

Groups: Handwritten notes

by

Atiq ur Rehman

<http://www.MathCity.org/atiq>

PARTIAL CONTENTS

1. Groups; definition and examples **1**
2. Order of group, order of element **3**
3. Periodic group, mixed group **4**
4. Subgroup **6**
5. Invalution **8**
6. Relation between groups, homomorphism, monomorphism, epimorphism, isomorphism, endomorphism, examples and related theorem **9**
7. Kernel, definition and related theorems **13**
8. Cyclic group, related theorems **18**
9. Complex in a group, product of complexes and related theorems **24**
10. Coset, definition and examples **30**
11. Index of subgroup, Lagrange's theorem **31**
12. Double coset, related theorem **33**
13. Normalizer, definition and related theorems **34**
14. Centralizer, centre of group, related theorem **36**
15. Conjugate or transform of a group, definition and related theorems **37**

16. Self conjugate, conjugacy class, related theorem **40**
17. Class equation, p-group, definition and related theorems **43**
18. Conjugate subgroup, definition and related theorems **45**
19. Normal subgroup, definition and related theorems **49**
20. Factor or quotient group, definition and related theorem **53**
21. 1st isomorphism theorem, related theorem **55**
22. 2nd isomorphism theorem **58**
23. 3rd isomorphism theorem **60**
24. Endomorphism, automorphism, definition and related theorem **62**
25. Conjugation as an automorphism **64**
26. Inner and outer automorphism, definition and related theorems **65**
27. Commutator of a group, definition and related theorem **70**
28. Derive group or commutative group, definition and related theorem **71**
29. Direct product of groups, definition and related theorems **73**
30. Invariant subgroup **79**
31. Characteristic subgroup **80**

Available at ***<http://www.MathCity.org/msc>***

If you have any question, ask at *<http://forum.mathcity.org>*

MathCity.org is a non-profit organization, working to promote mathematics in Pakistan. If you have anything (notes, model paper, old paper etc.) to share with other peoples, you can send us to publish on MathCity.org. You may earn money by participating. For more information visit: *<http://www.MathCity.org/participate.html>*

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.

$$A = \{I, \pm i, \pm j, \pm k\} \text{ with the condition}$$

$$i \cdot i = j \cdot j = k \cdot k = I$$

$$i \cdot j = j \cdot k = i, \quad j \cdot k = i, \quad k \cdot i = j$$

$$j \cdot i = -k, \quad k \cdot j = -i, \quad i \cdot k = -j$$

$$\& \quad Ix = x \quad \forall \quad x \in A$$

then A is called group.

Question:-

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

Solution:-

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

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 $\mathbb{Z}_n$.

i.e binary operation $\oplus$ is defined

- ii) $\oplus$ is associative in general.
- iii) $0 \in \mathbb{Z}_n$ is an identity element.
- iv) For $a \in \mathbb{Z}_n$, $n-a$ is inverse of a .

$$\therefore a + (n-a) = n = 0 \quad \left| \begin{array}{l} n \div n \Rightarrow \text{Remainder } 0 \end{array} \right.$$

Hence $\mathbb{Z}_n$ 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 12:16 PM

Available online at <http://www.MathCity.org>

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

$$a^p = a^q \quad \text{for some } p < n, q < n, p \neq q.$$

then

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

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

$$\Rightarrow p < q$$

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

hence $a^p \neq a^q$

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

Available online at <http://www.MathCity.org>

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

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

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

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

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

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

which is only possible if $r = 0$

$$\text{then } k = nq \Rightarrow n/k.$$

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.

$$\mathbb{R}' = \mathbb{R} - \{0\}$$

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 .

Available online at <http://www.MathCity.org>

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 $ab^{-1} \in F$.

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

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 .

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

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 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 $H_1 \cup H_2 = H_1$

$\therefore H_1$ & 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 $b \notin H_1$

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

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 contradiction

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

Available online at <http://www.MathCity.org>

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

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

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

then G contains invalution.

if $B \neq \emptyset$, 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.

$\therefore e \in A \Rightarrow A \neq \emptyset$

$\Rightarrow |A| \geq 2$

$\therefore$ order of A is even,

so it contain min. 2 elements

Since $A \subseteq G$

$\Rightarrow G$ contains an invalution

Available online at <http://www.MathCity.org>

* Relation between Groups:-

• Homomorphism

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

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)

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

✓ • Epimorphism

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

Example

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

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

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

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

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.

- $\phi: \mathbb{R}^+ \rightarrow \mathbb{R}$ 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 $f: G \rightarrow G'$ is isomorphic then $f^{-1}: G' \rightarrow G$ is also isomorphic.

Solution:-

Since $f: G \rightarrow G'$ is bijective

so $f^{-1}: G' \rightarrow G$ 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 $f(y) = b$

$$\text{or } x = f^{-1}(a) \text{ \& } y = f^{-1}(b)$$

$\therefore f$ is homomorphism

$$\therefore f(xy) = f(x) \cdot f(y)$$

as $f(xy) = ab \Rightarrow xy = f^{-1}(ab) \therefore f$ is bijective and

$$\begin{aligned} f^{-1}(a) \cdot f^{-1}(b) &= x \cdot y \\ &= f^{-1}(ab) \end{aligned}$$

Hence f^{-1} is homomorphism

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

Question:-

Let G, G', G'' be groups

and $f: G \rightarrow G', g: G' \rightarrow G''$ are isomorphism

then $g \circ f: G \rightarrow G''$ is also isomorphism.

Solution:-

Since composition of two bijective mapping is bijective so $g \circ f$ is bijective

$$\text{and } g \circ f(xy) = g(f(xy))$$

$$= g(f(x) \cdot f(y)) \therefore f \text{ is isomorphism}$$

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

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

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

Theorem:-

Prove that isomorphic groups form an equivalence relation.

Proof:-

i) Reflexive

Define $I: G \rightarrow G$ 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 $f: G \rightarrow G'$ an isomorphism

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

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

~~as $f(xy) = f(x) \cdot f(y)$~~ ~~so~~ ~~to~~ prove f^{-1} is homomorphism
as in previous Question.

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

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

prove $g \circ f$ is isomorphism

as in previous Question

Available online at <http://www.MathCity.org>

Definition (Kernel):

def - Let $\phi: G \rightarrow G'$ be a homomorphism
then kernel of ϕ is defined by

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

where e' is identity of G' .

Lemma:

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

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

Proof:

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

Since e' is identity of G'

$$\Rightarrow \phi(x) \cdot e' = \phi(x)$$

$$= \phi(x \cdot e) \quad \because x = x \cdot e$$

$$= \phi(x) \cdot \phi(e)$$

$$\text{i.e. } \phi(x) \cdot e' = \phi(x) \cdot \phi(e)$$

$$\Rightarrow e' = \phi(e) \quad \text{by cancellation law.}$$

$$\begin{aligned} \text{ii) } \phi(x) \cdot \phi(x^{-1}) &= \phi(x x^{-1}) \quad \because \phi \text{ is homomorphism} \\ &= \phi(e) \\ &= e' \end{aligned}$$

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

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

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

Available online at <http://www.MathCity.org>

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

~~$\therefore \phi(g_1 g_2) \in \phi(G)$~~

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

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

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

$\Rightarrow \phi(G)$ 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 $x \in G, x^{-1} \in G$

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

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

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

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

Theorem:

Let $\phi: G \rightarrow H$ be homomorphism of a group G into group H , then for $a, b \in G$
 $\phi(a) = \phi(b)$ iff $ab^{-1} \in \ker \phi$.

