Groups: Handwritten notes

by

Atiq ur Rehman

http://www.MathCity.org/atiq

Partial Contents

Group:-

A non-empty set G is group if

i) Closure law holds in G
i.e for $a, b \in G$, $a * b \in G$

ii) Associative law holds in G
i.e for $a, b, c \in G$, $a*(b*c) = (a*b)*c$

iii) Identity law holds in G
i.e for $a \in G$, $a*e = e*a = a$
where e is an identity element.

iv) Inverse law holds in G
i.e for $a \in G$ $\exists$ $a' \in G$ such that
$a * a' = a' * a = e$

If commutative law holds in G then G is called abelian group.

Example:-

$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\{\pm 1, \pm i\}, \cdot)$
are the examples of group.

$A = \{I, \pm i, \pm j, \pm k\}$ with the condition
$i \cdot i = j \cdot j = k \cdot k = I$
$i \cdot j = jk$, $j \cdot k = i$, $k \cdot i = j$
$j \cdot i = -k$, $k \cdot j = -i$, $i \cdot k = -j$
& $Ix = x \quad \forall \; x \in A$
then A is called group.

Question:-

Prove that $(\mathbb{Z}_n, \oplus)$ is a group.

Solution:-

$\mathbb{Z}_n = \{0, 1, 2, \ldots\ldots, n-1\}$

i) For $a, b \in \mathbb{Z}_n$, then $a+b \in \mathbb{Z}_n$ if $a+b<n$ and if $a+b \geq n$, then after dividing $a+b$ by n, then remainder is less than n and

So belongs to Z_n.
i.e binary operation $\oplus$ is defined

ii) $\oplus$ is associative in general.

iii) $0 \in Z_n$ is an identity element.

iv) For $a \in Z_n$; $n-a$ is inverse of a.

$\because a + (n-a) = n = 0$ | $n \div n \Rightarrow$ Remainder

Hence Z_n is group under $\oplus$.

Some Important Result:-

Let G be a group then

i) Cancellation law holds in G.

ii) Identity element is unique.

iii) Inverse of the element is unique.

iv) $(a^{-1})^{-1} = a \quad \forall \; a \in G$.

v) $(ab)^{-1} = b^{-1}a^{-1}$

End of Lesson at 1216 PST

Order of Group:-

def:- The number of element in a group G is called the order of G and is denoted by $|G|$.

A group G is said to be finite if G consists of only a finite number of elements. Otherwise G is said to be an infinite group.

Order of Element:-

def:- Let a be an element of a group G. A positive integer 'n' is said to be the order of a if $a^n = e$ and n is the least such positive integer.

Question:-

Let $a \in G$ and order of 'a' is 'n'. then the elements $a, a^2, a^3, \dots, a^{n-1}$ are all distinct.

Solution:

On the contrary let

$a^p = a^q$ for some $p<n$, $q<n$, $p \neq q$.

then

$$a^p \cdot a^{-q} = e$$

$$\Rightarrow a^{p-q} = e \Rightarrow p-q < n$$

a contradiction $\because$ order of a is n.

hence $a^p \neq a^q$

Since a^p, a^q are taken to be arbitrary therefore all elements are distinct.

Theorem:-

Let G be a group, for $a \in G$ let $a^n = e$ then for some integer k, $a^k = e$ iff n/k.

Solution:-

Let n/k then there is a some integer q such that $k = nq$.

$$a^k = a^{nq} = (a^n)^q = e^q = e.$$

Conversely, Let $a^k = e$ i.e $k > n$.

so there are integers q and r such that

$$k = nq + r \quad ; \quad r < n.$$

so

$$a^k = a^{nq+r} = e$$

$$\Rightarrow a^{nq} \cdot a^r = e$$

$$\Rightarrow (a^n)^q \cdot a^r = e$$

$$\Rightarrow (e)^q \cdot a^r = e \qquad \because n \text{ is order of } a.$$

$$\Rightarrow e \cdot a^r = e$$

which is only possible if $r = 0$

then $k = nq \Rightarrow n/k$.

Periodic Group:-

def:- If every element of a group G is of finite order then G is periodic group.

Mixed Group:-

def:- If a group G contains elements of finite as well as infinite order, then G is called mixed group.

e.g $(\mathbb{R}', \cdot)$ is mixed group $\quad | \; \mathbb{R}' = \mathbb{R} - \{0\}$

Sub-group:-

def:— Let H be a non-empty subset of a group G then H is subgroup of G if H itself is a ~~sub~~ group with the binary operation defined on G.

Imp
Theorem:

Let G be a group and H a non-empty subset of G. then H is ~~group~~ sub-group iff $a, b \in H \Rightarrow ab^{-1} \in H$

Proof:

Suppose that H is a subgroup of G, then $(H, \cdot)$ is a group, if $b \in H$, $b^{-1} \in H$

hence $a, b \in H \Rightarrow ab^{-1} \in H$

Conversely, suppose that $a, b \in H \Rightarrow ab^{-1} \in H$.

then $a, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$

Now $e, b \in H \Rightarrow eb^{-1} \in H \Rightarrow b^{-1} \in H$

Again $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} = ab \in H$.

Thus H is closed in G. The associative law holds for elements of H as it holds, in general for the element of G.

Hence all the axioms of a group are satisfied by the elements of H. Hence H is a group under the binary operation defined on G and so is a subgroup of G.

Theorem :-

Let G be a abelian group and F be subset of all element of G with finite order, then H is a subgroup.

Proof:-

Let $a, b \in F$ then there are integers m and n such that

$$a^m = e \quad \text{and} \quad b^n = e$$

we have to prove $ab^{-1} \in F$.

$$\begin{aligned}(ab^{-1})^{mn} &= (b^{-1})^{mn}(a)^{mn} \\ &= a^{mn}(b^{-1})^{mn} \quad \because G \text{ is abelian.} \\ &= a^{mn}.b^{-mn} \quad \because (b^{-1})^m = b^{-m} \\ &= (a^m)^n (b^n)^{-m} \\ &= e^n. e^{-m} \\ &= e.e = e\end{aligned}$$

implies that $ab^{-1} \in F$

therefore F is a subgroup.

Theorem:-

Intersection of any family of subgroups of a group G is subgroup of G.

Proof:-

Let $\{H_i\}$, $i \in I$ be a family of subgroups of G.

Let $H = \bigcap_{i\in I} H_i$

Let $a, b \in H$ then $a, b \in H_i$ for each $i \in I$

Since H_i is a subgroup of G

so $ab^{-1} \in H_i$ for each $i \in I$

therefore $ab^{-1} \in \bigcap_{i\in I} H_i = H$

Hence H is subgroup of G.

Note:- Union of two subgroup may not be a subgroup.

e.g. $Z_1 = \{0, 3\}$, $Z_2 = \{0, 2, 4\}$ are subgroup of a group $Z_6 = \{0, 1, 2, 3, 4, 5\}$ then $Z_1 \cup Z_2 = \{0, 2, 3, 4\}$ is not a subgroup.

Theorem:-

Let H_1, H_2 are two subgroup of a group G then $H_1 \cup H_2$ is a subgroup of a G iff either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Proof:-

Let $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

then $H_1 \cup H_2 = H_2$ or $H_1 \cup H_2 = H_1$

$\because$ H_1 & H_2 are subgroup so $H_1 \cup H_2$ is also subgroup.

Conversely:

Let $H_1 \cup H_2$ is a subgroup.

and let $H_1 \not\subseteq H_2$ or $H_2 \not\subseteq H_1$

then there are $a, b \in G$ such that

$a \in H_1 \setminus H_2$, $b \in H_2 \setminus H_1$

i.e. $a \in H_1$ but $a \notin H_2$ or $b \in H_2$ but $b \notin H_2$

$\Rightarrow a, b \in H_1 \cup H_2$

As $H_1 \cup H_2$ are subgroup

therefore $ab \in H_1 \cup H_2 \Rightarrow ab \in H_1$ or $ab \in H_2$

then

$a^{-1}(ab) = b \in H_1$

which is a cotradiction

hence $H_1 \cup H_2$ is subgroup iff $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

Invalution.-

def:- An element x of order 2 in a group G is called invalution in G.

Theorem:-

Every group of even order has atleast one invalution.

Proof:-

Let G be a group of order $2n$.

and let $A = \{e, x \mid x^2 = e \wedge x \in G\}$

& $B = \{y \mid y^2 \neq e \wedge y \in G\}$

then

$$A \cup B = G \quad \text{and} \quad A \cap B = \phi$$

if $B = \phi$ then $A = G$

then G contains invalution.

if $B \neq \phi$, let $y \in G$ then $y^2 \neq e \Rightarrow y \neq y^{-1}$

hence $(y^{-1})^2 \neq e \Rightarrow y^{-1} \in B$

i.e $y, y^{-1} \in B$

$\Rightarrow$ number of elements in B is even

As $|G| = |A| + |B|$. (only for disjoint sets)

and so number of elements in A is even.

$\because e \in A \Rightarrow A \neq \phi$

$\Rightarrow |A| \geqslant 2$ $\quad \because$ order of A is even, so it contain min. 2 elements

Since $A \subseteq G$

$\Rightarrow G$ contains an invalution.

* Relation between Groups:-

- **Homomorphism**

def:- Let $(G, *)$ and $(H, \cdot)$ be two groups. Define a mapping $\phi : G \to H$

The ϕ is homomorphism if $\phi(x * y) = \phi(x) \cdot \phi(y)$

e.g. $(\mathbb{R}, +)$, $(\mathbb{R}', \cdot)$ be two groups

define $\phi(x) = e^x \quad \forall\ x \in \mathbb{R}$

then for $x, y \in \mathbb{R}$

$$\begin{aligned}\phi(x+y) &= e^{x+y} \\ &= e^x \cdot e^y \\ &= \phi(x) \cdot \phi(y)\end{aligned}$$

$\Rightarrow \phi$ is homomorphism.

- **Monomorphism**

def:- A mapping $\phi : G \Rightarrow G'$ is called monomorphism if

i) ϕ is homomorphism

ii) ϕ is injective (one-one)

i.e $\phi(a) = \phi(b) \Rightarrow a = b$.

- **Epimorphism**

def:- A mapping $\phi : G \to G'$ is epimorphism such that

i) ϕ is homomorphism

ii) ϕ is surjective (onto)

i.e $\forall\ b \in G'$ there is $a \in G$ such that $\phi(a) = b$.

- Isomorphism

def:- A mapping $\phi : G \to G'$ is isomorphism if i) ϕ is homomorphism

ii) ϕ is bijective (one-one and onto).

(denoted as $G \sim G'$)

- Endomorphism

def:- A homomorphism mapping $\phi : G \to G$ is called endomorphism (i.e on same set).

Example

- Let $\phi : (\mathbb{R}, +) \to (\mathbb{R}_p, \cdot)$, where $\mathbb{R}$ is set of real number and $\mathbb{R}_p$ is the set of non-zero tive real number

define $\phi(x) = e^x \quad \forall \; x \in \mathbb{R}$

is isomorphism.

- Let $(Z, +)$ and $(E, +)$ be two groups under addition then the mapping $\phi : Z \to E$ defined by $\phi(n) = 2n$ is isomorphism between Z and E.

- Let $(Z, +)$ and $(\{\pm 1\}, \cdot)$ be two groups define a mapping $\phi : Z \to \{\pm 1\}$

by $\phi(x) = \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd,} \end{cases}$

prove that ϕ is homomorphism and hence epimorphism.

- $\phi : \mathbb{R}^+ \to \mathbb{R}$ defined by $\phi(x) = \log x$ where $(\mathbb{R}, \cdot)$ and $(\mathbb{R}, +)$ are two groups. then ϕ is isomorphism.

Question:-

Let G and G' are two groups and $f: G \to G'$ is isomorphic then $f^{-1}: G' \to G$ is also isomorphic.

Solution:-

Since $f: G \to G'$ is bijective
so $f^{-1}: G' \to G$ is also bijective
to prove f^{-1} is homomorphism
Let $a, b \in G'$ then there are $x, y \in G$ such that $f(x) = a$ and $f(y) = b$
or $x = f^{-1}(a)$ & $y = f^{-1}(b)$

$\because f$ is homomorphism
$\therefore f(x \cdot y) = f(x) \cdot f(y)$
as $f(xy) = ab \Rightarrow xy = f^{-1}(ab)$ $\because f$ is bijective.
and
$f^{-1}(a) \cdot f^{-1}(b) = x \cdot y$
$= f^{-1}(ab)$

Hence f^{-1} is homomorphism
as f^{-1} is bijective therefore f^{-1} is isomorphism.

Question:-

Let G, G', G'' are groups and $f: G \to G'$, $g: G' \to G''$ are isomorphism then $g \circ f: G \to G''$ is also isomorphism.

Solution:

Since composition of two bijective mapping is bijective so $g \circ f$ is bijective
and $g \circ f(xy) = g(f(xy))$
$= g(f(x) \cdot f(y))$ $\because f$ is isomorphism
$= g(f(x)) \cdot g(f(y))$
$= g \circ f(x) \cdot g \circ f(y)$

therefore $g \circ f$ is homomorphism and hence isomorphism.

Theorem:-

Prove that isomorphic groups form an equivalence relation.

Proof:-

i) Reflexive

Define $I: G \to G$ by $I(x) = x$

then I is one-one and onto

and also $I(x \cdot x) = x \cdot x = I(x) \cdot I(x)$

ii) Symmetric (i.e $G \sim G'$ then $G' \sim G$)

Define $f: G \to G'$ an isomorphic

then $f^{-1}: G' \to G$ is bijective

Now $f(xy) = f(x) \cdot f(y)$.

