Instruction Material

M.Sc(Mathematics)-Semester-I

Paper-I

Abstract Algebra

Editor

Prof. B. Surender Reddy

Course Writers

(1). Dr. B. Surender Reddy

Professor of Mathematics

Osmania University, Hyderabad

(2). Dr. V. Kiran

Associate Professor

Department of Mathematics

Osmania University, Hyderabad

Syllabus

Paper - I : Abstract Algebra

Unit-I

Automorphisms – Conjugacy and G-sets – Normal series – Solvable groups – Nilpotent groups. (Pages 104 to 128)

Unit-II

Structure theorems of groups : Direct products – Finitely generated abelian groups –Invariants of a finite abelian group- Sylow's theorems – Groups of orders p^2, pq. (Pages 138 to 155)

Unit-III

Ideals and homomorphisms – Sum and direct sum of ideals – Maximal and prime ideals –Nilpotent and nil ideals - Zorn's lemma. (Pages179 to 211)

Unit-IV

Unique factorization domains(UFD) – Principal ideal domains – Euclidean domains –Polynomial rings over UFD- Rings of Fractions. (Pages 212 to 228)

Text Book : Basic Abstract Algebra by P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul.

Reference :

[1] Topics in Algebra by I. N. Herstein.

[2] Elements of Modern Algebra by Gibert and Gilbert.

[3] Abstract Algebra by Jeffrey Bergen.

[4] Basic Abstract Algebra by Robert B Ash.

Contents

UNIT-I

LESSON-01

PRELIMINARIES

NORMAL SUBGROUPS-ISOMORPHISM THEOREMS

1.1 Introduction.

Recall that the symmetric group on three symbols is denoted by S_3 and is described as follows

$$S_3 = \{e, a, a^2, b, ab, a^2b / \ a^3 = 2 = b^2, ba = a^2b\}$$

Clearly $H = \{e, b\}$ is a subgroup of S_3.

Now consider the cosets aH, Ha where $a \in S_3$

$aH = \{ae, ab\} = \{a, ab\}$

and $Ha = \{ea, ba\} = \{a, ba\} = \{a, a^2b\}$.

Observe that $aH \neq Ha$ whereas if $N = \{e, a, a^2\}$ then we also know that N is a subgroup of S_3

Now for $b \in S_3$, we have $bN = \{be, ba, ba^2\} = \{b, a^2b, ab\}$.

and $Nb = \{b, ab, a^2b\}$.

In this case observe that $bN = Nb$. It is not a just coincidence.

E.Galois is the first mathematician, who recognised that those subgroups of a group for which the left and right cosets coincide are of some special one. This observation led to the following notion of normal subgroups.

1.2 Normal Subgroup.

1.2.1 Definition:

Let G be a group. A subgroup N of G is called a normal subgroup of G if $xNx^{-1} \subset N$ for every $x \in G$. We denote this by writing $N \lhd G$.

Observe that $G, \{e\}$ are always normal subgroups of a group G where $e \in G$ is the identity. Further note that, if G is an abelian group, then every subgroup of G is normal in G.

In the following theorem, we give some equivalent conditions for a subgroup of a group to be a normal subgroup.

1.2.2 Theorem

Let N be a subgroup of a group G. Then the following are equivalent.

(i) $N \triangleleft G$

(ii) $xNx^{-1} = N$ for every $x \in G$.

(iii) $xN = Nx$ for every $x \in G$.

(iv) $(xN)(yN) = xyN$ for all $x, y \in G$.

Proof.

Given that N is a subgroup of a group G.

To prove the theorem, we prove $(i) \Rightarrow (ii), (ii) \Rightarrow (iii), (iii) \Rightarrow (iv)$ and $(iv) \Rightarrow (i)$.

(1) $(i) \Rightarrow (ii)$

First suppose N is a normal subgroup of G i.e. $N \triangleleft G$. Let $x \in G$.

Then by definition of a normal subgroup, $xNx^{-1} \subset N$. Also we have $x^{-1} \in G$. Hence $xNx^{-1} \subset N$. Therefore $N = x(x^{-1}Nx)x^{-1} \subset xNx^{-1}$ which proves that $N \subset xNx^{-1}$. Hence $xNx^{-1} = N$, proving (ii).

(2) $(ii) \Rightarrow (iii)$

Now suppose $xNx^{-1} = N$ for every $x \in G$.

$$Nx = (xNx^{-1})x = xNe = xN.$$

proving (iii).

(3) $(iii) \Rightarrow (iv)$

Suppose $xN = Nx$ for every $x \in G$.

Let $y \in N$

Now $(xN)(yN) = x(Ny)N = x(yN)N = xyNN = xyN$.

Since $NN = N$ as N is a subgroup of G.

Therefore $xN.yN = xyN$.

(4) $(iv) \Rightarrow (i)$

Finally assume that (iv) holds

That is $xN.yN = xyN$ for all $x, y \in G$.

Now $xNx^{-1} = xNx^{-1}e \subset xx^{-1}N = eN = N$ since $x^{-1}e \in x^{-1}N$.

Proving that $xNx^{-1} \subset N$ (actually we have $xNx^{-1} = N$).

Hence $N \lhd G$. Hence the theorem.

Some other results on normal subgroup, we relegate to exercises.

1.3 Quotient group.

If N is a normal subgroup of G, we have shown that every left coset of N in G is a right coset of N in G and vice versa , that is we cannot distinguish between the left and right cosets of N.

We denote that set of all left (right) cosets of N in G by $\frac{G}{N}$. Also recall that this set is closed under multiplication of cosets namely $xN.yN = xyN$, where $x, y \in G$.

1.3.1 Definition.

Let N be a normal subgroup of a group G then the set $\frac{G}{N}$ of all left (right) cosets of N is a group under coset multiplication that $\frac{G}{N} = \{xN | x \in G\}$.

$$xN.yN = xyN \text{ where } x, y \in G.$$

It is easy to see that $\left(\frac{G}{N}, .\right)$ is a group under multiplication the group $\frac{G}{N}$ is called the quotient group of G by N.

1.3.2 Remark.

Recall if $(G, .)$ and $(G, *)$ are any two groups and $f : G \to G^{'}$ is a homomorphism, then the kernel of ϕ is denoted by $ker\phi$ and is defined as

$$kerf = \{x \in G/f(x) = e^{'}\}.$$

where $e^{'}$ is the identity of $G^{'}$.

Clearly $e \in kerf$ and $kerf$ is always a normal subgroup of G.

Further if the mapping $\phi : G \to \frac{G}{N}$ is defined by $\phi(x) = xN, x \in G$. Then ϕ is a surjective homomorphism and $ker\phi = N$. This mapping ϕ is called as the canonical homomorphism.

1.3.3 Definition

Let G be a group and S be a non empty subset of G. Then the normalizer of S in G is denoted by $N(S)$ and is defined as $N(S) = \{x \in G/xSx^{-1} = S\}$.

If $S = \{a\}$ that is the normalizer of a singleton set $\{a\}$ is denoted by $N(a)$.

Clearly $N(S)$ is a subgroup of G.

Further if H is any subgroup of G, then $N(H)$ is the largest subgroup of G in which H is normal. Also if K is a subgroup on $N(H)$, then H is a normal subgroup of KH.

1.4 Derived group

Let G be a group. For any $a, b \in G$, $aba^{-1}b^{-1}$ is called a commutator in G.

The subgroup of G generated by the set of all commutators in G is called as the commutator subgroup of G or the derived subgroup of G. We denote this by $G^{'}$.

1.4.1 Remark

It is easy to see that $G^{'}$ is a normal subgroup of G and the quotient group $\frac{G}{G^{'}}$ is abelian. Further if $H \lhd G$ then $\frac{G}{H}$ is abelian if and only if $G^{'} \subset H$.

1.5 Isomorphism Theorems

Let N be a normal subgroup of G. We know that the quotient group $\frac{G}{N}$ is the homomorphic image of G under the canonical homomorphism (Remark 1.3.2). We now prove this, that is every homomorphic image of a group G is isomorphic to a quotient group of G. More precisely, we state the first isomorphism theorem.

Theorem 1.5.1 First Isomorphism Theorem

Let $\phi : G \rightarrow G^{'}$ be a homomorphism of groups then $\frac{G}{ker\phi} \simeq Im\phi$. Hence in particular, if ϕ is surjective, then $\frac{G}{ker\phi} \simeq G^{'}$.

Proof.

Given that $\phi : G \rightarrow G^{'}$ be a homomorphism of groups let $K = ker\phi = \{x \in G/\phi(x) = e^{'}\}$. Also recall $Im\phi = \phi(G) = \{\phi(x)/x \in G\}$.

Now define the mapping $\psi : \frac{G}{K} \rightarrow Im\phi$ by $\psi(xK) = \phi(x)$ for any $xK \in \frac{G}{K}$.

First we show that ψ is well defined.

For any $x, y \in G$ let $xK = yK$ which implies $y^{-1}x \in K$. Thus we have $\phi(y^{-1}x) = e^{'}$ from which we get $\phi(y^{-1})\phi(x) = e^{'}$ which imply $\phi(x) = \phi(y)$.

Hence ψ is well defined.

We now prove that ψ is a homomorphism.

For $x, y \in G$, $\psi(xK.yK) = \psi(xyK) = \phi(xy) = \phi(x)\phi(y)$.

$= \psi(xK)\psi(yK)$ since K is a normal subgroup of G and ϕ is a homomorphism, proving that ψ is a homomorphism.

Also if $\psi(xK) = \psi(yK)$ we have $\phi(x) = \phi(y)$.

which imply $\phi(y)^{-1}\phi(x) = e^{'}$ which gives $\phi(y^{-1}x) = e^{'}$.

$\Rightarrow y^{-1}x \in K \Rightarrow xK = yK$, proving that ψ is one-one.

Also if $\phi(x) \in Im\phi$ for $x \in G$, we have $\psi(xK) = \phi(x)$, showing that ψ is onto.

Therefore $\frac{G}{K}$ is isomorphic to $Im\phi$ that is $\frac{G}{K} \simeq Im\phi$.

Further if ϕ is onto then $Im\phi = G'$, we have $\frac{G}{K} \simeq G'$, completing the proof.

As the second and third isomorphism theorems are simple consequences of first isomorphism theorem, we leave the proofs of these theorems to the reader as exercise. so we just state these results in the following theorems.

1.5.2 Theorem (Second isomorphism theorem)

Let H and N be subgroups of a group G and $N \lhd G$. Then $\frac{H}{H \cap N} \simeq \frac{HN}{N}$.

Proof. Exercise.

1.5.3 Theorem (Third isomorphism theorem)

Let H and K be normal subgroups of a group G and $K \subset H$. Then

$$\frac{\frac{G}{K}}{\frac{H}{K}} \simeq \frac{G}{H}.$$

Proof. Exercise.

The following theorem provides a relationship between the subgroups (normal subgroups) of a group G and the subgroups (normal subgroups) of another group G' where $\phi : G \to G'$ is a homomorphism. As the proof of this theorem is simple, the details are left to the reader. This result is known as correspondence theorem.

1.5.4 Theorem (Correspondence theorem)

Let $\phi : G \to G'$ be a homomorphism of group G onto a group G'. Then the following are true.

(i) $H < G \Rightarrow \phi(H) < G'$.

(ii) $H^{'} < G^{'} \Rightarrow \phi^{-1}(H^{'}) < G$.

(iii) $H \lhd G \Rightarrow \phi(G) \lhd G^{'}$.

(iv) $H^{'} \lhd G^{'} \Rightarrow \phi^{-1}(H^{'}) \lhd G$.

(v) The mapping $H \mapsto \phi(H)$ is a $1-1$ correspondence between the family of subgroups of G containing $ker\phi$ and the family of subgroups of $G^{'}$; further more, normal subgroups of G correspond to normal subgroups of $G^{'}$.

Proof. Exercise.

1.5.5 Remark

Let N be a normal subgroup of G. Given any subgroup $H^{'}$ of $\frac{G}{N}$, there is a unique subgroup H of G such that $H^{'} = \frac{H}{N}$. Further $H \lhd G$ if and only if $\frac{H}{N} \lhd \frac{G}{N}$.

1.6 Definition (Maximal normal Subgroup)

Let G be a group. A normal subgroup N of G is called a maximal normal subgroup of G if

(i) $N \neq G$.

(ii) $H \lhd G$ and $H \supset N \Rightarrow H = N$ or $H = G$.

1.6.1 Definition

A group G is said to be simple if G has no proper normal subgroups; that is G has no normal subgroups except $\{e\}$ and G.

1.6.2 Remark:

Let N be a proper normal subgroup of G. Then N is maximal normal subgroup of G if and only if $\frac{G}{N}$ is simple.

1.6.3 Remark

Let H and K be distinct normal subgroups of a group G then $H \cap K$ is maximal normal subgroup of H and also of K.

1.7 Summary

In this lesson we have introduced the notion of normal subgroup and then defined quotient group. Also we have defined the derived group.

Also we have observed that normal subgroups are kernels of homomorphisms and vice versa. Further we have proved first isomorphism theorem and stated correspondence theorem. At the end of the section, we have defined the notion of maximal subgroups and then stated a result which establishes the relation between simple groups and maximal normal subgroups.

1.7 Model Examination Questions

(1) Prove that the center $Z(G) = \{x \in G/xa = ax \ \forall a \in G\}$ is a normal subgroup of the group G.

(2) Let G be a group and H is a subgroup of index 2, then show that H is a normal subgroup of G.

(3) If N and M are normal subgroups of a group G such that $N \cap M = \{e\}$ then show that $nm = mn$ for all $n \in N, m \in M$.

(4) Give an example of a non abelian group each of whose subgroups is normal.

(5) If N is a normal subgroup of a group G and H is a subgroup of G then show that NH is a subgroup of G. Further if $H \lhd G$, then show that NH is also normal in G.

(6) Let H be a subgroup of G such that $x^2 \in H$ for every $x \in G$. Then show that H is a normal subgroup of G.

(7) Write down all normal subgroups of S_4.

(8) If G is a group with center $Z(G)$ and if $\frac{G}{Z(G)}$ is cyclic then show that G

is abelian.

(9) Show that there does not exist any group G such that $\left|\frac{G}{Z(G)}\right| = 37$.

(10) Show that a non abelian group of ordet 6 is isomorphic to S_3.

(11) Write down all the homomorphic images of

(i) the Klein four group.

(ii) the octic group.

(12) Show that each dihedral group is isomorphic to the group of order 2.

1.9 Glossary

Normal subgroup, Quotient group, Derived group, Simple group.

LESSON-02

AUTOMORPHISMS

2.1 Introduction.

The central idea which is common to all aspects of modern algebra is the notion of homomorphism. By this we mean a mapping from one algebraic system to another algebraic system which preserves structure

In the following section, we give some basic definitions which are useful in later sections of our lesson

2.2 Basic Definitions.

Let G and H be any two groups.

(i) A mapping $\phi : G \to H$ is called a homomorphism

if $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

(ii) If $\phi : G \to H$ is a one - one homomorphism, then ϕ is called

a monomorphism of G into H.

In this case we say that ϕ is an embedding of G into H

(iii) If $\phi : G \to H$ is an onto homomorphism,

then ϕ is said to be an epimorphism.

In this case we say that G is homomorphic to H

or H is said to be the homomorphic image of G

(iv) If $\phi : G \to H$ is a bijective homomorphism,

then ϕ is said to be an isomorphism of G onto H, and we say that G is isomorphic to H and in this case we denote it by writing $G \simeq H$.

(v) A homomorphism of G into itself is called an endomorphism of G

2.3 Definition: Automorphism

An isomorphism of a group G onto into itself is called an automorphism, that is an automorphism of group G is an automorphism of G is an isomorphism of G onto G itself.

The set of all automorphisms of G is denoted by Aut(G) that is

$Aut(G) = \{\phi : \phi : G \to G \text{ is an isomorphism}\}$

2.3.1 Remark:

For any group G, the identity map $i : G \to G$ defined by $i(x) = x \;\; \forall x \in G$ is an automorphism

Thus for any group G, $Aut(G)$ is non empty

2.3.2 Lemma:

Let G be a group. For every $g \in G$, the mapping $I_g : G \to G$ defined by $I_g(x) = gxg^{-1}$ for all $x \in G$ is an automorphism of G.

Proof: Given that G is a group.

For any $g \in G$, $I_g(x) = gxg^{-1}$ for any $x \in G$

First we prove that I_g is a homomorphism.

Let $x, y \in G$

$I_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = I_g(x)I_g(y)$.

I_g is one-one : For any $x, y \in G$,

If $I_g(x) = I_g(y)$, then $gxg^{-1} = gyg^{-1}$

We have $x = y$

Further I_g is onto: For each $x \in G$. There exists an element $gxg^{-1} \in G$ such that $I_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$

Therefore I_g is an automorphism of G.

2.3.3 Definition: Inner automorphism:

Let G be a group. For a given $g \in G$, the mapping $I_g : G \to G$ defined by $I_g(x) = gxg^{-1}$ for all $x \in G$ is an automorphism of G,is called an inner automorphism of G determined by $g \in G$.

The set of all inner automorphism of G is denoted by $Inn(G)$ or in G.

2.3.4 Remark:

For any group G, $Inn(G)$ is nonempty since every element of G determines an inner automorphism of G and $Inn(G)$ is subset of $Aut(G)$.

2.3.5 Theorem:

The set $Aut(G)$ of all automorphisms of a group G is a group under the composition of mappings and $Inn(G) \lhd Aut(G)$

Moreover $\frac{G}{Z(G)} \lhd Inn(G)$

Proof: Let G be any group. Then we know that the symmetric group S_G is the group of all permutations of G under the composition of mappings.

Since the identity map on G is an automorphism of G , we have $Aut(G)$ is non empty.

Clearly, $Aut(G) \subset S_G$

i) First we prove that $Aut(G)$ is a group

Let $\sigma, \tau \in Aut(G)$ then $\sigma\tau$ and σ^{-1} are bijective.

For all $x, y \in G$, we have

$$
\begin{aligned}
(\sigma\tau)(xy) = \sigma(\tau(xy)) &= \sigma(\tau(x)\tau(y)) \\
&= \sigma(\tau(x))\sigma(\tau(y) \\
&= (\sigma\tau)(x)(\sigma\tau)(y)
\end{aligned}
$$

Showing that $\quad \sigma\tau \in Aut(G)$

$$
\begin{aligned}
\text{Further, } \sigma(\sigma^{-1}(x)\sigma^{-1}(y)) &= \sigma(\sigma^{-1}(x))\sigma(\sigma^{-1}(y)) \\
&= (\sigma\sigma^{-1})(x)(\sigma\sigma^{-1}(y) \\
&= xy
\end{aligned}
$$

Which gives $\quad \sigma^{-1}(xy) = \sigma^{-1}(x)\sigma^{-1}(y)$

Thus $\quad \sigma^{-1} \in Aug(G) \;\; \forall \;\; \sigma \in Aut(G)$

Therefore $Aut(G)$ is a subgroup of the symmetric group S_G

Hence $Aut(G)$ is a group.

(ii) We now prove $\frac{G}{Z(G)} \cong Inn(G)$

Define a mapping $\phi : G \to Aut(G)$ by $\phi(a) = I_a$ for any $a \in G$

For any $a, b \in G$ and for all $x \in G$,

$$\begin{aligned} I_{ab}(x) &= (ab)x(ab)^{-1} \\ &= a(bxb^{-1})a^{-1} \\ &= I_a(bxb^{-1}) \\ &= I_a I_b(x) \end{aligned}$$

which implies $I_{ab} = I_a I_b$

That is $\phi(ab) = I_{ab} = I_a I_b = \phi(a)\phi(b)$

showing that ϕ is a homomorphism.

Also for every $I_a \in Aut(G)$, there exists $a \in G$ such that $\phi(a) = I_a$.

$$\begin{aligned} \text{Now, } \ker\phi &= \{a \in G/\phi(a) = \text{identity automorphism of G }\} \\ &= \{a \in G/I_a = \text{ identity automorphism of G }\} \\ &= \{a \in G/I_a(x) = x \ \ \forall x \in G\} \\ &= \{a \in G/axa^{-1} = x \ \ \forall x \in G\} \\ &= \{a \in G/ax = xa \ \ \forall x \in G\} \\ &= Z(G), \text{ the center of G.} \end{aligned}$$

Therefore, by the fundamental theorem of homomorphism, $\frac{G}{\ker\phi} \cong Inn(G)$

That is $\frac{G}{Z(G)} \cong Inn(G)$.

(iii) Finally, we prove $Inn(G) \lhd Aut(G)$

Let $\sigma \in Aut(G)$ and $I_a \in Inn(G)$ where $a \in G$.

$$\begin{aligned} \text{Now, } \ (\sigma I_a \sigma^{-1})(x) &= \sigma I_a(\sigma^{-1}(x)) \\ &= \sigma(I_a(\sigma^{-1}(x))) \end{aligned}$$

$$= \sigma(a\sigma^{-1}(x)a^{-1})$$
$$= \sigma(a)\sigma(\sigma^{-1}(x))\sigma(a^{-1})$$
$$= \sigma(a)x\sigma(a^{-1})$$
$$= I_{\sigma(a)}(x) \quad \text{for any } x \in G$$

Therefore, we have $\sigma I_a \sigma^{-1} = I_{\sigma(a)}$ where $\sigma(a) \in G$.

As $\sigma(a) \in G$, we have $I_{\sigma(a)} \in Inn(G)$

Hence we have $\sigma I_a \sigma^{-1} \in Inn(G) \ \forall \ \sigma \in Aut(G), \ I_a \in Inn(G)$

Which shows that $Inn(G) \lhd Aut(G)$

2.3.6 Remark:

If $Z(G) = \{e\}$, then from of the above theorem $G \cong Inn(G)$.

2.3.7 Definition: Complete group

A group G is said to be complete if (i) $Z(G) = \{e\}$, and

(ii) every automorphism of G is an inner automorphism of G

That is G is complete if $G \simeq Inn(G) = Aut(G)$.

2.3.8 Example.

Let σ be an automorphism of a group G. Then for any $x \in G$, x and $\sigma(x)$ are of same order

Proof:- Given that $\sigma : G \to G$ is an automorphism where G is any group and let $x \in G$

Let $o(x) = m$ and $\sigma(x) = n$

we now show that m=n

Now, $(\sigma(x))^m = \sigma(x).\sigma(x).\cdots\sigma(x)$ (m times)

$$= \sigma(x^m)$$

$$= \sigma(e)$$
$$= e$$

But $o(\sigma(x)) = n$. Therefore $n/m \to (1)$

Again $\sigma(x^n) = \sigma(x.x.x...x)$

$$= \sigma(x).\sigma(x).\sigma(x) \cdots \sigma(x) \quad \text{(n times)}$$
$$= (\sigma(x))^n$$
$$= e$$
$$= \sigma(e)$$

This implies $x^n = e$, since σ is one-one

But $o(x) = m$ Therefore $m/n \to (2)$

Form (1) and (2) it follows that m=n

In the following example, we prove S_3 is a complete group

2.3.9 Example:

The symmetric group S_3 is complete

Proof. We know that the symmetric group S_3 is as described as follows

$S_3 = \{< a, b > /a^3 = e = b^2, ba = a^2b\}$

$\quad = \{e, a, a^2, ab, a^2b\}$

observe that $o(a) = o(a^2) = 3, \quad o(b) = o(ab) = o(a^2b) = 2$

We now determine $Z(S_3)$.

Clearly $ba = a^2b \neq ab \quad \Rightarrow \quad a, b \notin Z(S_3)$

and $(ab)(a^2b) = a(ba)ab = a.a^2bab = bab = a^2b.b = a^2$

$(a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a^4b^2 = ae = a$

Thus $(ab)(a^2b) \neq (a^2b)(ab)$, from which we have $ab, a^2b \notin Z(S_3)$

Further, if $a^2 \in Z(S_3)$ then $a = a^2.a^2 \in Z(S_3)$, a contradiction.

Therefore $Z(S_3) = \{e\}$

Hence by theorem 2.3.3, we have $\frac{S_3}{Z(S_3)} \simeq Inn(S_3)$

That is $S_3 \simeq Inn(S_3)$

We now define $Aut(S_3)$

For any $\sigma \in S_3$, we have $\sigma(a) = a$ or a^2 and

$\sigma(b) = b,\ ab$ or a^2b (in view of example 2.3.6)

as a,b are generators of S_3, $\sigma(x)$ is known for any $x \in S_3$

Therefore $|Aut(S_3)| \leq 6$

since $Inn(S_3)$ is a subgroup of order 6

we must have $|Aut(S_3)| = 6$ and $Inn(S_3) = Aut(S_3)$

Therefore $S_3 \simeq Inn(S_3) = Aut(S_3)$

Hence S_3 is a complete group.

2.3.10 Example:

Let G be a finite abelian group of order n and m be a fixed positive integer relatively prime to n.

Then the mapping $\sigma : G \to G$ defined by $\sigma(x) = x^m$ is an automorphism.

Solution:- Given that G is a finite abelian group of order n , and m be a natural number such that (m,n)=1

Also $\sigma : G \to G$ is given by $\sigma(x) = x^m$

For any $x, y \in G$, $\sigma(xy) = (xy)^m = x^m y^m$ since G is abelian

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

proving that σ is a homomorphism.

since m and n are relatively prime, there exists integers u and v such that mu+nv=1

For all $x \in G$, we have $x^n = e$ since $|G| = n$

$x^1 = x^{mu+nv} = x^{mu}.x^{nv} = x^{mu}.(x^n)^v = x^{mu}$

Therefore, for every $x \in G$ there exists an element $x^u \in G$ such that $\sigma(x^u) = x^{mu} = x$

showing that σ is surjective.

$$\begin{aligned}\ker\sigma &= \{x \in G/\sigma(x) = e\}\\ &= \{x \in G/x^m = e\}\\ &= \{x \in G/x^{mu} = e\}\\ &= \{x \in G/x = e\} = \{e\}\end{aligned}$$

showing that σ is one-one

Therefore σ is an automorphism of G

2.3.11 Example:

If G is an abelian group, then its inner automorphism group is trivial

Proof:- Given that G is an abelian group and

I_g be the inner automorphism determined by $g \in G$

That is for all $g \in G$, $\quad I_g(x) = gxg^{-1}\ \forall\ \ x \in G$

$$\begin{aligned}I_g(x) &= gxg^{-1}\\ &= gg^{-1}x\\ &= x = i(x) \text{ for all } x \in G \text{ and for any } g \in G\\ I_g &= i\end{aligned}$$

Therefore $Inn(g) = \{i/i : G \to G$ is the identity map $\}$

2.3.12 Example:

If G is a group of order 2 then $Aut(G)$ is trivial

Proof:- Let G be a group of order 2 and $G = \{e, a\}$

Then $Inn(G)$ is trivial. Since every group of order 2 is abelian.

If $\sigma \in Aut(G)$ then $\sigma(e) = e$ and $\sigma(a) = a$

This implies that $Aut(G)$ is trivial.

2.3.13 Example:

An abelian group with the condition that

$a^2 \neq e$ for some $a \in G$, has a non trivial automorphism.

Proof:- Let G be an abelian group with the condition that $a^2 = e$ for some $a \in G$

That is $a \neq a^{-1}$

Now, define $\sigma : G \to G$ by $\sigma(x) = x^{-1}$

Clearly, σ is an automorphism, since G is abelian

Also, $\sigma(a) = a^{-1} \neq a$

showing that σ is non identity automorphism.

Thus $Aut(G)$ is non trivial.

2.3.14 Example:

A non abelian group G always has a non trivial automorphism. Moreover if G is finite $|Inn(G)| = [G : Z(G)]$

Proof:- Let G is a non abelian group, then there exists elements $a, b \in G$ such that $ab \neq ba$ that is $aba^{-1} \neq b$

For $a \in G$ we have $I_a \in Inn(G)$ such that $I_a(b) = aba^{-1} \neq b$

Therefore, I_a is a non identity automorphism.

Thus G has a non trivial automorphism.

Further if G is finite non abelian group then its center $Z(G)$ is a subgroup of G and $Z(G) \neq G$

Therefore $|Z(G) < |G|$

By Theorem 1.1.7, we have $\frac{G}{Z(G)} \simeq Inn(G)$

This implies $|Inn(G)| = |\frac{G}{Z(G)}| > 1.$

showing that there exists a non trivial (inner) automorphism and

$|Inn(G)| = [G : Z(G)]$

2.3.15 Example:

A finite group G having more than two elements and with the condition that $x^2 \neq e$ for some $x \in G$ must have a non trivial automorphism

Solution: Given that G is a finite group. We consider two cases

Case(i): First assume that G is an abelian

Now define $\sigma : G \to G$ by $\sigma(x) = x^{-1} \ \forall \ x \in G$

Then σ is an automorphism of G

Infact

σ is a homomorphism

since $\sigma(xy) = (xy)^{-1} = x^{-1}y^{-1} = \sigma(x)\sigma(y)$ as G is abelian .

Also note that σ is one-one .

For if $\sigma(x) = \sigma(y)$, for $x, y \in G$

$$x^{-1} = y^{-1}$$

$$x = y$$

σ is onto. Since for any $x \in G$, we have $x^{-1} \in G$ is such that

$\sigma(x^{-}) = (x)^{-1} = x$

Therefore σ is non identity automorphism.

Case(ii): Now assume that G is non abelian

Define $\tau : G \to G$ by $\tau(g) = xgx^{-1}$

If $\tau(g) = \tau(h)$

then $xgx^{-1} = xhx^{-1} \Rightarrow g = h$

showing that τ is one-one.

For any $g \in G$ consider $x^{-1}gx \in G$

$\tau(x^{-1}gx) \; = \; x(x^{-1}gx)x^{-1} = g$

proving that τ is onto

Also for any $\quad g, h \in G,$

$\tau(gh) = x(gh)x^{-1} = xgx^{-1}xhx^{-1} = \tau(g)\tau(h)$

Proving that $\tau \in Aut(G)$.

Therefore τ is a non trivial inner automorphism

Hence $\quad |Aut(G)| > 1$, in this case also .

2.3.16 Example:

If G is an infinite cyclic group then $|Aut(G)| = 2$

Proof:- Given that G is an infinite cyclic group.

We know that every infinite cyclic group is isomorphic to $\quad (\mathbb{Z}, +)$

Further we have $\quad \mathbb{Z} = \; < 1 > \; = \; < -1 >$

Let $\;\sigma : \mathbb{Z} \to \mathbb{Z}\quad$ be an automorphism

Since 1 is a generator of $\mathbb{Z}$, $\quad$ we have $\quad \sigma(1)\;$ is also a generator of $\;\mathbb{Z}$

Thus $\sigma(1)\quad$ has two choices namely 1 and -1.

If $\quad \sigma_1(1) = 1$

For $n \neq 1$, $\quad \sigma_1(n) = \sigma_1(1 + 1 + 1 + \cdot + 1) \qquad$ (n times)

$$= \sigma_1(1) + \sigma_1(1) + \cdot + \sigma_1(1)$$

$$= n.1 \quad = n$$

Also we know that $\sigma_1(-n) = -\sigma_1(n) = -n \quad$ since σ_1 is a homomorphism

This shows that $\sigma_1 = i$, $\quad$ the identity automorphism of $\mathbb{Z}$.

If $\sigma_2(1) = -1$ then $\quad \sigma_2(n) = -n \;\; \forall \;\; n \in \mathbb{Z}$

Thus $\quad \sigma_2^2 = i$

Therefore $\quad |Aut(\mathbb{Z})| = 2$

2.3.17 Example:

Let $G = [a]$ be a finite cyclic group of order n. Then the mapping σ defined by $a \vdash a^m$ is an automorphism of G if and only if (m,n)=1

Proof:- Given that $G = [a]$ and $|G| = n$. Hence $o(a) = n$

we have $\sigma : G \to G$ defined by $\sigma(x) = x^m$

If (m,n)=1 then by example 2.3.10, we have σ is an automorphism

Conversely, Suppose that σ is an automorphism of G.

Then the order of $\sigma(a) = a^m$ is same as that order of a.

That is $o(a^m) = o(a) = n$.

If (m,n)=d then $((a)^m)^{(\frac{n}{d})} = ((a)^n)^{(\frac{m}{d})} = e$

since $o(a) = n$ and also using the fact $o(a^m) = n$

We have n divides $\frac{n}{d}$. This possible if d=1

Therefore, (m,n)=1

2.3.18 Example:

If G is a finite cyclic group of order n, then show that $|Aut(G)| = \phi(n)$ where ϕ is Euler's totient function.

Proof:- Let $G = [a]$, $|G| = n$and $\sigma \in Aut(G)$.

If $x \in G$ then $x = a^k$ for some $k \in \mathbb{N}$.

Now, $\sigma(x) = \sigma(a^k) = (\sigma(a))^k$

Therefore σ is completely known if $\sigma(a)$ is known

Let $\sigma(a) = a^m$, $m \leq n$

By example 2.3.17, we know that

$\sigma \in Aut(G)$ if and only if (m,n)=1.

That is each positive integer less than n and relatively prime to n determines a unique $\sigma \in Aut(G)$ and conversely each $\sigma \in Aut(G)$ determines a unique positive integer m less than n and relatively prime to n.

Therefore $|Aut(G)| = |\{m \in \mathbb{Z}^+/1 \leq m \leq n, \ \ (m,n) = 1\} = \phi(n)$

2.3.19 Example:

Show that only cyclic group G of order $n > 2$ has an automorphism which is not an inner automorphism

Proof: Given that G is cyclic.

Therefore G is abelian.

Hence $Inn(G)$ is trivial.

We have $|Aut(G)| = \phi(n) > 1$ since $n > 2$.

Thus G has an automorphism which is not an inner automorphism.

2.4 Summary.

In section 2.3, we have defined inner automorphism of a group and complete group. Also we have determined the automorphism groups of a finite cyclic group and infinite cyclic group.

2.5 Model Examination Questions.

(1) If K is the klein four group, then find $Aut(G)$ also determine $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

(2) Let G be a group and $\sigma : G \to G$ is an automorphism of G. If for $a \in G$, $N(a) = \{x \in G/xa = ax\}$. Then prove that $N(\sigma(a)) = \sigma(N(a))$

(3) Let G be the group of order 9 generated by elements a and b, where $a^3 = b^3 = e$. Then find $Aut(G)$.

(4) Show that $Aut(\mathbb{Z}_2 \times \mathbb{Z}_3) \simeq Aut(\mathbb{Z}_2) \times Aut(\mathbb{Z}_3)$.

2.6 Glossary.

Automorphism, Inner automorphism, Complete group

LESSON-03

G-SETS AND CLASS EQUATION

3.1 Introduction.

Group actions are powerful tool for proving theorems for abstract group and for determining the structure of specific groups. The concept of an action is a method for studying how an algebraic structure interact with other structures. In this lesson we study the action of a group G on an arbitrary set first then on the group itself. We deduce orbit decomposition of any arbitrary set X under the action of a group G. Moreover we establish Cayley's theorem. Further using the conjugacy relation among the elements of a group G, we derive class equation. This class equations has numerous applications in studying finite groups. Also at the end of this lesson, we prove Burnside theorem.

3.2 Action of a group on a set.

3.2.1 Definition:

Let G be a group and X is any set. Then we say that G acts on X if there is a mapping $\phi : G \times X \to X$, with $\phi(a, x)$ written as $a * x$ such that for all $a, b \in G,\ x \in X$

(i) $a * (b * x) = (ab) * x$

(ii) $e * x = x$

The mapping ϕ is called the action of G on X and X is said to be a G-set.

In the above definition, we have defined the action of G on X on the left side. In a similar manner, we can define action on the right side also. From now onwards we restrict ourselves to groups acting on the left side only

3.2.2 Examples:

(a) Let G be any group. Take $X = G$. Define $a * x = axa^{-1}, \quad a \in G, x \in X$

For all $a, b, x \in G$ we have

(i) $a * (b * x) = a * (bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = ab * x$

(ii) $e * x = exe^{-1} = x$

Therefore G is a G-set.

This action of the group G on itself is called conjugation.

(b) Let G be a group and X= G. Define $a * x = ax,\ a \in G,\ x \in G$

For all $a, b, x \in G$ we have

(i) $a * (b * x) = a(bx) = (ab)x = (ab) * x$

(ii) $e * x = ex = x$

Showing that G is a G-set.

This action of the group G on it self is called translation.

(c) Let G be a group and H is subgroup of G. Let $X = \frac{G}{H}$ of left cosets can be made into a $G - set$ by defining $a * xH = axH,\ a \in G,\ xH \in \frac{G}{H}$.

Infact, for any $a, b \in G,\ xH \in \frac{G}{H}$, we have

(i) $a * (b * xH) = a * (bxH) = a(bx)H = (ab)xH = ab * xH$

(ii) $e * xH = ex$

Thus $\frac{G}{H}$ is G-set.

(d) Let G be a group and $H \lhd G$.

Consider $\frac{G}{H}$, the set of left cosets of H in G.

Define $a * xH = axa^{-1}H,\ a \in G,\ xH \in \frac{G}{H}$.

For all $a, b \in G,\ xH \in \frac{G}{H}$ we have

(i) $a * (b * xH) = a * (bxb^{-1}H) = abxb^{-1}a^{-1}H$

$$= abx(ab)^{-1}H$$

$$= ab * xH$$

(ii) $e * xH = exe^{-1}H = xH$

Hence $\frac{G}{H}$ is a G-set.

3.2.3 Remark:

(i) We can also define action of G on X on the right hand side also by defining $\phi : X \times G \to X$ with $\phi(x, a)$ written as $x * a$ satisfying

(i) $(x * a) * b = x * (ab)$

(ii) $x * e = x \quad \forall\ a, b \in G,\ x \in X.$

(ii) If X is a G-set, we write ax instead $a * x$ for the sake of simplicity.

3.2.4 Theorem:

Let G be a group and X is a non empty set. Then

(i) If X is a G-set, then the action of G on X induces a homomorphism $\phi : G \to S_X$.

(ii) Any homomorphism $\phi : G \to S_X$ induces an action of G onto X.

Proof: (i) Given that X is a G-set.

Therefore there is a map from $G \times X$ into X and

the image of $(a, x) \in G \times X$ is denoted by $a * x$

Now, define $\phi : G \to S_X$. by $\phi(a)(x) = a * x\ a \in G,\ x \in X$

Note that $\phi(a) \in S_X$, the permutation group on X.

Clearly $\phi(a)$ is bijective map on X.

Let $a, b \in G$. For all $x \in X$, we have

$$\begin{aligned} (\phi(ab))(x) = (ab) * x &= a * (b * x) \\ &= \phi(a)\big(\phi(b)(x)\big) \\ &= \phi(a)\phi(b)(x) \end{aligned}$$

$\Rightarrow \phi(ab) = \phi(a)\phi(b) \quad \forall\ a, b \in G$

Hence $\phi : G \to S_X$ is a homomorphism that arises due to the action of G on

X

(ii) Suppose $\phi : G \to S_X$ is a homomorphism.

Define $a * x = (\phi(a))(x)$ where $a \in G,\ x \in X$.

This defines a mapping whose domain is $G \times X$ and codomain is X

$$\begin{aligned} \text{Now, } a * (b * x) &= \phi(a)\big(\phi(b)(x)\big) \\ &= \big(\phi(a)\phi(b)\big)(x) \\ &= \phi(ab)(x) \\ &= ab * x \end{aligned}$$

since ϕ is homomorphism .

$e * x = (\phi(e))(x) = x$ as $\phi(e)$ is the identity on X.

Therefore X is a G-set.

3.2.5 CAYLEY'S THEOREM:

Let G be a group. Then G is isomorphic into the symmetric group S_G

Proof: Let G be a group. we now regard G itself as a G-set and apply the first part of the Theorem 3.2.4

Define $a * x = ax, \quad a \in G,\ x \in G$

Clearly $e * x = x \ \forall\ x \in G$ and since by associativity in G

we have $a * (b * x) = ab * x \ \ \forall\ a, b, x \in G$.

Thus G is a G-set and the action of G itself is $a * x = ax \ \forall\ a \in G,\ x \in G$

Thus by part (i) of the Theorem 3.2.4, this action induces a homomorphism.

$\phi : G \to S_G$ where $\phi(a)(x) = a * x = ax$ for all $a \in G,\ x \in G$.

$$\begin{aligned} \text{Now } \ker \phi &= \{a \in G / \phi(a) = \text{ the identity of } S_G\} \\ &= \{a \in G / (\phi(a))(x) = i(x) \forall\ x \in G\} \\ &= \{a \in G / ax = x\ \forall\ x \in G\} \\ &= \{a \in G / a = e\} \qquad = \{e\} \end{aligned}$$

Showing that is ϕ injective

Therefore G is isomorphic into S_G

Hence the theorem.

3.2.6 Remark :

An isomorphism of a group G into a group permutations is called a faithful representation of G by a group of permutations.

The action of G on $\frac{G}{H}$ gives another representation of G by a group of permutations, which is not necessary faithful.

3.2.7 Theorem :

Let G be a group and H is a subgroup of index n. Then there is a homomorphism $\phi : G \to S_n$ such that $\ker \phi = \bigcap\limits_{x \in G} xHx^{-1}$.

Proof: Given that G is a group and H is a subgroup of index n.

Let $\frac{G}{H}$ be the set of all left cosets of H in G and $|\frac{G}{H}| = n$.

Now, define $a * xH = axH,\ a \in G,\ xH \in \frac{G}{H}$

Clearly, this defines a mapping from $G \times \frac{G}{H}$ into $\frac{G}{H}$

For all $a, b \in G, xH \in \frac{G}{H}$, we have

(i) $a * (b * xH) = a(bx)H = (ab)xH = (ab) * xH$

(ii) $e * xH = exH = xH$.

Therefore $\frac{G}{H}$ is a G-set.

Thus the above action of G on $\frac{G}{H}$ induces a homomorphism

$\phi_1 : G \to S_{\frac{G}{H}}$ defined by $\big(\phi_1(a)\big)(xH) = axH$

$$\begin{aligned}
\text{Now, } \ker \phi_1 &= \{a \in G / \phi_1(a) = \text{ identity of } S_{\frac{G}{H}}\} \\
&= \{a \in G / (\big(\phi_1(a)\big)(xH) = xH\ \forall\ x \in G\} \\
&= \{a \in G / axH = xH \forall\ x \in G\} \\
&= \{a \in G / x^{-1}axH = H \forall\ x \in G\}
\end{aligned}$$

$$= \{a \in G/x^{-1}ax \in H \forall\ x \in G\}$$
$$= \{a \in G/a \in xHx^{-1} \forall\ x \in G\}$$
$$= \bigcap_{x \in G} xHx^{-1}.$$

But we have $S_{\frac{G}{H}} \simeq S_n$ sice $|\frac{G}{H}| = n$,

Now let $\phi_2 : S_{\frac{G}{H}} \to S_n$ be the isomorphism

Then let $\phi = \phi_2\phi_1$

Further note that $\phi : G \to S_n$ is a homomorphism since the composition of homomorphisms is a homomorphism and

$$\ker\phi = \{a \in G/\phi(a) = \text{ identity of } S_n\}$$
$$= \{a \in G/\phi_2(\phi_1(a)) = \text{ identity of } S_n\}$$
$$= \{a \in G/\phi_1(a) = \text{ identity of } S_{\frac{G}{H}}\}$$
$$= \ker\phi_1$$

Since ϕ_2 is an isomorphism

Therefore $\ker\phi = \bigcap_{x \in G} xHx^{-1}$.

3.2.8 Remark:

If $H = \{e\}$, we get the Cayley's representation in which case it is faithful.

3.2.9 Corollary:

Let G be a group with a normal subgroup H of index n, then

$\frac{G}{H}$ is isomorphic into S_n.

Proof: From the Theorem 3.2.7, when H is a subgroup of G, there is a homomorphism $\phi : G \to S_n$ with $\ker\phi$ with $\ker\phi = \bigcap_{x \in G} xHx^{-1}$.

Given that $H \lhd G$ and $\ker\phi = H$ Since $xHx^{-1} = H$ for all $x \in G$.

Therefore by first isomorphism theorem $\frac{G}{\ker\phi} \simeq Im(\phi)$

Thus $\frac{G}{H}$ is isomorphic into S_n (where $Im(\phi) < S_n$)

Hence the Corollary.

3.2.10 Corollary: Let G be a simple group with a subgroup H($\neq G$) of a finite index n then G is isomorphic into S_n.

Proof: Let H be a subgroup of G, $H \neq G$ and $[G : H] = n$

By Theorem 3.2.7, there is a homomorphism $\phi : G \to S_n$ such that

$\ker \phi = \bigcap\limits_{x \in G} xHx^{-1}$.

Since $|H| < |G|$, we must have $|\ker \phi| < |G|$

We have $\ker \phi \lhd G$. Since G is simple, $\ker \phi = \{e\}$.

By the first isomorphism theorem $\frac{G}{\ker \phi} \simeq Im(\phi)$

That is G is isomorphic into S_n

Hence the result.

3.3 Orbit and Stabilizers:

3.3.1 Definition: Orbit

Let G be a group acting on a set X and let $x \in X$. Then

the set $Gx = \{a * x / a \in G\} = \{ax / a \in G\}$ is called the Orbit of x in G.

3.3.2 Definition: Stabilizer

Let G be a group acting on a set X and let $x \in X$.

Then the set $G_x = \{g \in G / gx = x\}$ is called the stabilizer of x in G

Some times it is called as the isotropy group of x in G

3.3.3 Lemma: G_x is a subgroup of G.

Proof: We have G is a group acting on a set X

That is for all $g \in G$, $y \in X$, we have $g * y \in X$ and

$a * (b * y) = (ab) * y$, $e * y = y$, $\forall$ $a, b \in G$ and $y \in X$.

Let $x \in X$ and the stabilizer of x in G is denoted by G_x and

$G_x = \{a \in G / a * x = x\}$

Clearly $G_x \neq \phi$ and $G_x \subset G$

For any $g_1, \quad g_2 \in G_x$, we have

$(g_1g_2) * x = g_1 * (g_2 * x) = g_1 * x = x$

$x = e * x = (g_1^{-1}g_1) * x = g_1^{-1} * (g_1 * x) = (g_1^{-1} * x)$

$\Rightarrow \quad g_1g_2 \in G_x$ and $g_1^{-1} \in G_x \;\; \forall\, g_1, g_2 \in G_x$

showing that G_x is a subgroup of G

3.3.4 Remark:

(i) $G_x \subset X$

(ii) For any $y \in G_x,\ G_x = G_y$

Let $y = b * x, \quad b \in G$. Then

$$
\begin{aligned}
G_y = \{a * y/a \in G\} &= \{a * (b * x)/a \in G\} \\
&= \{(ab) * x/a \in G\} \\
&= \{c * x/c \in G\} \\
&= G_x
\end{aligned}
$$

(iii) If G acts on itself by translation then for $x \in G$

$G_x = \{a \in G/a * x = x\} = \{a \in G/ax = x\} = \{e\}$

$G_x = \{a * x/a \in G\} = \{ax/a \in G\} = G$

(iv) If G acts on itself by conjugation then for $x \in G$,

$$
\begin{aligned}
G_x = \{a \in G/a * x = x\} &= \{a \in G/axa^{-1} = x\} \\
&= \{a \in G/ax = xa\} \\
&= N(x)
\end{aligned}
$$

In this case the stabilizer of an element x in G is the normalizer of x in G.

(v) Let H be a normal subgroup of G and consider the set $\frac{G}{H}$

The stabilizer of a left coset xH is the subgroup

$$
\begin{aligned}
G_{xH} &= \{g \in G/gxH = xH\} \\
&= \{g \in G/x^{-1}gxH = H\}
\end{aligned}
$$

$= \{g \in G/x^{-1}gx \in H\}$

$= \{g \in G/g \in xHx^{-1}\}$

$= xHx^{-1}$

3.3.5 Conjugate Class of an element:

Let G be a group and $x \in G$, Then

$C(x) = \{axa^{-1}/a \in G\}$ is called the Conjugate class of x.

3.3.6 Remark:

(i) $x \in C(x)$ and hence $c(x)$ is non empty.

(ii) If G acts on itself by Conjugation then for $x \in G$

$G_x = \{a * x/a \in G\}$

$= \{axa^{-1}/a \in G\}$

$= C(x)$

That is the Orbit of x in G is the conjugate class of x.

Also, $G_x = \{a \in G/a * x = x\}$

$= \{a \in G/axa^{-1} = x\}$

$= \{a \in G/ax = xa\}$

$= N(a)$

3.3.7 Theorem:

Let G be a group acting on a set X. Then the set of all Orbits in X under G is a partition of X.

