(17) Corollary : (7)

If H & K are subgroups of G & O(H) is greater than $\sqrt{O(G)}$ O(K) > $\sqrt{O(G)}$ Then (H∩K) ≠ {e}.

proof :

since H & K are subgroup of a finite group G & O(H) > $\sqrt{O(G)}$, O(K) > $\sqrt{O(G)}$.

since HK is a subgroup of G

$\Rightarrow O(HK) \leq O(G)$

$\Rightarrow O(HK) \leq O(G)$

$\Rightarrow \frac{O(H)O(K)}{O(H \cap K)} \leq O(G)$

$\Rightarrow \frac{\sqrt{O(G)}\sqrt{O(G)}}{O(H \cap K)} < O(G)$

$\Rightarrow \frac{O(G)}{O(H \cap K)} < O(G)$

$\Rightarrow O(H \cap K) > 1$

$\Rightarrow H \cap K \neq \{e\}$.

Normal Subgroup :- (aH = Ha).

(aN = Na).

A Subgroup N(G) is said to be a Normal Subgroups of G, if for every $g \in G$ if $n \in N$, $gng^{-1} \in N$

(or) Equivalently the set of all gn

$n \in N$ then N is a normal subgroup of $G_1 \Leftrightarrow gNg^{-1} \subseteq N$ for only $g \in G_1$

lemma (10).

N is a Normal subgroup of $G_1 \Leftrightarrow gNg^{-1} = N \ \forall g \in G_1$.

PROOF: PART I:

Assume that $gNg^{-1} = N, \forall g \in G_1$

TO PROVE: N is a Normal subgroup of G_1

since $gNg^{-1} = N$

$\Rightarrow gNg^{-1} \subseteq N$

$\therefore N$ is a Normal subgroup of G_1

PART II:

Conversely, Assume that N is a normal subgroup of G_1.

Then $gNg^{-1} \subseteq N \longrightarrow (1), \forall g \in G_1$

Its enough to prove $N \subseteq gNg^{-1}$

since $g \in G_1 \Rightarrow g^{-1} \in G_1$, we gave

$g^{-1}N(g^{-1})^{-1} \subseteq N$

$\Rightarrow g[g^{-1}N(g^{-1})^{-1}]g^{-1} \subseteq gNg^{-1}$

$\Rightarrow (gg^{-1})N((g^{-1})^{-1}g^{-1}) \subseteq gNg^{-1}$

$\Rightarrow N \subseteq gNg^{-1} \longrightarrow (2)$

from (1) & (2) we have, get,

$gNg^{-1} = N \ \forall g \in G_1$

Lemma (10):

The subgroup $N(G_1)$ is a Normal subgroup of G_1 $\Leftrightarrow$ Every left coset of N in G_1 is a right coset of N in G_1.

proof:

Suppose N is a Normal subgroup of G_1. Then the every $g \in G_1$, we have,

$gNg^{-1} = N, \forall g \in G_1$ [by lemma10]

$\Rightarrow (gNg^{-1}) = Ng$

$\Rightarrow g(Ng^{-1}g) = Ng$

$\Rightarrow gN = Ng$.

(i.e) Every left coset of N in G_1 is a right coset of N in G_1.

Conversely, suppose that every left coset of N in G_1 is a right coset of N in G_1.

To prove: N is a Normal subgroup of

Then $gN = Ng$ ⟶ (1)

for some $g^{-1} \in G_1$ (by assumption

$gNg^{-1} = N \ \forall g \in G$.

Lemma (11):

The subgroup $N(G)$ is a Normal subgroup of $G \Leftrightarrow$ Every left coset of N in G is a right coset of N in G.

proof:

Suppose N is a Normal subgroup of G. Then the every $g \in G$, we have,

$gNg^{-1} = N, \forall g \in G$ [by lemma10]

$\Rightarrow (gNg^{-1}) = Ng$

$\Rightarrow g(Ng^{-1}g) = Ng$

$\Rightarrow gN = Ng$.

(i.e) Every left coset of N in G is a right coset of N in G.

Conversely, suppose that every left coset of N in G is a right coset of N in G.

To prove: N is a Normal subgroup of

Then $gN = Ng$ ⟶ (1)

for some $g^{-1} \in G$ (by assumption

(54)

Since $g \in N$, we have

$g = ge \in gN$

$\Rightarrow g \in gNg^{-1}$ [by ①]

$\Rightarrow Ng = Ng^{-1}$ [$\because a \in H / Ha = Hb$]

$\Rightarrow Ng = gN$ (by ①)

$\Rightarrow NgG^{-1} = gNg^{-1}$

$\Rightarrow N = gNg^{-1}$

By lemma ⑩

N is a Normal subgroup of G.

Note: ①.

For any 2 subsets A, B of G define $AB = \{x \in G / x = ab ; a \in A \& b \in B\}$

In a special case we have

$A = B = H$

Then the subgroup $HH = \{x \in G / x = h_1 h_2, h_1 \in H, h_2 \in H\}$.

Since H is called under multiplication we have $h_1, h_2 \in H$.

$\therefore HH \subset H$, but $HH \supset He = H$

$\therefore HH = H$.

Note: 2.

Suppose that N is a normal subgroup of G. $a, b \in G$.

(55)

Since N

By lemma

aN

Now, Na

Lemma ⑤

normal

right

right

Proof:

Then

righ

righ

pro

is

T

Since N is normal in G
By lemma (11), we have,
$aN = Na$
Now, $NaNb = N(aN)b = N(Na)b$
$= (NN)ab$
$= Nab$ [by note 1]

Lemma (12)

A subgroup N(G) is a normal $\Leftrightarrow$ the product of 2 right cosets of N in G is again a right coset of N in G.

Proof:

N is a normal subgroup of G. Then by note (ii), The product of two right coset of N in G is again a right coset of N in G.

conversely, suppose that the product of two right cosets of N in G is again a right coset of N in G.

TO PROVE: N is a normal subgroup of G. $g \in G$.

then $g^{-1} \in G$.

$\therefore Ng$ & Ng^{-1} are two right cose

of N in G.

(56)

By hypothesis, $NgNg^{-1}$ is again a right coset of N in G.

$$Ngg^{-1} = Ne = N.$$

Since $e \in N$, ege^{-1} is also a right coset of N in G.

But N itself is a right coset of N in G. Also if two right cosets have no element in common, they cosets must be identity.

$\therefore Ng\,Ng^{-1} = N_1$ ∀ for every $g \in G$. $\Rightarrow n_1 \cdot gng^{-1} \in N$, $\forall n_1 \in N$, $n \in N$ & $g \in G$.

$\Rightarrow n_1^{-1} \cdot (ng^{-1}hg^{-1}) \in n_1^{-1}N$

$\Rightarrow (n_1^{-1}n_1)(gng^{-1}) \in N$

$\Rightarrow gng^{-1} \in N$, $\forall g \in G$.

$\Rightarrow$ N is a normal subgroup of G.

Problems: (1)

Prove that x^n of two norms subgroups is again a normal subgroup.

(57)

Soln:

Let N
subgroup
subgroup

TO PROVE
subgr
eleme
of N∩

(6) Soln:

Let N & K be two normal subgroup of G since N & K are subgroup of G

we have

TO PROVE: $N \cap K$ is normal subgroup of G. Let g be any element of G & n be any element of $N \cap K$

(i.e) $n \in N \cap K$

$\Rightarrow n \in N$ & $n \in K$.

∴ since N is normal

$\Rightarrow g \in G, n \in N$

$\Rightarrow gng^{-1} \in N$

ALSO K is normal $g \in G, n \in K$.

$\Rightarrow gng^{-1} \in K$

$\therefore gng^{-1} \in N \cap K$

Hence $N \cap K$ is a normal subgroup of G.

such that subgroup of an abelian is normal.

Soln: Let G be an abelian group

(2) Let H be a subgroup of G
To prove:- H is normal
Let g be any element of G &
h be any element of H.

Now, $ghg^{-1} = g(hg^{-1})$
$= g(g^{-1}h)$

$\Rightarrow (gg^{-1})h = eh$

i.e. $ghg^{-1} = h \in H$

$\Rightarrow ghg^{-1} \in H$

∴ H is a normal subgroup of G.

Soln:

(3) Prove that subgroup of a cyclic group is normal.

Soln:

First we such that cyclic group is abelian.

Let $G = \{a^i / i = \pm 0, \pm 1, \pm 2, \ldots\}$

$= \langle a \rangle$

Let $a^r, a^s \in G$, where r, s are integers. Now, $a^r \cdot a^s = a^{r+s} = a^{s+r}$

$= a^s \cdot a^r$

$\Rightarrow$

G is abelian.

(3) By above problem (2), every subgroup of an abelian group is normal.

Hence every subgroup of a cyclic group is normal.

(4) If H is a subgroup of G & N is a normal subgroup of G. Such that $H \cap N$ is a normal subgroup of H.

Soln: Since H & N are subgroups of G. $H \cap N$ is also a subgroup of G.

To prove:

$H \cap N$ is a normal subgroup of H. Let x be any element of H n be element of $H \cap N$.

Then $n \in H$ & $n \in N$

Since N is a normal subgroup of G, we have $xnx^{-1} \in N$

Also, H is a subgroup of G. we have $x \in H, n \in H \Rightarrow xnx^{-1} \in H$.

$\therefore x n x^{-1} \in H \cap N, \forall x \in H$ — (1)

Then $H \cap K$ is a normal subgroup of H. — (2)

(5) If N is a normal subgroup of G & H is any subgroup of G, P.T NH is a subgroup of G.

Soln:

Given N is a normal subgroup of G. H is any subgroup of G.

TO PROVE: NH is a subgroup of G

It is enough to prove, $NH = HN$

By lemma (II) "HK is a subgroup.

(E) $HK = KH$"

Let $x \in HN$

$\Rightarrow x = hn$

$x \in hN$

but $hN = Nh$ (by lemma (II))

$\Rightarrow x \in Nh$

$\Rightarrow x = n_1 h_1 \quad \forall n_1 \in N$

$\Rightarrow x \in NH$

Thus $HN \subseteq NH$ ——— (1)

Sily, $NH \subseteq HN$ ——— (2)

from (1) & (2) we get,

$HN = NH$

(5) (c) If N & M are normal subgroup of G. Then P.T NM is also normal subgroup of G.

Soln:

By lemma "The subgroup N of G is a normal subgroup of G ⇔ every left coset of N in G is a right coset of N in G", we have,

(1) If H is a subgroup of G and let $N(H) = \{g \in G / gHg^{-1} = H\}$

P.T (a) N(H) is a subgroup of G.

(b) H is a normal in N(H).

(c) If H is a normal subgroup of K in G then $K \subset N(H)$

(d) H is normal in G $\Leftrightarrow N(H) = G$

Proof:

(a) Let $a, b \in N(H)$. Then by definition we have,

$$aHa^{-1} = H \ , \ bHb^{-1} = H$$

Now, $bHb^{-1} = H$

$$bb^{-1}Hb^{-1}b = b^{-1}Hb$$

$$(bb^{-1})H(b^{-1}b) = b^{-1}Hb$$

$$H = b^{-1}Hb \quad \text{---(1)}$$

$= aHa^{-1}$ (by ①)

$= H$

$\Rightarrow ab^{-1} \in N(H)$

Thus $a, b \in N(H)$

$\Rightarrow a \cdot b^{-1} \in N(H)$

$\therefore N(H)$ is a subgroup of G

Let h be any element of H.

Since $hHh^{-1} = H$

$\Rightarrow h \in N(H)$

$H \subseteq N(H)$

Hence H is a subgroup of $N(H)$

TO Slich that H is normal in of (H)

Let x be any element in $N(H)$

Thus $xHx^{-1} = H$

$\Rightarrow H$ is a normal subgroup of $N(H)$

[by lemma "N is a normal sb g of G)

$\Leftrightarrow gNg^{-1} = N$ $Hg \in G$

Let $K \in K$

TO Rlove : $K \subseteq N(H)$

Since H is a normal subgroup of K.

$kHk^{-1} = H$

$\Rightarrow k \in N(H)$

$\Rightarrow k \subseteq N(H)$

let H is a normal in G

TO PROVE: $N(H) = G$

let $x \in G$

Then $xHx^{-1} = H$ [H is normal in G]

$\Rightarrow x \in N(H)$, By definition,

$G \subseteq N(H)$ ——— (1)

by (a), "N(H) is a subgroup of G")

$\Rightarrow N(H) \subseteq G$ ——— (2)

From (1) & (2) we get,

$N(H) = G$

conversely assume that

TO PROVE H is normal

$\Rightarrow x \in N(H)$

$\Rightarrow xHx^{-1} = H$

$\therefore$ H is normal in G.

lemma (13):

If G is a group. N is a normal subgroup of G. Then G/N also a group.

(b) Proof: Let G/N denote the collection of all cosets of N in G.

(i) closure:

let $x, y \in G/N$

Then $x = Na$, $y = Nb$ for some $a, b \in G$

Now $xy = NaNb$

$= Nab \in G/N$ [by note (5)] ①

Thus $x, y \in G/N \Rightarrow xy' \in G$ (N) ②

$\therefore G/N$ is closed ③

(ii) Associative:

let $x, y, z \in G/N$

Then $x = Na$, $y = Nb$, $z = Nc$ for some

Now $(xy)z = (NaNb)Nc$.

$= (Nab)Nc$

$= Nab$

$= Na(Hbc)$

$= Na(NbNc)$

$= x(yz)$

associative law.

Existance of identity:-

Consider the element

$N = Ne \in G/N$

If $X \in G/N$ then $X = Na$ for some a

Now $XN = NaNe$

$= Nae = Na = X$.

i.e) $XN = X$

similarly, $NX = X$

$\therefore N = Ne$ is an identity element in G/N.

(iv) Existence of inverse:-

suppose $X = Na \in G/N$ for some $a \in G$.

$\Rightarrow a^{-1} \in G$

$\Rightarrow Na^{-1} \in G/N$

Now, $NaNa^{-1} = Naa^{-1}$

$= Ne = N$

Sly, $Na^{-1}Na = Ne$

$\therefore Na^{-1}$ is the inverse of Na in G/N

$\therefore G/N$ is a group under the multiplication

definition :-

(Quotient group).

Let G be a group, N is a normal subgroup of G. Then $O(G/N)$ is called a quotient group

If G is a finite group and N is a normal subgroup of G. Then $o(G/N) = \frac{o(G)}{o(N)}$.

proof:

Given G is a finite group & N is a normal subgroup of G.

Let G/N denote the quotient group. (i.e) It contains all the right cosets of N in G. The number of distinct right coset of G/N is denoted by $o(G/N)$

(i.e) $i_G(N) = o(G/N)$

(i.e) $\frac{o(G)}{o(N)} = o(G/N)$ (by lagrange's theorem).

definition: (Homomorphism:

A mapping $\phi: G \to \bar{G}$ is said to be a homomorphism if $\forall a, b \in G$.

$$\phi(ab) = \phi(a) \cdot \phi(b).$$

Eg:

The mapping $\phi: G \to G$ defined by $\phi(x) = \ldots$ $\forall x \in G$ is a homomorphism

(67) called a trivial homomorphism since $\varphi(x) =$ for every homomorphism

(2) Let G be the group of all real number under addition and G' the group of non-zero real number under multiplication:

Define $\phi : G \to G'$ by $\varphi(a) = x^a$

Now, $\phi(a+b) = 2^{a+b} = 2^a \cdot 2^b$

$= \varphi(a) \cdot \varphi(b)$

$\therefore \varphi$ is a homomorphism.

Lemma (15)

Suppose G is a group, N is a normal subgroup of G, Define a map $\varphi : G \to G/N$ by $\varphi(x) = Nx$, $\forall x \in G$. Then φ is a homomorphism of G onto G/N.

Soln:

TO prove φ is onto

For every element $x \in G/N$ is of the form.

$x = Ny$ & $\forall\ y \in G$.

so there exists $y \in G$ such that

$\varphi(y) = Ny = x$

φ is onto.

(58)

To prove φ is a homomorphism

let $Nx, Ny \in G/N$

$\Rightarrow x, y \in G$

$\Rightarrow \varphi(xy) = Nxy$

$= Nx\,Ny = \varphi(x)\,\varphi(y)$

$\therefore \varphi$ is a homomorphism of G onto G/N called canonical homomorphism.

Kernal of a homomorphism:

defn:

If φ is a homomorphism of G into Kernal of φ is $K\varphi$ defined by

$K\varphi = \{x \in G / \varphi(x) = \bar{e}\}$

where $\bar{e}$ is the identity in $\bar{N}$

Lemma (6)

If φ is a homomorphism of G then (i) $\varphi(e) = \bar{e}$, the unit element of G.