~~as $f(xy) = ab$~~ prove f^{-1} is homomorphism as in previous Question.

iii) Tansitive (i.e $G \sim G'$ and $G \sim G''$ then $G \sim G''$)

Suppose $f: G \to G'$ and $g: G' \to G''$ are isomorphism. then

prove $g \circ f$ is isomorphism

as in previous Question

Definition (Kernel):

def- Let $\varphi: G \to G'$ be a homomorphism then kernel of φ is defined by.

$$\ker\varphi = \{x \mid x \in G \wedge \varphi(x) = e'\}$$

where e' is ~~the~~ identity of G'.

Lemma:

i) If φ is homomorphism of group G to G' then $\varphi(e) = e'$ (i.e identity element of G is mapped to identity element of G').

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

Proof:

i) Let $x \in G$ then $\varphi(x) \in G'$

Since e' is identity of G'

$\Rightarrow \varphi(x).e' = \varphi(x)$

$= \varphi(x.e) \quad \because x = x.e$

$= \varphi(x).\varphi(e)$

i.e $\varphi(x).e' = \varphi(x).\varphi(e)$

$\Rightarrow e' = \varphi(e)$ by cancellation law.

ii) $\varphi(x).\varphi(x^{-1}) = \varphi(x x^{-1}) \quad \because \varphi$ is homomorphism

$= \varphi(e)$

$= e'$

$\Rightarrow \varphi(x^{-1})$ is inverse of $\varphi(x)$

but $[\varphi(x)]^{-1}$ is also inverse of $\varphi(x)$

$\Rightarrow \varphi(x^{-1}) = [\varphi(x)]^{-1}$ as inverse is unique

Theorem:-

The homomorphic image of a group is a group.

Proof.

Let G be a group and $\phi(G)$ be a homomorphic image of G under ϕ.

1) Let $g_1, g_2 \in G$ then $\phi(g_1), \phi(g_2) \in \phi(G)$

and $\phi(g_1 g_2) = \phi(g_1)\cdot\phi(g_2) \in \phi(G)$

~~$\because g_1 g_2 \in G \Rightarrow \phi(g_1 g_2) \in \phi(G)$~~

i.e $\phi(G)$ is closed.

2) Let $\phi(g_1), \phi(g_2), \phi(g_3) \in \phi(G)$ then

$$\begin{aligned}
\phi(g_1)\cdot[\phi(g_2)\cdot\phi(g_3)] &= \phi(g_1)\cdot(\phi(g_2 g_3)) \\
&= \phi(g_1(g_2 g_3)) \\
&= \phi((g_1 g_2)\cdot g_3) \\
&= \phi(g_1 g_2)\cdot\phi(g_3) \\
&= [\phi(g_1)\cdot\phi(g_2)]\cdot\phi(g_3)
\end{aligned}$$

$\Rightarrow \phi(G)$ is associative.

3) If e is identity of G then

$$\begin{aligned}
\phi(x)\cdot\phi(e) &= \phi(xe) \\
&= \phi(x)
\end{aligned}$$

$\Rightarrow \phi(e)$ is an identity of $\phi(G)$.

4) For $x \in G$, $x^{-1} \in G$

$$\begin{aligned}
\phi(x)\cdot\phi(x^{-1}) &= \phi(x x^{-1}) \\
&= \phi(e).
\end{aligned}$$

i.e $\phi(G)$ contains inverse of its each element

$\because \phi(G)$ satisfy all the axioms of group.

$\therefore \phi(G)$ is group.

Theorem:

Let $\phi : G \to H$ be homomorphism of a group G into group H, then for $a, b \in G$

$$\phi(a) = \phi(b) \quad \text{iff} \quad ab^{-1} \in \ker \phi .$$

Proof:

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

Now $\phi(ab^{-1}) = \phi(a).\phi(b^{-1})$

$= \phi(b).\phi(b^{-1}) \quad \because \phi(a) = \phi(b)$

$= \phi(bb^{-1})$

$= \phi(e) = e' \in H$

$\Rightarrow ab^{-1} \in \ker \phi .$

Conversely, suppose $ab^{-1} \in \ker \phi$.

then $\phi(ab^{-1}) = e'$ where e' is identity of H.

$\Rightarrow \phi(a).\phi(b^{-1}) = e' \quad \because \phi$ is homomorphism.

$\Rightarrow \phi(a)\,[\phi(b)]^{-1} = e'$

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

proved.

Theorem

Let $\phi : G \to H$ be a homomorphism then ϕ is one-one iff $\ker \phi = \{I_G\}$.

Proof:

Suppose ϕ is one-one.

It is obvious that $\{I_G\} \subseteq \ker \phi$

$\because \phi(I_G) = I_H$

$\Rightarrow I_G \in \ker \phi$

i.e $\{I_H\} \subseteq \ker \phi$

and let $a \in \ker \phi$

$\Rightarrow \phi(a) = I_H$

$\Rightarrow \phi(a) = \phi(I_G)$

and $\because \phi$ is one-one

$\therefore a = I_G \Rightarrow a \in \{I_G\}$

$\Rightarrow \ker \phi \subseteq \{I_G\}$ and hence $\ker \phi = \{I_G\}$

Conversely, let $\ker\phi = \{I_G\}$

to prove ϕ is one-one

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

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

$\Rightarrow \phi(ab^{-1}) = \phi(bb^{-1})$

$\Rightarrow \phi(ab^{-1}) = \phi(I_G)$

$\Rightarrow \phi(ab^{-1}) = I_H$

$\Rightarrow ab^{-1} \in \ker\phi$

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

$\Rightarrow a = b$

$\Rightarrow \phi$ is one-one

Theorem:

Let H be a subgroup of a group G.
Define a relation over G such that

$x \sim y$ iff $xy^{-1} \in H$

then relation $\sim$ is equivalence relation.

Proof:-

i) Reflexive

$\because e \in H \Rightarrow xx^{-1} \in H \quad \forall x \in H$

$\Rightarrow x \sim x$

i.e this relation is reflexive

ii) Symmetric

Let $x \sim y$ then $xy^{-1} \in H$

$\Rightarrow (xy^{-1})^{-1} \in H \quad \because H$ is group.

i.e $(xy^{-1})^{-1} = (y^{-1})^{-1} \cdot x^{-1}$

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

so $yx^{-1} \in H$ i.e $y \sim x$.

$\therefore \sim$ is symmetric.

iii) Transitive

Let $x \sim y$ then $xy^{-1} \in H$

also $y \sim z$ then $yz^{-1} \in H$

Now $(xy^{-1})(yz^{-1}) \in H$

or $x(y^{-1}y)z^{-1} \in H$

or $x(e)z^{-1} \in H$

or $xz^{-1} \in H$

$\Rightarrow x \sim z$ i.e $\sim$ is trasitive.

Hence the relation $\sim$ is equivalence.

Cyclic Group:-

def:- A group G is called a cyclic group if all of its element can be express as power of a single element say $a \in G$.

In this case 'a' is called to be a generator of G. i.e if 'a' is generator then for $x \in G$ there is an integer k such that $a^k = x$.

Let G be a finite group of order n then
$G = \{a, a^2, a^3, \ldots\ldots, a^{n-1}, a^n = e\}$.

Note that order of cyclic group is equal to the order of its generator. and the generating element is not necessary unique.

e.g

$\{\pm 1, \pm i\}$.

let $a = i$, $a^2 = i^2 = -1$

$a^3 = i^3 = i \cdot i^2 = -i$

$a^4 = (i^2)^2 = 1$

Also if $a = -i$, then this is also generator

i.e. $i, -i$ are a generator.

****

****

Theorem

Any two cyclic group of same order are isomorphic.

Proof:-

i) For finite order:-

Let G be a ~~cplclic~~ cyclic group of order n.

i.e $G = \langle a : a^n = e \rangle$.

Consider cyclic group C_n of n nth roots of unity. Consider a mapping $\phi : G \to C_n$ defined by

$$\phi(a^k) = e^{\frac{2k\pi}{n}i}$$

$x^n = 1 = 1 + 0i$
$= \cos 2k\pi + i \sin 2k\pi$
$x = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$
$= e^{\frac{2k\pi}{n}i}$

- ϕ is one-one

for $\phi(a^k) = \phi(a^m)$; $a^k, a^m \in G$

$\Rightarrow e^{\frac{2k\pi}{n}i} = e^{\frac{2m\pi}{n}i}$

$\Rightarrow \frac{2k\pi}{n}i = \frac{2m\pi}{n}i$

$\Rightarrow k = m \quad \Rightarrow a^k = a^m$

Thus ϕ is one-one

- ϕ is obviousely onto

$\because$ for every $e^{\frac{2k\pi}{n}i}$, where $k = 0, 1, 2, \ldots, n-1$

$\exists\ a^k \in G \ \forall\ k$.

- Now, $\phi(a^k . a^m) = \phi(a^{k+m})$

$= e^{\frac{2(k+m)\pi}{n}i}$

$= e^{\frac{2k\pi}{n}i} . e^{\frac{2m\pi}{n}i}$

$= \phi(a^k) . \phi(a^m)$

$\Rightarrow \phi$ is homomorphism i.e $G \cong C_n$

ii) For Infinite Order:-

for infinite ~~cylic~~ cyclic group we define a mapping $\phi : G \to \mathbb{Z}$ by $\phi(a^k) = k$.

then ϕ is one-one

$\because \phi(a^k) = \phi(a^m)$ for $a^k, a^m \in G$

$\Rightarrow k = m$

$\Rightarrow a^k = a^m.$

and also for each $k \in Z$ $\exists$ an element $a^k \in G$ such that $\phi(a^k) = k$

$\Rightarrow \phi$ is onto.

Also

$\phi(a^k \cdot a^m) = \phi(a^{k+m})$

$= k + m$

$= \phi(a^k) + \phi(a^m)$

$\Rightarrow \phi$ is homomorphism

hence $G \cong Z$.

and the proof is complete.

Theorem

Let G be a cyclic group of order n and generated by a. Let $d \mid n$, then there is a unique subgroup of order d.

Proof. Let $G = \langle a : a^n = e \rangle$

$\because d \mid n$ $\therefore \exists$ integer q such that $n = dq$.

Take $b = a^q$ then

$b^d = (a^q)^d = a^{qd} = a^n = e$

So $H = \langle b : b^d = e \rangle$ is required subgroup.

To see H is unique, suppose K is another subgroup of G of order d. Then K is generated by an element $c = a^k$, where k is least such +ve integer.

As K has order d

$\therefore a^{kd} = c^d = e$

where $kd = n$ so that

$k = \frac{n}{d} = q$

Hence $b = a^q = a^k = c$

so that $K = H$ and hence H is unique.

Theorem

Every subgroup of a cyclic group is cyclic.

Proof.

Let G be a cyclic group generated by a.
let H be a ~~st~~ subgroup of G and k be the least +ive integer such that $a^k \in H$.
we prove that H is generated by a^k.
For this let $x = a^m \in H \ \forall \ m > k$
then $\exists$ integers q and r such that

$$m = qk + r \quad ; \quad 0 \le r < k.$$

then $a^m = a^{qk+r}$

$$= a^{qk} \cdot a^r$$

$$\Rightarrow a^m \cdot a^{-qk} = a^r$$

$$\Rightarrow a^m \cdot (a^k)^{-q} = a^r$$

$\because$ a^m and $(a^k)^{-q}$ are in H

$$\Rightarrow a^r \in H$$

but k is smallest for which $a^k \in H$
and here $a^r \in H$ and $r < k$
so by minimality of k
$a^r \in H$ only if $r = 0$
but if $r = 0$
then $m = qk$
$\Rightarrow a^m = (a^k)^q$
$\Rightarrow a^k$ is generator of H i.e H is cyclic

Theorem:-

The homomorphic image of a cyclic group is cyclic.

Proof.

Let G be a cyclic group generated by a.
Let $\phi(G)$ be a homomorphic image of G under a homomorphism ϕ.

we show that $\phi(G)$ is cyclic.

Take $b = \phi(a)$

Let $x \in \phi(G)$, then there is an element $a^k \in G$ such that

$$\begin{aligned} x &= \phi(a^k) \\ &= \phi(a \cdot a \cdot a \cdots\cdots a) \quad (k \text{ times}) \\ &= \phi(a) \cdot \phi(a) \cdot \phi(a) \cdots\cdots \phi(a) \quad \because \phi \text{ is homo.} \\ &= b \cdot b \cdot b \cdots\cdots b \quad (k \text{ times}) \\ &= b^k \end{aligned}$$

So $\phi(G)$ is generated by b.

hence $\phi(G)$ is cyclic.

****

****

Theorem:-

i) Let G be a cyclic group of order n generated by a, then an element $a^k \in G$ is a generator of G iff k and n are relatively prime.

ii) If G is infinite cyclic group then a and a^{-1} are its generator only.

Proof:-

Let $G = \langle a : a^n = e \rangle$ be finite cyclic group.
Consider k and n are relatively prime then there exists integers p and q such that $pk + qn = 1$.
Let H be a subgroup generated by a^k,
to prove $H = G$.

$$a^1 = a^{pk+qn}$$
$$= (a^k)^p \cdot (a^n)^q$$
$$= (a^k)^p (e)^q \qquad \because a^n = e$$
$$= (a^k)^p$$

$\because (a^k)^p$ is an element of H

$\Rightarrow a \in H$

$\therefore H = G$

i.e G is also generated by a^k.