For any $x \in X$ there is a bijection $Gx \to \frac{G}{G_x}$ and hence

$$|Gx| = [G : G_x]$$

Therefore if X is a finite set $|X| = \sum\limits_{x \in C} [G : G_x]$

where C is a subset of X containing exactly one elements from each Orbit.

Proof: Given that the group G acts on X.

For all $a, b \in G, \quad x \in X$, we have $a * x \in X$ satisfying

(i) $a * (b * x) = (ab) * x$ and

(ii) $e * x = x$.

For every $x \in X$, we have

$G_x = \{a \in G / a * x = x\}$ is stabilizer of x

And $Gx = \{a * x / a \in G\}$ is the orbit of x.

Also note that the stabilizer G_x is a subgroup of G and Gx, the orbit of x is a subset of X.

Now define a relation $\sim$ on X as follows

For $x, y \in X, \quad x \sim y$ means $x = a * y$ for some $a \in G$.

(i) For all $x \in X$, we have $x = e * x \Rightarrow \quad x \sim x \;\forall\; x \in X$

Thus $\sim$ is reflexive.

(ii) Suppose $x \sim y$ then $x = a * y$ for some $a \in G$

As $\;y = e * y = (a^{-1}a) * y$

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

$$= a^{-1} * x$$

Showing that $\quad y \sim x$

Thus $\sim$ is symmetric

(iii) If $\;x \sim y, \quad y \sim z\;$ then

$x = a * y, \quad y = b * z\;$ for some $a, b \in G$

Now $(ab) * z = a * (b * z) = a * y = x$

$\Rightarrow \quad x \sim z$

Thus $\sim$ is transitive.

Hence $\sim$ is an equivalence relation on X.

Therefore $\;\sim\;$ partitions X into mutually disjoint equivalence classes whose union is X.

Let $\bar{x}$ be the equivalence class of $x \in X$

Now, $\bar{x} = \{y \in x/y \sim x\}$

$= \{y \in X/y = a * x \ , a \in G\}$

$= \{a * x/a \in G\}$

$= Gx$

$=$ the orbit of x in G

This shows that the set of all orbits forms a partition of X and hence

$$X = \bigcup_{x \in C} Gx \longrightarrow (1)$$

Note that the above union is disjoint.

Where C is any subset of X containing exactly one element from each orbit.

For a given $x \in X$, define a mapping $\phi : Gx \to \frac{G}{G_x}$ by

$\phi(a * x) = aG_x$ for all $a \in G$

Now, for any $a, b \in G$

Let $a * x = b * x$

Now $(a^{-1}b) * x = a^{-1} * (b * x)$

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

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

$= e * x$

$= x$

and $(a^{-1}b) * x = x \Rightarrow \ a * x = a * ((a^{-1}b) * x)$

$= (aa^{-1}b) * x$

$= (eb) * x$

$= b * x$

Therefore $a * x = b * x \ \Leftrightarrow \ (a^{-1}b) * x = x$

$$\Leftrightarrow \; a^{-1}b \in G_x$$
$$\Leftrightarrow \; aG_x = bG_x$$
$$\Leftrightarrow \; \phi(a * x) = \phi(b * x)$$

This shows that ϕ is well defined and injective.

For every left Coset aG_x, there exists an element

$a * x \in G_x$ such that $\phi(a * x) = aG_x$

Showing that ϕ is surjective.

Hence ϕ is a bijection.

Therefore, $|Gx| = \frac{G}{G_x} = [G : G_x] \longrightarrow (2)$

Suppose X is a finite set. Then from (1) and (2)

We have $|X| = \sum_{x \in C} |Gx|$

$= \sum_{x \in C} [G : G_x]$

Since X is the disjoint union of orbits Gx

3.3.8 Definition:

The Orbit decomposition of a set X under a group G.

The partition $P = \{Gx/x \in C\}$ of X under action of G on X is called the orbit decomposition of X under G, where C is a subset of X containing exactly one element from each orbit

3.3.9 Remark :

Let G be a group and $a \in G$. Recall that

(i) $C(a) = \{xax^{-1}/x \in G\}$ is called the conjugate class of a in G.

(ii) $N(a) = \{a \in G/xax^{-1} = a\}$ is called the normalizer of a in G

3.3.10 Theorem:

Let G be a group . Then the following are true.

(i) The set of Conjugate class of G is a partition of G.

(ii) $|C(a)| = [G : N(a)]$

(iii) If G is a finite set then $|G| = \sum [G : N(a)]$, where the summation runs over exactly one element from each conjugate class.

Proof: Given that G is a group.

(i) Define a relation $\sim$ on G as follows

For, $a, b \in G$

$a \sim b \Leftrightarrow a = xbx^{-1}$ for some $x \in G$.

Now it is easy to see that the relation $\sim$ is an equivalence relation on G.

Therefore $\sim$ partitions G into mutually disjoint equivalence classes.

Let $\bar{a}$ be the equivalence class of $a \in G$.

$$\begin{aligned} \text{Then } \bar{a} &= \{y \in G / y \sim a\} \\ &= \{xax^{-1} / x \in G\} \\ &= C(a), \quad \text{the conjugate class of a} \end{aligned}$$

Now $a \in C(a)$ since $a = eae^{-1}$

Thus $a \in C(a) \subset G$

$\Rightarrow \{a\} \subset C(a) \subset G$

$$\Rightarrow \quad G = \bigcup_{a \in C} C(a) \longrightarrow (1)$$

a disjoint union of conjugate classes, and C contains exactly one element from each conjugate class.

(ii) Let $a \in G$. Define a map $\phi : C(a) \to \frac{G}{N(a)}$ by $\phi(xax^{-1}) = xN(a)$.

For every $xN(a) \in \frac{G}{N(a)}$ there exists $x \in G$, $xax^{-1} \in N(a)$

such that $\phi(xax^{-1}) = xN(a)$.

Showing that ϕ is surjective.

For any $x, y \in G$

If $\phi(xax^{-1}) = \phi(yay^{-1})$

$\Rightarrow \quad xN(a) = yN(a)$

$\Rightarrow \quad y^{-1}x \in N(a)$

$\Rightarrow \quad y^{-1}xa = ay^{-1}x$

$\Rightarrow \quad xax^{-1} = yay^{-1}$

$\Rightarrow \quad \phi$ is injective.

Therefore ϕ is bijective and hence

$|C(a)| = |\frac{G}{N(a)}| = [G : N(a)] \longrightarrow (2)$

(iii) In case if G is finite, then from (1) and(2) we have

$|G| = \sum_{a \in C} |C(a)| = \sum_{a \in C} [G : N(a)]$

where the summation is extended over exactly one element from each Conjugate class.

3.4 The Class Equation.

Let G be any group and we know that G acts on itself by conjugation action. Then the partition $\mathcal{P} = \{c(a)/a \in C\}$ of G under this conjugation action is called the class decomposition of G and the equation

$$|G| = \sum_{a \in C} \left[G : N(a)\right]$$

is called as the class equation of the group G Where C is a subset of G containing exactly one element from each conjugate class.

3.4.1 Definition.

Let G be a group and S be a subset of G. If $x \in G$, then the set

$$x^{-1}Sx = \{x^{-1}sx/s \in S\}$$

is called a conjugate of S.

3.4.2 Definition.

Let S, T be two subsets of a group G. Then T is said to be conjugate to S

if there exists $x \in G$ such that $T = xSx^{-1}$.

3.4.3 Remark.

The relation being "conjugate" is an equivalence relation in the power set $\mathbb{P}(G)$ of the group G.

Let $\sim$ be the relation conjugate to that is $S, T \in \mathbb{P}(G)$, then $S \sim T$ if and only if $T = xSx^{-1}$ for some $x \in G$.

Clearly for $S \in \mathbb{P}(G)$, $S = eSe^{-1}$. Therefore we have $S \sim S$ and hence $\sim$ is reflexive.

Let $S, T \in \mathbb{P}(G)$ and $S \sim T$ then $S = xTx^{-1}$ for some $x \in G$.

Thus we have $T = x^{-1}Sx, x \in G$.

That is $x^{-1}S(x^{-1})^{-1} = T, x^{-1} \in G$.

which implies $T \sim S$.

Now let $S, T, U \in \mathbb{P}(G)$ such that $S \sim T, T \sim U$.

then $S = xTx^{-1}, x \in G$.

$T = yUy^{-1}, y \in G$.

Therefore $S = xTx^{-1}$.

$= xyUy^{-1}x^{-1}$.

$= xyU(xy)^{-1}, xy \in G$.

showing that $S \sim U$.

Hence the relation 'conjugate' is an equivalence relation.

3.4.4 Theorem:

Let G be a group. For any subset S of G $|C(S)| = [G : N(S)]$, where $N(S) = \{x \in G | x^{-1}Sx = S\}$

Proof.

Given that G is a group and let $\mathbb{P}(G)$ be its power set.

We know that G acts as $\mathbb{P}(G)$ by the action 'conjugation', given by

$x * S = \{xSx^{-1} : x \in S\}$ where $S \subset G$.

Define a relation $\sim$ on $\mathbb{P}(G)$ as follows. For $S, T \in \mathbb{P}(G)$, $S \sim T \Leftrightarrow S = xTx^{-1}$ for some $x \in G$.

Clearly $'\sim'$ is an equivalence relation and partitions $P(G)$ into equivalence classes.

$\mathbb{P}(G) = \bigcup C(S)$, $S \subset G$ and the union is disjoint.

Now define a mapping $\sigma : C(S) \to \frac{G}{N(S)}$ by $\sigma(xSx^{-1}) = xN(S), x \in G$.

Clearly σ is one-one.

Infact if $\sigma(xSx^{-1}) = \sigma(ySy^{-1}),$ for any $x, y \in G$.

$$\Rightarrow xN(S) = yN(S)$$
$$\Rightarrow y^{-1}xN(S) = N(S)$$
$$\Rightarrow y^{-1}x \in N(S)$$
$$\Rightarrow y^{-1}xS(y^{-1}x)^{-1} = S$$
$$\Rightarrow ySy^{-1} = xSx^{-1}$$

Proving σ is one-one.

σ is onto.

For any $xN(S) \in \frac{G}{N(S)}$, there exists $x \in G$ and $xSx^{-1} \in C(S)$ such that $\sigma(xSx^{-1}) = xN(S)$ showing that σ is onto.

Therefore $|C(S)| = \left|\frac{G}{N(S)}\right| = \big[G : N(S)\big]$.

That is $|C(S)| = \big[G : N(S)\big]$.

3.4.5 Theorem.

Let G be a group and $x \in G$. Then.

(i) $C(x) = \{x\} \Leftrightarrow x \in Z(G)$, Clearly $x \in C(x)$.

(ii) $x \in Z(G) \Leftrightarrow N(x) = G$.

(iii) $x \notin Z(G) \Leftrightarrow N(x)$ is a proper subgroup of G.

Proof.

Given that G is a group and $x \in G$. We have $C(x) = \{axa^{-1}/a \in G\}$.

(i) First suppose $C(x) = \{x\}$.

For any $a \in G$ we have $axa^{-1} = x$. That is $ax = xa$ showing that $x \in Z(G)$.

Conversely suppose that $a \in Z(G)$.

Then $xa = ax$ for all $x \in G$.

That is $a = xax^{-1}$ for all $x \in G$.

$$\begin{aligned} \text{Now } C(x) &= \{axa^{-1}/a \in G\} \\ &= \{xaa^{-1}/a \in G\} \\ &= \{x\} \end{aligned}$$

$$\begin{aligned} \text{(ii)}\quad x \in Z(G) &\Leftrightarrow C(x) = \{x\} \\ &\Leftrightarrow \big[G : N(x)\big] = |C(x)| = 1 \\ &\Leftrightarrow N(x) = G \end{aligned}$$

$$\begin{aligned} \text{(iii)}\quad x \notin Z(G) &\Leftrightarrow C(x) \neq \{x\} \\ &\Leftrightarrow \big[G : N(x)\big] = |C(x)| > 1 \\ &\Leftrightarrow N(x) \text{ is a proper subgroup of } G. \end{aligned}$$

Hence the theorem.

3.4.6 Theorem

Let G be a finite group then

$$|G| = |Z(G)| + \sum_{x \in C} \big[G : N(x)\big]$$

where C contains exactly one element from each conjugate class with more than one element.

Proof.

Given that G is a finite group. We know that the relation conjugacy on G is an equivalence relation and it partitions G into mutually disjoint equivalent classes. The equivalence class of an element $x \in G$ is $C(x)$, the conjugacy class of x .

$$\text{Therefore } G = \bigcup_{x \in C'} C(x). \text{ ————————-(1).}$$

Where C' contains exactly one element from each conjugate class.

Also we have $|C(x)| = \big[G : N(x)\big]$.

On separating those conjugation classes which contains exactly one element and those which contain more than one element and using the fact that $C(x) = \{x\} \Leftrightarrow x \in Z(G)$.

$$\text{We have } G = Z(G) \bigcup \bigcup_{x \in C} C(x) \text{ ——————(2)}$$

Where C contains exactly one element from each conjugate cases having more than one element.

The equation (2) is known as the class equation for group G.

Since G is finite,

$$|G| = |Z(G)| + \sum_{x \in C} |C(x)|.$$
$$= |Z(G)| + \sum_{x \in C} \big[G : N(x)\big]. \text{ ————————(3)}$$

The equation (3) is known as the class equation for finite group G.

3.4.7 Theorem.

Let G be a finite group of order p^n, where p is prime and $n > 0$. Then

(i) G has a non trivial centre $Z(G) = Z$

(ii) $Z \cap N$ is non trivial for any non trivial normal subgroup N of G.

(iii) If H is a proper subgroup of G, then H is properly contained in $N(H)$; hence, if H is a subgroup of order p^{n-1}, then $H \lhd G$.

Proof.

Given that G is a group of order p^n.

The class equation of G is

$$|G| = p^n = |Z| + \sum_{x\in C} \big[G : N(x)\big] \text{———————} (1)$$

Where $Z = Z(G)$ and C is a subset of G exactly one element x from each conjugate class not contained in Z.

If $x \notin Z$ then $N(x)$ is a proper subgroup of G then by Lagrange's theorem,

$|N(x)|/|G| \Rightarrow |N(x)|\big/p^n$

Since $N(x) \neq G$, $|N(x)| < p^n$, therefore $|N(x)| = p^r$, $r < n$.

$\big[G : N(x)\big] = \frac{|G|}{|N(x)|} = \frac{P^n}{p^r} = p^{n-r}$———————-(2)

where $n - r \geq 1$.

$\Rightarrow p$ divides $\big[G : N(x)\big]$ because p divides right hand side of equation (2) for each $x \notin Z$.

$\Rightarrow p$ divides $\sum\limits_{x\in C} \big[G : N(x)\big]$.

We have $p\big/|G|$ and $p\big/ \sum\limits_{x\in C} \big[G : N(x)\big]$.

$\Rightarrow p\big/|Z|$ (from (1))

$\Rightarrow |Z| \geq 2$

$\Rightarrow Z \neq \{e\}$

$\Rightarrow Z = Z(G)$ is non trivial.

(ii) We have from the class equation of G.

$G = Z \bigcup (\bigcup\limits_{x\in C} C(x)).$ (disjoint)

Let N be any non trivial normal subgroup of G.

Then $N = G \bigcap N = \Big(Z \bigcup \big(\bigcup\limits_{x\in C} C(x)\big)\Big) \bigcap N.$

$\Rightarrow N = (Z \cap N) \bigcup \big(\bigcup\limits_{x\in C} C(x) \cup N\big)$

$\Rightarrow |N| = |Z \cup N| + \sum\limits_{x\in C} \big|C(x) \cap N\big|$ ——————— (3)

We now prove that for any $x \in C$, $C(x) \cap N = \phi$ or $C(x)$.

If $x \in N$ then $C(x) \subset N$

Since $x \in N$ then $gx = xg \ \ \forall\, g \in G$.

$$\Rightarrow gxg^{-1} = x \ \ \forall\, g \in G.$$

But $C(x) = \{gxg^{-1}/g \in G\}$

$=\{x\}$.

That is $gxg^{-1} \in C(x)$ then $gxg^{-1} = x \in N$ which imply $C(x) \subset N$.

And further note that $x \notin N$ then $axa^{-1} \notin N \ \ \forall\, a \in G$.

$$\Rightarrow C(x) \cap N = \phi$$

That is if $x \in N \Rightarrow C(x) \subset N$

and if $x \notin N \Rightarrow C(x) \cap N = \phi$

Hence for every $x \in C$

$C(x) \cap N = \phi$ or $C(x)$

$|C(x) \cap N| = 0$ or $|C(x)|$

and $|C(x) \cap N| = 0$ or $\big[G : N(x)\big]$

But $|c(x)| = \big[G : N(x)\big]$

$\Rightarrow \sum_{x \in C} \big|C(x) \cap N\big| = \sum_{x \in C} \big[G : N(x)\big]$

$\Rightarrow p\big/ \sum_{x \in C} \big[G : N(x)\big]$ (by (1))

$\Rightarrow p\big/ \sum_{x \in C} |C(x) \cap N|$

Since N is a proper normal subgroup of G.

$\Rightarrow |N| = p^r$ for some $0 < r < n$

$\Rightarrow p\big/|N|$

Then from (3), we have $p\big/|Z \cap N|$

$\Rightarrow |Z \cap N| \geq 2$

$\Rightarrow Z \cap N \neq \{e\}$

$\Rightarrow Z \cap N$ is nontrivial for any nontrivial normal subgroup N of G.

(iii) Now let H be a proper subgroup of G.

Let K be a maximal normal subgroup of G contained in H.

Then K is a proper normal subgroup of G and hence the quotient group $\frac{G}{K}$ os of order p^r where $0 < r < n$.

Then by (1) of the theorem

$\frac{G}{K}$ has a nontrivial center say $\frac{L}{K}$

Clearly $K \lhd L$ and $K \neq L$

Now $\frac{L}{K} \lhd \frac{G}{K}$ implies $L \lhd G$.

(by correspondence theorem)

If L is contained in H that is $L \subset H$, then $K \subset L \subset H \subset G$ which implies $K \lhd L \lhd G$ which is a contradiction to the fact that K is a maximal normal subgroup of G. contained in H.

Hence L is not contained in H.

We now show that $L \subset N(H)$.

Let $h \in H, l \in L$. We have $\frac{L}{K}$ is the center of $\frac{G}{K}$.

Therefore the elements of $\frac{L}{K}$ and $\frac{G}{K}$ commute.

Hence $(hK)(lK) = (lK)(hK)$

$\Rightarrow hlK = lhK$

$\Rightarrow h^{-1}l^{-1}hlK = K$

$\Rightarrow h^{-1}l^{-1}hl \in K$

But $K \subset H$. Thus $h^{-1}l^{-1}hl \in H$

$\Rightarrow l^{-1}hl \in hH$

$\Rightarrow l^{-1}hl \in H$

$\Rightarrow hl \in lH$

$\Rightarrow Hl \subset lH$

Similarly $lH \subset Hl \ \ \forall \, l \in L$.

Therefore $lH = Hl \ \ \forall\, l \in L$.

$\Rightarrow l^{-1}Hl = H \ \ \forall\, l \in L$.

$\Rightarrow l \in N(H)$.

which gives that $L \subset N(H)$.

If $N(H) = H$ then $L \subset H$, again a contradiction to $L \not\subset H$.

Hence $H \neq N(H)$

$\Rightarrow H$ is properly contained in $N(H)$.

That is $H \subset N(H)$.

$H \subset N(H) \Rightarrow |H| < |N(H)|$ and $|H|$ divides $|N(H)|$ when G is finite.

If H is a proper subgroup of order p^{n-1} that is $|H| = p^{n-1}$ then $|N(H)| = p^n$.

$\Rightarrow N(H) = G$

$\Rightarrow xHx^{-1} = H \ \ \forall\, x \in G$

$\Rightarrow H \lhd G$.

3.4.8 Corollary

Every group of order p^2 is abelian, where p is a prime.

Proof.

Let G be a group of order p^2, where p is prime.

If possible assume that G is non abelian. Also by theorem 4.2.5, G has a nontrivial center $Z(G) = Z$ and $|Z| \neq 1$.

Now $|Z| \big/ |G|$ (by Lagranges theorem)

$\Rightarrow |Z| \big/ p^2$

$\Rightarrow |Z| = p$ or p^2. $(|Z| > 1)$

If $|Z| = p^2$ then $Z = G$ and hence G will be abelian, which is a contradiction.

Therefore $|Z| = p$

Let $a \in G$ and $a \notin Z$.

Now $x \in Z \Rightarrow xa = ax$

$\Rightarrow x \in N(a)$

Thus $Z \subseteq N(a)$.

Also note that $Z \neq N(a)$

If $Z = N(a)$ then $a \in Z$, which is not possible .

$\Rightarrow |N(a)| \big/ p^2$.

$\Rightarrow |N(a)| = p^2$ some $|Z| < |N(a)|$

$\Rightarrow N(a) = G$

$\Rightarrow ag = ga \ \ \forall \ g \in G$

$\Rightarrow a \in Z$, which is a contradiction.

Hence G is abelian.

3.4.9 Remark.

For a fixed $g \in G$, we define $X_g = \{x \in G \big/ gx = x\}$.

3.4.10 Burnside Theorem.

Let G be a finite group acting on a finite set X. Then the number k of orbits in X under G is $k = \frac{1}{|G|} \sum\limits_{g \in G} |X_g|$

Proof.

Let G be a finite group acting on a finite set X.

Let $*$ be the action of G on X that is

$* : G \times X \to X$ is the mapping satisfying

$$a * (b * x) = (ab) * x$$

$$e * x = x \ \ \forall \ a, b \in G, \ x \in X.$$

Let $S = \{(g, x) \in G \times X \big/ g * x = x\}$

$= \{(g, x) \in G \times X \big/ gx = x\}$

For any fixed $g \in G$, we have

$X_g = \{x \in X / g * x = x\}$

$\quad =\{x \in X / gx = x\}$

For any $x \in X$ we have $G_x = \{g \in G / g * x = x\}$

$\qquad\qquad\qquad\qquad\qquad =\{g \in G / gx = x\}$

Therefore for any fixed $x \in X$, the number of ordered pairs (g, x) in S is exactly equal to $|G_x|$

Thus $\sum\limits_{g \in G} |X_g| = |S| = \sum\limits_{x \in X} |G_x|$ ————————- (1)

By theorem 3.3.7, we have

(i) $X = \bigcup\limits_{x \in C} Gx$, where C is a subset of X containing exactly one element from each orbit.

(ii) $|Gx| = \left[G : G_x\right] = \frac{|G|}{|G_x|}$

Therefore $\sum\limits_{x \in X} |G_x| = \sum\limits_{x \in X} \frac{|G|}{|Gx|}$ (By 1)

$= |G| \sum\limits_{x \in X} \frac{1}{|Gx|}$

$= |G| \sum\limits_{a \in C} \sum\limits_{x \in Ga} \frac{1}{|Gx|}$

$=|G|\big(\sum\limits_{a \in C} \frac{1}{|Ga|} + \frac{1}{|Ga|} + \dots \frac{1}{|Ga|}\big)$ ($|Ga|$ times).

$= |G| \sum\limits_{a \in C} \frac{|Ga|}{|Ga|}$

$= |G| \sum\limits_{a \in C} 1$

$= |G| k$

where k is the number of distinct orbits of X under G.

From (1), $\sum\limits_{g \in G} |X_g| = |G| k$

$\Rightarrow k = \frac{1}{|G|} \sum\limits_{g \in G} |X_g|$

Hence the theorem.

3.4.11 Example

Let G be a group containing an element of finite order $n > 1$ and exactly two conjugate classes, prove that $|G| = 2$.

Sol.

Let $a \in G$ such that $a \neq e$ and $o(a) = n$. Consider the conjugate classes $\{e\}$ and $C(a)$ then $G = \{e\} \cup C(a)$.

Let $b \neq e$ be any other element of G. Then $b \in C(a) \Rightarrow b = gag^{-1}$ for some $g \in G$

$\Rightarrow o(b) = o(gag^{-1}) = o(a)$

$\Rightarrow o(b) = n$

Since $o(a) = n$

We shall show that n is a prime. Suppose $m|n$ then $n = mk$ for some integer k. Consider the cyclic group G generated by a then $a^n = e \Rightarrow a^{mk} = e$

$(a^k)^m = e$

Let $b = a^k$ then $b^m = e$

$\Rightarrow o(b) = m$

But $b \in C(a) \Rightarrow o(b) = o(a) = n$

$\Rightarrow m = n$

Showing that n is prime.

We shall prove that $a^2 = e$

Suppose $a^2 \neq e$ then $a^2 \in C(a)$

$\Rightarrow a^2 = xax^{-1}$ for some $x \in G$.

We now claim that $a^{2^i} = x^i a x^{-i}$

For $i = 1$, we have $a^2 = xax^{-1}$

Showing that the result is true for $i = 1$.

Now assume that the result is true for $i = k$

$a^{2^k} = x^k a x^{-k}$.

Consider $a^{2^{k+1}} = a^{2^k}.2 = a^{2^k} a^{2^k}$

$= (x^k a x^{-k})(x^k a x^{-k})$

$= x^k a^2 x^{-k}$

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

$= x^{k+1} a x^{-(k+1)}$

By induction, $a^{2^i} = x^i a x^{-i}$. for $i \geq 1$

On taking $i = n$, we have

$a^{2^n} = x^n a x^{-n}. = eae = a$ since $x^n = e$

$\Rightarrow a^{2^n}.a^{-1} = e$

$\Rightarrow a^{2^n} - 1 = e$

But $o(a) = n$ therefore $n/2^n - 1$

which is not possible since n is a prime.

Therefore $a^2 = e \;\; \forall \; a \in G$

$\Rightarrow G$ is abelian.

$C(a) = \{gag^{-1}/g \in G\} = \{a\}$

Thus $G = \{e\} \cup \{a\} = \{e, a\}$

proving that $|G| = 2$.

3.4.12 Example

Let H be a subgroup of a finite group G. Let $A, B \in P(G)$, the power set of G. Define A to be conjugate to B with respect to H. If $B = hAh^{-1}$ for some $h \in H$. Then

(i) Cojugacy defined in $P(G)$ is an equivalence relation.

(ii) If $C_H(A)$ is the equivalence class of $A \in P(G)$ (called the conjugate class of A with respect to H),

Then

$|C_H(A)| = \left[H : H \cap N(A)\right]$

Proof.

(i) The result is true by theorem 3.3.7 by taking $X = P(G)$ and H to be the group that acts on X by conjugation.

(ii) Let $\sigma : C_H(A) \to \frac{H}{H\cap N(A)}$ defined by $\sigma(hAh^{-1}) = h(H \cap N(A))$

σ is onto : Since for every $h(H \cap N(A))$ there exists $h \in H$ such that $\sigma(hAh^{-1}) = h(H \cap N(A))$

σ is one-one:

$\sigma(h_1Ah_1^{-1}) = \sigma(h_2Ah_2^{-1})$

$\Rightarrow h_1(H \cap N(A)) = h_2(H \cap N(A))$

$\Rightarrow H \cap N(A) = h_1^{-1}h_2(H \cap N(A))$

$\Rightarrow h_1^{-1}h_2 \in N(A)$

$\Rightarrow h_1^{-1}h_2A = Ah_1^{-1}h_2$

$\Rightarrow h_1Ah_1^{-1} = h_2Ah_2^{-1}$

$\Rightarrow \sigma$ is one-one.

Therefore σ is bijective.

$|C_H(A)| = \left|\frac{H}{H\cap N(A)}\right| = \frac{|H|}{|H\cap N(A)|} = [H : H \cap N(A)]$

3.5 Summary:

In section 3.2, we have defined the action of a group G on a set X and provided number of illustrations. Also we proved Cayley's theorem. In section 3.3 we have defined the notions of orbits and stabilizers of an element in a group G. Also we have defined the action of G on itself by conjugacy relation. In section 3.4, we have derived the class equation of a finite group and using this we established that every group of order p^2 (p is a prime) is abelian. At the end of this section we have proved Burnside theorem.

3.6 Model Examination Questions.

(1). Find the number of conjugate classes of the element (1 3) in D_4.

(2). Determine the number of conjugate classes of the symmetric group of degree 3 and verify that the number of elements in each conjugate class is a divisor of the order of group.

(3). In S_n , find the number of r-cycles.

Using this, find the number of conjugates of the r-cycle $(12...r)$ in S_n.

(4). Find all the conjugate classes in S_4.

(5) Let G be a finite group with a normal subgroup N such that $(|N|, \frac{|G|}{|N|}) = 1$. Show that every element order dividing $|N|$ is contained in N.

(6) If G be a group of order 125, then prove that there exists $a \neq e$, $a \in G$ such that $ax = xa$ for all $x \in G$.

(7) Show that every group of order 169 is abelian .

(8) Let G be a group, show that $Z(G) = \bigcup\limits_{|C(x)|=1} C(x)$, $x \in G$.

3.7 Glossary.

Action of a group, G-set, Orbit, Stabilizer, Conjugacy class.Class equation , Burnside theorem

LESSON-04

NORMAL SERIES AND SOLVABLE GROUPS

4.1 Introduction.

In this lesson we define normal and composition series of a group G. Moreover we establish the equivalence of composition series of a finite group(The Jordan-Holder theorem). Further we deduce the fundamental theorem of arithmetic as a consequence of Jordan-Holder theorem.
The class of groups which appears in the theory of polynomial equations is the class of solvable groups. In this lesson we also characterise solvable group. Especially the terminology of solvability comes from the correspondence between the groups and the polynomials which can be solvable by radicals. Here the solvability of polynomials means that there is an algebraic formula for the roots.

4.2 Definition: Normal Series.

Let G be a group. A sequence $(G_0, G_1 \ldots G_r)$ of subgroups of a group G is called a normal series (or subnormal series) of G if

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_{r-1} \subset G_r = G$$

where G_{i-1} is a normal subgroup of G_i, $1 \leq i \leq r$. The quotient groups $\frac{G_i}{G_{i-1}}$, $1 \leq i \leq r$ are called the factors of normal series.

4.2.1 Remark:

(i) For any group G, $\{e\} = G_0 \subset G_1 = G$ is trivially a normal series of G.

(ii) Any series of subgroups of an abelian group is a normal series.

(iii) $\{0\} \subset 20Z \subset 10Z \subset 5Z \subset Z$ is a normal series of Z.

4.2.2 Definition: Composition Series :

A normal series $(G_0, G_1 \ldots G_r)$ of a group G is said to be a composition series of G if its factors $\frac{G_i}{G_{i-1}}$, $1 \leq i \leq r$ are all simple groups.

The factors $\frac{G_i}{G_{i-1}}$, $1 \leq i \leq r$ are called composition factors of G.

4.2.3 Remarks:

(i) $\frac{G_i}{G_{i-1}}$ is simple if and only if there are no normal subgroups between G_{i-1} and G_i, $1 \leq i \leq r$ in the composition series of G.

(ii) For any simple group G, $\{e\} = G_0 \subset G_1 = G$ is the only composition series of G.

4.2.4 Theorem:

Every finite group has a composition series.

Proof.

Let G be a finite group.

We prove the theorem by using induction on the order of G.

If $|G| = 1$ then $G = \{e\}$ and (G) is the only composition series of G without composition factors, proving the result in this case.

If G is a simple group, then its only normal subgroups are $G_0 = \{e\}$ and $G_1 = G$. Now we have

$$\{e\} = G_0 \subset G_1 = G,\ G_0 \lhd G,\ \frac{G}{G_0} \text{ is simple.}$$

Also note that (G_0, G) is the only composition series of G proving the result in this case.

Now suppose that $|G| > 1$ and G is not simple and further assume that the result is true for all groups of order less than $|G|$.

As G is not simple, it has at least one proper normal subgroup.

Let H be the maximal normal subgroup of G. Since $|H| < |G|$, by induction hypothesis, H has a composition series say

$\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_r = H$

Also we have $\frac{G}{H}$ is simple.

Therefore

$\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_r = H \subset G$ is a composition series for G.

Hence the theorem.

4.2.5 Example:

For the group S_3, we have

$$\{e\} \subset \{e, (123), (132)\} \subset S_3$$

is a composition series where

$$S_3 = \{e, (123), (132), (12), (23), (13)\}$$

4.2.6 Example:

We know that the Dihedral group D_4 is generated by σ and τ where $\sigma^4 = e = \tau^2$ and $\tau\sigma = \sigma^3\tau$ here $\sigma = (1234)$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$

That is $D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$.

For this group D_4,

$\{e\} \subset \{e, \sigma^2\} \subset \{e, \sigma, \sigma^2, \sigma^3\} \subset D_4$ is a composition series.

Also $\{e\} \subset <\sigma^2> \subset <\sigma^2, \tau> \subset D_4$ is another composition series for D_4.

4.2.7 Example:

We know that the Quaternion group Q is generated by a, b with the defining relations $a^4 = b^4 = e$, $b^2 = a^2$, $b^{-1}ab = a^3$.

We can write Q in terms of matrices as follows

$$Q = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} -\sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix} \right\}$$

Here $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, b = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$.

Clearly the Quaternion group Q is of order 8 and all of its subgroups are normal. Also nothe that the cyclic groups $[a^2]$ and $[a]$ are subgroups of order 2 and 4 respectively.

Further observe that

$$\{e\} \subset [a^2] \subset [a] \subset Q$$

is a normal series for Q since $\big[\ [a] : [a^2]\ \big] = 2 = [\ Q : [a]\ ]$.

Also each factor of the series is isomorphic to the cyclic group of order 2, which is simple.

Hence $\{e\} \subset [a^2] \subset [a] \subset Q$ is a composition series of Q.

4.2.8 Example:

$\{0\} \subset \{0, 10\} \subset \{0, 5, 10, 15\} \subset \{0, 1, 2, \ldots 19\} = \frac{Z}{(20)}$ is a normal series of $\frac{Z}{<20>}$ since $\frac{Z}{<20>}$ is an abelian group. Further the factors of this composition series are respectively isomorphic to cyclic groups of orders 2, 2 and 5, which are simple. Thus

$S = (G_0, G_1, G_2, G_3)$ is a composition series of $\frac{Z}{<20>}$ where $G_0 = \{0\}$, $G_1 = [10],\ G_2 = [5],\ G_3 = \frac{Z}{<20>}$.

Further note that $S' = (G'_0, G'_1, G'_2, G'_3)$ is also a composition series of $\frac{Z}{<20>}$ where $G'_0 = [0],\ G'_1 = [10],\ G'_2 = [2],\ G'_3 = \frac{Z}{<20>}$. Here the composition factors of the series are respectively isomorphic to the cyclic groups of orders 2, 5 and 2.

4.3 Definition: Equivalence of Normal Series

Two normal series $S = (G_0, G_1, G_2 \ldots G_r)$ and $S' = (G'_0, G'_1, G'_2, \ldots G'_r)$ of G are siad to be equivalent, written $S \sim S'$, if the factors of one series are isomorphic to the factors of the other after some permutation; that is,

$$\frac{G_i^{'}}{G_{i-1}^{'}} \simeq \frac{G_{\sigma(i)}}{G_{\sigma(i)-1}},\ i = 1, 2, \ldots r$$

for some $\sigma \in S_r$.

4.3.1 Example:

The normal (composition) series $S = (G_0, G_1, G_2, G_3)$ and $S^{'} = (G_0^{'}, G_1^{'}, G_2^{'}, G_3^{'})$ of $\frac{Z}{<20>}$ of the example (4.3.8) are equivalent.

$\frac{G_1}{G_0} \simeq \frac{Z}{<2>}$, $\frac{G_2}{G_1} \simeq \frac{Z}{<2>}$, $\frac{G_3}{G_2} \simeq \frac{Z}{<5>}$ and $\frac{G_1^{'}}{G_0^{'}} \simeq \frac{Z}{<2>}$, $\frac{G_2^{'}}{G_1^{'}} \simeq \frac{Z}{<5>}$, $\frac{G_3^{'}}{G_2^{'}} \simeq \frac{Z}{<2>}$.

Now observe that $\frac{G_i^{'}}{G_{i-1}^{'}} \simeq \frac{G_{\sigma(i)}}{G_{\sigma(i)-1}}$,

$$\text{where } \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3.$$

Therefore we have $S \sim S^{'}$.

4.3.2 Lemma

The relation 'equivalence' of normal series on the set of all normal series of a group G is an equivalence relation.

Proof.

Let G be a group and $\mathcal{S}$ be the set of all normal series of G.

Let $S = (G_0, G_1, G_2 \ldots G_r)$ $S^{'} = (G_0^{'}, G_1^{'}, G_2^{'}, \ldots G_r^{'})$, $S^{''} = (G_0^{''}, G_1^{''}, G_2^{''}, \ldots G_r^{''})$ be elements in S.

We have $' \sim '$ the equivalence of normal series on $\mathcal{S}$ defined by $S \backsim S^{'}$ if

$$\frac{G_i^{'}}{G_{i-1}^{'}} \simeq \frac{G_{\sigma(i)}}{G_{\sigma(i)-1}},\ 1 \leq i \leq r \text{ for some } \sigma \in S_r.$$

(i) Let S be any normal series of G then clearly

$$\frac{G_i}{G_{i-1}} \simeq \frac{G_i}{G_{i-1}} = \frac{G_{\sigma(i)}}{G_{\sigma(i)-1}} \text{ where } \sigma(i) = i\ \ \forall\ i,\ 1 \leq i \leq r.$$

Thus $S \sim S\ \ \forall\ S \in \mathcal{S}$ and hence $\sim$ is reflexive.

(ii) Now let $S \sim S^{'}$ that is

$$\frac{G'_i}{G'_{i-1}} \simeq \frac{G_{\sigma(i)}}{G_{\sigma(i)-1}},\ 1 \le i \le r \text{ for some } \sigma \in S_r.$$

From this we write

$$\frac{G_j}{G_{j-1}} \simeq \frac{G'_{\sigma^{-1}(j)}}{G'_{\sigma^{-1}(j)-1}},\ 1 \le j \le r$$

where $\sigma(i) = j \Leftrightarrow \sigma^{-1}(j) = i, \sigma \in S_r$.

Showing that $'\sim'$ is symmetric.

(iii) Now let $S \sim S'$, $S' \sim S"$.

That is $\frac{G'_i}{G'_{i-1}} \simeq \frac{G_{\sigma(i)}}{G_{\sigma(i)-1}}$,

and $\frac{G"_i}{G"_{i-1}} \simeq \frac{G'_{\tau(i)}}{G'_{\tau(i)-1}}$, $1 \le i \le r$ for some $\sigma, \tau \in S_r$.

Now $\frac{G"_i}{G"_{i-1}} \simeq \frac{G'_{\tau(i)}}{G'_{\tau(i)-1}} \simeq \frac{G_{\sigma(\tau(i))}}{G_{\sigma(\tau(i))-1}} = \frac{G_{(\sigma\tau)i}}{G_{(\sigma\tau)i-1}}$

where $\sigma\tau \in S_r$, which proves that $S \sim S"$.

Therefore $'\sim'$ is transitive.

Hence $'\sim'$ is an equivalence relation on $\mathcal{S}$, which completes the proof.

The equivalence of composition series as proved in the example 5.2.1 is not a surprising result. More generally we have the following result, in case of finite groups.

4.3.3 Theorem (Jordan-Holder theorem)

Any two composition series of a finite group are equivalent.

Proof.

Let G be a finite group.

Then G has a composition series. We prove the theorem by using induction on $|G|$. Suppose the theorem is true for all groups of order less than $|G|$.

Now consider any two composition series of G say

$$S_1 : \{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_r = G \text{ ————- } (1)$$

$$S_2 : \{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_s = G \text{ ————- } (2)$$

Now consider two cases $G_{r-1} = H_{r-1}$ or $G_{r-1} \neq H_{r-1}$

Case(i) First let $G_{r-1} = H_{r-1}$ then

$$S_1^{'} : \{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_{r-1}$$

$$S_2^{'} : \{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_{r-1}$$

That is $S_1^{'}, S_2^{'}$ are obtained from S_1, S_2 after removing G from the series S_1 and S_2.

Now $S_1^{'}, S_2^{'}$ are composition series for G_{r-1}.

Since $|G_{r-1}| < |G|$, we have by induction hypothesis $S_1^{'} \sim S_2^{'}$. This implies $r - 1 = s - 1$ from which we get $r = s$ and hence the composition factors of $S_1^{'}$ are isomorphic to the composition factors of $S_2^{'}$ in some order.

In S_1 and S_2, we have $r = s$ and r^{th} composition factor in S_1 and S_2 is $\frac{G}{G_{r-1}}$ since $G_{r-1} = H_{r-1}$.

Clearly the r^{th} composition factors of S_1 and S_2 are isomorphic since every group is isomorphic to itself. Therefore the composition factors of S_1 are isomorphic to the composition factors of S_2 in some order as the first $r - 1$ composition factors of S_1 and S_2 are the composition factors of $S_1^{'}, S_2^{'}$ and r^{th} composition factor of S_1 and S_2 is $\frac{G}{G_{r-1}}$.

Hence $S_1 \sim S_2$ in this case.

Case(ii) Let $G_{r-1} \neq H_{s-1}$, that is G_{r-1} and H_{s-1} are distinct maximal normal subgroups of G.

Let $K = G_{r-1} \cap H_{s-1}$. Therefore K is a maximal normal subgroup of G_{r-1} and also of H_{s-1} (If H, K are different maximal normal subgroups of G, then $H \cap K$ is a maximal normal subgroup of H and also of K)

Since $|K| < |G_{r-1}| < G$, by induction hypothesis, K has a composition series say $\{e\} = K_0 \subset K_1 \subset \ldots \subset K_t = K$.

Now this gives two more composition series of G.

$S_3 : \{e\} = K_0 \subset K_1 \subset \ldots \subset K \subset G_{r-1} \subset G_r = G$ ———— (3)

$S_4 : \{e\} = K_0 \subset K_1 \subset \ldots \subset K \subset H_{s-1} \subset H_s = G$ ———— (4)

Also $G_{r-1}H_{s-1}$ is a normal subgroup of G containing H_{s-1}. Since G_{r-1}, H_{s-1} are normal subgroups of G we must have $G_{r-1}H_{s-1} = G$.

Therefore by second isomorphism theorm

$\frac{H_{s-1}}{G_{r-1} \cap H_{s-1}} \simeq \frac{G_{r-1}H_{s-1}}{G_{r-1}}$.

That is $\frac{H_{s-1}}{K} \simeq \frac{G}{G_{r-1}}$

and $\frac{G_{r-1}}{G_{r-1} \cap H_{s-1}} \simeq \frac{G_{r-1}H_{s-1}}{H_{s-1}}$.

That is $\frac{G_{r-1}}{K} \simeq \frac{G}{H_{s-1}}$.

Also recall that $\frac{K_i}{K_{i-1}} \simeq \frac{K_i}{K_{i-1}}$ since $S \sim S$.

and $\frac{G_{r-1}}{K_t} = \frac{G_{r-1}}{K} \simeq \frac{G}{H_{s-1}} = \frac{G_r}{H_{s-1}}$

and $\frac{G_r}{G_{r-1}} = \frac{G}{G_{r-1}} \simeq \frac{H_{s-1}}{K} = \frac{H_{s-1}}{K_t}$.

This shows that the composition factors of S_3 and S_4 are isomorphic in some order. Therefore $S_3 \sim S_4$.

Also by case (i) $S_1 \sim S_3$ and $S_2 \sim S_4$.

Note that

r=The number of composition factors of S_1.

=The number of composition factors of S_3.

=The number of composition factors of S_4.

=The number of composition factors of S_2.

$=s$.

we have $S_1 \sim S_3$ and $S_3 \sim S_4$.

Also $S_4 \sim S_2$

Thus we have $S_3 \sim S_2$ (since $' \sim '$ is transitive)

Now again $S_1 \sim S_3$, $S_3 \sim S_2$ implies $S_1 \sim S_2$.

Proving that any two composition series of a finite group G are equivalent.

Hence the theorem.

4.3.4 Example:

An abelian group G has a composition series if and only if G is finite.

Proof.

Let G be an abelian group.

If G is finite, then it has a composition series, since every finite group has a composition series. Conversely suppose that G has a composition series say

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_{r-1} \subset G_r = G$$

Since G is abelian, all the composition factors $\frac{G_i}{G_{i-1}}$ $(1 \leq i \leq r)$. are abelian and simple.

we now show that $\frac{G_i}{G_{i-1}}$ is a cyclic group of prime order p_i $(1 \leq i \leq r)$. If $\frac{G_i}{G_{i-1}}$ has a proper subgroup, then it is a proper normal subgroup of $\frac{G_i}{G_{i-1}}$ since $\frac{G_i}{G_{i-1}}$ is abelian.

which contradicts the fact that $\frac{G_i}{G_{i-1}}$ is simple. Thus $\frac{G_i}{G_{i-1}}$ has no proper subgroups.

Also we know that any non trivial simple group is cyclic and is of prime order.

Therefore each quotient group $\frac{G_i}{G_{i-1}}$ $(1 \leq i \leq r)$ is cycle and is of prime order p_i (say) for $1 \leq i \leq r$.

Now $\prod_{i=1}^{r} p_i = \prod_{i=1}^{r} \left|\frac{G_i}{G_{i-1}}\right|$

$$= \frac{|G_1|}{G_0} \frac{|G_2|}{|G_1|} \frac{|G_3|}{|G_2|} \cdots \frac{|G_{r-1}|}{|G_{r-2}|} \frac{|G_r|}{|G_{r-1}|}$$

$$= \frac{|G_r|}{|G_0|} = |G|$$

Thus $|G| = p_1 p_2 \ldots p_r$

proving that G is a finite group.
(Further note that the composition factors of a finite abelian group G are determined by the prime factors of $|G|$).

Hence the theorem.

4.3.5 Example

If a cyclic group has exactly one composition series, then it is a p-group.

Proof.

Let G be a cyclic group of order $p_1p_2\dots p_r$ where $p_1p_2\dots p_r$ are primes not necessarily distinct.
Let $G = [a]$.
But we know that every finite cyclic group G has exactly one subgroup of order d where d is a divisor of order of G, namely $|G|$.
Thus G has a unique subgroup G_i of order $p_1p_2\dots p_i$ namely
$G_i = [a^{p_{i+1}p_{i+2}\dots p_r}]$ for $i = 1, 2, \dots r-1$
More explicitly

$$\begin{aligned}
&G_1 = [a^{p_2p_3\dots p_r}]\\
&G_2 = [a^{p_3p_4\dots p_r}]\\
&\vdots\\
&G_{r-1} = [a^{p_r}]\\
&\text{ and } G_r = G.
\end{aligned}$$

As a convention, we have $G_0 = \{e\}$
Thus we have a composition series

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \dots G_{r-1} \subset G_r = G$$

such that $\left|\frac{G_i}{G_{i-1}}\right| = p_i$ for $i = 1, 2 \dots r$.
Also every permutation of the prime factors of $|G|$ determines a composition

series.

But it is given that G has a unique composition series.

Thus this is possible if and only if $p_1 = p_2 = \ldots = p_r$

Therefore $|G| = p^r$, showing that G is $p-$ group.

4.3.6 Example Let G be a group of order p^n, p is a prime. Then G has a composition series such that all its composition factors are of order p.

Proof.

We have $|G| = p^n$, where p is prime.

Since G is finite, G has a composition series

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_{r-1} \subset G_r = G$$

where $|G_i|$ is a power of p, $1 \leq i \leq r$.

Therefore any composition factor $\frac{G_i}{G_{i-1}}$ is of order p^k for some $k > 0$ and will have a non trivial center since a group of prime power order has a non trivial center.

As $\frac{G_i}{G_{i-1}}$ is simple, its center must be the group $\frac{G_i}{G_{i-1}}$ which implies $\frac{G_i}{G_{i-1}}$ is abelian.

Thus each composition factor of G is simple abelian and hence is a group of order p.

Hence the theorem.

4.3.7 Example

Give an example of two non isomorphic finite groups G which have isomorphic composition series.

Proof.

Consider the groups S_3 and $\frac{Z}{<6>}$

Clearly these two are not isomorphic since S_3 is not cyclic but $\frac{Z}{<6>}$ is cyclic

We know that

$$S_3 = \{e, (123), (132), (12), (13), (23)\}$$

write $N = \{e, (123)(132)\}$

Now

$\{e\} \subset N \subset S_3$ is a composition series of G. Let $H = \{0, 2, 4\}$

Now $\frac{N}{\{e\}} \simeq \frac{Z}{(3)} \simeq \frac{H}{\{0\}}$.

and $\frac{S_3}{N} \simeq \frac{Z}{(2)} \simeq \frac{Z/(6)}{H}$.

