < \deg f(x)$, $\quad$ if $\deg f(x) = 2$.

Hence, $f(x) \in F[x]$ is a reducible polynomial over the field F.

More generally we get

Theorem 1.6.13: Let $f(x) \in F[x]$ be any polynomial of degree > 1. If $a \in F$ is a zero of $f(x)$ in F, then $f(x)$ is reducible over F.

Proof : (As $f(x)$ and $(x-a)$ are in $F[x]$) By division algorithm, we get,

$$f(x) = (x-a) \cdot g(x) + r(x)$$

where $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

$$f(a) = 0 + r(x) \implies 0 = r(a). \qquad \ldots \text{ as } a \text{ is a zero of } f(x), f(a) = 0.$$

Thus, $\quad f(x) = (x-a) \cdot g(x)$.

Therefore,

$$\deg f(x) = \deg(x-a) + \deg g(x)$$

Therefore, $\quad \deg g(x) = \deg\, f(x) - 1 \; > 0$.

This shows that $f(x)$ is reducible.

We know that every ideal in $F[x]$ is a principle ideal. (Being an Euclidean domain, $F[x]$ is PID.) Using this fact we prove

Theorem 1.6.14: If F is a field, then the ideal $\langle p(x) \rangle \neq \{0\}$ of $F[x]$ is maximal iff $p(x)$ is irreducible over F.

Proof :

<u>Only if part :</u>

Let $\langle p(x) \rangle \neq \{0\}$ be a maximal ideal in $F[x]$.

To prove that $p(x)$ is irreducible over F. Let if possible $p(x)$ be reducible.

Hence, $\exists$ $g(x)$ and $h(x)$ in $F[x]$ such that $p(x) = g(x) \cdot h(x)$ where

$$0 < \deg\ g(x) < \deg\ p(x)$$

and $\quad 0 < \deg\ h(x) < \deg\ p(x).$

Now, $p(x) \in \langle p(x) \rangle \quad \Longrightarrow \quad g(x) \cdot h(x) \in \langle p(x) \rangle$.

As $\langle p(x) \rangle$ is a maximal ideal in $F[x]$, it is a prime ideal in $F[x]$

Hence, either $g(x) \in \langle p(x) \rangle$ or $h(x) \in \langle p(x) \rangle$.

But then $g(x) = p(x) \cdot q_1(x)$ or $h(x) = p(x) \cdot q_2(x)$, for some $q_1(x), q_2(x) \in F[x]$.

But then we can't have $\deg g(x)$ or $\deg h(x)$ less than the $\deg p(x)$.

Hence our assumption is wrong i.e. $p(x)$ is irreducible.

<u>If part :</u>

Let $p(x)$ be irreducible polynomial in $F[x]$.

To prove that $\langle p(x) \rangle$ is maximal.

Let A be an ideal in $F[x]$ such that $\langle p(x) \rangle \subseteq A \subseteq F[x]$. As $F[x]$ is PID, $A = \langle f(x) \rangle$ for some $f(x) \in F[x]$.

As $p(x) \in \langle p(x) \rangle$ we get $p(x) \in \langle f(x) \rangle$.

Hence $p(x) = f(x) \cdot g(x)$, for some $g(x) \in F[x]$.

As $p(x)$ is irreducible, we get

$$\deg\ g(x) = 0 \quad \text{or} \quad \deg\ f(x) = 0$$

<u>Case 1 :</u> $\deg\ g(x) = 0$

Then, $g(x)$ is a constant polynomial in $F[x]$.

Let $\quad g(x) = c \quad$ for some $c \in F$

Then, $\quad p(x) = f(x) \cdot c \quad$ implies $\quad f(x) = c^{-1} \cdot p(x)$.

[c^{-1} exists in F as c is a non zero element in F.]

Hence, $\quad f(x) = c^{-1} \cdot p(x)$ implies $g(x) \in \langle p(x) \rangle$ and hence $A = \langle g(x) \rangle = \langle p(x) \rangle$.

<u>Case 2 :</u> $\deg\ f(x) = 0$

Then, $f(x)$ is a non zero constant polynomial in $F[x]$.

Hence, $f(x)$ is a non zero element in F and hence $f(x)$ is a unit in F.

But then $\langle f(x) \rangle = A = F[x]$. This shows that there exists no proper ideal A in $F[x]$ such that $\langle p(x) \rangle \subset A \subset F[x]$.

Hence, $\langle p(x) \rangle$ is a maximal ideal in $F[x]$.

1.6.15 Examples :

(i) $x^2 - 3 \in Q[x]$ is an irreducible polynomial. Hence $\langle x^2 - 3 \rangle$ in $Q[x]$ is a maximal ideal in $F[x]$ and hence $\frac{Q[x]}{x^2-3}$ is a field.

(ii) $\frac{Q[x]}{I}$ where $I = \langle x^2 - 5x + 6 \rangle$ is not a field as $x^2 - 5x + 6 = (x-2)(x-3)$ shows that $x^2 - 5x + 6$ is a reducible polynomial in $Q[x]$ and hence I is not a maximal ideal in $Q[x]$.

If R is an integral domain with unity then every irreducible element in $R[x]$ is an irreducible polynomial in $R[x]$ (See Theorem 1.6.3). The converse need not be true. But it is true if R is a field.

Theorem 1.6.16: Let F be a field. $f(x) \in F[x]$ is an irreducible polynomial in $F[x]$ iff $f(x)$ is an irreducible element in $F[x]$.

Proof :

<u>Only if part :</u>

Let $f(x) \in F[x]$ be irreducible polynomial in $F[x]$.

Let $f(x) = g(x) \cdot h(x)$ for $g(x), h(x) \in F[x]$.

f being irreducible, either $\deg g(x) = 0$ or $\deg h(x) = 0$.

Suppose, $\deg g(x) = 0$. Then $g(x)$ is a constant polynomial in $F[x]$.

Let $g(x) = a$ $(a \in R)$.

Then $a \neq 0$ and $a \in F$.

Hence, a^{-1} exists in F. But this shows $g(x) = a$ is a unit in $F[x]$.

Hence, $f(x)$ is an irreducible element in $F[x]$.

<u>If part :</u>

Let $f(x) \in F[x]$ be an irreducible element in $F[x]$.

Then every field being an integral domain with unity, the result follows by Theorem 2.6.3 in 5. [Every irreducible element in $R[x]$ is an irreducible polynomial in $R[x]$.]

Theorem 1.6.17 : Let D be UFD and let F be a field of quotients of D. Let $f(x) \in D[x]$ where degree of $f(x) > 0$. Then

(i) $f(x)$ is irreducible in $D[x]$ $\Longrightarrow$ $f(x)$ is irreducible in $F[x]$.

(ii) $f(x)$ is primitive in $D[x]$ and $f(x)$ is irreducible in $F[x] \implies f(x)$ is irreducible in $D[x]$.

Proof :

(i) Degree of $f(x) > 0 \implies f(x)$ is non constant polynomial in $D[x]$.

Let $f(x) = g(x) \cdot h(x)$, where $g(x)$ and $h(x)$ are polynomials of lower degree in $F[x]$.

As F is a field of quotients of D, the coefficients in $g(x)$ and $h(x)$ are of the form $\frac{a}{b}$ for some $a, b \in D$. By clearing the denominators we get

$$(d)\, f(x) = g_1(x)\, h_1(x) \qquad \ldots (1)$$

where $d \in D$ and $g_1(x), h_1(x) \in D[x]$ such that

degree of $g_1(x)$ = degree of $g(x)$ and

degree of $h_1(x)$ = degree of $h(x)$.

Now, by theorem 1, $f(x) = (c) \cdot p(x)$, $g_1(x) = (c_1) \cdot p_1(x)$ and $h_1(x) = (c_2) \cdot p_2(x)$ where $c, c_1, c_2 \in D$ and $p(x), p_1(x), p_2(x) \in D[x]$ are primitive polynomials in $D[x]$.

Thus, from (1), we get,

$$(dc)\, p(x) = (c_1\, c_2)\, p_1(x)\, p_2(x) \qquad \ldots (2)$$

By theorem 1.4.10, the product $p_1(x) \cdot p_2(x)$ is also a primitive polynomials in $D[x]$. But then $c_1\, c_2 = (dc)\, u$ for some unit u in D.

Hence, from (2), we get,

$$(dc)\, p(x) = (dcu)\, p_1(x)\, p_2(x)$$

Hence, $\quad (c)\, p(x) = (cu)\, p_1(x)\, p_2(x)$

i.e. $\quad f(x) = (cu)\, p_1(x)\, p_2(x)$

This shows that $f(x)$ has a factorization in $D[x]$.

Thus, we have proved that $f(x)$ has a factorization in $F[x] \implies f(x)$ has a factorization in $D[x]$.

Hence, $f(x) \in D[x]$ is irreducible in $D[x]$, then it is irreducible in $F[x]$.

(ii) Let $f(x) \in D[x]$. As $D[x] \subseteq F[x]$.

We get, if $f(x)$ is reducible in $D[x]$ then $f(x)$ is reducible in $F[x]$.

Hence the result.

Corollary 1.6.18 : Let D be a UFD and let F be the field of quotients in D.

Let $f(x) \in D[x]$ be a non constant polynomial. Then $f(x)$ factors into the product of two polynomials of lower degree in $F[x]$ if an only if it has a factorization into polynomials of same degree in $D[x]$.

Proof :

Only if part :

Let $f(x) = g(x)\, h(x)$ be a factorization of $f(x)$ in $F[x]$ where degree of $g(x) = r$ and degree of $h(x) = s$. As in the proof of the theorem 4(1) we can prove

$$f(x) = (a)\, p_1(x)\, p_2(x)$$

where degree of $p_1(x)$ = degree of $g(x) = r$ and

degree of $p_2(x)$ = degree of $h(x) = s$ and

$p_1(x), p_2(x) \in D[x]$.

If part :

Let $f(x) = g(x)\, h(x)$, where $g(x), h(x) \in D[x]$.

Then, $g(x), h(x) \in F[x]$, since $D[x] \subseteq F[x]$, and the result follows.

1.7 Factorization in F[x] :

Throughout F denotes a field.

Definition 1.7.1 : Let $f(x), g(x) \in F[x]$. We say $g(x)$ divides $f(x)$ in $F[x]$ if there exists $q(x) \in F[x]$ such that $f(x) = g(x) \cdot q(x)$.

Example 1.7.2: Let $f(x) = 4x^3 + 4x^2 + 3x + 3$ and

$g(x) = 4x^2 + 3$

$f(x), g(x) \in Z_5[x]$ and $f(x) = g(x) \cdot (x + 1)$ in $Z_5[x]$.

Hence, $g(x)$ divides $f(x)$ in $Z_5[x]$.

$g(x)$	$f(x)$	$q(x)$
$4x^2 + 0 \cdot x + 3$	$4x^3 + 4x^2 + 3x + 3$	$x + 1$
	$\underset{-}{}4x^3 \underset{-}{+} 0x^2 \underset{-}{+} 3x$	
	$4x^2 + 3$	
	$\underset{-}{}4x^2 \underset{-}{+} 3$	
	0	

Theorem 1.7.3 : Let $p(x)$ be an irreducible polynomial in $F[x]$. If $p(x)$ divides $r(x) \cdot s(x)$ for $r(x),\ s(x) \in F[x]$, then either $p(x)/r(x)$ or $p(x)/s(x)$.

Proof : $p(x)/r(x) \cdot s(x) \quad \Rightarrow \quad r(x) \cdot s(x) = p(x) \cdot q(x)$ for some $q(x) \in F[x]$.

But this implies that $r(x) \cdot s(x) \in \langle p(x) \rangle$.

$p(x)$ being an irreducible polynomial in $F[x]$, $\langle p(x) \rangle$ is a maximal ideal in $F[x]$.

As $F[x]$ is a commutative ring with unity, $\langle p(x) \rangle$ is a prime ideal.

Hence, $r(x) \cdot s(x) \in \langle p(x) \rangle$ implies $r(x) \in \langle p(x) \rangle$ or $s(x) \in \langle p(x) \rangle$.

Hence, either $p(x)$ divides $r(x)$ or $p(x)$ divides $s(x)$ in $F[x]$.

Using the mathematical induction we get,

Corollary 1.7.4 : Let $p(x) \in F[x]$ be an irreducible polynomial. If $p(x)/r_1(x) \cdot r_2(x) \ldots r_n(x)$. for $r_i(x) \in F[x]$. Then $p(x)/r_i(x)$ for at least one i.

Theorem 1.7.5 : Let $f(x) \in F[x]$ be a non constant polynomial. Then $f(x)$ can be factored into a product of irreducible polynomials in $F[x]$. The irreducible polynomials will be unique except for order and for unit factors in F.

Proof : Let $f(x) \in F[x]$ be a non constant polynomial.

Case (I) : $f(x)$ is irreducible.

Then there is nothing to prove.

Case (II) : $f(x)$ is not irreducible.

Let $\quad f(x) = g(x) \cdot h(x)$

where $\quad$ degree of $g(x) <$ degree of $f(x)$ $\quad$ and

degree of $h(x) <$ degree of $r(x)$.

If $g(x)$ and $h(x)$ both are irreducible then we are through.

If $g(x)$ and $h(x)$ both are not irreducible then at least one of them factors into polynomials of lower degree. Continuing this process, we get,

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_n(x)$$

where each $p_i(x)$ is an irreducible polynomial in $F[x]$.

This completes the proof of the first part.

Now, let us assume that

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_r(x) \qquad \ldots (1)$$

$$f(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_s(x) \qquad \ldots (2)$$

be two factorizations of $f(x)$ into the irreducible polynomials in $F[x]$.

Now,

$$p_1(x)/p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_r(x) \qquad \text{implies}$$

$$p_1(x)/q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_s(x)$$

As $p_1(x)$ is an irreducible polynomial in $F[x]$, $p_1(x)/q_j(x)$, for some j.

Take $q_j(x) = q_1(x)$.

Since $q_1(x)$ is irreducible and $p_1(x)/q_1(x)$ we get, $q_1(x) = u_1\, p_1(x)$ where $u_1 \neq 0$.

Hence, $u_1 \in F$ is a unit in F.

Thus,

$$p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_r(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_s(x) \qquad \text{will imply}$$

$$p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_r(x) = u_1\, p_1(x) \cdot q_2(x) \cdot \ldots \cdot q_s(x)$$

Cancelling $p_1(x)$ from both side, we get,

$$p_2(x) \cdot \ldots \cdot p_r(x) = u_1 \cdot q_2(x) \cdot \ldots \cdot q_s(x)$$

Arguing as above, we get, $p_2(x) = u_2\, q_2(x)$, where $u_2 \neq 0$ is a unit in F.

Substituting this value in the above expression and cancelling $p_2(x)$ from both sides, we get,

$$p_3(x) \cdot \ldots \cdot p_r(x) = u_1 \cdot u_2 \cdot q_3(x) \cdot \ldots \cdot q_s(x)$$

Continuing in this way we arrive at

$$1 = u_1 \cdot u_2 \cdot \ldots \cdot u_r \cdot q_{r+1}(x) \cdot q_{r+2}(x) \cdot \ldots \cdot q_s(x).$$

But this is possible only when $s = r$. Hence,

$$1 = u_1 \cdot u_2 \cdot \ldots \cdot u_r$$

This shows that the irreducible factors $p_i(x)$ and $q_j(x)$ are the same except for order and unit factors.

1.7.6 Examples

Ex 1 : Let $f(x) = x^4 + 3x^3 + 2x + 4 \in Z_5[x]$.

$$x = 1 \quad \Rightarrow \quad f(1) = 1 + 3 + 2 + 4 = 10 = 0 \text{ in } Z_5[x].$$

Hence, $x = 1$ is a root / zero of $f(x)$.

$$f(x) = (x - 1) \cdot g(x)$$

$$
\begin{array}{c|c|l}
g(x) & f(x) & q(x) \\
\hline
x-1 & x^4+3x^3+2x+4 & x^3+4x^2+4x+1 \\
 & \underline{\underset{-}{x^4}\underset{+}{-}x^3} & \\
 & 4x^3+2x & \\
 & \underline{\underset{-}{4x^3}\underset{+}{-}4x^2} & \\
 & 4x^2+2x & \\
 & \underline{\underset{-}{4x^2}\underset{+}{-}4x} & \\
 & x+4 & \\
 & \underline{\underset{-}{x}\underset{+}{-}1} & \\
 & 5=0 \text{ in } Z_5[x] &
\end{array}
$$

Thus, $x = 1$ is a zero of $f(x)$ and $f(x) = (x^3 + 4x^2 + 4x + 1)\,(x - 1)$. . . . (1)

Let $g(x) = (x^3 + 4x^2 + 4x + 1)$.

Then, $g(x) \in Z_5(x)$ and

$g(1) = 10 \equiv 0(mod\ 5)$

$\therefore$ $(x - 1)$ is a factor of $g(x)$.

$$
\begin{array}{c|c|l}
 & & \\
\hline
x-1 & x^3+4x^2+4x+1 & x^2+4 \\
 & \underline{\underset{-}{x^3}\underset{+}{-}x^2} & \\
 & 0+0+4x+1 & \\
 & \underline{\underset{-}{4x}\underset{+}{-}4} & \\
 & 0 &
\end{array}
$$

This shows that $(x - 1)$ is a factor of $x^3 + 4x^2 + 4x + 1$ and hence $x - 1$ is also a factor of $f(x)$.

Again, $x = 1 \Rightarrow x^2 + 4 = 0$ in Z_5.

Hence, $(x - 1)$ is a factor of $x^2 + 4$.

$$
\begin{array}{c|c|l}
 & & \\
\hline
x-1 & x^2+4 & x+1 \\
 & \underline{\underset{-}{x^2}\underset{+}{-}x} & \\
 & x+4 & \\
 & \underline{\underset{-}{x}\underset{+}{-}1} & \\
 & 0 &
\end{array}
$$

This shows that $(x-1)$ is a factor of (x^2+4) and hence $(x-1)$ is a factor of $f(x)$.

Thus, we get,

$$f(x) = x^4 + 3x^3 + 2x + 4 = (x-1)^3 \cdot (x+1) \text{ in } Z_5[x].$$

This shows that $f(x)$ is factored as a product of irreducible polynomials in $Z_5[x]$.

These irreducible factors in $Z_5[x]$ are defined upto units in $Z_5[x]$.

e.g. $\quad (x-1)^3 \cdot (x+1) = (x-1)^2 \cdot (2x-2)(3x+3)$

Ex 2 : Show that the polynomial (x^4+4) can be factored into linear factors in $Z_5[x]$.

Solution : Let $f(x) = x^4 + 4$ in $Z_5[x]$.

Then $f(1) = 1 + 4 = 0$ in Z_5.

Hence, $x-1$ is a factor of $f(x)$.

$$\begin{array}{l|l|l}
x-1 & x^4+0\cdot x^3+0\cdot x^2+0\cdot x+4 & x^3+x^2+x+1 \\
 & \underline{\underset{-}{}x^4 \underset{+}{-} x^3} & \\
 & \quad x^3+0\cdot x^2 & \\
 & \quad \underline{\underset{-}{}x^3 \underset{+}{-} x^2} & \\
 & \qquad x^2+0\cdot x & \\
 & \qquad \underline{\underset{-}{}x^2 \underset{+}{-} x} & \\
 & \qquad\quad x+4 & \\
 & \qquad\quad \underline{\underset{-}{}x \underset{+}{-}1} & \\
 & \qquad\quad 0+0 &
\end{array}$$

Thus, $f(x) = (x-1)(x^3+x^2+x+1)$ $\quad \ldots (1)$

Consider $g(x) = (x^3+x^2+x+1)$ in $Z_5[x]$.

Then $g(-1) = -1 + 1 - 1 + 1 = 0$.

Hence, $(x+1)$ is a factor of $g(x)$ in $Z_5[x]$.

$$\begin{array}{l|l|l}
x+1 & x^3+x^2+x+1 & x^2+1 \\
 & \underline{\underset{-}{}x^3 \underset{-}{+} x^2} & \\
 & \qquad x+1 & \\
 & \qquad \underline{\underset{-}{}x \underset{-}{+} 1} & \\
 & \qquad 0+0 &
\end{array}$$

Thus, $g(x) = (x^3+x^2+x+1) = (x+1)(x^2+1)$

Hence, from (1), we get,

$$f(x) = (x-1)(x+1)(x^2+1) \qquad \ldots (2)$$

Let $\quad h(x) = (x^2+1)$ in $Z_5[x]$.

$$h(2) = 4 + 1 = 0.$$

Hence, $(x-2)$ is a factor of $h(x)$ in $Z_5[x]$.

$$\begin{array}{r|l|l}
x-2 & x^2 + 1 & x+2 \\
 & \underline{\underset{-}{x^2} \underset{+}{-} 2x} & \\
 & \quad 2x + 1 & \\
 & \quad \underline{\underset{-}{2x} \underset{+}{-} 4} & \\
 & \qquad 0 &
\end{array}$$

We know that, 'Q' the field of rational numbers is the field of quotients of an integral domain Z.

Hence applying theorem 1.6.6 to Q in particular, we get,

Result : Let $f(x) \in Z[x]$. If $f(x)$ is primitive an irreducible over Z then $f(x)$ is irreducible over Q.

- **Eisenstein Criteria for Irreducibility over Q :**

Theorem 1.7.7 : Let $p \in Z$ be a prime. Let $f(x) \in Z[x]$, where

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \ \ (a_n \neq 0)$$

such that $a_n \not\equiv 0 \ (mod\ p)$ but $a_i \equiv 0 \ (mod\ p)$, for $i < n$, with $a_0 \not\equiv 0 \ (mod\ p^2)$. Then $f(x)$ is irreducible over Q.

[p is a prime number such that $p/a_0, p/a_1, \ldots, p/a_{n-1}$ and $p \nmid a_n$ and $p^2 \nmid a_0$].

Proof : Assume that $f(x)$ is reducible in $Z[x]$.

Let

$$f(x) = g(x) \cdot h(x) \ ,$$

where $g(x), h(x)$ are non-constant polynomials in $Z[x]$ with degree < n.