Conversely,

Let a^k is generator of G
we prove k and n are relatively prime
$\because a^k$ is generator
so for some integer p.

$$(a^k)^p = a \Rightarrow a^{pk} = a$$
$$\Rightarrow a^{pk-1} = e$$
$$\Rightarrow n \mid pk-1 \qquad \because n \text{ is least such integer, that } a^n = e$$

so $\exists$ integer q such that

$$pk - 1 = qn$$
$$\Rightarrow pk - qn = 1$$

so k and n are relatively prime.

ii) Let $G = \langle a \rangle$ be infinite cyclic group.
Let a^k is also a generator of G.
then $(a^k)^p = a$ for some integer p.
$\Rightarrow a^{kp-1} = e$

$\Rightarrow kp-1 \neq 0$ or $kp-1 = 0$
if $kp-1 \neq 0$
then G is finite, a contradition
hence $kp-1 = 0 \Rightarrow kp = 1$
Since k and p are integers
therefore $k = p = 1$ or $k = p = -1$
i.e a, a^{-1} are only generators.

Complex in a group:
def:- A subset X of a group G is called complex in G.

Product of Complexes
def:- If X and Y are two complexes in G then the product XY is defined as
$$XY = \{xy : x \in X,\ y \in Y\}$$

****

****

imp

Theorem

Let H and K be two subgroup of a group G then HK is subgroup of G iff $HK = KH$.

Proof.

Let HK be a subgroup

let $h_1k_1 \in HK$ for $h_1 \in H$, $k_1 \in K$

$\Rightarrow (h_1k_1)^{-1} \in HK \quad \because HK$ is subgroup.

Now $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH \quad \because k_1^{-1} \in K,\ h_1^{-1} \in H$

i.e. $HK \subseteq KH$ ——— (i)

Now for $h \in H$, $k \in K$, $h^{-1}k^{-1} \in HK$

and for $kh \in KH$

$kh = (k^{-1})^{-1}(h^{-1})^{-1} = (h^{-1}k^{-1})^{-1} \in HK$

as HK is subgroup.

$\Rightarrow KH \subseteq HK$ ——— (ii)

From (i) and (ii)

$HK = KH$.

Conversely, let $HK = KH$, to prove HK is subgroup

Let $h_1k_1,\ h_2k_2 \in HK$

for some $h_1, h_2 \in H$, $k_1, k_2 \in K$.

$$\begin{aligned}
\Rightarrow (h_1k_1)(h_2k_2)^{-1} &= (h_1k_1)(k_2^{-1}h_2^{-1}) \\
&= h_1(k_1k_2^{-1})h_2^{-1} \\
&= h_1(k_3h_2^{-1}) && \text{for } k_1, k_2 \in K,\ k_3 = k_1k_2^{-1} \in K \\
&= h_1(h_2^{-1}k_3) && \because KH = HK \\
&= (h_1h_2^{-1})k_3 && \text{for } h_1, h_2 \in H,\ h_3 = h_1h_2^{-1} \in H \\
&= h_3k_3 \in HK.
\end{aligned}$$

therefore HK is a subgroup.

Question: If H is subgroup of group G then

i) Prove that $H^2 = H$

ii) Prove that $H^{-1} = H$ — Do yourself —

Theorem:-

If H and K are two subgroups of a finite group G and $H \cap K = \{e\}$ then,

$$O(HK) = O(H) \cdot O(K).$$

Proof:-

$HK = \{hk : h \in H, k \in K\}$ and $H \cap K = \{e\}$.

The only way in which $O(HK) \neq O(H) \cdot O(K)$ is that for some $h_1, h_2 \in H$, $h_1 \neq h_2$ and $k_1, k_2 \in K$, $k_1 \neq k_2$ we have $h_1 k_1 = h_2 k_2$.

Let us consider

$$h_1 k_1 = h_2 k_2$$
$$\Rightarrow h_2^{-1}(h_1 k_1) = k_2$$
$$\Rightarrow (h_2^{-1} h_1) k_1 = k_2$$
$$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1} = g \text{ (say)}$$

$\because$ $h_1, h_2 \in H$, $h_1, h_2^{-1} \in H \Rightarrow g = h_2^{-1} h_1 \in H$

and similarly $g = k_2 k_1^{-1} \in K$

i.e $g \in H$ and $g \in K$

$\Rightarrow g \in H \cap K = \{e\}$

$\Rightarrow g = e$

$\therefore h_2^{-1} h_1 = g$ and $k_2 k_1^{-1} = g$

$\Rightarrow h_2^{-1} h_1 = e$, $k_2 k_1^{-1} = e$

$\Rightarrow h_2 = h_1$, $k_2 = k_1$

which is a condradiction

hence $O(HK) = O(H) \cdot O(K)$.

OR

$$|HK| = |H| \cdot |K|$$

Example:

$H = \{1, \omega, \omega^2\}$

$K = \{\pm 1, \pm i\}$ are two subgroups of G

$H \cap K = \{1\}$

then

$HK = \{\pm 1, \pm i, \pm \omega, \pm \omega i, \pm \omega^2, \pm \omega^2 i\}$.

Question.

$G = \{e, f, g, gf, fg, g^2\}$

where $g^3 = e$, $f^3 = e$, $(fg)^2 = e$

prove that G is group.

Theorem:-

:- If H and K are subgroups of a group G such that $O(H\cap K) > 1$ i.e $H\cap K \neq \{e\}$ then

$$O(HK) = \frac{O(H)\cdot O(K)}{O(H\cap K)} \quad \text{or} \quad |HK| = \frac{|H|\cdot|K|}{|H\cap K|}$$

Proof:

Let $O(H) = p$, $O(K) = q$, $O(H\cap K) = r$, $O(HK) = m$.

as $HK = \{hk : h \in H, k \in K\}$

$= \{x_1, x_2, x_3, \ldots\ldots, x_m\}$ (say).

Also $O(H\cap K) = r$

so let $H\cap K = \{y_1, y_2, y_3, \ldots\ldots, y_r\}$

$\because$ each $y_i \in H\cap K \quad \forall\ i = 1, 2, \ldots, r$

and $H\cap K$ is a subgroup

$\therefore\ y_i^{-1} \in H\cap K \quad \forall\ i = 1, 2, \ldots, r$.

So $y_i, y_i^{-1} \in H$ and $y_i, y_i^{-1} \in K$.

Let $h \in H$, $k \in K$

$\Rightarrow hy_i \in H$, $y_i^{-1}k \in K$

$\Rightarrow (hy_i)(y_i^{-1}k) \in HK$.

but $(hy_1)(y_1^{-1}k) = (hy_2)(y_2^{-1}k) = (hy_3)(y_3^{-1}k) = \ldots\ldots$

$\ldots\ldots = (hy_r)(y_r^{-1}k) = hk = x$

i.e x is repeat r times in HK.

So total number of elements possible in HK is rm.

i.e $rm = pq$

$\Rightarrow m = \dfrac{pq}{r}$

i.e $O(HK) = \dfrac{O(H)\cdot O(K)}{O(H\cap K)}$.

proved

Corollary:-

Let H and K are subgroup of a group G such that $o(H) \geq \sqrt{o(G)}$, $o(K) \geq \sqrt{o(G)}$ then $H \cap K \neq \{e\}$.

Proof.

$\because$ $o(H) \geq \sqrt{o(G)}$, $o(K) \geq \sqrt{o(G)}$

as H and K are subgroup of G

$\Rightarrow H \subseteq G$, $K \subseteq G$

$\Rightarrow HK \subseteq G$

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

i.e $o(G) > o(HK)$

$$= \frac{o(H) \cdot o(K)}{o(H \cap K)}$$

$$\geq \frac{\sqrt{o(G)} \cdot \sqrt{o(G)}}{o(H \cap K)}$$

$$= \frac{o(G)}{o(H \cap K)}$$

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

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

Coset:-

def:- Let H be a subgroup of a group G then the set $Ha = \{ha : h \in H\}$ where $a \in G$ is called right coset of H in G.
Similarly $aH = \{ah : h \in H\}$ is left coset of H in G.

In case of addition $a+H$, $H+a$ are left and right coset respectively.

Example:-

Let $G = \{e, f, g, gf, fg, g^2\}$ be a group where

$$f^3 = e \quad , g^3 = e \quad , \quad (fg)^2 = e$$

Let $H = \{e, g, g^2\}$ be a subgroup.

$He = \{e, g, g^2\}$

$Hg = \{g, g^2, g^3 = e\}$

$Hg^2 = \{g^2, g^3, g^4\} = \{g^2, e, g\}$

$Hf = \{f, gf, g^2f\} = \{f, gf, fg\}$.

As

$(fg)^2 = e$

$\Rightarrow (fg)(fg) = e$

$\Rightarrow fg = g^{-1}f^{-1}$

$f^2 = e \Rightarrow f \cdot f = e \Rightarrow f = f^{-1}$

$g^3 = e \Rightarrow g^2 \cdot g = e \Rightarrow g^2 = g^{-1}$

$\Rightarrow fg = g^2 f$.

So

$Hgf = \{gf, g^2f, g^3f\} = \{gf, fg, f\}$.

$Hfg = \{fg, g(fg), g^2(fg)\} = \{fg, g(g^2f), g^2(g^2f)\}$

$= \{fg, f, gf\}$.

Now $He = Hg = Hg^2 = \{e, g, g^2\}$.

$Hf = Hfg = Hgf = \{f, gf, fg\}$.

i.e we have only two disjoint right coset.

Index of Subgroup:-

def:- The number of distinct left or right cosets of H in G is called index of H in G.

Index of subgroup:-

def:- The number of distinct left or right cosets of a subgroup H of a group G is called the index of H in G and is denoted by $[G:H]$.

Theorem:- (Lagrange's Theorem).

-: Both the order and index of a subgroup of a finite group divide the order of the group.

Proof:-

Let G be a group of order n and H be a subgroup of order m.

Also let k be the index of H in G.

Let $a_1H, a_2H, \ldots, a_kH$ are the distinct left cosets of H in G.

we prove $G = \bigcup_{i=1}^{k} a_iH$ and $a_iH \cap a_jH = \phi$, $i \neq j$ and $i, j = 1, 2, \ldots, k$.

Let $a_i \in G$

then $a_i = a_ie \in a_iH$ because $e \in H$.

so, $G \subseteq \bigcup a_iH$ ——— (i)

Also each a_iH is a subset of G

$\therefore \bigcup a_iH \subseteq G$ ——— (ii)

From (i) and (ii)

$$G = \bigcup_{i=1}^{k} a_iH.$$

Next, let aH and bH are distinct left cosets and $x \in aH \cap bH$.

then $x = ah_1 = bh_2$ for some $h_1, h_2 \in H$.

$\Rightarrow a = bh_2h_1^{-1}$

$= bh_3$ where $h_3 = h_2h_1^{-1}$ (say).

Now for $h \in H$, $ah \in aH$

but $ah = bh_3h$ is also an element of bH

$\Rightarrow aH \subseteq bH$

Similarly $bH \subseteq aH$

i.e $aH = bH$, a contradiction

hence $x \notin aH \cap bH$

$\Rightarrow aH \cap bH = \varphi$.

$\Rightarrow$ all left cosets of H in G define a partition.

i.e

$$|G| = |a_1H| + |a_2H| + \cdots + |a_kH| \quad \text{——— (iii)}$$

To find number of element in each coset we define a mapping $\varphi : H \to a_iH$ by

$$\varphi(h) = a_ih \quad , \quad h \in H.$$

for $h_1, h_2 \in H$

$\varphi(h_1) = \varphi(h_2)$

$\Rightarrow a_ih_1 = a_ih_2$

$\Rightarrow h_1 = h_2$

$\Rightarrow \varphi$ is one-one

Also for each $a_ih \in a_iH$ $\exists$ $h \in H$.

so φ is onto

hence the number of elements in H and a_iH is the same for $i = 1, 2, \ldots, k$

As H has m elements, each a_iH has m elements.

So from (iii) we have

$n = m + m + \cdots + m$ (k times)

$\Rightarrow n = km$

$\Rightarrow k \mid n$ and $m \mid n$

i.e order and index of subgroup divides order of group.

****

****

Double Cosets:-

def:- Let H and K are two subgroups of a group G then for $a \in G$ the set

$$HaK = \{hak : h \in H, k \in K\}$$

is called coset of module (H, K).

Theorem:-

Let H and K are two subgroup of a group G. then the collection of all double cosets defines a partition in G.

Proof:-

Let HaK be a collection of all double coset of H and K in G

we have to prove

$$G = \cup(HaK) \quad \text{and} \quad HaK \cap HbK = \phi.$$

Since each $HaK \subseteq G$

$$\Rightarrow \cup(HaK) \subseteq G \text{ ——— (i)}$$

if $a \in G$ then $eae \in HaK$

i.e $a \in HaK$

$$\Rightarrow G \subseteq \cup(HaK) \text{ ——— (ii)}$$

from (i) and (ii)

$$G = \cup(HaK)$$

Now consider HaK and HbK are two distinct double cosets

let $x \in (HaK) \cap (HbK)$

$\Rightarrow x \in HaK$ and $x \in HbK$

$\therefore x = hak$ and $x = h_1 b k_1$

$$\Rightarrow hak = h_1 b k_1$$

$$\Rightarrow ak = h^{-1} h_1 b k_1$$

$$\Rightarrow a = h^{-1} h_1 b k_1 k^{-1}$$

if $y \in HaK$

then $y = h_2 a k_2$

$= h_2(h^{-1}h_1 b k_1 k^{-1})k_2$

$= h_2 h^{-1} h_1 b k_1 k^{-1} k_2 \in HbK$

$\Rightarrow y \in HbK$

$\Rightarrow HaK \subseteq HbK$

Similarly, we can get

$HbK \subseteq HaK$

$\Rightarrow HaK = HbK$

which is contradiction as HaK and HbK are distinct.

hence $HaK \cap HbK = \phi$

The proof is complete.