(ii) $\varphi(x^{-1}) = [\varphi(x)]^{-1} \forall x \in G$

Proof:

(i) Let $x \in G$. Then $\varphi(x) = \varphi(xe)$

$\varphi(x) = \bar{e} = \varphi(x) \cdot \varphi(e)$

$\Rightarrow \varphi(e)^{-1} = \bar{e}$ where $\bar{e}$ is the identity.

(iv) Now $\bar{e} \cdot \bar{e} = \varphi(x)$

$= \varphi(x \cdot x)$

$= \varphi(x) \cdot \varphi(x)$

$\Rightarrow \varphi(x^{-1}) = [\varphi(x)]^{-1}$

Lemma (1)

If φ is a homomorphism of G into $\bar{G}$ with kernal K then K is a normal subgroup of G.

Proof:

we prove that K is a subgroup of G.

(i) To prove (i) $xy \in K \Rightarrow xy \in K$

(ii) $x \in K \Rightarrow x^{-1} \in K$

(i) let $x, y \in K$ then

$\varphi(x) = e$ and $\varphi(y) = \bar{e}$ where $\bar{e} \in \bar{G}$

now $\varphi(xy) = \varphi(x) \cdot \varphi(y)$

$\Rightarrow \bar{e} \cdot \bar{e} = \bar{e}$

Thus $x, y \in K \Rightarrow xy \in K$

(ii) let $x \in K$, Then $\varphi(x) = e$

From the above demma (b) we have

$\varphi(x) = (\varphi(x))^{-1} = (\bar{e})^{-1}$

$\varphi(x^{-1}) = e^{-1}$

$\Rightarrow x^{-1} \in K$

Thus $x \in K \Rightarrow x^{-1} \in K$.

next we p.T. K is a normal subgroup of G.

K is a normal subgroup of G.

Lemma (8)

If ϕ is a homomorphism of G onto $\bar{G}$ with kernal K, the set of all inverse integer of are $\bar{g} \in \bar{G}$ under ϕ in G is gn by Kn where x is any particular inverse image of $\bar{g}$ in G.

Proof:

Gin $\varphi : G \to \bar{G}$ is an onto homomorphism.

Let $x \in G$

Then $\varphi(x) = \bar{x} \in \bar{G}$

Let e and $\bar{e}$ be the identity element in G and $\bar{G}$ respectively

Define $\phi^{-1} : \bar{G} \to G$

(11)

By $\varphi^{-1}(\bar{x}) = \{a \in G \mid \varphi(a) = \bar{x}\}$

To prove:

$\varphi^{-1}(x) = Kx$

Let $y \in Kx$

Then $y = kx$ where $k \in K$

Now $\varphi(y) = \varphi(kx)$

$= \varphi(k) \cdot \varphi(x)$

$= \bar{e} \cdot \bar{x} = \bar{x}$

$\therefore y \in \varphi^{-1}(x)$

$\therefore Kx \subseteq \varphi^{-1}(x)$ ——— (1)

Let $z \in \varphi^{-1}(\bar{x})$

$\Rightarrow \varphi(z) = \bar{x}$ ——— (2)

consider,

$\varphi(zx^{-1}) = \varphi(z) \cdot \varphi(x^{-1})$

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

i.e. $\varphi(zx^{-1}) = \bar{e}$

$zx^{-1} \in K$

$\Rightarrow zx^{-1}x \in Kx$

$\Rightarrow z \in Kx$

$\Rightarrow \varphi^{-1}(x) \subseteq Kx$ ——— (3).

From (1) & (3) we have,

$\varphi^{-1}(x) = Kx$

Isomorphism :

A homomorphism φ from G_1 into G_1 is said to be a homomorphism if φ is 1-1.

Isomorphism :

Two groups G_1 & G_1^* are said to be isomorphism, if there is an isomorphic of G_1 onto G_1^*

In this case we write $G_1 \cong G_1^*$

Result :-

Prove that relation '$\cong$' is an equivalence relation.

Proof:

(i) '$\cong$' is Reflexive.

For any group G_1, $I : G_1 \to G_1$ is an isomorphism.

(ie) the relation '$\cong$' is reflexive,

(ii) '$\cong$' is symmetric

let $G_1 \cong G_1^*$

Then $\varphi : G_1 \to G_1^*$ be an isomorphism.

(ie) φ is a bijection

$\Rightarrow \varphi^{-1}$ exists

then $\varphi^{-1}: G_1^* \to G_1$ is also a bijection

let $\varphi(x) = x'$, $\varphi(y) = y'$

now $\varphi(xy) = \varphi(x)\varphi(y)$

$= x'y'$ (by def)

$\Rightarrow \varphi^{-1}(x'y') = xy = \varphi^{-1}(x')\varphi^{-1}(y')$

Thus φ^{-1} is an isomorphism

i.e. $G_1^* \cong G_1$

(ii) The relation '$\cong$' is symmetric

(iii) '$\cong$' is transitive

Let $G_1 \cong G_1^*$ & $G_1^* \cong G_1^{**}$

TO PROVE: $G_1 \cong G_1^{**}$

Now $f: G_1 \to G_1^*$, $g: G_1^* \to G_1^{**}$ are isomorphic.

since f & g are bijective we have gof is a mapping from $G_1 \to G_1^{**}$ is also bijective.

Let $x, y \in G_1$

Then $(gof)(xy) = g(f(xy))$

$= g(f(x) \cdot f(y))$

$= g(f(x)) \cdot g(f(y))$

$= [(gof)(x)][(gof)(y)]$

$\therefore gof$ is an isomorphism.

$G_1 \mathcal{R} G_2$ & $G_2 \mathcal{R} G_3$

Hence the relation $\mathcal{R}$ is transitive

equivalence relation.

corollary :-

A homomorphism φ of G_1 into $\bar{G}_1$ with kernal K_φ is an isomorphism of G_1 into $\bar{G}_1$ $\Leftrightarrow K_\varphi = (e)$

Proof:

A mapping $\varphi : G_1 \to \bar{G}_1$ is a homomorphism with kernal K_φ. Assume that φ is an isomorphism.

To prove:

$K_\varphi = (e)$

Let $a \in K_\varphi$.

Then $\varphi(a) = \bar{e}$

$\Rightarrow \varphi(a) = \varphi(e)$

since φ is an isomorphism

we have.

$a = e$

$\therefore K_\varphi = (e)$

Conversely, Assume that the mapping.

$\varphi : G \to \bar{G}$ is

with kernal

To prove φ is

ie) to prove :

let $\varphi(a) =$

$\varphi(a) (\varphi$

$\Rightarrow \varphi(a$

$\Rightarrow a$

$\Rightarrow$

$\Rightarrow$

$\Rightarrow$

Im φ

Theo

of

$\varphi : G \to \bar{G}$ is a homomorphism with kernal $K\varphi = (e)$

To prove: φ is an isomorphism.

i.e. to prove: φ is 1-1

Let $\varphi(a) = \varphi(b)$ $\forall a, b \in G$

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

$\Rightarrow \varphi(a)\varphi(b^{-1}) = \bar{e}$

$\Rightarrow \varphi(ab^{-1}) = \bar{e}$

$\Rightarrow ab^{-1} \in K\varphi$

$\Rightarrow ab^{-1} \in (e)$

$\Rightarrow ab^{-1} = e$

$\Rightarrow ab^{-1}b = eb$

$\Rightarrow ae = b$

$\Rightarrow a = b$

$\therefore \phi$ is an isomorphism.

(+) Theorem:

(Fundamental theorem of homomorphism).

Let ϕ be a homomorphic of G onto $\bar{G}$ with kernal K. Then $G/K \approx \bar{G}$ (or) Every homomorphic image of a group G is isomorphic to some quotient group of G.

(11)

Proof:

Let $\bar{G}$ be a homomorphic image of a group G and ϕ be the corresponding homomorphism. i.e. ϕ is a homomorphism of G onto $\bar{G}$.

If Lemma 11, If $a \in G$ then $Ka \in G/K$

$\Rightarrow \phi(a) \in \bar{G}$, $\phi : G \to \bar{G}$

$\phi : (a) \to \bar{G}$

consider the map $\phi : G/K \longrightarrow \bar{G}$ defined by $\phi(Ka) = \phi(a)$, $\forall a \in G$

i) To prove ϕ is well - defined & 1-1.

if $a, b \in G$ and $Ka = Kb$,

$\Leftrightarrow ab^{-1} \in K$

$\Leftrightarrow \phi(ab^{-1}) = \bar{e}$.

$\Leftrightarrow \phi(a) \cdot \phi(b^{-1}) = \bar{e}$

$\Leftrightarrow \phi(a) [\phi(b)]^{-1} = \bar{e}$

$\Leftrightarrow \phi(a) [\phi(b)]^{-1} = \bar{e}$

$\Leftrightarrow \phi(a) \cdot [\phi(b)]^{-1} \cdot \phi(b) = \bar{e} \cdot \phi(b)$

$\Leftrightarrow \phi(a) = \phi(b)$

$\Leftrightarrow \phi(Ka) = \phi(Kb)$

$\therefore \phi$ is well defined & 1-1

Next to prove ϕ is onto.

Let y be any element of $\bar{G}$ then $y = \phi(a)$ for some $a \in G$.

Now, $Ka \in G/K$ such that.

$\phi(Ka) = \phi(a) = y$

ϕ is onto.

To prove: ϕ is a homomorphism

$\phi(Ka\ Kb) = \phi(Kab)$

$= \phi(ab)$

$= \phi(a)\,\phi(b)$

$= \phi(Ka)\,\phi(Kb)$

$\therefore \phi$ is an homomorphism

Hence $\phi: G/K \to \bar{G}$ is an isomorphism

(ie) $G/K \cong \bar{G}$.

Lemma (14):

Let ϕ be a homomorphism of G onto $\bar{G}$ with kernal K for H is a subgroup of G. Let H be defined by $H = \{x \in G / \phi(x) \in \bar{H}\}$. Then H is a subgroup of G and H contains K. If $\bar{H}$ is normal in $\bar{G}$. Then H is normal in G. moreover, this association sets are 1-1 mapping. Then the set of all subgroup of G onto the set of all subgroup of G which contains K.

Proof:

To prove:

$K \subseteq H$

Given $\phi: G \to \bar{G}$ is an onto homomorphism.

Let $K = \{x \in G \mid \phi(x) \in H\}$

Let $x \in K$

$\Rightarrow \phi(x) = \bar{e}$

$\Rightarrow \bar{e} \in H$

$\Rightarrow \phi(x) \in H$

$\Rightarrow x \in H$

$\therefore K \subseteq H$

(ii) To prove:

H is a subgroup of G.

(i.e) To prove (a) $x, y \in H \Rightarrow xy \in H$

(b) $x \in H \Rightarrow x^{-1} \in H$

(a) Let $x, y \in H$

$\Rightarrow \phi(x) \in \bar{H}$ and $\phi(y) \in \bar{H}$

Now, $\phi(xy) = \phi(x)\phi(y) \in \bar{H}$

$\Rightarrow xy \in H$.

Thus $x, y \in H \Rightarrow xy \in H$

(b) If $x \in H$

Then $\phi(x) \in \bar{H}$

From lemma (4) we, have,

$\phi(\bar{x}^1) = [\phi(x)]^{-1} \in H$

$\Rightarrow \phi(\bar{x}^1) \in \bar{H}$

$\Rightarrow \bar{x}^1 \in H$

Thus $x \in G \Rightarrow \bar{x}^1 \in H$

From (a) & (b), H is a subgroup of G.

(iii) To prove:

H is normal in G.

(1) TO PROVE: $ghg^{-1} \in H$, $\forall g \in G$ and $h \in H$.

Now $h \in H$

Then $\varphi(h) \in \bar{H}$

Also, $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1})$

$= \varphi(g)\,\varphi(h)[\varphi(g)]^{-1} \in \bar{H}$

$\Rightarrow \varphi(ghg^{-1}) \in \bar{H}$

$\Rightarrow ghg^{-1} \in H$

Thus H is a normal in G.

Suppose L is a subgroup of G and $K \subset L$. define $\bar{L} = \{\bar{x} \in \bar{G} / \bar{x} = \varphi(l), l \in L\}$

TO PROVE:

$\bar{L}$ is a subgroup of $\bar{G}$

let $\bar{x}, \bar{y} \in \bar{L}$

$\Rightarrow \bar{x} = \varphi(l_1)$ & $\bar{y} = \varphi(l_2)$ for some $l_1, l_2 \in L$.

$\therefore \bar{x} \cdot \bar{y} = \varphi(l_1)\varphi(l_2)$

$= \varphi(l_1 l_2) \in \bar{L}$.

$\Rightarrow \bar{x}\bar{y} \in \bar{L}$

Now $(\bar{x})^{-1} = [\varphi(l)]^{-1}$

$= \varphi(l_1^{-1}) \in \bar{L}$

$\Rightarrow (\bar{x})^{-1} \in \bar{L}$.

consider the subgroup $T = \{y \in G$

and $L = \{y \in G / \phi(y) \in I\}$

(80)

Let $x \in L \Rightarrow \varphi(x) \in \bar{L}$

$\Rightarrow x \in T$ ——— (3)

$\therefore L \subseteq T$

Let $t \in T \Rightarrow \varphi(t) \in \bar{I}$

$\Rightarrow \varphi(t) = \varphi(l)$, for some $l \in L$

$\Rightarrow \varphi(t)[\varphi(l)]^{-1} = \varphi(l)\in \bar{I}\varphi(e)$

$\varphi(t)\varphi(l^{-1}) = \bar{e}$

$\varphi(tl^{-1}) = \bar{e}$

$\Rightarrow tl^{-1} \in K$

$\Rightarrow tl^{-1}l \in Kl \in K$

$\Rightarrow t \in KL$

$\Rightarrow t \in L$

$\Rightarrow T \subseteq L$ ——— (4)

From (3) & (4) we have,

$L = T$

Thus we have a 1-1 corresponding between the set of all subgroup of $\bar{G}$ and the set of all subgroup of G which contains K.

Let φ be a homomorphism of G onto $\bar{G}$ with kernal K and $\bar{N}$ be a normal subgroup of $\bar{G}$, $N = \{x \in G / \varphi(x) \in \bar{N}\}$

Then $\frac{G}{N} \cong \frac{\bar{G}}{\bar{N}}$ (or) equivalently

$\frac{G}{N} \cong \frac{(G/K)}{(N/K)}$

Proof:

Given φ is an homomorphism of G onto $\bar{G}$

(ie) $\varphi : G \to \bar{G}$ defined by $\varphi(g) = \bar{g}$, $\forall g \in G$.

consider the map $\varphi : G \to \frac{\bar{G}}{\bar{N}}$ by

$\varphi(g) = N\bar{g}$

(ie) $\varphi(g) = \bar{N}\varphi(g)$, by (1), $\forall g \in G$

To prove φ is onto,

For every $\bar{g} \in \bar{G}$, $\bar{g} = \varphi(g)$

For every element $N\bar{g}$ in $\bar{G}/\bar{N}$ $\exists$ an element $g \in G$ such that,

$\varphi(g) = \bar{N}\bar{g}$

$\therefore \quad = \bar{N}\varphi(g)$

$\therefore \varphi$ is onto.

To prove φ is a homomorphism.

let $a, b \in G$

Then $\varphi(ab) = \bar{N}\varphi(ab)$

$= \bar{N}\varphi(a)\varphi(b)$

$= \bar{N}\varphi(a) \cdot \bar{N}\varphi(b)$

$= \varphi(a) \cdot \varphi(b)$.

$\therefore \varphi$ is a homomorphism of G onto $\bar{G}/\bar{N}$.

(21)

To prove : $N = T$

Given $N = \{x \in G / \varphi(x) \in \bar{N}\}$ be the

Let $T = \{x \in G / \varphi(x) = \bar{N}\}$ be the kernal of φ

If $n \in N$, then $\varphi(n) \in \bar{N}$

$\Rightarrow \varphi(n) = \bar{N}\,\varphi(n)$, by (3). $\because \varphi(n) \in \bar{N}$

$\Rightarrow \varphi(n) = \bar{N}$

$\Rightarrow n \in T$

$\therefore N \subseteq T$ ——— (3)

Let $t \in T$, then $\varphi(t) = \bar{N}$ ——— (4)

But $\varphi(t) = \bar{N}\,\varphi(t)$

$\bar{N}\,\varphi(t) = \bar{N}$, by (4)

$\Rightarrow \varphi(t) \in \bar{N}$

$\Rightarrow t \in N$

$\therefore T \subseteq N$ ——— (5)

from (3) & (5), we have,

$N = T$

Thus φ is a homomorphism.

of G onto $\bar{G}/\bar{N}$ with kernal $T = N$.