Proof:

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

$$\begin{aligned} \text{Now } \phi(ab^{-1}) &= \phi(a) \cdot \phi(b^{-1}) \\ &= \phi(b) \cdot \phi(b^{-1}) \quad \because \phi(a) = \phi(b) \\ &= \phi(bb^{-1}) \\ &= \phi(e) = e' \in H \end{aligned}$$

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

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

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

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

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

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

proved

Theorem

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

Proof:

Suppose ϕ is one-one.

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

and let $a \in \ker \phi$

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

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

and $\because \phi$ is one-one

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

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

$$\begin{array}{l} \because \phi(I_G) = I_H \\ \Rightarrow I_G \in \ker \phi \\ \text{i.e. } \{I_G\} \subseteq \ker \phi \end{array}$$

Conversely, let $\ker \phi = \{I_G\}$
to prove ϕ is one-one

$$\text{Let } \phi(a) = \phi(b)$$

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

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

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

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

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

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

$$\Rightarrow a = b$$

$$\Rightarrow \phi \text{ is one-one}$$

Available online at <http://www.MathCity.org>

Theorem.

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

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

then relation $\sim$ is equivalence relation.

Proof:

i) Reflexive

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

$$\Rightarrow x \sim x$$

i.e. this relation is reflexive.

ii) Symmetric

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

$$\Rightarrow (x\bar{y}^{-1})^{-1} \in H \quad \because H \text{ is group.}$$

$$\begin{aligned} \therefore (x\bar{y}^{-1})^{-1} &= (\bar{y}^{-1})^{-1} \cdot x^{-1} \\ &= y \cdot x^{-1} \end{aligned}$$

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

$\therefore \sim$ is symmetric.

iii) Transitive

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

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

$$\text{Now } (x\bar{y}^{-1})(y\bar{z}^{-1}) \in H$$

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

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

$$\text{or } x\bar{z}^{-1} \in H$$

$$\Rightarrow x \sim z \quad \text{i.e. } \sim \text{ is transitive.}$$

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

$$G = \{a, a^2, a^3, \dots, a^{n-1}, a^n = e\}$$

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

e.g

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

$$\text{let } a = i, \quad a^2 = i^2 = -1$$

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

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

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

Available online at <http://www.MathCity.org>

Theorem

Any two cyclic group of same order are isomorphic.

Proof:-

(i) For finite order:-

Let G be a cyclic group of order n ,
i.e. $G = \langle a : a^n = e \rangle$

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

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

• ϕ is one-one

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

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

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

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

Thus ϕ is one-one

• ϕ is obviously onto

$\therefore$ for every $e^{\frac{2k\pi}{n}i}$, where $k = 0, 1, 2, \dots, n-1$
 $\exists a^k \in G \forall k$.

$$\bullet \text{ Now } \phi(a^k a^m) = \phi(a^{k+m})$$

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

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

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

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

(ii) For Infinite Order:-

For infinite cyclic group we define a mapping $\phi: G \rightarrow \mathbb{Z}$ by $\phi(a^k) = k$.

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

then ϕ is one-one

$$\because \phi(a^k) = \phi(a^m) \quad \text{for } a^k, a^m \in G$$

$$\Rightarrow k = m$$

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

and also for each $k \in \mathbb{Z}$ $\exists$ 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

$$G \cong \mathbb{Z}$$

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

$$\therefore a^{kd} = a^{cd} = e$$

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 +ve integer such that $a^k \in H$.

we prove that H is generated by a^k .

for this let $x = a^m \in H \quad \forall m > k$

then $\exists$ integers q and r such that

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

$$\begin{aligned} \text{then } a^m &= a^{qk+r} \\ &= a^{qk} \cdot a^r \end{aligned}$$

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

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

$\therefore a^m$ 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 $\varphi(G)$ is cyclic.

Take $b = \varphi(a)$

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

$$x = \varphi(a^k)$$

$$= \varphi(\underbrace{a \cdot a \cdot a \cdots a}_{(k \text{ times})})$$

$$= \varphi(a) \cdot \varphi(a) \cdot \varphi(a) \cdots \varphi(a) \quad \because \varphi \text{ is homo.}$$

$$= \underbrace{b \cdot b \cdot b \cdots b}_{(k \text{ times})}$$

$$= b^k$$

So $\varphi(G)$ is generated by b .
hence $\varphi(G)$ is cyclic.

Available online at <http://www.MathCity.org>

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 $H = G$

$$\begin{aligned} a^1 &= a^{pk+qn} \\ &= (a^k)^p \cdot (a^n)^q \\ &= (a^k)^p \cdot (e)^q \quad \because a^n = e \\ &= (a^k)^p \end{aligned}$$

$\therefore (a^k)^p$ 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 ,

$$(a^k)^p = a \Rightarrow a^{pk} = a$$

$$\Rightarrow a^{pk-1} = e$$

$$\Rightarrow n \mid pk-1 \quad \because n \text{ is least such integer, that } a^n = e$$

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

$$\Rightarrow kp-1 \neq 0 \quad \text{or} \quad kp-1 = 0$$

if $kp-1 \neq 0$

then G is finite, a contradiction

$$\text{hence } kp-1=0 \Rightarrow kp=1$$

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

$$XY = \{xy : x \in X, y \in Y\}$$

Available online at <http://www.MathCity.org>

imp ✓
Theorem

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

Proof.

Let HK be a subgroup

Let $h_1 k_1 \in HK$ for $h_1 \in H, k_1 \in K$

$\Rightarrow (h_1 k_1)^{-1} \in HK \quad \therefore HK$ is subgroup.

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

i.e. $HK \subseteq KH \quad \text{--- (i)}$

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.

$\Rightarrow KH \subseteq HK \quad \text{--- (ii)}$

from (i) and (ii)

$$HK = KH.$$

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

Let $h_1 k_1, h_2 k_2 \in HK$

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

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

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

$$= h_1 (k_3 h_2^{-1}) \quad \text{for } k_1, k_2 \in K$$

$$k_3 = k_1 k_2^{-1} \in K$$

$$= h_1 (h_2^{-1} k_3) \quad \therefore KH = HK$$

$$= (h_1 h_2^{-1}) k_3 \quad \text{for } h_1, h_2 \in H, h_3 = h_1 h_2^{-1} \in H$$

$$= h_3 k_3 \in HK.$$

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:-

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

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

$$h_1 k_1 = h_2 k_2$$

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

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

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

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

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

$$\text{i.e. } g \in H \text{ and } g \in K$$

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

$$\Rightarrow g = e$$

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

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

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

which is a contradiction.

$$\text{hence } |O(HK)| = |O(H)| \cdot |O(K)|$$

OR

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

Example.

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

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

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

then

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

Question.

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

$$\text{where } g^3 = e, f^3 = e, (fg)^2 = e$$

prove that G is group.

Available online at <http://www.MathCity.org>

Theorem:-

$\therefore$ 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 $HK = \{hk : h \in H, k \in K\}$
 $= \{x_1, x_2, x_3, \dots, x_m\}$ (say)

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

so let $H \cap K = \{\gamma_1, \gamma_2, \gamma_3, \dots, \gamma_r\}$

$\therefore$ each $\gamma_i \in H \cap K \quad \forall i = 1, 2, \dots, r$

and $H \cap K$ is a subgroup.

$\therefore \gamma_i^{-1} \in H \cap K \quad \forall i = 1, 2, \dots, r$

so $\gamma_i, \gamma_i^{-1} \in H$ and $\gamma_i, \gamma_i^{-1} \in K$.