Normalizer:

def:- Let X be a subset of a group G then the set $N_G(X) = \{a : a \in G, aX = Xa\}$ is called Normalizer of X in G.

here $aX = Xa$ means, for $x \in X$, there is $x' \in X$ such that $ax = x'a$

Theorem:

The normalizer $N_G(X)$ of a subset X is a subgroup of G.

Proof:-

Let $a, b \in N_G(X)$

then $aX = Xa$ and $bX = Xb$

$\because bX = Xb$

$\Rightarrow (bX)b^{-1} = (Xb)b^{-1}$

$\Rightarrow b(Xb^{-1}) = X(bb^{-1})$

$\Rightarrow b(xb^{-1}) = x$

$\Rightarrow xb^{-1} = b^{-1}x$

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

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

$= a(xb^{-1}) \quad \because b^{-1} \in N_G(x)$

$= (ax)(b^{-1})$

$= (xa)b^{-1} \quad \because a \in N_G(x)$

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

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

Hence $N_G(x)$ is a subgroup of G.

Corollary:-

If H is a subgroup of G then $H \subseteq N_G(H)$.

Proof:-

Let $h \in H$

then $hH = H = Hh \quad \because aH = H \Leftrightarrow a \in H$

i.e $hH = Hh$

$\Rightarrow h \in N_G(H)$

so $H \subseteq N_G(H)$.

Note:

The above corollary can also be state as.

" Normalizer of a subgroup contains that subgroup."

Also converse of above corollary may not true.

****

****

Centralizer

def:- Let X be a subset of a group G and $\forall\ x \in X$, then the set
$$C_G(X) = \{a : a \in G \wedge ax = xa\}$$
is called centralizer of X in G.

Centre of G

def:- The centralizer of G in G is called centre of G.

Theorem:-

The centralizer of X in G is a subgroup of G.

Proof:-

Let $a, b \in C_G(X)$

then by definition, $\forall\ x \in X$

$$ax = xa \text{ ——— (i)}$$
$$bx = xb \text{ ——— (ii)}$$

from (ii)

$$bx = xb \Rightarrow (bx)b^{-1} = (xb)b^{-1}$$
$$\Rightarrow b(xb^{-1}) = x(bb^{-1})$$
$$\Rightarrow b(xb^{-1}) = x$$
$$\Rightarrow xb^{-1} = b^{-1}x \text{ ——— (iii)}$$

Hence

$$(ab^{-1})x = a(b^{-1}x)$$
$$= a(xb^{-1}) \quad \text{by (iii)}$$
$$= (ax)b^{-1}$$
$$= (xa)b^{-1} \quad \text{by (i)}$$
$$= x(ab^{-1})$$
$$\Rightarrow ab^{-1} \in C_G(X)$$

hence $C_G(X)$ is a subgroup of G.

Conjugate or Transform in a group:-

def:- Let $a \in G$, then an element gag^{-1}, $g \in G$ is called conjugate of a.

or for $a, b \in G$, b is conjugate of a if $b = gag^{-1}$, $g \in G$.

Theorem:

-: The relation of conjugacy between element of group G is equivalence relation.

Proof:-

We denote the conjugacy relation of element by R or $\sim$.

i) ~~Refel~~ Reflexive

$\because a = eae^{-1}$, $e \in G \Rightarrow a \sim a$.

ii) Symmetric.

Let $a \sim b$

$\Rightarrow b = gag^{-1}$, $g \in G$

$\Rightarrow gag^{-1} = b$

$\Rightarrow ag^{-1} = g^{-1}b$

$\Rightarrow a = g^{-1}bg$

$\Rightarrow a = g^{-1}b(g^{-1})^{-1}$ where $g^{-1} \in G$.

$\Rightarrow b \sim a \Rightarrow \sim$ is symmetric.

iii) Transitive

Let $a \sim b$ & $b \sim c$

$\Rightarrow b = g_1 a g_1^{-1}$ & $c = g_2 b g_2^{-1}$ for $g_1, g_2 \in G$.

Since

$c = g_2 b g_2^{-1}$

$= g_2 (g_1 a g_1^{-1}) g_2^{-1}$

$= (g_2 g_1) a (g_1^{-1} g_2^{-1})$

$= (g_2 g_1) a (g_2 g_1)^{-1}$

$\Rightarrow a \sim c$

hence $\sim$ is an equivalence relation.

Question

G is a group such that

$$G = \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle$$

and subset i) $X = \{1, a^2\}$ ii) $X = \{1, a, a^2, a^3\}$

Find centralizer of X.

Solution:-

i) $G = \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle$

$= \{1, a, a^2, b, a^3, ab, a^2b, a^3b\}$

$\because a^4 = 1$	$b^2 = 1$
$\Rightarrow a^{-1} = a^3$	$\Rightarrow b^{-1} = b$
& $(ab)^2 = 1$	& $(ab)^2 = 1$
$\Rightarrow (ab)(ab) = 1$	$\Rightarrow (ab)(ab) = 1$
$\Rightarrow ab = b^{-1}a^{-1}$	$\Rightarrow a(ba)b = 1$
$= ba^3$	$\Rightarrow ba = a^{-1}b^{-1}$
	$= a^3b$

$C_G(X)$ contains those elements of G which commute with every element of X.

For a

$$a \cdot 1 = a = 1 \cdot a$$
$$a \cdot a^2 = a^3 = a^2 \cdot a$$

For a^2

$$a^2 \cdot 1 = 1 \cdot a^2$$
$$a^2 \cdot a^2 = a^2 \cdot a^2$$

For a^3

$$a^3 \cdot 1 = a^3 = 1 \cdot a^3$$
$$a^3 \cdot a^2 = a^5 = a^2 \cdot a^3$$

For b

$$b \cdot 1 = b = 1 \cdot b$$
$$b \cdot a^2 = (ba)a = (a^3b)a = a^3(ba)$$
$$= a^3(a^3b) = a^6b = a^4(a^2b) = a^2b$$

For ab

$$(ab) \cdot 1 = ab = 1 \cdot (ab)$$

$$(ab)\cdot a^2 = (ba^3)\cdot a^2 = ba^5 = (ba)a^4 = ba$$
$$= a^3 b = a^2(ab)$$

For $a^3 b$

$$a^3 b \cdot 1 = 1\cdot a^3 b$$
$$(a^3 b)\cdot a^2 = (ba)\cdot a^2 = ba^3 = ab$$
& $a^2\cdot(a^3 b) = a^5 b = a^4(ab) = ab$
$$\Rightarrow (a^3 b)\cdot a^2 = a^2\cdot(a^3 b)$$

For $a^2 b$

$$(a^2 b)\cdot 1 = 1\cdot(a^2 b)$$
$$(a^2 b)\cdot a^2 = a(ab)a^2 = a(ba^3)a^2$$
$$= a(ba) = a(a^3 b) = a^4 b = a^2\cdot(a^2 b)$$

As all element of G commute with element of X therefore $C_G(X) = G$.

ii) $X = \{1, a, a^2, a^3\}$

$ba \neq ab$ so b does not commute with a.

$a^2(ab) = a^3 b \neq ba^3$

$\therefore C_G(X) = \{1, a, a^2, a^3\} = X$.

Exercise.

Find the center of D_8

$D_8 = \langle a, b : a^4 = b^2 = (ab)^2 = e \rangle$

Ans: $C_G(G) = \{e, a^2\}$.

Exercise.

Find ~~$N_G(D_8)$~~ $N_G(X)$ if $G = D_8$

and i) $X = \{1, a^2\}$, ii) $X = \{1, a, a^2, a^3\}$.

Ans: i) G

ii) $\{1, a, a^2, a^3\}$

Remarks

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

$\Rightarrow b^m = (gag^{-1})^m = ga^mg^{-1}$ and $a^m = g^{-1}b^m(g^{-1})^{-1}$

i.e $a^m = e$ iff $b^m = e$

i.e order of a & b is same.

- If $X = \{x\}$ = singleton set then $C_G(X) = N_G(X)$.

Self-Conjugate:

—: An element $a \in G$ is called self-conjugate if for $g \in G$, $a = gag^{-1}$ i.e $ga = ag$

self conjugate elements also called central elements.

Corollary

—: An element x in a group G is self-conjugate iff $x \in C_G(G)$.

Proof:-

Let x is self-conjugate then there is $g \in G$ such that $x = \cancel{gag^{-1}}\ gxg^{-1}$

$\Rightarrow xg = gx$

$\Rightarrow x \in C_G(G)$.

Conversely,

Let $x \in C_G(G)$

then $xg = gx$

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

$\Rightarrow x$ is self conjugate.

Conjugancy Class

def:- Let $a \in G$ then the subset of all element of G conjugate to a is called conjugacy class. i.e $C_a = \{b : b \in G,\ b = gag^{-1},\ g \in G\}$.

Theorem

:- The number of elements in a conjugacy class C_a of an element $a \in G$ is equal to the index of its normalizer in G and hence divides the order of G.

Proof.

Let G be a group and $a \in G$. Let C_a be the conjugacy class of G containing a. Let N be a normalizer of $\{a\}$ in G i.e $N_G(\{a\}) = N$.

Let A be the collection of all right cosets of normalizer.

then we have to prove that number of elements in A is equal to number of elements in C_a.

Define a mapping

$\varphi : A \to C_a$ by $\varphi(Ng) = g^{-1}ag$, $g \in G$.

i) φ is well define

Let $Ng_1 = Ng_2$ where $g_1, g_2 \in G$

$\Rightarrow N = Ng_2g_1^{-1}$

$\Rightarrow g_2g_1^{-1} \in N$

if $a \in H$ then $aH = H$

$g_2g_1^{-1} = n$ (say $n \in N$)

Now

$$g_2^{-1}ag_2 = (ng_1)^{-1}a(ng_1) \qquad \because g_2 = ng_1$$
$$= (g_1^{-1}n^{-1})a(ng_1)$$
$$= g_1^{-1}(n^{-1}an)g_1$$
$$= g_1^{-1}ag_1 \qquad \because n^{-1}an = a$$

$\Rightarrow \varphi(Ng_2) = \varphi(Ng_1)$

$\Rightarrow \varphi$ is well defined.

ii) φ is onto as to every $g^{-1}ag \in C_a$, we have right coset Ng.

iii) φ is one-one

$$\varphi(Ng_1) = \varphi(Ng_2)$$
$$\Rightarrow g_1^{-1} a g_1 = g_2^{-1} a g_2$$
$$\Rightarrow g_2(g_1^{-1} a g_1) g_2^{-1} = a$$
$$\Rightarrow (g_2 g_1^{-1}) a (g_1 g_2^{-1}) = a$$
$$\Rightarrow (g_1 g_2^{-1})^{-1} a (g_1 g_2^{-1}) = a$$
$$\Rightarrow g_1 g_2^{-1} \in N$$
$$\Rightarrow g_1 \in Ng_2 \quad \text{but } g_1 \in Ng_1$$
$$\Rightarrow Ng_1 \subseteq Ng_2$$

Similarly

$$Ng_2 \subseteq Ng_1$$
$$\Rightarrow Ng_1 = Ng_2 \quad \text{so } \varphi \text{ is one-one.}$$

$\Rightarrow \varphi$ is bijective

i.e no. of elements in A = no. of elements in C_a

$\Rightarrow$ no. of elements in C_a is equal to the no. of right cosets of normalizer of $\{a\}$.

and since by Lagrange's theorem index (no. of right cosets) divides order of the group G.

Review:

- Let $a \in G$, then the subset of all element of G conjugate to a is called conjugacy class

  i.e $C_a = \{b : b \in G,\ b = gag^{-1},\ g \in G\}$.

- If $X = \{a\}$ then

$$N_G(X) = C_G(X)$$

i.e Normalizer of X in G = Centralizer of X in G.

Class Equation

def:- Let G be a finite group of order n. then the number of conjugacy classes will also be finite. Let $C_1, C_2, C_3, \ldots, C_r$ be the all conjugacy classes with $m_1, m_2, m_3, \ldots, m_r$ number of elements respectively.

then
$$\left.\begin{aligned} n &= |C_1| + |C_2| + \cdots + |C_r| \\ \text{i.e}\quad n &= m_1 + m_2 + \cdots + m_r \end{aligned}\right\} \text{—— (i)}$$

where each m_i divides n.

then equation (i) is called class equation.

P-Group

def:- Let G be a group of order p^n, where p is a prime number then p divides $|G| = p^n$. If order of every element $a \in G$ is also a power of that prime number p.

then G is called p-group.

Theorem.

-: The centre of p-group is non-trivial.

Proof.

Let G be a p-group of order p^n and its class equation

$$p^n = m_1 + m_2 + \cdots + m_r$$

where each m_i divides p^n

Since each m_i divides p^n so it must be of the form p^{α_i}

i.e $p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_r}$

Let one of them say m_i is one due to conjugacy class of identity element.