Let

$$g(x) = b_0 + b_1 x + \cdots + b_r x^r, \ \ (b_r \neq 0)$$

and $$h(x) = c_0 + c_1 x + \cdots + c_s x^s, \ \ (c_s \neq 0)$$

(i) $p^2 \nmid a_0 \quad \Longrightarrow \quad p^2 \nmid b_0 c_0$.

If p/b_0 and p/c_0 then $p^2/b_0 c_0$.

Hence, either $p \nmid b_0$ or $p \nmid c_0$ exclusively.

Assume that $p \nmid b_0$ but p/c_0.

(ii) $p \nmid a_n \quad \Longrightarrow \quad p \nmid b_r c_s \quad \Longrightarrow \quad p \nmid b_r$ and $p \nmid c_s$.

(iii) Thus, p/c_0 and $p \nmid c_s$.

Find the smallest k such that $p \nmid c_k$. Thus $p \nmid b_0$ and $p \nmid c_k \implies p \nmid b_0 c_k$.

But $b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0$ is a coefficient of x^k in $g(x)h(x)$.

As $f(x) = g(x) \cdot h(x)$, equating the coefficients of x^k, we get,

$$a_k = b_0 c_k + b_1 c_{k-1} + \cdots + b_k c_0$$

As $p \nmid b_0 c_k$, we get $p \nmid a_k$.

But then, by data, as $p/a_0, p/a_1, \ldots, p/a_{n-1}$ and $p \nmid a_n$ we must have $k = n$.

Hence, consequently we must have $s = n$. This contradicts our assumption that $s < n$.

Hence, $f(x)$ does not factor into polynomials in $Z[x]$.

By result 1,

$f(x)$ has no factorization as a product of two polynomials, both of lower degree in $Q[x]$.

Hence, $f(x)$ is irreducible over Q.

[Result 1 : Let $f(x) \in Z[x]$. $f(x)$ factors into a product of two polynomials of lower degrees r and s in $Q[x]$ if and only if it has such a factorization with polynomials of same degrees r and s in $Z(x)$.]

Remark 1.7.8 : $f(x) = g(x) \cdot h(x) \quad \Leftrightarrow \quad f(x+1) = g(x+1) \cdot h(x+1)$,

for $f(x),\ g(x),\ h(x) \in Z[x]$.

Hence, $f(x)$ is reducible iff $f(x+1)$ is reducible and $f(x)$ is irreducible iff $f(x+1)$ is irreducible.

Note that, we can take any integer in place of 1.

When the constant term in a polynomial $f(x) \in Z[x]$ is ± 1, we cannot apply Eisenstein criterion to check the irreducibility of $f(x)$ over Q. In such cases we find suitable $t \in Z$ such that $f(x+t)$ is irreducible over Q (if possible).

To illustrate this, consider the following polynomial

$$f(x) = x^3 + x^2 - 2x - 1 \in Z[x].$$

As there exists no prime in Z that divides 1, we cannot apply the criterion directly in this case.

$$f(x+1) = (x+1)^3 + (x+1)^2 - 2(x+1) - 1$$
$$= x^3 + 4x^2 + 3x - 1$$

Again, we cannot apply the criterion in this case.

$$f(x-1) = (x-1)^3 + (x-1)^2 - 2(x-1) - 1$$
$$= x^3 - 2x^2 - x + 1$$

We cannot apply the criterion for $f(x-1)$ also.

$$f(x+2) = x^3 + 7x^2 + 14x + 7$$

Here, take $p = 8$. Then p/a_0, p/a_1, p/a_2 and $p \nmid a_3$ and $p^2 \nmid a_0$.

Hence, by Eisenstein criterion, $f(x+2)$ is irreducible over Q.

Hence, $f(x)$ is irreducible over Q.

1.7.9 Example

Ex 1 : $f(x) = 8x^3 - 6x - 1$ is irreducible over Q.

Solution : Here $a_0 = -1, a_1 = -6, a_2 = 0, a_3 = 8$.

As $a_0 = -1$, Eisenstein criterion cannot be applied.

Hence, consider $f(x+1)$.

$$f(x+1) = 8(x+1)^3 - 6(x+1) - 1$$
$$= 8[x^3 + 3x^2 + 3x + 1] - 6x - 6 - 1$$
$$= 8x^3 + 24x^2 + 24x + 8 - 6x - 6 - 1$$
$$= 8x^3 + 24x^2 + 18x + 1$$

Again, we cannot apply the criterion for $f(x+1)$.

Hence, consider $f(x-1)$.

$$f(x-1) = 8(x-1)^3 - 6(x-1) - 1$$
$$= 8[x^3 - 3x^2 + 3x - 1] - 6x + 6 - 1$$
$$= 8x^3 - 24x^2 + 24x - 8 - 6x + 6 - 1$$
$$= 8x^3 - 24x^2 + 18x - 3$$

Take $p = 3$.

Then, by Eisenstein criterion, $f(x-1)$ is irreducible over Q.

Hence, $f(x)$ is irreducible over Q.

Ex 2 : $f(x) = x^4 + x^3 + x^2 + x + 1 \in Z[x]$ is irreducible over Q.

Solution : As the constant term in $f(x)$ is 1 we cannot apply Eisenstein criterion for $f(x)$.

Consider $f(x+1)$.

Then, $f(x+1) = (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1$

$$= (x^4 + 4x^3 + 6x^2 + 4x + 1) + (x^3 + 3x^2 + 3x + 1) + (x^2 + 2x + 1) + x + 2$$

$$= x^4 + 5x^3 + 10x^2 + 10x + 5$$

For $f(x+1)$, $a_0 = 5, a_1 = 10, a_2 = 10, a_3 = 5, a_4 = 1$.

Take $p = 5$.

Then, $p/a_0, p/a_1, p/a_2,\ p/a_3$ and $p^2 \nmid a_0$ and $p \nmid a_4$.

Hence, by Eisenstein criterion, $f(x+1)$ is irreducible over Q.

Hence, $f(x)$ is irreducible over Q.

Ex 3 : Show that the polynomial $2x^5 - 5x^4 + 5$ is irreducible over Q.

Solution : Let

$$f(x) = 2x^5 - 5x^4 + 5$$

$$= 5 + 0 \cdot x + 0 \cdot x^2 + 0 \cdot x^3 - 5x^4 + 2x^5$$

Hence, $a_0 = 5, a_1 = 0, a_2 = 0, a_3 = 0, a_4 = -5, a_5 = 2$.

Take $p = 5$, p is prime in Z.

$p/a_0, p/a_1, p/a_3, p/a_4$ and $p^2 \nmid a_0$ and $p \nmid a_5$.

Hence, by Eisenstein criterion, $f(x)$ is irreducible over Q.

Ex 4 : The cyclotomic polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over Q for any prime p.

Solution : Let

$$g(x) = \phi_p(x+1)$$

$$= \frac{(x+1)^p - 1}{(x+1) - 1}$$

$$= \frac{x^p + {}^pC_1\ x^{p-1} + \cdots + {}^pC_p\ x^{p-1} - 1}{x}$$

$$= x^{p-1} + {}^pC_1\ x^{p-2} + \cdots + p$$

Let $g(x) = a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}$. Then $a_0 = p,\ a_1 = {}^pC_{p-1},\ a_n = 1$.

Then, for prime number p, we get $p/a_0, \ldots, p/a_{p-1}$ and $p^2 \nmid a_0$ and $p \nmid a_p = 1$.

Hence, by Eisenstein criterion, $g(x)$ is irreducible over Q.

Now, if $\phi_p(x) = h_1(x)h_2(x)$ in $Z[x]$, then $\phi_p(x+1) = h_1(x+1)h_2(x+1)$ would be a factorization of $g(x)$ in $Z[x]$ and hence by result 1, we get $\phi_p(x+1)$ has factorization in $Q[x]$ which is not possible by Eisenstein criterion.

Hence, $\phi_p(x)$ is irreducible over Q.

Extra :

Applying the theory in particular for $Z[x]$, we get the following result.

Particular case of theorem 1.2.16 (ii) :

Theorem 1.7.10 : Let $f(x) \in Z[x]$ be primitive. If $f(x)$ is reducible over Q, then $f(x)$ is reducible over Z.

Proof : $f(x)$ is reducible over Q. Hence $f(x) = g(x) \cdot h(x)$ where $g(x),\ h(x) \in Q[x]$ and $g(x),\ h(x)$ are non constant. Then $f(x) = \left(\frac{a}{b}\right) g_1(x) \cdot\ h_1(x)$, where $g_1(x)$ and $h_1(x)$ are primitive polynomials in $Z[x]$. But then

$$b[f(x)] = (a)\ [g_1(x) \cdot h_1(x)]$$

$f(x)$ being primitive in $Z[x]$, b is the g.c.d. of coefficients in $b\ f(x)$.

As the product of two primitive polynomials is a primitive polynomial in

$a\ [g_1(x) \cdot h_1(x)]$. Hence a and b are unique upto the units.

As the units in Z are ± 1, we get $b = \pm a$.

Hence, $f(x) = \pm g_1(x) \cdot g_2(x)$. This shows that $f(x)$ is reducible in $Z[x]$.

Particular case of theorem 1.4.10:

Theorem 1.7.11 : If $f(x)$ and $g(x)$ are primitive polynomials in $Z[x]$ then so is their product.

Proof : Suppose $f(x) \cdot g(x)$ is not primitive. Let p be a prime integer in Z such that p divides all the coefficients of $f(x) \cdot g(x)$.

Let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

and $$g(x) = b_0 + + b_1 x + \cdots + b_n x^n.$$

$f(x)$ is primitive, hence p does not divide all $a_0, a_1, \dots, a_n$.

Let a_s be the first coefficient of f such that $p \nmid a_s$.

Similarly, let b_t be the first coefficient in $g(x)$ such that $p \nmid b_t$.

Now, the coefficient of x^{s+t} in $f(x) \cdot g(x)$ is

$$[a_0 b_{s+t} + a_1 b_{s+t-1} + \cdots + a_{s-1} b_{t+1}] + a_s b_t + [a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \cdots + a_{s+t} b_0]$$

As

$$p/a_0, \quad p/a_1, \quad \dots, \quad p/a_{s-1}$$

and $\quad p/b_0, \quad p/b_1, \quad \dots, \quad p/b_{t-1},$

we get,

$$p/[a_0 b_{s+t} + a_1 b_{s+t-1} + \cdots + a_{s-1} b_{t+1}]$$

and $\quad p/[a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \cdots + a_{s+t} b_0]$

As $p \nmid a_s$ and $p \nmid b_t$ and p is prime, we get $p \nmid a_s b_t$.

Hence, $p \nmid$ coefficient of x^{s+t} in $f(x) \cdot g(x)$, which is a contradiction.

This in turn shows that $f(x) \cdot g(x)$ is primitive.

Theorem 1.7.12 : If $f(x) \in Z[x]$ is reducible over Q then it is also reducible over Z.

Proof : $f(x) \in Z[x]$ is reducible over Q.

Let $f(x) = (c)\, f_1(x)$. Where $c =$ g.c.d. of the coefficient of $f(x)$, and $f_1(x)$ is a primitive polynomial in $Z[x]$.

Then $f_1(x)$ is reducible over Z and hence $f(x)$ is reducible over Z.

Theorem 1.7.13 : $f(x) \in Z[x]$. $f(x)$ is reducible over Q iff $f(x)$ is reducible over Z.

Proof : $f(x)$ is reducible over Z implies $f(x)$ is reducible over Q as $Z[x] \subseteq Q[x]$.

Conversely,

If $f(x)$ is reducible over Q then, $f(x)$ is reducible over Z.

Theorem 1.7.14 : Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \in Z[x]$ be a monic polynomial. If $f(x)$ has a root $a \in Q$, then $a \in Z$ and a/a_0.

Proof : $a \in Q \implies a = \dfrac{b}{c}$ for some relatively prime elements $b, c \in Z$.

$$f(a) = 0 \quad \Rightarrow \quad f\left(\frac{b}{c}\right) = 0$$

$$\Rightarrow \quad a_0 + a_1\left(\frac{b}{c}\right) + \cdots + a_{n-1}\left(\frac{b}{c}\right)^{n-1} + \left(\frac{b}{c}\right)^n = 0$$

$$\Longrightarrow \quad a_0 + a_1\left(\frac{b}{c}\right) + \cdots + a_{n-1}\left(\frac{b}{c}\right)^{n-1} = -\left(\frac{b}{c}\right)^n$$

$$\Longrightarrow \quad a_0c^{n-1} + a_1bc^{n-2} + \cdots + a_{n-1}b^{n-1} = -\frac{b^n}{n} \qquad \ldots (1)$$

$$\Longrightarrow \quad a_0c^{n-1} + a_1bc^{n-2} + \cdots + a_{n-1}b^{n-1} \in Z$$

we get, $-\frac{b^n}{n} \in Z$. Hence $c = \pm 1$.

Hence, by (1), we get,

$$a_0 + a_1b + \cdots + a_{n-1}b^{n-1} = \pm b^n.$$

Hence, $a_0 = -b[a_1 + a_2b + \cdots \pm b^{n-1}]$.

This shows that b/a_0. ... (2)

As $\quad a = \frac{b}{c} = \frac{b}{\pm 1} = \pm b$ ... (3)

From (1), (2) and (3), we get a/a_0 and $a \in Z$.

CHAPTER III : THEORY OF MODULES

Unit 1 : Modules :

1.1 Modules – Definition and examples.

1.2 Submodules.

1.3 Homomorphism

1.4 Fundamental theorem of homomorphism and its applications.

1.1 MODULES – Definition and Examples :

Definition 1.1.1 : Let R be a ring and let $\langle M,+\rangle$ be an abelian group. Let $(r,m) \longrightarrow rm$ be a mapping of $R \times M$ into M such that

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

ii) $(r_1 + r_2)m = r_1 m + r_2 m$

iii) $(r_1 r_2)m = r_1(r_2 m)$

iv) $1.m = m \quad if \;\; 1 \in R$

for all $m,\ m_1,\ m_2\ \in M$ and $r,\ r_1,\ r_2\ \in R$. Then M is called a left R-module.

Remarks 1.1.2 :

a) rm is called is called the scalar multiplication or just multiplication of m by r on the left.

b) Right R-modules can also be defined similarly.

c) If R is a commutative ring, every left module will be a right module or vice versa.

d) In a commutative ring R we will not distinguish between left and right R-modules and we and we simply call them R-modules.

e) If R is a field, the R-module is called a vector space.

Examples 1.1.3 :

1. Any ring R can be regarded as a left R-module.

   Define the scalar multiplication rm for $r,m \in R$ as usual multiplication in R.

2. Any additive abelian group G is a left L-module. For an abelian group $\langle G,+\rangle$ define

$n\,a = a + a + \ldots + a$ (n times) , for n > 0

$0 \cdot a = 0$

and $(-n)\,a = (-a) + (-a) + \ldots + (-a)$ (n times) , for n > 0

Then G is a L-module.

3. Let $\langle G, + \rangle$ be an abelian group.

$$R = \{f / f: G \longrightarrow G \text{ is a group homomorphism.}\}$$

$\langle R, +, \circ \rangle$ is a ring, where $f + g$ and f o g are defined by

$$(f + g)\,(x) = f\,(x) + g\,(x) \qquad \forall \quad x \in G$$

and $$(f \circ g)\,(x) = f\,[g\,(x)]$$

G is a left R-module where the scalar product fx is defined by

$$fx = f\,(x) \qquad \text{for } f \in R \text{ and } x \in G$$

4. Let $R[x]$ denote a polynomial ring over the ring R in an indeterminate x. Then $R[x]$ is a left R-module under the scalar multiplication defined by

$$r \cdot f(x) = r\,(a_0 + a_1 x + \cdots + a_n x^n)$$
$$= (ra_0) + (ra_1)x + \cdots + (ra_n)x^n \qquad \text{for } r \in R \text{ and } f(x) \in R[x]$$

where $f(x) = a_0 + a_1 x + \cdots + a_n x^n$

5. Let R be any ring and let I be a left ideal in R. Then $\langle I, + \rangle$ is an abelian group and for any $r \in R$ and $a \in I$, $ra \in I$ and this scalar multiplication $(r, a) \longrightarrow ra$ from $R \times I \longrightarrow I$ satisfies all the conditions stated in the definition. Hence I is a left R-module.

Exercise

1. Define right R-module M.
2. Give some examples of right R-modules.
3. Find an example of a left R-module which is not a right R-module.
4. Find an example of a right R-module which is not a left R-module.

Simple Properties :

Here onwards all modules are left modules otherwise stated.

Theorem 1.1.4 : Let M be any R-module. Then

i) $0 \cdot m = 0$ for all $m \in M$

ii) $r \cdot 0 = 0$ for all $r \in R$

iii) $(-r) \cdot m = (-rm) = r \cdot (-m\ )$ for all $r \in R$

Proof :

i) $r \cdot m = (r + 0) \cdot m$ for all $r \in R$ and $m \in M$

Hence, $rm + 0 = rm + 0 \cdot m$ (see definition)

This shows that $0 \cdot m = 0$ for all $m \in M$

ii) $r \cdot m = r \cdot (m + 0)$ for all $r \in R$ and $m \in M$

Thus, $rm + 0 = rm + r \cdot 0$ (see definition)

But then $r \cdot 0 = 0$ for all $r \in R$ as M is a group.

iii) $0 = 0 \cdot m$, by (i)

$= [r + (-r)]\, m$

$= rm + (-r)m$

Hence, $-(rm) = (-r)\, m$ . . . (1)

Also,

$0 = r \cdot 0$, by (ii)

$= r(m + (-m))$

$= rm + r(-m)$

Hence, $-(rm) = r(-m)$ . . . (2)

From (1) and (2), we get,

$(-r)\, m = -(rm) = r(-m),$ for all $r \in R$ and $m \in M$

Worked Examples

Example 1.1.5 : Let M be an R-module. Show that the set $\{x \in R\ /\ xM = \{0\}\}$ is an ideal of R, where $xM = \{xm\ /\ m \in M\}$.

Solution : Let $I = \{x \in R\ /\ xM = \{0\}\}$.

(i) By theorem (1), $0 \cdot m = 0,$ for all $m \in M$.

imply $0 \cdot M = \{0\}$

and hence $0 \in I$

Thus, $I \neq \phi$.

(ii) Let $x, y \in I$

$x, y \in I \implies xM = \{0\}$ and $yM = \{0\}$

Now, for any $m \in M$, we have

$(x - y)\, m = [x + (-y)]\, m$

$= xm + (-y)\, m$ (by definition)

$= xm - ym$ (by theorem 1.1.4 (iii)

$= 0 - 0$ ($\because$ $x, y \in R$ imply xm = 0 and ym = 0

Thus, $(x - y)\, m = 0$ for all $m \in M$.

Hence, $(x - y)\, M = \{0\}$.

This shows that $x - y \in I$, for all $x, y \in I$.

(iii) Let $r \in R$ and $x \in I$.

$x \in I \implies xM = \{0\}$

$\implies x \cdot m = 0$, for each $m \in M$.

Hence, $\{r\, x\}\, m = (r)\,(x\, m) = r\,.\,0 = 0$, (by theorem 1.1.4)

Hence, for $r \in R$ and $x \in I$, we get $rx \in I$.

Similarly,

$(xr)\, m = x\,(rm) = 0$, as $x \in I$ and $rm \in M$, for any $r \in R$.

Hence, given $x \in I$ and $r \in R$, $rx \in I$ and $xr \in I$.

From (i), (ii) and (iii), we get,

I is an ideal in R.

Remark : Let M be an R-module.

If the ideal $\left\{x \in R \;/\; xM = \{0\}\right\}$ is the zero ideal in R.

i.e., if $\left\{x \in R \;/\; xM = \{0\}\right\} = \{0\}$, then M is called a faithful module.

Example 1.1.6 : Let M and N be an R-modules. Define '$+$' in $M \times N$ by

$$(x, y) + (z, t) = (x + z, y + t) \quad \text{for } (x, y), (z, t) \in M \times N$$

and the scalar multiplication $'\cdot'$ by

$$r \cdot (x, y) = (r \cdot x,\; r \cdot y) \quad \text{for all } r \in R, (x, y) \in R \times R$$

Then, it can easily verified that $M \times N$ is an R-module.

Remarks 1.1.7 :

(1) The R-module $M \times N$ is called the direct product (external) of R-modules M and N.

(2) On the same line we can define the direct product (external) of any finite number of R-modules.

Example 1.1.8 : Let R be a ring. Define

$$R^n = \{(x_1, x_2, \dots, x_n) \;/\; x_i \in R\} \quad \text{for } n \in N.$$

Then show that R^n is a R-module.

Solution : We know that every ring R is an R-module. Hence every ring R is an R-module.

Hence, $R^n = R \times R \times \dots \times R$ is an R-module (being the direct product of n R-modules) by Example 1.1.6.

[Here in R^n, for $x, y \in R^n$ and where,

$$x = (x_1, x_2, \dots, x_n), \qquad x_i \in R$$

and $\quad y = (y_1, y_2, \dots, y_n), \qquad y_i \in R$

we have,

$$x + y = (x_1 + y_1, x_2 + y_2 \dots, x_n + y_n)$$

and $\quad r \cdot x = x = (rx_1, rx_2, \dots, rx_n)$]

Exercise

1. Let R be a field. Let $V = \{f \;\; f : R \longrightarrow R$ be a ring homomorphism$\}$ show that V is a vector space over R.
2. Let M be a left R-module. Define $(m\,, r) \longrightarrow rm$ for each $m \in M$ and $r \in R$ as a mapping from $M \times R$ to M. Show that M is a right module.
2. Let M be an R-module. For $x \in M$, show that $\{r \in R \;/\; rx = 0\}$ is a left ideal in R.

1.2 SUBMODULES :

Definition 1.2.1: Let M be an R-module. A non empty subset N of an R-module M is called R-submodule (or submodule) of M if

(i) $\quad a - b \in N$, $\qquad$ for all $a, b \in N$

(ii) $\quad r \cdot a \in N$, $\qquad$ for all $r \in R, \;\; a \in N$

Remark 1.2.2 :

(i) Not every subset of an R-module M is a submodule of M.

(ii) If N is a R-submodule of an R-module M then $\langle N,+\rangle$ is a (normal) subgroup of $\langle M,+\rangle$ which is closed under scalar multiplication.

(iii) If N is a R-submodule of an R-module of M, then N itself is a R-module.