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

$\Rightarrow h\gamma_i \in H, \gamma_i^{-1}k \in K$

$\Rightarrow (h\gamma_i)(\gamma_i^{-1}k) \in HK$

but $(h\gamma_1)(\gamma_1^{-1}k) = (h\gamma_2)(\gamma_2^{-1}k) = (h\gamma_3)(\gamma_3^{-1}k) = \dots$

$\dots = (h\gamma_r)(\gamma_r^{-1}k) = hk = x$

i.e. x is repeated r times in HK .

so total number of elements possible in HK is rm .

i.e. $rm = pq$

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

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

proved

Corollary:-

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

Proof.

$$\because |H| \geq \sqrt{|G|}, |K| \geq \sqrt{|G|}$$

as H and K are subgroup of G

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

$$\Rightarrow HK \subseteq G$$

$$\Rightarrow |HK| < |G|$$

$$\text{i.e. } |G| > |HK|$$

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

$$\geq \frac{\sqrt{|G|} \cdot \sqrt{|G|}}{|H \cap K|}$$

$$= \frac{|G|}{|H \cap K|}$$

$$\Rightarrow |H \cap K| > 1$$

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

Available online at <http://www.MathCity.org>

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

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

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

$$(fg)^2 = e$$

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

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

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

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

$$\Rightarrow fg = g^2f$$

So

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

$$\begin{aligned} Hfg &= \{fg, g(fg), g^2(fg)\} = \{fg, g(g^2f), g^2(g^2f)\} \\ &= \{fg, f, gf\} \end{aligned}$$

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

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

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

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

Let $a_i \in G$

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

so, $G \subseteq \bigcup_{i=1}^k a_iH$ — (i)

Also each a_iH is a subset of G

∴ $\bigcup_{i=1}^k a_iH \subseteq G$ — (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 $h_1, h_2 \in H$.

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

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

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 $x \notin aH \cap bH$

$$\Rightarrow aH \cap bH = \emptyset$$

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

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

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

$$\varphi(h) = a_i h, \quad h \in H$$

for $h_1, h_2 \in H$

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

$$\Rightarrow a_i h_1 = a_i h_2$$

$$\Rightarrow h_1 = h_2$$

$\Rightarrow \varphi$ is one-one

Also for each $a_i h \in a_i H \exists h \in H$

so φ is onto

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

As H has m elements, each $a_i H$ has m elements.

so from (iii) we have

$$n = m + m + \dots + m \quad (k \text{ times})$$

$$\Rightarrow n = km$$

$$\Rightarrow k \mid n \quad \text{and} \quad m \mid n$$

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

Available online at <http://www.MathCity.org>

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

$$G = U(HaK) \text{ and } HaK \cap HbK = \emptyset.$$

Since each $HaK \subseteq G$

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

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

$$\text{i.e. } a \in HaK$$

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

from (i) and (ii)

$$G = U(HaK)$$

Now consider HaK and HbK are two distinct double cosets

$$\text{let } x \in (HaK) \cap (HbK)$$

$$\Rightarrow x \in HaK \text{ and } x \in HbK$$

$$\therefore x = hak \text{ and } x = h_1 b k_1$$

$$\Rightarrow hak = h_1 b k_1$$

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

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

if $y \in H a K$

then $y = h_2 a k_2$

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

$$= h_2 h_1^{-1} h_1 b k_1 k_1^{-1} k_2 \in H b K$$

$$\Rightarrow y \in H b K$$

$$\Rightarrow H a K \subseteq H b K$$

Similarly, we can get

$$H b K \subseteq H a K$$

$$\Rightarrow H a K = H b K$$

which is contradiction as $H a K$ and $H b K$ are distinct.

hence $H a K \cap H b K = \emptyset$

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 $bX = Xb$

$$\therefore bX = Xb$$

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

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

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

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

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

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

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

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

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

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

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

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

Corollary:-

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

Proof:-

$$\text{Let } h \in H$$

$$\text{then } hH = H = Hh$$

$$\because aH = H \Leftrightarrow a \in H$$

$$\text{i.e. } hH = Hh$$

$$\Rightarrow h \in N_G(H)$$

$$\text{so } H \subseteq N_G(H)$$

Note.

The above corollary can also be state as

"Normalizer of a subgroup contains that subgroup."

Also converse of above corollary may not true.

Available online at <http://www.MathCity.org>

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, $\forall x \in X$

$$ax = xa \quad \text{--- (i)}$$

$$bx = xb \quad \text{--- (ii)}$$

from (ii)

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

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

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

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

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 $ga\bar{g}'$, $g \in G$ is called conjugate of a .

or for $a, b \in G$, b is conjugate of a

if $b = ga\bar{g}'$, $g \in G$.

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) ~~Reflex~~ Reflexive

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

ii) Symmetric.

Let $a \sim b$

$$\Rightarrow b = ga\bar{g}', g \in G$$

$$\Rightarrow ga\bar{g}' = b$$

$$\Rightarrow a\bar{g}' = \bar{g}'b$$

$$\Rightarrow a = \bar{g}'b g$$

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

$$\Rightarrow b \sim a \Rightarrow \sim \text{ is symmetric.}$$

iii) Transitive

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

$$\Rightarrow b = g_1 a \bar{g}_1' \quad \& \quad c = g_2 b \bar{g}_2' \quad \text{for } g_1, g_2 \in G.$$

Since

$$c = g_2 b \bar{g}_2'$$

$$= g_2 (g_1 a \bar{g}_1') \bar{g}_2'$$

$$= (g_2 g_1) a (\bar{g}_1' \bar{g}_2')$$

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

$$\Rightarrow a \sim c$$

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:-

$$\begin{aligned} \text{i) } G &= \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle \\ &= \{1, a, a^2, b, a^3, ab, a^2b, a^3b\} \end{aligned}$$

$$\because a^4 = 1$$

$$\Rightarrow a^{-1} = a^3$$

$$\& (ab)^2 = 1$$

$$\Rightarrow (ab)(ab) = 1$$

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

$$= ba^3$$

$$b^2 = 1$$

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

$$\& (ab)^2 = 1$$

$$\Rightarrow (ab)(ab) = 1$$

$$\Rightarrow a(ba)b = 1$$

$$\Rightarrow ba = a^{-1}b^{-1}$$

$$= a^3b$$

$C_G(x)$ 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

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

$$a^2 \cdot a^2 = a^4 = 1$$

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 $C_G(X) = G$.

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

$ba \neq ab$ 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

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

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

Exercise

Find ~~$N_G(x)$~~ $N_G(x)$ 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 ✓

$$\bullet \text{ Let } b = g a g^{-1} \Rightarrow a = g^{-1} b (g^{-1})^{-1} \\ \Rightarrow b^m = (g a g^{-1})^m = g a^m g^{-1} \text{ and } a^m = g^{-1} b^m (g^{-1})^{-1}$$

$$\text{i.e. } a^m = e \text{ iff } b^m = e$$

i.e. order of a & b is same.