Also conjugacy classes of self-conjugate element contain ~~only~~ only that element i.e a is self-conjugate then $C_a = \{a\}$

but if $b \in C_a$

then $b = gag^{-1}$

$\Rightarrow bg = ga$

$\Rightarrow bg = ag$ $\because$ a is self-conjugate

$\Rightarrow b = a$

Let such classes of the above two types ~~be~~ be K

without loss of generality those are

$m_1, m_2, \ldots, m_K$

Now

$$p^n = m_1 + m_2 + \cdots + m_K + m_{K+1} + m_{K+2} + \cdots + m_r$$

$$= 1 + 1 + \cdots + 1 + m_{K+1} + m_{K+2} + \cdots + m_r$$

$$= K + p^{\alpha_{K+1}} + p^{\alpha_{K+2}} + \cdots + p^{\alpha_r}$$

$$\Rightarrow K = p^n - (p^{\alpha_{K+1}} + p^{\alpha_{K+2}} + \cdots + p^{\alpha_r})$$

$$= p^n - \sum_{i=K+1}^{r} p^{\alpha_i}$$

Now

$p \mid p^n$ and $p \mid p^{\alpha_i}$ for each $i = K+1, K+2, \ldots, r$

$$\Rightarrow p \mid p^n - \sum_{i=K+1}^{r} p^{\alpha_i}$$

i.e. $p \mid K$

$\Rightarrow$ centre of p-group is non-trivial.

Alternative Statements:

- Every group of order p^n has non-trivial centre.
- Every finite p-group has non-trivial centre.

Conjugate Subgroup

def:– Let H be a subgroup of a group G. Define a set

$$K = gHg^{-1} = \{ghg^{-1} : h \in H\} \cancel{g \in G}$$

for some $g \in G$.

Theorem

:– If H is a subgroup of a group G and K is conjugate to H then K is also subgroup of G.

Proof:–

$$K = gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

Let $a, b \in K$

then $a = gh_1g^{-1}$, $b = gh_2g^{-1}$ where $h_1, h_2 \in H$.

Now

$$ab^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1}$$

$$= (gh_1g^{-1})(gh_2^{-1}g^{-1})$$

$$= gh_1(g^{-1}g)h_2^{-1}g^{-1}$$

$$= gh_1eh_2^{-1}g^{-1}.$$

$$= gh_1h_2^{-1}g^{-1}.$$

$\because h_1, h_2 \in H$ and H is subgroup

$\therefore h_1h_2^{-1} \in H$ & $h_1h_2^{-1} = h_3$ (say)

$\Rightarrow ab^{-1} = gh_3g^{-1}$

$\Rightarrow ab^{-1} \in K \Rightarrow K$ is subgroup

****

Available online at *http://www.MathCity.org*

****

Theorem

:- Let G be a group of finite order n then order of a subgroup H and that of its conjugate K is same.

OR

Conjugate subgroups H and K are isomorphism.

Proof:-

Let H and K are two subgroups where K is conjugate to H by g.

$$K = gHg^{-1} = \{ghg^{-1} : h \in H\}$$

Define a mapping

$$\phi : H \to K \quad \text{by} \quad \phi(h) = k$$

i) then ϕ is onto

$\because$ $k \in K$ is image of $h \in H$ as $k = ghg^{-1}$

ii) ϕ is one-one

$$\phi(h_1) = \phi(h_2)$$
$$\Rightarrow k_1 = k_2$$
$$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$$
$$\Rightarrow h_1 = h_2$$

$\Rightarrow$ ϕ is bijective mapping.

So no. of element in H and K are equal.

To prove $\phi(h_1h_2) = \phi(h_1)\phi(h_2)$ i.e. homomorphism.

$$\phi(h_1h_2) = gh_1h_2g^{-1}$$
$$= (gh_1)(h_2g^{-1})$$
$$= (gh_1)g^{-1}g(h_2g^{-1})$$
$$= (gh_1g^{-1})(gh_2g^{-1})$$
$$= \phi(h_1)\cdot\phi(h_2)$$

$\Rightarrow$ ϕ is homomorphism

$\because$ ϕ is bijective

$\therefore$ H and K are isomorphism.

Theorem

$\because$ H and K are finite subgroups of a group G then each double coset HaK contains $\frac{mn}{q}$ number of elements.

where $O(H) = m$, $O(K) = n$ and $O(Q) = q$.

with $Q = H \cap aK\bar{a}^1$.

Proof:

$\because$ H and K are finite subgroup of G so number of elements in HaK is also finite

Let $HaK = \{g_1, g_2, \ldots, g_r\} = \bigcup_{i=1}^{r} \{g_i\}$, $r<n$

then $\because HaK \subseteq G$

$$HaK\bar{a}^1 = \bigcup_{i=1}^{r} \{g_i \bar{a}^1\}$$

Define mapping $\phi : HaK \to HaK\bar{a}^1$ by $\phi(hak) = hak\bar{a}^1$

then each $g_i\bar{a}^1$ is distinct

but for $i \neq j$ if $g_i\bar{a}^1 = g_j\bar{a}^1$

$$\Rightarrow g_i = g_j$$

$$\Rightarrow |HaK| = |HaK\bar{a}^1| \quad \text{——— (i)}$$

Also let $aK\bar{a}^1 = K'$ then number of elements in K', being conjugate to K, is n.

Now

$$|HaK\bar{a}^1| = |HK'|$$

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

$$= \frac{m \cdot n}{|Q|} \quad \text{where } |H \cap K'| = |Q| \text{ (say)}$$

$$= \frac{mn}{q} \quad \text{——— (ii)} \quad |Q| = q \text{ (say)}$$

where $Q = H \cap K' = H \cap aK\bar{a}^1$.

By (i) and (ii)

$$|HaK| = \frac{mn}{q} \quad \text{proved}$$

Theorem

:- Let H and K ~~are~~ be subgroups of a group G, HaK is a double coset and $Q = H \cap aKa^{-1}$ then there is one-one correspondence between the left coset of K in HaK and the left coset of Q in H.

Proof.

Let A be the collection of all left cosets haK of K in HaK and B be the collection of all left cosets hQ of Q

Define a mapping $\phi : A \to B$ as follows:
For each $haK \in A$ we have a left coset hQ of Q in H

i.e $\phi(haK) = hQ$

then ϕ is well define

As $haK = h'aK$

$\Rightarrow hak = h'ak'$ for $k, k' \in K$

$\Rightarrow h'^{-1}h = ak'k^{-1}a^{-1} \in aKa^{-1}$ as $k'k^{-1} \in K$

$\Rightarrow h'^{-1}h \in Q$

$\Rightarrow h \in h'Q$ but $h \in hQ$

$\Rightarrow hQ \subseteq h'Q$

Similarly we can show

$h'Q \subseteq hQ \Rightarrow hQ = h'Q$

i.e $\phi(haK) = \phi(h'aK)$

so ϕ is well define.

ϕ is one one as

$\phi(haK) = \phi(h'aK)$

$\Rightarrow hQ = h'Q$

$\Rightarrow h'^{-1}hQ = Q$

$\Rightarrow h'^{-1}h \in Q$

So

$h'^{-1}h = aka^{-1}$ $\because Q = H \cap aKa^{-1}$

$\Rightarrow ha = h'ak \in h'aK$ *

* Also $ha = hae \in haK$

$\Rightarrow haK$ and $h'aK$ are not disjoint

$\Rightarrow haK = h'aK$

Also ϕ is onto obviously

So there is one-one correspondence between element of A and B

Normal Subgroup

def:- Let H be a subgroup of a group G.
If $a^{-1}Ha = H$ for $a \in G$.
or $a^{-1}ha \in H$ for $h \in H$, $a \in G$.
then H is called normal subgroup.
and we write $H \Delta G$.

Note:

If $a^{-1}ha \in H$ then $a^{-1}ha = h_1 \Rightarrow ha = ah_1$.

Theorem

Let G and H are two groups and $\phi : G \to H$ is a homomorphism. Then $\ker\phi$ is a normal subgroup of G.

Proof.

Let $a, b \in \ker\phi$
$\Rightarrow \phi(a) = I_H$ and $\phi(b) = I_H$

To prove $\ker\phi$ is a subgroup, we show that $ab^{-1} \in \ker\phi$.

$\phi(ab^{-1}) = \phi(a)\cdot\phi(b^{-1})$ $\quad \because \phi$ is homomorphism
$= I_H \cdot (\phi(b))^{-1}$ $\quad \because \phi(a) = I_H$
$= I_H \cdot (I_H)^{-1}$
$= I_H$

$\Rightarrow ab^{-1} \in \ker\phi$

Let $k \in \ker\phi$
to prove $gkg^{-1} \in \ker\phi$, $g \in G$.

$\phi(gkg^{-1}) = \phi(g)\cdot\phi(k)\cdot\phi(g^{-1})$ $\quad \because \phi$ is homomorphism
$= \phi(g)\cdot I_H \cdot \phi(g^{-1})$
$= \phi(g)\cdot\phi(g^{-1})$
$= \phi(gg^{-1})$
$= \phi(e) = I_H$

$\Rightarrow gkg^{-1} \in \ker\phi$.
$\Rightarrow \ker\phi$ is normal subgroup.

Theorem

:- If H and K are normal subgroup of G with $H \cap K = \{e\}$. Show that every element of H commute with every element of K

Proof.

Let $h \in H$ and $k \in K$

then we have to prove $hk = kh$.

For this we consider the element $hkh^{-1}k^{-1}$

As H is normal subgroup of G.

$\Rightarrow kh^{-1}k^{-1} \in H$ for $h^{-1} \in H$, $k \in K \subseteq G$.

$\Rightarrow h(kh^{-1}k^{-1}) \in H$ by closure law as $h \in H$.

or $hkh^{-1}k^{-1} \in H$

Also K is normal subgroup of G.

$\Rightarrow hkh^{-1} \in K$ for $k \in K$, $h \in H \subseteq G$.

$\Rightarrow (hkh^{-1})k^{-1} \in K$ by closure law as $k^{-1} \in K$

$\Rightarrow hkh^{-1}k^{-1} \in K$

$\because hkh^{-1}k^{-1} \in H$ and $hkh^{-1}k^{-1} \in K$

$\therefore hkh^{-1}k^{-1} \in H \cap K = \{e\}$

$\Rightarrow hkh^{-1}k^{-1} = e$

$\Rightarrow hk = kh$

proved

Corollary

:- Let G be an abelian group then each subgroup of G is normal in G.

Proof.

Let H is a subgroup of G.

$\because G$ is abelian $\therefore ab = ba \ \forall a, b \in G$

$\Rightarrow ah = ha \ \forall h \in H$ and $a \in G$

$\Rightarrow h = a^{-1}ha \in H$

hence H is normal in G.

Theorem

:- Let H be a subgroup of a group G then following are equivalent.

i) H is normal subgroup of G.

ii) $gHg^{-1} = H$ for each $g \in G$.

iii) $gH = Hg$.

Proof:

(i) $\Rightarrow$ (ii)

Let H is normal subgroup of G.

then $gHg^{-1} \in H$, $g \in G$

$\Rightarrow gHg^{-1} \subseteq H$ ——— (A)

If $h \in H$

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

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

$= gh'g^{-1} \in gHg^{-1}$

$\because H$ is normal

$\therefore g^{-1}hg \in H, g \in G$

$\Rightarrow g^{-1}hg = h'(\text{say}) \in H$

$\Rightarrow H \subseteq gHg^{-1}$ ——— (B)

from (A) and (B)

$gHg^{-1} = H$

Now (ii) $\Rightarrow$ (iii)

i.e $gHg^{-1} = H$

$\Rightarrow ghg^{-1} = h'$, $h, h' \in H$

or $h = g^{-1}h'g$

For $gh \in gH$

$gh = g(g^{-1}h'g)$

$= (gg^{-1})h'g = eh'g$

$= h'g \in Hg$

$\Rightarrow gH \subseteq Hg$ ——— (C)

Likewise $Hg \subseteq gH$ $\Rightarrow gH = Hg$.

(iii) $\Rightarrow$ (i)

$$gH = Hg$$

$\Rightarrow \quad gh = h'g \quad$ for $h, h' \in H$

$\Rightarrow \quad ghg^{-1} = h' \in H$

$\Rightarrow$ H is normal subgroup of group G.

Theorem

∴ Every subgroup of index two is a normal subgroup.
OR Let G be a group and H a subgroup of index two then $H \trianglelefteq G$.

Proof:

Let H be a subgroup of index two
i.e H has two distinct right (or left) coset in G.
One of the two right coset is $H = He$ and the other one is Ha.
then $a \notin H$ ∵ if $a \in H$ then $Ha = H$.
Similarly one left coset is $H\ (= eH)$ and the other left coset is aH
By Lagrange's theorem all right (or left) coset define a partition

i.e $G = H \cup Ha = H \cup aH$

and $H \cap Ha = aH \cap H = \phi$.

$\Rightarrow aH = Ha$

i.e each left coset is equal to right coset

$\Rightarrow \quad ah = ah' \quad$ for $h, h' \in H$ and $a \in G$.

$\Rightarrow \quad aha^{-1} = h' \in H$

$\Rightarrow \quad aha^{-1} \in H$

$\Rightarrow \quad H \trianglelefteq G$.

Factor or Quotient Group.

Let H be a normal subgroup of a group G. Consider a collection of all right cosets Ha of H in G.

i.e $Q = G/H = \{Ha : a \in G\}$

is called the quotient group of G by H.