$\therefore$ by the fundamental theorem of homomorphism we have,

$$\frac{G}{N} \cong \frac{\bar{G}}{\bar{N}}.$$

Again by fundamental theorem we have,

$\frac{G}{K} \cong G$ and $\frac{N}{K} \cong \bar{N}$

$\therefore \frac{G}{N} \cong \frac{(G/K)}{(N/K)}$

Automorphism:-

definition:

An isomorphism of a group G onto itself its called an automorphism.

Ex:

The identity map is an automorphism.

lemma

If G is a group. Then $A(G)$ is the set of all automorphism of G is also a group

Let $A(G)$ denote the set of all automorphism of G.

Being a subset of $A(G)$ the set of all 1-1 mapping, of G onto itself. For the element of $A(G)$, we can use the product of $A(G)$ is namely composition of matrix.

(184)

Since I is a identity element of G & $A(G)$ is non empty

closure axiom:

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

$(xy)T_1 = (xT_1)(yT_1)$

$(xy)T_2 = (xT_2)(yT_2)$

Now $(xy)(T_1 \circ T_2) = [(xy)T_1]T_2$

$= [(xT_1)(yT_2)]T_2$

$= [[(xT_1)T_2)((yT_1)T_2)]]$

$= (xT_1T_2)(yT_1T_2)$

$\Rightarrow (T_1 \circ T_2) \in A(G)$

$\therefore A(G)$ satisfies the closure axiom.

associative axiom:

Hence associative law is also hold in $A(G)$.

Inverse:

If $x, y \in G$ Then $[xT\bar{T}^{-1})(y\bar{T}^{-1})]T$

$= [(x\bar{T}^{-1})T\,[(y\bar{T}^{-1})T]$

$= [x(T^{-1}T)][y(T^{-1}T)]$

$= (xI)(yI)$

$= (xy)I$

$\Rightarrow (xT^{-1})(yT^{-1}) = (xy)T^{-1}$

$\Rightarrow T^{-1} \in A(G)$

$\therefore A(G)$ is a group.

problem:-

Let g be a fixed elements of a group G. Then the mapping $T_g : G \to G$ defined by

$x T_g = g^{-1} x g$, for every $x \in G$ is an automorphism.

Soln:

Given a mapping $T_g : G \to G$ defined by $x T_g = g^{-1} x g \longrightarrow (1) \; \forall x \in G$

TO prove:

T_g is an automorphism of G.

(i) let $x, y \in G$ we have $x T_g = y T_g$

$\Rightarrow g^{-1} x g = g^{-1} y g$

$\Rightarrow x = y$

$\therefore T_g$ is 1-1

(ii) T_g is onto, for a given $y \in G$,

let $x = g y g^{-1} \in G$

Then $x T_g = g^{-1} (g y g^{-1}) g$.

$= (g^{-1} g) y (g^{-1} \cdot g)$

$x T_g = y$

$\therefore T_g$ is onto.

(86)

Problem:

Let g be a fixed element of a group G. Then the mapping $T_g : G \to G$ defined by

$$xT_g = g^{-1}xg \text{ for every } x \in G$$ is an automorphism

Solution:

Given a mapping $T_g : G \to G$ defined by

$$xT_g = g^{-1}xg$$

(iii) T_g is an homomorphism :-

Let $x, y \in G$, Then $(xy)T_g = g^{-1}(xy)g$

$$= g^{-1}(xIy)g = g^{-1}(xgg^{-1}y)g$$
$$= (g^{-1}xg)(g^{-1}yg)$$
$$= (xT_g)(yT_g)$$

$\therefore T_g$ is a homomorphism

$\therefore T_g : G \to G$ is an isomorphism

Hence T_g is an automorphism.

defined:

Inner automorphism:

Let G be a group for $g \in G$

(87)

defined by T_g

$xT_g = g^{-1}xg$

automorphism

its called an

and is defi

lemma 5.1

automor

non

automo

Proof:

case i)

Let T_g

of G

defined by $T_g : G \to G$ defined by $xT_g = g^{-1}xg \; \forall x \in G$ and T_g is an automorphism. This automorphism is called an inner automorphism and is defined by.

$$I(G) = \{ T_g \in A(G) / g \in G \}$$

Lemma (1)

For an abelian group a only automorphism is identity where as non automorphism.

Proof:

case(i)

Suppose G is an abelian group. Let T_g be an inner automorphism of G. For $x \in G$ we have,

$$\begin{aligned} xIg &= g^{-1}xg \\ &= g^{-1}(xg) \\ &= g^{-1}(gx) \\ &= (g^{-1}g)x = Ix \end{aligned}$$

(ie) $xT_g = xI$

$\Rightarrow T_g = I$

(ie) T_g is an identity map of

case(ii) Let G be non abelian

Then there exists element a,b∈G such that

$\Rightarrow ab \neq ba$

$\Rightarrow b^{-1}(ab) \neq b^{-1}(ba)$

$\Rightarrow (b^{-1}a)b \neq (b^{-1}b)a$

(ie) $b^{-1}ab \neq Ia$

$aTb \neq aI$

$\Rightarrow Tb \neq I$

$\therefore Tb$ is non an identity map of G. Thus for a non-abelian group T a non abelian automorphism.

Case(s)

Let G be non abelian group. Then there exists element a,b∈G such that

$\Rightarrow ab \neq ba$

$\Rightarrow b^{-1}(ab) \neq b^{-1}(ba)$

$\Rightarrow (b^{-1}b)b \neq (b^{-1}b)a$

(ie) $b^{-1}ab \neq Ia$

Lemma (22).

I(G) is an automorphism of group G, where I(G) is a group of inner automorphism of group & Z is a centre of G, (i.e) $I(G) \cong G/Z$.

Proof:

Let $A(G)$ denote the group of all automorphism of G.

$I(G) = \{ T_g \in A(G) / g \in G \}$ be the set of all inner automorphism group G.

TO PROVE: $I(G)$ is a subgroup of $A(G)$

(ie) TO PROVE: (i) $T_{gh} = T_g \cdot T_h$

(ii) $T_g^{-1} = (T_g)^{-1}$

(i) If $x \in G$, we have,

$x T_g T_g^{-1} = (xT_g) T_g^{-1}$

$= (g^{-1} x g) T_g^{-1}$

$= (g^{-1})^{-1} (g^{-1} x g)(g^{-1})$

$= g (g^{-1} x g) g^{-1}$

$= (gg^{-1}) x (gg^{-1})$

$= x \Rightarrow xI$

$\Rightarrow T_g T_g^{-1} = I$

$\therefore T_g^{-1}$ is the inverse of T_g in A

(ie) $(T_g)^{-1} = T_g^{-1}$

(i) If $x \in G$, we have.

$x \cdot T_{gh} = (gh)^{-1} x (gh)$

$= (h^{-1}g^{-1})x(gh)$
$= h^{-1}(g^{-1}xg)h = x\,Tg\,Th$
$\Rightarrow Tgh = Tg\,Th$.

$\therefore I(G)$ is a subgroup of $A(G)$
consider the mapping $\varphi : G \to A(G)$ defined by $\varphi(g) = Tg$, Then φ is a homomorphism.

let $g, h \in G$, we have
$\varphi(gh) = Tgh$
$= Tg \cdot Th$
$= \varphi(g) \cdot \varphi(h)$

$\therefore \varphi$ is a homomorphism of G into $A(G)$ whose image is $I(G)$.

let K be the kernal of φ.
suppose $g_0 \in K$, Then $\varphi(g_0) = Tg_0 = I$
For any $x \in G$, $xTg_0 = xI = x$ ——→ (1)
By defn of Tg_0, we have,

$xTg_0 = g_0^{-1}xg_0$

$\Rightarrow g_0(g_0^{-1}xg_0) = g_0x$

$\Rightarrow xg_0 = g_0x \quad \forall x \in G$

$\therefore g_0$ computes with every element of G.

$\Rightarrow g_0 \in Z$, where Z is a centre of G

$\therefore K \subseteq Z$ —— (3)

Next to prove : $z \subseteq k$

let $z \in z$.

Then $xTz = z^{-1}xz = z$ as centre of G.

$= z^{-1}(zx)$

$xTz = Ix = xI$

$\Rightarrow Tz = I$

$\varphi(z) = Tz = I$

$\Rightarrow z \in I$

$\therefore z \subseteq k$ ——— (4)

from eqn (3) & (4)

$z = k$.

Thus φ is a homomorphism of G into $A(G)$ with image $I(G)$ and Kernal z.

$\therefore$ The fundamental theorem of homomorphism $g(z) \cong G/z$.

Lemma:

Let G be a group and φ is an automorphism of G If $a \in G$ is of order $o(a) = n$ then $o(\varphi(a)) = o(a)$.

Proof:

Suppose φ is an automorphism of G & $a \in G$ has order n.

ie) $o(a) = n$.

(ie) n is least +ve integer such that $a^n = e$ then $[\varphi(a)]^n$

$= \varphi(a)\,\varphi(a) \ldots$ n times $\varphi(a)$

$= \varphi(a \cdot a \ldots$ n times$)$

$= \varphi(a^n)$

$= \varphi(e) = e$

$[\varphi(a)]^n = e$

$\Rightarrow o(\varphi(a)) = n$

If $(\varphi(a))^m = e$ for $0 < m < n$

Then $\varphi(am) = [\varphi(a)]^m = e \Rightarrow \varphi(a^m) = \varphi(e)$

$\Rightarrow a^m = e$

which is a $\Rightarrow \Leftarrow$

This $\Rightarrow \Leftarrow$ shows that $o(\varphi(a)) = n$

(ie) $o(\varphi(a)) = o(a)$.

Theorem: Cayley's theorem

Every group is isomorphic to a subgroup of $A(S)$ for some appropriate S.

Every group is isomorphic to a subgroup of $A(S)$ for some appropriates S.

Proof.

$A(S)$ $\qquad$ $A(S)$

Let G be a group. For a set S be are used the element of G.

(ie) $S = G$

If $g \in G$, $T_g : S(=G) \to S(\in G)$

by $xT_g = xg, \forall x \in G$

To prove T_g is an isomorphism.

(i) T_g is 1-1.

If let $x, y \in S (= G)$

$xT_g = yT_g$

$\Rightarrow xg = yg$

$\Rightarrow x = y$

$\therefore T_g$ is 1-1

(ii) T_g is onto:

If y is an element of codamain. Then $\exists$ an element yg^{-1} in the domain such that,

$(yg^{-1})T_g = (yg^{-1})g$

$= y(g^{-1}g)$

$= y$

$\therefore y$ is onto.

(iii) T_g is homomorphism:

If $g, h \in S (= G)$, for an $x \in S (= G)$, we have, $xT_{gh} \Rightarrow xg$

$= (xg)h \Rightarrow (xg)T_h = (xT_g)T$

$= xT_g T_h$

$\Rightarrow T_g h$

(14)

$\therefore T_g$ is homomorphism

$\therefore T_g$ is an isomorphism

Hence T_g is an automorphism.

$\Rightarrow T_g \in A(S)$

Define the map $\varphi : G \to A(S)$ by,

$\varphi(g) = T_g$

TO PROVE: φ is an homomorphism

Let $g, h \in G$

we have $\varphi(gh) = T_{gh}$

$= T_g T_h$

i.e $\varphi(gh) = \varphi(g) \cdot \varphi(h)$

$\therefore \varphi$ is an homomorphism

Let K be the kernal of φ

TO PROVE : $K = (e)$

If $g_0 \in K$

Then $\varphi(g_0) = I = T_{g_0}$ is the identity element ans.

For $x \in G$, In particular $e \in G$,

$eT_{g_0} = eI = e$ ——— (1)

By defn of T_{g_0}, we have,

$eT_{g_0} = eg_0$

$eI = eg_0 \Rightarrow I = g_0 = (e)$ ——— (2)

From eq (1) & (2) we have

-: by corollary, we have, φ is an isomorphism of G into A(S). (Isomorphism corollary)

Lemma 24:

If G is a group - H is a subgroup of G and S is the set of all right cosets H in G, Then there is a homomorphism φ of G into A(S) and the kernal of φ is the largest normal subgroup of G which is contained in H

Proof: Let G be a group and H is a subgroup of G S is the set of all right cosets of H in G. (ie) $S = \{Hg / g \in G\}$ for $g \in G$, define $T_g : S \to S$ by $(Hx)T_g = Hxg$

TO PROVE:- T_g is an isomorphism.

(i) T_g is 1-1 :-

Let $Hx, Hy \in S$

we have, $(Hx)T_g = (Hy)T_g$.

$Hxg = Hyg$

$Hx = Hy$

$\Rightarrow T_g$ is 1-1

T_g is onto:

For every Hxg is an elemen of the codomain, $\exists$ an element Hx domain $\exists$ (such that)

$(Hx)T_g = Hxg \Rightarrow T_0$ is onto

(46)

(b) If $g,h \in G$ and $x \in S$ we have,
$(Hx)Tgh = Hxgh = (Hxg)h$
$= ((Hx)Tg)h$
$(Hx)Tgh = (Hx)TgTh$
$\therefore Tgh = TgTh$ $\quad Tg$ is an isomorphism
Define a map $\theta : G \to A(S)$ by $\theta(g) = Tg$,
To prove: θ is an homomorphism.
let $g,h \in G$
Then $\theta(gh) = Tgh = TgTh = \theta(g)\theta(h)$
$\therefore \theta$ is a homomorphism of $\theta : G \to A(S)$
let K be a kernal of θ. If $g \in K$, Then
$\theta(g) = Tg = i$ is an identity element of S
For every, $x \in S$, $xTg = x$ since
every element of S is a right cosets of
H in G. $\therefore HxTg = Hx \; \forall x \in G$
If $b \in G$ $\exists$ $Hxb = HxHx \in G$. Thus $K = \{b \in G /$
$Hxb = Hx, \forall x \in G\}$ we claim that,
is contain in H. If N is a normal subgroup
of G which contained in H.
To prove: N must be contained in K. If
$n \in N$, $a \in G$, we have, $ana^{-1} \in N \subseteq H$.
$\Rightarrow ana^{-1} \in H \Rightarrow Hana^{-1} = H \Rightarrow Hana^{-1}a = Ha$
$\Rightarrow Han = Ha \quad \therefore n \in K \Rightarrow \therefore N \subseteq K$.
next to prove: $K \subseteq H$
For $b \in K$, then $Hab = Ha, \forall a \in G$.
In particular, $Hb = Heb = He \Rightarrow Hb = H, \Rightarrow b \in H$
$\therefore K \subseteq H$, Hence the proof of G.

Permutation group:

Let S be a finite set having n distinct element $x_1, x_2, \ldots, x_n$

(e) $S = \{x_1, x_2, \ldots x_n\}$
If $\sigma \in A(S)$ is 1-1 mapping of S onto itself is called a permutation and the set of all permutation from S to S is called a permutation group (or) symmetric group w.r.to the composition of function and it is denoted by S_n.

Remark:

Let S be a set and $\theta \in A(S)$, given two elements $a, b \in S$, we definite $a \equiv_\theta b \Leftrightarrow b = a\theta^i$ for some integer i

TO PROVE: "$\equiv_\theta$" is an equivalence on S.

(i) Reflexive :- since $a = ae = a\theta^0 = \theta^a$.

"$\equiv_\theta$" is reflexive.

(ii) Symmetric :- $a \equiv_\theta b$ then $b = a\theta^i$

$b\theta^{-i} = a\theta^i\theta^{-i} = a\theta^0 \Rightarrow a$ $\quad a = b\theta^{(i)}$

$\Rightarrow b = \theta^a$.

$\therefore$ "θ" is symmetric.

(iii) Transitive :-

let $a = \theta^b$ and $b \equiv \theta^c$

Then $b = a\theta^i$ and $c = b\theta^j$ for some $i \& j$

$c = b\theta^j = (a\theta^i)\theta^j$.

$a \equiv \theta^c$, $\Rightarrow$ "$\equiv_\theta$" is transitive.

from (i), (ii), (iii) we have, "$\equiv_\theta$" is an equivalence relation.

orbit and cycle:

The equivalence class of a element is called the orbit

under σ. The orbit of s under σ consist of $s, s\sigma, s\sigma^2, \ldots, s\sigma^{l-1}$ where $l \geq 1, 2, \ldots$
The cycle of σ is the orbit said to be and its length is l.