(iv) $\{0\}$ and M are trivial submodule of an R-module M.

Examples 1.2.3 :

1. Let R be a ring. Then we know that the ring R is an R-module. Any left ideal I of R is a R-submodule.

2. Let M be any R-module. Let $x_1, x_2, \dots, x_n \in M$ (n is finite). Then the set

$$N = \left\{ \sum_{i=1}^{n} r_i\, x_i \;/\; r_i \in R \right\}$$

is a submodule of M.

Solution : Let $a, b \in N \implies a = \sum_{i=1}^{n} r_i\, x_i$ and $b = \sum_{i=1}^{n} r'_i\, x_i$

where $r_i, r'_i \in R$.

(i) $a - b = \sum_{i=1}^{n} r_i\, x_i - \sum_{i=1}^{n} r'_i\, x_i$

Hence, $a - b = \sum_{i=1}^{n} (r_i - r'_i)\, x_i$

as $r_i - r'_i \in R$, for each i, we get

$a - b \in N$

(ii) $r \cdot a = r \cdot \sum_{i=1}^{n} r_i\, x_i$

Hence, $r \cdot a = \sum_{i=1}^{n} (r \cdot r_i)\, x_i$

as $r,\ r_i \in R$, for each i, we get

$r \cdot a \in N$

Thus, for any $a, b \in N$ and $r \in R$, we have,

$a - b \in N$ and $r \cdot a \in N$.

Hence, N is a submodule of R-module M.

Remarks 1.2.4 :

(i) As a special case for example 2 we get for any R-module M, the set

$$Rx = \{rx \;/\; r \in R\}$$

is a R-module of M, for any $x \in R$.

(ii) If $1 \in R$, then the submodule Rx will contains the element x as $x = 1 \cdot x$.

Example 1.2.5 : Let M be an R-module and $x \in M$.

Define $N = \{rx + nx \;/\; r \in R \; and \; n \in Z\}$.

Then, N is a R-submodule of M containing x.

Solution : Obviously, $\langle N, +\rangle$ is a (abelian) subgroup of $\langle M, +\rangle$.

Hence, only to check that $a(rx + nx) \in N$ for any $a \in R$ and $(rx + nx) \in N$.

<u>Case I :</u> $n > 0$

$a\,(rx + nx) = a\,[\,rx + (x + x + \cdots + x \; n \; times)]$

$= a(rx) + (ax + ax + \cdots + ax \; n \; times)]$ ... by the definition of module

$= (ar)x + (a + a + \cdots + a \; n \; times)x\,]$ ... by the definition of module

$= [ar + (a + a + \cdots + a \; n \; times)]\, x$ ... by the definition of module

$= u \cdot x$ .... where $u = [ar + (a + a + \cdots + a \; n \; times)]$

As $u \in R$, we get $a\,(rx + nx) \in N$.

<u>Case II :</u> $n < 0$.

$a\,(rx + nx) = a\,[\,rx + ((-x) + (-x) + \cdots + (-x) \; n \; times)]$

$= a(rx) + a\,(-x) + a\,(-x) + \cdots + a\,(-x) \; n \; times)$

$= (ar)x + (-a)\,x + (-a)\,x + \cdots + (-a)\,x \; n \; times)x\,]$

... by the property of the module Theorem 1.1.4

$= [(ar) + (-a) + (-a) + \cdots + (-a)]\, x$... by the definition of module

$= t \cdot x$ .... where $t = ar + [(-a) + (-a) + \cdots + (-a)\;(n \; times)]$

As $t \in R$ we get $a\,(rx + nx) \in N$ when n < 0.

<u>Case III :</u> $n = 0$

$a\,(rx + nx) = a\,[\,rx + 0 \cdot x]$ … since n = 0

$= a\,[\,rx + 0]$ … since $0 \cdot x = 0$

$= a\,(rx) + a \cdot 0$

$= (ar)x + 0 \cdot x \in N$ … as $ar \in R$ and $0 \in Z$

$= (ar)x + 0$

Thus, from all the cases we get $a\ (rx + nx) \in N$.

Hence, N is a R-submodule of the module M.

Now selecting $r = 0$ and $n = 1$ $(1 \in Z)$ we get

$$0 \cdot x + 1 \cdot x = x \in N$$

Thus, the R-submodule N contains the element x.

Remarks 1.2.6:

(1) If k is a submodule of M containing x, then $N \subseteq K$. For any $r \in R,\ rx \in K$ and for any $n \in Z$,

$$nx = x + x + \cdots + x\ (n\ times) \in K, \qquad K \text{ being a submodule of } M.$$

But then $(rx + nx) \in K$ for any $r \in R$ and $n \in Z$.

Hence, $N \subseteq K$.

Thus, N is the smallest submodule of M containing x. Generally we denote N by $\langle x \rangle$.

(2) If $1 \in R$, then for $r \in R$ and $n \in N$

$$rx + nx = \{r + [1 + \ldots + 1(n\ times)\,]\,\}\,x$$
$$= tx \quad \text{where } t = r + (1 + \ldots + 1)\ n \text{ times}$$

as $t \in R$ we get $rx + nx \in Rx$

Hence, $N \subseteq Rx$. But $x \in N$ implies $Rx \subseteq N$.

Thus, $N = Rx = \langle x \rangle$; if $1 \in R$.

Example 1.2.7 : Let M be an R-module. Define

$$RM = \left\{ \sum_{i=1}^{n} r_i\, m_i \ /\ r_i \in R,\ m \in M \ and\ n\ is\ finite \right\}$$

Then RM is a submodule of M.

Solution : Let $a, b \in RM$ and $r \in R$.

Then, $\qquad a = \sum_{i=1}^{n} r_i\, m_i, \qquad r_i \in R,\ m_i \in M$ and n is finite.

and $\qquad b = \sum_{i=1}^{k} s_i\, t_i, \qquad s_i \in R,\ t_i \in M$ and k is finite.

(i) $a - b = \sum_{i=1}^{n} r_i m_i - \sum_{i=1}^{k} s_i t_i$

$= r_1 m_1 + r_2 m_2 + \cdots + r_n m_n + (-s_1) t_1 + (-s_2) t_2 + \cdots + (-s_k) t_k$

$\in RM$ as $r_i \in R$, $(-s_i) \in R$ and the sum contains at most $n + k$ elements.

(ii) $r \cdot a = r\left(\sum_{i=1}^{n} r_i m_i\right)$

$= \sum_{i=1}^{n} r (r_i m_i)$

$= \sum_{i=1}^{n} (r r_i) m_i$

as $r r_i \in R$ (for each i) we get $r \cdot a \in RM$.

Thus, from (i) and (ii), we get, RM is a R-submodule of M.

Theorem 1.2.8 : Let M be an R-module. For any two submodules N_1 and N_2 of M, $N_1 + N_2$ is a submodule of M, containing N_1 and N_2 both.

Proof : $N_1 + N_2 = \{n_1 + n_2 \,/\, n_1 \in N_1, n_2 \in N_2\}$.

Obviously, if $a, b \in N_1 + N_2$ then $a - b \in N_1 + N_2$. (as $\langle N_1, +\rangle$ and $\langle N_2, +\rangle$ are subgroups of an abelian group $\langle M, +\rangle$).

Hence, $\langle N_1 + N_2, +\rangle$ is a normal subgroup of $\langle M, +\rangle$.

Let $a \in R$ and $x \in N_1 + N_2$.

$x \in N_1 + N_2 \quad \Rightarrow \quad x = n_1 + n_2$ for $n_1 \in N_1, n_2 \in N_2$

$ax = a(n_1 + n_2) = a n_1 + a n_2$ (Since n_1, $n_2 \in M$ and M is a R-module)

Now, as N_1 is a R-submodule, $a n_1 \in N_1$.

Similarly,

N_2 is a R-submodule will imply that $a n_2 \in N_2$.

Therefore, $an_1 + an_2 \in N_1 + N_2$.

Thus,

$ax = a n_1 + a n_2 \in N_1 + N_2$, for any $a \in R$ and $x \in N_1 + N_2$.

This shows that $N_1 + N_2$ is a submodule of an R-module M. $n_1 \in N_1$ can be written as $n_1 = n_1 + 0,\ 0 \in N_2$.

Hence, $N_1 \subseteq N_1 + N_2$.

Similarly, $N_2 \subseteq N_1 + N_2$.

More generally, we get,

If $\{N_i\},\ 1 \le i \le k$ is the family of submodules of a module M. Then

$$\sum_{i=1}^{k} N_i = \{x_1 + x_2 + \cdots + x_k / x_i \in N_i,\ 1 \le i \le k\}$$

is the smallest submodule of m containing each $N_i,\ (1 \le i \le k)$

Proof : Let $S = \{x_1 + x_2 + \cdots + x_k / x_i \in N_i,\ 1 \le i \le k\}$. Then $S \neq \phi$ as $N_i \neq \phi \quad \forall\ i$.

(I) (i)If $x_1 + x_2 + \cdots + x_k$ and $y_1 + y_2 + \cdots + y_k$ are elements of S, then

$$\begin{aligned}(x_1 + x_2 + \cdots + x_k) - (y_1 + y_2 + \cdots + y_k) \\ &= (x_1 - y_1) + (x_2 - y_2) + \cdots + (x_k - y_k) \\ &\in S \qquad \text{as } (x_i - y_i) \in N_i \text{ for each } i,\ 1 \le i \le k\end{aligned}$$

(ii) Further if $r \in R$ and $x_1 + x_2 + \cdots + x_k \in S$ then

$$\begin{aligned}r \cdot (x_1 + x_2 + \cdots + x_k) &= r \cdot x_1 + r \cdot x_2 + \cdots + r \cdot x_k \\ &\in S, \qquad \text{as } r \cdot x_i \in N_i \text{ for each } i,\ 1 \le i \le k\end{aligned}$$

Thus, from (i) and (ii), S is a submodule of M.

(II) Let $x \in N_i$ then $x = 0 + 0 + \cdots + 0 + x + 0 + \cdots + 0$

$\uparrow i^{th}$ place

Hence, $x \in S$. This shows that $N_i \subseteq S$.

Thus, we get, $N_i \subseteq S \qquad \forall\ i,\ 1 \le i \le k$.

Hence, $\sum_{i=1}^{k} N_i \subseteq S$, S being a submodule of M.

(III) Let T is any other submodules o M containing each N_i, $1 \le i \le k$. Then obviously $S \subseteq T$.

From (I), (II) and (III) we get, S is the smallest submodule of M containing each N_i, $1 \le i \le k$.

Hence, $\quad S = \sum_{i=1}^{k} N_i$.

Theorem 8.2.9 : Let M be an R-module. If N_1 and N_2 are R-submodules of M, then $N_1 \cap N_2$ is a submodule of M.

Proof : As $0 \in N_1 \cap N_2$, we get $N_1 \cap N_2 \neq \phi$.

Let $x, y \in N_1 \cap N_2$ then $x, y \in N_1$ and N_1 is a submodule of M will give $x - y \in N_1$. Similarly,

$x, y \in N_2$ and N_2 is a submodule of M will give $x - y \in N_2$.

Thus, $x, y \in N_1 \cap N_2 \implies x - y \in N_1 \cap N_2$

Again, for any $r \in R$ and any $x \in N_1 \cap N_2$, we get,

$rx \in N_1$ and $rx \in N_2$, as N_1 and N_2 are submodules of M.

But then $rx \in N_1 \cap N_2$.

Thus, $x - y \in N_1 \cap N_2$, for all $x, y \in N_1 \cap N_2$

and $rx \in N_1 \cap N_2$, for all $x \in N_1 \cap N_2,\ r \in R$

Hence, $N_1 \cap N_2$ is a R-submodules of M.

Remark 1.2.10 : More generally, any arbitrary intersection of R-submodules of a given R-module M is a R-submodules of M.

i.e. if $\{N_\alpha \ / \ \alpha \in \Delta\}$ is a family of R-submodules of a given R-submodule M, then

$\bigcap\limits_{\alpha \in \Delta} N_\alpha$ is a $\mathrm{R-submodule\ of\ M}$.

Theorem 1.2.11 : A, B, C are R-submodules of an R-submodule M such that $A \subseteq B$. Then

$$A + (B \cap C) = B \cap (A + C)$$

Proof : As $A \subseteq B$ and $A \subseteq A + C$, we get,

$$A \subseteq B \cap (A + C) \qquad \ldots (1)$$

Again, $B \cap C \subseteq B$ and $B \cap C \subseteq C$ and $C \subseteq A + C$ will imply

$$B \cap C \subseteq B \cap (A + C) \qquad \ldots (2)$$

From (1) and (2), we get,

$$A + (B \cap C) \subseteq B \cap (A + C) \qquad \ldots (\mathrm{I})$$

(Since A and $B \cap C$ are normal subgroups of $\langle M, + \rangle$)

Now, let $x \subset B \cap (A + C)$ then $x \subset B$ and $x \subset A + C$.

Hence, $x = a + c$, for some $a \subset A$ and $c \subset C$

$a \in A$ and $A \subseteq B \implies a \in B$

$x \in B$ and $a \in B \implies x - a \in B$ (Since B is submodule)

Thus, c = x – a will imply $c \in B$. But then x = a + c will imply $x \in A + (B \cap C)$.

As $a \in A$ and $c \in B \cap C$.

This shows that

$$B \cap (A + C) \subseteq A + (B \cap C) \qquad \ldots \text{(II)}$$

From (I) and (II), we get

$$A + (B \cap C) = B \cap (A + C)$$

Worked Examples 1.2.12

Example 1 : Show by an example that union of any two submodules of an R-module need not be a submodule.

Solution : Consider Z as Z-module and let

$$N_1 =< 2 >= \{0, \pm 2, \pm 4, \ldots\}$$

$$N_2 =< 3 >= \{0, \pm 3, \pm 6, \ldots\}$$

Then N_1 and N_2 are submodules of the Z-module Z but $N_1 \cup N_2$ is not a Z-module.

Example 2 : Show that union of any chain of submodules of a given R-module M is a R-submodule of M.

Solution : Let $N_1 \subseteq N_2 \subseteq \cdots$ be any chain of submodules of a given R-module M. to prove that $\bigcup\limits_{i=1} N_i$ is a submodule of M.

(i) Obviously, $\bigcup\limits_{i=1} N_i \neq \phi$.

(ii) Let $a, b \in \bigcup\limits_{i=1} N_i$. Then $a \in N_i$ and $b \in N_j$ for some *i* and *j*.

If $i \leq j$ then $N_i \subseteq N_j$ and hence $a, b \in N_j$ is a submodule of M, $a - b \in N_j$ and hence

$$a - b \in \bigcup_{i=1} N_i.$$

(iii) Let $r \in R$ and $a \in \bigcup\limits_{i=1} N_i$ implies $a \in N_i$ for some *i*.

As N_i is a submodule of M, $ra \in N_j$ and hence $ra \in \bigcup\limits_{i=1} N_i$.

From (i), (ii) and (iii) we get $\bigcup\limits_{i=1} N_i$ is a submodule of M.

Example 3 : Give examples of three R-submodules A, B, C such that

$$A \cap (B + C) \neq (A \cap B) + (A \cap C)$$

Solution : Consider the module $\mathbb{R}^{(2)}$ over $\mathbb{R}$. [$\mathbb{R}^{(2)}$ is a vector space over the field $\mathbb{R}$].

Let $B = \{(x, 0)/ \, x \in \mathbb{R}\}$, $C = \{(0, y)/ \, y \in \mathbb{R}\}$ and $A = \{(z, z) \, / \, z \in \mathbb{R}\}$

Clearly, A, B, C are submodules of the R-module $\mathbb{R}^{(2)}$.

Then, $B + C = \mathbb{R}^{(2)}$

and $A \cap (B + C) = A \cap \mathbb{R}^{(2)} = A$ . . . (I)

Now, $A \cap \mathrm{B} = (0, 0)$ and $A \cap C = (0, 0)$

Hence,

$$(A \cap B) + (A \cap C) = \{(0, 0)\} \quad \text{. . . (II)}$$

Hence, from (I) and (II), we get,

$$A \cap (B + C) \neq (A \cap B) + (A \cap C)$$

Definition 1.2.13 : Simple Module :

A R-module M is called simple if its only submodules are $\{0\}$ and M.

Theorem 1.2.14 : Let R be a ring with unity. Let $M \neq \{0\}$, be am R-module. Then M is simple iff M = Rx for any $x \neq 0$ in M.

Proof : **Only if part :**

Let M be a simple R-module. Let $x \neq 0$. Then $Rx = \{rx \, / \, r \in R\}$ is a submodule of M containing x. (See remark (1) of example 2).

As $Rx \neq \{0\}$ and as M is a simple module, Rx = M. Thus M = Rx for any $x \neq 0$ in M.

If part :

Let M = Rx for each $x \neq 0$ in M.

To prove that M is a simple module.

Let N be a nonzero submodule of M. Select any $x \neq 0$ in N.

Then by assumption, M = Rx. As $x \in N$ we get $Rx \subseteq N$

i.e. $M \subseteq N$ and hence N = M.

This shows that M is a simple module.

We know that intersection of any number of submodules of a given R-module M is a submodule of M. as any non-empty subset S of an R-module M need not be a R-module, we introduce the concept of submodule generated by S.

Definition 1.2.15 : Let S be any nonempty subset of an R-module M. The submodule generated by S in M is the smallest submodule of M containing S.

This is denoted by $\langle S \rangle$.

Thus,

$$\langle S \rangle = \cap\{N \,/\, N \text{ is a submodule containing S}\}$$

If $S = \{x_1, x_2, \dots, x_n\}$ is a finite set, then $\langle S \rangle$ is also written as $\langle x_1, x_2, \dots, x_n \rangle$.

Definition 1.2.16 : An R-module M is called finitely generated if $M = \langle x_1, x_2, \dots, x_n \rangle$ for each $x_i \in M,\ 1 \le i \le n$.

The elements $x_1, x_2, \dots, x_n$ are said to generate M.

Definition 1.2.17 : An R-module M is called a cyclic module if $M = \langle x \rangle$, for some $x \in M$.

Theorem 1.2.18 : Let M be an R-module. Let $M = \langle x_1, x_2, \dots, x_n \rangle$. Then

$$M = \{r_1x_1 + r_2x_2 + \cdots + r_nx_n \,/\, r_i \in R, 1 \le i \le n\}$$

In this case we write $M = \sum_{i=1}^{n} Rx_i$.

Proof : Let $S = \{r_1x_1 + r_2x_2 + \cdots + r_nx_n \,/\, r_i \in R, 1 \le i \le n\}$ then S is a submodule of M.

$1 \in R \quad \Longrightarrow \quad 1 \cdot x_i \in Rx_i$ for each $i, 1 \le i \le n$.

Again $Rx_i \subseteq S$ for each $i, 1 \le i \le n$.

Hence $x_i \in S$ for each $i, 1 \le i \le n$.

If N is any other submodule containing $\{x_1, x_2, \dots, x_n\}$ then by the definition of submodule it follows that

$$r_1x_1 + r_2x_2 + \cdots + r_nx_n \in N \text{ for } r_i \in R$$

This will imply $S \subseteq N$.

Thus, we have proved that S is the submodule of M containing $\{x_1, x_2, \dots, x_n\}$.

Hence, $\langle x_1, x_2, \dots, x_n \rangle = S$.

Hence, by data $M = S$.

Remark 1.2.19 : The set of generators of a module need not be unique.

Let $M = \{f(x) \in F[x] \,/\, \text{degree of } f(x) \le n\}$. Then M is a vector space over the field. Then both $\{1, x, x^2, \dots, x^n\}$ and $\{1, 1 + x, x^2, \dots, x^n\}$ will generate M.

Definition 1.2.20 : Quotient Modules :

Let M be an R-module and N be a submodule of M. Then $\langle N, +\rangle$ is a normal subgroup of $\langle M, +\rangle$ and hence consider

$$\frac{M}{N} = \text{the set of cosets [right / left] of N in M}$$

$$= \{m + n \ / \ m \in M\}$$

Define addition and the Scalar multiplication on $\frac{M}{N}$ by

(i) $(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$

(ii) $r \cdot (m + N) = r \cdot m + N$

for $m_1,\ m_2, m \in M$ and $r \in R$.

Then it can be easily verified that $\langle\frac{M}{N}, +,\ \cdot\rangle$ is a R-module. This R-module is called the quotient module of M by the submodule N.

Definition 1.2.21 : Submodule Generated by A :

Let M be an R-module and let $A \subseteq M$. The smallest submodule of M containing the set A is called the submodule generated by A and is denoted by $\langle A\rangle$. Thus,

$$\langle A\rangle = \ \cap\ \{N \ / \ N \text{ is a submodule of M such that } A \subseteq N\} \qquad \ldots (1)$$

As M is a submodule of M containing A the family of sets representing R.H.S. of (1) is non empty.

1.3 Homomorphism :

Definition 1.3.1 : Let M and N be R-modules. A mapping $f: M \longrightarrow N$ is called R-homorphism or a module homorphism if it satisfy the following conditions.

(i) $f(x + y) = f(x) + \ f(y)$

(ii) $f(rx) = r \cdot f(x)$

for all $x, y \ \in M$ and $r \ \in R$.

Remarks 1.3.2:

(i) If $f: M \longrightarrow N$ is a module homorphism, then $f(0) = 0$, $f(-x) \ = \ -f(x)$ and hence

$$f(x - y) = f(x) - f(y)\ , \qquad \text{for } x, y \ \in M.$$

(ii) The collection of all R-homorphisms $f: M \longrightarrow N$ is denoted by Hom (M, N).

(iii) A R-homorphism $f: M \longrightarrow M$ is called an endomorphism on M and the set of endomorphism on M is denoted by $end_R(M, M)$.

Examples 1.3.3 :

Ex 1. Let M and N be R-modules and define $f: M \longrightarrow N$ by f(m) = 0 for each $m \in M$. Then f is an R-homomorphism and is called a zero homorphism.

Ex 2. Let M be an R-module. Define $i : M \longrightarrow M$ by $i(m) = m$ for each $m \in M$. Then the identity map is an R-endomorphism.

Ex 3. Let R be a commutative ring and let M be an R-module. Fix up any $r \in R$. Define the map $f : M \longrightarrow M$ by

$$f(m) = r \cdot m, \qquad \text{for each } m \in M$$

Then f is an endomorphism.