We define multiplication in Q by

For $Ha, Hb \in Q$

$$Ha \cdot Hb = Hab.$$

This multiplication is well define

for $h_1 a \in Ha$, $h_2 b \in Hb$

we have

$$h_1 a h_2 b = h_1 (a h_2) b$$
$$= h_1 (h_3 a) b$$
$$= (h_1 h_3)(ab)$$
$$= h_4 ab$$

$\because H \trianglelefteq G$

$aH = Ha$

$\Rightarrow a h_2 = h_3 a$, $h_2, h_3 \in H$

$h_4 = h_1 h_3$ (say) $\in H$

$$\Rightarrow Ha\,Hb = Hab$$

Also Q is group.

$\because$ i) Q is closed as $Ha \cdot Hb = Hab \in Q$

ii) Q is associative

$$Ha \cdot (Hb \cdot Hc) = Ha \cdot Hbc$$
$$= Ha(bc) = H(ab)c$$
$$= Hab \cdot Hc = (Ha \cdot Hb) \cdot Hc$$

iii) H is identity of Q.

$\because Ha \cdot H = Ha \cdot He = Hae = Ha$

and $H \cdot Ha = He \cdot Ha = Hea = Ha$

iv) for $a \in G$ $\exists$ $\bar{a}' \in G$

such that $Ha \cdot H\bar{a}' = Ha\bar{a}' = He = H$

also $H\bar{a}' \cdot Ha = H\bar{a}'a = He = H$

$\Rightarrow Q$ contain inverse of each right coset.

$\therefore Q = G/H = \{Ha : a \in G\}$

is a quotient group

Theorem

∴ Let H be a normal subgroup of G and $\phi : G \to G/H$ is a mapping given by $\phi(a) = Ha \ \forall \ a \in G$. then ϕ is epimorphism (homomorphism + onto) and $\ker\phi = H$.

Proof.

$\because \ \phi : G \to G/H$ is defined as

$$\phi(a) = Ha \quad , a \in G.$$

i) ϕ is well defined as

$$a = b \quad , \quad a, b \in G$$
$$Ha = Hb$$
$$\Rightarrow \phi(a) = \phi(b)$$

ii) ϕ is onto as

$Ha \in G/H$ is an image of $a \in G$ under ϕ.

iii) ϕ is homomorphism:

$$\phi(a) \cdot \phi(b) = Ha \cdot Hb$$
$$= Hab$$
$$= \phi(ab)$$

i.e $\phi(ab) = \phi(a) \cdot \phi(b) \Rightarrow \phi$ is homomorphism.

$\Rightarrow \phi$ is epimorphism as it is onto & homomorphism.

To prove $\ker\phi = H$

Let $a \in H \subseteq G$

$$\phi(a) = Ha$$
$$= H$$

$\because$ when $a \in H$ then $Ha = H$

$$= \text{identity of Quotient group}$$
$$\Rightarrow a \in \ker\phi$$
$$\Rightarrow H \subseteq \ker\phi \quad \text{——— (i)}$$

Conversely, Let $a \in \ker\phi$

$$\Rightarrow \phi(a) = H$$
$$\Rightarrow Ha = H$$
$$\Rightarrow a \in H$$
$$\Rightarrow \ker\phi \subseteq H \quad \text{——— (ii)}$$

From (i) and (ii)

$$\ker\phi = H \qquad \text{proved}$$

Ist Isomorphism theorem

-: Let $\phi : G \to G'$ be an epimorphism then the quotient group G/K is isomorphic to $G' = \phi(G)$ and K is $\ker\phi$.

Proof:

$$\phi : G \to G'$$

$$\Rightarrow \phi(g) = g' \quad \text{for } g \in G, \; g' \in G$$

Define a mapping ψ such that

$\psi : G/K \to G'$ defined by

$$\psi(gK) = g' = \phi(g)$$

$\because \phi$ is onto for each $g' \in G'$ $\exists\, g \in G$ such that $g' = \phi(g)$

then ψ is well define

for $g, g_1 \in G \Rightarrow gK, g_1K \in G/K$

if $gK = g_1K$

$\Rightarrow K = g^{-1}g_1K$

$\Rightarrow g^{-1}g_1 \in K$

$\Rightarrow \phi(g^{-1}g_1) = e'$

$\Rightarrow \phi(g^{-1}) \cdot \phi(g_1) = e' \quad \because \phi$ is homomorphism

$\Rightarrow \phi(g) \cdot \phi(g^{-1}) \cdot \phi(g_1) = \phi(g) \cdot e'$

$\Rightarrow \phi(gg^{-1}) \cdot \phi(g_1) = \phi(g)$

$\Rightarrow \phi(e) \cdot g_1' = g'$

$\Rightarrow e' \cdot g_1' = g'$

$\Rightarrow \psi(g_1K) = \psi(gK)$

$\Rightarrow \psi$ is well define.

ii) For $g' \in G'$

$g' = \phi(g)$ and $\phi(g) = \psi(gK)$

$\Rightarrow g' = \phi(g) = \psi(gK)$

i.e every element $g' \in G'$ is an image of $gK \in G/K$

$\Rightarrow \psi$ is onto.

iii) ψ is one-one

As $\psi(gK) = \psi(g_1K)$

$\Rightarrow \phi(g) = \phi(g_1)$

$\Rightarrow \phi(g^{-1})\cdot\phi(g) = \phi(g^{-1})\cdot\phi(g_1)$

$\Rightarrow \phi(g^{-1}g) = \phi(g^{-1}g_1)$ $\because \phi$ is homomorphism.

$\Rightarrow \phi(e) = \phi(g^{-1}g_1)$

$\Rightarrow e' = \phi(g^{-1}g_1)$ where $\phi(e) = e'$

$\Rightarrow g^{-1}g_1 \in K$

$\Rightarrow g_1 \in gK$ also $g_1 \in g_1K$

$\Rightarrow gK = g_1K$

$\Rightarrow \psi$ is one-one

iv) To prove ψ is homomorphism

for $gK, g_1K \in G/K$

$\psi(gK\cdot g_1K) = \psi(gg_1K)$ | by multiplication of quotient group

$= \phi(gg_1)$

$= \phi(g)\cdot\phi(g_1)$ $\because \phi$ is homomorphism

$= \psi(gK)\cdot\psi(g_1K)$

$\Rightarrow \psi$ is homomorphism.

Hence $G/K \cong \phi(G)$ or $G/K \cong G'$

Theorem

—: Let $\varphi : G \to G'$ be epimorphism then a subgroup H' of G' is normal in G' if, and only if, inverse image $H = \varphi^{-1}(H') = \{h : h \in H,\ \varphi(h) = h',\ h' \in H'\}$ is normal in G.

Proof.

Let H' be normal subgroup of G'

and $H = \varphi^{-1}(H') = \{h : \varphi(h) = h' \in H'\}$

Let $h \in H$, $g \in G$, to prove $ghg^{-1} \in H$

$$\varphi(ghg^{-1}) = \varphi(g)\cdot\varphi(h)\cdot\varphi(g^{-1}) \quad \because \varphi \text{ is homo.}$$

$$= \varphi(g)\cdot\varphi(h)\cdot(\varphi(g))^{-1} \in H' \quad \because H' \text{ is normal}$$

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

$$\Rightarrow ghg^{-1} \in \varphi^{-1}(H') = H \quad \because \varphi \text{ is onto}$$

$\Rightarrow$ H is normal subgroup of G.

Conversely, Let H is normal subgroup of G.

For $h' \in H'$, $g' \in G'$ consider the element $g'h'g'^{-1}$

Let g' and h' are image of $g \in G$, $h \in H$

$$\Rightarrow g'h'g'^{-1} = \varphi(g)\cdot\varphi(h)\cdot\varphi(g^{-1})$$

$$= \varphi(ghg^{-1}) \quad \because \varphi \text{ is homomorphism}$$

$$\because H \trianglelefteq G \Rightarrow ghg^{-1} \in H$$

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

i.e $g'h'g'^{-1} \in H'$

$$\Rightarrow H' \trianglelefteq G'$$

2nd Isomorphism Theorem

:- Let G be a group, H a subgroup and K a normal subgroup of G then

i) $H \cap K$ is normal subgroup of H.

ii) HK is subgroup of G.

iii) $H/H\cap K \cong HK/K$

Proof.

i) To prove $H \cap K$ is a normal subgroup

Let $x \in H \cap K$

$\Rightarrow x \in H$ and $x \in K$.

$\because K$ is normal subgroup

$\therefore hxh^{-1} \in K$ for $h \in H \leq G$.

also $hxh^{-1} \in H$ $\because h, x \in H$ and H is subgroup.

$\Rightarrow hxh^{-1} \in H \cap K$

$\Rightarrow H \cap K$ is normal subgroup

ii) To prove HK is a subgroup

Let $x_1, x_2 \in HK$

then $x_1 = h_1k_1$, $x_2 = h_2k_2$ for $h_1, h_2 \in H$, $k_1, k_2 \in K$

Now
$$x_1x_2^{-1} = (h_1k_1)(h_2k_2)^{-1}$$
$$= (h_1k_1)(k_2^{-1}h_2) = h_1(k_1k_2^{-1})h_2^{-1}$$
$$= h_1k_3h_2^{-1} \quad \text{where } k_1k_2^{-1} \in K$$
$$\Rightarrow k_1k_2^{-1} = k_3 \text{ (say)}$$
$$= h_1(h_2^{-1}h_2)k_3h_2^{-1}$$
$$= (h_1h_2^{-1})(h_2k_3h_2^{-1}) \in HK$$

because $h_1h_2^{-1} \in H$ and $h_2k_3h_2^{-1} \in K$ as K is normal.

$\Rightarrow HK$ is subgroup of G.

iii) To prove $H/_{H\cap K} \cong HK/_K$

Define a mapping
$$\varphi : H \to HK/_K$$
by $\varphi(h) = hK$ ——— (i)

then φ is obviously well define and onto

Now

$$\varphi(h_1h_2) = h_1h_2K$$
$$= (h_1K)(h_2K) \quad \text{by multiplication in quotient group.}$$
$$= \varphi(h_1)\cdot\varphi(h_2)$$

i.e φ is homomorphism

$\Rightarrow$ φ is epimorphism as it is onto & homomorphism.

By Ist isomorphism theorem

$$H/_{\text{Ker}\varphi} \cong \varphi(H)$$

i.e $\quad H/_{\text{Ker}\varphi} \cong HK/_K$

1st Isomorphism Th.
$\varphi: G \to G'$ is epimorphism
then. $G/_K \cong G'$
i.e $G/_{\text{Ker}\varphi} \cong \varphi(G)$

Now to prove $\text{Ker}\varphi = H \cap K$

Let $h \in \text{Ker}\varphi$

$\Rightarrow \varphi(h) = K$ $\qquad$ K is identity of quotient group.

$\Rightarrow hK = K$ $\quad$ by (i)

$\Rightarrow h \in K$ also $h \in H$

$\Rightarrow h \in H \cap K$

$\Rightarrow \text{Ker}\varphi \subseteq H \cap K$ ——— (ii)

Now Let $x \in H \cap K$

$\Rightarrow x \in H$ and $x \in K$

$\because \varphi(x) = xK$ $\quad$ by (i)

$= K \quad \because x \in K$

$\Rightarrow \varphi(x) = K$ (identity of quotient group)

$\Rightarrow x \in \text{Ker}\,\varphi$

$\Rightarrow H \cap K \subseteq \text{Ker}\,\varphi$ ——— (iii)

From (ii) and (iii)

$$\text{Ker}\varphi = H \cap K$$

$$\because H/_{\text{Ker}\varphi} \cong HK/_K$$

$$\Rightarrow H/_{H\cap K} \cong HK/_K$$

Q.E.D.

3rd Isomorphism Theorem

:- Let H and K are two normal subgroups of G with $H \subseteq K$ then
$$(G/H)/(K/H) \cong G/K$$

Proof.

Since $H \trianglelefteq G$ and $H \subseteq K$

$\Rightarrow H \trianglelefteq K$

To see K/H is normal in G/H.

For $kH \in K/H$ and $gH \in G/H$

$$\begin{aligned}(gH)kH(gH)^{-1} &= (gH)(kH)(g^{-1}H)\\ &= (gk\,H)(g^{-1}H)\\ &= gkg^{-1}H \quad \text{by multiplication of quotient group.}\end{aligned}$$

$\because K \trianglelefteq G \therefore gkg \in K$

so $gkg^{-1}H \in K/H$

$\Rightarrow K/H \trianglelefteq G/H$

Define a mapping $\phi : G/H \to G/K$

by $\cancel{\phi(gK) =}\ \phi(gH) = gK$

then ϕ is clearly onto

Also
$$\begin{aligned}\phi(g_1H \cdot g_2H) &= \phi(g_1g_2H)\\ &= g_1g_2K\\ &= g_1K \cdot g_2K\\ &= \phi(g_1H) \cdot \phi(g_2H)\end{aligned}$$

$\Rightarrow \phi$ is homomorphism.

$\therefore \phi$ is epimorphism as it is onto and homomorphism.

by 1st isomorphism theorem

$$(G/H)/\mathrm{Ker}\,\phi \cong G/K$$

if $\phi : G \to G'$ is epimorphism then $G/\mathrm{Ker}\,\phi \cong G'$.