Transposition: The cycle of length 2 is called transposition.
Eg: (1 4) is a transposition.

Disjoint cycle: Two cycles are said to be disjoint if they have no symbol in common.
Eg: (1, 3, 5) and (2, 6, 8, 9) are disjoint cycles. (1, 3)(1, 5) transposition.

Lemma:
Every permutation is a product of the cycles.
Proof: Let σ be the permutation then its cycles are of the form $(s, s\sigma, s\sigma^2, \ldots s\sigma^{l-1})$
By multiplication of cycles as defined above of s's ∈ S under σ is $s\sigma$ is the same as the image of s under the product φ of all the disjoint cycles of σ. So σ and φ have a same effect and every element of S.

Remark:
Every permutation can be uniquely expressed as a product of disjoint cycle.

6. Lemma
Every permutation is a product of 2 cycles (or) transposition.

proof: Consider a m cycles (1, 2, ... m) (1, 2, 3, ... m) = (1, 2) (1, 3) ... (1 m) more generally there m cycles $a_1, \ldots a_m$ = $(a_1 a_2)(a_1 a_3) \ldots (a_1 a_m)$. This decomposition is not unique. by this we mean that the m cycles can be written as a product of two cycles in more than one way.

By lemma 25, every permutation is a product of disjoint cycle and every cycles $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 7 & 1 & 6 & 2 & 9 & 8 \end{pmatrix}$ of product of.

Hence very permutation is a product of two cycles.

Even permutation: A permutation $\in S_n$ is said to be an even permutation, if it can be represented as a product of even numbers of transposition odd, if it is not an even permutation.

Note:

① The product of 2 even permutation is an even permutation.

② The product of 2 odd is an even permutation.

③ The product of even permutation and odd permutation is odd.

④ Identity permutation is also even.

Lemma: S_n has a normal subgroup of index 2 the alternative group A_n consisting of all even permutation

Proof: Let A_n be the subset of S_n consisting of all even permutation. Since the product of 2 even permutation is even. A_n must be a subgroup of S_n. We claim that

Let W be the group of real nos, $\{1, -1\}$ under multiplication. Define $\varphi: S_n \to W$ by

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

TO PROVE: φ is a homomorphism.

Case(i) Let $s_1, s_2 \in$ of S_n and both are odd permutation in S_n

Then $\varphi(s_1 s_2) = 1 = -1, -1$
$= \varphi(s_1) \cdot \varphi(s_2)$

Case(ii) Let s_1 be an odd permutation and s_2 be an even permutation. Then $\varphi(s_1 s_2) = -1$,
$= -1 \cdot 1 = \varphi(s_1) \cdot \varphi(s_2) \Rightarrow \varphi$ is a homomorphism

Then the kernal of φ is A_n, being the kernal of the homomophism, A_n is a normal subgroup of S_n.

homomorphism: $\frac{S_n}{A_n} \approx W$

$O(W) = 2$, $\therefore O\left(\frac{S_n}{A_n}\right) = O(W)$

$\Rightarrow \frac{O(S_n)}{O(A_n)} = 2$, $\Rightarrow \frac{n!}{O(A_n)} = 2$

$\Rightarrow O(A_n) = \frac{n!}{2}$.

UNIT - II

(1) Theorem :-

First part of sylow's theorem:

If p is a prime number and $p^d / o(G)$. Then G has a subgroup of order p^d.

Proof:

We prove this theorem by induction on $o(G)$

(i.e) For every prime p dividing order of G.

To prove,

G has a p-sylow subgroup of order p^d.

If $o(G) = 1$

It is trivially true

If $o(G) = 2$

Then $(0) = 2$

∴ The subgroup of G order 2 is G itself.

Assume that:

This theorem is true for all group of order less than $O(G)$

We have to prove:

This theorem is true for $O(G)$ Suppose,

$p^\alpha \mid O(G)$ and $p^{\alpha+1} \nmid O(G)$

where $\alpha \geq 1$ and p is prime

If $p^\alpha \mid O(G)$ for any sub-group H of G. where $H \neq G$

$\therefore O(H) < O(G)$

By induction then there exists a subgroup T of H such that $O(T) = p^\alpha$.

Since T is a subgroup of H.

H is a sub group of G.

T is a subgroup of G and $O(T) = p^\alpha$

If $p^\alpha \nmid O(H)$ for any subgroup H of G

(69)

where $H \leq G$ iff $a \in G$ then $N(a) = \{x \in G / xa = ax\}$ is a subgroup of G.

$a \in Z(G) \Leftrightarrow o(N(a)) \neq o(G)$

$\Leftrightarrow N(a) \neq G$.

since $N(a)$ is a subgroup of G.

$p^\alpha \nmid o(N(a))$ and $p^\alpha \mid o(G)$

$p \mid \frac{o(G)}{o N(a)}$ $\forall$ $a \in Z(G)$

$p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o N(a)}$ ⟶ (A)

But from the class eqn.

$$o(G) = o(Z(G)) + \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$

$$o(Z(G)) = o(G) - \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$$ ⟶ (1)

Since $p^\alpha \mid o(G)$

we have $p \mid o(G)$ and

$p \mid \sum_{a \notin Z(G)} \frac{o(G)}{o(N(a))}$ $\Rightarrow p \mid o(Z(G))$

(104) If p is a prime number, $p \mid O(G)$ then G has a By cauchy's theorem element of for finite group there order exist an element of order p. p. ? using of the

$a \neq e \in Z(G)$

Let $B = \langle a \rangle$ then $O(B) = O(a) = p$

Also, B is a subgroup of $Z(G)$ and B is a normal subgroup of G.

$\therefore$ The quotient group of G is in the form.

$$\frac{G}{B} = \bar{G}$$

$$O(\bar{G}) = O(G/B)$$

$$= \frac{O(G)}{O(B)}$$

$$= \frac{O(G)}{P}$$

$$O(\bar{G}) < O(G)$$

$p^{\alpha-1} \mid O(\bar{G})$ and $p^{\alpha} \nmid O(\bar{G})$

05

$$\begin{pmatrix} p^{\alpha+1} \nmid o(G) \\ p^{\alpha} \nmid \frac{o(G)}{p} \\ p^{\alpha} \nmid o(\bar{G}) \end{pmatrix} \begin{pmatrix} p^{\alpha} \mid o(G) \\ p^{\alpha-1} \mid \frac{o(G)}{p} \\ p^{\alpha-1} \mid o(\bar{G}) \end{pmatrix}$$

By induction there exist a subgroup $\bar{P}$ of $\bar{G}$, such that,

$$o(\bar{P}) = p^{\alpha-1}$$

Let $P = \{ x \in G / xB \in \bar{P} \}$

clearly, P is a subgroup of G. By fundamental theorem of homomorphism.

$$\bar{P} \cong P/B$$

$$p^{\alpha-1} = o(\bar{P}) = o(P/B) = \frac{o(P)}{o(B)}$$

$$o(P) = p^{\alpha-1} o(B)$$

$$= p^{\alpha-1}(p)$$

$$= p^{\alpha}$$

$$o(P) = p^{\alpha}$$

hence the Proof.

(106)

Theorem:-
second part of sylow theorem:

If G is a finite group p is a prime and $p^n / o(G)$ but $p^{n+1} \nmid o(G)$. Then every two subgroup of G of order p^n are conjugate.

Pf:

Gn G is a finite group. p is prime and $p^n / o(G)$ but $p^{n+1} \nmid o(G)$.

Let A and B be two subgroup of G each of order p^n.

$\therefore o(A) = o(B) = p^n$.

To prove,

$A \sim B$

i.e) To prove $A = xBx^{-1}$ for some $x \in G$.

Decompose G into double coset of A and B

i.e) $G = U[x]$.

$x \in G$

$= \bigcup_{x \in G} AxB$ (by Lemma)

$O(G) \leq \sum_{x \in G} O(AxB) \longrightarrow (1)$

$O(AxB) = \frac{O(A) \cdot O(B)}{O(A \cap xBx^{-1})} \longrightarrow (2)$

Suppose A is not conjugate to B then (AxB) then $A \neq xBx^{-1} \; \forall \; x \in G$ since $(A \cap xBx^{-1})$ is a subset of A.

i.e) $A \cap (xBx^{-1}) \leq A$

$\therefore O[A \cap xBx^{-1}] \leq O(A)$

Let $O(A \cap xBx^{-1}) = p^m$

when $m \leq n$.

case i)

If $m = n$ then $p^m = p^n$

$O(A \cap xBx^{-1}) = p^n = O(H)$

$\therefore A \cap xBx^{-1} = A$

$A = xBx^{-1}$

$O(A) = O(B) = O(xBx^{-1}) = p^n$.

The number of p-sylow subgroup in G for a prime p is of the form. $1+kp$. k is an integer.

Proof:

Let p be a p-sylow subgroup of G and $O(p) = p^n$.

We decompose G into double cosets of p and p.

$$G = \bigcup_{x \in G} [x] = \bigcup_{x \in G} (pxp)$$

$$O(G) = \sum_{x \in G} O(pxp) \quad \text{---} (1)$$

$$O(pxp) = \frac{O(p) \cdot O(p)}{O(p \cap xpx^{-1})}$$

$$= \frac{[O(p)]^2}{O(p \cap xpx^{-1})}$$

$$= \frac{p^{2n} \cdot p^n \cdot p^n}{O(p \cap (xpx^{-1}))}$$

$$(p^n \cdot p^n) = p^{2n}.$$

(11a)

$N(P) = \{x \in G \mid xp = px\}$

$= \{x \in G \mid xpx^{-1} = p\}$

If $x \in N(P)$, $xpx^{-1} = p$

$p \cap xpx^{-1} = p \cap p = p$

$O(p \cap xpx^{-1}) = O(p) = p^n$.

Also, $p(xp) = p(px) = px$

$\therefore \quad O(pxp) = O(px) \quad \forall x \in N(P)$

$$\sum_{x \in N(P)} O(pxp) = \sum_{K \in N(P)} O(px)$$

$$\sum_{x \in N(P)} O(pxp) = \sum_{x \in N(P)} O(px)$$

$$= O(N(P)) \longrightarrow (2)$$

If $x \notin N(P)$, $xpx^{-1} \neq P$

since $p \cap xpx^{-1} \subseteq p$

$O(p \cap xpx^{-1}) \leq O(p) = p^n$

Let $O(p \cap xpx^{-1}) = p^m$ where $m < n$.

$$O(pxp) = \frac{p^{2n}}{p^m}$$

$= p^{2n-m}$ if $x \notin N(P)$

$2n - m \geq$

$\therefore p^{n+1} \mid p^{2n-m} \Rightarrow o(xP) \forall x \notin N(P)$

$\therefore p^{n+1} \mid \sum_{x \notin N(P)} o(xP)$

There exists an $u \in \mathbb{Z}$ such that,

$$\sum_{x \in N(P)} o(xP) = up^{n+1} \quad \text{---(3)}$$

$$(1) \Rightarrow o(G) = \sum_{x \in G} o(xP)$$

$$= \sum_{x \in N(P)} o(xP) + \sum_{x \notin N(P)} o(xP)$$

$$o(G) = o(N(P)) + up^{n+1} \text{ (using (2) and (3))}$$

$$\frac{o(G)}{o(N(P))} = 1 + \frac{up^{n+1}}{o(N(P))} \quad \text{---(4)}$$

Since $N(P)$ is subgroup of G then by lagrange's theorem.

$o(N(P)) \mid o(G)$

$\therefore \frac{o(G)}{o(N(P))}$ is an integer

(10)

$\therefore p^{n+1} / p^{2n-m} = o(pxp) \; \forall \; x \notin N(p)$

$\therefore p^{n+1} \Big| \sum_{x \notin N(p)} o(pxp)$

There exists an $u \in \mathbb{Z}$ such that,

$$\sum_{x \in N(p)} o(pxp) = up^{n+1} \quad \text{---} (3)$$

$(1) \Rightarrow o(G) = \sum_{x \in G} o(pxp)$

$$= \sum_{x \in N(p)} o(px^p) + \sum_{x \notin N(p)} o(pxp)$$

$o(G) = o(N(p)) + up^{n+1}$ (using (2) and (3))

$$\frac{o(G)}{o(N(p))} = 1 + \frac{up^{n+1}}{o(N(p))} \quad \text{---} (4)$$

Since $N(p)$ is subgroup of G then by Lagrange's theorem.

$o(N(p)) \mid o(G)$

$\therefore \frac{o(G)}{o(N(p))}$ is an integer

From ④ $\frac{Up^{n+1}}{O(N(P))}$ is an integer

Say r.

$\therefore \frac{Up^{n+1}}{O(N(P))} = r$ say ⟶ ⑤

since P is a subgroup of N(P) then by lagrange's theorem.

$O(P) \mid O(N(P))$

$\therefore \frac{O(N(P))}{O(P)} = S$ (integer)

$\therefore O(N(P)) = p^n \cdot S$ ⟶ ⑥

$\therefore \frac{Up^{n+1}}{p^n \cdot S} = r$

$Up = rS \Rightarrow P/rS$

If $P/S \Rightarrow p^{n+1} / p^n \cdot S$

$\Rightarrow p^{n+1} / O(N(P))$ by ⑥

and $O(N(P)) / O(G)$

$\Rightarrow p^{n+1} / O(G)$

$\Rightarrow \Leftarrow$ to $p^{n+1} \nmid O(G)$

(113)

$\therefore p | r$

$\Rightarrow r/p = k$ is an integer

but $r \not\mid p = v/s$

$r/p = k = v/s$

From (3) $\Rightarrow$ (4) $\Rightarrow$

$$\frac{O(G_1)}{O(N(P))} = 1 + \frac{vp^{n+1}}{O(N(P))} \text{ using (6)}$$

$$\frac{O(G_1)}{O(N(P))} = 1 + \frac{vp^{n+1}}{p^n \cdot s}$$

$$= 1 + \frac{v \cdot p}{s}$$

$$= 1 + v/s \cdot p$$

$$= 1 + kp$$

by above lemma the number of p By low subgroup index as

$$\therefore \frac{O(G)}{O(N(P))}$$

$$\therefore \frac{O(G_1)}{O(N(P))} = 1 + kp.$$

hence the proof.

(14) Another counting principle:

If $a, b \in G$. Then b is said to be a conjugate of a in G, if there is an element $c \in G$ such that $b = c^{-1}ac$.

It is denoted by $a \sim b$.

① Lemma:

conjugacy is an equivalence relation on G.

Let G be a group $(G, \cdot)$

Let $a, b \in G$

defined the relation conjugacy

$a \sim b \Rightarrow b = c^{-1}ac$ for some $c \in G$

To prove,

conjugacy is an equivalence relation.

(i.e) To prove,

(i) $a \sim a$ (reflexive)

(ii) $a \sim b = b \sim a$ (symmetric)

(iii) $a \sim b,\ b \sim c \Rightarrow a \sim c$ (transitive)

For (i)

Let $a \in G$

clearly $e \in G$

$a = e^{-1}ae$

$a \sim a$

$\sim$ is reflexive.

For (ii)

Gn $a \sim b$

(ie) $b = c^{-1}ac$

$(c^{-1})^{-1} bc^{-1} = (c^{-1})^{-1} c^{-1} a c c^{-1}$

$(c^{-1})^{-1} bc^{-1} = a$

$y^{-1} by = a$

$\therefore b \sim a$ (where $y = c^{-1}$)

$\sim$ is symmetric.

For (iii) Gn $a \sim b,\ b \sim c \Rightarrow a \sim c$

Let $a, b \in G$

suppose $a \sim b$ and $b \sim c$

(i.e) $b = x^{-1} ax$ and $c = x^{-1} bx$

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

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

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

Z(G) is centre.