Solution : Let $m_1, m_2 \in M$.

Then $f(m_1 + m_2) = r \cdot (m_1 + m_2)$

$= rm_1 + rm_2$

Thus, $f(m_1 + m_2) = f(m_1) + f(m_2)$

Again for $m_1 \in M$ and $r_1 \in R$ we get,

$$\begin{aligned} f(r_1 m_1) &= r \cdot (r_1\, m_1) \\ &= (r \cdot r_1)\, m_1 \\ &= (r_1 \cdot r)\, m_1 && \text{... Since R is commutative.} \\ &= r_1 \cdot (r\, m_1) \\ &= r_1 \cdot f(m_1) \end{aligned}$$

Thus, $f(m_1 + m_2) = f(m_1) + f(m_2)$

and $f(r_1 m_1) = r_1 \cdot f(m_1)$ ... for all $m_1, m_2 \in M, r_1 \in R$

Hence, f is an R-endomorphism.

Ex 4. Let R be a ring. Consider the module $R^{(n)}$ over R and the ring R as an R-module. (See 1.1.4 problem 4). Define $f : R^{(n)} \longrightarrow R$ by

$$f(x_1, x_2, \dots, x_n) = x_i \qquad \text{for a fixed } i,\ 1 \le i \le n$$

Then f is a R-homomorphism.

Solution : Let $(x_1, x_2, \dots, x_n) \in R^{(n)}$ and $(y_1, y_2, \dots, y_n) \in R^{(n)}$.

Then

$$\begin{aligned} f\,[(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n)] &= f\,[(x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)] \\ &= x_i + y_i \end{aligned}$$

$$= f\ (x_1, x_2, \dots, x_n) + f(y_1, y_2, \dots, y_n)$$

Further for any $r \in R$ and $(x_1, x_2, \dots, x_n) \in R^{(n)}$ we get

$$f\ [r \cdot (x_1, x_2, \dots, x_n)] = f(rx_1, rx_2, \dots, rx_n)$$
$$= r \cdot x_i$$
$$= r \cdot f(x)$$

Thus,

$$f\ [(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n)] = f\ (x_1, x_2, \dots, x_n) + f(y_1, y_2, \dots, y_n)$$

and $\quad f\ [r \cdot (x_1, x_2, \dots, x_n)] = r \cdot f(x_1, x_2, \dots, x_n)$

... for all $(x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \in R^{(n)}, \ \ r \in R$

Hence, f is a R-homomorphism.

Ex 5. Let M be R-module and N be R-submodule of M. Define $f: M \longrightarrow \dfrac{M}{N}$ by

$$f(m) = m + N$$

Then f is an epimorphism.

Solution : For $m_1, m_2 \in M$ we get

$$f(m_1 + m_2) = (m_1 + m_2) + N \qquad \text{... by definition of } f$$
$$= (m_1 + N) + (m_2 + N) \qquad \text{... by definition of + in } \frac{M}{N}$$
$$= f(m_1) + f(m_2) \qquad \text{... by definition of } f$$

Further, for any $r \in R$ and $m \in M$ we get

$$f(rm) = rm + N \qquad \text{... by definition of } f$$
$$= r\ (m + N) \qquad \text{... by definition of} \cdot \text{in } \frac{M}{N}$$
$$= r\ f(m) \qquad \text{... by definition of } f$$

Thus, $\quad f(m_1 + m_2) = f(m_1) + f(m_2)$

and $\quad f(rm) = r\ f(m) \qquad$ ... for all $m_1,\ m_2, m \in M,\ \ r \in R$

Hence, f is a R-homomorphism.

Clearly, f is onto as for $m + N \in \dfrac{M}{N}$, we get $m \in M$ and $f(m) = m + N$.

Thus, f is an epimorphism.

Remark :

(i) This epimorphism $f: M \longrightarrow \dfrac{M}{N}$ defined by $f(m) = m + N$ is called a natural or canonical homomorphism.

(ii) Any quotient module $\frac{M}{N}$ of M by the submodule N is always a homomorphic image of M under the canonical mapping.

Theorem 1.3.4 : Let M be an R-module and let N be R-submodule of M. The submodules of the quotient module $\frac{M}{N}$ are of the form $\frac{U}{N}$, where U is a submodule of M containing N.

Proof : Let $f: M \longrightarrow \frac{M}{N}$ be the canonical mapping. We know that f is an onto homomorphism (1.2, example 5). Hence $\frac{M}{N} = f(M) = \{f(m)/\, m \in M\}$.

Let T be an R-submodule of $\frac{M}{N}$. Define

$$U = \{x \in M \,/\, f(x) \in T\}$$

<u>Claim 1 :</u> U is a R-submodule of M.

(i) $U \neq \phi$ as $T \neq \phi$.

(ii) Let $x, y \in U$. Then $f(x), f(y) \in T$.

As T is a submodule of $\frac{M}{N}$, $f(x) - f(y) \in T$.

f being a homomorphism,

$$f(x) - f(y) \in T \qquad \Rightarrow \qquad f(x-y) \in T$$

By the definition of U, we get $x - y \in U$.

(iii) Let $r \in R$ and $x \in U$. Then $f(x) \in T$.

f being an homomorphism,

$$f(rx) = r\, f(x)$$

As $f(x) \in T$ and $r \in R$

$$r \cdot f(x) \in T, \qquad \text{T being a submodule of } \frac{M}{n}.$$

i.e. $\qquad f(rx) \in T$.

This gives $rx \in U$.

Form (i), (ii) and (iii) it follows that U is a R-submodule of M.

<u>Claim 2 :</u> $N \subseteq U$.

Let $n \in N$. Then $f(n) = n + N = N \in T$. (Since N is the identity element of $\frac{M}{N}$ and T is a submodule of $\frac{M}{n}$).

But then, by the definition of U, $n \in U$ and hence $N \subseteq U$.

Claim 3 : T = f (U)

Let $\qquad x + N \in T$.

As $\qquad x \in M$ and $f(x) = x + N \in T$, we get $x \in U$.

But this shows $f(x) \in f(U)$.

Thus,

$$x + N \in T \quad \Rightarrow \quad f(x) \in T \quad \Rightarrow \quad f(x) \in f(U).$$

Hence $\qquad T \subseteq f(U)$.

As $\qquad f(U) \subseteq T$,

By the definition of U, we get T = f (U).

From claims 1, 2 and 3, for any submodule T of the quotient module M, there exists a submodule U of the module M, containing N and with f (U) = T.

But f being a canonical mapping, $f(U) = U + N$.

Hence, $\qquad T = f(U) \Rightarrow T = U + N$.

Thus, any submodule T of $\frac{M}{N}$ is of the form $\frac{U}{N}$, where U is a submodule of M containing N.

This completes the proof.

Definition 1.3.5 : Let M and N be R-modules. Let $f: M \longrightarrow N$ be a R-homomorphism.

The set

$$\ker f = \{m \in M \,/\, f(m) = 0\}$$

is called the kernel of the homomorphism f and the set

$$\operatorname{im} f = \{f(m) \in N \,/\, m \in M\}$$

is called the image of f.

Theorem 1.3.6 : For any module homomorphism $f: M \longrightarrow N$, $kerf$ is a submodule of the module M and im f is a submodule of the module N.

Proof :

(I) To prove that $kerf$ is a submodule of the module M.

(i) $\quad kerf \neq \phi$ as $f(0) = 0$ implies $0 \in kerf$.

(ii) $\quad$ Let $m_1, m_2 \in kerf$. Then $f(m_1) = 0, \ f(m_2) = 0$.

$f(m_1 - m_2) = f(m_1 + (-m_2))$

$= f(m_1) + f(-m_2)$ ... $\because$ f is a homomorphism

$= f(m_1) - f(m_2)$ ... $f(-x) = -f(x)$ for all $x \in M$

$= 0 - 0$ ... $\because$ $m_1,\ m_2 \in kerf$

$= 0$

But $f(m_1 - m_2) = 0$ implies $m_1 - m_2 \in kerf$.

Thus, $m_1 - m_2 \in kerf$, for $m_1,\ m_2 \in kerf$.

(iii) Let $m \in kerf$ and $r \in R$.

Then,

$f(r\, m) = r\ \cdot f(m)$ ... $\because$ f is a homomorphism

$= r \cdot 0$ ... $\because m \in kerf$

$= 0$ ... See 1.1.3 theorem 1

Thus, $f(r\, m) = 0$ implies $rm \in kerf$.

Thus, $rm \in kerf$, for $r \in R$ and $m \in M$.

From (i), (ii) and (iii), we get $kerf$ is a R-submodule of M.

(II) To prove that imf is a submodule of N.

(i) $imf \neq \phi$ as $M \neq \phi$.

(ii) Let $f(m_1,),\ f(m_2) \in im\, f$.

$f(m_1) \in im\, f \implies m_1 \in M$.

$f(m_2) \in im\, f \implies m_2 \in M$.

As M is a module, $m_1 - m_2 \in M$. But then $f(m_1 - m_2) \in imf$.

f being an homomorphism,

$$f(m_1 - m_2) = f(m_1) - f(m_2)$$

Thus, $f(m_1,),\ f(m_2) \in im\, f$ will imply $f(m_1) - f(m_2) \in im\, f$

(iii) Let $f(m) \in im\, f$ and $r \in R$. But then $rm \in M$ as $m \in M$, $r \in R$ and M is an R-module.

Hence, $f(rm) \in im\, f$.

As f is a homomorphism, $f(rm) = r\, f(m)$.

Thus, given $f(m) \in im\, f$ and $r \in R$ we get

$r\, f(m) \in im\, f$.

From (i), (ii) and (iii), we get, $im\, f$ is a R-submodule of N.

Theorem 1.3.7 : Let M and N be R-modules and let $f: M \longrightarrow N$ be R-homomorphism. Then f is one-one iff $kerf = \{0\}$.

Proof : **<u>Only if part :</u>**

Let f be one-one.

To prove that $\ker f = \{0\}$. Let $x \in \ker f$. Then

$$x \in \ker f \quad \Rightarrow \quad f(x) = 0$$
$$\Rightarrow \quad f(x) = f(0)$$
$$\Rightarrow \quad x = 0 \qquad \text{... as } f \text{ is one-one.}$$

Thus, $\ker f = \{0\}$.

<u>If part :</u>

Let $f: M \longrightarrow N$ be R-homomorphism such that $\ker f = \{0\}$.

To prove that f is one-one.

Let $f(x) = f(y)$ for some $x, y \in M$.

$$f(x) = f(y) \quad \Rightarrow \quad f(x) - f(y) = 0$$
$$\Rightarrow \quad f(x - y) = 0$$
$$\Rightarrow \quad x - y \in ker\, f$$
$$\Rightarrow \quad x - y \in \{0\}$$
$$\Rightarrow \quad x - y = 0$$
$$\Rightarrow \quad x = y$$

Thus, $f(x) = f(y) \quad \Rightarrow \quad x = y$

Hence, f is one-one.

Definition 1.3.8 : Let $f : M \longrightarrow N$ be a module homomorphism. If f is both one-one and onto we say f is an R-isomorphism or module isomorphism.

Remark 1.3.9 :

(i) If $f : M \longrightarrow M$ is an module isomorphism then $f^{-1} : N \longrightarrow M$ is also a module isomorphism.

(ii) Any two R-modules M and N are said to be isomorphic if there exists an module isomorphism $f: M \longrightarrow N$. In this case we write $M \cong N$.

(iii) The relation $\cong$ (being isomorphic) defined on the set of all R-modules is an equivalence relation.

Theorem 1.3.10 : Let M be a simple R-module. Any non zero homomorphism defined on M is an isomorphism.

Proof : Let $f: M \longrightarrow M$ be R-homomorphism where M is a simple R-module.

To prove that f is an isomorphism.

(I) We know that $ker\, f$ is a sub module of M.

M being simple, $ker\, f = \{0\}$ or $ker\, f = M$.

As f is a non zero homomorphism, $kerf \neq M$.

Therefore, $ker\, f = \{0\}$.

But then f is one-one. (see Theorem 2).

(II) By Theorem 1, $im\, f$ is a submodule of M.

M being simple, $im\, f = \{0\}$ or $im\, f = M$.

As f is a non zero homomorphism, $im\, f \neq \{0\}$.

Therefore, $im\, f = M$.

But then in this case f is onto.

From (I) and (II), we get the non zero homomorphism is both one-one and onto.

Hence, f is an isomorphism.

- ***Shur's Lemma :***

Theorem 1.3.11 : Let M be a simple R-module. Then

$$Hom_R(M, M) = \{f: M \longrightarrow M \,/\, f \text{ is a R} - \text{homomorphism}\}$$

is a division ring.

Proof :

(I) To prove $Hom_R(M, M)$ is a ring under ' $+$ ' and ' $\cdot$ ' defined by

$$(f + g)(x) = f(x) + g(x)\,, \qquad \forall \quad x \in M$$

and $$(f \cdot g)(x) = f\,[g(x)]\,, \qquad \forall \quad x \in M$$

for all $f,\ g \in Hom_R(M, M)$.

(i) $f + g \in Hom_R(M, M)$, for $f,\ g \in Hom_R(M, M)$

$f: M \longrightarrow M$ and $g: M \longrightarrow M$. Hence, $f + g : M \longrightarrow M$ and is well defined map.

Let $x,\ y \in M$. Then, we have

$(f + g)(x + y) = f(x + y) + g(x + y)$ .... By definition of $f + g$.

$= [f(x) + f(y)] + [g(x) + g(y)]$

.... Since f and g are R-homomorphism.

$= [f(x) + g(x)] + [f(y) + g(y)]$

.... Since $< M, +>$ is an abelian group.

$= (f + g)(x) + (f + g)(y)$ .... By definition of $f + g$.

Again, let $r \in R$ and $x \in M$.

$(f + g)(rx) = f\ (rx) + g\ (rx)$ .... By definition of $f + g$.

$= r\ [f(x)] + r\ [g(x)]$ .... Since f and g are R-homomorphism.

$= r\ [f(x) + g(x)]$

$= r\ (f + g)\ (x)$

Thus, we get,

$$(f + g)(x + y) = (f + g)(x) + (f + g)(y)$$

and $(f + g)(rx) = r\ (f + g)\ (x)$

for all $x, y \in M$ and $r \in R$.

This shows that $(f + g)$ is a R- homomorphism and hence $(f + g) \in Hom_R(M, M)$, for $f, g \in Hom_R(M, M)$.

(ii) To prove $f \circ g \in Hom_R(M, M)$ for $f, g \in Hom_R(M, M)$

$f \circ g$ is well defined map. $f + g : M \longrightarrow M$.

Let $x,\ y \in M$. Then we have

$(f \circ g)(x + y) = f[g(x + y)]$ .... By definition of $f \circ g$.

$= f\ [g(x) + g(y)]$ .... Since g is a homomorphism.

$= f\ [g(x)] + \ f\ [g(y)]$ .... Since f is a homomorphism.

$= (f \circ g)(x) + (f \circ g)(y)$ .... By definition of $f + g$.

Again for any $r \in R$ and $f \in Hom_R(M, M)$, we get

$(f \circ g)(rx) = f\ [g\ (rx)]$ .... By definition of $f + g$.

$= f\ [r \cdot g(x)]$ .... Since g is a R-homomorphism.

$= r\ \cdot [f(g(x))]$ .... Since f is a R-homomorphism.

$= r\ (f \circ g)\ (x)$

Thus, we get

$$(f \circ g)(x + y) = (f \circ g)(x) + (f \circ g)(y)$$

and $(f \circ g)(rx) = r[\ (f \circ g)\ (x)]$

for all $x, y \in M$ and $r \in R$.

Hence, $(f \circ g) \in Hom_R(M, M)$.

(iii) $< Hom_R(M, M), +>$ is an abelian group where the zero mapping $0: M \longrightarrow M$ defined by $0(x) = 0$ will be the ideal element w. r. t. '+' in $Hom_R(M, M)$.

Let $f \in Hom_R(M, M)$.

Define $(-f) : M \longrightarrow M$ by

$$(-f)(x) = -[f(x], \qquad \forall \quad x \in M$$

Then, it can be easily verified that $(-f)$ is a R-homomorphism defined on M and $(-f)$ will be additive inverse of f in $Hom_R(M, M)$.

(iv) $(f \circ g) \circ h = f \circ (g \circ h)$, $\qquad \forall \quad f, g, h \in Hom_R(M, M)$

(v) Let $f, g, h \in Hom_R(M, M)$ let $x \in M$, then

$$\begin{aligned} f \circ [g + h]\,(x) &= f\,[(g + h)\,(x)] \\ &= f\,[g(x) + h(x)] \\ &= f\,[g(x)] + f\,[h(x)] \\ &= (f \circ g)(x) + (f \circ h)(x)] \\ &= [(f \circ g) + (f \circ h)](x), \qquad \forall \quad x \in M \end{aligned}$$

Hence ,

$$f \circ [g + h] = (f \circ g) + (f \circ h)$$

Similarly, $\qquad (g + h) \circ f = (g \circ f) + (h \circ f) \qquad \forall \quad f, g, h \in Hom_R(M, M)$

From (i), (ii), (iii) and (iv), we get, $\langle Hom_R(M, M), +, \circ \rangle$ is a ring.

(II) The identity mapping $i : M \longrightarrow M$ defined by

$$i(x) = x, \qquad \text{for all } x \in M$$

will be the unity element in $Hom_R(M, M)$.

(III) Let ψ be any non-zero element in $Hom_R(M, M)$.

i.e. ψ is a non-zero R-homomorphism from M into M, where M is a simple module. Hence, ψ must be a bijective and hence ψ is an isomorphism.

But this will show that $\psi^{-1} \in Hom_R(M, M)$.

Thus, we have proved that, any non-zero R-homomorphism defined on M will have a multiplicative inverse in $Hom_R(M, M)$.

From (I), (II) and (III), we get, $Hom_R(M, M)$ is a division ring.

Theorem 1.3.12 : Let M be a R-module and $x \in M$ such that $rx = 0,\ r \in R$ implies $r = 0$. Then $Rx \cong R$ as R-module.

Proof : We know that Rx is a R-submodule and hence Rx is a R-module (See 2.2 example 2). Further R is also an R-module (See 1.2 example 1).

Define $f : R \longrightarrow Rx$ by $f(r) = r \cdot x$.

(I) Then,

(i) $f(r_1 + r_2) = (r_1 + r_2)\,(x)$

$= r_1(x) + r_2(x)$

$= f(r_1) + f(r_2)$

(ii) $f(r \cdot r_1) = (r\,r_1)\,(x)$

$= r\,(r_1 x)$

$= r \cdot f(r_1)$

For all $r, r_1, r_2 \in R$.

Hence, f is a R-homomorphism.

(II) f is onto obviously.

(III) Let $r \in ker\, f$. Then $f(r) = 0$. i.e. $r \cdot x = 0$. But by data $r \cdot x = 0 \quad \Rightarrow \quad r = 0$.

Hence, $ker\, f = \{0\}$. But this will imply f is one-one (See Theorem 2).

Form (I), (II) and (III), f is an isomorphism.

Hence, $R \cong Rx$ as R-module.

1.4 Fundamental Theorem for R-homomorphism and It's Application :

1.4.1 Fundamental Theorem for R-homomorphism :

Any homomorphic image of an R-module M is isomorphic with its suitable quotient module.

Proof : Let M and N be R-module and let N be a homomorphic image of M. Hence there exists an onto homomorphism $f : M \longrightarrow N$. As f is onto $N = f(M)$. Let $K = ker\, f$. Then K is a submodule of M. (See Theorem 1.3.4) and hence the quotient R-module $\frac{M}{K}$ is defined.

Define a $g : \frac{M}{K} \longrightarrow N = f(M)$ by

$$g(m + k) = f(m), \qquad \text{for each } m + k \in \frac{M}{K}$$

(I) g is well defined.

Let $m_1 + k = m_2 + k$ in $\frac{M}{K}$.

Then $m_1, m_2 \in M$ will imply $m_1 - m_2 \in M$.

As $m_1 + k = m_2 + k$ we get $m_1 - m_2 \in M$. i.e. $\quad m_1 - m_2 \in ker\, f$.

Hence $\quad f(m_1 - m_2) = 0$

$\Longrightarrow \quad f(m_1) - f(m_2) = 0$, ... Since f is homomorphism.

$\Rightarrow \quad f(m_1) = f(m_2)$

Thus, we get,

$$m_1 + K = m_2 + K \text{ in } \frac{M}{K} \text{ implies } g(m_1 + K) = g(m_2 + K)$$

This shows that g is well defined.

(II) g is a R-homomorphism.

(i) Let $m_1 + k \in \frac{M}{K}$ and $m_2 + k \in \frac{M}{K}$.

Then,

$g\,[(m_1 + K) + (m_2 + K)] = g\,[(m_1 + m_2)\,K]$ .... by the definition of '+' in $\frac{M}{K}$.

$= f\,(m_1 + m_2)$ .... by the definition of g.

$= f\,(m_1) + f(m_2)$ .... f is homomorphism.

$= g(m_1 + K) + g(m_2 + K)$ .... by the definition of g.

(ii) Let $r \in R$ and $m + K \in \frac{M}{K}$. Then,

$g\,[r\,(m + K)] = g\,[rm + K]$ .... by the definition of '·' in $\frac{M}{K}$.

$= f\,(rm)$ .... by the definition of g.

$= r \cdot f\,(m)$ .... f is homomorphism.

$= r \cdot g\,(m + K)$ .... by the definition of g.

From (i) and (ii), we get, g is a R-homomorphism.

(III) g is one-one.

Let $\quad g\,(m_1 + K) = g(m_2 + K)$ for some $m_1 + k, m_2 + k \in \frac{M}{K}$.

Then $\quad g\,(m_1 + K) = g(m_2 + K)$

$\Rightarrow \quad f\,(m_1) = f(m_2)$ .... by the definition of g.

$\Rightarrow \quad f\,(m_1) - f(m_2) = 0$

$\Rightarrow \quad f\,(m_1 - m_2) = 0$ .... f is homomorphism.

$\Rightarrow \quad m_1 - m_2 \in ker\, f = K$ .... f is homomorphism.