Hence the result.

4.3.8 Example

The Jordan-Holder theorem implies the fundamental theorem of arithmetic.

Proof.

The fundamental theorem of arithmetic states that if n is an integer such that $n > 1$ then $n = p_1 p_2 \ldots p_r$ where $p_1, p_2, \ldots p_r$ are primes (not necessarily distinct). Further this factorization is unique in the sense that if $n = q_1 q_2 \ldots q_s$ where $q_1, q_2, \ldots q_s$ are primes then $r = s$ and the p_i's are just the q_i's rearranged (if necessary).

Let G be a cyclic group of order n. Suppose that n has two factorisations into primes say $n = p_1 p_2 \ldots p_r$ and $n = q_1 q_2 \ldots q_s$. Then G has a unique subgroup of order $n = p_1 p_2 \ldots p_i$, $1 \leq i \leq r$.

Thus

$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_{r-1} \subset G_r = G$ is a composition series of G and the factors $\frac{G_i}{G_{i-1}}$ are cyclic groups of order p_i $(1 \leq i \leq r)$.

Similarly G has a composition series

$\{e\} = G_0^{'} \subset G_1^{'} \subset G_2^{'} \subset \ldots \subset G_s^{'} = G$ whose composition factors are cyclic groups of order q_i $(1 \leq i \leq s)$.

But from the Jordan-Holder theorem, we know that any two composition series of finite groups are equivalent.

Therefore, we have $r = s$ and the composition factors $\frac{G_i}{G_{i-1}}$ are isomorphic to the composition factors $\frac{G_i^{'}}{G_{i-1}^{'}}$ in some order.

Thus we have $r = s$ and $p_i = q_i$ (if hence we reorder $q_i's$)

Hence the result.

4.4 Derived group:

Let G be a group. For any $a, b \in G$ $aba^{-1}b^{-1}$ is called a commutator in G. The subgroup of G generated by the set S of all commutators in G is called the commutator subgroup of G or the derived group of G. It is denoted by $G^{'}$.

If $S = \{aba^{-1}b^{-1}/a, b \in G\}$.

Then $G^{-1} = [S]$.

$=$ the set of all possible finite products of elements of S.

$= \{x_1x_2 \ldots x_n/x_i \in S,\ n \geq 1\}$

4.4.1 Remark:

Let G be a group and $G^{'}$ be the derived group of G. Then we have the following.

(i) $G^{'} \lhd G$.

(ii) $G/G^{'}$ is a abelian.

(iii) If $H \lhd G$ then G/H is abelian if and only if $G^{'} \subset H$.

(iv) If G is abelian then $G^{'} = \{e\}$ where e is the identity of G.

4.4.2 Definition: n^{th} Derived group of G

Let n be any positive integer. Then the n^{th} derived group of a group G is denoted by $G^{(n)}$ and is defined as follows.

$G^{(1)} = G',\ G^{(n)} = (G^{(n-1)})',\ n > 1.$

Clearly $G^{(n)} \lhd G^{(n-1)}$ and $\frac{G^{(n-1)}}{G^{(n)}}$ is abelian.

(Inview of the remark 6.2.1).

4.5 definition: Solvable Group.

A group G is said to be solvable if there exists a positive integer k such that $G^{(k)} = \{e\}$.

4.5.1 Theorem:

Every abelian group is solvable

Proof.

Let G be an abelian group.

Let S be the set of all commutators in G that is

$S = \{aba^{-1}b^{-1}/a, b \in G\}.$

$=\{e\}$

since G is abelian.

Now G' = the derived group of G.

$=[S].$

=The smallest subgroup of G generated by S.

$= \{e\}.$

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

Proving that $G^{(1)} = G' = \{e\}$.

Hence the abelian group G is solvable.

4.5.2 Theorem

Let G be a group G. Then every subgroup of G and every homomorphic image of G are solvable. Conversely if N is a normal subgroup of G such that N and $\frac{G}{N}$ are solvable then G is solvable.

Proof.

Let G be a solvable group.

Therefore $G^{(k)} = \{e\}$ for some positive integer k.

(i) Let H be any subgroup of G

Also let $S = \{aba^{-1}b^{-1}/a, b \in H\}$.

and $\overline{S} = \{aba^{-1}b^{-1}/a, b \in G\}$ be the set of commutators in H and G respectively.

Clearly $S \subset \overline{S}$ which implies $S \subset [\overline{S}]$.

Therefore $H^{'} \subset G^{'}$.

That is $H^{(1)} \subset G^{(1)}$.

Which means that if H is a subgroup of G then the derived group $H^{(1)}$ is a subgroup of $G^{(1)}$.

Now assume that $H^{(i)} \subset G^{(i)}$ for some positive integer i.

Therefore $H^{(i)^{'}} \subset G^{(i)^{'}}$ which gives $H^{(i+1)} \subset G^{(i+1)}$.

Hence by the principle of mathematical induction, it follows that $H^{(n)} \subset G^{(n)}$ for any positive integer n.

Now we have $H^{(k)} \subset G^{(k)} = \{e\}$.

Proving that every subgroup of a solvable group is solvable.

(ii) Now let $\phi : G \to K$ be an epimorphism. That is ϕ is onto homomorphism.

$K = \phi(G)$, the homomorphic image of G, is a group.

Let $A = \{aba^{-1}b^{-1}/a, b \in G\}$ and $\overline{A} = \{xyx^{-1}y^{-1}/x, y \in \phi(G)\}$.

Now for any $a, b \in G$ and using the fact that ϕ is a homomorphism, we have

$$\begin{aligned}\phi(aba^{-1}b^{-1}) &= \phi(a)\phi(b)\phi(a^{-1})\phi(b^{-1})\\ &= \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1}\end{aligned}$$

Proving that the image of commutator in G is a commutator in $\phi(G)$.

Now $\phi(A) = \{\phi(aba^{-1}b^{-1})/a, b \in G\}$

$=\{\phi(a)\phi(b)\phi(a^{-1})\phi(b^{-1})/a, b \in G\}$

$=\overline{A}$

Since ϕ is surjective.

Further

$\phi(G^{'}) = \phi([A])$.

$=\{\phi(x_1x_2 \ldots x_n)/\ x_i \in A,\ n \geq 1\}$.

$=\{\phi(x_1)\phi(x_2), \ldots \phi(x_n)/\ x_i \in A,\ n \geq 1\}$.

$=\{y_1y_2 \ldots y_n/\ y_i \in \overline{A},\ n \geq 1\}$.

$=[\overline{A}] = (\phi(G))^{'}$.

Proving that $\phi\big(G^{(1)}\big) = \big(\phi(G)\big)^{(1)}$.

Now assume that $\phi\big(G^{(m)}\big) = \big(\phi(G)\big)^{(m)}$ for some natural number m.

Now $\phi\big(G^{(m+1)}\big) = \phi\Big(\big(G^{(m)}\big)^{'}\Big)$

$=\Big(\phi\big(G^{(m)}\big)\Big)^{'}$

$=\big(\phi(G)^{(m)}\big)^{'}$

$=\big(\phi(G)\big)^{m+1}$.

Therefore by the principle of mathematical induction, we have

$\phi\big(G^{(n)}\big) = \big(\phi(G)\big)^{(n)}$ for any $n \geq 1$.

As G is solvable,

$(\phi(G))^{k} = \phi(G^{(k)}) = \phi(\{e\}) = \{e^{'}\}$

where $e^{'}$ is the identity of $\phi(G)$.

Proving that $\phi(G)$ is solvable which establishes that the homomorphic image of a solvable group is solvable.

Conversely let $N \lhd G$ such that N and $\frac{G}{N}$ are solvable.

Then there exists positive integers k, l such that $N^{(k)} = \{e\}$ and $\left(\frac{G}{N}\right)^{(l)} = \{\bar{e}\}$ where $\bar{e}$ is the identity of $\frac{G}{N}$ namely N.

Let $\phi : G \to \frac{G}{N}$ be the canonical homomorphism.

That is $\phi(x) = Nx$.

Clearly ϕ is surjective.

That is $\frac{G}{N}$ is the homomorphic image of G under ϕ $\left(\text{i.e } \phi(G) = \frac{G}{N}\right)$.

Now for any natural number n,

$$\phi\big(G^{(n)}\big) = \big(\phi(G)\big)^{(n)}.$$

Hence $\phi\big(G^{(l)}\big) = \big(\phi(G)\big)^{(l)}$

$$=\left(\frac{G}{N}\right)^{(l)} = \{\text{N}\}.$$

which implies $G^{(l)} \subset ker\phi$ that is $G^{(l)} \subset N$.

From which we have $\phi\big(G^{(l)}\big)^{(k)} \subset N^{(k)}$

Therefore $\big(G^{(l+k)}\big) \subset \{e\}$

Thus we have $G^{(l+k)} = \{e\}$ proving that G is solvable.

In the following theorem, we characterise the solvable groups.

4.5.3 Theorem

A group G is solvable if and only if G has a normal series with abelian factors. Further a finite group is solvable if and only if its composition factors are cyclic groups of prime orders.

Proof

Let G be a group. We know that the derived group $G^{'}$ of G is a normal subgroup of G and is abelian.

Also for any natural number n, we define n^{th} derived group $G^{(n)}$ of a group G as follows

$G^{(1)} = G^{'}$, $G^{(n)} = \big(G^{(n-1)}\big)^{'}$ for $n > 1$.

Also as a convention we get $G^{(0)} = G$.

Now $G^{(n)} \lhd G^{(n-1)}$ and $\frac{G^{(n-1)}}{G^{(n)}}$ is abelian.

(i) First suppose that G is solvable.

Then $G^{(k)} = \{e\}$ for some natural number k.

Now

$\{e\} = G^{(k)} \lhd G^{(k-1)} \lhd G^{(k-1)} \lhd \ldots \lhd G^{(1)} \lhd G^{(0)} = G$ is a normal series of G and the factors $\frac{G^{(i-1)}}{G^{(i)}}$ are abelian for $i = 1, 2 \ldots k$

Thus G has a normal series with abelian factors.

Conversely suppose that G has a normal series

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_{r-1} \subset H_r = G$$

such that $\frac{H^{(i)}}{H^{(i-1)}}$ is abelian for $1 \leq i \leq r$.

For any $a, b \in H_i$

$$\begin{aligned}(aba^{-1}b^{-1})H_{i-1} &= (aH_{i-1})(bH_{i-1})(a^{-1}H_{i-1})(b^{-1}H_{i-1}). \\ &= (aH_{i-1})(bH_{i-1})(aH_{i-1})^{-1}(bH_{i-1})^{-1}. \\ &= H_{i-1}.\end{aligned}$$

Since $\frac{H_i}{H_{i-1}}$ is abelian.

Therefore we have $aba^{-1}b^{-1} \in H_{i-1}$ from which we get $H_i^{'} \subset H_{i-1}$ for $1 \leq i \leq r$.

Now $G^{'} = H_r^{'} \subset H_{r-1}$.

Thus by induction we have $G^{(i)} \subset H_{r-i}$ for $1 \leq i \leq r$.

For $i = r$, we get $G^{(r)} \subset H_0 = \{e\}$

Hence $G^{(r)} = \{e\}$ proving that G is solvable.

(ii) Now assume that G is a finite group.

Suppose that G is a solvable group. By part (i) G has a normal series.

$\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_{r-1} \subset H_r = G$ where each factor $\frac{H_i}{H_{i-1}}$,

$1 \leq i \leq r$ is abelian.

Clearly each $\frac{H_i}{H_{i-1}}$ is finite and H_{i-1} is the identity of $\frac{H_i}{H_{i-1}}$ and since each finite group has a composition series.

In particular $\frac{H_i}{H_{i-1}}$ has a composition series.

$$H_{i-1} = \frac{K_0}{H_{i-1}} \subset \frac{K_1}{H_{i-1}} \subset \frac{K_2}{H_{i-1}} \subset \ldots \subset \frac{K_n}{H_{i-1}} = \frac{H_i}{H_{i-1}}.$$

and the composition factors $\dfrac{K_j / H_{i-1}}{K_{j-1} / H_{i-1}}$ are simple.

Further these factors are abelian since $\frac{H_i}{H_{i-1}}$ is abelian. Also we know that every simple abelian group is of prime order and hence cyclic.

Therefore $\dfrac{K_j / H_{i-1}}{K_{j-1} / H_{i-1}}$ is of prime order and thus cyclic, from which it follows that $\frac{K_j}{K_{j-1}}$, $1 \leq j \leq n$ is of prime order and cyclic.

Further $\frac{K_{j-1}}{H_{i-1}} \lhd \frac{K_j}{H_{i-1}}$ imply $K_{j-1} \lhd K_j$ for $1 \leq j \leq n$.

Thus corresponding to the composition series of $\frac{H_i}{H_{i-1}}$, we get

$$H_{i-1} = K_0 \lhd K_1 \lhd K_2 \lhd \ldots \lhd K_n = H_i$$

where $K_{j-1} \lhd K_j$ and $\frac{K_j}{K_{j-1}}$ is of prime order and cyclic.

Now, on inserting the corresponding subgroups of H_i between H_{i-1} and H_i $(1 \leq i \leq r)$ in the normal series of G, we get a composition series of G in which each composition factor is a cyclic group of prime order.

Conversely suppose G has a composition series

$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_r = G$

such that each of its composition factors $\frac{G_i}{G_{i-1}}$, $1 \leq i \leq r$ is cyclic of prime order. As each composition series is a normal series and every cyclic group is abelian, we have a normal series for the group G and each factor of this series is abelian.

Therefore G is solvable by the first part. Hence the theorem.

4.5.4 Example:

The symmetric group S_3 is solvable.

Proof.

We know the symmetric group

$S_3 = \{e, a, a^2, b, ab, a^2b\}$

with the defining relation $a^3 = e = b^2$, $ba = a^2b$

Clearly $N = [a] = \{e, a, a^2\}$ is a cyclic subgroup of S_3 of order 3.

Now we have $\{e\} \subset N \subset S_3$

Clearly $\{e\} \lhd N$ and since index of N in S_3 in 2 we have $N \lhd S_3$.

Further $\frac{N}{\{e\}}$, $\frac{S_3}{N}$ are isomorphic to $\frac{Z}{<3>}$ and $\frac{Z}{<2>}$ respectively.

Thus S_3 has a normal series with abelian factors and hence S_3 is solvable (in view of theorem 6.3.3)

4.5.5 Example:

The dihedral group D_n is solvable.

Proof.

We know that the dihedral group D_n is of order $2n$ generated by two elements σ, τ satisfying $\sigma^n = e = \tau^2$ and $\tau\sigma = \sigma^{n-1}\tau$ where $\sigma = (12\ldots n)$ and

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & n & \ldots & 2 \end{pmatrix}$$

Now

$\{e\} \subset K =< \sigma >= \{e, \sigma, \sigma^2, \ldots \sigma^{n-1}\} \subset D_n$

is a normal series for D_n and $[D_n : K] = 2$, hence $K \lhd D_n$.

Further note that the factors in the above series $\frac{K}{\{e\}}$, $\frac{D_n}{K}$ are cyclic groups of orders n and 2 respectively.

Therefore D_n has normal series with abelian factors, proving that D_n is solvable.

4.5.6 Example:

A group of prime power order is solvable.

Sol.

Let G be a group of order p^n where p is a prime then G has composition series such that all its composition factors are of order p. Since a group of prime order is cyclic, G has a composition series such that all its composition factors are cyclic groups of prime order.

Thus G is solvable.

4.5.7 Example:

If M is a minimal normal subgroup of a finite solvable group G then M is a cyclic group of order p.

Sol.

Given that G is a finite solvable group. Therefore G has a composition series

$$\{e\} = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_n = G$$

whose composition factors are cyclic groups of prime orders. Since M is the minimal normal subgroup of G we must have $G_1 = M$ in the composition series of G. Then the composition factor $\frac{M}{\{e\}} = M$ is a cyclic group of order p.

Hence the result.

4.5.8 Example:

A simple solvable group is cyclic.

Proof.

Let G be a simple solvable group then $\{e\} \subset G$ is the only normal series and its only factor $\frac{G}{\{e\}} = G$ is abelian thus G is a simple abelian group and this implies G is of prime order.

Hence G is cyclic.

4.5.9 Example:

Let A, B are groups then $A \times B$ is solvable if and only if both A, B are solvable.

Proof.

Given that A, B are groups. Then $A \times B$ is a group under coordinate wise binary operation namely

$$(a, b).(c, d) = (ac, bd) \text{ for all } (a, b), (c, d) \in A \times B.$$

If e_1, e_2 are the identities of A, B then (e_1, e_2) is the identity of $A \times B$ and the inverse of (a, b) is denoted by $(a, b)^{-1}$ and is given by $(a, b)^{-1} = (a^{-1}, b^{-1})$.

This $A \times B$ is called as the direct product of groups A and B.

First we prove the following results.

(i) $\{e_1\} \times B \lhd A \times B$

$A \times \{e_2\} \lhd A \times B$

(ii) $\{e_1\} \times B \simeq B$

$A \times \{e_2\} \simeq A$

$\frac{A \times B}{\{e_1\} \times B} \simeq A$ and $\frac{A \times B}{A \times \{e_2\}} \simeq B$.

Proof of (i) Now define a map

$$\phi : A \times B \to B \text{ be } \phi((a, b)) = a \text{ for all } (a, b) \in A \times B.$$

Then clearly ϕ is a surjective homomorphism with $ker\phi = \{e_1\} \times B$.

Therefore by the first homomorphism theorem we have

$\frac{A \times B}{\{e_1\} \times B} \simeq B$

Similarly $\frac{A \times B}{A \times \{e_2\}} \simeq A$.

From the above it is clear that $\{e_1\} \times B \lhd A \times B$ and $A \times \{e_2\} \lhd A \times B$.

Proof of (ii) Define the map

$$\psi : \{e_1\} \times B \to B \text{ by } \psi((e_1, b)) = b \text{ for all } (e_1, b) \in \{e_1\} \times B.$$

Observe that ψ is an isomorphism.

Hence $\{e_1\} \times B \simeq B$.

Similarly $A \times \{e_1\} \simeq A$.

Proof of the example:

First suppose that $A \times B$ is solvable. Note that A and B are homomorphic images of $A \times B$ under the homomorphisms $(a, b) \mapsto a$ and $(a, b) \mapsto b$. Now it follows that A, B are solvable, since every homomorphic image of a solvable group is solvable.

Conversely suppose that A, B are solvable. Now we have to show $A \times B$ is solvable.

As $\{e_1\} \times B \lhd A \times B$, $\{e_1\} \times B \simeq B$ and $\frac{A \times B}{\{e_1\} \times B} \simeq A$.

Since A, B are solvable, it follows that $\{e_1\} \times B$, $\frac{A \times B}{\{e_1\} \times B}$ are solvable.

Therefore $A \times B$ is solvable (in view of theorem 4.5.3).

4.6 Summary

In this lesson, we have introduced the notion of normal series and composition series. Also we have established that any two composition series of a finite group are equivalent. Further we have deduced the fundamental theorem of arithmetic as a consequence of Jordan-Holder theorem.

In section 4.4, we have defined the derived group. In section 4.5, we have introduced the notion of solvable group and characterized solvable groups. Also at the end of the section, we have established that the direct product (external direct product) of two solvable groups is solvable.

4.10 Model Examination Questions

(1) Write down a composition series for the Klein four group.

(2) Find all composition series for $\frac{Z}{<30>}$. Show that they are equivalent.

(3) If G is a cyclic group such that $|G| = p_1 p_2 \ldots p_r$ where $p_i' s$ are distinct primes, then show that the number of distinct composition series of G is $r!$

(4) Let G be a finite group and $N \lhd G$. Show that G has a composition series in which N appears as a term.

(5) Find the composition factors of the additive group of integers modulo 8.

4.11 Glossary

Normal series, Composition series, Equivalence of composition series, Jordan-Holder theorem,Derived group, Solvable group, Direct product.

LESSON-05

NILPOTENT GROUPS

5.1 Introduction.

In this lesson we define nilpotent group and establish that every group of prime power order is nilpotent.

5.2 Definition: Center of a group

Let G be a group. We know that the center of group is denoted by $Z(G)$ and is defined as $Z(G) = \{x \in G/xg = gx \quad \forall g \in G\}$.
Clearly $Z(G)$ is an abelian subgroup of G and further $Z(G)$ is also normal in G.
Recall that $Z(G) = G$ if and only if G is abelian.

5.3 The n^{th} center of a group.

We define n^{th} center of a group G inductively as follows
For $n = 1$, let $Z_1(G) = Z(G)$ clearly $Z_1(G) \lhd G$.
Now consider the quotient group $\frac{G}{Z_1(G)}$.
The center $Z\left(\frac{G}{Z_1(G)}\right)$ of $\frac{G}{Z_1(G)}$ is again a normal subgroup of $\frac{G}{Z_1(G)}$.
That is $Z\left(\frac{G}{Z_1(G)}\right) \lhd \frac{G}{Z_1(G)}$.
Now there is a unique normal subgroup $Z_2(G)$ of G such that

$$Z\left(\frac{G}{Z_1(G)}\right) = \frac{Z_2(G)}{Z_1(G)}.$$

Hence $\frac{Z_2(G)}{Z_1(G)} \lhd \frac{G}{Z_1(G)}$.
Continuing in the above manner, we have a unique normal subgroup $Z_n(G)$ of G such that

$\frac{Z_n(G)}{Z_{n-1}(G)} = Z\left(\frac{G}{Z_{n-1}(G)}\right)$ for every natural number $n > 1$ and $Z_n(G)$ is called as the n^{th} center of G.

Thus we have $\frac{Z_n(G)}{Z_{n-1}(G)} = Z\left(\frac{G}{Z_{n-1}(G)}\right)$ for any natural number $n > 1$.

For $n = 0$, we set $Z_0(G) = \{e\}$.

5.3.1 Remark:

Observe that $(Z_n(G))' \subset Z_{n-1}(G)$.

From the definition of $Z_n(G)$,

$Z_n(G) = \{x \in G/Z_{n-1}(G)xZ_{n-1}(G)y = Z_{n-1}(G)yZ_{n-1}(G)x \ \ \forall y \in G\}$.

$\quad$ $=\{x \in G/Z_{n-1}(G)xyx^{-1}y^{-1} = Z_{n-1}(G) \ \ \forall y \in G\}$.

$\quad$ $=\{x \in G/xyx^{-1}y^{-1} \in Z_{n-1}(G) \ \ \forall y \in G$.

We have $(Z_n(G))' =$ the derived group of $Z_n(G)$.

$\quad$ $= [S]$.

where $S = \{xyx^{-1}y^{-1}/x, y \in Z_n(G)\}$.

From the above $S \subset Z_{n-1}(G)$.

Therefore showing that $(Z_n(G))' \subset Z_{n-1}(G)$.

5.3.2 Definition: The upper central series of G

The ascending series

$$\{e\} = Z_0(G) \subset Z_1(G) \subset Z_2(G) \subset \ldots \subset Z_{n-1}(G) \ldots \subset Z_n(G) \subset \ldots$$

of subgroups of a group G is called the upper central series of G.

5.4 Definition: Nilpotent Group

A group G is said to be nilpotent if $Z_m(G) = G$ for some natural number m.

The smallest m such that $Z_m(G) = G$ is called the class of nilpotency of G.

5.4.1 Example :

(1) Every abelian group G is a nilpotent group of class 1 since

$Z_1(G) = Z(G) = G$

5.4.2 Theorem:

A group of order p^n (p is a prime) is nilpotent.

Proof.

Let G be a group and $|G| = p^n$ where p is a prime and n is a natural number. We know that G has a nontrivial center $Z_1(G)$. Therefore $|Z_1(G)| > 1$. Now the quotient group $\frac{G}{Z_1(G)}$ is of order p^r, where r is a natural number with $r < n$ and r has a nontrivial center $\frac{Z_2(G)}{Z_1(G)}$.

Further $\left|\frac{Z_2(G)}{Z_1(G)}\right| > 1$.

which implies $\frac{|Z_2(G)|}{|Z_1(G)|} > 1$.

From which it follows that $|Z_1(G)| < |Z_2(G)|$.

Continuing in the above manner, after a finite number of steps, we get $|Z_m(G)| = p^n$ for some $m \leq n$.

Hence we have $Z_m(G) = G$

Showing that G is nilpotent.

5.4.3 Theorem

A group G is nilpotent if and only if G has a normal series.

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_m = G$$

such that $\frac{G_i}{G_{i-1}} \subset Z\left(\frac{G}{G_{i-1}}\right)$ for all $i = 1, 2, \ldots m$.

Proof.

Let G be a group. For any natural number n, the n^{th} center of G is denoted by $Z_n(G)$ is a normal subgroup of G such that $\frac{Z_n(G)}{Z_{n-1}(G)} = Z\left(\frac{G}{Z_{n-1}(G)}\right)$ where $Z_0(G) = \{e\}$. Also we have $Z_{n-1}(G) \lhd Z_n(G)$ and G has a upper central series

$$\{e\} = Z_0(G) \subset Z_1(G) \subset Z_2(G) \subset \ldots \subset Z_{n-1}(G) \ldots \subset Z_n(G) \subset \ldots$$

First suppose that G is a nilpotent group of class m where m is a natural number then

$$\{e\} = Z_0(G) \subset Z_1(G) \subset Z_e(G) \subset \ldots \subset Z_{m-1}(G) \ldots \subset Z_m(G) = G$$

is the required normal series with the stated condition.

Conversely suppose that G has a normal series

$$\{e\} = G_0 \subset G_1 \subset G_2 \ldots \subset G_m = G$$

such that $\frac{G_i}{G_{i-1}} \subset Z\left(\frac{G}{G_{i-1}}\right)$, $1 \leq i \leq m$

We now claim that $G_i \subset Z_i(G)$.

We prove this by induction on i.

For $i = 1$, we have $\frac{G_1}{G_0} = \frac{G_1}{\{e\}} \subset Z\left(\frac{G}{\{e\}}\right)$

i.e. $G_1 \subset Z_1(G)$

We assume that $G_{i-1} \subset Z_{i-1}(G)$.

From the condition $\frac{G_i}{G_{i-1}} \subset Z\left(\frac{G}{G_{i-1}}\right)$

For every $x \in G_i$, $y \in G$,

We have $G_{i-1}xG_{i-1}y = G_{i-1}yG_{i-1}x$

which imply $xyx^{-1}y^{-1} \in Z_{i-1}(G)$.

Thus we have $x \in Z_i(G)$. (By remark 7.4.1)

Proving that $G_i \subset Z_i(G)$.

Now for $i = m$, we have

$$G = G_m \subset Z_m(G)$$

giving that $Z_m(G) = G$.

which shows that G is nilpotent, completing the proof of the theorem.

5.4.4 Corollary.

Every nilpotent group is solvable.

Proof.

Let G be a nilpotent group of class m so that $Z_m(G) = G$.

By the above theorem 7.6.3, G has a normal series.

$$\{e\} = Z_0(G) \subset Z_1(G) \subset Z_2(G) \subset \ldots \subset Z_m(G) = G.$$

where $\frac{Z_i(G)}{Z_{i-1}(G)} = Z\left(\frac{G}{Z_{i-1}(G)}\right)$, $1 \leq i \leq m$.

Since the center is always abelian, all the factors of the above normal series are abelian. Thus G has a normal series with abelian factors.

Hence G is abelian.

5.4.5 Remark.

The converse of the above result is not true. That is every solvable group is not nilpotent.

As an example we have the following

Consider S_3, the symmetric group on 3 symbols.

We know that $Z(S_3) = \{e\}$ that is $Z_1(S_3) = \{e\}$

Also $\frac{Z_2(S_3)}{Z_1(S_3)} = Z\left(\frac{S_3}{Z_1(S_3)}\right) = Z\left(\frac{S_3}{\{e\}}\right) = Z(S_3) = \{e\}$.

which imply $Z_2(S_3) = \{e\} \neq S_3$.

Continuing in the same manner $Z_m(S_3) \neq S_3$ for no positive integer m.

Therefore S_3 is not nilpotent.

5.4.6 Remark.

We observe the following

cyclic groups $\subset$ abelian groups $\subset$ nilpotent groups $\subset$ solvable groups $\subset$ all groups.

Note that all the above containments are proper.

5.4.7 Theorem

Let G be a nilpotent group. Then

(i) Every subgroup of G is nilpotent.

(ii) Every homomorphic image of G is also nilpotent.

Proof.

Let G be a nilpotent group of class m, that is m is the least positive integer such that $Z_m(G) = G$.

(i) Let H be a subgroup of G.

We now show that $Z_m(H) = H$.

Recall that $Z_n(G) = \Big\{x \in G/xyx^{-1}y^{-1} \in Z_{n-1}(G) \ \ \forall y \in G\Big\}$.

For every $x \in H \cap Z_1G$ we have $xg = gx$ for all $g \in G$. From which we get $xh = hx$ for all $h \in H$ which imply $x \in Z_1(H)$.

Proving that $H \cap Z_1(G) \subset Z_1(H)$. ———————— (1)

Again for any $x \in H \cap Z_2(G)$ and for all $y \in H$ we have $x \in H$ and $y \in H$ and $x \in Z_2(G)$.

Now $xyx^{-1}y^{-1} \in H$ and $xyx^{-1}y^{-1} \in Z_1(G)$.

Thus $xyx^{-1}y^{-1} \in H \cap Z_1(G)$.

Hence $xyx^{-1}y^{-1} \in Z_1(H)$ for all $y \in H$.

Therefore $x \in Z_2(H)$.

Proving that $H \cap Z_2(G) \subset Z_2(H)$.———————— (2)

Continuing in the same manner, we get

$$H \cap Z_i(G) \subset Z_i(H),\ 1 \leq i \leq m.$$

Now $H = H \cap G = H \cap Z_m(G) \subset Z_m(H)$.

Hence proving that $Z_m(H) = H$ since $Z_m(H) \subset H$.

which shows that H is nilpotent.

(ii) Now let $\phi : G \to K$ be a surjective homomorphism. That is let $K = \phi(G)$ be the homomorphic image of G under ϕ.

Let $x \in Z_1(G)$. Then $xyx^{-1}y^{-1} = e$ forall $y \in G$.

As $\phi(x) \in \phi(Z_1(G))$ we have $\phi(xyx^{-1}y^{-1}) = \phi(e)$ for all $\phi(y) \in K$.

That is $\phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = e^{'}$, $\phi(y) \in K$

which proves $\phi(x) \in Z_1(K)$ since ϕ is surjective.

Thus showing that $\phi(Z_1(G)) \subset Z_1(K)$.

Also for any $x \in Z_2(G)$, we have $xyx^{-1}y^{-1} \in Z_1(G)$ for all $y \in G$.

Thus $\phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} \in \phi(Z_1(G))$ for all $\phi(y) \in K$.

which implies $\phi(x) \in Z_2(K)$ since $\phi(Z_1(G)) \subset Z_1(K)$ proving that $\phi(Z_2(G)) \subset Z_2(K)$.

Repeating the same argument, we obtain

$$\phi(Z_i(G)) \subset Z_i(K), \quad 1 \leq i \leq m.$$

Now $K = \phi(G) = \phi(Z_m(G)) \subset Z_m(K)$.

Hence $Z_m(K) = K$ since $Z_m(K) \subset K$.

Proving that $K = \phi(G)$ is nilpotent.

Thus every homomorphic image of a nilpotent group is nilpotent.

Hence the theorem.

5.4.8 Theorem:

Let H and K are nilpotent groups then $H \times K$ is nilpotent.

Proof.

Let H and K be nilpotent groups of class m and n respectively, that is m and n are the least positive integers such that $Z_m(H) = H$ and $Z_n(K) = K$. Without loss of generality, we may assume that $m \leq n$. Therefore we have $Z_n(H) = H$ and $Z_n(K) = K$.

Now,

$$\begin{aligned}
Z(H\times K) &= \Big\{(h,k)\in H\times K\big/(h,k)(x,y)=(x,y)(h,k)\ \forall\ (x,y)\in H\times K.\Big\}.\\
&= \Big\{(h,k)\in H\times K\big/hx=xh \ \text{ and }\ ky=yk\ \ \forall\ x\in H, y\in K\Big\}.\\
&= \Big\{(h,k)\in H\times K\big/h\in Z(G), k\in Z(K).\Big\}.\\
&= Z(H)\times Z(K).
\end{aligned}$$

Proving that $Z_1(H\times K)=Z_1(H)\times Z_1(K)$.

Also

$$\begin{aligned}
Z_2(H\times K) &= \Big\{(h,k)\in H\times K\big/(h,k)(x,y)(h,k)^{-1}(x,y)^{-1}\in Z_1(H\times K)\ \forall (x,y)\in H\times K\Big\}.\\
&= \Big\{(h,k)\in H\times K\big/(hxh^{-1}x^{-1},kyk^{-1}y^{-1})\in Z_1(H)\times Z_1(K)\ \forall x\in H, y\in K\Big\}.\\
&= \Big\{(h,k)\in H\times K\big/hxh^{-1}x^{-1}\in Z_1(H)\ \forall x\in H, kyk^{-1}y^{-1}\in Z_1(K)\ \forall y\in K\Big\}.\\
&= \Big\{(h,k)\in H\times K\big/h\in Z_2(H), k\in Z_2(K)\Big\}.\\
&= Z_2(H)\times Z_2(K).
\end{aligned}$$

Continuing in the same manner, we get

$Z_i(H\times K)=Z_i(H)\times Z_i(K), \quad 1\le i\le n.$

Hence $Z_n(H\times K)=Z_n(H)\times Z_n(K)=H\times K$.

Proving that $H\times K$ is nilpotent.

5.4.9 Corollary.

Let $H_1, H_2, \ldots H_n$ be any n nilpotent groups. Then $H_1\times H_2\times\ldots\times H_n$ is also nilpotent.

Proof.

Given that $H_1, H_2, \ldots H_n$ are nilpotent groups.

We now prove that $H_1 \times H_2 \times \ldots \times H_n$ is nilpotent by induction on n.

For $n = 2$, the result follows from the theorem 7.4.8

Now suppose that the theorem is true when the number of groups is less than n.

Therefore, $H = H_1 \times H_2 \times \ldots \times H_{n-1}$ is nilpotent.

Now $H \times H_n$ is nilpotent by the theorem 7.4.8 which proves that

$H \times H_n = H_1 \times H_2 \times \ldots \times H_{n-1} \times H_n$ is nilpotent.

Hence the theorem.

5.4.10 Example.

Give an example of a group G such that G has a normal subgroup N with both N and $\frac{G}{N}$ are nilpotent but G is not nilpotent.

Sol.

We have S_3, the symmetric group on three symbols

That is $S_3 = \{e, a, a^2, b, ab, a^2b\}$ with the defining relations $a^3 = e = b^2$, $ba = a^2b$.

Let $N = [a] = \{e, a, a^2\}$

Clearly $N \lhd S_3$ and $\frac{S_3}{N} \simeq \frac{Z}{<2>}$

Further observe that $N, \frac{S_3}{N}$ are nilpotent but S_3 is not nilpotent.

5.5 Summary

In section 5.3 we have defined n^{th} center of a group G. In section 5.4 the notion of nilpotent group introduced. At the end of section, we have proved the direct product of finite number of nilpotent groups is nilpotent.

5.6 Model Examination Questions

(1) Find the upper central series of A_4 and S_4.

(2) Show that D_4 is nilpotent of class 2.

(3) Show that S_n is not nilpotent for $n \geq 3$.

(4) Show that if $\frac{G}{Z(G)}$ is nilpotent then G is nilpotent.

5.7 Glossary

Upper cental series of a group, Nilpotent group, Class of nilpotency.

UNIT-II

LESSON-06

DIRECT PRODUCTS

6.1 Introduction

In this lesson the internal direct product (sum) of a finite number of subgroups of a group is introduced through a set of necessary and sufficient conditions. If a group G is isomorphic to the direct product of finite number of subgroups whose structures are known the structure of G can be generally determined.

6.2 Direct Product of Groups

6.2.1 Definition : Let $G_1, G_2, \ldots, G_n$ be groups then the cartesian product $G_1 \times G_2 \times \ldots \times G_n$ is a group under the point wise binary operation $(g_1, g_2, \ldots, g_n)(g_1^{'}, g_2^{'}, \ldots, g_n^{'}) = (g_1g_1^{'}, g_2g_2^{'}, \ldots, g_ng_n^{'})$ where $g_i, g_i^{'} \in G_i$, $1 \leq i \leq n$. If e_i is the identity of G_i then $(e_1, e_2, \ldots, e_n)$ is the identity of $G_1 \times G_2 \times \ldots \times G_n$ and $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$ is the inverse of $(g_1, g_2, \ldots, g_n)$. This group is called the external direct product of groups $G_1, G_2, \ldots, G_n$.

6.2.2 Theorem : Let $H_1, H_2, \ldots, H_n$ be a family of subgroups of a group G and let $H = H_1H_2 \ldots H_n$. Then the following are equivalent.

(i) $H_1 \times H_2 \times \ldots \times H_n \backsimeq H$ under the cononical mapping that sends $(x_1, x_2, \ldots, x_n)$ to $x_1x_2 \ldots x_n$.

(ii) $H_i \rhd H$ and every element $x \in H$ can be uniquely expressed as $x = x_1x_2 \ldots x_n$ where $x_i \in H_i$, $1 \leq i \leq n$.

(iii) $H_i \rhd H$ and if $x_1x_2 \ldots x_n = e$ then $x_i = e$ for each i.

(iv) $H_i \rhd H$ and $H_i \cap (H_1H_2 \ldots H_{i-1}H_{i+1} \ldots H_n) = (e)$, $1 \leq i \leq n$.

Proof. $(i) \Rightarrow (ii)$. Assume that (i) is true.

We have $H_1 \times H_2 \times \ldots \times H_n \backsimeq H$ under the canonical map σ defined by $\sigma(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n$ where $x_i \in H_i$, $1 \leq i \leq n$.

Let $H_i^{'} = \{(e, \ldots, h_i, \ldots, e) | h_i \in H_i\}$ then for each $x = (x_1, x_2, \ldots, x_n) \in H_1 \times H_2 \times \ldots \times H_n$, it is easy to see that $xH_i^{'}x^{-1} = H_i^{'}$. This shows that $H_i^{'} \rhd H_1 \times H_2 \times \ldots \times H_n$. Also $\sigma : H_i^{'} \to H_i$ defined by $\sigma((e, \ldots, h_i, \ldots, e)) = e \ldots h_i \ldots e = h_i \quad \forall \quad h_i \in H_i$. Clearly σ is bijective and is a homomorphism. Hence $H_i^{'} \backsimeq H_i$. Now $H_i^{'} \backsimeq H_i$, $H_i^{'} \rhd H_1 \times H_2 \times \ldots \times H_n$ and $H_1 \times H_2 \times \ldots \times H_n \backsimeq H \Rightarrow H_i \rhd H$. Suppose $x \in H$ has two representations $x = x_1 x_2 \ldots x_n = x_1^{'} x_2^{'} \ldots x_n^{'}$ where $x_i, x_i^{'} \in H_i (1 \leq i \leq n)$ then $\sigma(x_1, x_2, \ldots, x_n) = \sigma(x_1^{'}, x_2^{'}, \ldots, x_n^{'}) \Rightarrow x_1 x_2 \ldots x_n = x_1^{'} x_2^{'} \ldots x_n^{'}$ (σ is $1-1$) $\Rightarrow x_i = x_i^{'}$ for $i = 1, 2, \ldots, n$. Therefore each element $x \in H$ is uniquely written as $x = x_1 x_2 \ldots x_n$, $x_i \in H_i$ $1 \leq i \leq n$.

$(ii) \Rightarrow (iii)$. Assume that (ii) is true.

Let $x_1 x_2 \ldots x_n = e = ee \ldots e \Rightarrow x_i = e, 1 \leq i \leq n$. (by unique representation)

$(iii) \Rightarrow (iv)$. Assume that (iii) is true.

We first prove that $H_i \cap H_j = \{e\}$, $i \neq j$. If $x_i \in H_i \cap H_j$ then $e = x_i x_i^{-1} \in H_i H_j$. By (iii) $x_i x_i^{-1} = e \Rightarrow x_i = e = x_i^{-1}$. Thus $H_i \cap H_j = \{e\}$, $i \neq j$. Let $x \in H_i, y \in H_j, i \neq j$. Since H_i, H_j are normal subgroups of H then $xyx^{-1} \in H_j$ and $yxy^{-1} \in H_i$. Further $xyx^{-1}y^{-1} \in H_i$ and $xyx^{-1}y^{-1} \in H_j$, therefore $xyx^{-1}y^{-1} = e$, since $H_i \cap H_j = \{e\}$, $i \neq j \Rightarrow xy = yx \ \forall \ x \in H_i, y \in H_j$. Let $x_i = x_1 \ldots x_{i-1} x_{i+1} \ldots x_n$, where $x_i \in H_i, 1 \leq i \leq n$ this implies that $e = x_i^{-1} x_1 \ldots x_{i-1} x_{i+1} \ldots x_n = x_1 x_2 \ldots x_{i-1} x_i^{-1} x_{i+1} \ldots x_n$ by the commutation of the elements of H_i and H_j, $i \neq j$. By (iii) we get $x_i = e$, $1 \leq i \leq n$. Thus $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_n) = \{e\}$, $1 \leq i \leq n$

$(iv) \Rightarrow (i)$. Assume that (iv) is true.

We first note that $xy = yx \ \forall \ x \in H_i, y \in H_j, i \neq j$.

Define a map $\sigma : H_1 \times H_2 \times \ldots \times H_n \to H$ by $\sigma(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n$.

Clearly the map σ is surjective.

σ is homomorphism: For all $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n) \in H_1 \times H_2 \times \ldots \times H_n$ then we have $\sigma(x_1, x_2, \ldots, x_n) = x_1 x_2 \ldots x_n$ and $\sigma(y_1, y_2, \ldots, y_n) = y_1 y_2 \ldots y_n$

$$\begin{aligned}
\sigma\Big((x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n)\Big) &= \sigma(x_1 y_1, x_2 y_2, \ldots, x_n y_n) \\
&= x_1 y_1 x_2 y_2 \ldots x_n y_n \\
&= x_1 x_2 \ldots x_n y_1 y_2 \ldots y_n (\text{by the commutation}) \\
&= \sigma(x_1, x_2, \ldots, x_n)\sigma(y_1, y_2, \ldots, y_n)
\end{aligned}$$

Thus σ is a homomorphism. Now

$$\begin{aligned}
ker\sigma &= \{(x_1, x_2, \ldots, x_n) | \sigma(x_1, x_2, \ldots, x_n) = e\} \\
&= \{(x_1, x_2, \ldots, x_n) | x_1 x_2 \ldots x_n = e\} \\
&= \{(x_1, x_2, \ldots, x_n) | x_i^{-1} = x_1 x_2 \ldots x_{i-1} x_{i+1} \ldots x_n, 1 \leq i \leq n\} \\
&= \{(x_1, x_2, \ldots, x_n) | x_i = e, 1 \leq i \leq n\} \quad \text{by (iv)} \\
&= \{(e, e, \ldots, e)\}
\end{aligned}$$

σ is injective. Therefore $H_1 \times H_2 \times \ldots \times H_n \simeq H$.

6.3 Internal Direct Product

6.3.1 Definition : Let $H_1, H_2, \ldots, H_n$ be subgroups of a group G and let $H = H_1 H_2 \ldots H_n$ then we say that H is the internal direct product of H_i, $1 \leq i \leq n$ if the subgroup H_i satisfy any one of the statement of the theorem

(8.2.2).

It may be noted that the external direct product $H_1 \times H_2 \times \ldots \times H_n$ always exists, where as the internal direct product of H_i, $1 \leq i \leq n$ exists if and only if the canonical map $H_1 \times H_2 \times \ldots \times H_n \to H_1 H_2 \ldots H_n$ is an isomorphism.

The emphasis of the words internal and external may be dropped if the subgroups $H_i, 1 \leq i \leq n$ satisfy any one of the condition of theorem (6.2.2).

6.3.2 Direct Sum : If G is an additive group and H_i $(1 \leq i \leq n)$ are subgroups of G then the (internal) direct product of subgroups H_i of G is called the direct sum of H_i and is also written as $H_1 \oplus H_2 \oplus \ldots \oplus H_n$.

6.3.3 Example : If each non identical element of a finite group G is of order 2 then $|G| = 2^n$ and $G \backsimeq C_1 \times C_2 \times \ldots \times C_n$, where each C_i $(1 \leq i \leq n)$ is cyclic group of order 2.

Solution. Given that G is a finite group and each element $x \in G$, $x \neq e$ is of order 2. Therefore $x = x^{-1}$ $\forall$ $x \in G$. For all $a, b \in G$ we have $ab \in G$ and $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Hence G is abelian. Let $a_1 \in G, a_1 \neq e$ and $C_1 = [a_1]$. If $G = C_1$ then the result is true. Otherwise there exist an element $a_2 \in G$, $a_2 \notin C_1$. Let $C_2 = [a_2]$, consider the product C_1C_2, clearly C_1C_2 is a subgroup of G (since G is abelian), $C_1 \cap C_2 = \{\text{e}\}$ and $|C_1C_2| = |C_1||C_2| = 2^2$. Further C_1 and C_2 are normal in C_1C_2. On using theorem (8.3)(iv) we get $C_1C_2 \backsimeq C_1 \times C_2$. Thus the product is the direct product. If $G = C_1C_2$ then $|G| = 2^2$ and $G \backsimeq C_1 \times C_2$. Thus, the result follows. Otherwise C_1C_2 is a proper subgroup of G. This process continues and ultimately, we get $G = C_1C_2 \ldots C_n$ where $C_i = [a_i], 1 \leq i \leq n$. Observe that each C_i is normal in G (since G is abelian) and $C_i \cap (C_1C_2 \ldots C_{i-1}C_{i+1} \ldots C_n) = \{e\}, 1 \leq i \leq n$.

By the theorem (8.2.2)(iv) we get $C_1C_2\ldots C_n \backsimeq C_1 \times C_2 \times \ldots \times C_n$. Hence the result.

6.3.4 Example : A group G of order 4 is either cyclic group or $G \backsimeq C_1 \times C_2$ a direct product of two cyclic groups $C_i, i = 1, 2$ each of order 2.

Solution. Given $|G| = 4$ then by Lagranges theorem the order of every element $a(a \neq e)$ of G divides $4 \Rightarrow O(a) = 4$ or 2. In the case of $O(a) = 4$ we get $G = [a]$ a cyclic group. If $O(a) = 2$, so every non identity element of G is of order 2. Let $C_1 = [a]$ and $C_2 = [b]$, where $b \notin C_1$. Hence $G \backsimeq C_1 \times C_2$ by the above Example (8.3.3).

6.3.5 Note : Every group of order 4 is either cyclic group or isomorphic to klein's four group.

6.3.6 Example : Let G be a finite group of order pq, where p, q are district primes and if G has a normal subgroup H of order p and a normal subgroup K of order q then G is cyclic.

Solution. Given $|G| = pq$, where p and q are distinct primes. $H \rhd G, K \rhd G$ and $|H| = p$, $|K| = q$. By Lagrange's theorem $|H \cap K|$ divides both $|H|$ and $|K|$. Since p and q are distinct primes we get $|H \cap K| = 1$.Therefore $H \cap K = \{e\}$.

Let $h \in H, k \in K$ and H, K are normal in G we get $hkh^{-1}k^{-1} \in H \cap K \Rightarrow hk = kh \quad (H \cap K = \{e\})$. Thus HK is a subgroup of G. Further $|HK| = \frac{|H||K|}{H \cap K|} = pq = |G|$. Thus $G = HK$. Clearly $H \rhd HK$, $K \rhd HK$ and $HK \backsimeq H \times K$ by $8.3(iv)$. Since p, q are primes then H and K are cyclic. Let

$H = [h], K = [k]$ then

$$\begin{aligned} (hk)^{pq} &= (hk)(hk)\dots(hk) \quad (pq \text{ times }) \\ &= (hh\dots h)(kk\dots k) \\ &= h^{pq}k^{pq} \\ &= (h^p)^q(k^q)^p \\ &= e \quad \Rightarrow G =< hk > \end{aligned}$$

G is generated by hk. Thus G is cyclic and $G = H \times K$. Hence the result.

6.3.7 Example : If G is cyclic group of order mn, where $(m, n) = 1$ then $G \simeq H \times K$, where H and K are subgroup of G orders m and n respectively.