C(a) is conjugate, N(a) normalizer

$a \nsim c$

n transitive, hence conjugate is an equivalence relation.

conjugate class:

For $a \in G$ Let $C(a) = \{x \in G$

$a \sim x\} = \{x \in G : x = c^{-1} a c$ for some $c \in G\}$ This equivalence class containing is called conjugate class of a in G. we write $|a|$ to denote the number of elements in $C(a)$.

ie) $= o\, c(a)$

Normalizar of a:-

If $a \in G$, then $N(a)$ the normalizer of a in G is the set $N(a) = \{x \in G; xa = ax$

Lemma:

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

Subgroup $x, y \in N(a)$

Then $xa = ax$ and $ya = ay$

Now,

$$(xy)a = x(ya)$$
$$= x(ay)$$
$$= (xa)y$$
$$= (ax)y$$
$$= a(xy).$$

(ie) $x, y \in N(a)$ when $x, y \in N(a)$

Also,

$$x^{-1}a = x^{-1}ae$$
$$= x^{-1}a(xx^{-1})$$
$$= x^{-1}a(xx^{-1})$$
$$= x^{-1}(ax)x^{-1}$$
$$= x^{-1}(xa)x^{-1}$$
$$= x^{-1}xax^{-1} = eax^{-1} = ax^{-1}$$

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

$\therefore N(a)$ is a subgroup of G.

Theorem:- 4.

class equation:

If G is a finite group and then $C_a = \frac{O(G)}{O N(a)}$.

Ring identity element - 0
" " - 1
group "

UNIT - III

Ring theory : (associative Ring)

A non-empty set R is said to be an associative ring if in R there are defined two operations denoted by + and ·, respectively, such that $\forall a, b, c \in R$

* $a+b$ is in R.
* $a+b = b+a, \forall a, b \in R$
* $a+(b+c) = (a+b)+c \quad \forall a, b, c \in R$
* There is an element $0 \in R$ such that $a+0 = 0+a = a$ for every $a \in R$.

* There exists an element $a \in R$ such that $-a+a = a+(-a) = 0 \; \forall \; a \in R$
* $a \cdot b$ is in R
* $a \cdot (b \cdot c) = (a \cdot b) \cdot c \; \forall \; a, b, c \in R$
* $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$
* $(b+c) \cdot a = b \cdot a + c \cdot a \; \forall \; a, b, c \in R$

} Distributive law

2m / 8

Commutative ring: (abelian) (given in a group?)

A ring R is called a commutative ring if $a \cdot b = b \cdot a$ for every $a, b \in R$

Example:

$(R, +, \cdot)$ is a ring

R is the set of even integers under the usual operators of addition and multiplication. R is a commutative ring but has no unit element.

R is the set of integers mod 7 under the addition & multiplication mod 7 the element of R the seven symbols,

0, 1, 2, 3, 4, 5, 6.

(19) Divisor ring (or) skew field:

A ring in which the non-zero elements from a group is called a divisor ring (or) skew field. (or) zerodivisors.

Some special classes of rings:

Zero divisor:

If R is a commutative ring. Then $a \neq 0$ in R is said to be zero divisor. if there exist $a, b \in R$ $b \neq 0$ such that $ab = 0$

Ex:

$$\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ +1 & -1 \end{pmatrix} = \begin{pmatrix} -1+1 & 1-1 \\ 1-1 & -1+1 \end{pmatrix}$$

$$\begin{bmatrix} ab=0 \\ a\neq 0 \\ b\neq 0 \end{bmatrix} \quad ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Zerodivisors.

Integral domain:

A commutative ring is an integral domain if it has no zero divisor. $ab \neq 0$ $a=0$ $b=0$

Ex:-

A Finite integral domain is an field.

(18) **Division Ring:**

A ring is said to be an division ring if it's non-zero elements form a group under multiplication.

(19) **Field:**

A field is a commutative division ring.

Ex:- Q, R and C are fields under usual addition and multiplication.

imp (1) Bm (2) **Lemma:-**

If R is an ring then for all a, b ∈ R,

i) $a \cdot 0 = 0 \cdot a = a$

ii) $a(-b) = (-a)b = -ab$

iii) $(-a)(-b) = ab$

iv) If in addition R has unique element,

v) Then $(-1)a = -a$ $(-1)(-1) = 1$.

Proof:

For i)

If $a \in R$ Then $a \cdot 0 = a(0+0)$

$= a \cdot 0 + a \cdot 0$

$0 = a \cdot 0$ [RCL]

[Right distributive law]

similarly,

$0.a = (0+0)a$

$= 0.a + 0.a = a$ [LeL]

$a.0 = 0.a = 0$

For (ii) :-

Let $a, b \in R$ be arbitrary then

$a(-b) = (-a)b \Rightarrow -(ab)$

$a(-b) = -(ab)$

$a(-b) + (ab) = 0$

$a(-b+b) = 0$

$a.0 = 0$

$0 = 0$

$a(-b) + ab = 0$

$a(-b) = -(ab)$

$\Rightarrow (-a)b = -(ab)$

$\Rightarrow (-a)b + ab = 0$

$\Rightarrow (-a+a)b = 0$

$\Rightarrow 0.b = 0$

$\Rightarrow 0 = 0$

Hence $(-a)b = -ab$

sly,

$a(-b) = -ab$.

$(-a)b = -ab$

$= a(-b) \forall a, b \in R$

For (iii)

Let $a, b \in R$ be arbitrary

Then,

$$(-a)(-b) = -[a(-b)]$$

$$= -[-(ab)] = ab$$

Thus $(-a)(-b) = ab \quad \forall a, b \in R$.

For (iv)

Suppose that R has a unit element 1.

Then, $(a + (-1)a = 1 \cdot a + (-1)a$

$$= (1 + (-1))a$$

$$= 0 \cdot a$$

$$= 0$$

Hence $(-1)a = -a$

For (v)

In particular if $a = -1$

$$(-1)(-1) = -(-1) = 1$$

hence the lemma.

The pigeonhole principle:-

If n-objects are distributed over m-places and if $n > m$ then some place received atleast two objects

Lemma :-

A finite integral domain is a field.

Proof :

Let $R = \{x_1, x_2, x_3 \ldots x_n\}$ be an integral domain with n elements.

Let a in R $a \neq 0$

Consider the subset aR of R

$aR = \{ax_1, ax_2 \ldots, ax_k\}$

Now,

$ax_i = ax_j \Rightarrow x_i = x_j \quad i \neq j$

hence aR contains n distinct element of R

So $aR = R$

If $a \in R \Rightarrow a \in aR$

$\Rightarrow a = ax_d, x_d \text{ in } R$

We know that,

x_d is unity element in R

$x_i \in R \Rightarrow x_i \in aR$

$\Rightarrow x_i = ax_ix_d = (ax_d)x_i$

$= a(x_d)x_i$

$= ax_i$

$= x_i$ [$ax_d = a$]

$\Rightarrow xd$ is unity in R

Take $xd = 1$

a in R, $a \neq 0$

$\Rightarrow R = aR$

$\Rightarrow 1$ in aR

$\Rightarrow 1 = aR$

$\Rightarrow x = a^{-1}$

Thus every non-zero element in R is invertible.

Thus non-zero element has a multiplication inverse in R. Any finite integral domain is a field.

Corollary:-

If P is a prime number then JP the ring of integers mod p is a field.

proof:

By the above lemma it is enough to prove that JP is an integer domain.

since it has only finite number of elements.

If $a, b \in Jb$ and $ab = 0$ Then P must divide the ordinary

Finite charecteristic :-

An integral domain D is said to be finite charec-teristic if there exist a +ve integer m such that $ma = 0 \; \forall \; a \in D$.

Homomorphism :

A mapping ϕ from the ring R into the ring R' is said to be homomorphism If,

(i) $\phi(a+b) = \phi(a) + \phi(b)$

$\phi(ab) = \phi(a)\phi(b) \; \forall \; a, b \in R$

Lemma :-

If ϕ is a homomorphism of ring R into R'

Then (i) $\phi(a) = 0$

(ii) $\phi(-a) = -\phi(a)$ for every $a \in R$.

Proof: For (i):

Let $a \in R$ and $\phi(a) = \bar{a}$.

Then $\bar{a} + \phi(0) = \phi(a) + \phi(0)$.

$ar \in I(\phi)$

$\phi(ra) = \phi(r) \cdot \phi(a)$

$= \phi(r) \cdot 0$

$= 0 \Rightarrow ra \in I(\phi)$

If $a \in I(\phi)$, $r \in R$ both ar, $ra \in I(\phi)$.

Zero homomorphism :-

Let R and R' be two arbitrary rings and define $\phi(a) = 0$ $\forall a \in R$. trivially ϕ is a homomorphism and $I(\phi) = R$. ϕ is a called Zero homomorphism.

Isomomorphism :-

A homomorphism of R into R' is said to be an isomorphism if it is one-one mapping.

Isommorphism :

Two Rings are said to be isomorphic if there is an isomorphism of one, onto then other.

$\Rightarrow \phi(x) - \phi(y) = 0$

$\Rightarrow \phi(x) + \phi(-y) = 0$

$\Rightarrow \phi(x-y) = 0$

$\therefore \phi$ is one to one

Definition :-

A homomorphism of the group to itself is called an endomorphism.

If f is an homomorphism and onto then f is called epimorphism.

If f is a homomorphism and bijection then f is called isomorphism. A isomorphism of a group to itself is called on automorphism.

UNIT - IV

Ideals and Quotient Ring :-

Right ideal :-

A non-empty subset U of a ring R is said to be a

right ideal of R.
(i) U is a subgroup of R under addition.
(ii) for all $a \in U, r \in R \Rightarrow ar \in U$

Left ideal :-
A non-empty subset U of a ring R is said to be a left ideal of R. if
(i) U is a subgroup of R under addition.
(ii) for all $a \in U, r \in R$
$\Rightarrow ra \in U$.

Two sided ideal :-
A non-empty subset U of a ring R is said to be two sided of R.
(i) U is a subgroup of R under addition.
(ii) for all $a \in U, r \in R \Rightarrow ra \in U$

Result :-

(iii) In a commutative ring ideal = left ideal.

Lemma

If U is an ideal of a ring R then R/u is a ring and is a homomorphic image of R.

Proof:

denote $R/u = \{x+u \mid x \in U\}$ is a ring with respect to the following operation.

To prove,

(i) $(x+u)+(y+u) = (x+y)+u$

(ii) $(x+u)(y+u) = xy+u$

where $x+u, y+u \in R/u$.

The ring is called the Quotient ring of R with respect to u.

For (i)

To prove, R/u is well defined,

Suppose,

$x+u = x'+u$

$y+u = y'+u$

$\Rightarrow x-x' \in u,\ y-y' \in u$.

$\Rightarrow x = x'+u,\ y = y'+u$.

let $x-x' = a,\ y-y' = b$

$\Rightarrow (x+y) = (x'+a)+(y'+b)$

$= (x'+a)+(y'+b)$

$= (x'+y')+(a+b)$

$\Rightarrow (x+y)-(x'+y') = a+b;\ a+b \in U$

$\Rightarrow (x+y)-(x'+y') \in U$

$\Rightarrow (x+y)+u = (x'+y')+u$

$\Rightarrow (x+u)+(y+u) = (x'+u)+(y'+u)$

hence (i) is well defined.

For (ii)

$(xy) = (x'+a)(y'+b)$

$= x'(y'+b)+a(y'+b)$

$= x'y'+x'b+ay'+ab$

$xy-x'y' = x'a+ay'+ab \in u$.

$xy-x'y' \in u$

$\Rightarrow xy+u = x'y'+u$

$(x+u)(y+u) = (x'+u)(y'+u)$

hence (ii) is well defined.

To prove,

R is one-one

suppose $x+u = y+u$

$x-y \in u$.

(38) (1mp) 5m U-a

Fundamental theorem of homomorphism: 5m Q

[let R, R' be rings and ϕ be a homomorphism of R onto R with kernal φ then R' is isomorphic to R/u] Moreover there is a one-one correspondence between the set of ideals of R' and the set of R which contains u.

The correspondence can be achieved by associating with an ideal w' in R'. The ideal w in R is defined by.

$w = \{x \in R / \phi(x) \in w'\}$ with w so defined R/w is isomorphic to R'/w'.

Proof:-

Define $\phi: R \to R/u$ by $\phi(x) = x+u$ $\forall x \in R$

To claim that,

ϕ is an onto homomorphism

ϕ is onto.

let $x+u \in R/u$

$\Rightarrow x \in R$

$\Rightarrow \phi(x) = x+u$

hence ϕ is onto.

(39)

TO prove,

$\phi(x+y) = \phi(x) + \phi(y)$ $\forall$ $x, y \in R$

let $x, y \in R$ be arbitrary

Then

$\phi(x+y) = (x+y)+u$

$= (x+u)+(y+u)$

$= \phi(x) + \phi(y)$ $\forall x, y \in R$

$\phi(xy) = xy+u$

$= (x+u)(y+u)$

$= \phi(x)\phi(y)$ $\forall x, y \in R$

hence R/u is a homomorphic image of R,

conversely,

let R' be the homomorphic image of the ring R with kernal 0.

Suppose $\phi: R \to R'$ is the given ring homomorphism.

define $\varphi: R/0 \to R'$ by

$\varphi(x+u) = \phi(x)$ $\forall$ $x+u \in R/0$.

TO Prove,

φ is well defined

Suppose $x+u = y+u$ where $x+u, y+u \in R$

$\Rightarrow x-y \in u$.

$\phi(x-y) = 0$.

$\Rightarrow \phi(x) + \phi(-y) = 0$

$\Rightarrow \phi(x) - \phi(y) = 0$

$\Rightarrow \phi(x) = \phi(y)$

$\Rightarrow \varphi(x+u) = \varphi(y+u)$

Let $x+u, y+u \in R/v$ be arbitrary

$\varphi[(x+u)+(y+u)] = \varphi[(x+y)+v]$

$= \phi(x+y)$

$= \phi(x) + \phi(y)$

$= \varphi(x+v) + \varphi(y+v)$

$\varphi[(x+v)(y+v)] = \varphi(xy+v)$

$= \varphi(xy)$

$= \varphi(x)\,\varphi(y)$

$= \varphi(x+v)\varphi(y+v) \forall x+u, y+u \in R/v$

φ is onto:-

Let $x' \in R'$

$\Rightarrow$ There is $x \in R$ such that $\phi(x) = x'$

$\Rightarrow x+v$ in R/v and

$\varphi(x+v) = \phi(x) = x'$

φ is one-one:

Suppose $\varphi(x+u) = \varphi(y+v)$ $\forall$

$x+v, y+v \in R/v$

$\Rightarrow \phi(x) = \phi(y)$

$\Rightarrow \phi(x-y) = 0$

$x+v = y+v$

hence $R \cong R/v$

Define a mapping $\varphi: R/\omega \to R'/\omega'$

by $\varphi(a+\omega) = \phi(a) + \omega'$ $\forall a \in R$

φ is well defined.

Let $a_1+\omega = a_2+\omega$

$a_1 = a_2 \in \omega$

$a_1 - a_2 \in \omega$

$\Rightarrow \phi(a_1 - a_2) = 0$

$\phi(a_1) = \phi(a_2)$

$\phi(a_1)+\omega' = \phi(a_2)+\omega'$

$\phi(a_1+\omega) = \phi(a_2+\omega)$

φ is well defined.

φ is onto:

$\varphi(a) \in R'/\omega'$

$\Rightarrow a \in R$

$\Rightarrow \phi(a) = a_1 + \omega \in R/\omega$

$\Rightarrow \phi(a+\omega) = \phi(a) + \omega'$

φ is one-one:

$\varphi(a_1+\omega) = \varphi(a_2+\omega)$

$\phi(a_1)+\omega' = \phi(a_2)+\omega'$

$\phi(a_1 - a_2) \in \omega'$

$a_1+\omega = a_2+\omega$.

(i) $\varphi[(a+\omega)+(b+\omega)] = \varphi[(a+b)+\omega]$

$= \varphi(a+b)+\omega'$

$= \varphi(a)+\omega' + \varphi(b)+\omega'$

$= \varphi(a+\omega) + \varphi(b+\omega)$

(ii) $\varphi[(a+\omega)(b+\omega)] = \varphi[ab+\omega]$

$= \phi(ab)+\omega'$

$= [\varphi(a)+\omega'][\varphi(b)+\omega']$

$= \varphi(a+\omega)\,\varphi(b+\omega)$

let $x \in$ kernal φ

$\Rightarrow x \in R$ such that $\phi(x) = 0$ in R'/ω'

$\Rightarrow x \in R$ $\varphi(x) = 0$

$\Rightarrow x \in R$ $\exists$ $x+\omega = \omega$

$\Rightarrow x \in R$ $\exists$ $x \in \omega$

$\Rightarrow x \in \omega$.

kernal $\varphi \subseteq \omega$ ——— ①

let $x \in \omega$

$\Rightarrow x \in R$ $\exists$ $x \in \omega$

$\Rightarrow x \in R$ $\exists$ $x+\omega = \omega$

$\Rightarrow x \in$ kernal φ

$\omega \subseteq \ker\varphi$ ——— ②

More ideals and quotient Rings:-

Let R be a commutative ring with unit element whose only ideals are 0 and R Itself Then R is field.

proof:

Given R is a commutative ring with unit element whose only ideals are 0 and r itself.