To prove $\ker\phi = K/H$

Let $gH \in \ker\phi$

$\Rightarrow \phi(gH) = K$ (identity of quotient group)

Also $\phi(gH) = gK$

$\Rightarrow gK = K$

$\Rightarrow g \in K$

$\Rightarrow gH \in K/H$

$\Rightarrow \ker\phi \subseteq K/H$ ——— (i)

Now let $kH \in K/H$

then $\phi(kH) = kK$

$= K$ (identity)

$\Rightarrow kH \in \ker\phi$

$\Rightarrow K/H \subseteq \ker\phi$ ——— (ii)

From (i) and (ii)

$\ker\phi = K/H$

$\because \dfrac{(G/H)}{\ker\phi} \cong G/K$

$\Rightarrow \dfrac{(G/H)}{(K/H)} \cong G/K$

proved.

———— × ———— × ————

****

****

Endomorphism:-

def:- Let G be a group and $\alpha: G \to G$ be homomorphism from G into G then α is called endomorphism of G.

The set of endomorphism of G is usually denoted as $End(G)$ or $E(G)$.

Automorphism:-

def:- Let G be a group and $\alpha: G \to G$ be homomorphism, if the mapping α is bijective then α is called automorphism.

i.e $\alpha: G \to G$ is automorphism if

i) α is homomorphism

ii) α is bijective.

The set of all automorphism of G is usually denoted by $A(G)$ or $Aut(G)$.

Remarks:

It can be easily seen that $Aut(G) \subseteq End(G)$.

Theorem:

The set $A(G)$ or $aut(G)$ of all automorphism of G is a group. (under the composition of mappings)

Proof:

i) ~~The~~ Let $\alpha, \beta \in A(G)$, then since α, β are bijective mappings, so their product (cosmposition) $\alpha\beta$ is also bijective mapping.

and for $g_1, g_2 \in G$

$$\begin{aligned} \alpha o \beta(g_1 g_2) &= \alpha(\beta(g_1 g_2)) \\ &= \alpha(\beta(g_1)\cdot\beta(g_2)) \quad \because \beta \text{ is homo.} \\ &= \alpha(\beta(g_1))\cdot\alpha(\beta(g_2)) \quad \because \alpha \text{ is homo.} \\ &= \alpha o \beta(g_1)\cdot\alpha o \beta(g_2) \end{aligned}$$

$\Rightarrow \alpha o \beta$ is homomorphism $\Rightarrow \alpha\beta \in A(G)$.

ii) Since mappings are associative in general therefore associative property holds in $A(G)$.

iii) Define $I : G \to G$ by

$$I(g) = g \quad \forall \; g \in G$$

then

$$I(g_1 g_2) = g_1 g_2 = I(g_1) \cdot I(g_2)$$

$\Rightarrow$ I is homomorphism.

Also $\alpha I(g) = \alpha \circ I(g) = \alpha(I(g)) = \alpha(g)$

i.e $\alpha I = \alpha$

Similarly $I\alpha = \alpha$

$\Rightarrow$ I is identity of $A(G)$.

iv) To prove for $\alpha \in A(G)$ $\exists$ $\alpha^{-1} \in A(G)$

$\because$ $\alpha : G \to G$ is bijective

$\therefore$ $\alpha^{-1} : G \to G$ is also bijective.

$$\begin{aligned}
\alpha^{-1}(g_1 g_2) &= \alpha^{-1}(I(g_1 g_2)) \\
&= \alpha^{-1}(I(g_1) \cdot I(g_2)) \\
&= \alpha^{-1}(\alpha\alpha^{-1}(g_1) \cdot \alpha\alpha^{-1}(g_2)) \\
&= \alpha^{-1}\alpha(\alpha^{-1}(g_1) \cdot \alpha^{-1}(g_2)) \\
&= I(\alpha^{-1}(g_1) \cdot \alpha^{-1}(g_2)) \\
&= \alpha^{-1}(g_1) \cdot \alpha^{-1}(g_2)
\end{aligned}$$

$\Rightarrow$ α^{-1} is homomorphism $\Rightarrow$ $\alpha^{-1} \in A(G)$.

i.e for each mapping in $A(G)$ there exist inverse mapping in $A(G)$.

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

Lemma: (Conjugation as an automorphism)

-: Let G be a group, $a \in G$, define a mapping $\phi_a : G \to G$ by

$$\phi_a(g) = a^{-1} g a$$

then ϕ_a is automorphism

Proof.

i) ϕ is onto.

for $g \in G$, $a \in G$ we have $a g a^{-1} \in G$

then g is image of $a g a^{-1}$ under ϕ

$$\because \phi_a(a g a^{-1}) = a^{-1}(a g a^{-1}) a$$
$$= (a^{-1} a) g (a^{-1} a)$$
$$= g$$

$\Rightarrow \phi$ is onto.

ii) ϕ is one-one

$$\because \phi_a(g_1) = \phi_a(g_2)$$
$$\Rightarrow a^{-1} g_1 a = a^{-1} g_2 a$$
$$\Rightarrow g_1 = g_2$$

iii) ϕ is homomorphism

$$\phi_a(g_1 g_2) = \phi\, a^{-1} g_1 g_2 a.$$
$$= a^{-1} g_1 (a a^{-1}) g_2 a$$
$$= (a^{-1} g_1 a)(a^{-1} g_2 a)$$
$$= \phi_a(g_1) \cdot \phi_a(g_2)$$

hence ϕ_a is automorphism

Inner and Outer automorphism

def: The set $I(G)$ or $I_{nn}(G)$ of all mapping of the type $\phi_a = aga^{-1}$ is called inner automorphism of G.

and the set which is not containing inner automorphism is called outer automorphism.

Theorem

: The set $I(G)$ of all inner automorphism of a group G is a normal subgroup of $A(G)$.

Proof

Let $\phi_a, \phi_b \in I(G)$

then $\phi_a = aga^{-1}$, $\phi_b = bgb^{-1}$

Now

$$\phi_b \cdot \phi_{b^{-1}}(g) = \phi_b(b^{-1}g(b^{-1})^{-1})$$
$$= \phi_b(b^{-1}gb)$$
$$= b(b^{-1}gb)b^{-1}$$
$$= (bb^{-1})g(bb^{-1})$$
$$= ege^{-1}$$
$$= \phi_e$$

$$\Rightarrow \phi_{b^{-1}} = (\phi_b)^{-1}$$

Now let $x = \phi_a$, $y = \phi_b$

$$xy^{-1} = \phi_a(\phi_b)^{-1}(g)$$
$$= \phi_a\phi_{b^{-1}}(g) = \phi_a(b^{-1}gb)$$
$$= a(b^{-1}gb)a^{-1}$$
$$= (ab^{-1})g(ba^{-1})$$
$$= (ab^{-1})g(ab^{-1})^{-1}$$
$$= \phi_{ab^{-1}} \in I(G)$$

$\Rightarrow I(G)$ is a subgroup.

Let $\phi_a \in I(G)$, $\alpha \in A(G)$

Now

$$\alpha \phi_a \alpha^{-1}(g) = \alpha \phi_a(\alpha^{-1}(g))$$
$$= \alpha \{ a\, (\alpha^{-1}(g))\, a^{-1} \}$$
$$= \alpha(a) \cdot \alpha(\alpha^{-1}(g)) \cdot \alpha(a^{-1}) \quad \because \alpha \text{ is homo.}$$
$$= \alpha(a) \cdot g \cdot (\alpha(a))^{-1} \quad \because \alpha \text{ is bijective}$$
$$= \phi_{\alpha(a)} \in I(G)$$

i.e $\alpha \phi_a \alpha^{-1} \in I(G)$

Hence $I(G) \trianglelefteq A(G)$

Theorem

:- Let G be a group with $C(G)$ as its centre and $I(G)$ the group of inner automorphism then $G/C(G)$ is isomorphic to $I(G)$.

Proof:

Consider a mapping $\psi : G \to I(G)$ defined by

$$\psi(a) = \phi_a \quad \text{where } a \in G,\ \phi_a \in I(G)$$

i) then ψ is well defined

$$\text{if } a = b \Rightarrow a^{-1} = b^{-1}$$
$$\Rightarrow ag = bg$$
$$\Rightarrow aga^{-1} = bgb^{-1}$$
$$\Rightarrow \phi_a = \phi_b$$
$$\Rightarrow \psi(a) = \psi(b)$$

ii) ψ is clearly onto as every $\phi_a \in I(G)$ is an image of $a \in G$.

iii) ψ is homomorphism as

$$\psi(ab) = \phi_{ab}$$
$$= (ab)g(ab)^{-1}$$
$$= (ab)g(b^{-1}a^{-1})$$
$$= a(bgb^{-1})a^{-1}$$
$$= a(\phi_b)a^{-1}$$
$$= \phi_a(\phi_b) = \phi_a \circ \phi_b \quad (\text{composite fn.})$$
$$\cancel{= \phi(a)\,\psi(b)} = \phi_a \cdot \phi_b$$
$$= \psi(a).\psi(b)$$

$\Rightarrow \psi$ is epimorphism as it is homomorphism and onto.

Now By first isomorphism theorem

$$G/\ker\phi \cong I(G)$$

$\because$ if $\psi : G \to G'$ is epimorphism then $G/\ker\phi \cong G'$

To prove $\ker \psi = C(G)$.

Let $\ker\psi = \{a : a \in G \wedge \psi(a) = \phi_e\}$

$= \{a : a \in G \wedge \phi_a = \phi_e\}$

$= \{a : a \in G \wedge aga^{-1} = ege^{-1}\}$

$= \{a : a \in G \wedge aga^{-1} = g\}$

$= \{a : a \in G \wedge ag = ga\}$

$= C(G)$

$\Rightarrow G/C(G) \cong I(G)$

Theorem.

$\because$ $\phi : G \to G$ by $\phi(x) = x^{-1}$ then ϕ is automorphism iff G is abelian.

Proof.

Let G be abelian

$$\phi(g_1 g_2) = (g_1 g_2)^{-1}$$
$$= g_2^{-1} g_1^{-1}$$
$$= g_1^{-1} g_2^{-1} \quad \because G \text{ is abelian}$$
$$= \phi(g_1)\cdot\phi(g_2)$$

$\Rightarrow$ ϕ is homomorphism

ϕ is onto because each $g \in G$ we have:

$$\phi(g^{-1}) = (g^{-1})^{-1} = g$$

ϕ is one-one

$$\phi(g_1) = \phi(g_2)$$
$$\Rightarrow g_1^{-1} = g_2^{-1} \Rightarrow g_1 = g_2$$

$\Rightarrow$ ϕ is automorphism.

Conversely, let ϕ is automorphism

i.e ϕ is homomorphism

$$\phi(g_1 g_2) = \phi(g_1)\cdot\phi(g_2)$$
$$\Rightarrow (g_1 g_2)^{-1} = g_1^{-1} \cdot g_2^{-1}$$
$$\Rightarrow g_2^{-1} g_1^{-1} = g_1^{-1} \cdot g_2^{-1}$$
$$\Rightarrow g_1 g_2 = g_2 g_1$$

$\Rightarrow$ G is abelian

Commutator of a group

def:- Let G be a group and $a, b \in G$ then the element $x = aba^{-1}b^{-1}$ is called ~~com~~ commutator of G and we write $[a, b] = aba^{-1}b^{-1}$.

Theorem:

–: The following commutator results hold in G. For $a, b \in G$

i) $[b, a] = [a, b]^{-1}$

ii) $[ab, c] = [b, c]^{a}[a, c]$
$= a[b, c]a^{-1}.[a, c]$

$[b, c]^{a} = a[b, c]a^{-1}$

iii) $[a, bc] = [a, b][a, c]^{b}$

iv) $[a, b^{-1}] = [b, a]^{b^{-1}}$, $[a^{-1}, b] = [b, a]^{a^{-1}}$

Proof

$$\begin{aligned}[a, b][b, a] &= (aba^{-1}b^{-1})(bab^{-1}a^{-1})\\ &= aba^{-1}(b^{-1}b)ab^{-1}a^{-1}\\ &= ab(a^{-1}a)b^{-1}a^{-1}\\ &= a(bb^{-1})a^{-1}\\ &= aa^{-1} = e\end{aligned}$$

i.e $[b, a]$ is inverse of $[a, b]$

$\Rightarrow [a, b]^{-1} = [b, a]$

ii) $$\begin{aligned}[ab, c] &= (ab)c(ab)^{-1}c^{-1}\\ &= abcb^{-1}a^{-1}c^{-1}\\ &= abcb^{-1}c^{-1}ca^{-1}c^{-1}\\ &= abcb^{-1}c^{-1}a^{-1}aca^{-1}c^{-1}\\ &= a(bcb^{-1}c^{-1})a^{-1}(aca^{-1}c^{-1})\\ &= [b, c]^{a}[a, c]\end{aligned}$$

proved

iii) $$\begin{aligned}[a, bc] &= a(bc)a^{-1}(bc)^{-1}\\ &= abca^{-1}c^{-1}b^{-1}\\ &= aba^{-1}aca^{-1}c^{-1}b^{-1}\\ &= aba^{-1}b^{-1}baca^{-1}c^{-1}b^{-1}\end{aligned}$$

$$= (aba^{-1}b^{-1})\, b(aca^{-1}c^{-1})\, b^{-1}$$
$$= [a,b][a,c]^b \quad \text{proved.}$$

(iv) $[a, b^{-1}] = ab^{-1}a^{-1}(b^{-1})^{-1}$
$$= ab^{-1}a^{-1}b$$
$$= b^{-1}b\,ab^{-1}a^{-1}b$$
$$= b^{-1}(bab^{-1}a^{-1})\,b$$
$$= b^{-1}(bab^{-1}a^{-1})(b^{-1})^{-1}$$
$$= [b,a]^{b^{-1}} \quad \text{proved}$$

And

$[a^{-1}, b] = a^{-1}b(a^{-1})^{-1}b^{-1}$
$$= a^{-1}bab^{-1}$$
$$= a^{-1}bab^{-1}a^{-1}a$$
$$= a^{-1}(bab^{-1}a^{-1})\,a$$
$$= a^{-1}(bab^{-1}a^{-1})(a^{-1})^{-1}$$
$$= [b,a]^{a^{-1}} \quad \text{proved}$$

Derive Group or Commutative subgroup.

def: Let G be a group and G' be a subgroup of G. If G' is generated by a set of commutators then G' is called derived group

$$G' = \{x_1, x_2, \dots, x_n\}$$

Note: Product of two commutators may not be a commutator.