Solution. G is a cyclic group of order mn and $(m, n) = 1$. Since m and n divides $|G|$ and G is cyclic group there exist unique subgroups H and K of G order m and n respectively. (If G is a finite cyclic group of order n and d is a positive divisor of n then G has a unique subgroup of order d). By Lagrange theorem $|H \cap K|$ divides both $|H|$ and $|K|$, so $|H \cap K| = 1$ since $(m, n) = 1$. Therefore $H \cap K = \{e\}$ and $|HK| = \frac{|H||K|}{H \cap K|} = mn = |G|$, thus $G = HK$. Since G is cyclic group then H and K are normal in $G = HK$ and using theorem (8.3) we get $HK \simeq H \times K$. Hence $G \simeq H \times K$.

6.3.8 Example : If G is a finite cyclic group of order $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$, where p_i's are distinct primes $1 \leq i \leq k$. Then $G \simeq H_1 \times H_2 \times \dots \times H_k$, where H_i is a cyclic group order p_i, $1 \leq i \leq k$.

Solution. Given that G is a finite cyclic group and $|G| = n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$, where p_i's are distinct primes and e_i's are natural numbers $1 \leq i \leq k$. We shall prove the result by induction on n, the order G. Assume that the result is true for all groups whose order is less than n. We have $|G| = n = mp_k^{e_k}$, where $m = p_1^{e_1}p_2^{e_2}\ldots p_{k-1}^{e_{k-1}}$. Now $(m, p_k^{e_k}) = 1$ and using Example (8.10) we get $G \simeq H \times H_k$, where H and H_k are cyclic subgroups of G of orders m and $p_k^{e_k}$ respectively. Since $|H| = m < n$, by induction of hypothesis $H \simeq H_1 \times H_2 \times \ldots \times H_{k-1}$, where H_i is a cyclic group of order $p_i^{e_i}$, $1 \leq i \leq k-1$. Thus $G \simeq H \times H_k$. Hence $G \simeq H_1 \times H_2 \times \ldots \times H_{k-1} \times H_k$.

6.3.9 Example : Show that the group $(Z/(4), +)$ cannot be written as the direct sum of two non-trivial subgroups.

Solution. Assume that $Z/(4)$ is the direct sum of two non-trivial subgroups H and K then each of H and K must be of order 2 and $H \cap K =\{\bar{0}\}$. Since $Z/(4)$ has a unique subgroup $\{\bar{0}, \bar{2}\}$ of order 2 then $H = K = \{\bar{0}, \bar{2}\}$. This is not possible since $H \oplus K = H \neq Z/(4)$. Hence $(Z/(4), +)$ cannot be written as a direct sum of two non-trivial subgroups.

6.3.10 Example: Show that the group $Z/(10)$ is a direct sum of $H = \{\bar{0}, \bar{5}\}$ and $K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$.

Solution. We known that the group $Z/(10)$ is abelian. Note that $H = [\bar{5}], K = [\bar{2}]$.

H and K are normal of $Z/(10)$ and $H \cap K = \{\bar{0}\}$. Further $H \oplus K = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{5}, \bar{7}, \bar{9}, \bar{1}, \bar{3}\} = Z/(10)$. Therefore $Z/(10)$ is the (internal) direct sum of H and K.

6.4 Summary

In this lesson we have introduced the notion of direction product of a finite number of subgroups of a group. Also we have defined internal direct product and direct sum. At the end of this section we given examples.

6.5 Model Examination Questions

(1) Show that the group $Z/(8)$ cannot be written as the direct sum of two nontrivial subgroups.

(2) Let $N \triangleleft G = H \times K$. Prove that either N is a abelian or N intersects one of the subgroups $H \times \{e\}$, $\{e\} \times K$ nontrivially.

6.6 Glossary

Direct product, internal direct product, direct sum

LESSON-07

FINITELY GENERATED ABELIAN GROUPS AND THE INVARIANT OF A FINITE ABELIAN GROUP

7.1 Introduction : In this lesson we study that any finitely generated abelian group can be decomposed as a finite direct sum of cyclic groups. This decomposition, when applied to finite abelian groups, enables us to find the number of nonisomorphic abelian groups of a given order.

Let G be a group and S be a subset of G. Let $\mathscr{G}$ be the family of subgroups of G containing S. let $M = \cap A$, where the intersection is taken over all subgroups A of $\mathscr{G}$. Clearly M is the smallest subgroup of G containing S or M is called the subgroup of G generated by S and we write $M = [S]$. If S is empty then $M = \{e\}$.

If S is a nonempty subset of G then $M = [S]$, the subgroup generated by S, is the set of finite product $x_1 x_2 \dots x_n$ such that for each i, $x_i \in S$ or $x_i^{-1} \in S$. In other words every $m \in M$ is a finite product $m = x_{i_1}^{n_1} x_{i_2}^{n_2} \dots x_{i_k}^{n_k}$ where x_{i_j}'s are elements of S and are not necessarily distinct and n_j's are integers.

If $G = [S]$ for some nonempty subset S of G then S is called a set of generators of G. If S is finite and $G = [S]$ then G is said to be finitely generated group i.e., a group G is said to be finitely generated if it is generated by a finite subset of G.

The following may be noted

(i) Every cyclic group is finitely generated.

(ii) Every finite group is finitely generated and the converse is not true.

For example $(Z, +)$ is finitely generated but is not finite

(iii) All groups are not finitely generated. For example $(Q, +)$.

7.2 Fundamental theorem of finitely generated abelian groups

7.2.1 Theorem : Let A be a finitely generated abelian group then A can be decomposed as a direct sum of a finite number of cyclic groups C_i. Precisely $A = C_1 \oplus C_2 \oplus \ldots \oplus C_k$ such that either $C_1, C_2, \ldots, C_k$ are all infinite or for some $j \leq k$, $C_1, C_2, \ldots, C_j$ are of order $m_1, m_2, \ldots, m_j$ respectively with $m_1|m_2|\ldots|m_j$ and $C_{j+1}, \ldots, C_k$ are infinite.

Proof. Given that A is finitely generated abelian group i.e., A is generated by a finite number of elements of A.

Let k be the smallest number such that A is generated by a set of k elements. The theorem is proved by induction on k.

If $k = 1$ then A is generated by a single element i.e., A is cyclic group and the theorem follows trivially.

Let $k > 1$, and we assume that the theorem is valid for every group generated by a set of $k-1$ elements. Then we have the following possibilities.

(i) A has a generating set $S = \{a_1, a_2, \ldots, a_k\}$ with the property that for all $\alpha_1, \alpha_2, \ldots, \alpha_k \in Z$ such that the equation $\sum\limits_{i=1}^{n} \alpha_i a_i = 0 \Rightarrow \alpha_i = 0$ $(1 \leq i \leq k)$.

(ii) A has no generating set of k elements with the property stated in (i).

Case(i) In this case none of the elements of S is the additive identity. It is easy to see that every subset of S has the property stated in (i). Let $C_i = [a_i]$ be the cyclic subgroup generated by a_i, $1 \leq i \leq k$. Clearly $\alpha_i a_i = 0 \Rightarrow \alpha_i = 0$ hence C_i is an infinite cyclic group and $C_i \rhd A$. Every element $a \in A$ has a unique representation of the form $a = \sum\limits_{i=1}^{k} \alpha_i a_i$ where $\alpha_i \in Z$.

If $a = \sum\limits_{i=1}^{k} \alpha_i a_i = \sum\limits_{i=1}^{k} \beta_i a_i$ then $\sum\limits_{i=1}^{k} (\alpha_i - \beta_i) a_i = 0$ and this implies $\alpha_i = \beta_i$, $1 \leq i \leq k$. On using theorem (8.3) we get $A = C_1 \oplus C_2 \oplus \ldots \oplus C_k$ i.e., A is the direct sum of finite numbers of infinite cyclic subgroups. This proves a part of the theorem.

Case(ii) In this case given any generating set $\{p_1, p_2, \ldots, p_k\}$ of A there exists integers $\alpha_1, \alpha_2, \ldots, \alpha_k$ not all of them zero such that $\sum_{i=1}^{k} \alpha_i p_i = 0$. Since $\sum \alpha_i p_i = \sum (-\alpha_i) p_i = 0$, we may assume that $\alpha_i > 0$ for some i.

Now consider all possible generating sets of A with k elements and let X be the set of all k- tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ of integers such that $\sum_{i=1}^{k} \alpha_i q_i = 0$, $\alpha_i > 0$ for some i, some generating set $\{q_1, q_2, \ldots, q_k\}$ of A. Let m_1 be the least positive integer that occurs as a component in a k-tuple in X. Without loss of generality we may take m_1 to be the first component, so that for some generating set $S = \{a_1, a_2, \ldots, a_k\}$ we have $m_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_k a_k = 0$. By division algorithm we can write $\alpha_i = q_i m_1 + r_i,\ 0 \leq r_i < m_1,\ 2 \leq i \leq k$ putting $\alpha_i' s$ in the above we get

$$m_1 b_1 + r_2 a_2 + \ldots + r_k a_k = 0 \qquad (7.2.1(a))$$

where $b_1 = a_1 + q_2 a_2 + \ldots + q_k a_k = 0$, here $b_1 \neq 0$. If $b_1 = 0$ then $a_1 = -\sum_{i=2}^{k} q_i a_i$ and this implies that A is generated by $k-1$ elements which is a contradiction to the maximality of k. Further $b_1 = a_1 - \sum_{i=2}^{k} q_i a_i \Rightarrow S' = \{b_1, a_2, \ldots, a_k\}$ is a generating set of A. From the equation (7.2.1(a)) and by the minimal property of m_1 we get $r_2 = r_3 = \ldots = r_k = 0$. Thus we get $m_1 b_1 = 0$. Let $C_1 = [b_1]$. Now C_1 is a cyclic subgroup of A of order m_1, since m_1 is the least positive integer such that $m_1 b_1 = 0$ and $C_1 \rhd A$.

Let A_1 be the subgroup generated by $\{a_2, a_3, \ldots, a_k\}$. Clearly $A_1 \rhd A$ and $A = C_1 \oplus A_1$. By theorem (6.2.2)(iv), it is sufficient to prove that $C_1 \cap A_1 = \{0\}$. An element of C_1 is of the form $\alpha_1 b_1$, $\alpha_1 \in Z$, $0 \leq \alpha_1 < m_1$.

Suppose $\alpha_1 b_1 \in A_1$ then $\alpha_1 b_1 = \alpha_2 a_2 + \ldots + \alpha_k a_k$, where $\alpha_i \in Z$, $2 \leq i \leq k$. Therefore $\alpha_1 b_1 - \alpha_2 a_2 \ldots - \alpha_k a_k = 0 \Rightarrow \alpha_i = 0$ by the minimal property of m_1. Thus $A = C_1 \oplus A_1$. Now A_1 cannot be generated by less than $k-1$ elements, for otherwise A would be generated by less than k elements which is a contradiction to minimality of k. By induction of hypothesis $A = C_2 \oplus C_3 \oplus \ldots \oplus C_k$, where C_i, $2 \leq i \leq k$ are all cyclic groups which are all infinite or for some $j < k$, $C_2, C_3, \ldots, C_j$ are finite cyclic groups of orders $m_2, m_3, \ldots, m_j$ respectively with $m_2|m_3|\ldots|m_j$ and the remaining C_i, $i > j$ are infinite .

Let $C_i = [b_i]$, $2 \leq i \leq k$. Suppose that the order of C_2 is m_2 then $\{b_1, b_2, \ldots, b_k\}$ is a generating set of A and

$$m_1 b_1 + m_2 b_2 + 0.b_3 + \ldots + 0.b_k = 0 \qquad (7.2.1(b))$$

since m_1 is the least positive integer that occurs as a component in any k-tuple in X, by division algorithm $m_2 = m_1 q_2 + r_2$, $0 \leq r_2 < m_1$. From equation $(7.2.1(b))$ we get

$$m_1 d_1 + r_2 b_2 + 0.b_3 + \ldots + 0.b_k = 0 \qquad (7.2.1(c))$$

where $d_1 = b_1 + q_2 b_2$, here $d_1 \neq 0$. If $d_1 = 0$ then $C_1 = C_2$ which is a contradiction. Further $\{d_1, b_2, \ldots, b_k\}$ is a generating set of A. By the minimal property of m_1 and from equation (7.2.1(c)) we get $r_2 = 0$. Thus $m_2 = m_1 q_1$ and $m_1|m_2$. Hence the theorem.

7.2.2 Note : If A is a finite abelian group then $C_1, C_2, \ldots, C_k$ are all finite. In this section A denote a finite abelian group written additively.

7.2.3 Theorem : Let A be a finite abelian group then there exists a unique finite list of integer $m_1, m_2, \ldots, m_k$ (all > 1) such that $|A| = m_1 m_2 \ldots m_k$ and $m_1 | m_2 | \ldots | m_k$ and $A = C_1 \oplus C_2 \oplus \ldots \oplus C_k$, where $C_1, C_2, \ldots, C_k$ are cyclic group of A of order $m_1, m_2, \ldots, m_k$ respectively. Consequently $A \simeq Z_{m_1} \oplus Z_{m_2} \oplus \ldots \oplus Z_{m_k}$.

Proof. Given that A is a finite abelian group and hence A is finitely generated. By theorem (7.2.1) A is decomposed as an (internal) direct sum of a finite number of finite cyclic subgroups C_i, $1 \leq i \leq k$ with $|C_i| = m_i$ and $m_1 | m_2 | \ldots | m_k$. We have $A = C_1 \oplus C_2 \oplus \ldots \oplus C_k$ and by the definition of internal direct sum.

$$C_1 \oplus C_2 \oplus \ldots \oplus C_k \simeq C_1 \times C_2 \times \ldots \times C_k$$

Therefore $|A| = |C_1||C_2| \ldots |C_k| = m_1 m_2 \ldots m_k$. Further it is known that every cyclic group of order m is isomorphic to Z_m. Hence

$$A = C_1 \oplus C_2 \oplus \ldots \oplus C_k \simeq Z_{m_1} \oplus Z_{m_2} \oplus \ldots \oplus Z_{m_k}$$

We now prove the uniqueness of the list $m_1, m_2, \ldots, m_k$.

Suppose $A = C_1 \oplus C_2 \oplus \ldots \oplus C_k \simeq D_1 \oplus D_2 \oplus \ldots \oplus D_l$ where C_i, $1 \leq i \leq k$, D_j, $1 \leq j \leq l$ are all cyclic groups with $|C_i| = m_i$, $m_1 | m_2 | \ldots | m_k$ and $|D_j| = n_j$, $n_l | n_2 | \ldots | n_l$. Clearly every element of A is of order $\leq m_k$ and D_l has an element of order n_l, from this we get $n_l \leq m_k$. Reversing the argument we get $m_k \leq n_l$. Thus $m_k = n_l$. Now $m_{k-1}A = \{m_{k-1}a | a \in A\}$ from the above two decompositions of A, we get

$$\begin{aligned}m_{k-1}A =&(m_{k-1}C_1) \oplus \ldots \oplus (m_{k-1}C_{k-1}) \oplus (m_{k-1}C_k)\\ =&(m_{k-1}D_1) \oplus \ldots \oplus (m_{k-1}D_{l-1}) \oplus (m_{k-1}D_l)\\ \Rightarrow |m_{k-1}A| =&|m_{k-1}C_1| \ldots |m_{k-1}C_{k-1}|\ |m_{k-1}C_k|\\ =&|m_{k-1}D_1| \ldots |m_{k-1}D_{l-1}|\ |m_{k-1}D_l| \qquad (7.2.3(a))\end{aligned}$$

we have $m_i \big| m_{k-1}$, $1 \leq i \leq k-1 \Rightarrow m_{k-1}C_i = \{0\}$ and hence $|m_{k-1}C_i| = 1$, $1 \leq i \leq k-1$. From the equation (7.2.3(a)) we get

$$|m_{k-1}A| = |m_{k-1}C_k| = |m_{k-1}D_1| \ldots |m_{k-1}D_{l-1}|\ |m_{k-1}D_l|$$

since $m_k = n_l$, note that $|m_{k-1}C_k| = |m_{k-1}D_l|$ and it follows that

$$1 = |m_{k-1}D_1|\ |m_{k-1}D_2| \ldots |m_{k-1}D_{l-1}|$$

Hence $|m_{k-1}D_j| = 1$, $1 \leq j \leq l-1$. This implies in particular that $m_{k-1}D_{l-1}$ is trivial and m_{k-1} is a multiple of n_{l-1} that is $n_{l-1}/_{m_{k-1}}$.
By similar argument we get $m_{k-1}/_{n_{l-1}}$ Thus $m_{k-1} = n_{l-1}$. Continuing in this way, using the fact $m_1m_2 \ldots m_k = |A| = n_1n_2 \ldots n_l$, we get $k = l$ and $m_i = n_i$, $1 \leq i \leq k$. Hence the theorem.

7.3 THE INVARIANT OF A FINITE ABELIAN GROUP

7.3.1 Definition : Let A be a finite abelian group. If $A \simeq Z_{m_1} \oplus Z_{m_2} \oplus \ldots \oplus Z_{m_k}$ where $1 < m_1 | m_2 | \ldots | m_k$ then A is said to be of type $(m_1, m_2, \ldots, m_k)$ and the integers $m_1, m_2, \ldots, m_k$ are called invariants of A.

7.3.2 Remark : Two finite abelian groups are isomorphic iff they are of the same type.

7.3.3 Definition : A partition of a positive integer k is an r-tuple $(k_1, k_2, \ldots, k_r)$ of positive integers such that $k = k_1 + k_2 + \ldots + k_r$ and $k_i \leq k_{i+1}$, $1 \leq i \leq r-1$. The set of partitions of k is denoted by $P(k)$.

7.3.4 Lemma : Let F be the family of non-isomorphic abelian group of order p^e, where p is a prime then there is a one-one correspondence between F and the set $P(e)$ of partitions of e .

proof. Let $A \in F$. By theorem (9.4) we have $A \simeq Z_{m_1} \oplus Z_{m_2} \oplus \ldots \oplus Z_{m_k}$, where $1 < m_1 | m_2 | \ldots | m_k$ and determine a unique type $(m_1, m_2, \ldots, m_k)$. Now $|A| = p^e = m_1 m_2 \ldots m_k$ and $1 < m_1 | m_2 | \ldots | m_k$ then $m_1 = p^{e_1}, m_2 = p^{e_2}, \ldots, m_k = p^{e_k}$ with $e_1 \leq e_2 \leq \ldots \leq e_k$ and $e_1 + e_2 + \ldots + e_k = e$. Thus every $A \in F$ determines a partition $(e_1, e_2, \ldots, e_k)$ of e.

Define a map $\sigma : F \to P(e)$ by $\sigma(A) = (e_1, e_2, \ldots, e_k)$. If $B \in F$ and $B \neq A$ then A and B are not isomorphic then they determine different partitions of e, i.e., $\sigma(A) \neq \sigma(B)$. Thus shows that σ is injective.

For every $(e_1, e_2, \ldots, e_s) \in P(e)$ we have the abelian group

$$G = Z_{p^{e_1}} \oplus Z_{p^{e_2}} \oplus \ldots \oplus Z_{p^{e_s}} \in F$$

such that $\sigma(G) = (e_1, e_2, \ldots, e_s)$. This shows that σ is surjective. Thus there is a one-one correspondence between F and $P(e)$. Hence the lemma.

7.3.5 Lemma : Let A be a finite abelian group of order $p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, where p_i $(1 \leq i \leq k)$ are distinct primes and $e_i > 0$ then $A = S(p_1) \oplus S(p_2) \oplus \ldots \oplus S(p_k)$, where $|S(p_i)| = p_i^{e_i}$. This decomposition is unique,
i.e., if $A = H_1 \oplus H_2 \oplus \ldots \oplus H_k$ where $|H_i| = p_i^{e_i}$ then $H_i = S(p_i)$, $1 \leq i \leq k$.

Proof. We have A is a finite abelian group and $|A| = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, where

$p_i's$ are distinct primes and $e_i > 0$ $(1 \le i \le k)$. On using theorem (9.4) we get $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n$ where A_i $(1 \le i \le n)$ are cyclic subgroups of A with the property $1 < |A_1|/|A_2|/\ldots/|A_n|$.

Let $|A_i| = p_1^{e_{1i}} p_2^{e_{2i}} \ldots p_k^{e_{ki}}$ where $e_{ji} > 0$, $1 \le j \le k$, since A_i is cyclic group and A_i contains unique subgroups $A_{1i}, A_{2i}, \ldots, A_{ki}$ of orders $p_1^{e_{1i}}, p_2^{e_{2i}}, \ldots, p_k^{e_{ki}}$ respectively. Using the fact $p_i's$ are distinct and by Langranges theorem we get

$$A_{ji} \cap (A_{1i} \oplus \ldots \oplus A_{(j-1)i} \oplus A_{(j+1)i} \oplus \ldots \oplus A_{ki}) = \{0\}$$

for all $j = 1, 2, \ldots, k$. Further $A_{ji} \rhd A_i$, $1 \le j \le k$ and we have $A_i = A_{1i} \oplus A_{2i} \oplus \ldots \oplus A_{ki}$. Therefore

$$\begin{aligned} A =&[A_{11} \oplus A_{21} \oplus \ldots \oplus A_{k1}] \oplus [A_{12} \oplus A_{22} \oplus \ldots \oplus A_{k2}] \oplus \ldots \oplus [A_{1n} \oplus A_{2n} \oplus \ldots \oplus A_{kn}] \\ \Rightarrow A =&[A_{11} \oplus A_2 \oplus \ldots \oplus A_{1n}] \oplus [A_{21} \oplus A_{22} \oplus \ldots \oplus A_{2n}] \oplus \ldots \oplus [A_{k1} \oplus A_{k2} \oplus \ldots \oplus A_{kn}] \\ =&S(p_1) \oplus S(p_2) \oplus \ldots \oplus S(p_k) \end{aligned}$$

where $S(p_j) = A_{j1} \oplus A_{j2} \oplus \ldots \oplus A_{jn}$, $1 \le j \le k$ and $|S(p_j)| = |A_{j1}|\,|A_{j2}|\,\ldots|A_{jn}| = p_j^{e_{j1}+e_{j2}\ldots+e_{jn}} = p_j^{e_j}$. This proves the first part of the theorem.

Suppose $A = H_1 \oplus H_2 \oplus \ldots \oplus H_k$ where $|H_i| = P_i^{e_i}$, $1 \le i \le k$. Clearly each of the subgroups $S(P_i)$ and H_i is the subgroup containing all those elements of A whose orders are power of p_i. Hence $H_i = S(P_i)$, $1 \le i \le k$. This prove the uniqueness of the decomposition of A. Hence the theorem.

7.3.6 Theorem : Let $n = \prod_{j=1}^{k} p_j^{e_j}$, where p_j are distinct primes then the number of non-isomorphic abelian groups of order n is given by $\prod_{j=1}^{k} |P(e_j)|$.

Proof. Let A_n be the family of non isomorphic abelian groups of order n.

Let $A \in A_n$ and by lemma 10.6, we have $A = S(p_1) \oplus S(p_2) \oplus \ldots \oplus S(p_k)$, where $|S(p_j)| = p_j^{e_j}$, $1 \leq j \leq k$. By lemma 10.5, the number of non isomorphic abelian groups $S(p_j)$ is $|P(e_j)|$.

Therefore the number of non isomorphic abelian groups of order n is given by $|P(e_1)|\ |P(e_2)| \ldots |P(e_n)|$. Thus $|A_n| = \prod_{j=1}^{k} |P(e_j)|$. Hence the theorem.

7.3.7 Example : Find the non-isomorphic abelian groups of orders p, p^2 and p^3, where p is prime number.

Solution. If $n = p^e$, where p is prime number then by lemma (10.6), the number of non-isomorphic abelian group of order n is $|P(e)|$, where $P(e)$ is the set of partitions of e. The following may be noted

$$P(1) = \{(1)\} \quad \text{and} \quad |P(1)| = 1$$

$$P(2) = \{(1,1),(2)\} \quad \text{and} \quad |P(2)| = 2$$

$$P(3) = \{(1,1,1),(1,2),(3)\} \quad \text{and} \quad |P(3)| = 3$$

(i) The number of non-isomorphic abelian groups of order p is $|P(1)| = 1$. Therefore there is only one abelian group of order p of type (p) and it is given by Z_p. We know that every group of prime order is cyclic and abelian. Hence there is only one group of order p (up to isomorphism) given by Z_p.

(ii) The number of non-isomorphic abelian group of order p^2 is $|P(2)| = 2$. Hence there are only two non-isomorphic abelian groups of order p^2. They are of type (p,p) and (p^2) given by $Z_p \oplus Z_p$ and Z_{p^2} respectively.

(iii) The number of non isomorphic abelian groups of order p^3 is $|P(3)| = 3$. Hence there are only three non-isomorphic abelian groups of order p^3. They are of type $(p,p,p),(p,p^2),(p^3)$ given by $Z_p \oplus Z_p \oplus Z_p$, $Z_p \oplus Z_{p^2}$ and Z_{p^3} respectively.

7.3.8 Example : Find the non-isomorphic abelian groups of order 360.

Solution. We have $n = 360 = 2^3.3^2.5^1$

where $e_1 = 3,\ e_2 = 2,\ e_3 = 1\ \ p_1 = 2,\ p_2 = 3,\ p_3 = 1$ and

$|P(3)| = 3,\ |P(2)| = 2,\ |P(1)| = 1$

The number of non-isomorphic abelian groups of order 360 is

$$\prod_{j=1}^{3} |P(e_j)| = |P(3)|\ |P(2)|\ |P(1)|$$

$$= 3 \times 2 \times 1$$

$$= 6$$

They are of the types : $(2,2,2,,3,3,5)$, $(2,2,2,9,5)$, $(2,4,3,3,5)$,

$(2,4,9,5)$, $(8,3,3,5)$, $(8,9,5)$

The above six types determine the following 6 non isomorphic abelian groups

$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \oplus Z_5$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_9 \oplus Z_5$$
$$Z_2 \oplus Z_4 \oplus Z_3 \oplus Z_3 \oplus Z_5$$
$$Z_2 \oplus Z_4 \oplus Z_9 \oplus Z_5$$
$$Z_8 \oplus Z_3 \oplus Z_3 \oplus Z_5$$
$$Z_8 \oplus Z_9 \oplus Z_5$$

7.4 Summary

In this lesson we have defined any finitely generated abelian group can be decomposed as a finite direct sum of cyclic groups and also we have defined the number of non isomorphic abelian groups of a given order

7.5 Model Examination Questions

(1) State and prove fundamental theorem of finitely generated abelian groups.

(2) Let A be a finite abelian group then there exists a unique finite list of integer $m_1, m_2, \ldots, m_k$ (all > 1) such that $|A| = m_1 m_2 \ldots m_k$ and $m_1 | m_2 | \ldots | m_k$ and $A = C_1 \oplus C_2 \oplus \ldots \oplus C_k$, where $C_1, C_2, \ldots, C_k$ are cyclic group of A of order $m_1, m_2, \ldots, m_k$ respectively. Consequently $A \simeq Z_{m_1} \oplus Z_{m_2} \oplus \ldots \oplus Z_{m_k}$.

(3) Let F be the family of non-isomorphic abelian group of order p^e, where p is a prime then there is a one-one correspondence between F and the set $P(e)$ of partitions of e .

(4) Let $n = \prod_{j=1}^{k} p_j^{e_j}$, where p_j are distinct primes then the number of non-isomorphic abelian groups of order n is given by $\prod_{j=1}^{k} |P(e_j)|$.

(5) Find the non-isomorphic abelian groups of order 2020.

7.6 Glossary

Finitely generated abelian group, finite direct sum cyclic groups, Invariants, partition of a integer, partion set, invariants of a finitely generated abelian group.

LESSON-8

CAUCHY'S THEOREM FOR ABELIAN GROUP AND SYLOW THEOREMS

8.1 Introduction : The decomposition of a finite abelian group A as a direct sum of finite number of cyclic groups gives a complete description of the structure A. The sylow's theorems yields a powerful set of tools for studying the structure and the classification of finite groups. we study the existence or non existence of simple group of a given order.Moreover we analyse the groups of order p^2 and pq, where $p \; q$ are prime numbers.

8.2 Cauchy's theorem for abelian group and first sylow theorem

8.2.1 Definition : ***p*-group** Let p be a prime number. A group G is said to be a p-group if the order of every element of G is a power of p.

8.2.2 Example : (i) $\mathbf{Z}_4$ is a 2-group.

(ii) $\mathbf{Z}_2 \times \mathbf{Z}_2$ is a 2-group.

(iii)$\mathbf{Z}_{27}$ is a 3-group.

8.2.3 Definition : ***p*-subgroup** A subgroup H of a group G is said to be a p-subgroup of G if the order of every element of H is a power of p, where p is a prime number.

8.2.4 Definition : **Sylow *p*-subgroup** Let G be a group and p be a prime number. Let $p^m/|G|$ and $p^{m+1} \nmid |G|$ (i.e., p^{m+1} does not divides $|G|$) where $m \in \mathrm{N}$ then any subgroup of order p^m of G is called a Sylow p-subgroup of G (i.e., a maximal p-subgroup of a group G is a Sylow $p-$subgroup of G).

8.2.5 Lemma : (Cauchy's theorem for abelian group) Let A be a finite abelian group and p be a prime number. If $p/|A|$ (i.e., p divides $|A|$) then A has an element of order p.

Proof. Let A be a finite abelian group. Let $|A| = n$. Let $p/|A|$, where p is prime number.

Case(i) If $|A| = p$ then A is cyclic group of order p. Let $A =< a >$, where $a \in A \;\Rightarrow O(a) = p \Rightarrow$ there exists an element $a \in A$ of order p.

Case (ii) Let A be any cyclic group then $p/|A| \Rightarrow |A| = pk$ for some k. Let $a \in A$ then $a^{|A|} = e \Rightarrow a^{pk} = e \Rightarrow (a^k)^p = e \Rightarrow O(a^k) = p$.

We shall prove the theorem by induction on $|A| = n$. Let us assume that the theorem is true for all groups whose order is less than $|A|$.

Consider $B =< a^k >$, the cyclic group generated by a^k of order p then $|B| = p$ where $p < n$. Therefore we have $p/|B|$ and $p < n$ then by induction B has an element of order p. Since $B < A$ then A has an element of order p.

Case (iii) Let A is not cyclic group. Suppose there exist $b \neq e$ in A such that $A \neq< b >$ a cyclic group generated by b (Since $b \in A$, $A \neq< b >$ if $A =< b >$ then A is cyclic group. But given A is not cyclic therefore $A \neq< b >$).

If $p/| < b > |$ then $< b >$ has an element of order p by induction. But $< b > \;<\; A \Rightarrow A$ is also has an element of order p.

Suppose $p \nmid | < b > |$ then consider the quotient group $\frac{A}{<b>}$ then $p/|\frac{A}{<b>}|$.

But $|\frac{A}{<b>}| = \frac{|A|}{|<b>|} < |A|$ then by induction $\frac{A}{<b>}$ has an element of order p.

Let $\bar{a} \in \frac{A}{<b>}$ be an element of order p then $\bar{a} = a < b >$ for some $a \in A$.

Let $O(a) = k$ then $a^k = \; e$.

Now $(\bar{a})^k = (a < b >)^k \;=\; a < b > a < b > \ldots a < b >$ (k times) $=a^k < b >$ $= \; e < b > \;=\; < b >$ which is the identity of $\frac{A}{<b>}$

$\Rightarrow p/k \;\Rightarrow p/| < a > |$, where $< a >$ is a cyclic subgroup of A generated by $a \in A$. Then by induction $< a >$ has an element of order $p \Rightarrow A$ has an element of order p.

8.2.6 Theorem : (First Sylow theorem) Let G be a finite group and let

p be a prime number. If $p^m/|G|$ then G has a subgroup of order p^m.

Proof. Let $|G| = n$. Given that p is a prime number and p^m/n.

We prove the theorem by induction on n. If $n = 1$ then the result is trivial.

Assume that the result is true for all groups of order less than n

i.e., If H is a finite group of order less than n and $p^k/|H|$ then H has a subgroup of order p^k.

Consider $\mathbf{Z}(G)$ the centre of G and we have the following two cases.

case(i) Suppose $p/|\mathbf{Z}(G)|$, since $\mathbf{Z}(G)$ is abelian by Cauchy's theorem for abelian group (11.6) there exist an element say $a \in \mathbf{Z}(G)$ of order p.

Now consider the cyclic group C generated by a, i.e., $C =< a >$ where $a \in \mathbf{Z}(G)$ then $C \triangleright G$.

Since $C =< a >= \{a^i | i = 1, 2, \dots, p\}$, consider for any $g \in G$ we have

$ga^ig^{-1} = (gag^{-1})(gag^{-1}) \dots (gag^{-1})$ (i times)

$= a^i \in C \qquad (a \in \mathbf{Z}(G) \Rightarrow ga = ag)$

Consider the quotient group $\frac{G}{C}$, we have $p^m/|G| \Rightarrow |G| = p^m k$, for some k and $|C| = p \qquad$ (since $|C| = |a| = p$)

then $|\frac{G}{C}| = \frac{|G|}{|C|} = \frac{p^m k}{p} = p^{m-1}k < |G|$ and also $p^{m-1}/|\frac{G}{C}|$

then by induction $\frac{G}{C}$ has a subgroup say $\bar{H}$ of order p^{m-1}.

Then there exist a unique subgroup H of G such that $\bar{H} = \frac{H}{C}$

$\Rightarrow |\bar{H}| = |\frac{H}{C}| = \frac{|H|}{|C|}$

$\Rightarrow |H| = |\bar{H}||C| = p^{m-1}p = p^m$

$\Rightarrow G$ has a subgroup of order p^m.

Case(ii) Suppose $p \nmid |\mathbf{Z}(G)|$. We have the class equation of G

$n = |G| = |\mathbf{Z}(G)| + \sum_a [G : N(a)]$

where the summation runs over one element from each conjugate class having more than one element, we have $p/|G|$ and $p \nmid |\mathbf{Z}(G)|$

$\Rightarrow p \nmid [G : N(a)]$, for some $a \in G, a \notin \mathbf{Z}(G)$

If $p/[G : N(a)]$ for every a then $p/\sum[G : N(a)]$

$\Rightarrow p/|G|$ and $p/\sum[G : N(a)]$

$\Rightarrow p/|\mathbf{Z}(G)|$ which is a contradiction.

For the above a we have $|G| = |N(a)|[G : N(a)]$ and $p \nmid [G : N(a)]$

$a \notin \mathbf{Z}(G) \Rightarrow |N(a)| = p^m l$ for some $l < k$. Therefore $p^m/|N(a)|$.

Clearly $|N(a)| < |G| = n$. Hence by induction of hypothesis $N(a)$ has a subgroup H of order p^m. Thus G has a subgroup H of order p^m.

8.2.7 Corollary : (Cauchy's theorem) Let G be a finite group and p is prime. If $p/|G|$ then G has an element of order p.

Proof. Let G be a finite group such that $p/|G|$ then by first sylow theorem G has a subgroup H of order p.

Since p is prime and $|H| = p \Rightarrow H$ is cyclic.

$\Rightarrow$ every non identity element of H is of order p. Therefore H has $p-1$ elements of order p. But every element of H is an element of G then G has at least $p-1$ elements of order p. Hence the result.

8.2.8 Corollary : A finite group G is a p-group if and only if its order is a power of p.

Proof. Suppose that the order of G is a power of p say p^m. For any element $a \in G$, we have $O(a)/|G| \Rightarrow O(a)/p^m \Rightarrow O(a) = p^k$, for some $k \leq m$.

Thus every element of G has order a power of p. Hence G is a $p-$group.

Conversely, suppose that G is a p-group i.e. every element of G has order power of p.

Suppose $|G| = p^m$ then there is nothing to prove.

Suppose $|G| = q^n$, for some prime number $q \neq p$ then $q/|G|$. By Cauchy's theorem G has an element of order $q(\neq p)$ which is a contradiction, since G is a p-group. Therefore the order G is a power of p. Hence the result.

8.2.9 Definition : Let H be a subgroup of a group G then
$N(H) = \{g \in G | gHg^{-1} = H\}$ is called the normalizer of H in G.

8.2.10 Note : (i) $N(H) < G$

(ii) $H \triangleright N(H)$

(iii) $N(H)$ is the largest subgroup of G in which H is normal.

(iv) If K is a subgroup of $N(H)$ then $H \triangleright KH$.

8.2.11 Lemma : Let H and K be subgroups of a group G and $C_H(K) = \{hKh^{-1} | h \in H\}$ the set of H-conjugates of K then $|C_H(K)|$=$[H : N(K) \cap H]$.

Proof. Define a mapping $f : C_H(K) \to N(K) \cap H$ by
$f(hKh^{-1}) = (N(K) \cap H)h$. Clearly f is onto.

Now to prove f is one-one: $f(h_1Kh_1^{-1}) = f(h_2Kh_2^{-1})$

$$\Rightarrow h_1^{-1}h_2 \in N(K) \cap H$$
$$\Rightarrow h_1^{-1}h_2 \in N(K)$$
$$\Rightarrow h_1^{-1}h_2Kh_2^{-1}h_1 = K$$
$$\Rightarrow h_1Kh_1^{-1} = h_2Kh_2^{-1}$$

Thus there is one-one correspondence between $C_H(K)$ and the set of distinct right cosets of $N(K) \cap H$ in H. Therefore $|C_H(K)| = [H : N(K) \cap H]$. Hence the lemma.

8.2.12 Theorem : Let G be a finite group and let p be a prime number then all Sylow p-subgroups of G are conjugate and their number n_p divides $O(G)$ and satisfies $n_p \equiv 1(mod\ p)$.

Proof. (i) Suppose that $|G| = p^m q$, where $p \nmid q$ then by first Sylow theorem

G has a subgroup K of order p^m, since $p^m/|G|$ and $p^{m+1} \nmid |G|$. Let K be a Sylow $p-$subgroup of G and $C(K)$ be the family of G-conjugates to K i.e., $C(K) = C_G(K) = \{gKg^{-1}|g \in G\}$. By Lemma (8.2.11), we get $|C(K)| = |C_G(K)| = [G : N(K) \cap G] = [G : N(K)]$, since $N(K)$ is a subgroup of G).

Given G is finite then $|C(K)| = |G|/|N(K)|$. It may be seen that $p^m/|N(K)|$.

Since $N(K)$ is the largest subgroup of G in which K is normal and $|K| = p^m$. Therefore

$$p \nmid (|G|/|N(K)|) \Rightarrow p \nmid |C(K)| \qquad (8.2.12(a))$$

Let H be any Sylow p-subgroup of G. We shall show that H is conjugate to K. Now the set $C(K)$ is an H-set by conjugation. For any $L \in C(K)$, let $C_H(L) = \{hLh^{-1}|h \in H\}$ the orbit of L.

Now $C_H(L) = \{hgKg^{-1}h^{-1}|g \in G, h \in H\}$

$$\Rightarrow C_H(L) \subset C_G(K) = C(K) \text{ and}$$

$$C(K) = \bigcup_{L \in C(K)} C_H(L) \quad \text{(a partition))} \qquad (8.2.12(b))$$

where the union runs over one element L from each conjugate class $C_H(L)$ (orbit). By Lemma (8.2.11), since H is a Sylow p-subgroup of order p^m

$$|C_H(L)| = [H : N(L) \cap H] = p^e, \quad e \geq 0 \qquad (8.2.12(c))$$

Claim $P^e = 1 \Leftrightarrow H = L$

If $H = L$ then $p^e = [L : N(L) \cap L] = [L : L] = 1$.

Conversely suppose that $p^e = 1 \Rightarrow H = N(L) \cap H \Rightarrow H \subset N(L)$

$\Rightarrow HL = LH \Rightarrow HL$ is a subgroup of G.

Further $H \subset N(L) \Rightarrow L \rhd HL$. (by Note (8.2.10) (iv))

By second isomorphism theorem $\frac{HL}{L} \simeq \frac{H}{H \cap L}$

$\Rightarrow |\frac{HL}{L}| = \frac{H}{H \cap L} = p^f$ $(f \geq 0)$.

If $f > 0$ then $|HL| > |L| = p^m$ and $\frac{|HL|}{|G|}$ this is not possible.

Therefore $f = 0 \Rightarrow HL = L \Rightarrow H \subset L \Rightarrow H = L$, since $|H|{=}|L| = p^m$.

Hence the claim

From the equations (8.2.12(b)) and (8.2.12(c)) we get

$$|C(K)| = \sum p^e \qquad (8.2.12(d))$$

From the equation (8.2.12(a)), we have that p does not divide $|C(K)|$. This implies that there should be atleast one term p^e is 1 in $\sum p^e$. This shows that $e = 0$ atleast once in the summation. By our claim above $H = L$, where $L \in C(K)$ i.e., L is conjugate of K and hence H is conjugate to K. Thus any two Sylow p-subgroups of G are conjugate. This proves the second Sylow theorem.

(ii) We have proved in (i) that any Sylow p-subgrop of G is conjugate to K. Therefore n_p, the number of Sylow p-subgroups of G is given by $|C(K)|$ and

$$n_p = |C(K)| = |G|/|N(K)| \qquad (8.2.12(e))$$

This shows that n_p divides $|G|$.

From the above claim, it is clear that there is only one term in $\sum p^e$ is 1. Therefore from the equations (8.2.12(d)) and (8.2.12(e)) we get

$$n_p = \sum_{e \geq 0} p^e = 1 + \sum_{e > 0} p^e = 1 + kp$$

$$\Rightarrow n_p \equiv 1 (mod\ p)$$

This proves the third Sylow theorem. Hence the theorem.

8.3 Applications of Sylow theorems

8.3.1 Corollary : A Sylow $p-$subgroup of a finite group is unique if and only if it is normal.

Proof. Let G be a finite group of order $p^m q$, where p is a prime number and $p \nmid q$. Let K be a Sylow $p-$subgroup of G then

K is unique $\Leftrightarrow n_p = 1$

$\Leftrightarrow |C(K)| = 1$

$\Leftrightarrow gKg^{-1} = K \quad \forall \quad g \in G$

$\Leftrightarrow K \rhd G$

Hence the result.

8.3.2 Example : If d is a divisor of n, the order of a finite abelian group A then A contains a subgroup of order d.

Solution. Given a finite abelian group A of order n and d/n .

Let $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, where p_i's are distinct primes and $e_i > 0$.

Then by Lemma (7.3.5) we get

$$A = S(p_1) \oplus S(p_2) \oplus \ldots \oplus S(p_k)$$

where $|S(p_i)| = p_i^{e_i},\ 1 \leq i \leq k$.

Let $d = p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}$, since $p_i^{f_i}$ divides $p_i^{e_i}$, then by first Sylow theorem $S(p_i)$ has a subgroup $S^{'}(p_i)$ of order $p_i^{f_i}, \quad 1 \leq i \leq k$

Now, it may be seen that $B = S^{'}(p_1) \oplus S^{'}(p_2) \oplus \ldots \oplus S^{'}(p_k)$ is a subgroup of A of order d.

8.3.3 Example : Prove that every group of order $2p$ must have a normal subgroup of order p, where p is prime number.

Solution. Let G be a group of order $2p$, where p is a prime. Since $p|_{|G|}$ then by first Sylow theorem G has subgroup H of order p. Since $[G : H] = 2$ then $H \triangleright G$. Thus G has a normal subgroup of order p.

8.3.4 Example : If a group G of order p^n (p is a prime) contains exactly one subgroup of orders $p, p^2, \ldots, p^{n-1}$ then G is cyclic group.

Solution. Given a group G and $|G| = p^n$, where p is a prime and n is positive integer. By first Sylow's theorem G has a subgroup H of order p^{n-1}.

Again by first Sylow theorem H has subgroups of orders $p, p^2, \ldots, p^{n-2}$. Since G has exactly one subgroup each of orders $p, p^2, \ldots, p^{n-1}$ then all proper subgroups of G are subgroups of H.

Let $a \in G$ and $a \notin H$. Suppose $O(a) < p^n$ then a generates a proper subgroup K of order less that p^n. Hence $K \subset H$ and there by $a \in H$ which is a contradiction. Therefore $O(a) = p^n$ and $G = [a]$. Hence the result.

8.3.5 Example : If H is normal subgroup of a finite group G and if the index of H in G is prime to p then H contains every Sylow p-subgroup of G.

Sol. Let $|G| = p^m q,\ (p, q) = 1$. Given $H \triangleright G$ and $([G : H], p) = 1$

$\Rightarrow \left(\frac{|G|}{|H|}, p\right) = 1 \Rightarrow |H| = p^m q_1,\ (p, q_1) = 1$

By first Sylow theorem H has a Sylow p-subgroup K, where $|K| = p^m$.

Now K is also a Sylow p-subgroup of G.

Let L be any Sylow p-subgroup of G then by second Sylow theorem L is conjugate to K.

Let $L = gKg^{-1}$ for some $g \in G$ then $L = gKg^{-1} \subset gHg^{-1} = H$ (since $H \triangleright G$).

Thus all Sylow p-subgroups of G are contained in H. Hence the result.

8.3.6 Example : Every group of order p^2q, where p, q are distinct primes, contains a normal Sylow p-subgroup and it is solvable.

Solution. Let G be a group and $|G| = p^2q$ where p, q, are distinct primes. By first Sylows theorem G has a Sylow p-subgroup and a Sylow q-subgroup.

Case (i) Let $p > q$. The number n_p of Sylow p-subgroup of G is given by $n_p = 1 + kp$, where k is a non negative integer and $(1 + kp)/q$.

Now $1 + kp = 1$ since $p > q \Rightarrow n_p = 1$. Therefore G has a unique Sylow p-subgroup H of G of order p^2. Hence $H \triangleright G$.

Case (ii) Let $p < q$. The number n_q of Sylow q-subgroups of G is given by $n_q = 1 + kq$ and $(1 + kq)/p^2$.

$$\Rightarrow 1 + kq = 1, \ p \ \text{ or } \ p^2.$$

If $1 + kq = 1$ then G has a unique Sylow q-subgroup L of order q and $L \triangleright G$.

Suppose $1 + kq \neq 1$ then $1 + kq \neq p$, since $q > p$.

Thus $1 + kq = p^2$ i.e., there are p^2 Sylow q-subgroups each of order q in G.

Hence G has $p^2(q-1)$ distinct non identity elements of order q and G has $p^2q - p^2(q-1) = p^2$ elements which are not of order q. These p^2 elements must be the elements of a Sylow p-subgroup of G. This shows that G ha a unique Sylow p-subgroup H of order p^2 and hence $H \triangleright G$

In any case G has either a normal Sylow p-subgroup H of order p^2 or a normal Sylow q-subgroup L of order q. This proves the first part.

If G has a subgroup H then $\{e\} \subset H \subset G$ is a normal series whose factors are H and $\frac{G}{H}$ which are abelian (since every group of order p^2 and p are abelian). Hence G is solvable.

If G has a subgroup L then $\{e\} \subset L \subset G$ is a normal series whose factors are abelian. Hence G is solvable in this case also. In any case G is solvable.

8.3.7 Example : Prove that there are only two non abelian groups of order 8.

Solution. Let G be a non abelian group and $|G| = 8$.

If G contains an element of order 8 then G is cyclic and abelian which is a contradiction.

If every element of G is of order 2 then G is abelian which is a contradiction.

Therefore G has an element a of order 4. Let $b \in G$ such that $b \notin [a]$ then $G = [a] \cup [a]b$.

If $b^2 \in [a]b$ then $b \in [a]$ which is a contradiction. Therefore $b^2 \in [a]$.

If $b^2 = a^2$ or a^3 then $O(b) = 8$ and G becomes abelian which is a contradiction. Thus $b^2 = e$ or a. Since $[a]$ is of index 2 in G, $[a] \triangleright G$. Hence $b^{-1}ab \in [a]$.

Since $O(b^{-1}ab) = O(a) = 4$, we have either $b^{-1}ab = a$ or a^3.

If $b^{-1}ab = a$ then $ab = ba$ and G is abelian which is contradiction. Thus $b^{-1}ab = a^3$

Thus we have two non abelian groups of order 8.

(i) $G_1 = [a, b]$ with defining relations $a^4 = e,\ b^2 = e,\ \ b^{-1}ab = a^3$.

(ii) $G_2 = [a, b]$ with defining relations $a^4 = e,\ b^2 = a^2,\ \ b^{-1}ab = a^3$.

The first is the octic group and the second is the quaternion group. It may be seen that the quaternion group contains only one element of order 2, where as the octic group has more than one element of order 2.

Therefore G_1 and G_2 are non isomorphic. Hence the result.