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

Self-Conjugate:

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

$$\Rightarrow x g = g x$$

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

Conversely,

$$\text{let } x \in C_G(G)$$

$$\text{then } x g = g x$$

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

$$\Rightarrow x \text{ is self conjugate.}$$

✓ # Conjugacy Class

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

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

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

i) φ is well define

$$\text{Let } Ng_1 = Ng_2 \text{ where } g_1, g_2 \in G.$$

$$\Rightarrow N = g_1 Ng_2 g_1^{-1}$$

$$\Rightarrow g_2 g_1^{-1} \in N$$

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

$$g_2 g_1^{-1} = n \text{ (say } n \in N)$$

$$\text{Now } g_2^{-1} a g_2 = (n g_1^{-1}) a (n g_1) \quad \therefore g_2 = n g_1$$

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

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

$$= g_1^{-1} a g_1$$

$$\therefore n^{-1} a n = a$$

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

$\Rightarrow \varphi$ 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

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

$$\Rightarrow \bar{g}_1^{-1} a g_1 = \bar{g}_2^{-1} a g_2$$

$$\Rightarrow g_2 (\bar{g}_1^{-1} a g_1) \bar{g}_2^{-1} = a$$

$$\Rightarrow (g_2 \bar{g}_1^{-1}) a (g_1 \bar{g}_2^{-1}) = a$$

$$\Rightarrow (g_2 \bar{g}_1^{-1})^{-1} a (g_1 \bar{g}_2^{-1}) = a$$

$$\Rightarrow g_1 \bar{g}_2^{-1} \in N$$

$$\Rightarrow g_1 \in Ng_2 \quad \text{but } g_1 \in Ng_1$$

$$\Rightarrow Ng_1 \subseteq Ng_2$$

Similarly

$$Ng_2 \subseteq Ng_1$$

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

$$\Rightarrow \varphi \text{ is bijective}$$

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

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

• 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 $C_1, C_2, C_3, \dots, C_r$ be the all conjugacy classes with $m_1, m_2, m_3, \dots, m_r$ number of elements respectively.

$$\left. \begin{array}{l} \text{then } n = |C_1| + |C_2| + \dots + |C_r| \\ \text{i.e. } n = m_1 + m_2 + \dots + m_r \end{array} \right\} \text{--- (i)}$$

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

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

where each m_i divides p^n .

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

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

Let one of them say m_1 is one due to conjugacy class of identity element.

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

but if $b \in C_a$

then $b = gag^{-1}$

$$\Rightarrow bg = ga$$

$$\Rightarrow bg = ag \quad \because a \text{ is self-conjugate}$$

$$\Rightarrow b = a$$

Let such classes of the above two types be K .
Without loss of generality these are

$$m_1, m_2, \dots, m_K$$

Now

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

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

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

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

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

Now

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

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

$$\text{i.e. } p \mid K$$

$\Rightarrow$ 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

$$K = gHg^{-1} = \{ghg^{-1} : h \in H\} \quad \text{for some } g \in G.$$

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

$$\begin{aligned} ab^{-1} &= (gh_1g^{-1})(gh_2g^{-1})^{-1} \\ &= (gh_1g^{-1})(gh_2^{-1}g^{-1}) \\ &= gh_1(g^{-1}g)h_2^{-1}g^{-1} \\ &= gh_1eh_2^{-1}g^{-1} \\ &= gh_1h_2^{-1}g^{-1} \end{aligned}$$

∵ $h_1, h_2 \in H$ and H is subgroup

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

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

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

Available online at <http://www.MathCity.org>

Theorem

$\therefore$ 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

$$\varphi : H \rightarrow K \text{ by } \varphi(h) = k$$

i) then φ is onto

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

ii) φ is one-one

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

$$\Rightarrow k_1 = k_2$$

$$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$$

$$\Rightarrow h_1 = h_2$$

$\Rightarrow \varphi$ is bijective mapping.

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

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

$$\begin{aligned} \varphi(h_1h_2) &= gh_1h_2g^{-1} \\ &= (gh_1)(h_2g^{-1}) \end{aligned}$$

$$= (gh_1)g^{-1}g(h_2g^{-1})$$

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

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

$\Rightarrow \varphi$ is homomorphism

$\therefore \varphi$ is bijective

$\therefore H$ and K are isomorphism.

Theorem

∴ 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 $Q = H \cap aKa^{-1}$.

Proof:

∵ H and K are finite subgroup of G so number of elements in Hak is also finite

Let $Hak = \{g_1, g_2, \dots, g_r\} = \bigcup_{i=1}^r \{g_i\}$, $r < n$.
then $Hak \subseteq G$

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

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

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

$$\Rightarrow |Hak| = |Hak\bar{a}^{-1}| \quad (i)$$

Also let $aKa^{-1} = K'$ then

number of elements in K' , being conjugate to K , is n .

Now

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

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

$$= \frac{m \cdot n}{|Q|}$$

$$= \frac{mn}{q} \quad \text{where } |H \cap K'| = |Q| \text{ (say)}$$

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

where $Q = H \cap K' = H \cap aKa^{-1}$

By (i) and (ii)

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

Define mapping

$$\phi: Hak \rightarrow Hak\bar{a}^{-1}$$

$$\text{by } \phi(hak) = hak\bar{a}^{-1}$$

Theorem

$\therefore$ Let H and K ~~be~~^{be} subgroups of a group G , HaK is a double coset and $Q = H \cap aK\bar{a}^{-1}$ 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 $\phi: A \rightarrow B$ as follows:

For each $haK \in A$ we have a left coset hQ of Q in H .

$$\text{i.e. } \phi(haK) = hQ$$

Then ϕ is well define

$$\text{As } haK = h'aK$$

$$\Rightarrow haK = h'aK \quad \text{for } k, k' \in K$$

$$\Rightarrow h^{-1}h' = a k' k^{-1} a^{-1} \in aK\bar{a}^{-1} \quad \text{as } k'k^{-1} \in K$$

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

$$\Rightarrow h \in h'Q \quad \text{but } h \in hQ$$

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

Similarly we can show

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

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

so ϕ is well define.

ϕ is one one as

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

$$\Rightarrow hQ = h'Q$$

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

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

So

$$h^{-1}h' = a k \bar{a}^{-1}$$

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

* Also $ha = h'ae \in haK$
 $\Rightarrow haK$ and $h'aK$ are not disjoint

$$\Rightarrow haK = h'aK$$

Also ϕ is onto obviously

So there is one-one correspondence between

$\therefore Q = H \cap aK\bar{a}^{-1}$ 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 $H \trianglelefteq G$.

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 $\varphi: G \rightarrow H$ is a homomorphism. Then $\ker \varphi$ is a normal subgroup of G .

Proof:

Let $a, b \in \ker \varphi$

$$\Rightarrow \varphi(a) = I_H \text{ and } \varphi(b) = I_H$$

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

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

$$= I_H \cdot (\varphi(b))^{-1} \quad \because \varphi(a) = I_H$$

$$= I_H \cdot (I_H)^{-1}$$

$$= I_H$$

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

Let $k \in \ker \varphi$

to prove $gkg^{-1} \in \ker \varphi, g \in G$

$$\varphi(gkg^{-1}) = \varphi(g) \cdot \varphi(k) \cdot \varphi(g^{-1}) \quad \because \varphi \text{ is homomorphism}$$

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

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

$$= \varphi(gg^{-1})$$

$$= \varphi(e) = I_H$$

$$\Rightarrow gkg^{-1} \in \ker \varphi$$

$\Rightarrow \ker \varphi$ 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 $k^{-1} \in K$.

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

$\therefore hkh^{-1}k^{-1} \in H$ 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 .

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

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

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

hence H is normal in G .

Theorem

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

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

If $h \in H$

$$\begin{aligned} h &= (g\bar{g})h(g\bar{g}) \\ &= g(\bar{g}hg)\bar{g} \\ &= gh'g^{-1} \in gHg^{-1} \end{aligned}$$

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

From (A) and (B)

$$gHg^{-1} = H$$

Now (ii) $\Rightarrow$ (iii)

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

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

$$\text{or } h = \bar{g}h'g$$

For $gh \in gH$

$$\begin{aligned} gh &= g(\bar{g}h'g) \\ &= (g\bar{g})h'g = eh'g \\ &= h'g \in Hg \end{aligned}$$

$$\Rightarrow gH \subseteq Hg \quad \text{--- (C)}$$

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

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

$$gH = Hg$$

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

$$\Rightarrow gh\bar{g}' = h' \in H$$

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

Theorem

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

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 $a \notin H \therefore$ 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

$$\text{i.e. } G = H \cup Ha = H \cup aH$$

$$\text{and } H \cap Ha = aH \cap H = \emptyset$$

$$\Rightarrow aH = Ha$$

i.e. each left coset is equal to right coset

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

$$\Rightarrow ah\bar{a}' = h' \in H$$

$$\Rightarrow ah\bar{a}' \in H$$

$$\Rightarrow H \triangleleft G$$

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 .