$\Rightarrow \quad m_1 + K = m_2 + K$

Thus, $g\,(m_1 + K) = g(m_2 + K) \quad \Rightarrow \quad m_1 + K = m_2 + K$ and hence g is one-one.

(IV) g is onto.

Let $n \in N$. As $N = f(M)$, there exists some $m \in M$ such that $f(m) = n$. But for this $m \in M,\ m + K \in \frac{M}{K}$ and we get $g(m + K) = f(m) = n$.

This shows that g is onto.

From (I), (II), (III) and (IV), we get, g is an isomorphism. Hence $\frac{M}{k} \cong N$.

This completes the proof.

Theorem 1.4.2: Let A and B be R-submodules of an R-module M. Then $\frac{A+B}{A} \cong \frac{B}{A \cap B}$.

Proof : $A + B = \{a + b \,/\, a \in A,\ b \in B\}$ is a R-module of M and $B \subseteq A + B$. Hence B is a submodule of A + B. (See Theorem 1.2.8).

Hence $\frac{A+B}{A}$ is defined.

$A \cap B$ is a R-module of M (See 2.3 theorem 2) and $A \cap B \subseteq B$. Hence $\frac{B}{A \cap B}$ is defined.

Define $f: A + B \longrightarrow \frac{B}{A \cap B}$ by

$$f(a + b) = b + (A \cap B), \qquad \text{for } a + b \in A + B.$$

(I) f is well defined map.

Let $a_1 + b_1 = a_2 + b_2$ for $a_1,\ a_2 \in A$ and $b_1,\ b_2 \in B$.

Then, $a_1 - a_2 = b_2 - b_1 \in A \cap B$.

As $b_2 - b_1 \in A \cap B$ we have $b_2 + (A \cap B) = b_1 + (A \cap B)$

Thus, $a_1 + b_1 = a_2 + b_2$ will imply $b_1 + (A \cap B) = b_2 + (A \cap B)$ and hence $f(a_1 + b_1) = f(a_2 + b_2)$.

This shows that f is well defined map.

(II) To prove that f is R-homomorphism.

(i) Let $a_1 + b_1$ and $a_2 + b_2$ be any element of $A + B$.

$$f[(a_1 + b_1) + (a_2 + b_2)] = f[(a_1 + a_2) + (b_1 + b_2)]$$

... $\langle M, + \rangle$ is an abelian group.

$= (b_1 + b_2) + (A \cap B)$ ... by the definition of f.

$= [b_1 + (A \cap B)] + [b_2 + (A \cap B)]$

$= f(a_1 + b_1) + f(a_2 + b_2)$

(ii) Let $r \in R$ and $a_1 + b_1 \in A + B$. Then

$f[r\,(a_1 + b_1)] = f[ra_1 + rb_1]$ ... $a_1, b_1 \in M$ and $r \in R$.

$= rb_1 + (A \cap B)$ ... $ra_1 \in A$ and $rb_2 \in B$.

$= r[b_1 + (A \cap B)]$

$= r\, f(a_1 + b_1)$

From (i) and (ii), it follows that f is a R-homomorphism.

(III) f is an onto mapping.

Let $b + (A \cap B) \in \frac{B}{A\cap B}$. Then $b \in B$.

Consider $0 + b$.

Then, as $0 \in A$ we get $0 + b \in A + B$ and $f(0 + b) = b + (A \cap B)$

But this shows that f is onto.

From (I), (II) and (III), f is onto homomorphism.

Hence, the R-module $\frac{B}{A\cap B}$ is a homomorphic image of the R-module $A + B$ under the homomorphism f.

Hence, by fundamental theorem of homomorphism (See 1.4 theorem 5)

$$\frac{A+B}{kerf} \cong \frac{B}{A\cap B} \qquad \ldots (1)$$

Now

$$\begin{aligned} kerf &= \{x \in A + B \;/\; f(x) = 0\} \\ &= \{a + b \in A + B \;/\; f(a + b) = 0\} \\ &= \{a + b \in A + B \;/\; b + (A \cap B) = A \cap B\} \\ &= \{a + b \in A + B \;/\; b \in (A \cap B)\} \\ &= \{a + b / a \in A \text{ and } b \in B\} = A \end{aligned}$$

Thus, $\qquad kerf = A \qquad \ldots (2)$

From (1) and (2), we get,

$$\frac{A+B}{A} \cong \frac{B}{A\cap B}$$

This completes the proof of the theorem.

Theorem 1.4.3: Let A and B be submodule of R-module M and N respectively. Then

$$\frac{M\times N}{A\times B} \cong \frac{M}{A} \times \frac{N}{B}$$

Proof : $M \times N$ is an R-module (See 1.4, problem 2). A is a submodule of an R-module M and hence the quotient R-module $\frac{M}{A}$ is defined. Similarly the quotient R-module $\frac{N}{B}$ is defined. Hence $\frac{M}{A} \times \frac{N}{B}$ is an R-module.

Define the map $f : M \times N \longrightarrow \frac{M}{A} \times \frac{N}{B}$ by

$$f(m,n) = (m+A,\ n+B), \qquad \text{for all } (m,n) \in M \times N$$

(I) f is well defined.

Let $(m_1, n_1) = (m_2, n_2)$ in $M \times N$.

Then, $m_1 = m_2$ and $n_1 = n_2$.

Therefore,

$$m_1 - m_2 = 0 \in A \text{ and } n_1 - n_2 = 0 \in B$$

But then

$$m_1 + A = m_2 + A \qquad \text{and} \qquad n_1 + B = n_2 + B$$

This shows that $(m_1 + A,\ n_1 + B) = (m_2 + A,\ n_2 + B)$

i.e. $f(m_1, n_1) = f(m_2, n_2)$

Hence, f is a well defined map.

(II) f is a homomorphism.

(i) Let $(m_1, n_1),\ (m_2, n_2) \in M \times N$

$f[(m_1, n_1) + (m_2, n_2)]$

$= f[(m_1 + m_2, n_1 + n_2)]$ … by the definition of $+$ in $M \times N$

$= [(m_1 + m_2) + A,\ (n_1 + n_2) + B]$ ... by the definition of f

$= [(m_1 + A) + (m_2 + A),\ (n_1 + B) + (n_2 + B)]$

… by the definition of $+$ in $\frac{M}{A}$ and $\frac{N}{B}$

$= (m_1 + A,\ n_1 + B) + (m_2 + A,\ n_2 + B)$ … by the definition of $+$ in $\frac{M}{A} \times \frac{N}{B}$

$= f(m_1, n_1) + f(m_2, n_2)$ … by the definition of f

(ii) Let $r \in R$ and $(m,n) \in M \times N$. Then

$f[r\,(m,n)] = f[(rm, rn)]$ … by the definition of $\cdot$ in $M \times N$

$= (rm + A,\ rn + B)$ … by the definition of f

$= (r(m + A),\ r(n + B))$ … by the definition of $\cdot$ in $\frac{M}{A}$ and $\frac{N}{B}$

$= r\,(m + A,\ n + B)$ … by the definition of $\cdot$ in $M \times N$

$= r\,f\,(m,\ n)$ … by the definition of f

From (i) and (ii), we get f is homomorphism.

(III) f is onto.

Let $(m + A,\ n + B) \in \frac{M}{A} \times \frac{N}{B}$.

Then obviously, $(m,n) \in M \times N$ and $f(m,n) = (m + A,\ n + B)$.

But this shows that f is onto.

From (I), (II) and (III), it follows that $\frac{M}{A} \times \frac{N}{B}$ is a homomorphic image of $M \times N$.

Hence, by the fundamental theorem of homomorphism,

$$\frac{M \times N}{kerf} \cong \frac{M}{A} \times \frac{N}{B} \qquad \ldots (1)$$

Now,

$$kerf = \{(m,n) \in M \times N \ / \ f(m,n) = 0\}$$
$$= \{(m,n) \in M \times N \ / \ (m + A,\ n + B) = (A, B)\}$$
$$= \{(m,n) \in M \times N \ / \ m + A = A \text{ and } n + B = B\}$$
$$= \{(m,n) \in M \times N \ / \ m \in A \text{ and } n \in B\}$$

Thus, $\quad kerf = A \times B \qquad \ldots (2)$

From (1) and (2), we have,

$$\frac{M \times N}{A \times B} \cong \frac{M}{A} \times \frac{N}{B}$$

This completes the proof.

Let M be an R-module. We know that, if there exists $x \in M$ such that $M = Rx$ then M is called cyclic module generated by x. Here $Rx = \{rx \ / \ r \in R\}$.

e.g. The ring R is a R-module. As $R = R \cdot 1$, we get R is a cyclic module.

Theorem 1.4.4 : Let an R-module M be a cyclic module Rx. Then $M \cong \frac{R}{ann\ x}$.

Proof : $\quad M = Rx = \{rx \ / \ r \in R\}$.

Define $f: R \longrightarrow Rx$ by

$$f(r) = r \cdot x, \qquad \text{for each } r \in R$$

[Here the ring R is considered as an R-module]. Then f is an epimorphism (See 1.3, theorem 5). Hence by the fundamental theorem of homomorphism,

$$\frac{R}{kerf} \cong Rx \qquad \ldots (1)$$

Now,

$$kerf = \{r \in R \ / \ f(r) = 0\}$$
$$= \{r \in R \ / \ rx = 0\}$$

$ker\ f$ is a submodule of an R-module R and hence it is a left ideal of R. This ideal is called the annihilator ideal of x in R and it is denoted by $ann\ x$.

Hence, for a cyclic module $M = Rx$, we get,

$$Rx = M \cong \frac{R}{ann\ x}.$$

Theorem 1.4.5 : Let R be a ring such that $1 \in R$. An R-module M is cyclic iff $M \cong \frac{R}{I}$ for some left ideal I of R.

Proof : <u>Only if part :</u>

Let M be cyclic.

Hence, $M = Rx$ for some $x \in M$. By Theorem 1.4.4, $M \cong \frac{R}{ann\ x}$ where $ann\ x$ is a left ideal in R and thus we get $M \cong \frac{R}{I}$ for left ideal $I = ann\ x$ in R.

<u>If part :</u>

Let $M \cong \frac{R}{I}$, where I is left ideal of R.

$1 \in R \quad \Rightarrow \quad 1 + I \in \frac{R}{I}$.

Further, $\quad R(1 + I) = \{r(1 + I) \,/\, r \in R\}$

$$= \{r + I \,/\, r \in R\}$$

$$= \frac{R}{I}$$

This shows that, $\frac{R}{I}$ is a cyclic module generated by $(1 + I)$. As $M \cong \frac{R}{I}$ and $\frac{R}{I}$ is cyclic, we get, M is a cyclic module (Since isomorphic image of a cyclic module is a cyclic module).

Theorem 1.4.6 : Let R be a ring with unity 1. Let $M \neq (0)$ be an R-module. Then M is simple iff $M \cong \frac{R}{I}$ where I is a maximal left ideal of R.

Proof : <u>Only if part :</u>

Let M be a simple R-module.

As $M \neq (0)$ and M is we get $M = Rx$ for any $x \neq 0$ in M.

As $M = Rx$, a cyclic module then $M \cong \frac{R}{I}$ where I is a left ideal of R. by theorem 1.4.4.

As isomorphic image of a simple module is a simple module, we get $\frac{R}{I}$ is a simple module. Now the submodules of $\frac{R}{I}$ are of the form $\frac{U}{I}$ where U is a submodule of the module R containing I. But the submodules of an R-module R are the left ideals in R. Hence $\frac{R}{I}$ being simple there do not exists any left ideal in R containing I. But this shows that I is a maximal left ideal in R. Hence M is a simple module and $M \neq \{0\}$ will imply $M \cong \frac{R}{I}$, where I is a maximal left ideal in R.

If part :

Let $M \cong \frac{R}{I}$, where I is a maximal left ideal in R. But this in turn will imply that there does not exists any proper ideal in $\frac{R}{I}$. Hence $\frac{R}{I}$ must be a simple R-module.

As $M \cong \frac{R}{I}$, we get M is a simple r-module (since isomorphic image of a simple module is a simple module).

Unit 2 : SUM AND DIRECT SUM OF SUBMODULES :

2.1 Sum of modules

2.2 Direct sum of modules

2.3 Free modules

2.4 Completely reducible modules

2.1 Sum of submodules :

Definition 2.1.1: Let M be an R-module. Let $M_1, M_2, \dots, M_k$ (k finite) be R-submodules of M.

The submodule generated by $\bigcup_{i=1}^{k} M_i$ is called the sum of submodules $M_i,\ 1 \le i \le k$ and is denoted by $M_1 + \cdots + M_k$ or simply $\sum_{i=1}^{k} M_i$.

Note that the submodule generated by $\bigcup_{i=1}^{k} M_i$ is the smallest R-submodule of M, containing each $M_i,\ 1 \le i \le k.$

Theorem 2.1.2 : For the submodules $M_1, M_2, \dots, M_k$ of an R-module M

$$\sum_{i=1}^{k} M_i = \{x_1 + x_2 + \ldots + x_k \,/\, x_i \in M_i\}$$

Proof : Let $T = \{x_1 + x_2 + \ldots + x_k / x_i \in M_i\}$.

(I) $T \neq \phi$ as $M_i \neq \phi$ for each i.

(II) Let $x, y \in T$. Then

$x = x_1 + x_2 + \ldots + x_k$ and $y = y_1 + y_2 + \ldots + y_k$, where $x_i,\ y_i \in M_i$ for each i.

Now,

$$x - y = (x_1 + x_2 + \ldots + x_k) - (y_1 + y_2 + \ldots + y_k)$$
$$= (x_1 - y_1) + (x_2 - y_2) + \cdots + (x_k - y_k)$$

... Since $x_i,\ y_i \in M_i$ for all i and <M, +> is an abelian group.

But as M_i is a submodule of M, $x_i - y_i \in M_i$ for each i.

Hence, $x - y \in T$.

This shows that $x, y \in T \implies x - y \in T$.

(III) Let $x \in T$ and $r \in R$. Then $x = x_1 + x_2 + \cdots + x_n,\quad x_i \in M_i,\ \forall\ i$

Now $rx = r(x_1 + x_2 + \cdots + x_n)$

$$= rx_1 + rx_2 + \cdots + rx_n \qquad \ldots \text{ By the definition of module}$$

As M_i is a R-submodule of M, $r \in R$ and $x_i \in M_i$ will imply $r \cdot x_i \in M_i$ for each i. Hence, $rx \in T$.

Thus, for any $r \in R$ and $x \in T$ we get $rx \in T$.

From (I), (II) and (III), we get, T is a R-submodule of M.

(IV) Let $x_i \in M_i$. Then $0 \in M_i$ for each i will imply,

$$x_i = 0 + 0 + \cdots + \underset{\uparrow\, i^{th} \text{ place}}{x_i} + 0 + \cdots + 0 \quad \in T$$

Hence, $M_i \subseteq T$, for each i, $1 \le i \le k$.

Therefore, $\bigcup_{i=1}^{k} M_i \subseteq T$.

(V) Let J be any other submodule of M containing $\bigcup_{i=1}^{k} M_i$. Then each $M_i \subseteq J$.

Let $x \in T$. Then $x = x_1 + x_2 + \cdots + x_k$ where $x_i \in M_i$ for each i, $1 \le i \le k$. As $M_i \subseteq J$ we get, $x_i \in J$ for each i, $1 \le i \le k$.

Hence, J being a submodule of a module M,

$$x_1 + x_2 + \cdots + x_n \in J, \qquad \text{i.e. } x \in J$$

This shows that $T \subseteq J$.

Thus, we have proved that T is a submodule of an R-module M containing $\bigcup_{i=1}^{k} M_i$ and is the smallest submodule of M containing $\bigcup_{i=1}^{k} M_i$.

Hence, by the definition, $T = \sum_{i=1}^{k} M_i$.

Therefore,

$$\sum_{i=1}^{k} M_i = \{x_1 + x_2 + \ldots + x_k \,/\, x_i \in M_i\}$$

Definition 2.1.3: Let $\{M_\alpha \,/\, \alpha \in \Delta\}$ be any family of submodules of an R-module M. The submodule generated by $\bigcup_{\alpha \in \Delta} M_\alpha$ is called the sum of submodules M_α and is denoted by $\sum_{\alpha \in \Delta} M_\alpha$.

Remark 2.1.4: $\sum_{\alpha \in \Delta} M_\alpha$ is the smallest submodule of an R-module M containing each submodule M_α.

Theorem 2.1.5 : Let $\{M_\alpha \,/\, \alpha \in \Delta\}$ be a family of R-submodules of an R-module M. Then

$$\sum_{\alpha \in \Delta} M_\alpha = \left\{ \sum_{finite} x_i \,/\, x_i \in M_i \right\}$$

Where $\sum_{finite} x_i$ denotes any finite sum of elements of M_i, $\quad i \in \Delta$.

Proof : Define

$$T = \left\{ \sum_{finite} x_i \,/\, x_i \in M_i \right\}$$

As in theorem 1, we can prove that T is a submodule of M containing each M_α, $(\alpha \in \Delta)$ and is the smallest submodule of an R-module M containing each M_α, $(\alpha \in \Delta)$.

Hence, $T = \sum_{\alpha \in \Delta} M_\alpha$.

2.1.6 *Worked Examples*

Example 1 : Let $V = \mathbb{R}^3$ be a vector space over the field $\mathbb{R}$. Let $x_1 = (1,0,0), x_2 = (1,1,0)$, $x_3 = (1,1,1)$. Show that $V = \mathbb{R}x_1 + \mathbb{R}x_2 + \mathbb{R}x_3$.

Solution : We know that $\mathbb{R}x_1$, $\mathbb{R}x_2$ and $\mathbb{R}x_3$ are submodules of an R-module $\mathbb{R}^3$. (Note that every vector space is a module). Hence $\mathbb{R}x_1 + \mathbb{R}x_2 + \mathbb{R}x_3$ is a submodule of $\mathbb{R}^3 = V$. Hence, $\mathbb{R}x_1 + \mathbb{R}x_2 + \mathbb{R}x_3 \subseteq V$. Let $x \in V$ then $(a,b,c) \in V = \mathbb{R}^3$.

Further, $\quad (a,b,c) = (a-b)\,x_1 + (b-c)\,x_2 + c\,x_3$

will imply $\quad x = (a,b,c) \in \mathbb{R}x_1 + \mathbb{R}x_2 + \mathbb{R}x_3$.

By theorem 1.3.4, (as $a,b,c \in R$ we get $a-b, b-c \in R$.

Hence, $(a-b)\,x_1 \in \mathbb{R}x_1$,

$(b-c)\,x_2 \in \mathbb{R}x_2$ and $x_3 \in \mathbb{R}x_3$).

But this shows that $V \subseteq \mathbb{R}x_1 + \mathbb{R}x_2 + \mathbb{R}x_3$.

Combining both the inclusions, we get,

$$V = \mathbb{R}^3 = \mathbb{R}x_1 + \mathbb{R}x_2 + \mathbb{R}x_3$$

2.2 Direct Sum of Submodules :

Definition 2.2.1: Let M be an R-module. Let $M_1,\ M_2, \ldots, M_k$ be submodules of the module M. The sum $\sum_{i=1}^{k} M_i$ is a direct sum if each element $x \in \sum_{i=1}^{k} M_i$ can be uniquely expressed as $x = x_1 + x_2 + \cdots + x_k$, where $x_i \in M_i$ for each i, $1 \leq i \leq k$.

In this case we write $\oplus \sum_{i=1}^{k} M_i$ or $M_1 \oplus M_2 \oplus \ldots \oplus M_k$.

Each M_i is called the direct summand of the direct sum $M_1 \oplus M_2 \oplus \ldots \oplus M_n$.

Theorem 2.2.2 : Let M be an R-module and let $M = M_1 \oplus M_2$.

Then $M_1 \cong \frac{M}{M_2}$ and $M_2 \cong \frac{M}{M_1}$.

Proof : Let $M = M_1 \oplus M_2$. Hence, any $x \in M$ has a unique representation as $x = x_1 + x_2$, where $x_1 \in M_1$ and $x_2 \in M_2$.

Define $f : M \longrightarrow M_1$ by

$f(x) = x_1$

i.e. $f(x_1 + x_2) = x_1$, for each $x \in M$.

By the uniqueness of the expression, f is a well defined map.

(i) Let $x, y \in M$. Let $x = x_1 + x_2$ and $y = y_1 + y_2$ where $x_1,\ y_1 \in M_1$ and $x_2,\ y_2 \in M_2$ be unique expressions of x and y.

$f(x + y) = f(x_1 + y_1 + x_2 + y_2)$

$= f(x_1 + x_2 + y_1 + y_2)$ … Since <M, +> is an abelian group

$= x_1 + y_1$ … $x_1,\ y_1 \in M_1 \implies x_1 + y_1 \in M_1$, M_1 being a submodule.

$= f(x) + f(y)$ … By definition of f.

Thus, $f(x + y) = f(x) + f(y)$ … for all $x,\ y \in M$.

(ii) Now, let $x \in M$ and $r \in R$. Assume that $x = x_1 + x_2$ where $x_1 \in M_1$ and $x_2 \in M_2$.

Then,

$$rx = r(x_1 + x_2) = rx_1 + rx_2$$

As M_1 and M_2 are submodules of M, we get $rx_1 \in M_1$ and $rx_2 \in M_2$.

Hence, by the definition of f,

$$f(rx) = rx_1 = r\, f(x)$$

Thus, $f(rx) = r\, f(x)$ for each $r \in R$ and $x \in X$.

From (i) and (ii), we get, f is a R-homomorphism.

Hence, by the fundamental theorem of homomorphism,

$$\frac{M}{kerf} \cong M_1 \qquad \text{. . . (I)}$$

Now,

$$\begin{aligned} kerf &= \{x \in M \,/\, f(x) = 0\} \\ &= \{x_1 + x_2 \in M \,/\, f(x_1 + x_2) = 0,\ x_1 \in M_1,\ x_2 \in M_2\} \\ &= \{x_1 + x_2 \in M \,/\ x_1 = 0, x_1 \in M_1,\ x_2 \in M_2\} \\ &= \{0 + x_2 \in M \,/\ x_2 \in M_2\} \\ &= M_2 \end{aligned}$$

Thus, $\quad kerf = M_2$ . . . (II)

From (I) and (II), we get,

$$\frac{M}{M_2} \cong M_1$$

Similarly, we can prove that $\frac{M}{M_1} \cong M_2$.