TO Prove,

R is field

for any $a \neq 0 \in R$.

There is an element $b \neq 0 \in R$ such

Suppose that $a \neq 0 \in R$

consider, the set $Ra = \{ra / r \in R\}$

we claim that,

Ra is an ideal of R, in order to prove this we must show, that,

Ra is a subgroup of R under addition.

If $v \in Ra$ and $r \in R$.

$\Rightarrow ru \in Ra$

since R is a commutative ring

$ru = ur$

Now, if $u, v \in Ra$.

Then $u = r_1 a$, $v = r_2 a$ forsome

$r_1, r_2 \in R$.

(144)

Thus $u+v = r_1a + r_2a$

$= (r_1+r_2)a \in Ra \quad \forall r_1, r_2 \in R$

similarly,

$-u = -r_1 a = (-r_1)a \in Ra$

hence Ra is additive subgroup of R

If $r \in R$, $ru = r(r_1 a)$

$= (r r_1)a \in Ra$.

$\therefore$ Ra is an ideal of R

By our assumption on R

$Ra = (0)$ or $Ra = R$.

$0 \neq a$

$\therefore a \in Ra$

$\Rightarrow Ra \neq (0)$

Thus $Ra = R$

Every element in R is a multiple of by some element of Ra.

In particular if $1 \in R$

Then it is realised that 1 is a multiple of a.

i.e) $\exists$ an element $b \in R$ such that $ba = 1$.

hence the proof

(145)

Maximal ideal

An ideal $M \neq R$ in a ring R is said to be an maximal ideal of R If whenever U is an ideal of R such that $M \subset U \subset R$ Then either $R = U$ or $M = U$

ex:

A field F has a only two ideals F and $\{0\}$ It is easy to see then that $\{0\}$ is the only maximum ideal of F.

Theorem:

If R is a commutative ring with unit element and M is an ideal of R then (M is a maximal ideal of R) iff (R/m is a field).

Proof:

Assume that:

R/m is a feild

TO PROVE,

M is a maximal ideal of R

Then $M \neq R$ has atleast two elements

$M \subset U \subset R$.

If $m \neq u$, Then there is $a \in U$.

$a \notin m$

$\Rightarrow a + M \neq M$

$\Rightarrow (a+m)^{-1}$ exist

let $\beta + m = (a+m)^{-1}$

For $(a,b) \sim (c,d) \Leftrightarrow ad = bc$.

$\Leftrightarrow bc = ad$

$\Leftrightarrow cb = da$

$\Leftrightarrow (c,d) \sim (a,b)$.

$\sim$ is transitive:

$(a,b) \sim (c,d)$ and $(c,d) \sim (g,h)$

$\Rightarrow (a,b) \sim (g,h)$.

For $(a,b) \sim (c,d)$ and $(c,d) \sim (g,h)$

$\Leftrightarrow ad = bc$ and $ch = dg$

$\Leftrightarrow adh = bch$ and $bch = bdg$

($\because bh \neq 0$)

$\Leftrightarrow adh = bdg$

$\Leftrightarrow ah = bg$ $\quad d \neq 0$

D has no zero divisor

$\Leftrightarrow (a,b) \sim (g,h)$

$\sim$ is an equivalence relation on D. Now the equivalence relation on D will partition the set $D \times D'$ into mutually disjoint equivalence.

Denote the equivalence class containing (a,b) by $[a,b] = a/b$

Then by definition.

(ie) $a/b = [a,b] = \{(x,y) \in D \times D' : (x,y) \sim (a,b)\}$

Then by definition.

(ie) $a/b = [a,b] = \{(x,y) \in D \times D' : (x,y) \sim (a,b)\}$

Let F be the family of all equivalent classes thus obtained

Then R is called the set of quotients]

Let a/b, c/d, g/h be arbitrary elements of F. Obviously $a/b = c/d \Leftrightarrow (a,b) \sim (c,d)$ iff $ad = bc$ ②

Also, $a/b = ax/bx \; \forall x \in D$

are define the operation. addition and multiplication on F as follows

(i) $a/b + c/d = \dfrac{ad+bc}{bd}$

(ii) $a/b \cdot c/d = ac/bd$

first we show that (i)(ii) are well defined if,

$a/b = a'/b'$, $c/d = c'/d'$

Then $a/b + c/d = a'/b' + c'/d'$ and

$a/b \; c/d = a'/b' \cdot c'/d'$

To prove,

$\dfrac{ad+bc}{bd} = \dfrac{a'd'+b'c'}{b'd'}$ and

(100)

$\frac{ac}{bd} = \frac{a'c'}{b'd'}$

(ie) $(ad+bc)\,b'd' = (a'd' + b'c')\,bd$ and $(ac)\,b'd' = (a'c')\,bd$

$\Rightarrow (ad+bc)\,b'd' = ad\,b'd' + bc\,b'd'$

$= (ab')(dd') + (bb')(cd')$

$= (bd)(a'd') + (bb')(c'd')$

$(ad+bc)\,b'd' = bd\,(a'd') + (b'c')$

$(ac)(b'd') = ac\,b'd'$

$= (ab')(cd')$

$= (ab')(c'd)$

$= (bd)(a'c')$

① , ② are well defined,

TO PROVE, $(F,+)$ is a field.

F is closed with respect to.

$a/b + c/d \in F$ if $a/b, c/d \in F$

$a/b + c/d = \frac{ad+bc}{bd}$, $f = \{(a,b)/a,b \in D, b \neq 0\}$

$a/b + c/d \in F \Rightarrow a,b,c,d \in D \; b,d \neq 0$

$\Rightarrow ad, bc \in D \; bd \neq 0$

$\Rightarrow \frac{ad+bc}{bd} \in F$

$\Rightarrow a/b + c/d \in F$

+ is associative :-

$a/b + (c/d + g/h) = (a/b + c/d) + g/h$

(101)

For $a/b + (c/d + g/h) = a/b + \left(\frac{ch+dg}{dh}\right)$

$= \frac{a(dh)+bc(h+dg)}{bdh}$

$\Rightarrow \frac{adh+bch+bgd}{bdh}$

Sim,

$(a/b + c/d) + g/h = \frac{adh+bch+bgd}{bdh}$

$0/x \in F$ is additive identity $\forall x \in F$.

For $a/b + 0/x = \frac{ax+b0}{bx} = a/b$

additive inverse of $a/b \in F \Rightarrow -a/b \in F$

For $a/b \in F \Rightarrow a,b \in ① \; b \neq 0$

$\Rightarrow -a,b \in ① \; b \neq 0$

$\Rightarrow -a/b \in F$

$-a/b + a/b = \frac{-ab+ab}{b^2}$

$= 0/b^2$

$= 0/x \Rightarrow$ zero element.

addition is commutative :-

$a/b + c/d = c/d + a/b$

For $a/b + c/d = \frac{ad+bc}{bd} \Rightarrow \frac{da+cb}{bd}$

$\Rightarrow \frac{cb+da}{bd}$

$\Rightarrow c/d + a/b$

P is closed with respect to $\cdot$.

$a/b \, c/d \in F$ if $a/b \; c/d \in F$

$a/b \cdot c/d \in F \Rightarrow a, b, c, d \in D, b, d \neq 0$

$\Rightarrow ac, bd \in D, bd \neq 0$

$\Rightarrow ac/bd \in F$

multiplication is associative:-

$[(a/b) \cdot (c/d)](g/h) = a/b(c/d \cdot g/h)$

For L.H.S $= \left(\frac{ac}{bd}\right)(g/h)$

$= \frac{acg}{bdh} = \frac{a(cg)}{b(dh)}$

$= a/b \, (c/d) \cdot (g/h)$

L.H.S = R.H.S

$x/x \in F$ is multiplication identity of F $\forall x \in F$.

For $a/b \, x/x = ax/bx = a/b$

$a/b \cdot x/x = a/b$.

$x \neq 0 \Rightarrow x \in D' \Rightarrow x \in D \Rightarrow x/x \in F$.

Every non zero elements of F has multiplicative inverse of F.

let $a/b \in F$ such that $b/a \neq 0/x$.

UNIT-II

Another counting principle:-

Defn:

Let G be a group if $a, b \in G$. Then b is said to be a conjugate of a in G if $\exists$ an element $c \in G$ such that $b = c^{-1}ac$. It is denoted by $a \sim b$, and refered to its relation as conjugate.

lemma: (1)

Conjugacy is an equivalence relation of G

Proof:

Given that G is a group, the relation $\sim$ onto G, its denoted by $a \sim b$, then means b is conjugate of a.

TO prove:

$\sim$ is an equivalence relation.

(ii) Reflexive :-

Let $a \in G$ be arbitary

since $a = e^{-1}ae$ we have.

$a \sim a \;\forall\; a \in G$

$\therefore \sim$ is Reflexive

(iii) symmetric :-

Let $a, b \in a$ be arbitrary

suppose, $a \sim b \Rightarrow b = c^{-1}ac$ for some $c \in G$

$(c^{-1})^{-1} b (c^{-1}) = (cc^{-1})^{-1} (c^{-1}ac) \cdot (cc^{-1})$

$= c (c^{-1}ac) c^{-1}$

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

ie $(c^{-1})^{-1} b (c^{-1}) = a$

ie $a = (c^{-1})^{-1} b (c^{-1})$

ie $a = y^{-1}by$ where $y = c^{-1}$

$\Rightarrow b \sim a$

Thus $a \sim b \Rightarrow b \sim a \;\forall\; a, b \in G$

$\therefore \sim$ is symmetric.

(iii) transitive :-

Let $a, b, c \in G$ are arbitrary,

suppose $a \sim b$ and $b \sim c$

$\Rightarrow b = x^{-1}ax$ & $c = y^{-1}by$ where $x, y \in G$

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

$c = z^{-1}az$ where $z = xy$

$a \sim c$

Thus $a \sim b$ & $b \sim c \Rightarrow a \sim c$.

$\therefore \sim$ is transitive.

from (i), (ii), (iii) we have,

conjugacy is an equivalence relation

definition :

For $a \in G$. let $C(a) = \{xax^{-1} / x \in G\}$.

Then $C(a)$, the equivalence class of a in G under our relation as usually called conjugate class of a in G It consists of the set of all distinct of element of the form $y^{-1}ay$. as y range over G

Note :

① $o(G) = \Sigma\, ca$ where the sum runs over the set of $a \in G$, using one a in each conjugate class.

② $C(a)$ has ca elements if G is finite.

normalizer :-

If $a \in G$, then $N(a)$ the normalizer of a in G is the set

$N(a) = \{x \in G / xa = axy\}$.

ie $N(a)$ consist of there elements of G which commutes with a.

(156)

Lemma 2

$N(a)$ is a subgroup of G

Proof

To prove:

(i) $x, y \in N(a) \Rightarrow xy \in N(a)$

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

(i) Let $x, y \in N(a) \Rightarrow xa = ax$ and $ya = ay$

Now $(xy)a = x(ya)$

$= x(ay) = (xa)y$

$= (ax)y = a(xy)$

$\Rightarrow xy \in N(a)$. Thus $x, y \in N(a) \Rightarrow xy \in N(a)$

(ii) Let $x \in N(a)$

$\Rightarrow xa = ax$

Now, $x^{-1}a = x^{-1}ae$

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

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

$= x^{-1}(xa)x^{-1}$

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

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

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

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

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

Theorem:

If G is a finite group then $Cl(a) = \frac{O(G)}{O(N(a))}$. In otherwords the number

(157)

of elements conjugate to a in G is the index of normalizer of a in G.

Proof

Given that G is a finite group

Let $a \in G$ we have,

$N(a) = \{x \in G / xa = ax\}$

$C(a) = \{y \in G / a \sim y\}$

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

$O[C(a)] = Ca$

Denote $M =$ the set of right cosets of $N(a)$ in G

i.e. $M = \{N(a) \cdot x / x \in G\}$

Define $f : M \to C(a)$ defined by

$f(N(a)x) = x^{-1}ax \quad \forall x \in G$

(i) f is well defined:-

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

Suppose $N(a)x = N(a)y$

$\Leftrightarrow xy^{-1} \in N(a)$

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

$\Leftrightarrow x^{-1}(axy^{-1})y = x^{-1}(xy^{-1}a)y$

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

$\Leftrightarrow (x^{-1}ax) = y^{-1}ay$.

$\Leftrightarrow f(N(a)x) = f(N(a)y)$.

f is well defined & 1-1.

ii) f is onto

let $y \in C(a)$ be arbitary

$\Rightarrow y = x^{-1}ax$ where $x \in G$

iii) for any $y \in C(a)$, f an element.

$f(N(a)x) = x^{-1}ax = y$.

$\therefore f$ is onto

Hence f is bijection.

$\Rightarrow O(C(a)) = O(m)$

$C(a)$ = Number of right cosets of $N(a)$ in G

= in $N(a)$

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

Corollary:

$O(G) = \sum \frac{O(G)}{O(N(a))}$, where the sum runs over one elements a in each conjugate class.

Proof

W.K.T $G = \bigcup_{a \in G} C(a)$

(ie) $O(G) = \sum_{a \in G} O(C(a))$

$= \sum_{a \in G} C(a)$

(ie) $O(G) = \sum_{a \in G \& a \notin Z} \frac{O(G)}{O(N(a))}$ (by theorem 5.D) ①

Note:-

The eqn ① is called the class equation of G.

defn:

Let G be a group, then the centre of group G — by $Z(G)$ and is defined by $Z(G) = \{a \in G \text{ s.t } ax = xa, \forall x \in G\}$

① Sub-lemma:

$a \in Z$ iff $N(a) = G$ if G is finite

$a \in Z \Leftrightarrow O(N(a)) = O(G)$

Proof

Assume that $a \in Z$,

TO prove:-

$N(a) = G$.

W.K.T $N(a) \subseteq G$ — ① (by lemma ③)

Now $a \in Z \Rightarrow ax = xa, \forall x \in G$, by defn of Z,

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

$\Rightarrow x \in N(a)$

$\Rightarrow G \subseteq N(a)$ — ②

from ① & ② we get,

$N(a) = G$

Conversely, $N(a) = G$

$ax = xa, \forall x \in G$

$ax = xa, \forall x \in G$.

$\Rightarrow a \in Z$

next assume that G is finite.

$a \in Z \Leftrightarrow N(a) = G$ by (i)
$\Leftrightarrow o(N(a)) = o(G)$.

2nd Theorem ②

If $o(G) = p^n$, where p is a prime number then $Z(G) \neq 0$.

Since $N(a)$ is a subgroup of G

$\Rightarrow o[N(a)] \mid o(G) = p^n$

$\Rightarrow o(N(a))$ must be of the form p^{na} where $0 \leq na \leq n$.

W.K.T $a \in Z \Leftrightarrow N(a) = G$ [by definition]
$\Leftrightarrow o(N(a)) = o(G)$
$\Leftrightarrow p^{na} = p^n$
$\Leftrightarrow na = n$

by the class equation, we have,

$$o(G) = \sum_{a \in G} \frac{o(G)}{o(N(a))} \longrightarrow (1)$$

Let $z = |Z(G)|$

Then for each element in $Z(G)$, we have,

$na = n$

i.e. $\frac{o(G)}{o(N(a))} = 1$, for each elements in $Z(G)$. Thus there are z elements in the class equation.

$na = n$

∴ equ (1) becomes,

$$o(G) = \sum_{na=n} \frac{o(G)}{o(N(a))} + \sum_{na<n} \frac{o(G)}{o(N(a))}$$

i.e. $p^n = z + \sum_{na<n} \frac{o(G)}{o(N(a))}$

now $p \mid p^n$ and $p \mid \frac{p^n}{p^{na}}$

$\Rightarrow p \mid \sum_{na<n} \frac{p^n}{p^{na}}$

$\Rightarrow p \mid \left(p^n - \sum_{na<n} \frac{p^n}{p^{na}}\right)$

$\Rightarrow p \mid z$

Since $e \in Z(G) \Rightarrow z \neq 0$.

i.e. z is the +ve integer divisible by the prime p.

$\Rightarrow z > 1$
$\Rightarrow o(Z(G)) > 1$
$\Rightarrow Z(G) \neq e$.

2nd Corollary :

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

Proof :

Let $o(G) = p^2$ where p is a prime number.

TO prove : G is abelian.