8.3.8 Note : (i) We have already seen that there are only three abelian groups of order 8. They are of types $(2, 2, 2)$, $(2, 4)$, (8).

The following are the non isomorphic abelian groups of order 8.

$$Z_2 \oplus Z_2 \oplus Z_2 \ , \quad Z_2 \oplus Z_4 \ , \quad Z_8$$

(ii) There are five groups of order 8 upto isomorphism. Three of them are abelian and the remaining two are non abelian (octic and quaternion)

8.3.9 Example : Prove that there are no simple groups of orders 63, 56 and 36.

Solution. Let G be a group of given order .

(i) Given $|G| = 63 = 3^2.7$

By first Sylow theorem G has a Sylow 3-subgroup of order 9 and a Sylow 7-subgroup of order 7. By third Sylow theorem n_p the number of Sylow p-subgroups of G divides $|G|$ and $n_p = 1 + kp$.

Therefore $n_7 = 1 + 7k$ and $(1 + 7k)/3^2.7$

$$\Rightarrow (1 + 7k)/3^2$$
$$\Rightarrow (1 + 7k)/9$$
$$\Rightarrow k = 0$$

Thus $n_7 = 1$ and hence G has unique Sylow 7-subgroup H and $H \rhd G$. Thus G is not simple, since it has a normal subgroup of order 7.

(ii) Given $|G| = 56 = 2^3.7$

By first Sylow theorem G has a Sylow 2-subgroup of order 8 and a Sylow 7-subgroup of order 7. By third Sylow theorem n_7 the number of Sylow 7-

subgroups of G divides $|G|$ and $n_7 = 1 + 7k$.

$\Rightarrow (1 + 7k)/8$

$\Rightarrow k = 0$ or $k = 1$

$\Rightarrow n_7 = 1$ or 8.

If $n_7 = 1$ then G has a normal subgroup of order 7 and G is not simple.

Suppose $n_7 = 8$ then G has eight Sylow 7-subgroups of order 7 and each Sylow 7-subgroup has $7 - 1 = 6$ elements of order 7. Therefore there are $8(7 - 1) = 8(6) = 48$ elements of order 7 and the remaining elements $56 - 48 = 8$ elements must form a unique Sylow 2-subgroup.

Since G has normal subgroup of order 8 then G is not simple in this case also. Hence the result.

(iii) Given $|G| = 36 = 2^2.3^2$

The number of Sylow 3-subgroups $n_3 = 1 + 3k$ divides $|G| = 2^2.3^2$.

Thus $(1 + 3k)/2^2 \Rightarrow k = 0$ or $1 \Rightarrow n_3 = 1$ or 4.

If $n_3 = 1$ then G has unique subgroup of order $3^2 = 9$. Therefore G has a normal subgroup of order $3^2 = 9$ and G is not simple.

If $n_3 = 4$ then G has four Sylow 3-subgroups of order 9 and each Sylow 3-subgroup has $3^2 - 1 = 8$ elements of order 3. Therefore there are $4(3^2 - 1) = 32$ elements of the Sylow 3-subgroups and the remaining $36 - 32 = 4$ elements must form a unique Sylow 2-subgroup of order 4. Thus G has a normal subgroup of order 4 and G is not simple in this case also. Hence the result.

Alternative Method : Given $|G| = 2^2.3^2$. By the first Sylow theorem G has a Sylow $3-$ subgroup H of order 9. Since $[G : H] = 4$ then there exist a homomorphism $\phi : G \to S_4$ with $ker\phi = \bigcap\limits_{x \in G} xHx^{-1}$.

If $ker\phi = \{e\}$ then ϕ is one-one and $G \subset S_4 \Rightarrow G$ is isomorphic to a subgroup of S_4. This is not possible, since $|G| = 36$ and $|S_4| = 24$.

Now $ker\phi = \bigcap_{x \in G} xHx^{-1} \neq G$ and $ker\phi \triangleright G$. Thus G has nontrivial normal subgroup and G is not simple. Hence the result.

8.3.10 Example : Prove that a group of order 108 has a normal subgroup of order 27 or 9. i.e., there is no simple group of order 108.

Solution. Let G be a group and $|G| = 108 = 2^3.3^3$.

The number of Sylow 3-subgroups is $n_3 = 1 + 3k$ and $(1 + 3k)/2^2.3^2$

$\Rightarrow (1 + 3k)/2^2$

$\Rightarrow k = 0$ or 1

If $k = 0$ then $n_3 = 1$ and hence G has a unique Sylow 3-subgroup of order 27 then by Example (13.2), we have H is normal in G. Thus G has normal subgroup of order 27.

Suppose $k = 1$ then $n_3 = 4$ and G has four Sylow 3-subgroups of order 27. Let H and K be any two distinct Sylow 3-subgroups of G, we have

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{27(27)}{|H \cap K|} \leq 108$$
$$\Rightarrow |H \cap K| \geq \frac{27}{4}$$

Further $|H \cap K|/27$. Since H and K are distinct we must have $|H \cap K| = 9$. Now $|H \cap K| \triangleright H$ and $|H \cap K| \triangleright K$ (since every subgroup of order p^{n-1} is normal in a group G of order p^n).

Consider $N(H \cap K)$. Now $H \subset N(H \cap K)$ and $K \subset N(H \cap K)$

Since $N(H \cap K)$ is the largest subgroup of G in which $H \cap K$ is normal.

Therefore $HK \subset N(H \cap K)$. Note that

$$|N(H \cap K)| \geq |HK| = \frac{|H||K|}{|H \cap K|} = \frac{27(27)}{9} = 81$$

Further by Lagrange's theorem we get $|N(H \cap K)|/|G|$

$\Rightarrow |N(H \cap K)| = 108 = |G|$ and $N(H \cap K) = G$. Hence $H \cap K \rhd G$.

Thus G has a normal subgroup of order 9 and G is not simple group.

8.4 Groups of order pq, where p, q are primes and $q > p$:

Let G be a finite group and $|G| = pq$, where p, q are prime numbers and $q > p$. By first Sylow theorem G has Sylow p-subgroup of order p and a Sylow q-subgroup of order q.

By third Sylow theorem n_q the number of Sylow q-subgroup of order q is given by $n_q = 1 + \lambda q$, where λ is a non-negative integer and $(1 + \lambda q)|p$. If $\lambda > 0$ then $1 + \lambda q > p$ (since $q > p$) and hence $(1 + \lambda q) \nmid p \Rightarrow \lambda = 0$ and $n_q = 1$. Therefore G has unique Sylow q-subgroup K of order q and $K \rhd G$. Since q is prime then K is cyclic.

Let $K = [b]$, where $b^q = 1 = e$. Further n_p the number of Sylow p-subgroups of order p is given by $n_p = 1 + \mu p$ and $(1 + \mu p)|q$. Since q is prime, we must have either $1 + \mu p = 1$ or $1 + \mu p = q \Rightarrow 1 + \mu p = 1$ or $q \equiv 1(mod\ p)$. Therefore we consider the following two cases:

case(i) suppose $1 + \mu p = 1$ then $n_p = 1$. Therefore G has a unique Sylow p-subgroup H of order p and $H \rhd G$. Since p is prime then H is cyclic group. Let $H = [a]$, where $a^p = e$. Clearly $H \cap K$ is trivial. Therefore $hk = kh\ \forall$ $h \in H,\ k \in K$. Now $ab \in G$ and $O(ab) = pq$. $\Rightarrow G = [ab]$ and G is cyclic.

case(ii) Suppose $q \equiv 1(mod\ p)$ then $n_p = 1 + \mu p = q$ and G has q Sylow p-subgroups of order p. Since p is prime then they are cyclic groups. Let

$H = [a]$ be one of the Sylow p-subgroups of G, where $a^p = e$ then $[a, b]$ is the group generated by a and b, contains both H and K. Hence both $|H|$ and $|K|$ divides $|[a, b]| \Rightarrow |[a, b]| = pq$ and $G = [a, b]$.

We have $K \rhd G$ then $a^{-1}ba = b^r$, for some integer r.

If $r \equiv 1(mod\ q)$ then $r = 1 + kq$ and $a^{-1}ba = b^r = b^{1+kq} = b \Rightarrow ab = ba \Rightarrow G$ is abelian. $\Rightarrow n_p = 1$ which is a contradiction. This shows that $r \not\equiv 1(mod\ q)$. Thus $G = [a, b]$ with the following relations:

$$a^p = 1 = b^q,\ a^{-1}ba = b^r,\ r \not\equiv 1(mod\ q) \qquad (8.4(a))$$

We have $a^{-1}ba = b^r \Rightarrow (a^{-1}ba)^2 = b^{2r} \Rightarrow a^{-1}b^2a = b^{2r}$. By induction we get $a^{-1}b^ra = b^{r^2}$. Further $a^{-1}ba = b^r \Rightarrow a^{-1}(a^{-1}ba)a = a^{-1}b^ra = b^{r^2} \Rightarrow a^{-2}ba^2 = b^{r^2}$. By induction we get $a^{-p}ba^p = b^{r^p} \Rightarrow b = b^{r^p}$ (since $a^p = 1$) $\Rightarrow r^p \equiv 1(mod\ q)$ (since $O(b) = q$)

The integer r in the equation (14.2(a)) is a solution of the congruence equation

$$Z^p \equiv 1(mod\ q) \qquad (8.4(b))$$

Conversely, if r is a solution of the equation (14.2(b)) then the defining relation equation (14.2(a)) determine a group consisting pq elements a^jb^j, $0 \leq i \leq p-1$, $0 \leq j \leq q-1$.

We have $r^p \equiv 1(mod\ q) \Rightarrow r^pr^p \equiv 1(mod\ q) \Rightarrow (r^2)^p \equiv 1(mod\ q)$. Therefore r^2 is a solution of equation (14.2(b)). By induction, it may be seen that r^j is a solution of equation (14.2(b)), $2 \leq j \leq p-1$ and they all give rise to the same group, because replacing a by a^j as a generator of H replaces r by r^j.

It may be seen that the condition in case(i) $1 + \mu p = 1$ is independent of p and q. Hence a cyclic group of order pq always exists. If $q > p$ and $q \equiv 1(mod\ p)$ then a non-abelian group $G = [a, b]$ also exists, besides the cyclic group of order pq with the following defining relations.

$$a^p = 1 = b^q,\ a^{-1}ba = b^r,\ r \not\equiv 1(mod\ q),\ r^p \equiv 1(mod\ q) \qquad (8.4(c))$$

From the above discussion we conclude the following:

There are atmost two groups G of order pq, where p, q are prime numbers and $q > p$.

(i) The cyclic groups G of order pq.

(ii) The non-abelian group $G = [a, b]$ with the defining relations given in the equation (8.4(c)), if $q \equiv 1(mod\ p)$.

8.4.1 Note : (i) If $q \not\equiv 1(mod\ p)$ then there exist only one cyclic group of order pq.

(ii) If $q \equiv 1(mod\ p)$ then there exist two non-isomorphic group of order pq.

8.4.2 Remark : If p, q are prime numbers and $q > p$ then every group G of order pq has a unique Sylow q-subgroup of order q and this subgroup is normal in G. Hence there is no group of order pq is simple (if $q > p$).

8.4.3 Example : (i) Every group order 15, 35 are cyclic.

(ii) There are no simple groups of order 15 and 35.

8.5 Groups of order p^2, where p is prime number.

We know that every group of order p^2 is abelian and there are only two abelian groups of order p^2. Therefore there are only two group of order p^2.

(i) The abelian group of type (p, p) and it is $\mathbf{Z}_p \oplus \mathbf{Z}_p$.

(ii) The abelian group of type (p^2) and it is $\mathbf{Z}_{p^2}$.

8.6 Summary

In this lesson we have defined of p-group, p-subgroup and sylow p-group. Also we have proved Cauchy's theorem for abelian group and first, second and third sylow theorems. Further we have proved the applications of sylow theorems and we have discussed the groups of order pq and groups of order p^2, where p, q are prime numbers.

8.7 Model Examination Questions

(1) Let G be a finite group and p is prime. If $p/|G|$ then G has an element of order p.

(2) Let G be a finite group and let p be a prime number. If $p^m/|G|$ then G has a subgroup of order p^m.

(3) Let G be a finite group and p is prime. If $p/|G|$ then G has an element of order p.

(4) A finite group G is a p-group if and only if its order is a power of p.

(5) Let G be a finite group and let p be a prime number then all Sylow p-subgroups of G are conjugate and their number n_p divides $O(G)$ and satisfies $n_p \equiv 1(mod\ p)$.

(6) Prove that a group of order 1986 is not simple.

(7) If the order of a group is 42. Prove that its Sylow 7-subgroup is normal.

(8) Let G be a group then prove that $|\frac{G}{Z(G)}| \neq 77$.

(9) Show that a group of order p^2q, where p and q are distinct primes, must contain a normal Sylow subgroup and be solvable.

8.8 Glossary

p-group, p-subgroup, sylow p-group, Cauchy's theorem and sylow theorem, Conjugate subgroups, sylow p-subgoup,unique normal subgroup, simple group, cyclic group.

UNIT-III

LESSON-9

IDEALS OF RINGS

9.1 Introduction : In this lesson, we study the ideals of rings, principal ideal ring and quotient ring.

9.2 Ideals of Rings

9.2.1 Definition : A non empty subset S of a ring R is called an ideal (two sided ideal) of R if (i) $a - b \in S \ \forall \ a, \ b \in S$.

(ii) $ar \in S$ and $ra \in S \ \forall \ r \in R, a \in S$.

9.2.2 Definition : A non empty subset S of a ring R is called a right (left) ideal if (i) $a - b \in S \ \forall \ a, \ b \in S$.

(ii) $ar \in S$ $(ra \in S)$ $\forall \ r \in R, a \in S$.

9.2.3 Property : Prove that every ideal of a ring R is a subring of R.

Proof. Let S be an ideal of R then $a - b \in S \ \forall a, \ b \in S$.

Also $a \in S, \ b \in S \Rightarrow a \in S$ and $b \in R \qquad (S \subset R)$

$\Rightarrow ab \in S \qquad$ (since $ar \in S$). Therefore S is a subring of R.

9.2.4 Note : Converse of the above property need not be true.

9.2.5 Example : Prove that $S = (Z, +, .)$ is a subring of $R = (Q, +, .)$, but not an ideal of $R = (Q, +, .)$.

Sol. S is a subring of R but S is not an ideal of R because $ar \notin S$ for $r \in R$, $a \in S$, since $r = \frac{1}{3}, a = 2 \Rightarrow ar = \frac{2}{3} \notin S$.

9.2.6 Note : (i) Every ideal is both right and left ideal.

(ii) In a commutative ring every right or left ideal is a two sided ideal.

(iii) Every ring R has at least two ideals $\{0\}$ and R itself then these two ideals are called trivial ideals of R. If R has any ideal other than these two then they are called proper ideals of R.

9.2.7 Example : Prove that every subring of the ring of integers $(Z, +, .)$ is an ideal of $(Z, +, .)$.

Sol. Let S be a subring of Z. For any $a,\ b \in S \Rightarrow a - b \in S$

Let $r \in Z$ and $a \in S$ then

$ra = a + a + \cdots + a$ (r times) if $r > 0$

$\quad = 0 \qquad\qquad\qquad$ if $r = 0$

$\quad = (-a) + (-a) \cdots + (-a)$ (r times) if $r < 0$

Since S is a subring we have for any $a \in S$

$a + a + \ldots + a$ (r times)$\in S$ (by closure of addition) and $0 \in S$,

$(-a) + (-a) + \ldots + (-a) \in S \Rightarrow ra \in S \ \ \forall\, r \in Z,\ \ a \in S$

Similarly $ar \in S \ \ \forall \ \ r \in Z,\ \ a \in S$. Therefore S is an ideal of Z.

9.2.8 Example : Prove that the right as well as left ideals of a division ring are trivial ideals only.

Proof. Let D be a division ring. Let I be any ideal of D.

If $I = \{0\}$ then there is nothing to prove.

Let $I \neq 0$. Let a be any nonzero element of $I \Rightarrow a \in D \Rightarrow a^{-1} \in D$

We have $a \in I$, $a^{-1} \in D \Rightarrow aa^{-1} \in I \qquad$ (I is an ideal)

$\qquad\qquad\qquad\qquad\qquad \Rightarrow 1 \in I.$

For any $r \in D$ we have $1r \in I \Rightarrow r \in I$

Therefore $D \subset I$, but we have $I \subset D$. Hence $I = D$

$\therefore D$ has only trivial ideals.

9.2.9 Example : Let R be a ring and $a \in R$ then $aR = \{ax : x \in R\}$ is a right ideal of R and $Ra = \{xa : x \in R\}$ is left ideal of R.

Sol. (i) $aR = \{ax : x \in R\}$

$0 \in R \Rightarrow a0 = 0 \in aR$. $\therefore aR$ is a nonempty subset of R

Let ax_1, ax_2 be any two elements of R, where $x_1, x_2 \in R$

$\Rightarrow ax_1 - ax_2 = a(x_1 - x_2) \in aR \qquad (x_1 - x_2 \in R)$

Let $r \in R$ and $ax_1 \in aR$ then $(ax_1)r = a(x_1 r) \in aR \qquad (x_1 r \in R)$

$\therefore aR$ is a right ideal of R. Similarly Ra is a right ideal of R.

9.2.10 Note : (i) If R is commutative then aR is an ideal of R.

(ii) If R has unity then $a = a1 \in aR$

(iii) aR is the smallest ideal of R containing a.

Suppose $a_1 R$ is another ideal of R containing a. Let ar be any element of aR we have $a \in a_1 R$ and $r \in R \Rightarrow ar \in a_1 R \quad (a_1 R$ is an ideal)

$\Rightarrow aR \subset a_1 R$. $\therefore aR$ is the smallest ideal of R containing a.

9.3 Rings of Matrices

9.3.1 Rings of Matrices : Let R be a ring and R_n be the set of all $n \times n$ matrices whose elements are from R then R_n forms a ring with respect matrix addition and matrix multiplication.

In general if $A, B \in R_n$ where $n > 1$ then $AB \neq BA$

$\therefore$ For $n > 1$, R_n is a non commutative ring. Also R_n is not an integral domain because R_n has nonzero divisors, $A \neq 0, B \neq 0 \Rightarrow AB = 0$

Suppose R has unity we denote by e_{ij} the matrices in R_n whose (i, j) entry is 1 and whose other entries are zeroes.

i.e. In R_3 consider $e_{11} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $e_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ etc.

The ${e_{ij}}'s$, $1 \leq i, j \leq n$ are called matrix units.

From the definition of multiplication of matrices, it follows that

$e_{ij}e_{kl} = 0$ if $j \neq k$

$\quad = e_{il}$ if $j = k$ $\qquad$ i.e. $e_{ij}e_{kl} = \delta_{jk}e_{il}$

where $\delta_{jk} = 0$ if $j \neq k$

$\quad = 1$ if $j = k$, is called the Kronecker delta.

In R_3, consider $e_{11} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $e_{23} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$, $e_{13} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

then

$$e_{11}e_{23} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$e_{11}e_{13} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = e_{13}$$

Also if $A = (a_{ij}) \in R_n$ then A can be uniquely expressed as a linear combination of $e_{ij}{}'s$ over R i.e., $A = \sum\limits_{1 \leq i,j \leq n} a_{ij}e_{ij}, \quad a_{ij} \in R$.

For example $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ then

$$A = \sum_{1 \leq i,j \leq 3} a_{ij}e_{ij}$$

$$= a_{11}e_{11}+a_{12}e_{12}+a_{13}e_{13}+a_{21}e_{21}+a_{22}e_{22}+a_{23}e_{23}+a_{31}e_{31}+a_{32}e_{32}+a_{33}e_{33}$$

$$= \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & a_{12} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & a_{33} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Let S be the set of $n \times n$ matrices in which all the entries below diagonal are zero

i.e., Let S consist of matrices $\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ . & . & . & . \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}, \quad a_{ij} \in R.$

then S is a ring with the usual addition and multiplication of matrices and is called the ring of upper triangular matrices. Similarly we have the ring of lower triangular matrices.

9.3.2 Example : Let R be the $n \times n$ matrix ring over a field F, for any $1 \leq i \leq n$. Let A_i(or B_i) be the set of matrices in R having all rows(columns) except possibly the i^{th} row(column) zero then A_i is a right ideal and B_i is a left ideal in R.

Sol. $A_i = \left\{ \begin{pmatrix} 0 & 0 & \dots & 0 \\ . & . & . & . \\ a_{i1} & a_{i2} & \dots & a_{in} \\ . & . & . & . \\ 0 & 0 & \dots & 0 \end{pmatrix} \middle| a_{ij} \in F \right\}$

$$\text{Let } A = \begin{pmatrix} 0 & 0 & \dots & 0 \\ . & . & . & . \\ a_{i1} & a_{i2} & \dots & a_{in} \\ . & . & . & . \\ 0 & 0 & \dots & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & \dots & 0 \\ . & . & . & . \\ b_{i1} & b_{i2} & \dots & b_{in} \\ . & . & . & . \\ 0 & 0 & \dots & 0 \end{pmatrix} \text{ be any}$$

two elements of A_i, $a_{ij}, b_{ij} \in F$

$$A - B = \begin{pmatrix} 0 & 0 & \dots & 0 \\ . & . & . & . \\ a_{i1} - b_{i1} & a_{i2} - b_{i2} & \dots & a_{in} - b_{in} \\ . & . & . & . \\ 0 & 0 & \dots & 0 \end{pmatrix}, \quad \text{where } a_{ij} - b_{ij} \in F$$

$\Rightarrow A - B \in A_i$

$$\text{Let } r = \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ . & . & . & . \\ r_{i1} & r_{i2} & \dots & r_{in} \\ . & . & . & . \\ r_{n1} & r_{n2} & \dots & r_{nn} \end{pmatrix} \in R \quad \text{then}$$

$$Ar = \begin{pmatrix} 0 & 0 & \dots & 0 \\ . & . & . & . \\ a_{i1} & a_{i2} & \dots & a_{in} \\ . & . & . & . \\ 0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ . & . & . & . \\ r_{i1} & r_{i2} & \dots & r_{in} \\ . & . & . & . \\ r_{n1} & r_{n2} & \dots & r_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & \dots & 0 \\ . & . & . & . \\ a_{i1}r_{11} + a_{i2}r_{21} + \dots + a_{in}r_{n1} & a_{i1}r_{12} + a_{i2}r_{22} + \dots + a_{in}r_{n2} & \dots & a_{i1}r_{1n} + a_{i2}r_{2n} + \dots \\ & & & +a_{in}r_{nn} \\ . & . & . & . \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$\Rightarrow Ar \in A_i$, where each element of i^{th} row in F.

$\therefore A_i$ is the right ideal of R. Similarly B_i is the left ideal of R.

9.3.3 Example : Let R be the ring of 2×2 upper triangular matrices over a field F then the subset $I = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \middle| a \in F \right\}$ is an ideal of R.

Sol. Let $A,\ B \in I \Rightarrow A = \begin{pmatrix} 0 & a_1 \\ 0 & 0 \end{pmatrix},\ \ B = \begin{pmatrix} 0 & a_2 \\ 0 & 0 \end{pmatrix}$, $a_1, a_2 \in F$

$$A - B = \begin{pmatrix} 0 & a_1 - a_2 \\ 0 & 0 \end{pmatrix} \in I, \quad a_1 - a_2 \in F$$

$$Ar = \begin{pmatrix} 0 & a_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} r_1 & r_2 \\ 0 & r_3 \end{pmatrix} \quad \text{where } r = \begin{pmatrix} r_1 & r_2 \\ 0 & r_3 \end{pmatrix} \in R$$

$$= \begin{pmatrix} 0 & a_1 r_3 \\ 0 & 0 \end{pmatrix} \in I$$

$$rA = \begin{pmatrix} r_1 & r_2 \\ 0 & r_3 \end{pmatrix} \begin{pmatrix} 0 & a_1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & r_1 a_1 \\ 0 & 0 \end{pmatrix} \in I.$$

Hence I is an ideal of R.

9.3.4 Example : Let R be the ring of all functions from the closed interval $[0, 1]$ to the field of real numbers. Let $c \in [0, 1]$ and $I = \{f \in R | f(c) = 0\}$

then I is an ideal of R.

Sol. Let $f, g \in I \Rightarrow f(c) = 0,\ g(c) = 0$

$(f - g)c = f(c) - g(c) = 0 - 0 = 0$

$\therefore f - g \in I \ \forall \ f, g \in I$

Let $f \in I$ and $r \in R$

Consider $(rf)(c) = r(c)f(c)$

$$= r(c).0$$

$$= 0$$

$$\Rightarrow rf \in I$$

Similarly $fr \in I \ \forall \ f \in I,\ r \in R$.

Hence I is an ideal of R.

9.3.5 Example : Let $R = F_2$ be the 2×2 matrix ring over a field F. Let $S = \begin{pmatrix} F & F \\ 0 & F \end{pmatrix}$ be the set of all upper triangular matrices over F then S is a sub ring of R. If $I = \begin{pmatrix} 0 & F \\ 0 & 0 \end{pmatrix}$ then I is an ideal of S but I is neither right nor a left ideal of R.

Sol. Let $S = \left\{ \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} \middle| a_1, a_2, a_3 \in F \right\}$ be sub ring of R.

$$I = \left\{ \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \middle| a \in F \right\}$$

(i) Let $A = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in I, \quad a, b \in F$

$$A - B = \begin{pmatrix} 0 & a - b \\ 0 & 0 \end{pmatrix} \in I, \quad a - b \in F$$

$$r \in S \Rightarrow r = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}$$

$$Ar = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} = \begin{pmatrix} 0 & aa_3 \\ 0 & 0 \end{pmatrix} \in I$$

$$rA = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & aa_3 \\ 0 & 0 \end{pmatrix} \in I$$

$\therefore I$ is an ideal of S.

(ii) To prove that I is neither right nor left ideal of R.

Let $r \in R \Rightarrow r = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \quad a_i \in F$

Let $A \in I \Rightarrow A = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \quad a \in F$

$$Ar = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} aa_3 & aa_4 \\ 0 & 0 \end{pmatrix} \notin I$$

$$rA = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} 0 & a \\ o & o \end{pmatrix} = \begin{pmatrix} 0 & a_1 a \\ 0 & a_3 a \end{pmatrix} \notin I$$

$\therefore I$ is neither right nor left ideal of R.

9.3.6 Example : If A is an ideal in the ring R then the ring A_n of all $n \times n$ matrices with entries from A is an ideal of R_n.

Sol. Given A is an ideal in R.

Let $B_1 = (b_{ij})$ and $C_1 = (c_{ij})$ be the elements of A_n where $b_{ij}, c_{ij} \in A$ for

$B_1 - C_1 = (b_{ij} - c_{ij})$ where $b_{ij} - c_{ij} \in A$, $1 \leq i, j \leq n$

$\Rightarrow B_1 - C_1 \in A_n$

Let $r = (r_{ij}), \quad r_{ij} \in R$

$$B_1 r = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ . & . & . & . \\ . & . & . & . \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix} \begin{pmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ . & . & . & . \\ . & . & . & . \\ r_{n1} & r_{n2} & \dots & r_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} b_{11}r_{11} + b_{12}r_{21} + \ldots + a_{1n}r_{n1} & b_{11}r_{12} + b_{12}r_{22} + \ldots + b_{1n}r_{n2} & \dots & \begin{matrix} b_{11}r_{1n} + b_{12}r_{2n} + \ldots \\ +b_{1n}r_{nn} \end{matrix} \\ . & . & . & . \\ . & . & . & . \\ b_{n1}r_{11} + b_{n2}r_{21} + \ldots + b_{nn}r_{n1} & b_{n1}r_{12} + b_{n2}r_{22} + \ldots + b_{nn}r_{n2} & \dots & \begin{matrix} b_{n1}r_{1n} + \ldots \\ +b_{nn}r_{nn} \end{matrix} \end{pmatrix}$$

where all the entries belongs to A. $\Rightarrow B_1 r \in A_n$.

Similarly $rB_1 \in A_n$, Therefore A_n is an ideal of R_n.

9.3.7 Theorem : If a ring R has unity then every ideal I in the matrix ring R_n is of the form A_n, where A is an ideal of R.

Proof. Let (e_{ij}), $i, j = 1, 2, \ldots, n$ denote the matrix units in R_n.

Let $A = \{a_{11} \in R \big| \ \sum a_{ij}e_{ij} \in I\}$ then we claim that A is an ideal of R.

Let $a_{11}, b_{11} \in A$ then there exists matrices

$\alpha = \sum a_{ij}e_{ij}$ and $\beta = \sum b_{ij}e_{ij}$ in I then

$\alpha - \beta = \sum(a_{ij} - b_{ij})e_{ij} \in I \qquad (\because I \text{ is an ideal})$

$\qquad \Rightarrow a_{11} - b_{11} \in A$

Let $r \in R$ and $a_{11} \in A$ with $\sum a_{ij}e_{ij} \in I$

Consider $(\sum a_{ij}e_{ij})(re_{11})$

$\qquad = (a_{11}e_{11} + a_{12}e_{12} + \ldots)(re_{11})$

$\qquad = a_{11}e_{11}re_{11} + a_{12}e_{12}re_{11} + \ldots$

$= \sum (a_{ij}e_{ij})re_{11}$

$= \sum a_{i1}re_{i1} \in I \quad (e_{ij}e_{kr} = e_{ir} \text{ if } j = k) \text{ i.e., } e_{ij}e_{11} = e_{i1} \text{ if } j = 1)$

$\Rightarrow a_{11}r \in A$

Similarly $ra_{11} \in A \quad \forall\, r \in R, \quad a_{11} \in A$

$\therefore A$ is an ideal of R.

Now to show that $I = A_n$. Let $x = \sum a_{ij}e_{ij} \in I$

Let r and s be some fixed integers between 1 and n

Consider $e_{1r}(\sum a_{ij}e_{ij})e_{s1}$

$=e_{1r}(\sum a_{is}e_{i1}) \quad (e_{ij}e_{s1} = e_{i1} \text{ if } j = s \text{ and } e_{1r}e_{i1} = e_{11} \text{ if } r = i)$

$=\sum e_{1r}(a_{is}e_{i1})$

$=\sum a_{rs}e_{11} \in I$

$\Rightarrow a_{rs} \in A$ for any r and s

$\Rightarrow a_{ij} \in A$ for any i and j

$\Rightarrow$ all the entries in the matrix $x = \sum a_{ij}e_{ij}$ are in A

$\Rightarrow x \in A_n$

$\therefore I \subset A_n \quad$ (15.3.7(a))

Conversely let $x = \sum a_{ij}e_{ij} \in A_n$.

For $a_{ij} \in A$ there exists a matrix $\sum b_{rs}e_{rs} \in I$ such that $b_{11} = a_{ij}$

then $e_{i1}(\sum b_{rs}e_{rs})e_{1j}$

$= e_{i1}(\sum b_{rs}e_{rs}e_{1j})$

$= e_{i1}(\sum b_{r1}e_{rj}) \quad (e_{rs}e_{1j} = e_{rj} \text{ if } s = 1)$

$= \sum e_{i1}(b_{r1}e_{rj})$

$= b_{11}e_{ij} \in I \quad (e_{i1}e_{rj} = e_{ij} \text{ if } 1 = r)$

$= a_{ij}e_{ij} \in I$ for each $\quad 1 \leq i, j \leq n$

$\Rightarrow \sum a_{ij}e_{ij} \in I \quad (\because I \text{ is an ideal})$

$\Rightarrow x \in I$

$\therefore A_n \subset I$ (15.3.7(b))

On using (9.3.7(a)) and (15.3.7(b)) we get $A_n = I$

9.3.8 Corollary : If D is a division ring then $R = D_n$ has non trivial ideals.

Proof. Let I be any ideal in D_n

If $I = \{0\}$ there is nothing to prove

Let I be any non zero ideal in D_n then $I = A_n$, where A is some ideal in D.

But D is a division ring

$\Rightarrow D$ has only trivial ideals

$\Rightarrow A = D$

$\Rightarrow A_n = D_n$

$\Rightarrow I = D_n$

$\therefore D_n$ has only trivial ideals.

9.3.9 Note : (i) D has only $\{0\}$ and D are right as well as left ideals. But we have seen in the Example (15.3.2) for $n > 1$. D_n has nontrivial right as well as left ideals. But from the theorem (15.3.7) since $\{0\}$ and D are the only right or left ideals.

$\therefore D_n$ cannot have non ideal right (or) left ideals which is not true.

$\therefore$ In general the theorem (15.18) is not true if the word ideal is replaced by right or left ideals.

(ii) If R is a ring without unity then theorem (15.3.7) is not necessarily true. i.e. R is a ring with unity is also must in the theorem (15.3.7).

9.3.10 Example : Let $(R, +)$ be an additive group of order p, where p is prime number. Define multiplication in R by $ab = 0 \;\; \forall \;\; a, \; b \in R$. Then R has no unity.

If $1 \in R$ then $1.a = a.1 = a$

But by the definition of multiplication $1.a = 0$

$\therefore R$ has no unity.

If X is any additive subgroup of $(R, +)$ then X is an ideal of R.

because if $x \in X$ and $r \in R$, we have

$xr = 0 = rx \in X \qquad (0 \in X)$

$\therefore X$ is an ideal of R.

$\therefore$ Any subset X of R is an ideal of R iff X is a subgroup of R under addition.

But R is of order p then the only subgroups of R are $\{0\}$ and R itself.

$\therefore$ The only ideals of R are $\{0\}$ and R itself. Then by the theorem (15.3.7)

The only ideals of R_2 are $(0)_{2\times 2}$ and R_2 only $\qquad$ (15.3.10(a))

Now consider $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in R \right\}$ then I is an ideal of R_2

Also $I \neq \{0\}$ and $I \subset R_2$ which is a contradiction to (15.3.10(a))

Therefore, in general the theorem is not true for rings which is not unity.

9.3.11 Theorem: Let $(A_i)_{i\in\wedge}$ be a family of right (left) ideals in a ring R.

Then $\bigcap\limits_{i\in\wedge} A_i$ is also a right(left) ideal.

Proof. Let $a, b \in \bigcap\limits_{i\in\wedge} A_i \Rightarrow a \in A_i, b \in A_i$ for each i

$\Rightarrow a - b \in A_i$ for each $i \Rightarrow a - b \in \bigcap\limits_{i\in\wedge} A_i$

Let $r \in R$ and $a \in \bigcap\limits_{i\in\wedge} A_i \Rightarrow r \in R$ and $a \in A_i$ for each i

$\Rightarrow ra \in A_i$ for each $i \quad$ (A_i is an left ideal)

Similarly $ar \in A_i$ for each $i \quad$ (A_i is an right ideal)

$\therefore ra \in \bigcap\limits_{i\in\wedge} A_i \Rightarrow \bigcap\limits_{i\in\wedge} A_i$ is a left ideal.

$ar \in \bigcap\limits_{i\in\wedge} A_i \Rightarrow \bigcap\limits_{i\in\wedge} A_i$ is a right ideal.

9.3.12 Definition : Let S be a subset of R. Let $\mathcal{A} = \{A \mid A$ is a right ideal of R containing $S\}$

then $\mathcal{A}$ is non empty, since $R \in \mathcal{A}$

Let $I = \bigcap\limits_{A \in \mathcal{A}} A$. Since $S \subset A$ for each $A \in \mathcal{A}$

$\Rightarrow I$ is the smallest ideal containing S

$\Rightarrow I$ is an ideal generated by S.

If $\mathcal{A}$ contains all right ideals A, where $S \subset A$ for each $A \in \mathcal{A}$ then I is called the smallest right ideal of R containing S and is denoted by $(S)_r$. The smallest right ideal of R containing a subset S is called a right ideal generated by S.

Similarly if $\mathcal{A}$ contains all left ideals A, where $S \subset A$ for each $A \in \mathcal{A}$ then I is called the smallest left ideal of R containing S and is denoted by $(S)_l$. The smallest left ideal of R containing a subset S is called a left ideal generated by S.

If $S = \{a_1, a_2, \ldots, a_m\}$ is a finite set then $(S)_r$ is also written as $(a_1, a_2, \ldots, a_m)_r$. Similarly $(S)_l$ is also written as $(a_1, a_2, \ldots, a_m)_l$. S is also written as $(a_1, a_2, \ldots, a_m)$.

9.4 Principal Ideal :

9.4.1 Definition: A right ideal I of a ring R is called finitely generated if $I = (a_1, a_2, \ldots, a_m)_r$ for some $a_i \in R$, $1 \leq i \leq m$.

9.4.2 Definition : A right ideal I of a ring R is called principal right ideal if $I = (a)_r$ for some $a \in R$ (i.e., generated by single element).

9.4.3 Note : In a similar manner we define a finitely generated left ideal, a finitely generated ideal, a principal left ideal and a principal ideal.

9.4.4 Definition : A ring in which each ideal is principal is called a principal ideal ring (PIR). If R is an integral domain with unity which is a PIR then it is called principal ideal domain.

9.4.5 Example : All the ideals in the ring of integers Z are principal ideals.

Sol. Let I be any non zero ideal in Z

Let n be the smallest positive integer in I then for any $m \in I$ we write $m = nq + r$ where $0 \leq r < n$ (by division of algorithm)

$\Rightarrow r = m - nq \in I$ ($m \in I$, I is an ideal,$\Rightarrow nq \in I$ for any $q \in Z$)

$\Rightarrow r \in I$ where $0 \leq r < n$

$\Rightarrow r = 0$ (by choice of n i.e. n is the smallest positive integer in I)

$\Rightarrow m = nq$

$\Rightarrow I = (n)$

9.4.6 Note : Let I be an ideal in R for $a, b \in R$ we define $a \equiv b(mod\ I)$ if $a - b \in I$ then this congruence is an equivalence relation in R. Every equivalence relation give rise to equivalence classes.

Let R/I denote the set of equivalence class and $\bar{a} \in R/I$ be the equivalence class containing a.

Consider $\bar{a} \in R/I$

Let $b \in \bar{a} \Rightarrow b \equiv a(mod\ I)$

$\Rightarrow b - a \in I$

$\Rightarrow b - a = x$, for some $x \in I$

$\Rightarrow b = a + x$, for some $x \in I$

$\Rightarrow$ every element of $\bar{a}$ is of the form $a + x$, for some $x \in I$

$\Rightarrow \bar{a} = a + I$

We shall define addition and multiplication in R/I

$\bar{a} + \bar{b} = \overline{a + b}\ \forall\ \bar{a},\ \bar{b} \in R/I$ and

$\bar{a}.\bar{b} = \overline{ab}\ \ \forall\ \bar{a},\ \bar{b} \in R/I$

To show that these binary operations are well defined.

Let $\bar{a} = \bar{c}$, $\bar{b} = \bar{d}$ then $a - c \in I$, $b - d \in I$

$$(a-c)+(b-d) \in I \Rightarrow (a+b)-(c+d) \in I$$

$$\Rightarrow \overline{a+b} = \overline{c+d}$$

$$\Rightarrow \bar{a}+\bar{b} = \bar{c}+\bar{d}$$

$ab-cd = a(b-d)+(a-c)d$ $\qquad$ ($a-c, b-d \in I$ which is an ideal)

$$\Rightarrow ab-cd \in I$$

$$\Rightarrow \overline{ab} = \overline{cd}$$

$$\Rightarrow \bar{a}\bar{b} = \bar{c}.\bar{d}$$

(i) Let $\bar{a}, \bar{b}, \bar{c} \in R/I$ then

$$\bar{a}+(\bar{b}+\bar{c}) = \bar{a}+(\overline{b+c}) = \overline{a+(b+c)}$$

$$= \overline{(a+b)+c}$$

$$= (\overline{a+b})+\bar{c} \qquad (a, b, c \in R)$$

$$= (\bar{a}+\bar{b})+\bar{c}$$

(ii) $\bar{0}$ is the additive identity in R/I

(iii) For every $\bar{a} \in R/I$ we have

$$\bar{a}+(-\bar{a}) = \overline{a+(-a)} = \bar{0}$$

$$(-\bar{a})+\bar{a} = 0$$

(iv) $\bar{a}+\bar{b} = \overline{a+b} = \overline{b+a}$

$$= \bar{b}+\bar{a} \qquad \forall\ \bar{a}, \bar{b} \in R/I$$

(v) $\bar{a}(\bar{b}.\bar{c}) = \bar{a}(\overline{bc}) = \overline{a(bc)}$

$$= \overline{(ab)c} = (\overline{ab})\bar{c}$$

$$= (\bar{a}.\bar{b})\bar{c}$$

(vi) $\bar{a}.(\bar{b}+\bar{c}) = \bar{a}.\bar{b}+\bar{a}.\bar{c}$ and

$$(\bar{b}+\bar{c}).\bar{a} = \bar{b}.\bar{a}+\bar{c}.\bar{a}$$

Then $(R/I, +, .)$ is a ring called quotient ring modulo I.

9.4.7 Definition : Let I be an ideal of a ring R then the ring $(R/I, +, .)$

is called the quotient ring modulo I.

If $I = R$ then R/I is the zero ring.

If $I = (0)$ then R/I is the same as the ring R which we identify $a + (0)$ with $a \in R$

9.4.8 Note : If S is any subset of R then the ideal generated by S is the smallest ideal containing S.

We shall show that

$$(a) = \left\{ \sum_{i(finitesum)} r_i a s_i + ra + as + na \ / \ r, s, r_i, s_i \in R, n \in Z \right\}$$

$$(a)_r = \left\{ ar + na \ / \ r \in R, n \in Z \right\}$$

$$(a)_l = \left\{ ra + na \ / \ r \in R, n \in Z \right\}$$

If $1 \in R$ the they will become

$$(a) = \left\{ \sum_{i(finitesum)} r_i a s_i / r_i, s_i \in R \right\}$$

$(a)_r = \left\{ ar \ / \ r \in R \right\}$ and $(a)_l = \left\{ ra \ / \ r \in R \right\}$

In this case the symbols RaR, aR and Ra are used for $(a), (a)_r$ and $(a)_l$ respectively.

Let $S = \left\{ \sum_{i(finitesum)} r_i a s_i + ra + as + na \ / \ r, s, r_i, s_i \in R, n \in Z \right\}$

We shall show that $a \in S$ and S is the smallest ideal containing a.

Taking $r_i = s_i = r = s = 0$ and $n = 1$ we get $a \in S$

We shall show that S is an ideal.

Consider $\sum r_i a s_i + ra + as + na$ and $\sum {r_i}' a {s_i}' + r' a + as' + n' a$ be any two elements of S then

$$\left(\sum_{finitesum} r_i a s_i + ra + as + na \right) - \left(\sum_{finitesum} {r_i}' a {s_i}' + r' a + as' + n' a \right)$$

$$= \left(\sum_{finitesum} r_i a s_i - \sum_{finitesum} {r_i}' a {s_i}' \right) + (r - r')a + (s - s')a + (n - n')a \in S$$

where $r-r^{'} \in R, s-s^{'} \in R, n-n^{'} \in Z$

$\Rightarrow S$ is a subgroup of R under addition.

Let $r^{'} \in R$ and $\sum\limits_{finitesum} r_i as_i + ra + as + na) \in S$

Consider $r^{'}[\sum\limits_{finitesum} r_i as_i + ra + as + na)]$

$$= \sum_{i(finitesum)} r^{'} r_i as_i + r^{'} ra + r^{'} as + r^{'} na)$$

$$= \sum_{j(finitesum)} r_j as_i + r_l a + r^{'} as + r^{'} (a + a + \ldots + n \ \text{ times})$$

where $r_j = r^{'} r_i$ and $r_l = r^{'} r$

$$= [\sum_{j(finitesum)} r_j as_i + r^{'} as] + (r_1 + r^{'})a + (r^{'} a + r^{'} a + \ldots + r^{'} a) \ (n-1 \text{ times})$$

$$= [(\sum_{j(finitesum)} r_j as_i + r^{'} as) + r_l a + 0s + 0a] + (0 + r^{'} a + 0s + 0a) + \ldots + (0 + r^{'} a + 0s + 0a) + \ldots \quad (n-1) \text{ times}$$

$$\in S \qquad (\because S \text{ is closed under addition})$$

Similarly $[\sum r_i as_i + ra + as + na]r^{'} \in S$

$\therefore S$ is an ideal.

Suppose $S^{'}$ is another ideal of R containing a i.e. $a \in S^{'}$

then $ra \in S^{'} \ \forall \ r \in R$, and $as \in S^{'} \ \forall \ s \in R$, $na \in S^{'} \ \forall \ n \in Z$ and $\sum r_i as_i \in S^{'}$ for $r_i s_i \in R$

$\Rightarrow \sum r_i as_i + ra + as + na \in S^{'}$

$\Rightarrow S \subset S^{'}$

$\Rightarrow S = (a)$

9.4.9 Example : Let I be a right (left) ideal of R and it contains a unit of R then $I = R$

Sol. Let I be a right ideal of $R \Rightarrow I \subset R$

Let u be any unit in $I \Rightarrow u^{-1}$ exists and $u^{-1} \in R$

$\Rightarrow uu^{-1} = 1 \in I$ $\quad$ ($\because I$ is right ideal)

$\therefore 1 \in I$ then $I = R$

9.4.10 Example : Let $(n) = \{na|a \in Z\}$ be an ideal in Z. If $n \neq 0$ then the quotient ring $Z/(n)$ is Z_n

Sol. Consider $Z/(n) = \{a + (n) \big| \; a \in z\}$

$$= \big\{0 + (n), 1 + (n), \ldots, (n-1) + (n)\big\}$$
$$= \big\{\bar{0}, \bar{1}, \ldots\ldots, \overline{n-1}\big\}$$
$$= Z_n$$

9.4.11 Example : Let R be a ring with unity and let $R[x]$ be the polynomial ring over R. Let $I = (x)$ be the ideal in $R[x]$ consisting of the multiples of x then the quotient ring $R[x]/I = \{\bar{a} \mid a \in R\}$

Sol. Let $I = (x)$ then $x \in I \Rightarrow \bar{x} = x + I = I$

$\Rightarrow \bar{x} = \bar{0}$

Consider any element $\overline{a + bx + cx^2 + \ldots\ldots} \in R[x]/I$ then

$$\overline{a + bx + cx^2 + \ldots\ldots} = \bar{a} + \bar{b}\bar{x} + \bar{c}\overline{x^2} + \ldots\ldots$$
$$= \bar{a} \qquad (\bar{x} = \bar{0})$$

$\therefore R[x]/I = \{\bar{a} \mid a \in R\}$

9.4.12 Example : Find the quotient ring $R[x]/(x^2 + 1)$

Sol. $x^2 + 1 \in (x^2 + 1)$

$\Rightarrow \overline{x^2 + 1} = \bar{0}$

$\Rightarrow \overline{x^2} + \bar{1} = \bar{0}$

$\Rightarrow \overline{x^2} = \bar{0} - \bar{1}$

$= -\bar{1}$

$\overline{x^3} = \overline{x^2 x} = \overline{x^2}.\bar{x} = -\bar{x}$ and $\overline{x^4} = \overline{x^2 x^2} = \overline{x^2}.\overline{x^2} = (-\bar{1}).(-\bar{1}) = \bar{1}$

Also $\overline{x^5} = \overline{x^2x^3} = (-\bar{1})(-\overline{x}) = \bar{x}$

In general $\overline{x^n} = \pm\ \bar{1}$ if n is even

$= \pm\ \bar{x}$ if n is odd.

Let $\overline{a + bx + cx^2 + \ldots\ldots}$ be any element of $R[x]/(x^2+1)$ then

$$\begin{aligned}
\overline{a + bx + cx^2 + \ldots\ldots} &= \bar{a} + \overline{bx} + \overline{cx^2} + \ldots\ldots \\
&= \bar{a} + \bar{b}\bar{x} + \bar{c}\overline{x^2} + \ldots\ldots \\
&= \bar{a} + \bar{b}\bar{x} + \bar{c}(-\bar{1}) + d(-\overline{x}) + e(1) + \ldots\ldots \\
&= (\bar{a} - \bar{c} + \bar{e}) + (\bar{b} - \bar{d} + \bar{f})\bar{x} \\
&= \bar{\alpha} + \bar{\beta}\bar{x} \qquad \text{where } \alpha = a - c + e \ldots\ldots \in R \\
&\qquad\qquad\qquad \beta = b - d + f \ldots\ldots \in R
\end{aligned}$$

$\therefore R[x]/(x^2+1) = \left\{\bar{\alpha} + \bar{\beta}x \ /\alpha, \beta \in R\right\}$ where $\overline{x^2} = -\bar{1}$

9.4.13 Note : $R[x]/(x^2+1)$ is the field of complex numbers where $\bar{\alpha}, \alpha \in R$ is identified with α and $\bar{x}$ is identified with $\sqrt{-1}$.