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

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 $h_1a \in Ha$, $h_2b \in Hb$

we have

$$\begin{aligned} h_1a h_2b &= h_1(a h_2)b \\ &= h_1(h_3a)b \\ &= (h_1h_3)(ab) \\ &= h_4ab \end{aligned}$$

$$\left\{ \begin{array}{l} \because H \trianglelefteq G \\ aH = Ha \\ \Rightarrow ah_2 = h_3a, h_2, h_3 \in H \\ h_4 = h_1h_3 (\text{say}) \in H \end{array} \right.$$

$$\Rightarrow Ha \cdot Hb = Hab$$

Also Q is group.

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

ii) Q is associative

$$\begin{aligned} Ha \cdot (Hb \cdot Hc) &= Ha \cdot Hbc \\ &= Ha(bc) = H(ab)c \\ &= Hab \cdot Hc = (Ha \cdot Hb) \cdot Hc \end{aligned}$$

iii) H is identity of Q

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

$$\text{and } H \cdot Ha = He \cdot Ha = Hea = Ha$$

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

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

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

$\Rightarrow Q$ 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 $\phi: G \rightarrow G/H$ is a mapping given by $\phi(a) = Ha \quad \forall a \in G$.

then ϕ is epimorphism (homomorphism + onto) and $\ker \phi = H$.

Proof.

$\therefore \phi: G \rightarrow G/H$ is defined as

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

i) ϕ is well defined as

$$a = b, \quad a, b \in G$$

$$Ha = Hb$$

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

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 $a \in H \subseteq G$

$$\phi(a) = Ha$$

$$= H$$

$\therefore$ when $a \in H$

then $Ha = H$

= 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)

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

1st Isomorphism theorem

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

Proof:

$$\phi: G \rightarrow G'$$

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

Define a mapping ψ such that

$$\psi: G/K \rightarrow G' \text{ defined by}$$

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

then ψ is well define

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

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

$$\text{if } gK = g_1K$$

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

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

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

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

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

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

$$\Rightarrow \phi(e) \cdot g'_1 = g'$$

$$\Rightarrow e' \cdot g'_1 = g'$$

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

$$\Rightarrow \psi \text{ is well define.}$$

ii) For $g' \in G'$

$$g' = \phi(g) \text{ and } \phi(g) = \psi(gK)$$

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

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

$$\Rightarrow \psi \text{ is onto.}$$

iii) ψ is one-one

$$\text{As } \psi(gK) = \psi(g_1K)$$

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

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

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

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

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

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

$$\Rightarrow g_1 \in gK \quad \text{also } g_1 \in g_1K$$

$$\Rightarrow gK = g_1K$$

$$\Rightarrow \psi \text{ is one-one}$$

iv) To prove ψ is homomorphism

for $gK, g_1K \in G/K$

$$\psi(gK \cdot g_1K) = \psi(gg_1K)$$

$$= \phi(gg_1)$$

$$= \phi(g) \cdot \phi(g_1) \quad \because \phi \text{ is homomorphism}$$

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

$$\Rightarrow \psi \text{ is homomorphism}$$

$$\text{hence } G/K \cong \phi(G) \quad \text{or } G/K \cong G'$$

Available online at <http://www.MathCity.org>

Discuss your problems at <http://forum.mathcity.org>

Theorem

Let $\varphi: G \rightarrow G'$ 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 $ghg^{-1} \in H$

$$\begin{aligned}\varphi(ghg^{-1}) &= \varphi(g) \cdot \varphi(h) \cdot \varphi(g^{-1}) \quad \because \varphi \text{ is homo.} \\ &= \varphi(g) \cdot \varphi(h) \cdot (\varphi(g))^{-1} \in H' \quad \because H' \text{ is normal}\end{aligned}$$

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

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

$$\Rightarrow H \text{ is normal subgroup of } G$$

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 $g \in G, h \in H$

$$\begin{aligned}\Rightarrow g'h'g'^{-1} &= \varphi(g) \cdot \varphi(h) \cdot \varphi(g^{-1}) \\ &= \varphi(ghg^{-1}) \quad \because \varphi \text{ is homomorphism}\end{aligned}$$

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

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

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

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

2nd Isomorphism Theorem

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

i) HNK is normal subgroup of H .

ii) HK is subgroup of G .

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

Proof.

i) To prove HNK is a normal subgroup

Let $x \in HNK$

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

∵ K is normal subgroup

∴ $hxh^{-1} \in K$ for $h \in H \subseteq G$

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

$\Rightarrow hxh^{-1} \in HNK$

$\Rightarrow HNK$ is normal subgroup

ii) To prove HK is a subgroup

Let $x_1, x_2 \in HK$

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

Now

$$x_1 x_2^{-1} = (h_1 k_1) (h_2 k_2)^{-1}$$

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

$$= h_1 k_3 h_2^{-1} \quad \text{where } k_1 k_2^{-1} \in K$$

$$\Rightarrow k_1 k_2^{-1} = k_3 \text{ (say)}$$

$$= h_1 (h_2^{-1} h_2) k_3 h_2^{-1}$$

$$= (h_1 h_2^{-1}) (h_2 k_3 h_2^{-1}) \in HK$$

because $h_1 h_2^{-1} \in H$ and $h_2 k_3 h_2^{-1} \in K$ as K is normal.

$\Rightarrow HK$ is subgroup of G .

iii) To prove $H/HNK \cong HK/K$

Define a mapping

$$\varphi: H \rightarrow HK/K$$

$$\text{by } \varphi(h) = hK \quad \text{--- (i)}$$

then φ is obviously well define and onto

Now

$$\begin{aligned}\varphi(h_1 h_2) &= h_1 h_2 K \\ &= (h_1 K)(h_2 K) \quad \text{by multiplication in quotient group.} \\ &= \varphi(h_1) \cdot \varphi(h_2)\end{aligned}$$

i.e φ is homomorphism

$\Rightarrow \varphi$ is epimorphism as it is onto & homomorphism

By 1st isomorphism theorem

$$H/\ker \varphi \cong \varphi(H)$$

$$\text{i.e } H/\ker \varphi \cong HK/K$$

Now to prove $\ker \varphi = H \cap K$

Let $h \in \ker \varphi$

$$\Rightarrow \varphi(h) = K$$

$$\Rightarrow hK = K \quad \text{by (i)}$$

$$\Rightarrow h \in K \quad \text{also } h \in H$$

$$\Rightarrow h \in H \cap K \quad \text{--- (i)}$$

$$\Rightarrow \ker \varphi \subseteq H \cap K \quad \text{--- (ii)}$$

Now let $x \in H \cap K$

$$\Rightarrow x \in H \quad \text{and } x \in K$$

$$\therefore \varphi(x) = xK \quad \text{by (i)}$$

$$= K \quad \therefore x \in K$$

$$\Rightarrow \varphi(x) = K \quad (\text{identity of quotient group})$$

$$\Rightarrow x \in \ker \varphi$$

$$\Rightarrow H \cap K \subseteq \ker \varphi \quad \text{--- (iii)}$$

From (ii) and (iii)

$$\ker \varphi = H \cap K$$

$$\therefore H/\ker \varphi \cong HK/K$$

$$\Rightarrow H/H \cap K \cong HK/K$$

Q.E.D.