(17) Theorem: Cayley's (Cauchy's Theorem)

If p is a prime number p|o(G). Then G has an element of order p.

Proof:

Given that p is a prime number & p|o(G).

To prove:

ie) To find an elements $a \in x$ such that $a_i = e$, we have prove this theorem by induction on o(G)

Let $o(G) = 1 \Rightarrow G = e$

$e^i = e$

∴ G has an element of order p.

∴ Assume that the theorem is true for all group.

T such that $o(T) < o(G)$ and $p | o(T)$

Let ω be a proper subgroup of G and $p | o(G)$ element of order p.

Now, assume that p is not a divisor of proper subgroup of G.

In particular it $a \notin z(G)$ [since $N(a) \neq G$]

ie) $N(a) \subset G$.

$\Rightarrow p | o(N(a))$

$\Rightarrow p | o(G)$ but $p \nmid o(N(a))$

$\Rightarrow p | \frac{o(G)}{o(N(a))} \Rightarrow p \nmid \sum_{N(a) \neq G} \frac{o(G)}{o(N(a))}$

(16)

$\Rightarrow p \mid \left(o(G) - \sum_{a \neq 0} \frac{o(G)}{o(a)o(a)}\right)$

$\Rightarrow p \mid o(z(G))$

(by class eqn)

$(o(G) = \sum_{a=0} \frac{o(G)}{o(a)o(a)} + \sum_{a \neq 0}$.

order is divisible by p

which is a ↯ to our assumption

so $z(G)$ cannot be a proper subgroup of G. Hence $z(G) = G$.

$\Rightarrow G$ is abelian.

Then ~~$z(G) = G$~~ the Cauchy theorem for abelian group we get a $a \in G$ such that $a^p = e$.

(ie) G has an element of order p.

partition of n:

Let n be any integer then the sequence of +ve integer $n_1, n_2, n_3 \ldots n_r$ with $n_1 \leq n_2 \leq \ldots \leq n_r$ constitute a partition of n.

if $n = n_1 + n_2 + \ldots + n_r$

Let $p(n)$ denote the no of partitions of n, let us determine $p(n)$

(17)

the number of partitions of n

small values of n

$p(1) = 1$, since $1 = 1$ is only partition of 1

$p(2) = 2$ since $2 = 2, 2 = 1+1$.

$p(3) = 3$, since $3 = 3, 3 = 1+2, 1+1+1$.

$p(4) = 5$ since $4 = 1, 2+1+1, 3+1, 2+2, 1+1+1+1$

$p(5) = 7$ since $5 = 5, 5 = 1+4, 1+2+2, 2+3, 1+1+3+2, 1+1+1+1+1, 1+1+3$.

$p(6) = 1, 121, 505$,

cycle partition (or) permutation partition (or) cycle decomposition:

Let p be a permutation $\in S_n$.

Then p is the product of the cycles of permutation and $n_1 \leq n_2 \leq \ldots \leq n_r$ with $n_1 + n_2 + \ldots + n_r = n$.

Then $\{n_1, n_2, \ldots n_r\}$ is called a cycle partition of the permutation in p.

σ in S_9 is given by,

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

$= (1)(213)(4,5,6)(7)(8,9)$

Then σ has cycle decomposition set containing $\{1, 2, 3, 1, 1, 2, 2, 3\}$.

, (ie) the cycle partition is $1+1+2+2+3$

Lemma:

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

Proof:

First we prove that two permutations

Some cycle decomposition

Let $\sigma \in S_n$ such that $\sigma(i) = j$.

Let $\theta \in S_n$ such that $\theta(1) = s$ & $\theta(i) = t$.

Then $\theta^{-1}\sigma\theta$ sends $s \to t$.

i.e. $(\theta^{-1}\sigma\theta)(s) = t$

In other words, to compute $\theta^{-1}\sigma\theta$ it is enough to replace every symbol in σ by its image under θ

For example

To determine,

Let $\sigma = (1,2,3)(4,7)$

and $\sigma = (5,6,7)(3,4,2)$

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

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

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

$$(\theta^{-1}\sigma)\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 1 & 5 & 6 & 4 & 3 \end{pmatrix}$$

$= (1,7,3)(5,4,6)$

Now, let $\sigma = (a_1, a_2, \ldots a_{n_1})(b_1, b_2 \ldots b_{n_2}) \ldots (x_1, x_2 \ldots x_{n_r})$

Then $\tau = \theta^{-1}\sigma\theta$, where

$\theta = \begin{pmatrix} (a_1 a_2 \ldots a_{n_1})(b_1 b_2 \ldots b_{n_2}) \ldots \\ (\alpha_1 \alpha_2 \ldots \alpha_{n_1})(\beta_1 \beta_2 \ldots \beta_{n_2}) \ldots \end{pmatrix}$ $(x_1, x_2 \ldots x_{n_r})$ $(\gamma_1, \gamma_2 \ldots \gamma_{n_r})$

Hence σ and τ are conjugate.

$\therefore S_n$ has exactly p(n) conjugate class. Hence the proof.

Sylow's theorem:

The number of ways of picking a subset of r element is given by,

i.e. $nC_r = \binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{1.2.\ldots(n-1)n}{r!(n-r)!}$

$$= \frac{n(n-1)(n-2)\ldots(n-r+1)}{1.2.3\ldots r}$$

Choose $n = p^\alpha m$ and $r = p^\alpha$, where p is a prime number.

Then $\binom{p^\alpha m}{p^\alpha} = \frac{(p^\alpha m)(p^\alpha m-1)(p^\alpha m-2)\ldots(p^\alpha m-\beta)}{1.2.3\ldots(p^\alpha-1)p^\alpha}$

$$= \frac{(p^\alpha m)(p^\alpha m-1)\ldots(p^\alpha m-i)\ldots(p^\alpha m-i-1)\ldots(p^\alpha m-p^\alpha+1)}{(p^\alpha)(p^\alpha-1)(p^\alpha-2)\ldots(p^\alpha-i)\ldots(p^\alpha-p^\alpha+1)}$$

The same as the of $p^{\alpha}\beta$ so all the powers of p cancel out except the power which devides

Thus $p^{\gamma} / \binom{p^{\alpha}m}{p^{\alpha}}$ But $p^{\gamma+1} \nmid \binom{p^{\alpha}m}{p^{\alpha}}$

Sylow's Theorem:

If p is the prime number and $\frac{p^{\alpha}}{o(G)}$ Then G has a subgroup of order p^{α}

Proof

Let M be the set of all subset of G which have p^{α} element.

Thus M has $\binom{p^{\alpha}m}{p^{\alpha}}$

Given $M_1, M_2 \in M$ define $M_1 \sim M_2$. If there exists an element $g \in G$ such that $M_1 = M_2 g$ Then $\sim$ is an equivalence relation on M.

We claim that, there is atleast one equivalence class of element in M such that the number of element in this class not a multiple of $p(\gamma+1)$

(ie) To claim $p^{\gamma+1}$ does individe atleast one class $o'm$ in $\left(\frac{p^{\gamma+1}}{m_i}\right)$ for if $p^{\gamma+1}$ is a divisor of the size of each equivalence class

Hence, ——— of elements in M

Since M has $\binom{p^{\alpha}m}{p^{\alpha}}$

$\Rightarrow p^{\gamma} \mid \binom{p^{\alpha}m}{p^{\alpha}}$ But, $p^{\gamma+1} \nmid \binom{p^{\alpha}m}{p^{\alpha}}$

Let $\{m_1, m_2, \ldots m_n\}$ be a such an equivalence class in m where $p^{\gamma+1} \nmid n$

By the defn, of the equivalence class in m if $g \in G$, for each $i = 1, 2, \ldots n$

$m_i g = m_j$ for some j, $1 \le j \le n$.

Let $H = \{g \in G \mid m_i g = m_i\}$ Then H is a subgroup of G.

for if $a, b \in H$

$\Rightarrow m_i a = m_i$

$m_i b = m_i$

$\Rightarrow m_i(ab) = (m_i a) b$

$= m_i b$

$= m_i$

ie) $m_i(ab) = m_i \Rightarrow ab \in H$ and

$m_i e = m_i \Rightarrow e \in H$.

① Note:

Every finite group has a tree cycles of roots for every prime p dividing its order.

② The conjugate of a p-Sylow subgroup is also a p-Sylow subgroup.

The
$p^{n(k)} | (p^k)!$ but $p^{n(k)+1} \nmid (p^k)!$

Lemma:

$$n(k) = 1 + p + p^2 + \dots + p^{k-1}$$

Proof:

If $k=1$. Then, since $p! = 1, 2, \dots (p-1)p$
It is clear that $p | (p)!$ but $p^2 \nmid p!$

Hence $n(1) = 1$.

The term in the expansion of $(p^k)!$ can contribute the powers of p dividing $(p^k)!$ are the multiples of p.

(i) They are $p, 2p, 3p \dots p^{(k-1)}p$.

(ii) $n(k)$ is a power of p which divides $(p^k)!$

$\therefore p | p, 2p \dots (p^{k-1})p = (p^{p^{k-1}})(p^{k-1})!$

$\therefore n(k) = 1 + p + p^2 + \dots + p^{k-2} + p^{k-1}$

$\therefore n(k) = p^{k-1} + n(k-1)$.

$\Rightarrow n(K) = n(K-1) = p^{K-1}$

Similarly $n(K-1) - n(K-2) = p^{K-2}$

$n(2) - n(1) = p^1$

$n(1) = 1$

Adding all these terms we get

$n(K) = 1 + p + p^2 + \cdots + p^{K-1}$

Lemma 6

Sp^K has a p-Sylow's subgroup of order $p^{n(K)}$

Proof:

These will be proved by induction on n. suppose $K=1$ then the elements $\{1, 2, \cdots p\}$ in Sp is of order p

$\Rightarrow Sp$ has a subgroup of order p.

Thus the result is true for $K=1$

Assume that the result is true for $K-1$,

ie) Sp^{K-1} has a subgroup of order p^{K-1} to prove that the result is true for K divide the integers $1, 2, \cdots p^{K-1}$ into p-groups each either p^{K-1} as follows.

$\{1, 2, \cdots p^{K-1}\}\ \{p^{K-1}+1, p^{K-1}+2, \cdots 2p^{K-1}\}$

$\cdots \{(p-1)p^{K-1}+1 \cdots p^K\}$

The permutation σ is defined by.

$\sigma = (1, p^{K-1}+1, 2p^{K-1}+1, \cdots (p-1)p^{K-1}+1)$

$(2, p^{K-1}+2 \cdots p^K)\ (p^K+2, p^{K-1}+2 \cdots p^K)$

Thus σ has a following properties

(1) $\sigma^p = I$. The identity permutation

(2) If τ is a permutation that leaves all fixed for $\tau > p^{K-1}$

(3) Then σ', τ, σ moves only elements in —

generally whose only elements in $\{jp^{K-1}+1, jp^{K-1}+2 \cdots (j+1)p^{K-1}\}$.

consider $A = \{\tau \in Sp^K / \tau(i) = i, \text{ if } i > p^{K-1}\}$

Then A is a subgroup of Sp^K and the element in A can carryout any permutation on $1, 2, \cdots p^{K-1}$.

From this it follows that $A \approx Sp^K$ By induction hypothesis. A has a subgroup P, of order $p^{n(K-1)}$ — (1)

Let $\tau = P_1(\sigma^{-1}P_1\sigma)(\sigma^{-2}P_1\sigma^2) \cdots [\sigma^{-(p-1)}P_1\sigma^{(p-1)}]$

$= P_1 P_2 \cdots P_p$ where $P_{i+1} = \sigma^{-1}P_i\sigma^{i+1}$. — (2)

Each P_i is isomorphic to P_1

(3) $P_i \approx P_i$

so that $O(P_1) = O(P_2) = \cdots = O(P_{(p)}) = p^{n(K-1)}$ by (1)

(14) Also p is a subgroup of sp^k.

$o(T) = o(P_1)o(P_2) \dots o(P_p)$ p times

$= p^{n(k-1)} p^{n(k-1)} \dots$ p times

$= p^{n(k-1)} \dots$ p times

$o(T) = p^{p n(k-1)} \rightarrow (1)$

let $P = \{\sigma^{ik} / k \in T, 0 \le i \le p\}$

Since $\sigma \in T$, $\sigma^{-1} T \sigma = T$, we have,

Two things (1) P is a subgroup of sp^k and further more.

$o(P) = o(\sigma^i) o(T)$

(2) $o(P) = p^i [p^{pn(k-1)}] = o(\sigma) o(T)$

$= p^{i + pn(k-1)} = p o(T) = p^1 + p^2 + p^3 + \dots + p^{k-2}$

$= p^1 + p^2 + p^3 + \dots + p^{k-1} = p^{n(k)}$

(By lemma)

Hence sp^k has a subgroup of order $p^{n(k)}$

$\Rightarrow sp^k$ has a subgroup p of order $p^{n(k)}$ and $p^{n(k)} / p^{n-1}$ and $p^{n(k+1)}$ fr

$\Rightarrow sp^k$ has a p-cycles Sylows subgroups.

V.I. (1) Find the 2-Sylows cyclic group in S_4.

(15) Proof:

Here $S_4 = S_2^3$

Divide $\{1,2,3,4\}$ into two sets $\{1,2\}$ $\{3,4\}$

Let $\sigma = \{1,3\}, \{2,4\}$

$P_1 = \{1,2\}$, $P_2 = \sigma^{-1} P \sigma = \{3,4\}$

Our 2-Sylows subgroup generated by

$T = P_1, P_2, \sigma$

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

V.I. (2) Find the 2-sylow subgroup in S_8.

proof:

Here $S_8 = S_2^3$

Divide $\{1,2 \dots 8\}$ into two sets

$\{1,2,3,4\}$ $\{5,6,7,8\}$.

Let $\sigma = \{1,5\}, \{2,6\}, \{3,7\}$ $\{4,8\}$

Thus 2-sylows subgroup are generated by $T = P_1 P_2 \sigma = \{1,2,3,4\}$

$\{5,6,7,8\}$ $\{(1,5)(2,6)(3,7)(4,8)\}$

3. Find the 3-sylow subgroup in S_9.

Proof:

Here $S_9 = S_3^2$

Divide $\{1, \dots 9\}$ into three sets

(170)

$\{1,2,8\}\{4,5,6\}\{7,9,3\}$

let $\sigma = \{1,4,7\}, \{2,5,8\}, \{3,6,9\}$

let $P_1 = \{1,2,8\}, P_2 = \{4,5,6\}$

$P_3 = \{7,8,9\}$

The sylow subgroups are generated by.

$T = P_1, P_2, P_3, \sigma$

$= \{(1,2,8),(4,5,6),(7,8,9),(1,4,7),$
$(2,5,8),(3,6,9)\}$

Definition:

Let G be a group. Let A, B be the subgroup of a group G. If $x, y \in G$ define $x \sim y$ if $y = axb$ for some $a \in A$ & $b \in B$

Lemma 7

Let G be a group. Let A, B be the subgroup of a group G. If $x, y \in G$, define $x \sim y$ if $y = axb$ for some $a \in A$ and $b \in B$. The relation defined as about an equivalence relation.

If $x \in G$ is the set $AxB = \{axb / a \in A, b \in B\}$.

Proof:

Give that G is a group and A, B are the subgroup of G.

(171)

The reaction is defined by $x \sim y$ if $y = axb$ for some $a \in A, b \in B$

claim: $\sim$ is an equivalence relation

(i) Reflexive:

Let $x \in G$ be arbitary. Then $x = exe$ where $e \in A$ & $e \in B \Rightarrow x \sim x \; \forall x \in G$.

(ii) Symmetric:

Let $x, y \in G$ be arbitary suppose $x \sim y \Rightarrow y = axb, a \in A, b \in B$.

now, $a^{-1} y b^{-1} = a^{-1}(axb)b^{-1} = (a^{-1}a)x(bb^{-1})$

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

(ip) $x = a^{-1} y b^{-1}$, where $a^{-1} \in A$ and $b^{-1} \in B$

$\therefore \Rightarrow y \sim x$

Thus $x \sim y \Rightarrow y \sim x, \forall x, y \in G$.

The relation is symmetric.

(iii) transitive:

Let $x, y, z \in G$ be arbitarty

suppose $x \sim y$ & $y \sim z \Rightarrow y = axb$ and $z = cy$

where $a, c \in A$ and $b, d \in B$

$= c(axb)d = (ca)x(bd)$

$z = fxg$ where $f = ca \in A$ and $g = bd \in$

[illegible]

$\Rightarrow x \sim z$

Thus $x \sim y$ and $y \sim z \Rightarrow x \sim z$ [illegible] $x, y, z \in G$

$\therefore \sim$ is transitive

Hence $\sim$ is an equivalence relation is called the equivalence class.