This completes the proof of the theorem.

Theorem 2.2.3 : Let M be an R-module. Let M contains submodules $M_1,\ M_2, \dots, M_k$ having the property,

For each i, $1 \le i \le k$,

$$M_i \cap [M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k] = \{0\} \qquad \text{. . . (A)}$$

Then, the sum $\sum_{i=1}^{k} M_i$ is a direct sum.

Proof : Let $x \in \sum_{i=1}^{k} M_i$, have two expressions say

$$x = x_1 + x_2 + \cdots + x_k$$

and $\quad x = y_1 + y_2 + \cdots + y_k$

where $x_i,\ y_i \in M_i$ for each i, $1 \le i \le k$.

Then, $0 = (x_1 - y_1) + (x_2 - y_2) + \cdots + (x_k - y_k)$.

But this shows that

$$-(x_i - y_i) = \sum_{\substack{j=1 \\ j \neq 1}}^{k} (x_j - y_j) \qquad \ldots (1)$$

As M_i is a submodule of M,

$$-(x_i, - y_i) \in M_i \qquad \ldots (2)$$

Now, $\sum_{\substack{j=1 \\ j \neq 1}}^{k} (x_j - y_j) \in M_1 + M_2 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_k$

From (1), we get,

$$-(x_i, - y_i) \in M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k \ldots (3)$$

From (2) and (3), we have,

$$-(x_i - y_i) \in M_i \cap \left[\sum_{\substack{j=1 \\ j \neq 1}}^{k} M_j \right] = \{0\} \qquad \ldots \text{ by (A)}$$

Hence, $x_i = y_i$.

As this is true for each i, $1 \leq i \leq k$, we get the expression for x is unique.

Hence, the sum $\sum_{i=1}^{k} M_i$ is a direct sum.

Theorem 2.2.4 : Let M be an R-module and let $M_1, \ldots, M_k$ be submodules of an R-module M. The following statements are equivalent.

(i) The sum $\sum_{i=1}^{k} M_i$ is a direct sum.

(ii) For any i, $1 \leq i \leq k$,

$$M_i \cap [M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k] = \{0\}$$

Proof :

(i) ⟹ (ii) :

Let $x \in M_i \cap [M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k]$. Then $x \in M_i$ and

$x = y_1 + y_2 + \cdots + y_{i-1} + y_{i+1} + \cdots + y_k$ where $y_j \in M_j$, $1 \leq j \leq k$.

Thus, we have

$$y_1 + y_2 + \cdots + y_{i-1} + (-x) + y_{i+1} + \cdots + y_k = 0$$

As $0 \in \sum_{i=1}^{k} M_i$ and $\sum_{i=1}^{k} M_i$ is a direct sum, the expression $0 = 0 + 0 + \ldots + 0$ of $0 \in \sum_{i=1}^{k} M_i$ must be unique.

Hence, $-x = 0$, i.e. $x = 0$. This shows that

$$M_i \cap [M_1 + M_2 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k] = \{0\}$$

(ii) ⟹ (i) :

Proof of this implication follows from theorem 1.3.10.

Hence, (i) ⟺ (ii).

Theorem 2.2.5 : Let M be an R-module. Let $M_1, M_2, \ldots, M_k$ be submodules of an R-module M. The following statements are equivalent.

(i) $\sum_{i=1}^{k} M_i$ is a direct sum.

(ii) $0 = \sum_{i=1}^{k} x_i$, $x_i \in M_i \ \forall\ i,\ 1 \le i \le k$

$\Rightarrow$ $x_i = 0$ for each i, $1 \le i \le k$

(iii) $M_i \cap \left[\sum_{\substack{j=1 \\ j \neq 1}}^{k} M_j \right] = \{0\}$

Proof :

(i) ⟹ (ii) :

The implication (i) ⟹ (ii) follows directly by the definition of the direct sum.

(ii) ⟹ (iii) :

Let $x \in M_i \cap \left[\sum_{\substack{j=1 \\ j \neq 1}}^{k} M_j \right]$

Then, $x \in M_i$ and $\in \sum_{\substack{j=1 \\ j \neq 1}}^{k} M_j$.

Hence, $x = y_1 + y_2 + \cdots + y_{i-1} + y_{i+1} + \cdots + y_k$ where $y_i \in M_j$ for $1 \leq j \leq k$ and $j \neq i$.

Therefore,

$$y_1 + y_2 + \cdots + y_{i-1} + (-x) + y_{i+1} + \cdots + y_k = 0$$

by (ii), we get, $-x = 0$. i.e. $x = 0$.

But this shows that

$$M_i \cap \sum_{i=1}^{k} M_i = \{0\}$$

<u>(iii) ⟹ (i) :</u>

The implication (iii) ⟹ (i) follows by the theorem 1.3.10.

Thus, (i) ⟹ (ii) ⟹ (iii) ⟹ (i) and this completes the proof.

2.2.6 Worked Examples

Example 1 : Let M be an R-module and let $M_1, M_2, \ldots, M_k$ be submodules of M such that $M = \sum_{i=1}^{k} M_i$ and the triangular set of conditions

$$M_1 \cap M_2 = \{0\},$$

$$(M_1 + M_2) \cap M_3 = \{0\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(M_1 + \cdots + M_{k-1}) \cap M_k = \{0\}$$

hold. Show that $M = \oplus \sum_{i=1}^{k} M_i$.

Solution : By corollary 6, it is enough to prove that if $x_i \in M_i$ for each i, $1 \leq i \leq k$ and if $x_1 + x_2 + \cdots + x_k = 0$ then $x_i = 0$ for each i, $1 \leq i \leq k$.

$$x_1 + x_2 + \cdots + x_k = 0 \qquad \ldots (1)$$

Hence, $-x_k = x_1 + x_2 + \cdots + x_{k-1}$

As $-x_k \in M_k$ and $x_1 + x_2 + \cdots + x_{k-1} \in \sum_{i=1}^{k-1} M_i$

We get, $\quad -x_k \in M_k \cap [M_1 + M_2 + \cdots + M_{k-1}]$

Hence, $\quad -x_k \in \{0\}$ … by data

Thus, $\quad x_k = 0$ … (2)

Substituting $x_k = 0$ in (1), we get,

$$x_1 + x_2 + \cdots + x_{k-1} = 0$$

Therefore, $\quad -(x_{k-1}) \in [M_1 + M_2 + \cdots + M_{k-2}] \cap M_{k-1} = \{0\}$

Hence, $\quad x_{k-1} = 0$ … (3)

Continuing in this way, we get,

$$x_1 = x_2 = \cdots = x_k = 0$$

Hence, the sum $\sum_{i=1}^{k} M_i$ is a direct sum.

i.e. $\quad M = \oplus \sum_{i=1}^{k} M_i$

Example 2 : Let $V = \mathbb{R}^3$ be a vector space over the field $\mathbb{R}$. Let $x_1 = (1,0,0), x_2 = (1,1,0)$,

$x_3 = (1,1,1)$. Show that $V = \oplus \sum_{i=1}^{3} \mathbb{R}x_i$.

Solution : We have proved that $V = \sum_{i=1}^{3} \mathbb{R}x_i$.

Hence, only to prove that $V = \oplus \sum_{i=1}^{3} \mathbb{R}x_i$.

Let $0 = r_1x_1 + r_2x_2 + r_3x_3$, for some $r_1,\ r_2,\ r_3 \in \mathbb{R}$.

Then,

$$(0,0,0) = r_1(1,0,0) + r_2(1,1,0) + r_3(1,1,1)$$

Hence, $\quad (0,0,0) = (r_1 + r_2 + r_3,\ r_2 + r_3,\ r_3)$.

This shows,

$$r_3 = 0, \qquad r_2 + r_3 = 0, \qquad r_1 + r_2 + r_3 = 0$$

Solving the three equations, we get,

$$r_1 = 0,\ r_2 = 0,\ r_3 = 0.$$

Thus, $\quad 0 = r_1x_1 + r_2x_2 + r_3x_3 \quad \Longrightarrow \quad r_1 = r_2 = r_3 = 0.$

Hence, by corollary 6, we get

$$V = \mathbb{R}x_1 + \mathbb{R}x_2 + \mathbb{R}x_3$$

Example 3 : Let M be an R-module. Let $K \subset N \subset M$ be submodules of M. Show that if N is a direct summand of M, then $\frac{N}{k}$ is a direct summand of $\frac{M}{K}$.

Solution : Let $M = N \oplus N'$. $K \subseteq N$.

$$\frac{M}{K} = \frac{N + N'}{K} = \frac{N}{K} + \frac{N'}{K}$$

$$\frac{N}{K} \cap \frac{N'}{K} = \frac{N \cap N'}{K} = \frac{\{0\}}{K} = \{K\}$$

as $N \cap N' = \{0\}$. Hence,

$$\frac{M}{K} = \frac{N}{K} \oplus \frac{N'}{K}$$

Example 4 : Let M be an R-module. Let $K \subset N \subset M$. If K is a direct summand of N and N is a direct summand of M then K is a direct summand of M.

Solution : Let $N = K \oplus K'$, and $M = N \oplus N'$.

Hence, $M = K \oplus K' \oplus N'$.

Hence, K is a direct summand of M.

Example 5 : M is a R-module. $K \subset N \subset M$ are submodules of M. If K is a direct summand of M, then K is direct summand of N.

Solution : Let $M = K \oplus K'$. $N = M \cap N = (K \oplus K') \cap N$.

Claim : $N = K \oplus (K' \cap N)$

(i) $N = K + (K' \cap N)$

Let $x \in M \quad \Longrightarrow \quad x = K + K'$, $\qquad$ where $k \in K$ and $k' \in K$.

Then, $k \in K = K \cap N$

$\qquad k' = K'$

$x - k = k' \quad \Longrightarrow \quad k' \in N$

Hence, $k' \in K' \cap N$.

Thus, $x = k + k'$, $\; k \in K$ and $k' \in K' \cap N$

$\Longrightarrow \quad x \in K + (K' \cap N)$.

Thus, $N \subseteq K + (K' \cap N)$.

Obviously, $K + (K' \cap N) \subseteq N$.

Hence, $N = K + (K' \cap N)$

(ii) $K \cap (K' \cap N) = \phi$

$K \cap (K' \cap N) = (K \cap K') \cap N = \phi \cap K' \cap N = \phi$.

Since $(K \cap K') = \phi$ as $M = K \oplus K'$.

From (i) and (ii), we get,

$$N = K \oplus (K' \cap N)$$

This shows that K is a direct summand of N.

Example 6 : Let M be a R-module. Let $K \subset N \subset M$. If K is a direct summand of M and if $\frac{N}{K}$ is a direct summand of $\frac{M}{K}$ then N is direct summand of M.

Solution : As K is a direct summand of M, we have

$$M = K \oplus K'.$$

$$\Longrightarrow \quad \frac{N}{K} \cong K \qquad \ldots (1)$$

By example (5), $N = K \oplus (K' \cap N)$

$$\Longrightarrow \quad \frac{N}{K} \cong K' \cap N \qquad \ldots (2)$$

From (1) and (2), we get, if $\frac{N}{K}$ is a direct summand of $\frac{M}{K}$, then $K' \cap N$ must be the direct summand of K'. Hence let us assume that

$$K' = (K' \cap N) \oplus L \qquad \ldots (3)$$

Again$M = K \oplus K'$ will imply

$$M = K \oplus (K' \cap N) \oplus L$$

Hence, $\quad M = N \oplus L$, $\qquad$ (Since $N = K \oplus (K' \cap N)$)

This shows that N is a direct summand of M.

Example 7 : Let $M = K \oplus K' = M = L \oplus L'$. If K = L, then show that $K' \cong L'$.

Solution : Let $m \in M$. Then m can be uniquely expressed by $m = k + s$ where $k \in K$ and $s \in S$

Then,

$$s = m - k \in K'.$$

As $K = L$ we get $m - k \in L'$.

Define $f : K' \longrightarrow L'$ by

$$f(s) = m - k$$

(i) f is well defined.

$$s_1 = s_2$$

Then, $m_1 = k_1 + s_1$.

Let $f(s_1) = m_1 - k_1$ and $f(s_2) = m_2 - k_2$.

Then, $m_1 = k_1 + s_1$ is the unique representation of m_1.

Hence, $s_1 = (m_1 - k_1) = s_2 = m_2 - k_2$ will imply $f(s_1) = f(s_2)$.

Definition 2.2.7 : The sum $\sum_{\alpha \in \Delta} M_\alpha$ of the family $\{M_\alpha \,/\, \alpha \in \Delta\}$ of submodules of an R-module M is a direct sum if each $x \in \sum_{\alpha \in \Delta} M_\alpha$ can be uniquely expressed as $x = \sum x_i$ where $x_i \in M$ and $x_i = 0$ for almost all i.

Generalizing the result of Theorem 2.2.5, we get the following theorem.

Theorem 2.2.8 : Let $\{M_\alpha \,/\, \alpha \in \Delta\}$ be a family of submodules of an R-module M. The following statements are equivalent.

(i) $\sum_{\alpha \in \Delta} M_\alpha$ is a direct sum.

(ii) $0 = \sum_i x_i \in \sum_{\alpha \in \Delta} M_\alpha$, $\Longrightarrow$ $x_i = 0$, for all i

(iii) $M_i \cap \left[\sum_{\substack{i \neq j \\ i, j \in \Delta}}^{k} M_j \right] = \{0\}$

- ***Fundamental Structure Theorem for Finitely generated Modules over P. I. D. :***

Result 2.2.9 : Let D be P.I.D. Any submodule K of the free module $D^{(n)}$ is free with base of $m \leq n$ elements.

Result 2.2.10 : If A is any $m \times n$ matrix with entries in p.i.d. D, then there exits an invertible matrix P of order $m \times m$ with entries in D and an invertible matrix Q with entries in D such that $PAQ = diag\{d_1, d_2, \dots, d_r, 0,0, \dots ,0\}$ where $d_i \neq 0$ and d_i/d_j if $i \leq j$.

- ***Fundamental Structure Theorem :***

Theorem 2.2.11 : Let $M \neq 0$ be a finitely generated module over a p.i.d. D. M is a direct sum of cyclic modules.

$$M = DZ_1 \oplus DZ_2 \oplus \dots \oplus DZ_s$$

such that the order ideals $ann\ Z_i$ satisfy

$$ann\ Z_1 \supset ann\ Z_2 \supset \cdots \supset ann\ Z_s, \qquad \text{where } ann\ Z_k \neq D.$$

Proof : $M \neq (0)$ is a finitely generated D-module. Let $\{x_1, x_2, \dots, x_n\}$ be the set of generators of M.

Then, $$M = Dx_1 + Dx_2 + \cdots + Dx_n.$$

i. e. $$M = \sum_{i=1}^{n} Dx_i$$

We know that, $D^{(n)} = \{(r_1, r_2, \dots, r_n) \,/\, r_i \in D\}$ is a free D-module with base $(e_1, e_2, \dots, e_n)$, where $e_i = (0, 0, \dots, 0, 1, 0, \dots, 0)$.

$\uparrow$ i^{th} place

Define $f : D^{(n)} \longrightarrow M$ by

$$g(x) = g\left(\sum_{i=1}^{n} r_i\, e_i\right)$$

$$= \sum_{i=1}^{n} r_i\, x_i, \quad r_i \in D, \qquad \text{for each } i,\ 1 \leq i \leq n$$

Claim 1 : g is an epimorphism.

(i) g is obviously well defined as $(e_1, e_2, \dots, e_n)$ is a base for $D^{(n)}$ any $x \in D^{(n)}$ can be uniquely expressed as $\sum_{i=1}^{n} r_i\, e_i$ where $r_i \in D$ for each i, $1 \leq i \leq n$.

(ii) g is a homomorphism.

Let $x, y \in D^{(n)}$. Then,

$$x = \sum_{i=1}^{n} r_i\, e_i \qquad \text{and} \qquad y = \sum_{i=1}^{n} r'_i\, e_i$$

where $r_i,\ r_i' \in D$ for each i.

$$g(x+y) = g\left[\sum_{i=1}^{n} r_i\, e_i \; + \; \sum_{i=1}^{n} r_i'\, e_i\right]$$

$$= g\left[\sum_{i=1}^{n} (r_i + r_i')\, e_i\right]$$

$$= \sum_{i=1}^{n} (r_i + r_i')\, x_i \ , \qquad \text{(by the definition of } g\text{)}$$

$$= \sum_{i=1}^{n} r_i\, x_i + \sum_{i=1}^{n} r_i'\, x_i$$

$$= g(x) + g(y)$$

Now, let $r \in D$ and $x = \sum_{i=1}^{n} r_i\, e_i \in D^{(n)}$ with $r_i \in D$.

$$g(r \cdot x) = g\left[r \ \cdot \ \sum_{i=1}^{n} r_i\, e_i\right]$$

$$= g\left[\sum_{i=1}^{n} (r \cdot r_i)\, e_i\right]$$

$$= \sum_{i=1}^{n} (r \cdot r_i)\, x_i \ , \qquad \text{(by the definition of } g\text{)}$$

$$= r \ \cdot \sum_{i=1}^{n} r_i\, x_i$$

$$= r \cdot g(x)$$

Thus, for any $x, y \in D^{(n)}$ and $r \in D$, we get

$$g(x+y) = g(x) + g(y) \qquad \text{and} \qquad g(r \cdot x) = r \cdot g(x)$$

Hence, g is a homomorphism.

As g is obviously onto, we get g is an epimorphism.

Thus, the D-module M is a homomorphic image of the D-module $D^{(n)}$.

Hence, by fundamental theorem of homomorphism,

$$M \cong \frac{D^{(n)}}{kerg}$$

Let $K = kerg$. Then K is a submodule of the free module $D^{(n)}$.

Hence, by Result 2.2.9, K is a free module with base containing m elements, where $m \leq n$.

Let $\{f_1, f_2, \dots, f_m\}$ be the set of generators in term of the base $\{e_1, e_2, \dots, e_n\}$ (as $f_i \in D^{(n)}$ for each i, $1 \leq i \leq n$).

$$f_1 = a_{11}e_{11} + a_{12}e_2 + \cdots + a_{1n}e_n$$
$$f_2 = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n$$
$$\dots \dots \dots$$
$$f_m = a_{m1}e_1 + a_{m2}e_2 + \cdots + a_{mn}e_n$$

Define $\quad A = (a_{ij})$.

Then, A is a matrix of order $m \times n$ with entries in D.

Hence, there exists an invertible matrix $P = (p_{ij})$ of order $n \times n$ and an invertible matrix $Q = (q_{ij})$ of order $m \times m$ such that QAP^{-1} is a diagonal matrix given by,

$diag\,\{d_1, d_2, \dots, d_r, 0,0, \dots, 0\}$ …… By result 2.2.10

Define $\quad e'_i = \sum_{j=1}^{n} p_{ij}\, e_j$. Then $\{e'_1, e'_2, \dots, e'_n\}$ will form an another base for $D^{(n)}$.

Define $\quad f'_k = \sum_{i=1}^{m} q_{kl}\, f_l$. If $Q^{-1} = \left(q^*_{kl}\right)$, then

$$q^*_{kl}\, f'_k = \sum_{k=1}^{m} q^*_{rk}\, q_{kl}\, f_l = f_r$$

But this shows that $\{f_1, f_2, \dots, f_n\}$ is contained in the submodule generated by $\{f'_1, f'_2, \dots, f'_m\}$. Hence $\{f'_1, f'_2, \dots, f'_m\}$ generates K.

Now,

$$f'_k = \sum_{k=1}^{m} q_{kl} f_l = \sum_{l,j} q_{kl}\, a_{lj}\, e_j = \sum_{l,j,i} q_{kl}\, a_{lj}\, p^*_{jl}\, e'_i$$

where $\quad P^{-1} = \left(p^*_{ij}\right)$.

Hence, the new relation matrix is $A' = QAP^{-1}$.

But by the choice of P and Q,

$$QAP^{-1} = diag\,\{d_1, d_2, \dots, d_r, 0,0, \dots, 0\}$$

Hence ,

$$f'_1 = d_1 e'_1, \quad f'_2 = d_2 e'_2, \quad \dots., \quad f'_r = d_r e'_r$$

$$f'_{r+1} = 0, \qquad f'_{r+2} = 0, \quad \ldots., \qquad f'_m = 0 \qquad \ldots (1)$$

Define $\quad y_i = \sum_{j=1}^{n} p_{ij} x_j$.

Then $\quad \sum_{j=1}^{n} p^*_{rk}\, y_k = \sum p^*_{rk}\, p_{ki}\, x_i = x_i$; where $P^{-1} = \left(p^*_{ij}\right)$; shows that the submodule generated by $\{y_1, y_2, \ldots, y_n\}$ contains $\{x_1, x_2, \ldots, x_n\}$.

Hence, $\{y_1, y_2, \ldots, y_n\}$ generates M.

Thus, $M = Dy_1 + Dy_2 + \cdots + Dy_n$

i.e. $\quad M = \sum_{k=1}^{n} Dy_k \qquad \ldots (2)$

Let $\quad \sum_{i=1}^{n} b_i\, y_i = 0$ for $b_i \in D$, $\qquad$ for each $i,\ 1 \le i \le n$.