3rd Isomorphism Theorem

$\therefore$ 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 $gH \in G/H$

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

$$\therefore K \trianglelefteq G \therefore gkg^{-1} \in K$$

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

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

Define a mapping $\Phi: G/H \rightarrow G/K$

$$\text{by } \Phi(gH) = gK$$

then Φ is clearly onto

Also

$$\Phi(g_1H \cdot g_2H) = \Phi(g_1g_2H)$$

$$= g_1g_2K$$

$$= g_1K \cdot g_2K$$

$$= \Phi(g_1H) \cdot \Phi(g_2H)$$

$\Rightarrow \Phi$ is homomorphism.

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

by 1st isomorphism theorem

$$(G/H)/\text{Ker } \Phi \cong G/K$$

if $\Phi: G \rightarrow G'$ is epimorphism then

$$G/\text{Ker } \Phi \cong G'$$

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

Let $gH \in \ker \phi$

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

Also

$$\phi(gH) = gK$$

$$\Rightarrow gK = K$$

$$\Rightarrow g \in K$$

$$\Rightarrow gH \in K/H$$

$$\Rightarrow \ker \phi \subseteq K/H \quad \text{--- (i)}$$

Now let $kH \in K/H$

$$\begin{aligned} \text{then } \phi(kH) &= kK \\ &= K \text{ (identity)} \end{aligned}$$

$$\Rightarrow kH \in \ker \phi$$

$$\Rightarrow K/H \subseteq \ker \phi \quad \text{--- (ii)}$$

From (i) and (ii)

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

$$\therefore (G/H) / \ker \phi \cong G/K$$

$$\Rightarrow (G/H) / (K/H) \cong G/K$$

proved

Available online at <http://www.MathCity.org>

Endomorphism:-

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

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

Automorphism:-

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

i.e. $\alpha: G \rightarrow G$ 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 $\text{Aut}(G)$.

Remarks:

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

Theorem:

The set $A(G)$ or $\text{aut}(G)$ 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 (composition) $\alpha\beta$ is also bijective mapping.

and for $g_1, g_2 \in G$

$$\alpha\beta(g_1, g_2) = \alpha(\beta(g_1, g_2))$$

$$= \alpha(\beta(g_1) \cdot \beta(g_2)) \quad \because \beta \text{ is homo.}$$

$$= \alpha(\beta(g_1)) \cdot \alpha(\beta(g_2)) \quad \because \alpha \text{ is homo.}$$

$$= \alpha\beta(g_1) \cdot \alpha\beta(g_2)$$

$$\Rightarrow \alpha\beta \text{ is homomorphism} \Rightarrow \alpha\beta \in A(G)$$

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

iii) Define $I: G \rightarrow G$ 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.

$$\text{Also } \alpha I(g) = \alpha \circ I(g) = \alpha(I(g)) = \alpha(g)$$

$$\text{i.e. } \alpha I = \alpha$$

Similarly $I\alpha = \alpha$

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

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

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

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

$$\alpha^{-1}(g_1 g_2) = \alpha^{-1}(I(g_1 g_2))$$

$$= \alpha^{-1}(I(g_1) \cdot I(g_2))$$

$$= \alpha^{-1}(\alpha \alpha^{-1}(g_1) \cdot \alpha \alpha^{-1}(g_2))$$

$$= \alpha^{-1} \alpha (\alpha^{-1}(g_1) \cdot \alpha^{-1}(g_2))$$

$$= I(\alpha^{-1}(g_1) \cdot \alpha^{-1}(g_2))$$

$$= \alpha^{-1}(g_1) \cdot \alpha^{-1}(g_2)$$

$\Rightarrow \alpha^{-1}$ 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)

$\therefore$ Let G be a group, $a \in G$, define a mapping $\varphi_a : G \rightarrow G$ by

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

then φ_a is automorphism

Proof:

i) φ is onto

for $g \in G$, $a \in G$ we have $ag\bar{a}' \in G$
then g is image of $ag\bar{a}'$ under φ

$$\begin{aligned}\therefore \varphi_a(ag\bar{a}') &= \bar{a}'(ag\bar{a}')a \\ &= (\bar{a}'a)g(\bar{a}'a) \\ &= g\end{aligned}$$

$\Rightarrow \varphi$ is onto.

ii) φ is one-one

$$\begin{aligned}\therefore \varphi_a(g_1) &= \varphi_a(g_2) \\ \Rightarrow \bar{a}'g_1a &= \bar{a}'g_2a \\ \Rightarrow g_1 &= g_2\end{aligned}$$

iii) φ is homomorphism

$$\begin{aligned}\varphi_a(g_1g_2) &= \bar{a}'g_1g_2a \\ &= \bar{a}'g_1(a\bar{a}')g_2a \\ &= (\bar{a}'g_1a)(\bar{a}'g_2a) \\ &= \varphi_a(g_1) \cdot \varphi_a(g_2)\end{aligned}$$

Hence φ_a is automorphism

Inner and Outer automorphism

def. The set $I(G)$ or $\text{Inn}(G)$ of all mapping of the type $\phi_a = a g a^{-1}$ is called inner automorphism of G .

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

Theorem

$\therefore$ 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 $\phi_a = a g a^{-1}$, $\phi_b = b g b^{-1}$

Now

$$\begin{aligned} \phi_b \cdot \phi_b^{-1}(g) &= \phi_b(b^{-1} g (b^{-1})^{-1}) \\ &= \phi_b(b^{-1} g b) \\ &= b(b^{-1} g b) b^{-1} \\ &= (b b^{-1}) g (b b^{-1}) \\ &= e g e^{-1} \\ &= \phi_e \end{aligned}$$

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

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

$$x y^{-1} = \phi_a (\phi_b)^{-1}(g)$$

$$\begin{aligned} &= \phi_a \phi_b^{-1}(g) = \phi_a(b^{-1} g b) \\ &= a(b^{-1} g b) a^{-1} \\ &= (a b^{-1}) g (b a^{-1}) \\ &= (a b^{-1}) g (a b^{-1})^{-1} \\ &= \phi_{a b^{-1}} \in I(G) \end{aligned}$$

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

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

Now

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

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

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

Available online at <http://www.MathCity.org>

- ❖ FSc
- ❖ BSc
- ❖ MSc / BS
- ❖ MPhil / MS
- ❖ PhD
- ❖ Old Papers / Entry Test

o Check out all these at

▪ <http://www.MathCity.org>

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 $\psi : G \rightarrow I(G)$ 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

$$\begin{aligned} \psi(ab) &= \phi_{ab} \\ &= (ab)g(ab)^{-1} \end{aligned}$$

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

$$= a(bg b^{-1})a^{-1}$$

$$= a(\phi_b)a^{-1}$$

$$= \phi_a(\phi_b) = \phi_a \circ \phi_b \quad (\text{composite fn.})$$

$$\phi_a \circ \phi_b = \phi_a \cdot \phi_b$$

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

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

Now By first isomorphism theorem

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

$\because$ if $\psi : G \rightarrow G'$ is epimorphism then

$$G/\ker \psi \cong G'$$

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

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

$$= \{a : a \in G \wedge \varphi_a = \varphi_e\}$$

$$= \{a : a \in G \wedge aga^{-1} = ege^{-1}\}$$

$$= \{a : a \in G \wedge aga^{-1} = g\}$$

$$= \{a : a \in G \wedge ag = ga\}$$

$$= C(G)$$

$$\Rightarrow G/C(G) \cong I(G)$$

Available online at <http://www.MathCity.org>

Ask questions at <http://forum.mathcity.org>

- ❖ FSc
- ❖ BSc
- ❖ MSc / BS
- ❖ MPhil / MS
- ❖ PhD
- ❖ Old Papers / Entry Test

o Check out all these at

▪ <http://www.MathCity.org>

Theorem:

$\therefore \varphi: G \rightarrow G$ by $\varphi(x) = x^{-1}$ then φ is automorphism iff G is abelian.