9.4.14 Example : Let $R = \begin{pmatrix} Z & Q \\ 0 & 0 \end{pmatrix}$ and let $A = \begin{pmatrix} 0 & Q \\ 0 & 0 \end{pmatrix}$ be an ideal of R then $R/A = \left\{ \overline{\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}} /n \in Z \right\}$

Sol. Let $\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \in \begin{pmatrix} 0 & Q \\ 0 & 0 \end{pmatrix}$, where $x \in Q$

i.e. $\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} \in A$, where A is an ideal of $R \Rightarrow \overline{\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}} = \bar{0}$

Consider any element $\overline{\begin{pmatrix} n & x \\ 0 & 0 \end{pmatrix}} \in R/A$ then

$$\overline{\begin{pmatrix} n & x \\ 0 & 0 \end{pmatrix}} = \overline{\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}} + \overline{\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}} = \overline{\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}} + \bar{0} \quad \left(\therefore \overline{\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}} = \bar{0}\right)$$

$$= \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$$

$$\therefore R/A = \left\{ \begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix} \middle| n \in Z \right\}$$

9.4.15 Note : If the element $\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$ is identified with $n \in Z$, then R/A is identified with ring of integers, where $\begin{pmatrix} n & 0 \\ 0 & 0 \end{pmatrix}$ is identified with n.

9.4.16 Example : Find the non trivial (i) right ideals
(ii) ideals of the ring $R = \begin{pmatrix} Z & Q \\ 0 & 0 \end{pmatrix}$

Sol. (i) Let A be any non zero right ideal of R

Let $X = \left\{ n \in Z \middle| \begin{pmatrix} n & a \\ 0 & 0 \end{pmatrix} \in A \text{ for some } a \in Q \right\}$ then X is a subgroup of Z under addition. Let $n_1, n_2 \in X$

$$n_1 \in X \Rightarrow \begin{pmatrix} n_1 & a_1 \\ 0 & 0 \end{pmatrix} \in A, \text{ where } n_1 \in Z,\ a_1 \in Q$$

$$n_2 \in X \Rightarrow \begin{pmatrix} n_2 & a_2 \\ 0 & 0 \end{pmatrix} \in A, \text{ where } n_2 \in Z,\ a_2 \in Q$$

$$\Rightarrow \begin{pmatrix} n_1 & a_1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} n_2 & a_2 \\ 0 & 0 \end{pmatrix} \in A \qquad (A \text{ is a right ideal})$$

$$\Rightarrow \begin{pmatrix} n_1 - n_2 & a_1 - a_2 \\ 0 & 0 \end{pmatrix} \in A$$

$$\Rightarrow n_1 - n_2 \in X$$

$\therefore X$ is a subgroup of Z

Since every subgroup of Z is of the form nZ, for some $n \in Z$

Let $X = n_o Z$, for some $n_o \in Z$

$$X = \left\{ n \in Z : \begin{pmatrix} n & a \\ 0 & 0 \end{pmatrix} \in A \right\}$$

Case (1) $X \neq (0)$ i.e., $n_0 \neq 0$

We shall show that $A = \begin{pmatrix} n_0 Z & Q \\ 0 & 0 \end{pmatrix}$

Let $a \in Q$ be such that $\begin{pmatrix} n_0 & a \\ 0 & 0 \end{pmatrix} \in A$. Let $z \in Z$ and $q \in Q$ then

$$\begin{pmatrix} n_0 Z & q \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n_0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Z & q/_{n_0} \\ 0 & 0 \end{pmatrix} \in A$$

$$\left(A \text{ is right ideal and } \begin{pmatrix} n_0 & a \\ 0 & 0 \end{pmatrix} \in A \text{ and } \begin{pmatrix} Z & q/_{n_0} \\ 0 & 0 \end{pmatrix} \in R \right)$$

$\Rightarrow$ any element of $\begin{pmatrix} n_0 Z & q \\ 0 & 0 \end{pmatrix}$ is in A

$\Rightarrow \begin{pmatrix} n_0 Z & Q \\ 0 & 0 \end{pmatrix} \subset A$

But $A \subset \begin{pmatrix} n_0 Z & Q \\ 0 & 0 \end{pmatrix}$ Since $x = n_0 Z$

$\Rightarrow A = \begin{pmatrix} n_0 Z & Q \\ 0 & 0 \end{pmatrix}$. Also, we have seen that every element of A

$$\begin{pmatrix} n_0 Z & q \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n_0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} Z & q/_{n_0} \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} n_0 & a \\ 0 & 0 \end{pmatrix} r \qquad \text{where } r = \begin{pmatrix} Z & q/_{n_0} \\ 0 & 0 \end{pmatrix} \in R$$

$\Rightarrow A$ is generated by $\begin{pmatrix} n_0 & a \\ 0 & 0 \end{pmatrix}$

$\Rightarrow A$ is a principal right ideal.

case(2) Let $X = (0)$ i.e. $n_0 = 0$

Let $K = \{q \in Q / \begin{pmatrix} 0 & q \\ 0 & 0 \end{pmatrix} \in A$. Then K is a subgroup of Q

For $q_1, q_2 \in K \Rightarrow \begin{pmatrix} 0 & q_1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & q_2 \\ 0 & 0 \end{pmatrix} \in F.$

$\Rightarrow \begin{pmatrix} 0 & q_1 - q_2 \\ 0 & 0 \end{pmatrix} \in A \quad (\therefore A \text{ is an ideal}) \quad \Rightarrow q_1 - q_2 \in K$

$\therefore A = \begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix}$, where $K \subset Q$

(ii) The non trivial right ideals

$A = \begin{pmatrix} n_0 Z & Q \\ 0 & 0 \end{pmatrix}, n_0 \neq 0 \in Z$ and

$A = \begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix}$, where K is additive subgroup of Q, R are also left ideals.

$$\text{Consider} \begin{pmatrix} n_1 & q_1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} n_0 Z & q \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} n_1 n_0 Z & n_1 q \\ 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} n_0(n_1 Z) & q_1^{'} \\ 0 & 0 \end{pmatrix} \in A \qquad \forall \qquad A = \begin{pmatrix} n_1 & q_1 \\ 0 & 0 \end{pmatrix} \in R$$

$\Rightarrow A$ is left ideal of R

Similarly $\begin{pmatrix} 0 & K \\ 0 & 0 \end{pmatrix}$ is also left ideal of R.

$\therefore$ Even if R is non commutative we have right ideals which are also left ideals. But each left ideal of R is not a right ideal

Consider $A = \left\{ \begin{pmatrix} n_0 m & ma \\ 0 & 0 \end{pmatrix} \Big/ m \in Z \right\}$ where n_0 and a are fixed elements in Z and Q. Then A is a left ideal of R but A is not a right ideal of R.

9.4.17 Example : Let R be a commutative ring with unity. Suppose R has no non trivial ideals then prove that R is a field.

Sol. Let R be a commutative ring with unity

Let R has no non trivial ideals then the ideals of R are (0) and itself. We shall show that every non zero element in R has multiplicative inverse

Let a be any non zero element of R.

Consider the left ideal $Ra = \{ra : r \in R\}$ of R.

Since R is commutative then Ra is also right ideal of R

$\Rightarrow Ra$ is an ideal of R

$1 \in R \Rightarrow a = 1a \in Ra$ where $a \neq 0$

$\Rightarrow Ra \neq \{0\}$

$\Rightarrow Ra = R$ only $\quad$ (since $\{0\}$, R are the only ideals of R)

Since $1 \in R$ then $1 = ba$ for some $b \in R$

$\Rightarrow ab = 1 \quad$ (R is commutative)

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

$\therefore R$ is a field.

9.4.18 Note : (i) Conversely if R is a field then R is a division ring and hence it has no proper ideals.

(ii) Every field is a principal ideal ring.

9.5 Summary

In this lesson we have defined ideals of rings. Also we have defined rings of matrices. At end of the section we have introduced the notion of quotient rings.

9.6 Model Examination Questions

(1) Let R be a commutative ring with unity. Suppose R has no nontrivial ideals then prove that R is a field.

(2) Find all ideal in a pollynomial ring $F[x]$ over a field F.

(3) Find right ideals, left ideals and ideals of a ring $R = \begin{pmatrix} Q & Q \\ 0 & 0 \end{pmatrix}$

9.7 Glossary

Ideal of rings, rings of matrices, principal ideal rings.

LESSON-10

HOMOMORPHISMS OF RINGS

10.1 Introduction : In this lesson, we define homomorphism between two rings. Further we established the fundamental theorem of homomorphism and the correspondence theorem. Moreover we introduce the notion of anti-homomorphism.

10.2 Homomorphism of Rings

10.2.1 Definition : Let f be a mapping from a ring R into a ring S such that

(i) $f(a+b) = f(a) + f(b) \ \ \forall \ \ a, \ b \in \mathrm{R}$

(ii) $f(ab) = f(a)f(b) \ \ \forall \ \ a, \ b \in \mathrm{R}$

Then f is called a homomorphism of R into S.

If f is one-one then f is called an isomorphism (monomorphism) from R into S. In this case f is called an embedding of R into S (or R is embeddable in S). We also say that S cotains a copy of R and R may be identified with a subring of S. The symbol $R \subset S$ means that R is embeddable in S.

10.2.2 Note : (i) If a homomorphism f from a ring R into a ring S is both $1-1$ and onto then there exists a homomorphism g from S into R that is also $1-1$ and onto. In this case we say that the two rings R and S are isomorphic. It is denoted by $R \simeq S$.

(ii) If $R \simeq S$ then $S \simeq R$. Also the identity mapping gives $R \simeq R$ for any ring. It is easy to verify that if $f : R \to S$ and $g : S \to T$ are isomorphisms of R onto S and S onto T respectively then gf is also a isomorphism of R onto T i.e., $R \simeq S$ and $S \simeq T$ then $R \simeq T$. Therefore isomorphism is an equivalence relation in the class of rings.

10.2.3 Theorem : Let $f : R \to S$ be an isomorphism of a ring R into a ring S then we have the following

(i) If 0 is the zero of R then $f(0)$ is the zero of S.

(ii) If $a \in R$ then $f(a) = -f(a)$.

(iii) The set $\{f(a)|a \in R\}$ is a subring of S is called the homomorphic image of R by the mapping f and is denoted by Imf or $f(R)$.

(iv) The set $\{a \in R|f(a) = 0\}$ is an ideal in R called the kernel of f and is denoted by $kerf$ or $f^{-1}(0)$.

(v) If $1 \in R$ then $f(1)$ is the unity of the subring $f(R)$.

(vi) If R is commutative then $f(R)$ is commutative.

Proof.(i) Let $a \in R$

Consider $f(a) = f(a + 0) = f(a) + f(0)$ (f is homomorphism)

Similarly $f(a) = f(0) + f(a)$

Therefore, $f(0)$ is the zero of S we denote $f(0) = 0$.

(ii) Consider $f(0) = f(a + (-a)) = f(a) + f(-a)$

Therefore $f(-a) = -f(a)$

(iii) $f(\mathbb{R}) = \{f(a)|a \in R\}$

Let $f(a), f(b) \in R$ where $a,\ b \in R$

Consider $f(a) - f(b) = f(a - b) \in f(R)$ (since $a - b \in R$)

Similarly $f(a)f(b) = f(ab) \in f(R)$ (since $ab \in R$)

Therefore $f(R)$ is a subring of S.

(iv) Let $kerf$= $\{a \in R|f(a) = 0\}$

Let $a,\ b \in kerf \Rightarrow f(a) = 0,\ f(b) = 0$

Consider $f(a - b) = f(a) - f(b)$ ($\because f$ is homomorphism)

$= 0 - 0 = 0$. Therefore $a - b \in kerf$.

Consider $f(ar) = f(a)f(r) = 0f(r) = 0$. Therefore $ar \in kerf$.

Similarly $ra \in kerf$. Therefore $kerf$ is an ideal of R

(v) Let $a \in R$. Consider $f(a)f(1) = f(a.1) = f(a)$

Similarly $f(1)f(a) = f(1.a) = f(a)$. Therefore $f(1)$ is the identity of $f(R)$

(vi) Let $f(a), f(b) \in f(R)$ where $a, b \in R$

$$\begin{aligned} f(a)f(b) &= f(ab) \\ &= f(ba) \qquad (ab = ba \quad \forall \ a, \ b \in R) \\ &= f(b)f(a) \end{aligned}$$

Therefore $f(R)$ is commutative.

10.2.4 Theorem : Let $f : R \to S$ be a homomorphism of a ring R into a ring S then $kerf = (0)$ iff f is $1-1$.

Proof. (i) Let $kerf = \{0\}$

If $f(a) = f(b) \Rightarrow f(a) - f(b) = 0$

$$\begin{aligned} &\Rightarrow f(a-b) = 0 \\ &\Rightarrow a - b = 0 \qquad (kerf = (0)) \\ &\Rightarrow a = b. \qquad (\because f \textbf{ is } 1-1) \end{aligned}$$

(ii) If f is $1-1$ then to prove that $kerf = \{0\}$

Let $a \in kerf \Rightarrow f(a) = 0 \Rightarrow f(a) = f(0) \Rightarrow a = 0 \qquad (\because f \textbf{ is } 1-1)$

Therefore $kerf = \{0\}$

10.2.5 Theorem : Let N be an ideal in a ring R then $\exists$ a onto homomorphism from $R \to R/N$, where R/N is the quotient ring of R modulo N.

(It is called the canonical or natural homomorphism)

Proof. Let $f : R \to R/N$ defined by $f(x) = x + N = \bar{x} \ \ \forall \ x \in \mathrm{R}$

f is homomorphism : $f(x+y) = \overline{x+y} = \bar{x}+\bar{y} = f(x)+f(y) \quad \forall \ x, y \in R$

Also $f(xy) = \overline{xy} = \bar{x}\bar{y} = f(x).f(y) \ \ \forall \ x, y \in R$.

Therefore f is homomorphism.

f is onto : Let $\bar{x} \in R/N \;\; \exists \;\; x \in R \;\; \ni f(x) = \bar{x}$. Therefore f is onto.

$\Rightarrow R/N$ is a homomorphic image of R.

Hence there exists onto homomorphism from $R \to R/N$.

$\Rightarrow$ Every homomorphic image of a ring is of the type a quotient of R modulo some ideal of R. This homomorphism is called natural homomorphism or canonical homomorphism.

10.2.6 Theorem : (Fundamental Theorem of Homomorphisms)

Let f be a homomorphism of a ring R into a ring S with kernel N then $R/N \simeq Imf$

Proof. Define $g : R/N \to Imf$ by $g(a+N) = g(\bar{a}) = f(a)$

g is well defined : Let $a + N = b + N$

$$\begin{aligned}
&\Rightarrow (a-b) + N = N \\
&\Rightarrow a - b \in N \\
&\Rightarrow f(a-b) = 0 \\
&\Rightarrow f(a) - f(b) = 0 \qquad (f \quad \text{is homomorphism}) \\
&\Rightarrow f(a) = f(b) \\
&\Rightarrow g(a+N) = g(b+N)
\end{aligned}$$

g is homomorphism : Consider $g(\bar{a}+\bar{b}) = g(\overline{a+b}) = f(a+b) = f(a)+f(b)$ $= g(\bar{a}) + g(\bar{b})$.

Also $g(\bar{a}.\bar{b}) = g(\overline{ab}) = f(ab) = f(a)f(b) = g(\bar{a})g(\bar{b}) \;\; \forall \;\; \bar{a}, \; \bar{b} \in R/N$.

Therefore g is homomorphism.

g is onto : Let $b \in Imf \;\; \exists \;\; a \in R \;\; \ni \;\; f(a) = b$

$\Rightarrow g(\bar{a}) = f(a) = b$. Therefore g is onto.

g is 1-1 : Let $\bar{a}, \; \bar{b} \in R/N$.

Let $g(\bar{a}) = g(\bar{b}) \Rightarrow f(a) = f(b)$

$$\Rightarrow f(a) - f(b) = 0$$
$$\Rightarrow f(a-b) = 0$$
$$\Rightarrow a - b \in N$$
$$\Rightarrow a \equiv b (modN)$$
$$\Rightarrow \bar{a} = \bar{b}.$$

Therefore $R/N \simeq Imgf$.

10.2.7 Note : This theorem can also be stated as given a homomorphism of rings $f : R \to S$ there exists a unique injective homomorphism $g : R/kerf \to S$ such that $f = g\eta$, where η is the canonical homomorphism.

Proof. $g : R/kerf \to S$ is a homomorphism defined by $g(\bar{a}) = f(a)$ then g is injective.

Also $f = g\eta$. Since $f(a) = g(\bar{a}) = g(\eta(a))$ $\quad (\eta(a) = a + N = \bar{a} \;\forall\; a \in R)$

g is unique : Let $f = h\eta$, where $h : R/kerf \to S$ is a homomorphism then

$$g\eta = h\eta \Rightarrow g\eta(a) = h\eta(a) \;\forall\; a \in R$$
$$\Rightarrow g(\bar{a}) = h(\bar{a}) \;\forall\; a \in R/kerf$$
$$\Rightarrow g = h$$

10.2.8 Note : Let f be a mapping from a set R into a set S and $A \subset S$. Let $f^{-1}(A) = \{r \in R | f(r) \in A\}$ then

(1) f^{-1} is a mapping of subsets of S into subsets of R.

(2) $f(f^{-1}(A)) \subset A$

(3) If f is onto then $A \subset f(f^{-1}(A))$

(4) If f is onto then $f(f^{-1}(A)) = A$

(5) If X is any subset of R then $X \subset f^{-1}(f(X))$.

10.3 Correspondence Theorem :

10.3.1 Theorem : Let $f : R \to S$ be a homomorphism of a ring R onto a ring S and let $N = kerf$. Then the mapping $F : A \to f(A)$ defines one-one correspondence from the set of all ideals (right ideals, left ideals) in R that contain N onto the set of all ideals (right ideals, left ideals) in S. It prserves ordering in the sense that $A \subsetneq B$ iff $f(A) \subsetneq f(B)$.

Proof. Let $f : R \to S$ be a homomorphism of a ring R onto a ring S. Let $N = kerf$. Let X be any arbitary ideal in S and the set $A = f^{-1}(X)$. Now show that $f^{-1}(X)$ is an ideal in R, where

$$f^{-1}(X) = \{x \in R/f(x) \in X\}$$

Let $a,\ b \in f^{-1}(X) \Rightarrow f(a),\ f(b) \in X$

$$\Rightarrow f(a) - f(b) \in X \quad (\because X \text{ is an ideal of } S)$$

$$\Rightarrow f(a-b) \in X$$

$$\Rightarrow a - b \in f^{-1}(X)$$

Let $a \in f^{-1}(X)$ and $r \in R \Rightarrow f(a) \in X$ and $f(r) \in S$

$$\Rightarrow f(a)f(r) \in X \quad (\because X \text{ is an ideal of } S)$$

$$\Rightarrow f(ar) \in X$$

$$\Rightarrow ar \in f^{-1}(X)$$

Similarly $ra \in f^{-1}(X)$. Therefore $f^{-1}(X)$ is an ideal in R.

Let A be an ideal in R then $f(A)$ is an ideal in S for if $f(a),\ f(b) \in f(A)$, where $a,\ b \in A$. Consider $f(a) - f(b) = f(a-b) \in f(A)$ $(\because\ a - b \in A)$

Let $f(a) \in f(A)$ and $s \in S$. Since f is onto from R to $S \Rightarrow s \in S$ has pre image say r in R such that $f(r) = s$ then $f(a)s = f(a)f(r) = f(ar) \in f(A)$. Similarly $sf(a) \in f(A)$. Therefore $f(A)$ is an ideal in S

Let $R' = \{A : A \text{ is an ideal in } R \text{ containing } N = kerf\}$ and S'=\{all ideals of S \}. Define $F : R' \to S'$ by $F(A) = f(A)$

F is onto: Let $X \in S' \Rightarrow X$ is an ideal in $S \Rightarrow f^{-1}(X)$ is an ideal in R

Let $A = f^{-1}(X)$. We shall show that $f(f^{-1}(X)) = X$.

Let $f(a) \in f(f^{-1}(X))$, where $a \in f^{-1}(X)$

Since $a \in f^{-1}(X) \Rightarrow f(a) \in X$

$$\Rightarrow f(f^{-1}(X)) \subset X \qquad (10.3.1(\text{a}))$$

Let $x \in X$ then since f is onto there exists $a \in R$ such that $f(a) = x$ $\Rightarrow f(a) \in X \Rightarrow a \in f^{-1}(X)$ then $x = f(a) \in f(f^{-1}(X))$

$$\Rightarrow X \subset f(f^{-1}(X)) \qquad (10.3.1(\text{b}))$$

On using (10.3.1(a)) and (10.3.1(b)) we get $X = f(f^{-1}(X))$, where $f^{-1}(X) = A$ is an ideal in R. We shall show that $N \subset A$, where $A = \{x \in R : f(x) \in X\}$

Let $x \in N$ then $f(x) = \bar{0}$ $\quad$ ($\therefore X$ is an ideal of $S \Rightarrow \bar{0} \in X$)

$\Rightarrow f(x) \in X \Rightarrow x \in f^{-1}(X) \Rightarrow x \in A$. Therefore $N \subset A$

$\therefore$ for every $X \in S^{'}$ $\exists$ $A = f^{-1}(X) \in R^{'}$ such that $F(A) = f(A) = f(f^{-1}(X)) = X$. Hence F is onto.

F **is one-one:** Let $F(A) = F(B)$, where A, B are in $R^{'}$ i.e., A and B are the ideals of R containing N.

$F(A) = F(B) \Rightarrow f(A) = f(B)$

we shall show that $f^{-1}(f(A)) = A$

Let $a \in A \Rightarrow f(a) \in f(A) \Rightarrow a \in f^{-1}(f(A))$

$$\Rightarrow A \subset f^{-1}(f(A)) \qquad (10.3.1(\text{c}))$$

Let $x \in f^{-1}(f(A)) \Rightarrow f(x) \in f(A)$

$$\begin{aligned}
&\Rightarrow f(x) = f(a), \qquad \text{for some } a \in A\\
&\Rightarrow f(x) - f(a) = \bar{0}\\
&\Rightarrow f(x - a) = \bar{0}\\
&\Rightarrow x - a \in N = kerf \quad \text{but} \quad N \subset A\\
&\Rightarrow x - a \in A
\end{aligned}$$

$$\Rightarrow x \in A$$

$$\Rightarrow f^{-1}(f(A)) \subset A \qquad (10.3.1(d))$$

On using (10.3.1(c)) and (10.3.1(d)), we get $A = f^{-1}(f(A))$.

Similarly $f^{-1}(f(B)) = B$

$\therefore f(A) = f(B) \Rightarrow f^{-1}(f(A)) = f^{-1}(f(B))$

$\Rightarrow A = B$. Therefore F is one-one.

$\Rightarrow \exists$ a one-one correspondence between the ideals of R containing N and ideal of S'.

Let A and B be an ideals in R such that $A \subsetneq B$ i.e., $A \subset B$, but $A \neq B$

$\Rightarrow f(A) \subset f(B)$, because if $f(a) \in f(A)$, where $a \in A$ and $A \subset B \Rightarrow a \in B$

$\Rightarrow f(a) \in f(B) \Rightarrow f(A) \subset f(B)$

if $f(A) = f(B)$ then $f^{-1}(f(A)) = f^{-1}(f(B)) \Rightarrow A = B$ which is not true.

Therefore $f(A) \subsetneq f(B)$

Conversely let $f(A) \subsetneq f(B)$

$$\Rightarrow f(A) \subset f(B)$$

$$\Rightarrow f^{-1}(f(A)) \subset f^{-1}(f(B)) \Rightarrow A \subset B.$$

Also $A \neq B$ for if $A = B$ then $f(A) = f(B)$ which is not true. Therefore $A \neq B$ i.e., $A \subsetneq B$.

10.3.2 Theorem : If K is an ideal in a ring R then each ideal (right or left ideal) in R/K is of the form A/K where A is an ideal (right or left ideal) in R containing K.

Proof. Consider the canonical homomorphism $f : R \to R/K$ which is an onto homomorphism. Then by the correspondence theorem any ideal in R/K is of the form $f(A)$, where A is any ideal containing $ker f = K$ then K is an ideal of A $\quad$ (A is an ideal of R and K is an ideal of $R \Rightarrow K \subset A$)

and $f(A) = \{f(x) : x \in A\} = \{x + K : x \in A\} = A/K$.

$\Rightarrow$ any ideal in R/K is of the form A/K where A is an ideal containing K.

10.3.3 Definition : Let R and S be rings. A mapping $f : R \to S$ is an anti-homomorphism if $f(x + y) = f(x) + f(y)$ and $f(xy) = f(y)f(x)$ for all $x,\ y \in R$. An anti-homomorphism which is both $1 - 1$ and onto is called an anti-isomorphism.

10.3.4 Example : Let $R = (R, +, .)$ be a ring. Define a binary operation o in R as $x\ o\ y\ =\ y.x$ for all $x,\ y \in R$ then prove that $(R, +, o)$ is a ring.

Sol. $(R, +)$ is an abelian group

Let $x, y \in R \Rightarrow y.x \in R$ $\quad (\because (R, +, .)$ is a ring$)$

$\Rightarrow x\ o\ y \in R$

Consider $x\ o\ (y\ o\ z) = x\ o\ (zy)$

$= (zy)x$

$= z(yx)$

$= z(x\ o\ y)$

$=(x\ o\ y)o\ z$

Also $x\ o(y + z) = (x\ o\ y) + (x\ o\ z)$ and $(y + z)o\ x = (y\ o\ x) + (z\ \mathrm{o}\ x)$

Therefore $(R, +, o)$ is a ring.

10.3.5 Definition : Let $(R, +, .)$ be a ring then the opposite ring of R written R^{op}, is defined to be the ring $(R, +, o)$ where $x\ o\ y\ =\ y.x$ for all $x, y \in R$.

10.3.6 Example : Prove that the homomorphism from the ring of integers Z to Z are the identity and zero mappings only.

Sol. If f is a zero mapping then f is a homomorphism,

since $f(a + b) = 0 = 0 + 0 = f(a) + f(b) \quad \forall\ a,\ b \in Z$

and $f(ab) = 0 = f(a)f(b) \quad \forall \;\; a, \; b \in Z$

If f is a non zero homomorphism then consider

$(f(1))^2 = f(1)f(1) = f(1.1) = f(1)$ and $f(1) \neq 0$

because if $f(1) = 0$ for any $x \in Z$, we have

$$f(x) = f(1.x) = f(1)f(x) = 0f(x) = 0 \Rightarrow f = 0 \text{ which is not true.}$$

$\therefore f(1) \neq 0$ and $f(1)^2 = f(1)$.

i.e. $f(1)$ is a non zero idempotent element in $f(Z) \subset Z$.

But the only nonzero idempotent element in Z is $1 \Rightarrow f(1) = 1$

$$\begin{aligned} \text{Now consider } f(n) &= (1 + 1 + 1 + \ldots + 1) \qquad (n \text{ times if } n > 0) \\ &= f(1) + f(1) + \ldots + f(1) \quad (n \text{ times}) \\ &= \text{n if } n > 0 \qquad (\because f(1) = 1) \end{aligned}$$

Also $f(n) = 0$ if $n = 0$.

If $n < 0$ then

$$\begin{aligned} f(n) &= (-1 - 1 - 1 - \ldots - 1) \\ &= f(-1) + f(-1) + \ldots + f(-1) \quad (n \text{ times}) \\ &= (-1) + (-1) + (-1) + \ldots + (-1) \quad (n \text{ times}) \\ &= -n \text{ if } n < 0 \end{aligned}$$

$\therefore f(n) = n \; \forall \; n \in Z$. Therefore f is identity mapping.

10.3.7 Example : Let A and B be ideals in R such that $B \subseteq A$ then prove that $R/A \simeq (R/B)/(A/B)$.

Sol. Define a mapping $f : R/B \to R/A$ by $f(x + B) = x + A \quad \forall \quad x \in R$ then f is well defined if $x_1 + B = x_2 + B$ then $x_1 - x_2 + B = B \Rightarrow x_1 - x_2 \in B$

$$\begin{aligned} \text{But } B \subseteq A &\Rightarrow x_1 - x_2 \in A \\ &\Rightarrow x_1 - x_2 + A = A \\ &\Rightarrow x_1 + A = x_2 + A \end{aligned}$$

$$\Rightarrow f(x_1 + B) = f(x_2 + B)$$

We shall show that f is an onto homomorphism

Consider $f((x_1 + B) + (x_2 + B)) = f(x_1 + x_2 + B)$

$= x_1 + x_2 + A$

$= (x_1 + A) + (x_2 + A)$

$= f(x_1 + B) + f(x_2 + B)$

Also $f((x_1 + B).(x_2 + B))= f(x_1x_2 + B)$

$=x_1x_1 + A$

$=(x_1 + A)(x_2 + A)$

$=f(x_1 + B)f(x_2 + B)$

$\therefore f$ is a homomorphism.

f **is onto:** Since for every $x + A \in R/A$, we have $x \in R$ such that $f(x + B) = x + A$

$\Rightarrow f$ is onto.

Now $ker f = \{x + B \in R/B : f(x + B) = \bar{0}\}$

$=\{x + B : x + A = A\}$

$=\{x + B : x \in A\}$ $=A/B$

Then by first isomorphism theorem we get, $(R/B)/(A/B) \simeq R/A$.

10.3.8 Example : Prove that any ring R can be embedded in a ring S with unity.

Sol. Let S be the cartesian product of R and the set of integers Z

i.e., $S = R \times Z$.

Define the binary operations + and . in S by $(a, m) + (b, n) = (a + b, m + n)$ and $(a, m).(b, n) = (ab + na + mb, mn)$, where $a,\ b \in R$ and $m,\ n \in Z$

Consider $(a, m) - (b, n) = (a - b, m - n)$, where, $a - b \in R$ and $m - n \in Z$

$\therefore$ S is an abelian group under addition and also

$(a, m).(b, n) = (ab + na + mb, mn) \in R \times Z$ $\quad (\because ab + na + mb \in R$ and $mn \in Z$, where $ab \in R$, $na = a + \ldots + a \in R$, $mb = b + \ldots + b \in R)$

Therefore S is a ring.

The unity is given by $(0, 1)$, because $(a, m).(0, 1) = (0 + 1a + 0, m1) = (a, m)$

Similarly $(0, 1).(a, m) = (0 + 0 + a, m)$=$(a, m)$

Define a mapping $f : R \to S$ by $f(a) = (a, 0)$ $\forall$ $a \in R$ then f is a homomorphism.

Consider $f(a + b) = (a + b, 0)$

$$=(a, 0) + (b, 0)$$

$$=f(a) + f(b) \quad \forall \ a,\ b \in R$$

$$f(ab) = (ab, 0) = (a, 0)(b, 0)=f(a)f(b) \quad \forall \ a,\ b \in R$$

f is one-one: Let $f(a) = f(b) \Rightarrow (a, 0) = (b, 0) \Rightarrow a = b$

Therefore f is an embedding ring of R into S.

10.3.9 Example : Find all ideals of $Z/(10)$.

Sol. $Z/(10) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$

(0) and $Z/(10)$ are trivial ideals.

Also $(\bar{2})$= $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ and $(\bar{5})$= $\{\bar{0}, \bar{5}\}$ are also ideal of $Z/(10)$

Therefore the ideals of $Z/(10)$ are $(0), \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$, $\{\bar{0}, \bar{5}\}$ and $Z/(10)$.

10.3.10 Example : Let R be a ring then prove that $(R_n)^{op} \simeq (R^{op})_n$

Sol. Define a mapping $f : (R_n)^{op} \to (R^{op})_n$ by $f(A) = t_A$, the transpose of A. Recall that as sets $R = R^{op}$ and $R_n = (R_n)^{op}$ then by the definition of the transpose of a matrix $t_{A+B} = t_A + t_B$ so $f(A + B) = f(A) + f(B)$. We now show that $f(A \text{ o } B) = f(A)f(B)$, where the multiplication of matrices $f(A)$ and $f(B)$ is in the ring $(R^{op})_n$

Assume $A = (a_{ij}),\ \ B = (b_{ij})$

$f(A) = t_A = (a'_{ij})$ and $f(B) = t_B = (b'_{ij})$ then

$a'_{ij} = a_{ji}$ and $b'_{ij} = b_{ji}$ for all $1 \leq i, j \leq n$

Now $f(A \text{ o } B) = f(BA) = t_{BA}$

The (i, j) entry of t_{BA} is the (j, i) entry of BA which is given by

$$\sum_{k=1}^{n} b_{jk}a_{ki} = \sum_{k=1}^{n} a_{ki} \text{ o } b_{jk} = \sum_{k=1}^{n} a'_{ik} \text{ o } b'_{kj} = (i, j) \quad \text{entry of} \quad t_A t_B \in (R^{op})_n$$

Hence $t_{BA} = t_A t_B$

$\therefore f(A \text{ o } B) = f(A)f(B)$

f **is one-one:** If $f(A) = f(B) \Rightarrow t_A = t_B \Rightarrow A = B$. Also f is onto.

Hence $(R_n)^{op} \simeq (R^{op})_n$

10.4 Summary

In this lesson we have defined homomorphism of rings. Also we have observed that the kernel of homomorphism is $\{0\}$ if and only if it is one-one. Further we have proved fundamental theorem of homomorphism and correspondence theorem.

10.5 Model Examination Questions

(1) Show that any nonzero homomorphism of a field F into a ring R is one-one.

(2) Let $f : F \to F$ be a nonzero homomorphism of a field F into itself then show that f need not be onto.

(3) Let R be a ring. Show that R is anti-isomorphic to R^{op}.

10.6 Glossary

homomorphism of rings, isomorphism of rings, correspondence theorem, anti homomorphism of rings.

LESSON-11

Sum and Direct Sum of Ideals

11.1 Introduction : In this lesson, we study sum and direct sum of ideals.

11.2 Definition : Let $A_1, A_2, \ldots, A_n$ be a family of right ideals in a ring R. Then the smallest right ideal of R containing each $A_i,\ 1 \leq i \leq n$ (i.e., the intersection of all right ideals in R containing each A_i) is called the sum of $A_1, A_2, \ldots, A_n$ and is denoted by $A_1 + A_2 + \ldots + A_n$.

11.3 Theorem : If $A_1, A_2, \ldots, A_n$ are right ideals in a ring R, then $S = \{a_1 + a_2 + \ldots + a_n / a_i \in A_i,\ 1 \leq i \leq n\}$ is the sum of right ideals $A_1, A_2, \ldots, A_n$.

Proof. Let $S = \{a_1 + a_2 + \ldots + a_n / a_i \in A_i,\ 1 \leq i \leq n\}$.

To prove that S is an ideal in R

Let $x,\ y \in S$ and $r \in R$, then $x = a_1 + a_2 + \ldots + a_n$ and $y = b_1 + b_2 + \ldots + b_n$ where $a_i,\ b_i \in A_i,\ 1 \leq i \leq n$

Now $x - y = (a_1 + a_2 + \ldots + a_n) - (b_1 + b_2 + \ldots + b_n)$

$= (a_1 - b_1) + (a_2 - b_2) + \ldots + (a_n - b_n) \in S$

$\Rightarrow x - y \in S$. (since A_i is an ideal, $a_i,\ b_i \in A_i \Rightarrow a_i - b_i \in A_i,\ 1 \leq i \leq n$)

Also $xr = (a_1 + a_2 + \ldots + a_n)r = a_1r + a_2r + \ldots + a_nr$

$\Rightarrow xr \in S$ (since $a_ir \in A_i$ for $1 \leq i \leq n$)

Thus S is a right ideal of R.

If $a_1 \in A_1$ then a_1 can be written as $a_1 = a_1 + 0 + \ldots + 0$ and by the definition of S we get $a_1 \in S \Rightarrow A_1 \subset S$.

Similarly $A_2, A_3, \ldots, A_n$ are contained in S.

Let T be any right ideal of R contained each A_i then $a_1, a_2, \ldots, a_n \in T$

$\Rightarrow a_1 + a_2 + \ldots + a_n \in T$ (since T is an ideal). Therefore $S \subset T$.

$\therefore$ S is the smallest right ideal of R containing each A_i. i.e., S is the intersection of all the right ideal in R containing each A_i. Therefore S is the sum of the right ideals $A_1, A_2, \ldots, A_n$.

11.4 Note : The sum of right (left) ideals $A_1, A_2, \ldots, A_n$ in a ring R is denoted by $A_1 + A_2 + \ldots + A_n = \sum_{i=1}^{n} A_i$.

11.5 Definition : A sum $A = \sum_{i=1}^{n} A_i$ of right (left) ideal in R is called a direct sum if each element $a \in A$ is uniquely expressible in the from $\sum_{i=1}^{n} a_i$, where $a_i \in A_i$, $1 \leq i \leq n$. If the sum $A = \sum_{i=1}^{n} A_i$ is a direct sum we write it as $A = A_1 \oplus A_2 \oplus \ldots \oplus A_n = \oplus \sum_{i=1}^{n} A_i$.

11.6 Theorem : Let $A_1, A_2, \ldots, A_n$ be right (left) ideals in a ring R then the following are equivalent

(i) $A = \sum_{i=1}^{n} A_i$ is a direct sum.

(ii) If $0 = \sum_{i=1}^{n} a_i$, $a_i \in A_i$ then $a_i = 0$, for $i = 1, 2, \ldots, n$.

(iii) $A_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{n} A_j = (0)$, $i = 1, 2, \ldots, n$

Proof. (i) $\Rightarrow$ (ii)

Assume that (i) is true. Suppose $\sum_{i=1}^{n} a_i = 0$ and since A is direct sum of $A_1, A_2, \ldots, A_n$, each element of A has a unique representation

we have $0 \in A$ and $0 = 0 + 0 + \ldots + 0$

$$\because a_1 + a_2 + \ldots + a_n = 0 = 0 + 0 + \ldots + 0$$

$\Rightarrow a_1 = a_2 = \ldots = a_n = 0$. Thus $\sum_{i=1}^{n} a_i = 0 \;\Rightarrow\; a_i = 0$, for $i = 1, 2, \ldots, n$.

(ii) $\Rightarrow$ (iii)

Assume that (ii) is ture. Let $x \in A_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{n} A_j$ then $x \in A_i$ and $x \in \sum_{\substack{j=1 \\ j \neq i}}^{n} A_j$

$\Rightarrow x = a_1 + a_2 + \ldots + a_{i-1} + a_{i+1} + \ldots + a_n$

$\Rightarrow 0 = a_1 + a_2 + \ldots + a_{i-1} + (-x) + a_{i+1} + \ldots + a_n$

from (ii) we get each $a_j = 0$, for $j = 1, 2, \ldots, n,\ j \neq i$ and $-x = 0 \Rightarrow x = 0$

Thus $A_i \cap \sum\limits_{\substack{j=1 \\ j\neq i}}^{n} A_j = (0)$.

(iii) $\Rightarrow$ (i)

Assume that (iii) is ture. Let $a \in A = \sum\limits_{i=1}^{n} A_i$ and assume that a has two representations say $a = a_1 + a_2 + \ldots + a_n$ and $a = b_1 + b_2 + \ldots + b_n$, where $a_i,\ b_i \in A_i$ for $1 \leq i \leq n$

$\Rightarrow (a_1 + a_2 + \ldots + a_n) - (b_1 + b_2 + \ldots + b_n) = 0$

$\Rightarrow (a_1 - b_1) + (a_2 - b_2) + \ldots + (a_n - b_n) = 0$

$\Rightarrow a_1 - b_1 = -(a_2 - b_2) - \ldots - (a_n - b_n)$

Now A_1 is an ideal of R, we have $a_1 - b_1 \in A_1$ and

$-(a_2 - b_2) - \ldots - (a_n - b_n) \in A_2 + A_3 + \ldots + An = \sum\limits_{j=2}^{n} A_i$

$\Rightarrow a_1 - b_1 \in A_1 \cap \sum\limits_{j=2}^{n} A_j$, but by (iii) we have $A_i \cap \sum\limits_{\substack{j=1 \\ j\neq i}}^{n} A_j = (0)$

Therefore $a_1 - b_1 = 0 \Rightarrow a_1 = b_1$. Similarly we get $a_2 = b_2, \ldots, a_n = b_n$.

Hence each $a \in A = \sum\limits_{i=1}^{n} A_i$ has a unique representation. $\therefore A$ is a direct sum.

11.7 Theorem : Let $R_1, R_2, \ldots, R_n$ be a family of rings and let $R = R_1 \times R_2 \times \ldots \times R_n$ be their direct product. Let $R_i^* = \{(0, \ldots, 0, a_i, 0, \ldots, 0)/a_i \in R_i\}$ then $R = \oplus \sum\limits_{i=1}^{n} R_i^*$ is a direct sum of ideals R_i^* and $R_i^* \simeq R_i$ as rings. On the other hand if $R = \oplus \sum\limits_{i=1}^{n} A_i$, a direct sum of ideal of R then $R \simeq A_1 \times A_2 \times \ldots \times A_n$ the direct product of the A_i's considered as rings on their own right.

Proof. Clearly R_i^*'s are ideals in R and $R = R_1^* + R_2^* + \ldots + R_n^*$.

We prove that R is a direct sum of ideals R_i^*

Let $x \in R_i^* \cap \sum\limits_{\substack{j=1 \\ j\neq i}}^{n} R_j^*$ then $x = (0, 0, \ldots, a_i, 0, \ldots, 0) = (a_1, a_2, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n)$

$\Rightarrow a_i = 0$ and hence $x = 0$. Therefore $R = \oplus \sum_{i=1}^{n} R_i^*$

For the second part we note that, if $x \in R$ then x can be uniquely expressed as $a_1 + a_2 + \ldots + a_n,\ a_i \in A_i,\ 1 \leq i \leq n$.

Define a mapping $f : \oplus \sum_{i=1}^{n} A_i \to A_1 \times A_2 \times \ldots \times A_n$ by

$f(a_1 + a_2 + \ldots + a_n) = (a_1, a_2, \ldots, a_n)$, f is well defined since $\sum_{i=1}^{n} A_i$ is direct sum. It is also clear that f is both one-one and onto.

f is homo : Let $x,\ y \in \sum_{i=1}^{n} A_i$ then $x = a_1 + a_2 + \ldots + a_n$ and $y = b_1 + b_2 + \ldots + b_n$, where $a_i,\ b_i \in A_i,\ 1 \leq i \leq n$, it is easy to see that $f(x+y) = f(x) + f(y)$.

Now to show that $f(xy) = f(x)f(y)$, since $a_i,\ b_i \in A_i,\ 1 \leq i \leq n$ then for $i \neq j,\ a_ib_j = 0$ and $a_ib_j \in A_i \cap A_j = (0)$. Therefore f is isomorphism.

11.8 Note : The direct sum $R = \oplus \sum_{i=1}^{n} A_i$ is also called the (internal) direct sum of ideals $A_1, A_2, \ldots, A_n$ in R and the direct product $A_1 \times A_2 \times \ldots \times A_n$ is called the (external) direct sum of the family of ideals $A_1, A_2, \ldots, A_n$.

11.9 Definition : A right (left) ideal I in a range R is called minimal if

(i) $I \neq (0)$ and

(ii) If J is a non-zero right (left) ideal of R contained in I then $J = I$.

11.10 Example : If R is a divison ring then R itself is a minimal right ideal as well as minimal left ideal.

11.11 Example : For any two ideals A and B in a ring R then

(i) $\frac{A+B}{B} \simeq \frac{A}{A \cap B}$

(ii) $\frac{A+B}{A \cap B} \simeq \frac{A+B}{A} \times \frac{A+B}{B} \simeq \frac{B}{A \cap B} \times \frac{A}{A \cap B}$

Sol. (i) Let A and B be two ideals in a ring R then

$A + B = \{a_i + b_i : a_i \in A, b_i \in B\}$ and $A + B$ is an ideal in R.

Let $x = a_1 + b_1$ and $y = a_2 + b_2$ be any two elements of $A + B$ then

$$x - y = (a_1 + b_1) - (a_2 + b_2) = a_1 + (b_1 - a_2) - b_2$$
$$= (a_1 - a_2) + (b_1 - b_2) \in A + B \quad (\because A, B \text{ are ideals})$$

Also $rx = r(a_1 + b_1) = ra_1 + rb_1 \in A + B$, for any $r \in R$

Similarly $xr = (a_1 + b_1)r \in A + B$.

Therefore $A + B$ is an ideal in R and also $A \cap B$ is an ideal in R.

Since B is an ideal of R such that $B \subseteq A + B \Rightarrow B$ is an ideal of $A + B$

$\Rightarrow \frac{A+B}{B}$ is a Quotient ring.

Define $f : A \to \frac{A+B}{B}$ by $f(a) = a + B \ \ \forall\ a \in A$ then f is a onto homomorphism

f is homomorphism : $f(a_1 + a_2) = (a_1 + a_2) + B = (a_1 + B) + (a_2 + B) = f(a_1) + f(a_2)$ and $f(a_1 a_2) = a_1 a_2 + B = (a_1 + B)(a_2 + B) = f(a_1)f(a_2)$.

f is onto: Let $x + B \in \frac{A+B}{B}$, where $x = a_1 + b_1 \in A + B$

consider $f(a_1) = a_1 + B = a_1 + b_1 + B = x + B$ (since $b_1 + B = B$).

Therefore f is onto.

Now $ker\ f = \{a \in A; f(a) = \bar{0}\} = \{a \in A; a + B = B\}$
$$= \{a \in A; a \in B\} = A \cap B.$$

Then by first Isomorphism theorem we get $\frac{A}{A\cap B} \simeq \frac{A+B}{B}$.

(ii) To prove that $\frac{A+B}{A\cap B} \simeq \frac{A+B}{A} \times \frac{A+B}{B} \simeq \frac{B}{A\cap B} \times \frac{A}{A\cap B}$

Let $g : A + B \to \frac{A+B}{A} \times \frac{A+B}{B}$ defined by $g(x) = (x + A, x + B)$, where $x \in A + B$.

g is homomorphism: For any $x,\ y \in A + B$, we have

$$g(x + y) = (x + y + A, x + y + B) = (x + A + y + A, x + B + y + B)$$
$$= (x + A, x + B) + (y + A, y + B) = g(x) + g(y)$$
$$g(xy) = (xy + A, xy + B) = ((x + A)(y + A), (x + B)(y + B))$$
$$= (x + A, x + B)(y + A, y + B) = g(x)g(y)$$

Therefore g is homomorphism.

g **is onto:** Let $(x+A, y+B) \in \frac{A+B}{A} \times \frac{A+B}{B}$, where $x,\ y \in A+B$ such that $x = a_1 + b_1,\ y = a_2 + b_2, \quad a_1,\ a_2 \in A$ and $b_1,\ b_2 \in B$.

Therefore $(x+A, y+B) = (a_1+b_1+A, a_2+b_2+B) = (b_1+A, a_2+B)$

Now $a_2+b_1 \in A+B$ be such that $g(a_2+b_1) = (a_2+b_1+A, a_2+b_1+B) = (b_1+A, a_2+B) = (x+A, y+B)$.

For any $(x+A, y+B) \in \frac{A+B}{A} \times \frac{A+B}{B}$ there exists $a_2+b_1 \in A+B$ such that $g(a_2+b_1) = (x+A, y+B)$. Therefore g is onto.

$$
\begin{aligned}
\text{Now} \qquad ker\ g &= \{x \in A+B / g(x) = (A, B)\} \\
&= \{x \in A+B / (x+A, x+B) = (A, B)\} \\
&= \{x \in A+B / x+A = A \text{ and } x+B = B\} \\
&= \{x \in A+B / x \in A \text{ and } x \in B\} = A \cap B
\end{aligned}
$$

Hence g is homomorphism from $A+B$ onto $\frac{A+B}{A} \times \frac{A+B}{B}$ with kernel $A \cap B$, then by first isomorphism theorem we get

$$\frac{A+B}{A \cap B} \simeq \frac{A+B}{A} \times \frac{A+B}{B} \qquad (18.11.1)$$

From (i), we have $\frac{A+B}{B} \simeq \frac{B}{A \cap B}$ and $\frac{A+B}{B} \simeq \frac{A}{A \cap B}$ then the equation (18.11.1) becomes

$$\frac{A+B}{A \cap B} \simeq \frac{B}{A \cap B} \times \frac{A}{A \cap B}$$

If $R = A+B$ then we have

$$\frac{R}{A \cap B} \simeq \frac{R}{A} \times \frac{R}{B}$$

11.12 Summary

In this lesson we defined external direct product and also established equivalent conditions which determines the external direct product.