Consider $g(e'_i)$.

$$f(e'_i) = g\left[\sum_{j=1}^{n} p_{ij}\, e_j\right]$$

$$= \sum_{j=1}^{n} p_{ij}\, x_j \ , \qquad \text{by the definition of } g.$$

$$= y_i.$$

Thus, $\quad g(e'_i) = y_i, \qquad$ for each $i,\ 1 \le i \le n. \qquad \ldots (3)$

Hence, $\quad \sum_{i=1}^{n} b_i\, y_i = 0 \quad \Rightarrow \sum_{i=1}^{n} b_i\, g\left(e'_i\right) = 0$

$$\Rightarrow g\left[\sum_{i=1}^{n} b_i\, e'_i\right] = 0 \qquad \ldots\ g \text{ is a homomorphism}$$

$$\Rightarrow \sum_{i=1}^{n} b_i\, e'_i \in k$$

As $k = (f_1, f_2, \ldots, f_m)$ we get

$$\sum_{i=1}^{n} b_i\, e'_i \ = \ \sum_{i=1}^{m} c_i\, f'_i \ , \qquad \text{for } c_i \in D,\ \ \forall\ i,\ 1 \le i \le m.$$

$$= \sum_{i=1}^{m} c_i \left(d_i e_i^{'}\right), \qquad (\because \quad f_i' = d_i e'_i)$$

Thus, $\displaystyle\sum_{i=1}^{n} b_i e_i^{'} = \sum_{i=1}^{m} \left(c_i d_i\right) e_i^{'}$

$\therefore \quad \displaystyle\sum_{i=1}^{n} \left(b_i - c_i d_i\right) e_i^{'} = 0$

As $\{e'_1, e'_2, \dots, e'_n\}$ forms a base for $D^{(n)}$ we must have

$b_i - c_i d_i = 0.$ i.e. $b_i = c_i d_i$, for $i,\ 1 \le i \le n.$

But $b_i = c_i d_i$ for each i will imply

$$\begin{aligned}
b_i\, y_i &= (c_i\, d_i)\, y_i \\
&= c_i\, (d_i\, y_i) \\
&= c_i\, \big(d_i\ \ g(e'_i)\big) && \dots \text{by 2,} \quad g(e'_i) = y_i \\
&= c_i\, [g(d_i e'_i)] && \dots \text{Since } g \text{ is a homomorphism.} \\
&= c_i\, [g(f'_i)] && \dots \text{by 1.} \\
&= c_i\ \cdot 0 && \dots \text{Since } f'_i \in kerf \\
&= 0
\end{aligned}$$

Hence, $b_i\, y_i = 0$ for each i.

Thus, we have proved that $\displaystyle\sum_{i=1}^{n} b_i\, y_i = 0$ then $b_i\, y_i = 0$, for each $i,\ 1 \le i \le n.$

But this in turn shows that the sum $M = \displaystyle\sum_{i=1}^{n} Dy_i$ is a direct sum.

i.e. $\quad M = \oplus \displaystyle\sum_{i=1}^{n} Dy_i$

Thus, $\quad M = Dy_1 \oplus Dy_2 \oplus \dots \oplus Dy_n.$

Now, $\quad b_i = c_i\, d_i \quad \Rightarrow \quad b_i \in (d_i).$

Again $b_i\, y_i = 0 \quad \Rightarrow \quad (c_i\, d_i)\, b_i \in (d_i)$

$\Rightarrow \quad c_i\, (d_i\, y_i) = 0$

$\Rightarrow \quad d_i\, y_i = 0$

Hence, $\quad ann\, y_i = (d_i).$

As $d_1/d_2,\ d_2/d_3, \dots$ we get,

$$(d_1) \supset (d_2) \supset \cdots \supset (d_n)$$

If d_i is a unit element in D, then $d_i\, y_i = 0 \quad \Longrightarrow \quad y_i = 0$. ($\because$ D is a domain)

Hence, drop those elements y_i from the set $\{y_1, y_2, \dots, y_n\}$ for which $y_i = 0$.

Assume without loss of generality, $d_1, d_2, \dots, d_t$ are units and $d_{t+1}, d_{t+2}, \dots$ are not units in D. Put $Z_1 = y_{t+1}, \dots, Z_{n-t} = y_n$. We get,

$$M = DZ_1 \oplus DZ_2 \oplus \dots \oplus DZ_{n-t}$$

where $DZ_t = (0)$ and

$$ann\, Z_1 \supset ann\, Z_2 \supset \cdots \supset ann\, Z_s$$

where $s = n - t$ and $ann\, Z_k \neq D$.

2.3 Free Module :

Throughout this section R denotes a ring with unity 1.

Definition 2.3.1 : Let M be an R-module. A finite sequence $x_1,\ x_2,\ \dots, x_n$ of distinct elements of M is said to be linearly independent if for any $a_1,\ a_2,\ \dots, a_n$ in R, $\sum_{i=1}^{n} a_i x_i = 0$ implies $a_1 = a_2 = \cdots = a_n = 0$.

A finite sequence $x_1,\ x_2,\ \dots, x_n$ of distinct elements in M is said to be linearly dependent if it is not linearly independent.

A subset S of an R-module is called linearly independent if for every finite sequence of distinct elements of S is linearly independent. Otherwise S is called linearly dependent.

Definition 2.3.2 : Let M be an R-module. A subset B of M is called a basis if

(i) M is generated by B.

(ii) B is linearly independent set.

Example 2.3.3 : Let R be a ring with unity 1. Define $R^{(n)} = \{(x_1,\ x_2,\ \dots, x_n) \,/\, x_i \in R\}$. Then $R^{(n)}$ is an R-module with $\{e_1, e_2, \dots, e_n\}$ as a base, where

$$e_i = (0, 0, \dots, 1, 0, \dots, 0)$$

$\uparrow i^{th}$ place.

Solution : $R^{(n)} = \{(x_1,\ x_2,\ \dots, x_n) \,/\, x_i \in R\}$. Define addition, 0-element and scalar multiplication in $R^{(n)}$ as

$$(x_1,\ x_2,\ \dots, x_n) + (y_1,\ y_2,\ \dots, y_n) = (x_1 + y_1,\ x_2 + y_2,\ \dots, x_n + y_n)$$

$0 = (0, 0, \dots, 0)$

$r \cdot (x_1, x_2, \dots, x_n) = (r \cdot x_1, r \cdot x_2, \dots, r \cdot x_n)$

for $r \in R$ and $(x_1, x_2, \dots, x_n)$, $(y_1, y_2, \dots, y_n) \in R^{(n)}$.

Then, it can be easily verified that $\langle R^{(n)}, +, \cdot \rangle$ is a module over R.

Put $\quad e_i = (0, 0, \dots, 1, 0, \dots, 0)$, $\quad$ for each i, $1 \le i \le n$.

$\uparrow i^{th}$ place.

(i) Let $a_i \in R$, for each i, $1 \le i \le n$ and $\sum_{i=1}^{n} a_i e_i = 0$.

But $\sum_{i=1}^{n} a_i e_i = (a_1, a_2, \dots, a_n)$

Hence, $\sum_{i=1}^{n} a_i e_i = 0 \Rightarrow (a_1, a_2, \dots, a_n) = (0, 0, \dots, 0)$.

$\Longrightarrow \quad a_1 = 0, a_2 = 0, \dots, a_n = 0$

(ii) Again any $x \in R^{(n)}$ can be written as $x = (x_1, x_2, \dots, x_n)$ where $x_i \in R$, $\forall\ i$, $1 \le i \le n$. In this case,

$x = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n \quad$ as $x_i e_i = (0, 0, \dots, x_i, 0, \dots, 0)$

$\uparrow i^{th}$ place.

But this in turn shows that, the set $B = \{e_1, e_2, \dots, e_n\}$ generates $R^{(n)}$.

From (i) and (ii), we get, B is a base for an R-module $R^{(n)}$.

Theorem 2.3.4 : Let M be an R-module $(1 \in R)$. Let $\{u_1, u_2, \dots, u_n\}$ be a base for M. Then $M \cong R^{(n)}$.

Proof : We know that, $R^{(n)}$ is an R-module with base $\{e_1, e_2, \dots, e_n\}$, where

$e_i = (0, 0, \dots, 1, 0, \dots, 0)$

$\uparrow i^{th}$ place.

for each i, $1 \le i \le n$.

Hence, any $x \in R^{(n)}$ can be expressed as $x = \sum_{i=1}^{n} r_i e_i$ where $r_i \in R$, $\forall\ i$, $1 \le i \le n$.

As $\{u_1, u_2, \dots, u_n\}$ is a base for M, $\sum_{i=1}^{n} r_i u_i$ where $r_i \in R$ is an element of M.

Define $f: R^{(n)} \longrightarrow M$ by

$$f(x)=f\left(\sum_{i=1}^{n} r_i e_i\right)=\sum_{i=1}^{n} r_i u_i$$

(I) f is well defined map.

Let $x = y$ in $R^{(n)}$.

Then, let $x=\sum_{i=1}^{n} r_i e_i$ and $y=\sum_{i=1}^{n} r'_i e_i$ where $r_i,\ r'_i \in R,\ \forall\ i.$

$$x = y \implies \sum_{i=1}^{n} r_i e_i = \sum_{i=1}^{n} r'_i e_i$$

$$\implies \sum_{i=1}^{n} r_i e_i - \sum_{i=1}^{n} r'_i e_i = 0$$

$$\implies \sum_{i=1}^{n} (r_i - r'_i) e_i = 0$$

$$\implies r_i - r'_i = 0 \qquad \forall\ i,\ 1 \le i \le n.$$

As $\{e_1,\ e_2, \dots, e_n\}$ is a base for $R^{(n)}$.

As $r_i = r'_i$ for each $i,\ 1 \le i \le n$ we get

$$\sum_{i=1}^{n} r_i u_i = \sum_{i=1}^{n} r'_i u_i$$

Thus ,

$$x = y \implies \sum_{i=1}^{n} r_i e_i = \sum_{i=1}^{n} r'_i e_i \implies \sum_{i=1}^{n} r_i u_i = \sum_{i=1}^{n} r'_i u_i \implies f(x) = f(y)$$

This shows that f is well defined.

(II) f is a R-homomorphism.

(i)Let $x,\ y \in R^{(n)}$. Let $x=\sum_{i=1}^{n} r_i e_i$ and $y=\sum_{i=1}^{n} r'_i e_i$

$$f(x+y) = f\left(\sum_{i=1}^{n} r_i e_i + \sum_{i=1}^{n} r'_i e_i\right)$$

$$= f\left(\sum_{i=1}^{n} \left(r_i + r'_i\right) e_i\right)$$

$$= \sum_{i=1}^{n} \left(r_i + r'_i\right) u_i$$

$$= \sum_{i=1}^{n} r_i u_i + \sum_{i=1}^{n} r_i' u_i$$

$$= f(x) + f(y)$$

Thus, $f(x+y) = f(x) + f(y)$ for all $x, y \in R^{(n)}$.

(ii) Let $r \in R$ and $x \in R^{(n)}$. Let $x = \sum_{i=1}^{n} r_i e_i, \quad r_i \in R$

$$f(rx) = f\left(r \sum_{i=1}^{n} r_i e_i\right)$$

$$= f\left(\sum_{i=1}^{n} (r r_i) e_i\right)$$

$$= \sum_{i=1}^{n} (r r_i) u_i$$

$$= r \sum_{i=1}^{n} r_i u_i$$

$$= r\ f(x)$$

Thus, $f(rx) = r\,f(x)$ for all $r \in R$ and $x \in R^{(n)}$.

From (i) and (ii), we get, f is a R- homomorphism.

(III) f is an onto mapping.

As $f(e_i) = u_i$ for each $i, 1 \le i \le n$, we get $im\,f = \{f(x)/\ x \in R^{(n)}\}$ contains u_i for each $i, 1 \le i \le n$.

Thus, $im\ f$ is a submodule of M containing $u_1,\ u_2, \dots, u_n$.

By data $\{u_1,\ u_2, \dots, u_n\}$ is a base for M and hence it generates M.

Thus, $im\ f = M$. But this shows that f is onto.

(IV) f is one-one.

Let $x \in kerf$ then $f(x) = 0$.

Let $x = \sum_{i=1}^{n} r_i e_i$. Then

$$f(x) = f\left(\sum_{i=1}^{n} r_i e_i\right)$$

$$= \sum_{i=1}^{n} r_i u_i$$

$= 0$

As $\{u_1, u_2, \dots, u_n\}$ is a base for M, $\sum_{i=1}^{n} r_i u_i = 0 \quad \Rightarrow \quad r_i = 0$ for each $i, 1 \leq i \leq n$.

But this in turn shows that $x = \sum_{i=1}^{n} r_i e_i = 0$. Thus $kerf = \{0\}$.

This shows that f is one-one. (See 1.3, theorem 3).

From (I), (II), (III) and (IV) we get,

$f: R^{(n)} \longrightarrow M$ is an isomorphism and hence $R^{(n)} \cong M$.

Remark 2.3.5 : Thus existence of a base of n-elements for an R-module implies that $M \cong R^{(n)}$. In this case we shall say that M is a free R-module of rank n.

Theorem 2.3.6 : If M is a module over commutative ring R with unity 1 and if M has bases of m and n elements, then $m = n$.

Proof : Assume that $m < n$.

Let $\{e_1, e_2, \dots, e_n\}$ and $\{f_1, f_2, \dots, f_m\}$ be basis for M. As $f_j \in M$ and $\{e_i \,/\, 1 \leq i \leq n\}$ is a base for M, we get

$$f_j = \sum_{i=1}^{n} a_{ji} e_i \qquad \text{where } a_{ji} \in R. \qquad \dots (1)$$

Similarly, as $e_i \in M$ and $\{f_1, f_2, \dots, f_m\}$ is a base for M, we get

$$e_i = \sum_{j=1}^{m} b_{ij} f_j \qquad \text{where } b_{ij} \in R. \qquad \dots (2)$$

From (1) and (2) ,we get,

$$f_j = \sum_{i=1}^{n} \sum_{j'=1}^{m} a_{ji} b_{ij'} f_{j'} \qquad \dots (3)$$

and

$$e_i = \sum_{j=1}^{m} \sum_{i'=1}^{n} b_{ij} a_{ji'} e_{i'} \qquad \dots (4)$$

But $\{f_i \,/\, 1 \leq j \leq m\}$ and $\{e_i \,/\, 1 \leq i \leq n\}$ are bases for M and hence

$$\sum_{i=1}^{n} a_{ji}\ b_{ij'}\ e_{i'} = \begin{cases} 1 & if\, j = j' \\ 0 & if\, j \neq j' \end{cases}, \qquad \text{for } 1 \leq j, j' \leq m. \qquad \ldots (5)$$

and

$$\sum_{j=1}^{m} b_{ij}\ a_{ji'} = \begin{cases} 1 & if\ \ i = i' \\ 0 & if\ \ i \neq i' \end{cases}, \qquad \text{for } 1 \leq i, i' \leq n. \qquad \ldots (6)$$

From (1) and (2), we obtain the two $n \times m$ matrices A and B defined as follows.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \\ 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}_{n\times m}$$

and

$$B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1m} & 0 & \cdots & 0 \\ b_{21} & b_{22} & \cdots & b_{2n} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & 0 & \cdots & 0 \\ b_{n1} & b_{n2} & \cdots & b_{nm} & 0 & \cdots & 0 \end{bmatrix}_{n\times m}$$

But form (6), we get, $BA = 1$.

Since R is commutative, $BA = 1 \implies AB = 1$.

But $AB = 1$ is impossible as the matrix AB contains last $n - m$ rows zero.

Hence our assumption $m < n$ is wrong. Therefore $m \geq n$.

Similarly, we can prove that $m \leq n$.

Hence $m = n$.

Corollary 2.3.7 : If R is commutative, $R^{(m)} \cong R^{(n)}$ implies $m = n$.

Proof : We know that any free module M with a base containing m elements is isomorphic with $R^{(m)}$ (See theorem 3.3.4). Thus, if $R^{(m)} \cong R^{(n)}$ then we have a free module M which has bases of m and n elements. By theorem 3.3.6 it follows that, $m = n$ and we are through.

Theorem 2.3.8 : Given one ordered base $e_1, e_2, \ldots, e_n$ for a free module over a commutative ring R, we obtain another ordered base $\{f_1, f_2, \ldots, f_n\}$ by applying the matrices $A = L_n(R)$ to $(e_1,\ e_2, \dots, e_n)$ in the sence that $f_j = \sum_{i=1}^{n} a_{ij}\, e_i$, $A = (a_{ij})$ and conversely. Here $L_n(R)$ denotes the group of $n \times n$ invertible matrices with entries in R.

Proof : Let $(e_1,\ e_2, \dots, e_n)$ and $(f_1,\ f_2, \dots, f_n)$ be a bases for a free module M. As $f_j \in M$ and $(e_1,\ e_2, \dots, e_n)$ is a base for M, we get

$$f_j = \sum_{i=1}^{n} a_{ji}\, e_i \qquad \forall\ j,\ \ 1 \le j \le n,\ a_{ij} \in R\ \ \forall\ j,\ i.$$

Similarly, $e_i \in M$ and $(f_1,\ f_2, \dots, f_n)$ is a base for M, will give

$$e_i = \sum_{j=1}^{n} b_{ij}\, e_j\ , \qquad \forall\ i,\ \ 1 \le i \le n,\ \ b_{ij} \in R\ \ \forall\ i,\ j.$$

Define $A = (a_{ij})$ and $B = (b_{ij})$.

Then, $A, B \in L_n(R)$, as AB = 1 and BA = 1 imply A and B are invertible.

Conversely, suppose that $(e_1,\ e_2, \dots, e_n)$ be a base for a free module M and $A = (a_{ij}) \in L_n(R)$.

Define $$f_j = \sum_{i=1}^{n} a_{ji}\, e_i\ , \qquad \forall\ j,\ \ 1 \le j \le n.$$

Claim : $(f_1,\ f_2, \dots, f_n)$ is a base for M.

(i) Now $A \in L_n(R)$. Hence A^{-1} exists. Let $A^{-1} = B$. Then AB = 1 = BA and let $B = (b_{ij})_{n\times n}$.

Consider $\sum_{j=1}^{n} b_{kj}\, f_j$. Then ,

$$\sum_{j=1}^{n} b_{kj}\, f_j = \sum_{i=1}^{n}\ \sum_{j=1}^{n} b_{kj}\, a_{ji}\, e_i = e_k \text{ as BA = 1.}$$

As $\{e_1, e_2, \dots, e_n\}$ generate M we get $\{f_1, f_2, \dots, f_n\}$ generate M.

(ii) Let $\sum_{i=1}^{n} r_j\, f_j = 0$ for some $r_i \in R,\ 1 \le i \le n$. Then

$$\sum_{j=1}^{n}\ \sum_{i=1}^{n} r_j \left[\ a_{ji}\, e_i \right] = 0$$

i.e. $$\sum_{i=1}^{n} \sum_{j=1}^{n} \left[r_j \, a_{ji} \right] e_i = 0$$

As $\{e_1, e_2, \ldots, e_n\}$ is a base for M, we get

$$\sum_{j=1}^{n} r_j \, a_{ji} = 0 \quad , \qquad \forall \quad i, \; 1 \leq i \leq n.$$

Hence $$\sum_{i=1}^{n} \sum_{j=1}^{n} r_j \, a_{ji} \, b_{ih} = 0 \quad , \qquad \forall \quad h, \; 1 \leq h \leq n.$$

But AB = 1 and hence $r_j = 0$ for all $j, \; 1 \leq i \leq n$.

Thus, $$\sum_{j=1}^{n} r_j \, f_j = 0 \qquad \Rightarrow \quad r_j = 0 \text{ for each } j, \; 1 \leq i \leq n.$$

From (1) and (2), we get $\{f_1, f_2, \ldots, f_n\}$ is a base for M.

Theorem 2.3.9 : Let D be a p. i. d. and let $D^{(n)}$ be the free module of rank n over D. Then every submodule K of $D^{(n)}$ is free with base of $m \leq n$ elements.

Proof :

Case I : n = 0.

If K = (0), then K is a free module with rank 0 (with empty base). Hence the result is trivially true for n = 0.

Case II : n = 1.

$D^{(n)} = D$. Hence any submodule of D is an ideal in D, which is a principal ideal. Hence $K = (f)$ for some $f \in D$. Obviously $\{f\}$ generates K.

If f = 0, then K = (0) and the result follows as rank of K = 0.

Let $f \neq 0$. Then $af = 0$ for some $a \in D$ will imply $a = 0$ as D is an integral domain. Thus, $\{f\}$ will form a base for $K = (f)$.

Hence, K is a free module with rank ≤ 1.

Case III : n > 1.

Let K be any submodule of $D^{(n)}$.

We prove the result my induction on n. Let $\{e_1, e_2, \ldots, e_n\}$ be a base for $D^{(n)}$. Let $D^{(n-1)}$ denote a submodule of $D^{(n)}$ generated by $\{e_2, e_3, \ldots, e_{n-1}, e_n\}$. Then $D^{(n-1)}$ is a free module of rank n – 1. Hence $\frac{D^{(n)}}{D^{(n-1)}}$ is a free module of rank 1. The base for is $\frac{D^{(n)}}{D^{(n-1)}}$ is $\{\bar{e}_1\}$ where $\bar{e}_1 = e_1 + D^{(n-1)}$.

As K is a submodule of $D^{(n)}$, $\frac{k+D^{(n-1)}}{D^{(n-1)}}$ is a submodule of $\frac{D^{(n)}}{D^{(n-1)}}$.

Let

$$\overline{K} = \frac{K+D^{(n-1)}}{D^{(n-1)}} \qquad \text{and} \qquad \overline{D} = \frac{D^{(n)}}{D^{(n-1)}}$$

(I) If $\overline{K} = (0)$, then $k + D^{(n-1)} \subseteq D^{(n-1)}$ and hence $K \subseteq D^{(n-1)}$.

By induction, K will be a free module with base containing $m \leq n-1$ elements and hence the result is true in this case.

(II) If $\overline{K} = \{0\}$, then as in case (I), $\overline{K}$ will contain a base consisting of one element say $\bar{f}_1$ where $\bar{f}_1 = f_1 + D^{(n-1)}$. As $\overline{K} = \frac{K+D^{(n-1)}}{D^{(n-1)}}$ we select $f_1 \in K$.

Subcase I : $K \cap D^{(n-1)} \neq (0)$.

Then $K \cap D^{(n-1)} \neq (0)$ is a submodule of $D^{(n-1)}$. Hence by induction hypothesis, $K \cap D^{(n-1)}$ has a base say $\{f_1, f_2, \dots, f_m\}$ with $0 < m-1 < n-1$.

Claim : $\{f_1, f_2, \dots, f_m\}$ will form a base for K.

Let $y \in K$. Then $\bar{y} = y + D^{(n-1)} \in \overline{K}$. Hence $\bar{y} = b_1\bar{f}_1$ for some $b_1 \in D$.