Proof:

Let G be abelian

$$\begin{aligned}\varphi(g_1 g_2) &= (g_1 g_2)^{-1} \\ &= g_2^{-1} g_1^{-1} \\ &= g_1^{-1} g_2^{-1} \quad \because G \text{ is abelian} \\ &= \varphi(g_1) \cdot \varphi(g_2)\end{aligned}$$

$\Rightarrow \varphi$ is homomorphism

φ is onto because each $g \in G$ we have:

$$\varphi(g^{-1}) = (g^{-1})^{-1} = g$$

φ is one-one

$$\varphi(g_1) = \varphi(g_2)$$

$$\Rightarrow g_1^{-1} = g_2^{-1} \Rightarrow g_1 = g_2$$

$\Rightarrow \varphi$ is automorphism

Conversely, let φ is automorphism

i.e. φ is homomorphism

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

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

$$\Rightarrow g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1}$$

$$\Rightarrow g_1 g_2 = g_2 g_1$$

$\Rightarrow G$ is abelian

Commutator of a group

def:- Let G be a group and $a, b \in G$
then the element $x = ab\bar{a}'\bar{b}'$ is called ~~com~~
commutator of G and we write $[a, b] = ab\bar{a}'\bar{b}'$.

Theorem:

-: The following commutator results hold in G .

For $a, b \in G$

$$i) [b, a] = [a, b]^{-1}$$

$$ii) [ab, c] = [b, c]^a [a, c] \quad \left| \quad [b, c]^a = a[b, c]\bar{a}' \right.$$

$$= a[b, c]\bar{a}'[a, c]$$

$$iii) [a, bc] = [a, b][a, c]^b$$

$$iv) [a, b^{-1}] = [b, a]^{-1}, \quad [\bar{a}', b] = [b, a]^{-1}$$

Proof

$$\begin{aligned} [a, b][b, a] &= (ab\bar{a}'\bar{b}')(ba\bar{b}'\bar{a}') \\ &= ab\bar{a}'(\bar{b}'b)a\bar{b}'\bar{a}' \\ &= ab(\bar{a}'a)\bar{b}'\bar{a}' \\ &= a(bb^{-1})\bar{a}' \\ &= a\bar{a}' = e \end{aligned}$$

i.e. $[b, a]$ is inverse of $[a, b]$

$$\Rightarrow [a, b]^{-1} = [b, a]$$

$$\begin{aligned} ii) [ab, c] &= (ab)c(ab)^{-1}\bar{c}' \\ &= abc\bar{b}'\bar{a}'\bar{c}' \\ &= abc\bar{b}'\bar{c}'e\bar{a}'\bar{c}' \\ &= abc\bar{b}'\bar{c}'\bar{a}'a\bar{c}'\bar{c}' \\ &= a(bc\bar{b}'\bar{c}')\bar{a}'(ac\bar{a}'\bar{c}') \\ &= [b, c]^a [a, c] \quad \text{proved} \end{aligned}$$

$$\begin{aligned} iii) [a, bc] &= a(bc)\bar{a}'(bc)^{-1} \\ &= ab\bar{c}'\bar{a}'\bar{c}'\bar{b}' \\ &= ab\bar{a}'ac\bar{a}'\bar{c}'\bar{b}' \\ &= ab\bar{a}'\bar{b}'bac\bar{a}'\bar{c}'\bar{b}' \end{aligned}$$

$$\begin{aligned}
 &= (a b \bar{a}' \bar{b}') b (a c \bar{a}' \bar{c}') \bar{b}' \\
 &= [a, b] [a, c]^b \quad \text{proved.}
 \end{aligned}$$

$$\begin{aligned}
 \text{(iv)} \quad [a, b'] &= a b' \bar{a}' (\bar{b}')^{-1} \\
 &= a b' \bar{a}' b \\
 &= b' b a b' \bar{a}' b \\
 &= b' (b a b' \bar{a}') b \\
 &= b' (b a b' \bar{a}') (\bar{b}')^{-1} \\
 &= [b, a]^{b'} \quad \text{proved}
 \end{aligned}$$

And

$$\begin{aligned}
 [\bar{a}', b] &= \bar{a}' b (\bar{a}')^{-1} \bar{b}' \\
 &= \bar{a}' b a b' \bar{a}' \\
 &= \bar{a}' b a b' \bar{a}' a \\
 &= \bar{a}' (b a b' \bar{a}') a \\
 &= \bar{a}' (b a b' \bar{a}') (\bar{a}')^{-1} \\
 &= [b, a]^{\bar{a}'} \quad \text{proved}
 \end{aligned}$$

Derived 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~~ Let for $g \in G$

$$g[a, b]g^{-1} = g(a b \bar{a}' \bar{b}')g^{-1}$$

$$\begin{aligned}
&= g a b \bar{a}' b' \bar{g}'^{-1} \\
&= g a \bar{g}' g b \bar{g}' g \bar{a}' \bar{g}' g b' \bar{g}' \\
&= (g a \bar{g}') (g b \bar{g}') (g \bar{a}' \bar{g}') (g b' \bar{g}') \\
&= (g a \bar{g}') (g b \bar{g}') (g a \bar{g}')^{-1} (g b \bar{g}')^{-1} \\
&= a^g b^g (a^g)^{-1} (b^g)^{-1} = [a^g, b^g] \in G' \\
&\Rightarrow G' \text{ is normal subgroup of } G.
\end{aligned}$$

ii) Let $aG', bG' \in G/G'$ where $a, b \in G$
 then

$$\begin{aligned}
[aG', bG'] &= (aG')(bG')(aG')^{-1}(bG')^{-1} \\
&= (aG')(bG')(\bar{a}'G')(\bar{b}'G') \\
&= (a b \bar{a}' b') G' \quad \text{by multiplication of quotient group} \\
&= [a, b] G' \\
&= G' \quad \because [a, b] \in G' \\
&= \text{Identity of Quotient group}
\end{aligned}$$

$\Rightarrow G/G'$ is abelian

$$\begin{array}{l}
\text{if } [a, b] = e \\
\Rightarrow a b \bar{a}' \bar{b}' = e \\
\Rightarrow a b = b a
\end{array}$$

iii) Since $aK \cdot bK (aK)^{-1} (bK)^{-1} = K \quad \because G/K \text{ is abelian}$
 $\Rightarrow aK \cdot bK \cdot \bar{a}'K \cdot \bar{b}'K = K$
 $\Rightarrow (a b \bar{a}' \bar{b}') K = K$
 $\Rightarrow [a, b] K = K$
 $\Rightarrow [a, b] \in K$
 $\Rightarrow G' \subseteq K$

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 $kh^{-1}k^{-1} \in H \quad \because H \trianglelefteq G$

$\Rightarrow h(kh^{-1}k^{-1}) \in H \quad \because h \in H$

also $hkh^{-1} \in K \quad \because K \trianglelefteq G$

$\Rightarrow (hkh^{-1})k^{-1} \in K \quad \because k^{-1} \in K$

i.e. $hkh^{-1}k^{-1} \in H \cap K = \{e\} \quad (\text{given})$

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

$\Rightarrow hk = kh$

$\Rightarrow$ every element of H is permutable with every element of K .