11.13 Glossary

Direct sum, External direct product.

LESSON-12

MAXIMAL,PRIME AND NILPOTENT IDEALS

12.1 Introduction : In this lesson we study and characterise maximal,prime ideals and simple rings.Further we introduced the notions of nilpotent and nil ideals. Moreover using Zorn's lemma, we prove an existence theorem for maximal ideal.

12.2 Co-maximal Ideal

12.2.1 Definition : Two ideals $A,\ B$ in any ring R are called co-maximal if $A + B = R$.

12.2.2 Example : If $A = (p_1^{e_1})$ and $B = (p_2^{e_2})$ are ideals in Z generated by $p_1^{e_1}$ and $p_2^{e_2}$ respectively, where $p_1,\ p_2$ are distinct primes and $e_1,\ e_2$ are positive integers then $A + B = Z$. Hence $A,\ B$ are co-maximal ideals in Z.

12.3 Maximal Ideal

12.3.1 Definition : An ideal A in a ring R is called maximal ideal if (i) $A \neq R$ and (ii) For any ideal $B \supseteq A$ either $B = A$ or $B = R$

i.e., An ideal A in a ring R is called a maximal ideal if $A \neq R$ and if for any ideal B in R such that $A \subset B \subset R$ then either $B = A$ or $B = R$.

12.3.2 Theorem : An ideal A in a ring R is maximal ideal if and only if for all ideals $X \not\subset A$. the pair $X,\ A$ is co-maximal.

Proof. Let A be a maximal ideal of R. Let X be any ideal in R.

If $X \subset A$ then $X + A = A$ and the pair X, A is not co-maximal.

Suppose $X \not\subset A$ then $X + A$ is an ideal in R and $A \subset X + A \subset R$.

Since A is maximal ideal we get $X + A = A$ or $X + A = R$.

Since $X \not\subset A$ we get $X + A = R$. Therefore $X,\ A$ are co-maximal.

Conversely assume that $X,\ A$ are co-maximal for all $X \not\subset A$ then $X + A = R$.

Let B be any ideal in R such that $A \subset B \subset R$

we have either $B = A$ or $B = R$.

If $B \neq A$ then $B \not\subset A$ and $B + A = B$, since $A \subset B$.

But we have $B + A = R$ as $B,\ A$ are co-maximal.

Therefore $B = R$. Hence A is maximal ideal.

12.3.3 Theorem : For any ring R and any ideals $A \neq R$. The following are equivalent.

(i) A is maximal.

(ii) The quotient ring R/A has no nontrivial ideals.

(iii) For any element $x \in R$, $x \notin A$, $A + (x) = R$.

Proof. Suppose A is an ideal in a ring R and $A \neq R$.

(i)$\Rightarrow$ (ii)

Assume that (i) is true. We know that the ideals of R/A are of the from B/A, where B is an ideal in R containing A. Thus we have $A \subset B \subset R$. Since A is maximal ideal we have $A = B$ or $B = R$.

Therefore B/A is either A or R/A.

If B/A is non zero then $B \neq A$ i.e., $A \subseteq B$ and $B \neq A \Rightarrow B = R$, since A is maximal ideal then B/A=R/A.

Hence R/A has only two ideals, they are zero ideal and R/A itself.

(ii)$\Rightarrow$(iii)

Assume that(ii) is true. Let R/A has no non trivial ideals . Let $x \in R$ and $x \notin A$ then $A + (x) \neq A$ and $A + (x)$ is an ideal of R properly containing A. Therefore, $A + (x)/A$ is an ideal of R/A and it is non zero ideal in R/A.

$$\Rightarrow A + (x)/A = R/A \qquad \text{(by (ii))}$$

$$\Rightarrow A + (x) = R$$

(iii)$\Rightarrow$ (i)

Assume that (iii) is true. We have for any $x \in R$, $x \notin A$, $A + (x) = R$

Let us assume that $A \subset B \subset R$.

If $B = A$ then A is maximal ideal and there is nothing to prove.

If $B \neq A$, choose an element $x \in B$, $x \notin A$ then $A + (x) = R$ (by(iii)).

Also since $A \subset B$, $x \in B$, where B is an ideal

$$\Rightarrow A + (x) \subset B$$

$$\Rightarrow R \subseteq B \text{ and we have } B \subset R. \text{ Hence } B = R.$$

Therefore A is maximal ideal.

12.4 Simple Ring

12.4.1 Definition : A ring R is called a simple ring if the only ideals of R are the zero ideal and R itself (i.e., R has no nontrivial ideals.)

12.4.2 Example : (i) Every field is a simple ring.

(ii) A commutative simple ring with unity must be a field.

12.4.3 Theorem : In a non-zero commutative ring with unity then an ideal M is maximal ideal if and only if R/M is a field.

i.e., Let R be a commutative ring with unity then an ideal M in R is maximal ideal if and only if R/M is a field.

Proof. Let R be a non-zero commutative ring with unity then for any ideal M in R we have R/M is a commutative ring with unity,

where $R/M = \bar{R} = \{a + M | a \in R\} = \{\bar{a} | a \in R\}$ and $\bar{1} = 1 + M$.

Let M be maximal ideal then by previous theorem R/M has no non-trivial ideal $\Rightarrow R/M$ is simple ring.

Let $\bar{a}$ be any nonzero element in $\overline{R} = R/M$ then $\overline{a}\overline{R}$ is a nonzero ideal in $\overline{R}$. Since $\overline{R}$ has no non-trivial ideals we get $\overline{a}\overline{R} = \overline{R}$. ($aR$ is an ideal of R and

$\bar{a}\overline{R}$ is an ideal of $\overline{R}$)

Now $\bar{1} \in \overline{R} = \bar{a}\overline{R}$ there exists $\bar{b} \in \overline{R}$ such that $\bar{a}\bar{b} = \bar{1}$

Since $\overline{R}$ is commutative we have $\bar{b}\bar{a} = \bar{1} = \bar{a}\bar{b}$

Thus every nonzero element of $\overline{R}$ is invertible in $\overline{R}$. Hence $\overline{R}$ is a field.

Conversely assume that $\overline{R}$ is a field then $\overline{R}$ is a simple ring.

To prove that M is maximal ideal.

Let K be any ideal in R such that $M \subset K \subset R$.

If $K = M$ then there is nothing to prove.

If $K \neq M$ then K/M is an ideal in $\overline{R} = R/M$.

But $\overline{R}$ has only trivial ideal and K/M is non zero ideal of R/M.

Therefore $K/M = R/M \Rightarrow K = R \Rightarrow M$ is maximal ideal in R.

12.4.4 Example : An ideal M in the ring if integer Z is a maximal ideal if and only if $M = (p)$, where p is some prime number.

Sol. We know that Z is Principal ideal ring then every ideal M in Z is of the form (n), for any integer n. Further $(n) = (-n)$. Therefore, we may assume that n is non negative integer.

Suppose $M = (n)$ is a maximal ideal in Z then $Z/(n)$ is a field.

To prove that n is prime number.

Assume that n is a composite number.

Let $n = n_1 n_2$, where $n_1 > 1, n_2 > 1$ and $n_1 < n,\ n_2 < n$ then

$\bar{n} = \overline{n_1 n_2} = \overline{n_1}\ \overline{n_2} = \bar{0}$ (since $\bar{n} = \bar{0}$ is zero in $Z/(n)$)

$\Rightarrow \overline{n_1}, \overline{n_2}$ are zero divisors in $Z/(n)$, where $\overline{n_1} \neq \overline{0}$, $\overline{n_2} \neq \overline{0}$

which is a contradiction to $Z/(n)$ is a field. Therefore n is a prime number

Conversely assume that $M = (p)$ is an ideal in Z, where p is prime number, then $Z/(p) = Z_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ is a commutative ring with unity.

Let $\bar{a} \in Z/(p)$ and $\bar{a} \neq \bar{0}$ then a is not multiple of $p \Rightarrow p$ does not divides a i.e., $(p, a) = 1$ and there exist $x, y \in Z$ such that $ax + py = 1$

$$\Rightarrow \overline{ax + py} = \bar{1}$$

$$\Rightarrow \bar{a}\bar{x} + \bar{p}\bar{y} = \bar{1}$$

$$\Rightarrow \bar{a}\bar{x} = \bar{1} \qquad (\text{since } \bar{p} = \bar{0})$$

$\Rightarrow \bar{a}$ is invertible in $Z/(p)$. Thus every non zero element in $Z/(p)$ is invertible. Hence $Z/(p)$ is a field. Thereofere $M = (p)$ is a maximal ideal.

12.4.5 Example : If R is the ring of 2×2 matrices over a field F of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, where $a,\ b \in F$ then the set $M = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b \in F \right\}$ is a maximal ideal in R.

Sol. $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a, b \in F \right\} = \begin{pmatrix} F & F \\ 0 & 0 \end{pmatrix}$ is a ring, where F is a field.

Let $M = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b \in F \right\} = \begin{pmatrix} 0 & F \\ 0 & 0 \end{pmatrix}$ is an ideal of R.

Let $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in F \right\} = \begin{pmatrix} F & 0 \\ 0 & 0 \end{pmatrix}$ then S is a subring of R.

Let $f : S \to F$ defined by $f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \right) = a$ then f is homomorphism, one-one and onto $\Rightarrow S \backsimeq F$. Since F is a field then S is also field.

Further $g : R \to S$ defined by $g\left(\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \right) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ then g is onto homomorphic. Now

$$ker\ g = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R \middle| g\left(\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \right) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

$$= \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

$$= \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a = 0 \right\}$$

$$= \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| b \in F \right\} = M.$$

Then by the fundamental theorem of homomorphism we get $R/M \simeq S$. Since S is a field then R/M is field. Hence M is a maximal ideal in R.

12.5 Product of Ideals

12.5.1 Definition : Let A and B be right (left) ideals in a ring R then the set

$$\left\{ \sum_{finite\ sum} a_i b_i \middle| \ a_i \in A,\ b_i \in B \right\}$$

which is a right (left) ideal in R is called the product of A and B and written as AB.

12.5.2 Note : (i) If A and B are right ideals in R. then their product AB is a right ideal in R.

(ii) If A and B are ideals in R then $A \cap B$ is also an ideal in R.

12.5.3 Theorem : LetA, B and C be right (left) ideals in a ring R then

(i) $(AB)C = A(BC)$

(ii) $A(B + C) = AB + AC$ and $(B + C)A = BA + CA$.

Proof.(i) Follows from the associativity of multiplication in R.

(ii) Clearly $AB, AC \subset A(B + C)$.

Also if $a \in A,\ \ b \in B,\ \ c \in C$ then $a(b + c) = ab + ac \in AB + AC$

Hence $AB + AC = A(B + C)$.

12.5.4 Definition : If $A_1, A_2, \ldots, A_n$ are right (left) ideals in a ring R then their product is denoted by $A_1A_2\ldots A_n$ and defined as

$$A_1A_2\ldots A_n = \left\{ \sum_{finite\ sum} a_1a_2\ldots a_n \middle| a_i \in A_i,\ i = 1, 2, \ldots n \right\}$$

12.5.5 Definition : If $A_1 = A_2 = \ldots = A_n$ then their product is A^n.

12.5.6 Note : (i) If p is prime number and p/ab then p/a or p/b.

(ii) If $ab \in (p)$ then $a \in (p)$ or $b \in (P)$.

Equivalently if $(a)(b) \subseteq (ab) \subset (p)$ then $(a) \subset (p)$ or $(b) \subset (p)$.

12.6 Prime Ideal

12.6.1 Definition : An ideal P in a ring R is called a prime ideal if $P \neq R$ and has the following property.

If A and B are ideals in R such that $AB \subseteq P$ then either $A \subseteq P$ or $B \subseteq P$.

12.6.2 Theorem : If R is a ring with unity then each maximal ideal is prime ideal.

Proof. Let M be any maximal ideal in R.

Let A, B are two ideals in R such that $AB \subseteq M$.

If $A \subseteq M$ then M is a prime ideal.

Suppose $A \not\subset M$ then $\exists$ an element $a \in A$ and $a \notin M \Rightarrow M + (a) = R$.

But $a \in A \Rightarrow (a) \subseteq A$ $\quad$ ($\because$ A is an ideal)

$\Rightarrow M + (a) \subseteq M + A$

$\Rightarrow R \subseteq M + A$, but $M + A \subseteq R$ always. Therefore $M + A = R$

Since $1 \in R \Rightarrow 1 \in M + A \Rightarrow 1 = m + a$, for some $a \in A,\ m \in M$

(since $A \not\subset M$ then $A,\ M$ are co maximal ideals and $A + M = R$)

Let $b \in B$ then $b = mb + ab \in M$ (since $m \in M$ and M is ideal $\Rightarrow mb \in M$ and $ab \in AB \subseteq M \Rightarrow ab \in M \Rightarrow mb + ab \in M$)

$\Rightarrow b \in M$.

$\Rightarrow B \subseteq M$. Hence M is a prime ideal in R.

12.6.3 Note : The converse of the above theorem is not true in general.

12.6.4 Example : The ideal (0) in the ring of integers Z is prime ideal but not maximal ideal.

Sol. Let $a,\ b \in Z$ and $ab \in (0) \Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$

$\Rightarrow (a) = (0)$ or $(b) = (0) \Rightarrow (0)$ is a prime ideal but not maximal ideal, since $(0) \subset (x) \subset Z$ for any $x \in Z$ where $x \neq 0$.

For example $(0) \subset (2) \subset Z$.

12.6.5 Theorem : If R is a commutative ring then prove that an ideal P in R is prime ideal iff $ab \in P,\ a \in R,\ b \in R \Rightarrow\ a \in P$ or $b \in P$.

Proof. We have R is a commutative ring and P is an ideal in R, $P \neq R$. Suppose P is a prime ideal in R (i.e., $P \neq R$) and if A, B are ideals in R such that $AB \subseteq P$ then $A \subseteq P$ or $B \subseteq P$. Let $ab \in P$, where $a,\ b \in R$.

Since R is a commutative ring, we have $(a) = \{na + ar/n \in Z,\ r \in R\}$

$(b) = \{mb + bs/m \in Z, s \in R\}$

Now $(a)(b) = \{ \sum\limits_{finitesum} xy \big| x \in (a),\ y \in (b)\}$

The element $xy = (na + ar)(mb + bs)$

$$= nmab + nabs + mabr + abrs$$

Since P is prime ideal and $ab \in P$ and $r,\ s \in R$

$\Rightarrow xy \in P$ (The finite sum of such element also belongs to P)

$(a)(b) \subseteq P \Rightarrow (a) \subseteq P$ or $(b) \subseteq P$ (P is prime ideal)

$\Rightarrow a \in P$ or $b \in P$ (since $ab \in P$ and P is an ideal R we get $(na + ar)(mb + bs)$ or finite sum of such products are in P)

Conversely assume that $ab \in P,\ a,\ b \in R \Rightarrow a \in P$ or $b \in P$

Let A and B be ideals in R such that $AB \subseteq P$.

If $A \subseteq P$ then P is prime ideal.

Suppose $A \not\subseteq P$, there exists an element $a \in A$ such that $a \notin P$ then for each $b \in B$, we have $ab \in AB \subseteq P \Rightarrow ab \in P \;\; \forall \;\; b \in B$

But by our hypothesis $b \in P$ (since $a \notin P$)

$\Rightarrow B \subseteq P$ ($ab \in P \Rightarrow a \in p$ or $b \in P$)

Thus $AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$.

Hence P is a prime ideal.

12.6.6 Example : In an integral domain R prove that the ideal $\{0\}$ is prime ideal.

Sol. Let R be an integral domain

If $ab \in (0)$, $a,\; b \in R$ then $ab = 0 \Rightarrow a = 0$ or $b = 0$ (R has no zero divisors)

$\Rightarrow a \in (0)$ or $b \in (0)$. Hence (0) is a prime ideal in R.

12.6.7 Example : A commutative ring R is an integral domain iff (0) is a prime ideal.

Sol. Let R be a commutative ring.

If R is an integral domain then (0) is a prime ideal.

Suppose (0) is a prime ideal.

Thus if $ab \in (0)$, $a,\; b \in R$ then either $a \in (0)$ or $b \in (0)$

$\therefore ab = 0 \Rightarrow a = 0$ or $b = 0$

$\Rightarrow R$ has no zero divisors. Hence R is an integral domain.

12.6.8 Example : For each prime integer p prove that the ideal (p) in the ring of integers Z is prime ideal.

Sol. For $a,\; b \in Z$, Let $ab \in (p)$ then $p/ab \Rightarrow p/a$ or p/b

$\Rightarrow a \in (p)$ or $b \in (p)$. Hence (p) is a prime ideal.

12.6.9 Theorem : Let R be a commutative principle ideal domain with unity then prove that any non zero ideal $P \neq R$ is prime ideal iff P is a maximal ideal.

Proof. Let R be commutative principal ideal domain with unity.

Let $P \neq R$ be any nonzero prime ideal in R and $ab \in P \Rightarrow a \in P$ or $b \in P$.

Suppose P is not maximal ideal then there exists an ideal M in R such that $P \subset M \subset R \Rightarrow P \neq M$ and $M \neq R$. Since R is a principal ideal domain we have $M = bR$ for some $b \in R$ and $P = aR$, $a \in R$.

Thus $aR \subset bR$ and $aR \neq bR$

This implies $a \in P$ and $a = bx$ for some $x \in R$ and $b \notin P = aR$.

Since P is a prime ideal, $a = bx \in P$, $b \notin P \Rightarrow x \in P$

Then $x = ay$ for some $y \in R$

Now $a = bx = bay \Rightarrow a(1 - by) = 0$

Since $a \neq 0$ and R is principal ideal domain we get $1 - by = 0$

$\Rightarrow 1 = by \in M = bR$

$\Rightarrow 1 \in M$

$\Rightarrow M = R$ which is a contradiction. Hence P is a maximal ideal.

OR

Let R be a commutative principal ideal domain with unity.

Let $P \neq R$ be any nonzero prime ideal of R then $P = (a)$ for some $a \in R$

$\Rightarrow P = aR$ $\qquad\qquad (P = (a) = \{ar/r \in R\} = aR)$

If possible, let P be not maximal ideal then there exists an ideal M such that $P \subseteq M \subseteq R \Rightarrow M \neq P$ and $M \neq R$

Since M is a principal ideal then $M = aR$, for some $b \in R$, where $bR \neq aR$ and $bR \neq R$.

$P \subset M \Rightarrow aR \subset bR$

$\Rightarrow a \in bR$

$\Rightarrow a = bx$, for some $x \in R$

Also $\quad bR \nsubseteq aR \qquad$ (If $bR \subseteq aR$ and $aR \subseteq bR \Rightarrow aR = bR$)

$\Rightarrow b \notin aR$.

But $aR = P$ is a prime ideal and

$a \in P \Rightarrow bx \in P$

$\Rightarrow x \in P \qquad (b \notin aP = P)$

$\Rightarrow x = ay,\quad$ for some $y \in R \qquad (P = aR)$

$\Rightarrow x = bay = aby$

$\Rightarrow a(1 - by) = 0$

$\Rightarrow 1 - by = 0 \qquad (a \neq 0)$

$\Rightarrow by = 1 \qquad$ (R is integral domain)

$\Rightarrow 1 \in M$

$\Rightarrow M = R$ which is a contradiction to $M \neq R$

$\Rightarrow P$ is a maximal ideal.

Conversely let P be a maximal then P is prime ideal (by previous theorem).

12.6.10 Example : Let R be a commutative ring with unity in which each ideal is prime ideal then prove that R is a field.

Proof. Suppose R is a commutative ring with unity in which each ideal is a prime ideal. In particular (0) is a prime ideal in R.

Let $a,\ b \in R$ and $ab = 0 \Rightarrow ab \in (0) \Rightarrow a \in (0)$ or $b \in (0)$

$\therefore$ R has nonzero divisors and so R is an integral domain.

Let $a \in R$ and $a \neq 0$ then

$(a)(a) = \{ \sum\limits_{finitesum} r_1 a . r_2 a / r_1, r_2 \in R \} = \{ r^2 a^2 /\ r \in R \} = (a^2)$

But (a^2) is a prime ideal, therefore $(a) \subseteq (a^2)$. It is easy to see that $(a^2) \subseteq (a)$

Thus we get $(a) = (a^2) \Rightarrow a \in (a^2)$

$\Rightarrow a = a^2x$, for some $x \in R$

$\Rightarrow a(1 - ax) = 0$

$\Rightarrow 1 - ax = 0$ (since $a \neq 0$, R is an integral domain)

$\Rightarrow ax = 1$

$\Rightarrow a$ has an inverse in R.

Thus every non zero element of R is invertible in R, Hence R is a field

12.6.11 Example : Let R be a Boolean ring then prove that each prime ideal $P \neq R$ is maximal ideal.

Proof. Suppose R is a Boolean ring then $x^2 = x \ \forall\, x \in R$ and R is commutative ring. Let $P \neq R$ be a prime ideal in R

Consider the quotient ring R/P then R/P is also commutative.

We first show that R/P is an integral domain.

Let $a,\ b \in R$. Since P is prime ideal we have $ab \in P \Rightarrow a \in P$ or $b \in P$.

Thus if $\overline{ab} = \bar{0}$ then $\bar{a}\bar{b} = 0 \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

(since $a \in P$ or $b \in P \Rightarrow a + P = P$ or $b + P = P \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$)

where $\bar{x} = x + P \in R/P$ and $\bar{0} = 0 + P = P$.

Therefore R/P has no zero divisors. Hence R/P is an integral domain.

For all $x \in R$, we have

$(\bar{x})^2 = (x + P)(x + P) = x^2 + P = x + P = \bar{x}$ $(x^2 = x)$

$\therefore R/P$ is a Boolean ring.

But every integral domain has only idempotent element 0 and possibly 1

$\therefore R/P = \{\bar{0}\}$ or $R/P = \{\bar{0}, \bar{1}\}$

If $R/P = \{\bar{0}\} \Rightarrow R = P$ which is not true (since $P \neq R$)

$\therefore R/P$=$\{\bar{0},\bar{1}\}$ is finite integral domain

$\Rightarrow R/P$ is field. Hence P is maximal ideal.

(OR)

Consider R/P where P is a prime ideal and $P \neq R$

Then $ab \in P \Rightarrow a \in P$ or $b \in P$

i.e., $ab + P = P \Rightarrow a + P = P$ or $b + P = P$

$\Rightarrow \bar{a}\bar{b} = 0 \Rightarrow \bar{a} = \bar{0}$ or $\bar{b} = \bar{0}$

R/P is an integral domain

Also for all $x \in R$ we have

$(x + P)^2 = (x + P)(x + P) = x^2 + P = x + P \;\; \forall\, x \in R$ since $(x^2 = x)$

$\therefore (x + P)^2 = (x + P)$ for all $x + P \in R/P$

$\Rightarrow R/P$ is a Boolean ring and also an integral domain.

We know that an integral domain has no idempotent element except zero and possibly unity.

$R/P = \{\bar{0}\}$ or $R/P = \{\bar{0},\bar{1}\}$

(In an integral domain $x^2 = x \Rightarrow x(1 - x) = 0 \Rightarrow x = 0$ or $x = 1$)

If $R/P = \{0\} \Rightarrow R = P$ which is a contradiction to $P \neq R$

$\therefore R/P = \{\bar{0},\bar{1}\}$ is finite integral domain

$\therefore R/P$ is field $\Rightarrow P$ is maximal ideal.

12.6.12 Example : Let a be a non nilpotent element in a ring and let $S = \{a, a^2, a^3, \ldots\}$. Suppose P is maximal ideal in the family F of all ideals in R that are disjoint from S then P is a prime ideal.

(Note that the statement dose not say that P is maximal ideal in R precisely, it means that there does not exist any ideal $X \in F$ such that $X \supsetneq P$).

Sol. Let $AB \subseteq P$ where A and B are ideals in R.

If possible let $A \not\subset P$ and $B \not\subset P$ then $A+P \supset P$ and $B+P \supset P$.

By maximality of P we have $(A+P) \cap S \neq \Phi$ and $(B+P) \cap S \neq \Phi$.

Thus there exist positive integers i and j such that $a^i \in A+P$ and $a^j \in B+P$ then $a^i a^j \in (A+P)(B+P) = AB + AP + BP \subseteq P$ because $AB \subseteq P$ and P is an ideal in R. Thus $P \cap S \neq \Phi$ is a contradiction.

Hence $AB \subseteq P \Rightarrow$ either $A \subseteq P$ or $B \subseteq P$. Therefore P is a prime ideal.

12.6.13 Example : Let $R = C[0,1]$ be the ring of all real-valued continuous functions on the closed unit integral. If M is a maximal ideal of R then there exists a real number γ, $0 \leq \gamma \leq 1$ such that $M = M_\gamma = \{f \in R \ / \ f(\gamma) = 0\}$ and conversely.

Sol. Let M be a maximal ideal of $C[0,1]$.

We claim that there exist $\gamma \in [0,1]$ such that $f(\gamma) = 0$ for all $f \in M$. Otherwise for each $x \in [0,1]$ there exist $f_x \in M$ such that $f_x(x) \neq 0$. Because f_x is continuous there exists an open integral say I_x such that $f_x(y) \neq 0$ for all $y \in I_x$. Clearly $[0,1] = \bigcup\limits_{x \in [0,1]} I_x$. By the Heine-Borel theorem in analysis there exists a finite subfamily say $I_{x_1}, I_{x_2}, \ldots I_{x_n}$ of this family of open integrals I_x, $x \in [0,1]$ such that $[0,1] = I_{x_1} \cup I_{x_2} \cup \ldots \cup I_{x_n}$

Consider $f = \sum\limits_{i=1}^{n} f_{x_i}^2$ and suppose $f(z) = 0$ for some $z \in [0,1]$.

Now $[0,1] = \bigcup\limits_{i=1}^{n} I_{x_i}$ implies that there exists I_{x_k} such that $z \in I_{x_k}$ $(1 \leq k \leq n)$ then $f_{x_k}(z) \neq 0$. But $f(z) = 0 \Rightarrow \sum (f_{x_i}(z))^2 = 0 \Rightarrow f_{x_k}(z) = 0$ is a contradiction. Thus $f(z) \neq 0$ for any $z \in [0,1]$ which is in turn yields that f is invertible and $M = C[0,1]$ which is not true.

Conversely, we show that M_γ is a maximal ideal of $C[0,1]$ for any $\gamma \in [0,1]$. It is easy to cheek that M_γ is an ideal. To see that it is maximal ideal, we note that $C[0,1]/M_\gamma$ is a field isomorphic to R.

Alternatively, we may proceed as follows

Let J be an ideal of $C[0,1]$ properly containing M_γ.

Let $g \in J, \quad g \notin M_\gamma$ then $g(\gamma) \neq 0$.

Let $g(\gamma) = \alpha$, then $h = g - \alpha$ is such that $h(\gamma) = 0$

i.e., $h \in M_\gamma$ so $\alpha = g - h \in J$. But $\alpha \neq 0$ implies that α is invertible. Consequently $J = R$ which proves the converse.

12.7 Nilpotent Ideal

12.7.1 Definition : A right (left) ideal A in a ring R is called nilpotent ideal if $A^n = (0)$, for some positive integer n.

12.7.2 Example : (i) In any ring R the zero ideal $A = (0)$ is nilpotent ideal

(ii) The ideal $A = \{\bar{0}, \bar{2}\}$ is not zero a ideal in a ring $R = Z/ < 4 >$, but it is nilpotent ideal.

Since $A^2 = A.A = \{\bar{0}, \bar{2}\}\{\bar{0}, \bar{2}\} = \{\bar{0}, \bar{0}, \bar{0}, \bar{0}\} = (0) \Rightarrow A^2 = (0)$

(iii) The ideal $A = \begin{pmatrix} 0 & Z \\ 0 & 0 \end{pmatrix}$ is a nilpotent ideal in a ring $R = \begin{pmatrix} Z & Z \\ 0 & Z \end{pmatrix}$ of 2×2 upper triangular matrices. Since $A^2 = A.A = 0_{2\times 2} = (0)$.

12.7.3 Note : (i) Every zero ideal is a nilpotent ideal but converse need not be true.

ii) Every element in a nilpotent ideal is a nilpotent element but converse need not be true.

(iii) The set of nilpotent elements in ring R is not necessarly form a nilpotent ideal (this set may not be an ideal).

(iv) A ring R may have nonzero nilpotent element but it may not posses a nonzero nilpotent ideal.

12.7.4 Example : Let $R = F_n$ be the ring of $n \times n$ matrices over field F then R has nonzero nilpotent elements such as e_{ij}, $i \neq j$, $1 \leq i, j \leq n$.

Sol. Let I be a nilpotent right ideal in R with $I^k = (0)$, where k is some positive integer then consider the ideal

$$\underbrace{(RI)(RI)\ldots(RI)}_{k \quad \text{times}} = R\underbrace{(IR)\ldots(IR)}_{(k-1) \quad \text{times}} I \subseteq R\underbrace{I\ldots\ldots I}_{(k-1) \quad \text{times}} I = RI^k = (0).$$

Hence RI is a nilpotent ideal in R. But we know that the ring $R = F_n$ has no nontrivial ideal then $RI = (0)$ or $RI = R$.

Since R has unity $\neq 0$ then $RI \neq R$. Therefore $RI = (0)$ only.

For any $a \in I$ we have $a = 1a \in RI = (0) \Rightarrow a = 0$. Hence $I = (0)$

12.8 Nil Ideal

12.8.1 Definition : A right (left) ideal A in a ring R is called a nil ideal if each element of A is a nilpotent element.

12.8.2 Note : Every nilpotent right (left) ideal is nil ideal but converse is not true.

12.8.3 Example : Let $R = \oplus \sum Z/(p^i)$, for $i = 1, 2, \ldots,$ be the direct sum of the rings $Z/(p^i)$, where p is prime number then R contains non zero nilpotent elements such as $(0 + (p), p + (p^2), 0 + (p^3) \ldots\ldots)$

Let I be the set of all nilpotent elements then I is an ideal in R because R is commutative, so I is a nil ideal. But I is not nilpotent ideal if $I^k = (0)$ for some positive integers $k > 1$ then the element

$x = (0 + (p), 0 + (p^2), \ldots, 0 + (p^k), p + (p^{k+1}), 0 + (p^{k+2}) \ldots\ldots)$ is nilpotent.

So $x \in I$. But $x^k \neq 0$ which is a contradiction.

Hence I is not nilpotent ideal.

12.9 Some Basic Definitions

12.9.1 Definition : (Partial Order) Let S be a nonempty set. A binary relation on S denotes by $\leqslant$ " is called a partial order on S if the following conditions are satisfied for all $a,\ b,\ c \in S$ (i) $a \leq a \ \forall\ a \in S$ (reflexive)

(ii) $a \leq b$ and $b \leq a \Rightarrow a = b$ (antisymmetric)

(iii) $a \leq b$ and $b \leq c \Rightarrow a \leq c$ (transitive)

12.9.2 Definition : (Poset or Partially Ordered Set) A poset is a system $(S, \leqslant)$ consisting of a nonempty set S and a partial order $\leqslant$ on S.

12.9.3 Definition : (Chain) A subset C of S is said to be a chain in a poset $(S, \leqslant)$ if for every $a,\ b \in C$ we have either $a \leqslant b$ or $b \leqslant a$.

12.9.4 Definition : (Upper Bound) An element $u \in S$ is said to be an upper bound of C if $a \leq u$ for every $a \in C$.

12.9.5 Definition : (Maximal Element) An element $m \in S$ is said to be a maximal element of poset $(S, \leq)$ if $m \leq a,\ a \in S$ then $m = a$.

We now state Zorn's lemma without proof. **12.9.6 Definition : (Zorn's Lemma)** If every chain C in a poset $(S, \leq)$ has an upper bound in S then $(S, \leq)$ has a maximal element.

12.10 Existence of Maximal Ideal

12.10.1 Theorem : If R is a nonzero ring with unity 1 and I is an ideal in R such that $I \neq R$ then there exist a maximal ideal M of R such that $I \subseteq M$.

Proof. Let R be a ring with unity and $I \neq R$ is an ideal in R.

Let S be the set of all ideals $X \neq R$ in R such that $I \subseteq X$ then $(S, \subseteq)$ is a partially ordered set under inclusion

(i) $A \subseteq A \ \forall\ A \in S$

(ii) $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$

(iii) $A \subseteq B$, $B \subseteq C \Rightarrow A \subseteq C$

Let C be only chain in S and $U = \bigcup\limits_{x \in C} X$ then $I \subseteq U$ and U is an upper bound of C.

To prove that U is an ideal : Let $a,\ b \in U$ then there exists ideals A, B in C such that $a \in A$ and $b \in B$. Since C is chain we have either $A \subseteq B$ or $B \subseteq A$ i.e., either $a,\ b \in A$ or $a,\ b \in B$

$\Rightarrow a - b \in A$ or $a - b \in B$ (since A, B are ideals)

$\Rightarrow a - b \in U$

Further $a \in U \Rightarrow a \in A$, for some $A \in C$

$\Rightarrow ar$ and $ra \in A,\ \forall\ r \in R$

$\Rightarrow ar$ and $ra \in U$

$\therefore U$ is an ideal in R.

If $U = R$ then $1 \in U$

$\Rightarrow 1 \in X$, for some $X \in C$

$\Rightarrow X = R$ which is a contradiction to $X \neq R$. Hence $U \neq R$.

If $I \subseteq X$ for all $X \in C \Rightarrow I \subseteq U \Rightarrow U \in S$ and also U is an upper bound for C. This shows that the chain C in a poset $(S, \subseteq)$ has an upper bound in S. Since C is arbitrary, we see that every chain in $(S, \subseteq)$ has an upper bound in S. Therefore by Zorn's lemma (21.14) we get $(S, \subseteq)$ has a maximal element say M

i.e., M is an ideal in R, $I \subseteq M$ and $M \neq R$.

Let N be an ideal in R such that $M \subset N \subset R$, $M \neq N$.

If $N \neq R$ then $N \in S$ (since $I \subseteq M \subset N \Rightarrow I \subset N$)

which is a contradiction to the maximality of M. Hence $N = R$

Therefore M is a maximal ideal in R.

12.11 Summary

In this lesson maximal ideals and prime ideals were characterised. Moreover we established an existence theorem for maximal ideals

12.12 Glossary

Maximal Ideal, Prime Ideal, Nilpotent Ideal, Nil Ideal, Poset, Chain, Zorn's lemma .

UNIT-IV

LESSON-13

UNIQUE FACTORISATION DOMAINS

13.1 **Introduction:** In this lesson we define unique factorisation domain. Further, we prove that every prime element is irreducible element in an Integral domain.

13.2 **Divisiblity:**

13.2.1 **Definition:** Let a and b be two nonzero elements in a commutative integral domain R with unity. We say that b divides a (or b is a divisor of a or a is divisible by b or a is multiple of b) if there exists an element $c \in R$ such that $a = bc$. If b divides a then we write $b \mid a$ or $a \equiv 0 (mod\text{b})$.

13.2.2 **Definition:** An element $u \in R$ is said to be unit in R if u has a multiplicative inverse in R i.e., an element u is a unit in R if there exists an element $v \in R$ such that $uv = 1$.

13.2.3 **Definition:** Two elements a , b in R are said to be an associates if there exist an unit $u \in R$ such that $a = bu$.

13.2.4 **Theorem:** Let R be a commutative integral domain with unity then

(i) an element $u \in R$ is a unit if and only if $u \mid 1$.

(ii) a, b are associates in R if and only if $a \mid b$ and $b \mid a$.

Proof. (i) If u is a unit in R then u is invertble, there exists $v \in R \ni uv = 1$. Therefore $u \mid 1$. Conversely if u is a divisor of 1 then there exists $v \in R \ni 1 = uv$ and hence u is a unit in R.

(ii) If a, b are associates in R then $a = bu$ for some unit $u \in R$. Thus $b \mid a$. If u is a unit in R there exists $v \in R \ni uv = 1$. Now $av = buv = b.1 = b$. Therefore $b = av \Rightarrow a \mid b$. Conversely, suppose $a \mid b$ and $b \mid a$. If $a \mid b$

$\Rightarrow b = ax$ for some $x \in R$. If $b \mid a \Rightarrow a = by$ for some $y \in R$. Now $b = ax = byx = bxy \Rightarrow b(1 - xy) = 0 \Rightarrow xy = 1$, where $a \neq 0$ and $b \neq 0$. Thus x and y are units. Therefore a, b are associates.

13.2.5 **Definition:** An element b in a commutative integral domain R with unity is called an improper divisor of an element a in R if b is either a unit or associate of a.

13.2.6 **Theorem:** Let R be a commutative integral domain with unity then

(i) $b \mid a$ if and only if $(a) \subset (b)$.

(ii) a and b are associates if and only if $(a) = (b)$.

(iii) u is a unit in R if and only if $(u) = R$.

Proof. (i) Suppose $b \mid a$. Then $a = br$ for some $r \in R$. Now $x \in (a) \Rightarrow x = as$ for some $s \in R$. Now $x = as = (br)s = b(rs) \in (b)$. Thus $(a) \subset (b)$.

(ii) a and b are associates $\iff$ $a \mid b$ and $b \mid a$ $\iff$ $(b) \subset (a)$ and $(a) \subset (b)$ $\iff$ $(a) = (b)$

(iii) u is a unit in R $\iff$ u is a divisor of 1 $\iff$ $(1) \subset (u)$ $\iff$ $R \subset (u)$ $\iff$ $(u) = R$ (since $(u) \subset R$).

13.2.7 **Definition:** A nonzero element a of an integral domain R with unity is said to be an irreducible element if (i) a is not a unit and (ii) every divisor of a is improper, i.e., $a = bc$, $b, c \in R \Rightarrow$ either b is a unit or c is unit (i.e., the only divisors of a are units and associates).

13.2.8 **Definition:** A nonzero element p of an integral domain R with unity is said to be a prime element if (i) a is not unit and (ii)if $p \mid ab$, $a, b \in R$, then either $p \mid a$ or $p \mid b$.

13.2.9 **Theorem:** Every prime element is an irreducible element in an integral domain R with unity.

Proof. Suppose p is a prime element in R. To prove that p is irreducible element. Let $p = bc$ for some $b, c \in R$.

$p = bc \Rightarrow p.1 = bc \Rightarrow p \mid bc \Rightarrow p \mid b$ or $p \mid c$ $\quad$ ($\therefore p$ is prime element)

If $p \mid b \Rightarrow b = px$ for some $x \in R$. Now $p = bc = pxc \Rightarrow xc = 1 \Rightarrow c$ is a unit.

If $p \mid c \Rightarrow c = py$ for some $y \in R$. Now $p = bc = bpy \Rightarrow by = 1 \Rightarrow b$ is a unit.

Therefore p is an irreducible element.

13.2.10 **Remark:** In an integral domain R with unity, every prime element is an irreducible element. But an irreducible element need not be prime element.

13.3 **Principal Ideal Domain:**

13.3.1 **Defintion:** A commutative integral domain R with unity is said to be principal ideal domain (PID) if each ideal in R is of the form $(a) = aR$, $a \in R$.

13.3.2 **Theorem:** Prove that an irreducible element in a commutative principal ideal domain (PID) is always a prime element.

Proof. Let R be a PID and let $p \in R$ is an irreducible element. Therefore p is not a unit. Suppose that $p \mid ab$, where $a, b \in R$. To show that either $p \mid a$ or $p \mid b$. Assume that $p \nmid a$. Consider (p) and (a) are ideals in R then $(p) + (a)$ is also an ideal in R. Since R is a PID then $(p) + (a)$ is a principal ideal in R. Therefore $(p) + (a) = (c)$, for some $c \in R$,

$p \in (p) \subseteq (p) + (a) = (c) \Rightarrow p \in (c)$.

$$\therefore p = cd \text{ for some } d \in R.$$

As p is irreducible, we have either c in a unit or d in a unit.

Assume that d is a unit then $p = cd \Rightarrow p, c$ are associates $\Rightarrow (p) = (c)$.

But $(p) + (a) = (c) = (p)$ $\quad$ ($\because A + B = A \Rightarrow B \subseteq A$)

$\Rightarrow (a) \subseteq (p)$

$a \in (a) \subseteq (p) \Rightarrow a = px$ for some $x \in R$. $\Rightarrow p \mid a$ which is a contradiction to d is unit.

Hence c is a unit. $(c) = R$.

Now $(a) + (p) = (c) \Rightarrow (a) + (p) = R$.

$1 \in R \Rightarrow 1 \in (a) + (p)$.

$\Rightarrow 1 = au + pu$, for some $uv \in R$.

$\Rightarrow b = b(au + pv) = abu + pbv$.. Therefore $abu + pbv = b$.

But $p \mid ab$ and $p \mid pb$. Therefore $p \mid abu + pbv = b \Rightarrow p \mid b$. Therefore p is an prime element.

13.4 **Unique factorisation domain (UFD)**

13.4.1 **Definition:** A Commutative integral domain R with unity is called a UFD if

(i) Every nonunit element in R is a finite product of irreducible factors.

(ii) Every irreducible element in R is a prime element.

13.4.2 **Theorem:** If R is a UFD, then the factorization of any (nonunit) element in R as a finite product of irreducible factors is unique up to order and unit factors.

Proof. Let R be a UFD. Let a be a nonunit in R, $a \neq 0$.

If a is irreducible, then $a = bc \Rightarrow$ either b or c is a unit.

The theorem is true in case a is irreducible. Suppose a is not irreducible then a can be written as a finite product of irreducible elements say $a = p_1 p_2 \dots p_n$, where p_j are irreducible elements in R.

Let $a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_n$, where p_i, q_j are irreducible (and also prime) we prove that $m = n$ and each p_i is an associate of some q_j. we prove this by using induction on m. If $m = 1$ then $a = p_1$ where p_1 is irreducible. Assume by induction hypothesis that the result is true for $m-1$ (factors). Now $p_1p_2\dots p_{m-1}p_m = q_1q_2\dots q_{n-1}q_n$.

$\Rightarrow p_m \mid q_1q_2\dots q_n$ (p_m is prime).

$\Rightarrow p_m \mid q_j$ for some j say $p_m \mid q_k$.

$q_k = u_1p_m$, q_k is irreducible.

$\Rightarrow u_1$ is a unit.

$$p_1p_2\dots p_{m-1}p_m = q_1q_2\dots q_{k-1}u_1p_mq_{k+1}\dots q_n.$$

Then ${p_m}^{-1}a = p_1p_2\dots p_{m-1} = u_1q_2q_3\dots q_{k-1}q_{k+1}\dots q_n$. ${p_m}^{-1}a \in R$.

Therefore By the induction hypothesis, we get $m-1 = n-1 \Rightarrow m = n$ and each p_i in a associate of some q_j. This complete the proof.

13.4.3 **Definition:** An element d in an commutative integral domain R with unity is called a greatest common divisor of $a, b \in R$ if

(i) $d \mid a, d \mid b$ and

(ii) if for $c \in R$, $c \mid a$ and $c \mid b$ then $c \mid d$.

It is denoted by $(a, b) = d$.

13.16 **Note:** (i) If d is a gcd of a, b then every associate of d is also a gcd.

(ii) If $d = (a, b)$ $u \in R$ is a unit, then ud is also gcd.

13.5 **PROBLEMS ON UNIQUE FACTORIZATION DOMAINS**

13.5.1 **Problem:** Suppose R is commutative integral domain with unity. Let $a, b, c \in R$ Then Prove the following:

(i) $c(a, b)$, (ca, cb) are associates.

(ii) $(a, b) = 1$, $a \mid c$, $b \mid c \Rightarrow ab \mid c$.

(iii) $(a, b) = 1$, $b \mid ac \Rightarrow b \mid c$.

(iv) $(a, b) = 1$, $(a, c) = 1 \Rightarrow (a, bc) = 1$.

Sol. (i) Let $(a, b) = d$, $(ca, ab) = e$.

$d \mid a, d \mid b \Rightarrow cd \mid ca,\ cd \mid cb.$

$\Rightarrow cd \mid e.$

$\Rightarrow e = cdx$ for some $x \in R$.

$e \mid ca, e \mid cb \Rightarrow cdx \mid ca.$

$\Rightarrow ca = cdxy$ for some $y \in R$.

$\Rightarrow a = dxy.$

$\Rightarrow dx \mid a$. similarly $dx \mid b$.

$dx \mid a,\ dx \mid b \Rightarrow dx \mid (a, b).$

$\Rightarrow cdx \mid c(a, b) = cd.$

$\Rightarrow e \mid cd.$

e, cd are associates.

(ca, cb), $c(a, b)$ are associates. $\therefore$ we can take $(ca, cb) = c(a, b)$.

(ii) Suppose $(a, b) = 1$, $a \mid c$, $b \mid c$.

$a \mid c \Rightarrow ab \mid bc.$

$b \mid c \Rightarrow ab \mid ac.$

$ab \mid ac,\ ab \mid bc.$

$\therefore ab \mid (ac, bc)\ ab \mid c(a, b)$

$\therefore ab \mid c. \quad [\because (a, b) = 1]$

(iii) Suppose $(a, b) = 1$.

$b \mid ac,\ b \mid bc$

$\therefore b \mid (ac, bc) = c(a, b) = c.$

$\therefore b \mid c.$

(iv) Let $(a, b) = 1$, $(a, c) = 1$ and $(a, bc) = d$.

To prove $d = 1$.

$$(a,bc)=d \Rightarrow d \mid a,\ d \mid bc$$
$$\Rightarrow d \mid ac,\ b \mid bc \Rightarrow d \mid (ac,bc)$$
$$\Rightarrow d \mid c(a,b) \Rightarrow d \mid c \quad (\because (a,b)=1)$$
$$d \mid a,\ d \mid c \Rightarrow d \mid (a,c)=1 \Rightarrow d=1.$$
$$\therefore (a,bc)=1$$

13.5.2 **Problem:** Show that $2+\sqrt{-5}$ is irreducible but not a prime in $Z[\sqrt{-5}]$.

Sol.$R=Z[\sqrt{-5}]=\{a+b\sqrt{-5}:a,b\in Z\}=\{a+b\sqrt{5}i:a,b\in Z\}$

It is clear that R is commutative integral domain with unity.

Define $N:R\to Z$ by $N(\alpha)=\alpha\bar{\alpha},\alpha\in R$, where $\alpha=a+i\sqrt{5}b$, $\bar{\alpha}=a-i\sqrt{5}b$.

Now $\alpha\bar{\alpha}=a^2+5b^2$

$$N(a+i\sqrt{5}b)=a^2+5b^2\in Z.$$

For $\alpha,\beta\in R$, we have

(i) $N(\alpha)\geq 0$, $N(\alpha)=0 \iff \alpha=0$.

(ii) $N(\alpha\beta)=N(\alpha)N(\beta)$.

(iii) α is a unit $\iff N(\alpha)=1$.

Let $\alpha=a+i\sqrt{5}b$, $\beta=c+i\sqrt{5}d$

$N(\alpha)=a^2+5b^2\geq 0$

$$N(\alpha)=0 \iff a^2+5b^2=0$$
$$\iff a=0,b=0$$
$$\iff \alpha=0$$

$$N(\alpha\beta)=(\alpha\beta)(\overline{\alpha\beta})=(\alpha\overline{\alpha})(\beta\overline{\beta})$$
$$=N(\alpha)N(\beta)$$

Suppose α is a unit , then $\exists\ \beta\ \in R\ \ni\ \alpha\beta=1$.

$\therefore N(\alpha\beta)=N(1)=1$

$N(\alpha)N(\beta) = 1$

$\therefore N(\alpha) \mid 1, N(\alpha) \geq 0.$

$N(\alpha) = 1.$

Suppose $N(\alpha) = 1 \Rightarrow \alpha\overline{\alpha} = 1 \Rightarrow \overline{\alpha} = \alpha^{-1}$

$\Rightarrow \alpha$ is a unit

$\therefore \alpha$ is a unit $\iff N(\alpha) = 1.$

We shall now find units of R.

Let $a + i\sqrt{5}b$ be a unit in R.

Then $a^2 + 5b^2 = 1$, $a, b \in Z$.

$\therefore b = 0$ and $a^2 = 1$ or $a = \pm 1$, $b = 0$.

$\therefore$ units are ± 1.

We now show that $2 + \sqrt{-5}$ is irreducible in R.

Let $2 + \sqrt{-5} = \alpha\beta$ for some $\alpha, \beta \in R$.

Let $\alpha = a + \sqrt{-5}b$, $\beta = c + \sqrt{-5}d$, $\quad a, b, c, d \in Z$.