But this means that

$$y - b_1f_1 = b_2f_2 + b_3f_3 + \cdots + b_mf_m$$

$$y = b_1f_1 + b_2f_2 + b_3f_3 + \cdots + b_mf_m \qquad \dots (1)$$

Now, let us assume that $\sum_{i=1}^{m} d_if_i = 0$ for $d_i \in D$. Hence $d_1f_1 = -\sum_{j=2}^{m} d_jf_j$.

This implies

$$d_1\overline{f}_1 = -\sum_{j=2}^{m} d_j\overline{f}_j \ .$$

But $\{f_2, f_3, \dots, f_m\}$ is a base for $K \cap D^{(n-1)}$. Hence $\sum_{j=2}^{n} d_j\overline{f}_j = 0$ and therefore $d_1\overline{f}_1 = 0$. But $\{\bar{f}_1\}$ is a base for $\overline{K}$ will imply $d_1 = 0$.

Thus,

$$\sum_{j=2}^{m} d_j f_j = 0 \qquad\qquad (\text{Since } d_1\overline{f}_1 = -\sum_{j=2}^{m} d_j\overline{f}_j$$

As $\{f_2, f_3, \dots, f_m\}$ is a base for $K \cap D^{(n-1)}$ we get $d_2 = d_3 = \cdots = d_m = 0$. Thus

$$\sum_{k=1}^{m} d_k f_k = 0 \quad \Rightarrow \quad d_k = 0 \qquad \forall \quad k,\ 1 \le k \le m$$

Hence, $\{f_1, f_2, \dots, f_m\}$ will form a base K.

Subcase II : $K \cap D^{(n-1)} = \{0\}$.

If $K \cap D^{(n-1)} = \{0\}$, then $\{f_1\}$ will form a base for K.

$f_1 \in K \quad \Rightarrow \quad (f_1) \subseteq K$, where $(f_1) = Df_1$.

Let $y \in K$. Then $\bar{y} = y + D^{(n-1)} \in \overline{K}$.

Hence, $\bar{y} = b_1\bar{f}_1$ for some $b_1 \in D$.

$\Rightarrow \quad y - b_1 f_1 \in D^{(n-1)}$.

As $f_1 \in K$ and $y \in K$, we get $y - b_1 f_1 \in K$.

Thus, $y - b_1 f_1 \in K \cap D^{(n-1)} = \{0\}$.

Hence, $y = b_1 f_1$. This shows that $K \subseteq (f_1)$.

Hence, $K = (f_1) = Df_1$.

Further, $b_1 f_1 = 0$ and $f_1 \neq 0 \quad \Rightarrow \quad b_1 = 0$.

Hence, $\{f_1\}$ will form a base for K.

Thus in either cases, K is a free module with base consisting of m elements, where $m \le n$.

2.4 Completely Reducible Modules :

Definition 2.4.1 : An R-module M is called completely reducible if $M = \sum M_\alpha$ where M_α are simple R-modules.

Theorem 2.4.2 : Let M be a completely reducible R-module. Let $M = \sum_{\alpha\in\Delta} M_\alpha$ where M_α is a simple R-modules of M. For any submodule K of M, $\exists$ a subset Δ' and Δ such that $\sum_{\alpha\in\Delta'} M_\alpha$ is a direct sum and

$$M = K \oplus \sum_{\alpha\in\Delta'} M_\alpha .$$

Proof : $\mathcal{K} = \left\{ A \subseteq \Delta \ / \sum_{\alpha \in A} M_\alpha \text{ is a direct sum and } K \cap \sum_{\alpha \in \Delta} M_\alpha = \{0\} \right\}.$

Then $\mathcal{K}$ is a non empty set as $\phi \in \mathcal{K}$.

As,

$$\sum_{\alpha \in \phi} M_\alpha = \{0\}$$

$\langle \mathcal{K}, \subseteq \rangle$ is partially ordered set.

Let $\mathcal{C}$ be a chain in $\mathcal{K}$. Then

$$\bigcup_{c \in \mathcal{C}} c \in \mathcal{K}$$

Hence, by Zorn's lemma, $\mathcal{K}$ contains a maximum element say B.

Thus, $\sum_{\alpha \in B} M_\alpha$ is a direct sum and $K \cap \sum_{\alpha \in \Delta} M_\alpha = \{0\}$

Let $N = K \oplus \sum_{\alpha \in B} M_\alpha$.

Claim that M = N. i.e. to prove that $\oplus \sum_{\alpha \in \Delta} M_\alpha = K \oplus \sum_{\alpha \in B} M_\alpha$.

Let $\beta \in \Delta$. Then M_β is a direct sum and of M and M_β is simple. Hence $M_\beta \cap N$ is a submodule of M_β will imply $M_\beta \cap N = M_\beta$ or $M_\beta \cap N = \{0\}$.

Let $M_\beta \cap N = \{0\}$ then $M_\beta \cap \sum_{\alpha \in B} M_\alpha \subseteq M_\beta \cap N = \{0\}$.

This implies that $M_\beta \cap \sum_{\alpha \in B} M_\alpha = \{0\}$.

But then $\sum_{\alpha \in B \cup \{\beta\}} M_\alpha$ is a direct sum and

$$K \cap \left[\sum_{\alpha \in B \cup \{\beta\}} M_\alpha \right] = \left[K \cap \sum_{\alpha \in B} M_\alpha \right] \cup [K \cap M_\beta]$$

$$= \{0\} \cup \{0\} = \{0\} \qquad \text{(as } M_\beta \cap N = \{0\} \implies M_\beta \cap K = \{0\}$$

Thus, $B \cup \{\beta\} \in \mathcal{K}$.

B being a maximal element of $\mathcal{K}$ we get a contradiction.

Hence, $\quad M_\beta \cap N = M_\beta \qquad$ i.e. $M_\beta \subseteq N \qquad \forall \ \beta \in \Delta$.

But this will imply

$$\sum_{\beta \in \Delta} M_\beta \subseteq N. \quad \text{i.e. } M \subseteq N.$$

Hence, M = N.

Thus, $M = K \oplus \sum_{\alpha \in B} M_\alpha$ where $B \subseteq \Delta$ such that $\sum_{\alpha \in B} M_\alpha$ is a direct sum.

Corollary 2.4.3 : Let $M = \sum_{\alpha \in \Delta} M_\alpha$ where M_α is a simple R-submodule of M. Then $\exists$ a subfamily Δ' of Δ such that $M = \oplus \sum_{\alpha \in \Delta'} M_\alpha$.

Proof : We know that for any submodule K of M, $\exists$ $\Delta' \subseteq \Delta$ such that $M = K \oplus \sum_{\alpha \in \Delta'} M_\alpha$ and $\sum_{\alpha \in \Delta'} M_\alpha$ is a direct sum.

Now, take $K = \{0\}$. Then $M = \oplus \sum_{\alpha \in \Delta'} M_\alpha$.

2.4.4 Worked Examples

Example 1 : Let M be a completely reducible module and let K be a nonzero submodule of M. Show that K is completely reducible. Also show that K is completely reducible. Also show that K is a direct summand of M.

Solution : Let $M = \sum_{\alpha \in \Delta} M_\alpha$ where each M_α is a simple submodule.

By theorem 2, $M = K \oplus \sum_{\alpha \in \Delta'} M_\alpha$, $\Delta' \subseteq \Delta$ shows that K is a direct summand of M.

Again, $$\frac{M}{K} \cong \sum_{\alpha \in \Delta'} M_\alpha$$

and $$\frac{M}{\sum_{\alpha \in \Delta'} M_\alpha} \cong K$$

Thus ,

$$K \cong \frac{M}{\sum_{\alpha \in \Delta'} M_\alpha} \cong \frac{\sum_{\alpha \in \Delta'} M_\alpha \oplus \sum_{\alpha \in \Delta''} M_\alpha}{\sum_{\alpha \in \Delta'} M_\alpha} \cong \sum_{\alpha \in \Delta''} M_\alpha$$

$\frac{M}{K} \cong \sum_{\alpha \in \Delta'} M_\alpha$ is a submodule of M. Hence again applying theorem 1, we get,

$$K = \left[\sum_{\alpha \in \Delta'} M_\alpha\right] \oplus \left[\sum_{\alpha \in \Delta''} M_\alpha\right], \qquad \text{for some } \Delta'' \subseteq \Delta.$$

$$\frac{M}{\sum_{\alpha \in \Delta} M_\alpha} = \frac{\sum_{\alpha \in \Delta'} M_\alpha + \sum_{\alpha \in \Delta''} M_\alpha}{\sum_{\alpha \in \Delta'} M_\alpha} \cong \sum_{\alpha \in \Delta''} M_\alpha$$

Thus ,

$$K \cong \sum_{\alpha \in \Delta''} M_\alpha \quad (\Delta'' \subseteq \Delta.$$

As each $M_\alpha,\ \alpha \in \Delta''$ is simple we get $\sum_{\alpha \in \Delta''} M_\alpha$ is completely reducible module. Hence K is completely reducible being an isomorphic image of a completely reducible module.

Example 2 : Let M be a completely reducible module and let K be a submodule of M. If $K \neq M$ then show that $\frac{M}{K}$ is completely reducible.

Solution : M be completely reducible. Hence $M = \sum_{\alpha \in \Delta} M_\alpha$ where each M_α is simple. K is a submodule of M. Therefore by theorem 1, $M = K \oplus \sum_{\alpha \in \Delta'} M_\alpha$ for some $\Delta' \subseteq \Delta$.

But then $\frac{M}{K} \cong \sum_{\alpha \in \Delta'} M_\alpha$.

As $\sum_{\alpha \in \Delta'} M_\alpha$ is completely reducible, we get $\frac{M}{K}$ is completely reducible.

Unit 3: NOETHERIAN AND ARTINIAN MODULES :

3.1 Noetherian and Artinian module

3.2 Artinian module

3.1 Noetherian Modules :

Definition 3.1.1 : Let M be an R-module. If for every ascending sequence of R-submodules of M, $M_1 \subseteq M_2 \subseteq \cdots \subseteq \cdots$ there exists a positive integer n such that $M_n = M_{n+1} = \cdots$, then M is called Noetherian module.

Remark 3.1.2 : If M is a Noetherian module, we say that ascending chain condition (acc) for submodules hold in M or M has acc.

3.1.3 Examples

Example 1 : Let Z denote a Z-module and $n \in Z$. we know that (n) is a submodule of Z. Consider the ascending chain of submodules in Z given below.

$$(n) \subset (n_1) \subset (n_2) \subset \cdots$$

Then, $\quad (n) \subset (n_1) \quad \Rightarrow \quad n_1 \mid n$

$$(n_1) \subset (n_2) \quad \Rightarrow \quad n_2 \mid n_1$$

Hence, the ascending chain of submodules in Z, starting with (n) will have atmost n distinct elements.

This shows that Z as a Z-module is a Noetherian module.

Example 2 : Let V be an n-dimensional vector space over a field F. Then any ascending chain of subspaces of V cannot have more than $n + 1$ elements. Hence V must be Noetherian.

Theorem 3.1.4 : Let M an R-module. The following statements are equivalent.

(i) M is Noetherian.

(ii) Every submodule of M is finitely generated.

(iii) Any non-empty family of submodules of M has a maximal element.

Proof :

(i) ⟹ (ii) :

Let N be a submodule of a Noetherian module M.

Assume that N is not finitely generated.

Select $a_1 \in N$. Then $N \neq (a_1)$, by assumption.

Hence, select $a_2 \in N$ such that $a_2 \notin (a_1)$. (This is possible as $(a_1) \subset N$).

Then, by assumption,

$$N \neq (a_1,\ a_2) \qquad \text{and} \qquad (a_1) \subset (a_1,\ a_2) \subset N.$$

Hence, select $a_3 \in N$ such that $a_3 \notin (a_1,\ a_2)$.

Then $N \neq (a_1,\ a_2,\ a_3)$, by assumption and

$$(a_1) \subset (a_1,\ a_2) \subset (a_1,\ a_2,\ a_3) \subset N.$$

Continuing in this way, we get an infinite ascending chain of submodules of N and hence of M.

But this contradicts the fact that M is Noetherian module.

Hence, N must be finitely generated.

(ii) ⟹ (iii) :

Let $\mathcal{K}$ denote the non empty family of submodules of the module M.

Let $N_0 \in \mathcal{K}$.

If N_0 is a maximal ideal of $\mathcal{K}$, then we are through.

If N_0 is not a maximal element of $\mathcal{K}$, then there exist $N_1 \in \mathcal{K}$ such that $N_0 \subset N_1$.

If N_1 is a maximal element of $\mathcal{K}$, then we are through.

If N_1 is not a maximal element of $\mathcal{K}$, then there exist $N_2 \in \mathcal{K}$ such that $N_0 \subset N_1 \subset N_2$.

Thus, if $\mathcal{K}$ does not contain a maximal element, we get an infinite chain of submodules of M as below

$$N_0 \subset N_1 \subset N_2 \subset \cdots \qquad \ldots \text{(I)}$$

Define $N = \bigcup_{i=1} N_i$.

Then, N is a submodule of M. By assumption N must be finitely generated.

Let $(x_1, x_2, \ldots, x_k)$, where $x_i \in N,\ \ \forall\ i \leq i \leq K$.

The finite number of elements $x_1, x_2, \ldots, x_k$ must belong to the finite number of submodules. N_i (this number $\leq k$), by the definition of N.

Hence, select a positive integer s such that $x_1, x_2, \ldots, x_k \in N_s$ and s is the smallest positive integer satisfying this property. Thus,

$$x_1, x_2, \ldots, x_k \in N_s \text{ implies } (x_1, x_2, \ldots, x_k) \subseteq N_s$$

and hence $N \subseteq N_s \subseteq N$.

This shows that $N = N_s$.

For the infinite chain in I we have $s > 0$ such that

$$N_s = N_{s+1} = N_{s+2} = \ldots = N$$

This in turn shows that N will be the maximal element in $\mathcal{K}$ and the implication follows.

(iii) $\Longrightarrow$ (i) :

Let $M_1 \subset M_2 \subset \ldots$ be any ascending sequence of submodules of an R-module M.

Consider the family $\mathcal{K} = \{M_1, M_2, \ldots\}$.

Then, $\mathcal{K}$ is the family of submodules of M and hence by assumption, $\mathcal{K}$ contains a maximal element say M_n. But then $M_n = M_{n+1} = \ldots$.

This in turn shows that M is Noetherian.

Thus, we have proved $1 \Longrightarrow 2 \Longrightarrow 3 \Longrightarrow 1$.

Hence, all the statements are equivalent.

Theorem 3.1.5 : Every submodule of a Noetherian module is a Noetherian module.

Proof : Let M be Noetherian module. Let N be submodule of M.

To prove N is Noetherian.

Let $\mathcal{K}$ be any non empty family of submodules of N.

Then obviously, $\mathcal{K}$ is a any non empty family of submodules of M.

M being Noetherian, $\mathcal{K}$ contains a maximal element (See theorem 3.1.4).

But this in turn will imply N is Noetherian.

Theorem 3.1.6 : Every quotient module of a Noetherian module is Noetherian.

Proof : Let M be a Noetherian module. Let N be any submodule of M.

To prove that $\frac{M}{N}$ is Noetherian.

Let $\mathcal{K}$ denote a non-empty family of submodules of a module $\frac{M}{N}$.

Let $\mathcal{K} = \left\{\frac{U_1}{N}, \frac{U_2}{N}, \frac{U_3}{N}, \ldots\right\}$. As $\frac{U_i}{N}$ is a submodule of $\frac{M}{N}$, by theorem 1 in 1.3, we get U_i is a submodule of M containing N.

Consider the family $\mathcal{F} = \{N,\ U_1, U_2,\ \dots\}$. Then $\mathcal{F}$ is a nonempty family of submodule on M (since $N \in \mathcal{F}$). As M is Noetherian, the family $\mathcal{F}$ contains a maximal element say U_k.

Then $\frac{U_k}{N}$ will be the maximal element of the family $\mathcal{K}$.

Hence, $\frac{M}{N}$ is Noetherian module, by theorem 3.1.4.

Theorem 3.1.7 : Every homomorphic image of a Noetherian module is Noetherian.

Proof : Let $f : M_1 \longrightarrow M_2$ be R-homomorphism of an R-module M_1 onto the R-module M_2.

Claim 1 : If N is a submodule of M_1 then $f(N)$ is a submodule of M_2.

(i) $f(N) \neq \phi$ as $N \neq \phi$

(ii) $x, y \in f(N)$. Hence $\exists$ $a, b \in N$ such that $x = f(a)$ and $y = f(b)$.

Then $x - y = f(a) - f(b)$

$= f(a - b)$, … Since f is homomorphism.

This shows that $x - y \in f(N)$ as $a - b \in N$, N being a module in M_1.

(iii) Let $r \in R$ and $x \in f(N)$. Then $x = f(a)$ for some $a \in N$.

As N is a submodule of M_1, $r \cdot a \in N \implies f(r \cdot a) \in f(N)$.

But as f is an R- homomorphism, $f(r \cdot a) = r \cdot f(a) = r \cdot x \in f(n)$.

From (i), (ii) and (iii), we get, $f(N)$ is a submodule of M_2.

Claim 2 : If X is a submodule of M_2, then $f^{-1}(X)$ is a submodule of M_1.

(i) $f^{-1}(X) \neq \phi$ as $X \neq \phi$

(ii) $a, b \in f^{-1}(X)$. Then $f(a) \in X$, $f(b) \in X$.

As X is a submodule, $f(a) - f(b) \in X$

f being homomorphism, $f(a) - f(b) = f(a - b)$.

Thus, $f(a - b) \in X$ and hence $a - b \in f^{-1}(X)$.

(iii) Let $r \in R$ and $a \in f^{-1}(X)$.

Then $f(a) \in X$, X being a submodule of M, $r \cdot f(a) \in X$.

As f is a homomorphism $f(r \cdot a) = r \cdot f(a)$.

Thus, $r \cdot a \in f^{-1}(X)$.

From (i), (ii) and (iii), we get, $f^{-1}(X)$ is a submodule of M_1.

Claim 3 : M_2 is a Noetherian module.

Let $\mathcal{K}' = \{N_1', N_2', \dots\}$ be any nonempty family of submodules of the module M_2.

Then the family, $\mathcal{K}' = \{f^{-1}(N_1'), f^{-1}(N_2'), \dots\}$ is a non empty family of submodules of the module M_1(by claim 2).

As M_1 is Noetherian, $\mathcal{K}$ contains a maximal element (by theorem 3.1.4).

Let it be $f^{-1}(N_k')$.

Then, N_k' will be maximal element in $\mathcal{K}'$ (by claim 1). This in turn shows that M_2 is Noetherian (See theorem 3.1.4).

Thus, homomorphic image of a Noetherian module is Noetherian.

Theorem 3.1.8 : Let M be an R-module and let N be a submodule of M. M is Noetherian iff both N and $\frac{M}{N}$ are Noetherian.

Proof : Only if part :

Let M be Noetherian. Then both N and $\frac{M}{N}$ are Noetherian (See theorem 3.1.5 and theorem 3.1.6).

If part :

Let N and $\frac{M}{N}$ both be Noetherian.

To prove that M is Noetherian.

N is Noetherian implies N is finitely generated (See theorem 3.1.4).

Let $N = (x_1, x_2, \dots, x_k)$.

$\frac{M}{N}$ is Noetherian implies $\frac{M}{N}$ is finitely generated (See theorem 3.1.4).

Let $\frac{M}{N} = (y_1 + N, y_2 + N, \dots, y_s + N)$

Then $M = (x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_s)$

As M is a finitely generated module, M is Noetherian (See theorem 3.1.4).

Theorem 3.1.9 : Let M be an R-module. Let M_1 and M_2 be submodules of M such that $M = M_1 \oplus M_2$. If M_1 and M_2 are Noetherian, then M is Noetherian.

Proof : We know that $M = M_1 \oplus M_2$ will imply $M_1 \cong \frac{M}{M_2}$ and $M_2 \cong \frac{M}{M_1}$ (See theorem 3.1.6).

Now, M_1 is Noetherian and $M_1 \cong \frac{M}{M_2}$.

Hence, by theorem 3.1.7, $\frac{M}{M_2}$ is Noetherian.

As M_2 and $\frac{M}{M_2}$ both are Noetherian we get M is Noetherian (by theorem 3.1.8).

Corollary 3.1.10 : Let M be an R-module and let $M_1, M_2, \dots, M_k$ be Noetherian submodules of M such that

$$M = M_1 \oplus M_2 \oplus \dots \oplus M_k$$

Then, M is Noetherian.

Proof : The result is true for $n = 2$ by theorem 3.1.9.

[Hence by induction on n, we get, if $M = M_1 \oplus M_2 \oplus \dots \oplus M_k$ then M is Noetherian when each M_i is a Noetherian module].

Let the result be true for all $k \leq n$.

Then $[M_1 \oplus M_2 \oplus \dots \oplus M_{n-1}] = N$ is Noetherian module.

But in this case $M = N \oplus M_n$.

As N and M_n both are noertherian, we get M is Noetherian.

3.2 Artinian Module :

Definition 3.2.1 : An R-module M is called Artinian if for every decreasing sequence of R-submodules of M

$$M_1 \supseteq M_2 \supseteq \cdots \supseteq \cdots$$

there exists a positive integer n such that $M_n = M_{n+1} = \cdots$.

Remark 3.2.2 : If M is Artinian module, we say that descending chain condition (dcc) for submodules hold in M or M has dcc.

Example 3.2.3 : Any finite dimensional vector space over the field F is an Artinian module.

Remark 3.2.4 : Any finite dimensional vector space over the filed F is both Noetherian and Artinian module. But Z as Z-module is a Noetherian module which is not Artinian as the decreasing sequence

$$(n) \supset (n^2) \supset \cdots$$

is an infinite properly decreasing sequence in Z.

Now we only mention the characterizing properties of Artinian modules, the proof being similar to the proof of theorem 3.1.4.

Theorem 3.2.5 : Let M be an R-module. Following statements are equivalent.

(i) M is Artinian.

(ii) Every submodules of M is finitely generated.

(iii) Every non-empty set $\mathcal{K}$ of submodules of M has a minimal element.

Exercise : Show that every submodule and every homomorphic image of an Artinian module is Artinian.

[Hint : See 3.1, theorem 3.1.5 and theorem 3.1.7].