Theorem:-

Let G be a group then

i) the derived group G' is a normal subgroup of G.

ii) The quotient group G/G' is abelian.

iii) If K is normal subgroup of G such that G/K is abelian then $G' \subseteq K$.

Proof:

To prove $G' \trianglelefteq G$, Let for $g \in G$

$$g[a,b]g^{-1} = g(aba^{-1}b^{-1})g^{-1}$$

$= gaba^{-1}b^{-1}g^{-1}$

$= gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1}$

$= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1})$

$= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$

$= a^g b^g (a^g)^{-1}(b^g)^{-1} = [a^g, b^g] \in G'$

$\Rightarrow G'$ is normal subgroup of G.

ii) Let $aG', bG' \in G/G'$ where $a, b \in G$

then

$[aG', bG'] = (aG')(bG')(aG')^{-1}(bG')^{-1}$

$= (aG')(bG')(a^{-1}G')(b^{-1}G')$

$= (aba^{-1}b^{-1})G'$ by multiplication of quotient group

$= [a,b]G'$

$= G'$ $\because [a,b] \in G'$

$=$ Identity of Quotient group

$\Rightarrow G/G'$ is abelian

if $[a,b] = e$
$\Rightarrow aba^{-1}b^{-1} = e$
$\Rightarrow ab = ba$

iii)

Since $aK \cdot bK(aK)^{-1}(bK)^{-1} = K$ $\because G/K$ is abelian.

$\Rightarrow aK \cdot bK \cdot a^{-1}K \cdot b^{-1}K = K$

$\Rightarrow (aba^{-1}b^{-1})K = K$

$\Rightarrow [a,b]K = K$

$\Rightarrow [a,b] \in K$

$\because$ if $aH = H$
$\Rightarrow a \in H$

$\Rightarrow G' \subseteq K$.

****

Check out notes of other subjects at *http://www.MathCity.org*

****

Direct Product of Groups

def:- Let H and K are two subgroups of a group G we define the direct product of these two groups by

$$H \times K = \{(h, k) : h \in H \wedge k \in K\}$$

under multiplication

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

Note: Under multiplication $H \times K$ is a group with identity (e, e') where e is identity of H and e' is identity of K. And inverse of (h, k) is (h^{-1}, k^{-1}).

Theorem

-: Let a group G be a direct product of its two normal subgroups H with $H \cap K = \{e\}$, $G = HK$ then

i) Every element of H is permutable (commute) with every element of K.

ii) Every element of G is uniquely expressible as $g = hk$

iii) $G \cong H \times K$ i.e $HK \cong H \times K$.

Proof:

Consider an element $hkh^{-1}k^{-1}$

then $kh^{-1}k^{-1} \in H$ $\because H \trianglelefteq G$

$\Rightarrow h(kh^{-1}k^{-1}) \in H$ $\because h \in H$.

also $hkh^{-1} \in K$ $\because K \trianglelefteq G$

$\Rightarrow (hkh^{-1})k^{-1} \in K$ $\because k^{-1} \in K$

i.e $hkh^{-1}k^{-1} \in H \cap K = \{e\}$ (given)

$\Rightarrow hkh^{-1}k^{-1} = e$

$\Rightarrow hk = kh$

$\Rightarrow$ every element of H is permutable with every element of K.

ii) Let if possible, g has two expressions

$g = h_1 k_1$ & $g = h_2 k_2$

for $h_1, h_2 \in H$, $k_1, k_2 \in K$

$h_1 \neq h_2$, $k_1 \neq k_2$

$\Rightarrow h_1 k_1 = h_2 k_2$

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

$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$

$\Rightarrow h_2^{-1} h_1 = e$ & $k_2 k_1^{-1} = e$

$\Rightarrow h_1 = h_2$ & $k_1 = k_2$

which is a contradiction

hence $g = h_1 k_1$ is a unique representation.

iii) To prove $G \cong H \times K$

Define a mapping $\phi : G \to \cancel{G \times H}\ H \times K$

by $\phi(g) = (h, k)$

a) The mapping is well define as

for $g_1 = g_2$

$\Rightarrow h_1 k_1 = h_2 k_2$ $\because G = HK$

$\Rightarrow h_1 = h_2$, $k_1 = k_2$

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

$\Rightarrow \phi(g_1) = \phi(g_2)$.

b) ϕ is onto as

$(h, k) \in H \times K$ is image of $g = hk \in HK = G$

$\because (h, k) \in H \times K$

$\Rightarrow h \in H$, $k \in K$ $\Rightarrow hk \in HK$.

c) ϕ is one-one

$\phi(g_1) = \phi(g_2)$

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

$\Rightarrow h_1 = h_2 \;,\; k_1 = k_2$

$\Rightarrow h_1 k_1 = h_2 k_2$

$\Rightarrow g_1 = g_2 \qquad \because g = hk$

d) ϕ is homomorphism

$$\phi(g_1 \cdot g_2) = \phi(h_1 k_1 \cdot h_2 k_2)$$
$$= \phi(h_1 (k_1 h_2) k_2)$$
$$= \phi(h_1 (h_2 k_1) k_2) \qquad \text{by (i)}$$
$$= \phi(h_1 h_2 \cdot k_1 k_2)$$
$$= (h_1 h_2 \,,\, k_1 k_2)$$
$$= (h_1 , k_1) \cdot (h_2 , k_2)$$
$$= \phi(h_1 k_1) \cdot \phi(h_2 k_2)$$
$$= \phi(g_1) \cdot \phi(g_2)$$

i.e ϕ is homomorphism.

and hence ϕ is isomorphism as it is also one-one and onto.

$\Rightarrow G \cong H \times K$ or $HK \cong H \times K$.

Note: G is abelian group if $H = \{e\}$ is derived group.

Lemma

Let G be a direct product of two subgroup H and K and $H_1 \trianglelefteq H$ then prove that $H_1 \trianglelefteq G$.

Proof

Let $h_1 \in H_1$ and $g \in G$

then $g = hk$ for $h \in H$, $k \in K$

Now

$$
\begin{aligned}
g h_1 g^{-1} &= (hk) h_1 (hk)^{-1} \\
&= (hk) h_1 (k^{-1} h^{-1}) \\
&= h (k h_1)(k^{-1} h^{-1}) && \because h_1 \in H_1 \subseteq H \\
&= h (h_1 k)(k^{-1} h^{-1}) && \text{\& } H \text{ and } K \text{ commute element wise.} \\
&= h h_1 (k k^{-1}) h^{-1} \\
&= h h_1 h^{-1} \in H_1 && \because H \trianglelefteq H_1
\end{aligned}
$$

$\Rightarrow g h_1 g^{-1} \in H_1$

$\Rightarrow H_1 \trianglelefteq G$ proved.

Theorem

If $G = H \times K$ then show that
$$C(G) = C(H) \times C(K)$$
where $C(G)$, $C(H)$ and $C(K)$ denotes centre of G, H and K respectively.

Proof.

To prove $C(H) \times C(K) \subseteq C(G)$

Let $x \in C(H) \times C(K)$

then $x = z_1 z_2$ where $z_1 \in C(H)$, $z_2 \in C(K)$

Let $g = hk$ for $h \in H$, $k \in K$, $g \in G$

then

$$
\begin{aligned}
gx &= (hk)(z_1 z_2) \\
&= h (k z_1) z_2 \\
&= h (z_1 k) z_2
\end{aligned}
$$

$= (hz_1)(kz_2)$

$= (z_1 h)(z_2 k)$

$= z_1 (h z_2) k$

$= (z_1 z_2)(hk)$

$= xg$

$\Rightarrow x \in C(G)$

Hence

$C(H) \times C(K) \subseteq C(G)$ ——— (i)

Now to prove $C(G) \subseteq C(H) \times C(K)$

Let $z \in C(G)$

$\Rightarrow gz = zg$ for $g \in G$.

in particular

$zh = hz \; , \quad zk = kz$ $\quad \Big| \because h \in H \leq G, \; k \in K \leq G$

Let $z = h'k'$ for $h' \in H$, $k' \in K$

so $zh = (h'k')h = h'(k'h) = h'hk'$

and $hz = hh'k'$

$\because hz = zh$

$\Rightarrow hh'k' = h'hk'$

$\Rightarrow hh' = h'h \Rightarrow h' \in C(H)$

Similarly $k' \in C(K)$

Hence $h'k' \in C(H) \times C(K)$

$\Rightarrow z \in C(H) \times C(K) \quad \because z = h'k'$

$\Rightarrow C(G) \subseteq C(H) \times C(K)$ ——— (ii)

from (i) and (ii)

$C(G) = C(H) \times C(K)$ proved.

Theorem

:- If $G = H \times K$, then the factor group G/K is isomorphic to H.

Proof.

$G/K = \{gK = hkK = hK \ , \ h \in H\}$ $\quad \because g = hk$

Define a mapping

$\phi : G/K \to H$ by $\phi(gK) = \phi(hK) = h$

then ϕ is well define as

$$g_1 K = g_2 K$$
$$\Rightarrow h_1 K = h_2 K$$
$$\Rightarrow h_2^{-1} h_1 K = K$$
$$\Rightarrow h_2^{-1} h_1 \in K \quad \text{but also } h_2^{-1} h_1 \in H$$
$$\Rightarrow h_2^{-1} h_1 \in H \cap K = \{e\}$$
$$\Rightarrow h_2^{-1} h_1 = e \Rightarrow h_1 = h_2$$
$$\Rightarrow \phi(h_1 K) = \phi(h_2 K)$$

ϕ is onto and one-one as

For $h \in H$ there is a coset $hK \in G/K$ i.e $\phi(hK) = h$

and $\phi(h_1 K) = \phi(h_2 K)$

$$\Rightarrow h_1 = h_2$$
$$\Rightarrow h_1 K = h_2 K$$

Now

$$\begin{aligned}\phi(g_1 K \cdot g_2 K) &= \phi(h_1 K \cdot h_2 K) \\ &= \phi(h_1 h_2 K) \\ &= h_1 h_2 \\ &= \phi(h_1 K) \cdot \phi(h_2 K) \\ &= \phi(g_1 K) \cdot \phi(g_2 K)\end{aligned}$$

$\Rightarrow \phi$ is homomorphism

therefore $G/K \cong H$ proved

Lemma:

H and K are cyclic groups of order m and n respectively, where m and n are relatively prime then H×K is a cyclic group.

Proof:

$$H = \langle a : a^m = e \rangle$$

$$K = \langle b : b^m = e \rangle$$

and element of H×K is of the form (a, b)

for $(a, b)^k = (a^k, b^k) = (e, e)$ iff $m \mid k$, $n \mid k$.

As m, n are relatively prime

$\Rightarrow mn \mid k$

As no. of element in H×K is mn

also

$$(a, b)^{mn} = (a^{mn}, b^{mn})$$

$$= ((a^m)^n, (b^n)^m) = (e, e)$$

i.e $H \times K = \langle (a, b) : (a, b)^{mn} = e \rangle$

$\Rightarrow$ H×K is cyclic group of order mn.

Invariant Subgroup

def:- Let G be a group and $\phi : G \to G$ is endomorphism then an element $\phi(g) = g$ is called invarient element.

A subgroup H of G is fully invarient if under all endomorphism $\phi(h) \in H$ or $\phi(H) \subseteq H$.

Example:

Commutator subgroup G' is fully invarient

Let $[x, y] \in G'$

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

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

$$= \phi(x) \cdot \phi(y) \cdot (\phi(x))^{-1} (\phi(y))^{-1} = [\phi(x), \phi(y)] \in G'$$

$\Rightarrow G'$ is fully invarient.

Characteristic Subgroup:

A subgroup H of G is characteristic subgroup if it remain fully invarient under all automorphism.
i.e for all $h \in H$, for all $\phi \in Aut(G)$

$$\phi(h) \in H \quad \text{or} \quad \phi(H) = H.$$

Question

-: Centre of G is characteristic subgroup of G.

Solution

Let $x \in C(G)$

$\Rightarrow \; gx = xg \quad \forall \; g \in G$

Let $\phi : G \to G$ be an automorphism

$\phi(gx) = \phi(xg)$

$\Rightarrow \; \phi(g)\phi(x) = \phi(x)\phi(g)$

As $g \in G \;\Rightarrow\; \phi(g) \in G$

so $\phi(x) \in C(G)$

$\Rightarrow \; C(G)$ is characteristic.

Question

-: Every characteristic subgroup is normal.

Solution:

Let H is a characteristic subgroup of G,

then $\phi(H) = H \quad \forall \; \phi \in aut(G)$

In particular

$\phi_g(H) = H \quad \because \phi_g$ is an inner automorphism.

$\Rightarrow \; gHg^{-1} = H$

$\Rightarrow \; H$ is normal subgroup of G.

****

={ The End }=

****