$N(\alpha\beta)$=$N(2 + \sqrt{-5})$= $2^2 + 5.1^2 = 9$.

$N(\alpha)N(\beta) = 9.$

$N(\alpha) \mid 9 \Rightarrow N(\alpha) = 1$ or 3 or 9.

Claim: $N(\alpha) = 1$ or $N(\alpha) = 9$

i.e. $N(\alpha) \neq 3$.

Suppose if possible $N(\alpha) = 3$.

$$a^2 + 5b^2 = 3, \;\; a, b \in Z. \text{ ——————- } (1)$$

But thus equation has no solution in Z.

$\therefore N(\alpha) \neq 3$

$\therefore$ Either $N(\alpha) = 1$ or $N(\alpha) = 9 \Rightarrow N(\beta) = 1,$

$\Rightarrow$ Either α is a unit or β is a unit.

$\therefore 2+\sqrt{-5}$ is an irreducible element in R.

$$3, 3 \in R \qquad 3 \times 3 = 9.$$

$$(2+\sqrt{-5})(2-\sqrt{-5}) = 9.$$

$$\therefore 2+\sqrt{-5} \mid 3X3, \quad 3 \in R. \text{———}(2)$$

Claim: $2+\sqrt{-5} \mid 3$. Suppose if possible, $2+\sqrt{-5} \nmid 3$.

Then $\exists\ \alpha \in R \ni 3 = (2+\sqrt{-5})$

$$\therefore N(3) = N(\alpha)N(2+\sqrt{-5})$$

$$9 = N(\alpha) \times 9$$

$$\therefore N(\alpha) = 1 \ \alpha \text{ is a unit .}$$

$$\alpha = \pm 1.$$

$3 = \pm(2+\sqrt{-5})$, which is absurd.

$\therefore 2+\sqrt{-5} \nmid 3$, even though $2+\sqrt{-5} = 3 \times 3$, $3 \in R$.

$\therefore 2+\sqrt{-5}$ is not a prime.

$\therefore Z[\sqrt{-5}]$ is not a UFD.

13.5.3 **Problem:** Show that 3 is irreducible but not a prime in $Z[\sqrt{-5}]$.

13.5.4 **Problem:** Find gcd of $10+11i$, $8+i$ in $Z[i]$, where $Z[i] = \{a+bi : a, b \in Z\}$ is the ring of Gaussian integers.

LESSON-14

PRINCIPAL IDEAL DOMAIN AND EUCLIDEAN DOMAIN

14.1 Introduction : In this lesson we define Euclidean domain and also prove that every ED is a PID but not conversely

14.2 Theorem: Every commutative PID with unity is a UFD, but not conversely.

Proof.

Suppose R is a PID, R is commutative and $1 \in R$.

To prove that R is a UFD, we show that

(i) Every irreducible element in R is a prime.

(This one is already proved)

(ii) Every non-unit in R is a finite product of irreducible elements.

To prove (ii), we establish the following.

$\star$ R doesn't contain any infinite ascending chain of ideals.

Suppose $A_1 \subseteq A_2 \subseteq A_3 \subseteq \ldots \subseteq A_n \subseteq \ldots$ is an ascending chain of ideals in R. ———— (1)

R is a PID.

$\therefore$ Each A_i is a principal ideal, say $A_i = (a_i)$ for some $a_i \in R$.

i.e. $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots (a_n) \subseteq \ldots$.

Consider $A = \bigcup\limits_{n=1}^{\infty} A_n = \bigcup\limits_{n=1}^{\infty} (a_i)$.

Claim: A is an ideal.

Let $x, y \in A$, $r \in R$.

$x, y \in A = \cup A_n \Rightarrow x \in A_{n_1}, y \in A_{n_2}$ for some n_1, n_2.

But we have either $A_{n_1} \subseteq A_{n_2}$ or $A_{n_2} \subseteq A_{n_1}$.

$\therefore x, y \in A_{n_1}$ or A_{n_2}.

$x - y,\, rx \in A_{n_1}$ or A_{n_2}.

$\therefore x - y,\, rx \in A$

$\therefore A$ is an ideal in R.

But then A is a principal ideal. $\quad (\because R$ is a PID$)$

Let $A = (a)$ for some $a \in R$.

$a \in A = \cup A_n$.

$\Rightarrow a \in A_k$ for some k.

Now $a \in A_k$

$\Rightarrow (a) \subseteq A_k$

$\Rightarrow A \subseteq A_k$.

But $A_k \subseteq A$..

$\therefore A = A_k$.

$\therefore A_m = A$ for $m \geq k$.

$\therefore A_1 \subseteq A_2 \ldots \subseteq A_k = A = A \ldots . \therefore (1)$ is a finite ascending chain of ideals.

i.e., There are no infinite ascending chain of ideals in R. This proves $\star$.

We now prove (ii).

Let $a \in R$, be a nonzero non unit.

If a is irreducible, then we are done.

So suppose a is not irreducible.

Then $a = a_1 b_1$ for some $a_1, b_1 \in R$ such that neither a_1 nor b_1 is a unit.

If both a_1, b_1 are irreducible then a is a product of two irreducible elements.

So suppose a_1 is not irreducible, b, is irreducible.

$a = a_1, b_1 \Rightarrow a \in (a_1) \Rightarrow (a) \subseteq (a_1)$.

Then $a_1 = a_2 b_2$ where neither a_2 not b_2 is a unit

$$a = a_1,\, b_1 = a_2 b_2 b_1.$$

If both a_2, b_2 are irreducible then a is a product of their irreducible elements.

$$(a) \subsetneq (a_1) \subsetneq (a_2).$$

If this process continues indefinitely, we get an infinite ascending chain of ideals in R, which leads to a contradiction to $\star$.

$\therefore$ The process terminates after a finite number of steps, say k steps.

$a = a_1, b_1 \ldots a_k$, where each a_g is irreducible this prove (ii).

We now show that there are UFDs which are not such PIDs.

We know that every field F is a UFD.

(we prove "R is a UFD $\Rightarrow R(x)$ a UFD" later)

Then $F[x]$ is a UFD. $F[x, y] = F[x]F[y]$ is also a UFD.

Take $(x), (y)$ which are ideals in $F[x, y]$.

$(x) + (y)$ is an ideal in $F[x, y]$.

Claim: $(x) + (y)$ is not a principle ideal in $F[x, y]$.

suppose if possible $(x) + (y)$ is a principle ideal in $F[x, y]$ say $(x) + (y) = (f(x, y))$, for some $f(x, y) \in F[x, y]$.

$$x \in (x) \subseteq F[x, y] \Rightarrow x = f(x, y)c(x, y)$$

similarly $y = f(x, y)\ d(x, y)$ for some $c(x, y), d(x, y) \in F[x, y]$.

If $f(x, y)$ is a unit then $(x) + (y) = F[x, y]$ which is not true.

Also $f(x, y) \neq 0$.

$\therefore$ deg $f(x, y) \geq 1$.

$x = f(x, y)c(x, y)$.

$\Rightarrow c(x, y) =$const polynomial$=c$(say)

deg$f(x, y) = 1$.

Similarly $d(x, y) = d$ (a const p)

$$\therefore x = cf(x, y),\ y = df(x, y).$$

$$cy = dx.$$

But this is a contradiction to the fact that x, y are two distinct variables.

$\therefore (x) + (y)$ is an ideal in $F[x, y]$ which is not a principal ideal.

$\therefore F[x, y]$ is not a PID even though it is a UFD.

14.3 Euclidean Domain

14.3.1 Definition: Suppose R is a commutative integral domain with unity. If there is a function $\phi : R \to Z$ satisfying

(i) $a, b \in R - (0)$, $a \mid b \Rightarrow \phi(a) \leq \phi(b)$.

(ii) For $a, b \in R, b \neq 0 \ \exists \ q, r \in R \ \ni a = qb + r$, where either $r = 0$ or $\phi(r) < \phi(b)$.

Then R is called a Euclidean domain.

14.3.2 Theorem: Every Euclidean is a PID.

Proof. Suppose R is a ED with $\phi : R - (0) \to Z$.

To prove that R is PID.

Let A be an ideal in R.

If $A = (0)$, then there is nothing to prove.

So suppose $A \neq 0$. $\exists \ a \in A \ni a \neq 0$.

Consider $S = \{\phi(a) : a \in R, a \neq 0\} \subseteq Z$.

$$1 \mid a \ \ \forall \ a \neq 0.$$

$$\therefore \phi(1) \leq \phi(a).$$

$$\phi(1) \in S.$$

i.e. $S(\subseteq Z)$, which is bounded below.

$\therefore$ By the Well ordering principle, there is a least element in S, say $\phi(d)$.

Then $\alpha \in A$, $d \neq 0$, and $\phi(d) \leq \phi(a) \ \ forall \ a \neq 0 \in A$.

Claim: $A = (d)$

$$d \in A \Rightarrow (d) \subseteq A \text{ ————— } (1)$$

Let $x \in A$

$$\therefore x \in R, d \in R, d \neq 0$$

$$\therefore \exists\, q, r \in R \ni$$

$$x = qd + r,\ r = 0 \text{ or } \phi(r) < \phi(d).$$

Suppose if possible $r \neq 0$. Then $\phi(r) < \phi(d)$.

$x \in A$, $d \in A$, A ideal $\Rightarrow x, qd \in A$.

$$\Rightarrow x - qd \in A.$$

$$\Rightarrow r \in A.$$

$$\therefore r \neq 0,\ r \in A,\ \phi(r) < \phi(d).$$

$$\phi(r) \in S \text{ and } \phi(r) < \phi(d).$$

But this is a contradiction to the nature of $\phi(d)$.

$$\therefore r = 0.$$

$$x = qd \in (d)$$

$$\therefore x \in (d)$$

$$\therefore A \subseteq (d) \text{ ———— } (2)$$

(1) and (2) $\Rightarrow A = (d)$, a principal ideal.

$\therefore R$ is a PID.

14.3.3 Note: Every ED is a UFD.

ED $\Rightarrow PID \Rightarrow UFD$.

14.3.4 Example. Z is a ED (and hence Z is a UFD)

Define $\phi(a) = |a|\ \forall\ a \in Z$.

Let $a, b \in Z$, $a \neq 0, b \neq 0$ and $a \mid b$.

Then $b = ac$ for some $c \in Z$

$$|b| = |ac| = |a||c|$$

$\therefore |a| \leq |b|$

By the division algorithm in Z, we get for $a, b \in Z$, $b \neq Z$ $\exists$ unique $q, r \in Z \ni$

$$a = qb + r, \quad r = 0 \text{ or } 0 < r < |b|.$$

$$a = qb + r, \quad \phi(r) < \phi(b).$$

$\therefore Z$ is a ED.

14.3.5 Example. $Z[i]$, the ring of Gaussian integers is a ED.

Define $\phi : Z[i] \to Z$ by

$$\phi(a + ib) = a^2 + b^2 = (a + ib)(a - ib) \ \forall \ a + ib \in Z[i]$$

For each $\alpha \in Z[i]$, $\phi(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$.

Then

(i) $\phi(\alpha) \geq 0, \quad \phi(\alpha) = 0 \iff \alpha = 0.$

(ii) $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$

(iii) α is a unit $\iff \phi(\alpha) = 1.$

Sol.

(i) $\phi(\alpha) = |\alpha|^2 \geq 0, \phi(\alpha) = 0 \iff |\alpha| = 0 \iff \alpha = 0.$

(ii) $\phi(\alpha\beta) = |\alpha\beta|^2 = |\alpha|^2|\beta|^2 = \phi(\alpha)\phi(\beta).$

(iii) Suppose α is a unit.

$\exists \ \beta \in Z[i] \ni \alpha\beta = 1$

i.e. $\phi(\alpha\beta) = \phi(1) = 1$

$\phi(\alpha)\phi(\beta) = 1.$

$$\Rightarrow \phi(\alpha) \mid 1.$$

$$\Rightarrow \phi(\alpha) = 1.$$

Suppose $\phi(\alpha) = 1.$

$\Rightarrow |\alpha|^2 = 1. \Rightarrow \alpha\overline{\alpha} = 1.$

$\overline{\alpha} = \alpha^{-1} \in Z[i]$.

$\therefore \alpha$ is a unit.

Let $a + ib$ be a unit in $Z[i]$.

Then $a^2 + b^2 = 1$, $a, b \in Z$.

$\therefore (a = \pm 1 \text{ and } b = 0) \Rightarrow \pm 1$

or

$(a = 0, b = \pm 1) \Rightarrow \pm i$

$\therefore \pm 1, \pm i$ are the units in $Z[i]$.

Let $\alpha \mid \beta$.

$\Rightarrow \beta = \alpha r$, for some $r \in Z[i]$.

$\Rightarrow \phi(\beta) = \phi(\alpha)\phi(r)$.

$\Rightarrow \phi(\alpha) \mid \phi(\beta)$.

$\Rightarrow \phi(\alpha) \leq \phi(\beta)$.

Let $\alpha, \beta \in Z[i], \beta \neq 0$.

Consider $\alpha \mid \beta$, which may or may not lie in $Z[i]$.

Write $\alpha \mid \beta = a + ib$, $a, b \in R$.

$\alpha = (a + ib)\beta$.

Consider integers m, n such that

$|a - m| \leq \frac{1}{2}$, $|b - n| \leq \frac{1}{2}$.

We are sure to get such integers m, n.

Take $\gamma = m + in \in Z[i]$.

Then $\alpha = (a + ib)\beta$

$=((a - m) + i(b - n))\beta + \gamma\beta$.

Write $\delta = ((a - m) + i(b - n))\beta$.

Then $\alpha = \gamma\beta + \delta$, where $\alpha, \beta, \gamma \in Z[i]$.

$\Rightarrow \gamma\beta \in Z[i]$.

$\Rightarrow \alpha - \gamma\beta \in Z[i]$.

$\Rightarrow \delta \in Z[i]$.

Thus $\exists\ \gamma, \delta \in Z[i] \ni \alpha = \gamma\beta + \delta$.

$\phi(\delta) = |\delta|^2 = |(a-m) + i(b-n)\beta|^2$.

$=|(a-m) + i(b-n)|^2|\beta|^2$

$\leq (\frac{1}{4} + \frac{1}{4})|\beta|^2$.

$=\frac{1}{2}|\beta|^2 < |\beta|^2$

$= \phi(\beta)$

$\phi(\delta) < \phi(\beta)$.

$\therefore Z[i]$ is a Euclidean domain.

$\therefore Z[i]$ is a PID and hence a UFD.

14.3.6 Problems. Suppose R is a ED with $\phi : R \to Z$. Prove the following

(i) $b \neq 0 \Rightarrow \phi(0) < \phi(b)$.

(ii) a, b are associates $\Rightarrow \phi(a) = \phi(b)$.

(iii) $a \mid b$ and $\phi(a) = \phi(b) \Rightarrow a, b$ are associates.

Sol. (i) $b \neq 0$.

$\Rightarrow a, b \in R,\ b \neq 0$.

$\Rightarrow 0 = 0.b + 0$.

$\therefore \phi(0) < \phi(b)$.

(ii) Suppose a, b are associates.

$\Rightarrow a \mid b$ and $b \mid a$.

$\Rightarrow \phi(a) \leq \phi(b) \leq \phi(a)$.

$\Rightarrow \phi(a) = \phi(b)$.

(iii) Suppose $a \mid b$ and $\phi(a) = \phi(b)$.

Then to prove that $b \mid a$.

$\exists\ q, r \in R \ni a = bq + r$, where $\phi(r) < \phi(b)$.

Suppose if possible $r \neq 0$.

$a \mid b$.

$\Rightarrow b = ax$ for some $x \in R$.

$a = q(ax) + r$.

$\Rightarrow r = a(1 - qx)$.

$\Rightarrow a \mid r$.

$\Rightarrow \phi(a) \leq \phi(r) \leq \phi(b)$.

i.e. $\phi(a) < \phi(b) = \phi(a)$.

$\therefore \phi(a) < \phi(a)$, absurd.

$\therefore r = 0$.

$a = qb$ or $b \mid a$.

Thus $a \mid b$ and $b \mid a$.

$\Rightarrow a, b$ are associates.

14.4 Summary

In this lesson we have established that every ED ia a PID. Also $Z[i]$, the ring of Gaussian integers is a ED and hence a PID and UFD

14.5 Glossary

Euclidean domain, The ring of Gaussian integers.

LESSON-15

POLYNOMIAL RINGS OVER UNIQUE FACTORIZATION DOMAIN

15.1 Introduction : In this lesson we study Polynomial rings over a commutative integral domain. Also we prove that a polynomial ring over a UFD is also a PID

15.2 Polynomial Ring

15.2.1 Definition: Suppose R is a commutative ring. Then $R[x] = \{(a_0, a_1, a_2, \ldots) : a_i \in R\}$, the set of all finite sequences of members in R. $(a_0, a_1, a_2, \ldots)$ is a finite sequence we mean $a_i = 0 \; \forall \; i > k$ for some k.

For $(a_0, a_1, a_2, \ldots)$, $(b_0, b_1, b_2, \ldots) \in R[x]$, define

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1 + a_2 + b_2, \ldots)$$

$$(a_0, a_1, a_2, \ldots).(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots), \text{ where}$$

$$\begin{aligned} c_0 &= a_0b_0,\ c_1 = a_0b_1 + a_1b_0 \\ c_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &\vdots \\ c_r &= a_0b_r + a_1b_{r-1} + a_2b_{r-2} + \ldots + a_rb_0 \\ &\vdots \end{aligned}$$

Then $R[x]$ is a ring under these operations, called the polynomial ring over R in the variable x.

Suppose $(a_0, a_1, a_2, \ldots) \in R[x]$. Then $\exists \; k \ni (a_0, a_1, a_2, \ldots, a_{k-1}, a_k, 0, 0, 0, \ldots)$, $a_k \neq 0$

we denote the element by $a_0 + a_1x + a_2x^2 + \ldots + a_kx^k$ and this is a polynomial in x.

$$(a_0, a_1, a_2, \ldots, a_k, 0, 0, 0, \ldots) \rightarrow a_0 + a_1x + a_2x^2 + \ldots + a_kx^k$$

write $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_kx^k$, $a_k \neq 0$, $k > 0$.

a_k is called the leading coefficient of $f(x)$ and k is called the degree of the polynomial $f(x)$. If $a_i = 0 \, \forall \, i$, we call $f(x)$, the zero polynomial for which we does not assign any degree.

In case $f(x) = a_0$, $a_0 \neq 0$, $f(x)$ is called a constant polynomial and degree of $f(x)$ is taken as zero.

Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_kx^k$, $(a_k \neq 0)$

$f(x) = b_0 + b_1x + b_2x^2 + \ldots + b_kx^l$, $(b_l \neq 0)$

Then

$$f(x).g(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots + a_kb_lx^{k+l}.$$

Suppose $R[x] = \{f(x) \;:\; f(x) \text{is a polynomial with coefficients in} R\}$. Let $f(x) \in R[x]$, where R is a UFD, with $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, $(a_n \neq 0)$

If a_n is a unit, then $f(x)$ is called a monic polynomial.

If $\gcd(a_0, a_1, a_2, \ldots, a_n)$ is a unit, then $f(x)$ is called a primitive polynomial. $\gcd(a_0, a_1, a_2, \ldots, a_n)$ is called the context of $f(x)$ and is denoted by $c(f(x))$ or $c(f)$

15.2.2 Note: Every monic polynomial is a primitive polynomial.

15.2.3 Example: Consider $Z[x]$ $f(x) = 1 + x + x^2 - x^3$, $g(x) = 2 + 4x - 6x^2 + x^3$ are monic polynomials in $Z[x]$.

15.2.4 Example: $f(x) = 2 + 6x - 10x^2$is not a primitive polynomial.

Sol. Since $\gcd(2, 6, -10) = 2$ is not a unit. Hence given $f(x)$ is not a primitive polynomial.

Here $c(f(x)) = 2$

$f(x) = 2(1 + 3x - 5x^2) = 2(f_1(x))$, where $f_1(x) = 1 + 3x - 5x^2$

$f_1(x))$ is primitive.

15.2.5 Note: If $f(x) \in Z[x]$, then $f(x) = cf_1(x)$, where $f_1(x)$ is a primitive polynomial.

15.2.6 Theorem (Division Algorithm):

Let $R = F[x]$, where F is a commutative integral domain. Let $f(x), g(x) \neq 0 \in F[x]$ of degrees m and n respectively. Let $k = max\{m - n + 1, 0\}$. Suppose that a is the leading coefficient of $g(x)$, then there exists polynomials $q(x), r(x)$ in $F[x]$ uniquely satisfying $a^k f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ or deg $r(x) <$ deg $g(x)$.

Proof. Let b be the leading coefficient of $f(x)$.

We prove the theorem by using induction on m (=deg $f(x)$). Infact to prove the existence of $q(x)$ and $r(x)$.

If $m < n$, then take $q(x) = 0$ and $r(x) = f(x)$, so that

$$f(x) = 0.g(x) + f(x), \text{ deg } f(x) = m < n = \text{ deg } g(x)$$

$$\text{where } k = max\{m - n + 1, 0\} = 0 \to a^k f(x) = f(x).$$

Suppose $m \geq n$.

Suppose by the induction hypothesis $q(x), r(x)$ exists for all polynomials of degree $< m$. ————— (1)

Let $f_1(x) = af(x) - bx^{m-n}g(x) \in F[x]$. Note that deg$f_1(x) < m$.

Then by the induction hypothesis, we get polynomials $q_1(x), r_1(x)$ in $F[x] \ni$

$$a^{k_1} f_1(x) = q_1(x)g(x) + r_1(x)$$

where $r_1(x) = 0$ or deg$r_1(x) <$ deg $g(x)$.

Here $k_1 = max\{m - 1 - n + 1, 0\} = max\{m - n, 0\} = m - n$

$$a^{m-n} f_1(x) = q_1(x)g(x) + r_1(x)$$

Now $a^{m-n}\Big(af(x) - bx^{m-n}g(x)\Big) = q_1(x)g(x) + r_1(x)$

$a^{m-n+1}f(x)\Big(a^{m-n}bx^{m-n} + q_1(x)\Big)g(x) + r_1(x)$

$\therefore a^k f(x) = q(x)g(x) + r(x)$, where $r(x) = r_1(x)$

$q(x) = a^{m-n}bx^{m-n} + q_1(x) \in F[x]$, deg $r(x) <$ deg $g(x)$.

This proves the existance of $q(x)$ and $r(x)$.

We now prove the uniqueness $q(x)$ and $r(x)$.

Suppose $q^{'}(x)$, $r^{'}(x)$ are such that

$$a^k f(x) = q^{'}(x)g(x) + r^{'}(x), \text{ deg } r^{'}(x) < \text{deg } g(x).$$

We also have $a^k f(x) = q(x)g(x) + r(x)$,

$$\Big(q^{'}(x) - q(x)\Big)g(x) = r(x) - r^{'}(x) \text{ ————- } (2)$$

As deg $r(x)$, deg $r^{'}(x) < n$, unless $r(x) = r^{'}(x)$ (2) leads to an absurdity

$\therefore r(x) = r^{'}(x)$

As $g(x) \neq 0$, $q(x) = q^{'}(x)$.

This completes the proof.

15.2.7 GAUSS LEMMA

Suppose $f(x), g(x) \in R[x]$, where R is a UFD. Then $c\big(f(x)g(x)\big) = c\big(f(x)\big)c\big(g(x)\big)$ i.e. the product of two primitive polynomials is a primitive polynomial.

Proof.

$f(x) = c\big(f(x)\big)f_1(x)$.

p$g(x) = c\big(g(x)\big)g_1(x)$, where $f_1(x), g_1(x)$ are primitive.

$f(x)g(x) = c_1f_1(x)c_2g_1(x)$, $c_1 = c\big(f(x)\big)$, $c_2 = c\big(g(x)\big)$.

$f(x)g(x) = c_1c_2f_1(x)g_1(x)$.

To prove that $c\big(f(x)g(x)\big) = c_1c_2$, it is enough to show that $f_1(x)g_1(x)$ is a primitive polynomial.

$\therefore$ In order to prove the theorem it is enough to show that the product of any two primitive polynomials is a primitive polynomial. We now prove that $f_1(x)g_1(x)$ is a primitive polynomial.

Suppose $f_1(x)g_1(x)$ is not a primitive polynomial. Then there is a prime (or irreducible) element p in R such that p divides each of the coefficients of $f_1(x)g_1(x)$. ———— (1)

Write $f_1(x) = a_0 + a_1x + a_2x^2 + \ldots + a^m x^m, \quad a_m \neq 0.$

$$g_1(x) = b_0 + b_1x + b_2x^2 + \ldots + b^m x^m, \quad b_m \neq 0, \qquad a_i, b_j \in R.$$

Then $f_1(x)g_1(x) = c_0 + c_1(x) + c_2x^2 + \ldots + c_tx^t + \ldots + a_mb_nx^{m+n}.$

where $\quad c_0 = a_0b_0.$

$$c_1 = a_0b_1 + a_1b_0.$$

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0.$$

$$\vdots$$

$$c_t = a_0b_t + a_1b_{t-1} + \ldots + a_tb_0.$$

$$\vdots$$

We have $p \mid c_j \ \forall \ j$ ————- (2)

$f_1(x)$ is a primitive polynomial.

Let s be the least index $\ni p \nmid a_s$.

$g_1(x)$ is also primitive.

$\therefore k \ni p \nmid b_k, \qquad k$ least.

$$\text{i.e} \quad \left.\begin{array}{l} p \mid a_0, p \mid a_1, p \mid a_2, \ldots, p \mid a_{s-1} \text{but} p \nmid a_s \\ p \mid b_0, p \mid b_1, p \mid b_2, \ldots, p \mid b_{k-1} \text{but} p \nmid a_k \end{array}\right\} \text{———— (3)}$$

Consider $c_{s+k} = a_0b_{s+k} + a_1b_{s+k-1} + \ldots + a_{s-1}b_{k+1} + a_sb_k + a_{s+1}b_{k-1} + \ldots + a_{s+k}b_0.$

By (2) and (3), we see that $p \mid a_s b_k$. p is prime.

$\therefore$ But $p \nmid a_s$, $p \nmid b_k$.

This contradicts the primality of p.

$\therefore$ $f_1 g_1(x)$ is a primitive polynomial.

15.2.8 Theorem: If R is a UFD, then $R[x]$ is also a UFD.

Proof. As R is a commutative integral domain with unity so is $R[x]$.

We first prove that every non-zero element of $R[x]$ is a finite product of irreducible elements.————-(1)

Let $f(x)(\neq 0) \in R[x]$.

We prove this by using induction on deg $f(x)$.

Let deg $f(x) = 0$. Then $f(x) = a \in R$, $a \neq 0$. R is a UFD.

$\Rightarrow a = p_1 p_2 \ldots p_s$, a finite product of irreducible elements.

Assume that, by the induction hypothesis, the result (1) is same for all the polynomials of degree $<$ deg $f(x)$. ————-(2)

In case $f(x)$ is irreducible, then there is nothing to prove.

So suppose $f(x)$ is not irreducible. Then $f(x) = f_1(x) f_2(x)$ for some $f_1, f_2(x) \in R[x]$, wherein neither $f_1(x)$ nor $f_2(x)$ is a unit.

Note that deg $f_1(x) <$ deg $f(x)$, deg $f_2(x) <$ deg $f(x)$,

$\therefore$ By the induction hypothesis (2) $f_1(x)$ and $f_2(x)$ can be written as a finite product of irreducible elements in $R[x]$ and hence $f(x)$ is also a finite product of irreducible elements of $R[x]$.

This proves (1)

We now prove that every irreducible element of $R[x]$ is a prime element.

Let $p(x)$ be an irreducible element.

Let $p(x) \mid f(x)g(x)$, $f(x), g(x) \in R[x]$.

It is enough to prove that either $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Assume that $p(x) \nmid f(x)$

Suppose deg $p(x) = 0$. Then $p(x) \in R$, say $p(x) = b$, $b \in R$. R is a UFD.

$$\begin{aligned} c \mid f(x)g(x) &\Rightarrow f(x)g(x) = bh(x) \text{ for some } h(x). \\ &\Rightarrow c\Big(f(x)\Big)c\Big(g(x)\Big) = bc\Big(h(x)\Big). \\ &\Rightarrow b \mid c\Big(f(x)\Big)c\Big(g(x)\Big). \\ &\Rightarrow b \mid c\Big(f(x)\Big) \text{ or } b \mid c\Big(g(x)\Big). \end{aligned}$$

But $f(x) = c\Big(f(x)\Big)f_1(x)$, $g(x) = c\Big(g(x)\Big)g_1(x)$.

$\therefore b \mid c\Big(f(x)\Big)f_1(x)$ or $b \mid c\Big(g(x)\Big)g_1(x)$.

i.e $b \mid f(x)$ or $b \mid g(x)$.

$p(x) \mid f(x)$ or $p(x) \mid g(x)$.

$\therefore p(x)$ is prime in this case.

So suppose deg $p(x) > 0$. Consider the ideal generated by $p(x)$ and $f(x)$ i.e $\Big\langle p(x), f(x)\Big\rangle$ in $R[x]$.

Infact

$$S = \Big\langle p(x), f(x)\Big\rangle = \Big\{A(x)p(x) + B(x)p(x) : A(x), B(x) \in R[x]\Big\}.$$

Let $\phi(x)$ be a polynomial of least degree in $\Big\langle p(x), f(x)\Big\rangle$.

Let a be the leading coefficient of $\phi(x)$. $f(x), \phi(x) \in R[x]$, $\phi(x) \neq 0$.

$\therefore$ By the division algorithm.

$$a^k f(x) = q(x)\phi(x) + r(x),\ r(x) = 0 \text{ or deg } r(x) < \text{deg } \phi(x),$$
$$\text{where } r(x), q(x) \in R[x].$$

$a^k f(x) \in S$, $\phi(x) \in S$, $q(x) \in R[x]$. $\Rightarrow q(x)\phi(x) \in S$.

$\therefore a^k f(x) - q(x)\phi(x) \in S$, $r(x) \in S$.

If $r(x) \neq 0$, then this leads to a contradiction to the nature of $\phi(x)$.

$\therefore r(x) = 0$.

$\therefore a^k f(x) = q(x)\phi(x).$

$= q(x)c(\phi)\phi_1(x)$, $\phi_1(x)$ is primitive.

$\Rightarrow \phi_1(x) \mid a^k f(x).$

$\Rightarrow a^k f(x) = t(x)\phi_1(x).$

$\Rightarrow a^k c(f) = c(t)c(\phi_1)$, By Gauss Lemma.

$\Rightarrow a^k c(f) = c(t)$ ($\because c(\phi_1) = 1$ as ϕ_1 is prime).

$\Rightarrow a^k \mid c(t)$ (But $t(x) = c(t)t_1(x)$).

$\Rightarrow a^k \mid c(t)t_1(x) = t(x).$

$\Rightarrow a^k \mid t(x).$

$\therefore \phi_1(x) \mid f(x).$

Similarly we can see that $\phi_1(x) \mid p(x)$.

But $p(x)$ is irreducible and $p(x) \nmid f(x)$ i.e. $p(x), f(x)$ are relatively prime.

$\phi_1(x) \mid \gcd\Big(p(x), f(x)\Big).$

$\therefore \phi_1(x)$ is a unit i.e. $\phi_1(x) \in R$.

But $\phi(x) = c(\phi)\phi_1(x) \in R$.

$\therefore \phi(x) = a \in S.$

$\therefore \exists\ A(x), B(x) \in R[x] \ni a = A(x)p(x) + B(x)f(x).$

$\Rightarrow ag(x) = A(x)p(x)g(x) + B(x)f(x)g(x)$

But $p(x) \mid f(x)g(x), p(x) \mid p(x)g(x)$.

$\therefore p(x) \mid A(x)p(x)g(x) + B(x)f(x)g(x) = ag(x).$

$\therefore p(x) \mid ag(x).$

$ag(x) = t(x)p(x)$ for some $t(x) \in R[x]$.

$ac(g) = c(t)c(p)$, by Gauss Lemma.

$ac(g) = c(t)$. $\qquad$ ($p(x)$ is irreducible $\Rightarrow c(p) = 1$)

$\therefore a \mid c(t).$

$$\Rightarrow a \mid c(t)t_1(x) \qquad (\because t(x) = c(x)t_1(x)).$$

$$\Rightarrow a \mid t(x).$$

Now $a \mid t(x)$, $ag(x) = t(x)p(x)$.

$$\therefore p(x) \mid g(x).$$

15.3 Summary

In this lesson we have established the division algorithm in a polynomial ring $F[x]$. Moreover we proved that the product any two primitive polynomials is again primitive.

15.4 Glossary

Polynomial ring, Division algorithm, Primitive polynomial .

LESSON-16

RINGS OF FRACTIONS

16.1 Introduction : In this lesson we study the rings of fractions.

16.2 Definition: Suppose R is a commutative ring. An element $a(\neq 0) \in R$, which is not a zero divisor is called a regular element of R.

16.3 Definition: Let $S \subset R$. If $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$. Then S is called a multiplicative set.

If S is a multiplicative subset of R in which each element is regular then S is called a regular multiplicative set.

16.4 Note: Suppose R is a commutative integral domain. Then $R-(0)$ is a regular multiplicative set.

Proof. Let $a, b \in R-(0)$.

$\Rightarrow a \neq 0$, $b \neq 0$.

$\Rightarrow ab \neq 0$

$\Rightarrow ab \in R-(0)$.

$\therefore R-(0)$ is a multiplicative set.

Infact every $a \in R-(0)$, $a \neq 0$ and a is not a zero divisor.

Hence every element of $R-(0)$ is a regular element.

Showing that $R-(0)$ is a regular multiplicative set.

16.5 Theorem: suppose R is a commutative ring and S a multiplicative subset of R. Then define a relation $\sim$ on $R \times S$ as follows:

For $(a, s_1), (b, s_2) \in R \times S$, define

$$(a, s_1) \sim (b, s_2) \Rightarrow \exists\ s_3 \in S \ni s_3(as_2 - bs_1) = 0.$$

Then $\sim$ is an equivalence relation on $R \times S$.

Proof.

Let $(a, s) \in R \times S$. For any $s_1 \in S$, we have $s_1(as - as) = 0$

giving $(a, s) \sim (a, s)$, proving $\sim$ is reflexive.

Let $(a, s_1) \sim (b, s_2)$.

$\Rightarrow \exists s_3 \in S \ni s_3(as_2 - bs_1) = 0$

$\Rightarrow s_3(bs_1 - as_2) = 0$

$\Rightarrow (b, s_2) \sim (a, s_1)$

showing $\sim$ is symmetric.

Let $(a, s_1) \sim (b, s_2)$, $(b, s_2) \sim (c, s_3)$. To prove that $(a, s_1) \sim (c, s_3)$. Then $\exists\ s^{'}, s^{''} \in S \ni s^{'}(as_2 - bs_1) = 0$, $s^{''}(bs_3 - cs_2) = 0$.

Now $s^{''}s_3s^{'}(as_2 - bs_1) = 0$ and

$s^{'}s_1s^{''}(bs_3 - cs_2) = 0$. Adding these two we get

$s^{''}s_3s^{'}s_2a - s^{'}s_1s^{''}s_2c = 0$.

$s^{'}s^{''}s_2(as_3 - cs_1) = 0. \qquad (\because s^{'''} = s^{'}s^{''}s_2 \in S)$

$s^{'''}(as_3 - cs_1) = 0$.

which implies $(a, s_1) \sim (c, s_3)$, proving $\sim$ is transitive.

Hence $\sim$ is an equivalence relation.

16.6 Theorem: Denote the equivalent class of $(a, s) \in R \times S$ by $\frac{a}{s}$. Write

$$R_S = \left\{\tfrac{a}{s} : a \in R, s \in S\right\}.$$

Define $+, .$ on R_s as follows:

$$\tfrac{a_1}{s_1} + \tfrac{a_2}{s_2} = \tfrac{a_1s_2 + a_2s_1}{s_1s_2}.$$

$$\tfrac{a_1}{s_1}.\tfrac{a_2}{s_2} = \tfrac{a_1s_2.a_2s_1}{s_1s_2}. \qquad (\forall\ \tfrac{a_1}{s_1}, \tfrac{a_2}{s_2} \in R_s)$$

Then R_s is called the ring of fractions of R with respect to S or localisation of R at S or quotient ring of R with respect to S.

Proof.

Let $\frac{a}{s}$ be the equivalent class of (a, s)

$\frac{a}{s} = [(a, s)]$

$$= \left\{(b, s^{'}) : (b, s^{'}) \sim (a, s)\right\}$$
$$= \left\{(b, s^{'}) : s^{''}(as^{'} - bs) = 0 \text{ for some } s^{''} \in S\right\}$$

Clearly

$R_s = \left\{\frac{a}{s} : a \in R, s \in S\right\}$, $\frac{a}{s} = [(a, s)]$ is a ring with unity (with zero $\frac{0}{s}$ and unity $\frac{s}{s}$ for any $s \in S$)

$$\frac{a}{s_1} + \frac{0}{s} = \frac{a_1 s + 0.s_1}{s_1 s} = \frac{a_1 s}{s_1 s} = \frac{a_1}{s_1}$$

$\Bigg($ since $\frac{a}{s} = \frac{as_1}{ss_1}$

$\iff [(a, s)] = [(as_1, ss_1)], \quad (a, s) \in [(a, s)]$

$\iff (a, s) \sim (as_1, ss_1)$ because

$s^{'}(ass_1 - as_1 s) = 0 \; \forall \; s^{'} \in S$

Therefore $(as_1, ss_1) \in [(a, s)]$

$(as_1, ss_1) \in [(as_1, ss_1)]$

proving $[(a, s)] = [(as_1, ss_1)]$

Which gives $\frac{a}{s} = \frac{as_1}{ss_1}\Bigg)$

$\frac{a_1}{s_1} . \frac{s}{s} = \frac{a_1 s}{s_1 s} = \frac{a_1}{s_1}$.

16.7 Theorem: Suppose S is a multiplicative subset of a commutative ring R. Let R_s be the ring of fractions of R with respect to S. If $0 \in S$, then $R_s = (0)$.

Proof.

$0 \in S$; $\frac{a}{s} \in R_s$

$\frac{a}{s} = \frac{as_1}{ss_1} \; \forall \; s_1 \in s$.

In particular, 0 in the place of s_1, gives

$\frac{a}{s} = \frac{0}{0} = \frac{0}{s^{'}} \qquad (s^{'} = 0 \in S)$

$\therefore R_s = 0 \qquad (\frac{0}{0} = 0$ of R_s

$\frac{0}{0} = 1$ of R_s)

$\frac{0}{0} = \frac{s^{'}}{s^{'}}, s^{'} = 0 \in S \Rightarrow \frac{0}{0}$ is unity.

$$(0 = 1 \in R_s \text{ if } 0 \in S).$$

16.8 Theorem: Suppose S is a multiplicative subset of R, where R is a commutative ring. Then there is a natural homomorphism $f : R \to R_s$ given by $f(a) = \frac{as}{s}$ $\forall$ $a \in R$ and for some fixed $s \in S$. Moreover, f is a monomorphism (i.e $1-1$ homeomorphism)

$\Longleftrightarrow$ "$x \in S, a \in R, xa = 0 \Rightarrow a = 0$"

Proof.

Clearly $f : R \to R_s$ ($\because as \in R, s \in S \Rightarrow \frac{as}{s} \in R_s$)

Let $a_1, a_2 \in R$. Then $f(a_1) + f(a_2) = \frac{a_1 s}{s} + \frac{a_2 s}{s}$

$$= \frac{a_1 ss + a_2 ss}{ss}$$

$$= \frac{a_1 s^2 + a_2 s^2}{s^2} = \frac{(a_1 + a_2)s^2}{s^2}$$

$$= \frac{(a_1 + a_2)s}{s}$$

$f(a_1 + a_2) = \frac{(a_1 + a_2)s}{s}$

$f(a_1)f(a_2) = \frac{a_1 s}{s} . \frac{a_2 s}{s} = \frac{a_1 a_2 ss}{ss} = \frac{a_1 a_2 s}{s}$

$f(a_1 a_2) = \frac{a_1 a_2 s}{s}$.

$\therefore$ f is homomorphism.

f is monomorphism $\Longleftrightarrow$ $ker f = (0)$

$\Longleftrightarrow$ $\{a \in R : f(a) = 0 \text{ of } R_s\} = (0)$

$\Longleftrightarrow$ $\{a \in R : \frac{as}{s} = \frac{0}{s}\} = (0)$

$\Longleftrightarrow$ $\{a \in R : (as, s) \sim (0, s)\} = (0)$

$\Longleftrightarrow$ $\{a \in R : \exists s^{'} \in \ s \ni \ s^{'}(ass - 0s) = 0\} = (0)$

$\Longleftrightarrow$ $\{a \in R : \exists s^{'} \in S \ \ni \ as^2 s^{'} = 0\} = (0)$

$\Longleftrightarrow$ $\{a \in R : ax = 0, x \in S\} = (0)$

$\Longleftrightarrow$ "$ax = 0, x \in S \Rightarrow a = 0$"

16.9 Theorem: Suppose R is a commutative ring with some regular elements. Let S be the set of all regular elements of R. Then we have the following statements.

(i) R can be embedded in R_s.

Treating R to be a subring of R_s, we have

(ii) Every regular element of R is invertible in R_s.

(iii) Every element $\frac{a}{s} \in R_s$ can be written as $as^{'}, a \in R, s \in S$.

Proof.

Claim: S is a multiplicative subset of R.

Let $s_1, s_2 \in S$. Then s_1, s_2 are regular elements.

$\therefore s_1, s_2 \neq 0$ (otherwise s_1, s_2 become zero divisors)

If $\exists\ s \in S \ni (s_1 s_2)s = 0$, then $s_1(s_2 s) = 0$.

But s_1 being not a zero divisor, we have $s_2 s = 0$

s_2 is not also a zero divisor.

$\therefore s = 0$.

$\therefore s_1 s_2$ is not a zero divisor.

$\therefore s_1 s_2 \in S$.

$\therefore S$ is a multiplicative set.

Let R_s be the ring of fractions of R with respect to S.

We know that $f : R \to R_s$ given by $f(a) = \frac{as}{s}$ is a homomorphism.

Let $x \in S, a \in R \ni ax = 0$.

$x \in S \Rightarrow x$ is a regular element.

$\Rightarrow x$ is not a zero divisor.

$\therefore a = 0$

$\therefore f$ is $1 - 1$ homomorphism. $R \hookrightarrow R_s$

$\therefore R$ is embedded in R_S.

As such we can treat R as a subring of R_s by identifying $a \in R$ with $\frac{as}{s} \in R_s$.

$$a \leftrightarrow \frac{as}{s}$$

Let $a \in S$ i.e. a is a regular element of R.

Consider $b = \frac{s}{as}$ (for some $s \in S$)

$\Big(\because a \in S \Rightarrow as \in S$

$s \in (S \subset) R \Rightarrow \frac{s}{as} \in R_s \Big)$.

Then $b \in R_s$.

$a.b = a.\frac{s}{as} = \frac{as}{s}.\frac{s}{as} = \frac{ass}{sas} = \frac{s'}{s'} = 1 \in R_s$.

$(s' = as^2 \in S)$

$b \in R_s$ and $a^{-1} = b$

$$\therefore a^{-1} = \frac{s}{as}$$

Let $\frac{a_1}{s_1} \in R_S$

$a_1.s_1^{-1} = a_1.\frac{s}{s_1 s} = \frac{a.s}{s}.\frac{s}{s_1 s} = \frac{a_1 ss}{s_1 ss} = \frac{a_1}{s_1}$

$$\therefore \frac{a_1}{s_1} = a_1 s_1^{-1}$$

16.10 Theorem: Every commutative integral domain can be embedded in a field.

Proof. Suppose R is a commutate integral domain.

Take $S = R - (0)$, which is the set of all regular elements of R.

$\therefore R \hookrightarrow R_s$, where every regular element of R is invertible in R_s.

Let $\frac{a_1}{s_1} \in R_s, \frac{a_1}{s_1} \neq 0$ of R_s $\quad \frac{a_1}{s_1} \neq \frac{0}{s}$

$s_1 \in S = R - (0) \Rightarrow s_1 \neq 0$.

$\frac{a_1}{s_1} = \frac{0}{s} \Rightarrow a_1 \neq 0 \Rightarrow a_1 \in S$.

$a_1 \in S$, $s_1 \in (S \subseteq R) \Rightarrow \frac{s_1}{a_1} \in R_s$.

Then $\frac{a_1}{s_1}.\frac{s_1}{a_1} = \frac{a_1 s_1}{s_1 a_1} = \frac{s'}{s'}$, $(s' = a_1 s_1 \in S)$

$= 1$ of R_s

$\therefore (\frac{a_1}{s_1})^{-1} = \frac{s_1}{a_1}$.

$\therefore R_s$ is a field and R is embedded in R_s.

R_s is called the field of fractions.

16.11 Definition (Local Rings):

Suppose R is a ring with unity. If R has a unique maximal right ideal, then R is called a Local ring.

16.12 Theorem: Suppose R is a commutative ring, P a prime ideal in R. Let $S = R - p$. Then S is a multiplicative subset of R and R_s is a local ring with the unique manimal ideal p_s, where $p_s = \{\frac{a}{s} : a \in p, s \in S\}$

Proof. Let $s_1, s_2 \in S$. $S = R - p$

$\Rightarrow s_1, s_2 \notin p \Rightarrow s_1 s_2 \notin p$ ($\because p$ is a prime ideal)

(For, if $s_1 s_2 \in p$, p is a prime ideal in R, R commutative.

$\Rightarrow s_1 \in p$ or $s_2 \in p$ which is not true.)

$s_1 s_2 \notin p \Rightarrow s_1 s_2 \in R - p = S \Rightarrow s_1 s_2 \in S$.

$\therefore S$ is a multiplicative set.

$\therefore R_s$ is a commutative ring.

Consider $p_s = \{\frac{a}{s} : a \in p, s \in S\}$.

Let $\frac{a_1}{s_1}, \frac{a_2}{s_2} \in p_s$. Then $\frac{a_1}{s_1} - \frac{a_2}{s_2} = \frac{a_1 s_2 - a_2 s_1}{s_1 s_2}$

p is a (prime) ideal, $a_1 \in p, a_2 \in p, s_1 s_2 \in (S \subset) R$

$\Rightarrow a_1 s_2 - a_2 s_1 \in p$

$\therefore \frac{a_1}{s_1} - \frac{a_2}{s_2} \in p_s$

Let $\frac{x}{s} \in R_s, \frac{a_1}{s_1} \in p_s$.

$\frac{x}{s} . \frac{a_1}{s_1} = \frac{x a_1}{s s_1}$, where $s s_1 \in S$.

$x \in R$, $a_1 \in p$, p is an ideal $\Rightarrow x a_1 \in p$.

$\therefore \frac{xa_1}{ss_1} \in p_s$

$\therefore p_s$ is an ideal in R_s.

We now prove the manimal ideal nature of p_s.

Let A be an ideal in $R_s \ni p_s \subseteq A \subseteq R_s$.

Let $p_s \neq A$ i.e.$p_s \subsetneq A$.

Then $\exists \frac{x}{s} \in A \ni \frac{x}{s} \in p_s$. Here $x \in S$, $x \notin p$.

$x \notin p \Rightarrow x \in R - p = S \Rightarrow x \in S$

$s \in (S \subseteq R), x \in S \Rightarrow \frac{s}{x} \in R_s$.

Now $\frac{s}{x} \in R_s, \frac{x}{a} \in A$, A is an ideal.

$\therefore \frac{s}{x}.\frac{x}{s} \in A$ i.e $\frac{xs}{xs} \in A$.

A contains the unity of R_s.

$\therefore A = R_s$.

$\therefore P_s$ is a maximal ideal in R_s.

To prove that R_s a local ring it remains to be shown that P_s is unique.

Let B be a maximal ideal in R_s and $B \neq p_s$.

Then $B \neq R_s$.

Then $\exists \frac{x}{a} \in p_s$ but $\frac{x}{s} \in B$ and $\left(\exists \frac{y}{s_1} \in p_s \text{ but } \frac{y}{s_1} \notin B\right)$

Let $\frac{x}{s} \in B$ but $\frac{x}{s} \in p_s$.

Then $B = R_s$, which is a contradiction.

$\therefore R_s$ is a local ring.

16.12 Summary

In this lesson Every commutative integral domain can be embedded in a field.

16.13 Glossary

Regular element, Ring of fractions, Local element.