The equivalence class of x in G is the set $AxB = \{axb / a \in A, b \in B\}$. This set is called the double coset of A and B in G.

Lemma: 8

If A and B are finite subgroup of G. Then $O(AxB) = \dfrac{O(A)\,O(B)}{O(A \cap xBx^{-1})}$

Proof:

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

Define $T : AxB \to AxBx^{-1}$ by $(axb)T = axbx^{-1}$ where $axb \in AxB$.

claim T is a bijection

T is 1-1:

suppose $(axb)T = (cxd)T$

$\Rightarrow axbx^{-1} = cxdx^{-1}$ where $axb, cxd \in AxB$

$\Rightarrow axb = cxd$

$\therefore T$ is 1-1.

T is onto:

let $y \in AxBx^{-1}$ be arbitrary then $y = axbx^{-1}$ $\exists$ an element axb in such that $T(axb) = axbx^{-1}$

$\therefore T$ is onto $\therefore T$ is a bijection.

$$O(AxB) = O(AxBx^{-1})$$

$$= \frac{O(A) \cdot O(xBx^{-1})}{O(A \cap xBx^{-1})} \quad [\because xBx^{-1} \text{ is a subgroup of order } O(B) = O(xBx^{-1})]$$

$$= \frac{O(A) \cdot O(B)}{O(A \cap xBx^{-1})}$$

Lemma: 9

Let G be a finite group and suppose that G is a subgroup of a finite group of M. Suppose further subgroup of M be a p-sylow subgroup & then other p-sylow subgroup P.

$P = G \cap xMx^{-1}$ for some $x \in M$.

Proof

Given that G is a finite group and G is a subgroup of finite group of m suppose further that m has a p sylow subgroup.

Suppose $p^n \mid o(m)$ and $p^{n+1} \nmid o(m)$.

$\Rightarrow m$ has a p sylow subgroup of order p^n.

—

Let $o(G) = p^n t$ where $p \nmid t$ we want to produce a subgroup of order consider the double coset of decomposition of m.

Given by G' and R

$M = O(G \backslash x R)$

$o(M) = \sum o(G \cap xRx^{-1})$ where the sum runs over the element from each double coset by lemma (B), we have

$$o(G \backslash x R) = \frac{o(G)o(R)}{o(G \cap xRx^{-1})} = \frac{(p^n t)(p^m)}{o(G \cap xRx^{-1})}$$

$$\Rightarrow o(G \backslash x R) = \frac{t p^{m+n}}{o(G \cap xRx^{-1})} \longrightarrow (1)$$

Since $G \cap xRx^{-1}$ is a subgroup of xRx^{-1}. Its order is p^{mx} we claim that $mx \leq n$ for some $x \in m$

If $mx > n$ then $o(G \cap xRx^{-1}) \geq \frac{t p^{m+n}}{p^{mx}}$

$= t p^{m+n-mx}$

Then $p^{m+n} \mid p^{m+n-mx} \Rightarrow p^{m+1} \mid o(G \cap xRx^{-1})$

$\Rightarrow p^{m+1} \mid \sum o(G \cap xRx^{-1})$ where sum runs over one element in each double cosets.

$\Rightarrow p^{m+1} \mid o(m)$.

This contradiction $p^{m+n} \mid o(m)$

$\therefore mx = n$ for some $x \in m$

$\therefore o(G \cap xRx^{-1}) = p^{mx} = p^n$

since $G \cap xRx^{-1} = P$ is a subgroup of G and has order —

second part sylow's theorem :

If G is a finite group p is a prime and $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$. Then two subgroup of order p^n are conjugate.

Proof:

Given that G is a finite group P is a prime and $p^n \mid o(G)$ but $p^{n+1} \nmid o(G)$.

(12)

Proof:

Suppose A and B are any two subgroup of G each of order p^n.

TO Prove: A and B are conjugate.

(ie) To prove $A = gBg^{-1}$ for some $g \in G$.

Decompose G into double cosets A and B

$\Rightarrow G = \cup AxB$.

$\Rightarrow O(G) = \Sigma O(AxB)$ where the sum runs over one element in each double cosets by Lemma (5) we have,

$$O(AxB) = \frac{O(A) \cdot O(B)}{O(A^1 \cap BxB^{-1})} = \frac{p^n p^n}{O(A \cap xBx^{-1})}$$

$$= \frac{p^{2n}}{O(A \cap xBx^{-1})} \longrightarrow (1)$$

Suppose $A \neq xBx^{-1}$ for some $x \in G$ since $A \cap xBx^{-1}$ is a subgroup of A.

(ie) $A \cap xBx^{-1} \subset A$

$\Rightarrow O(A \cap xBx^{-1}) < O(A)$

$\Rightarrow O(A \cap xBx^{-1}) \leq p^m$, where $m < n$

$$O(AxB) = \frac{p^{2n}}{p^m} = p^{2n-m}$$

$\Rightarrow p^{n+1} / p^{2n-m} \Rightarrow p^{n+1} / O(AxB)$ for every x.

(13)

$\Rightarrow p^{n+1} / \Sigma O(AxB) \Rightarrow p^{n+1} / O(G)$ which is a $\Rightarrow \Leftarrow$ to $p^{n+1} / O(G)$

$\therefore A = xBx^{-1}$ for some $x \in G$

(ie) $A = gBg^{-1}$ for some $g \in G$.

Hence any two subgroup of G of order p^n are conjugate.

Definition: Index.

Let G be a group and H the subgroup of G the set $\underline{\text{normalizer of H}}$ as denoted by $N(H)$ and is defined by $N(H) = \{x \in G \mid x^{-1}Hx = H\}$

The number of distinct conjugate xHx^{-1} of H in G is called the $\underline{\text{index of H}}$ of $N(H)$ in G.

Lemma:

Statement:

The number of p-sylow subgroups of G equals $O(G) / O(N(a))$ where p is any p-sylow subgroup of G. In particular this number of the order of G.

Third part of sylow's theorem:

(14) Statement:

The number of p-sylow subgroup in G for given prime is of the form 1+kp

Proof:

Let P be p-sylow subgroup of G of order p^n To prove, number of p-sylow subgroup in G is of the form 1+kp, where k is an integer.

Decompose G into double cosets pxP & $G=\cup PxP$.

$o(G) = \sum o(PxP)$, where the sum runs over one

$= \sum o(PxP) + \sum o(PxP)$ element → (1)
in each double cosets $x \notin N(P)$

Then $o(PxP) = \frac{o(P)\,o(P)}{o(Px \cap Px^{-1})} = \frac{p^n p^n}{o(Px \cap Px^{-1})}$

$= \frac{p^{2n}}{o(Px \cap Px^{-1})}$ → (2)

Consider the normalizer of P in G.

(i) $N(P)$

Case (i)

$x \notin N(P)$

$\Rightarrow xPx^{-1} \neq P \Rightarrow Px \cap Px^{-1} \neq PxP$

$\Rightarrow Px \cap Px^{-1} \neq P \Rightarrow o(Px \cap Px^{-1}) = p^m$, m<n

(2) becomes,

$o(PxP) = \frac{p^{2n}}{p^m} = p^{2n-m}$.

(15)

$\Rightarrow p^{n+1} \mid p^{2n-m} \Rightarrow p^{n+1} \mid o(PxP)$

$\Rightarrow o(PxP) = \cup p^{n+1}$

Case (ii) $x \in N(P)$

$\Rightarrow xPx^{-1} = P$.

$\Rightarrow (Px \cap Px^{-1}) = P \cap P = O$

$o(Px \cap Px^{-1}) = o(P)$

(ie) $o(Px \cap Px^{-1}) = p^n$

$o(PxP) = \frac{p^{2n}}{p^n} = p^n = o(P)$

(1) becomes, $o(G) = o(N(P)) - 1 + \sum o(PxP)$

where $o[N(P)] = \sum o(PxP)$, $x \in P$.

$o(G) = o[N(P)] + \cup p^{n+1}$ [throughout by case (2)]

we have,

$\frac{o(G)}{o[N(P)]} = 1 + \frac{\cup p^{n+1}}{o[N(P)]}$ → (3)

By lagrange's theorem, $o[N(P)] \mid o(G)$ is an integer.

$\therefore \frac{\cup p^{n+1}}{o[N(P)]}$ is also integer.

Also since $p^{n+1} \nmid o(G)$

(ie) $p^{n+1} \nmid o[N(P)]$

But then $\frac{\cup p^{n+1}}{o[N(P)]}$ must be divisible by p

(13)

since $(a_1, b_1), (a_2, b_2) \in A \times B$

$\Rightarrow (a_1, b_1)(a_2, b_2) \in A \times B$

ii) Associative

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

$\Rightarrow a_1, a_2, a_3 \in A$ & $b_1, b_2, b_3 \in B$.

$\Rightarrow a_1(a_2 a_3) = (a_1 a_2)a_3$ and $b_1(b_2 b_3) = (b_1 b_2)b_3$

$\Rightarrow (a_1 (a_2 a_3), b_1 (b_2 b_3)) = ((a_1 a_2)a_3, (b_1 b_2) b_3)$

$\Rightarrow (a_1, b_1)(a_2 a_3, b_2 b_3) = (a_1 a_2, b_1 b_2)(a_3 b_3)$

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

for all $(a_i, b_i) \in A \times B$

iii) Existence of identity

Let e_1 and e_2 be identity of $A \times B$ respectively, $\exists (e_1, e_2) \in A \times B$

Let $(a_1, b_1) \in A \times B$ be arbitrary

Now, $(a_1, b_1)(e_1 e_2) = (a_1 e_1)(b_1 e_2) = (a_1, b_1)$

Similarly $(e_1, e_2)(a_1, b_1) = (e_1 a_1, e_2 b_1) = (a_1, b_1)$

$\Rightarrow (a_1, b_1)(e_1 e_2) = (e_1 e_2)(a_1, b_1) = (a_1, b_1) \in A \times B$.

(14)

iv) Existence of inverse

Let $(a_1, b_1) \in A \times B$, be arbitrary

$\Rightarrow a_1 \in A$ & $b_1 \in B \Rightarrow a_1^{-1} \in A$, $b_1^{-1} \in B$.

$\Rightarrow (a_1^{-1}, b_1^{-1}) \in A \times B$.

Similarly $(a_1^{-1}, b_1^{-1})(a_1, b_1) = (a_1^{-1} a_1, b_1^{-1} b_1)$

$\Rightarrow (a_1^{-1}, b_1^{-1})$ is the inverse of (a_1, b_1) in $A \times B$

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

Remark :

we called the group $G = A \times B$ as a external direct product of A & B.

Note :

1) Group $G_1 \times G_2$ is an abelian group iff G_1 & G_2 are both abelian group

2) $G_1 \times G_2$ is a finite group iff both G_1 & G_2 the finite group.

$\therefore G_1 \times G_2 \cong G_2 \times G_1$.

Remark

Suppose A & B are group then the subset $A \times \{e_2\}$ & $\{e_1\} \times B$ are normal subgroups of $A \times B$ & B respectively.

Proof :

Given that A & B are groups.

Then $A \times B$ is also a group [by previous result]

Prove:

i) A' and B' are normal subgroups of $A \times B$

ii) $A' \cong A$, $B' \cong B$

Proof:

Let $(a,b) \in A \times B$ & $(a_1,b_1) \in A'$

$\Rightarrow (a,b)(a_1,e_2)(a,b)^{-1}$

$\Rightarrow (a,b)(a_1,e_2)(a^{-1},b^{-1})$

$\Rightarrow (aa_1a^{-1}, bb^{-1}) \in A'$

$\Rightarrow A'$ is a normal subgroup of $A \times B$.

Similarly we can prove B' is a normal subgroup of $A \times B$.

Part (ii):

Now $A' \cong \{(a_1,e_2) : (a_1,e_2) \in A'\}$

Let $(a,b) \in A'$

$\Rightarrow a = (a_1,e_2)$ & $b = (b_1,b_2)$

where $a_1, b_2 \in A$.

$\Rightarrow ab^{-1} = (a_1,e_2)(b_1,e_2)^{-1} = (a_1,e_2)(b_1^{-1},e_2)$

$ab^{-1} = (a_1b_1^{-1}, e_2) \in A'$

$\Rightarrow A'$ is a subgroup of $A \times B$.

Similarly B' is also a subgroup of $A \times B$.

Next to prove $A' \cong A$

For define $\varphi : A' \to A$ by

$\varphi(a_1,e_2) = f(a_1) \; \forall (a_1,e_2) \in A'$.

φ is 1-1:

Suppose $\varphi(a_1,e_2) = \varphi(b_1,e_2)$ where (a_1,e_2) & $(b_1,e_2) \in A'$

$\Rightarrow a = b \Rightarrow (a_1,e_2) = (b_1,e_2)$

$\therefore \varphi$ is 1-1.

φ is onto:

Let a be arbitrary.

Then $\exists$ an element $(a_1,e_2) \in A'$ s.t. $\varphi(a_1,e_2) = a$.

φ is a homomorphism:

Let (a_1,e_2) $(b_1,e_2) \in A'$ be arbitrary. $\varphi[(a_1,e_2)(b_1,e_2)] = \varphi(ab_1,e_2)$

$= ab$

$= \varphi(a_1,e_2)\varphi(b_1,e_2)$

φ is a homomorphism.

If $\sigma : \bar{A} \cdot \bar{B}$ where $\bar{A} = A \times \{e_2\}$ & $\bar{B} = \{e_1\} \times B$. Then every $g \in \sigma$ has a unique representation of the form $g = \bar{a} \cdot \bar{b}$, where $\bar{a} \in \bar{A}$ & $\bar{b} \in \bar{B}$.

Proof:

Let $g \in \sigma$ be arbitrary

$\Rightarrow x = e$ by the uniqueness

$\Rightarrow N_1 \cap N_2 = \{e\}$

For (ii)

Suppose $a \in N_1$, $b \in N_2$ for if $\neq$

TO PROVE $ab = ba$

Now $aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in N_2$ [$\because N_2$ is a normal subgroup of G]

Also $aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in N_1$.

$\therefore aba^{-1}b^{-1} \in N_1 \cap N_2 = \{e\}$

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

$\Rightarrow (ab)a = e$

$\Rightarrow ab = ba$ (Hence the proof)

Lemma 2.16

Let G be a group & suppose that G is the internal direct product of $N_1, N_2, \ldots N_n$. Let $T = N_1 \times N_2 \times \ldots \times N_n$. Then $G \cong T$ i.e. isomorphism.

Soln:

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

Let $T = N_1 \times N_2 \ldots N_n$

TO prove:

$T \cong G$.

For define $\phi : T \to G$ by $\phi(a_1, a_2 \ldots a_n)$

$= a_1 a_2 \ldots a_n$ where $(a_1, a_2 \ldots a_n) \in T$.

(14)

We claim:- φ is an isomorphism

Suppose $(a_1, a_2 \ldots a_n) = (b_1, b_2 \ldots b_n)$

$\Leftrightarrow a_1 = b_1, a_2 = b_2 \ldots a_n = b_n$

$\Leftrightarrow a_1, a_2, \ldots a_n = b_1, b_2 \ldots b_n.$

$\Leftrightarrow \varphi(a_1, a_2 \ldots a_n) = \varphi(b_1 b_2 \ldots b_n)$

Thus φ is well defined & 1-1.

ii) φ is onto:

Take any element $g \in G$

$g = m_1 m_2 \ldots m_n$ where $m_i \in S$

$\Rightarrow (m_1 m_2 \ldots m_n) \in T$

$\Rightarrow \varphi(m_1 m_2 \ldots m_n) =$

$m_1 m_2 \ldots m_n = g$

$\Rightarrow \varphi$ is onto.

iii) φ is homomorphism.

let $(a_1 a_2 \ldots a_n), (b_1 b_2 \ldots b_n) \in T$

Then $\varphi[(a_1 a_2 \ldots a_n)(b_1 b_2 \ldots b_n)]$

$= \varphi[a_1 b_1, a_2 b_2 \ldots a_n b_n]$

$= (a_1 a_2 \ldots a_n)(b_1 b_2 \ldots b_n)$

$= \varphi(a_1 a_2 \ldots a_n)\varphi(a_1 b_1 \ldots b_n)$.

$\rightarrow \varphi$ is an homomorphism

$\therefore \varphi$ is an isomorphism