ii) Let if possible, g has two expressions

$$g = h_1 k_1 \quad \& \quad g = h_2 k_2$$

$$\text{for } h_1, h_2 \in H \rightarrow k_1, k_2 \in K$$

$$h_1 \neq h_2 \rightarrow k_1 \neq k_2$$

$$\Rightarrow h_1 k_1 = h_2 k_2$$

$$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1} \in K \text{ and } H$$

$$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$$

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

$$\Rightarrow h_1 = h_2 \quad \& \quad k_1 = k_2$$

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 $\phi: G \rightarrow H \times K$

$$\text{by } \phi(g) = (h, k)$$

a) The mapping is well define as

$$\text{for } g_1 = g_2$$

$$\Rightarrow h_1 k_1 = h_2 k_2 \quad \therefore G = HK$$

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

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

$$\Rightarrow \phi(g_1) = \phi(g_2)$$

b) ϕ is onto as

$(h, k) \in H \times K$ is image of $g = hk \in HK = G$

$$\therefore (h, k) \in H \times K$$

$$\Rightarrow h \in H, \quad k \in K \Rightarrow hk \in HK$$

c) ϕ is one-one

$$\phi(g_1) = \phi(g_2)$$

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

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

$$\Rightarrow h_1 k_1 = h_2 k_2$$

$$\Rightarrow g_1 = g_2 \quad \because g = hk$$

d) ~~ii)~~ ϕ is homomorphism

$$\phi(g_1 \cdot g_2) = \phi(h_1 k_1 \cdot h_2 k_2)$$

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

$$= \phi(h_1 (h_2 k_1) k_2) \quad \text{by (i)}$$

$$= \phi(h_1 h_2 \cdot k_1 k_2)$$

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

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

$$= \phi(h_1 k_1) \cdot \phi(h_2 k_2)$$

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

i.e. ϕ is homomorphism

and hence ϕ is ~~an~~ isomorphism as it is also one-one and onto.

$$\Rightarrow G \cong H \times K \quad \text{or} \quad HK \cong H \times K$$

Note: G is abelian group if $H = \{e\}$ is derived group.

- ❖ FSc
- ❖ BSc
- ❖ MSc / BS
- ❖ MPhil / MS
- ❖ PhD
- ❖ Old Papers / Entry Test

o Check out all these at

▪ <http://www.MathCity.org>

Lemma

Let G be a direct product of two subgroups 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

$$\begin{aligned}
 gh_1g^{-1} &= (hk)h_1(hk)^{-1} \\
 &= (hk)h_1(k^{-1}h^{-1}) \\
 &= h(kh_1)(k^{-1}h^{-1}) && \because h_1 \in H_1 \subseteq H \\
 &= h(h_1k)(k^{-1}h^{-1}) && \because H \text{ and } K \text{ commute element wise.} \\
 &= hh_1(kk^{-1})h^{-1} \\
 &= hh_1k^{-1} \in H_1 && \because H \trianglelefteq H_1
 \end{aligned}$$

$$\Rightarrow gh_1g^{-1} \in H_1$$

$$\Rightarrow H_1 \trianglelefteq G$$

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

$$\begin{aligned}
 gx &= (hk)(z_1 z_2) \\
 &= h(kz_1)z_2 \\
 &= h(z_1 k)z_2
 \end{aligned}$$

$$\begin{aligned}
 &= (hz_1)(kz_2) \\
 &= (z_1h)(z_2k) \\
 &= z_1(hz_2)k \\
 &= (z_1z_2)(hk) \\
 &= xg
 \end{aligned}$$

hence $\Rightarrow x \in C(G)$

$$C(H) \times C(K) \subseteq C(G) \quad \text{--- (i)}$$

Now to prove $C(G) \subseteq C(H) \times C(K)$

let $z \in C(G)$

$$\Rightarrow gz = zg \quad \text{for } g \in G.$$

in particular

$$zh = hz, \quad zk = kz$$

$$\begin{array}{l}
 \because h \in H \subseteq G \\
 k \in K \subseteq G
 \end{array}$$

let $z = h'k'$ for $h' \in H, k' \in K$

so

$$zh = (h'k')h = h'(k'h) = h'hk'$$

and

$$hz = hh'k'$$

$$\therefore hz = zh$$

$$\Rightarrow hh'k' = h'hk'$$

$$\Rightarrow hh' = h'h \Rightarrow h' \in C(H)$$

Similarly

$$k' \in C(K)$$

hence $h'k' \in C(H) \times C(K)$

$$\Rightarrow z \in C(H) \times C(K) \quad \because z = h'k'$$

$$\Rightarrow C(G) \subseteq C(H) \times C(K) \quad \text{--- (ii)}$$

from (i) and (ii)

$$C(G) = C(H) \times C(K)$$

proved

Theorem

$\therefore$ 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

$$\varphi: G/K \rightarrow H \text{ by } \varphi(gK) = \varphi(hK) = h$$

then φ is well define as

$$g_1K = g_2K$$

$$\Rightarrow h_1K = h_2K$$

$$\Rightarrow h_2^{-1}h_1K = K$$

$$\Rightarrow h_2^{-1}h_1 \in K \quad \text{but also } h_2^{-1}h_1 \in H$$

$$\Rightarrow h_2^{-1}h_1 \in H \cap K = \{e\}$$

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

$$\Rightarrow \varphi(h_1K) = \varphi(h_2K)$$

φ is onto and one-one as

for $h \in H$ there is a coset $hK \in G/K$ i.e. $\varphi(hK) = h$

and $\varphi(h_1K) = \varphi(h_2K)$

$$\Rightarrow h_1 = h_2$$

$$\Rightarrow h_1K = h_2K$$

Now

$$\varphi(g_1K \cdot g_2K) = \varphi(h_1K \cdot h_2K)$$

$$= \varphi(h_1h_2K)$$

$$= h_1h_2$$

$$= \varphi(h_1K) \cdot \varphi(h_2K)$$

$$= \varphi(g_1K) \cdot \varphi(g_2K)$$

$\Rightarrow \varphi$ 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 $H \times K$ is a cyclic group.

Proof:

$$H = \langle a : a^m = e \rangle$$

$$K = \langle b : b^n = e \rangle$$

and element of $H \times K$ 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 $H \times K$ is mn

also

$$\begin{aligned} (a, b)^{mn} &= (a^{mn}, b^{mn}) \\ &= ((a^m)^n, (b^n)^m) = (e, e) \end{aligned}$$

$$\text{i.e. } H \times K = \langle (a, b) : (a, b)^{mn} = e \rangle$$

$\Rightarrow H \times K$ is cyclic group of order mn .

Invariant Subgroup

def:- Let G be a group and $\phi: G \rightarrow G$ is endomorphism then an element $\phi(g) = g$ is called invariant element

A subgroup H of G is fully invariant if under all endomorphism $\phi(h) \in H$ or $\phi(H) \subseteq H$

Example:

Commutator subgroup G' is fully invariant

Let $[x, y] \in G'$

$$\begin{aligned} \phi([x, y]) &= \phi(x y x^{-1} y^{-1}) \\ &= \phi(x) \cdot \phi(y) \cdot \phi(x^{-1}) \cdot \phi(y^{-1}) \\ &= \phi(x) \cdot \phi(y) \cdot (\phi(x))^{-1} \cdot (\phi(y))^{-1} = [\phi(x), \phi(y)] \in G' \end{aligned}$$

$\Rightarrow G'$ is fully invariant.

Characteristic Subgroup:

A subgroup H of G is characteristic subgroup if it remain fully invariant under all automorphism, i.e for all $h \in H$, for all $\phi \in \text{Aut}(G)$

$$\phi(h) \in H \quad \text{or} \quad \phi(H) = H$$

Question

$\therefore$ Centre of G is characteristic subgroup of G .

Solution

Let $x \in C(G)$

$$\Rightarrow gx = xg \quad \forall g \in G$$

Let $\phi: G \rightarrow G$ be an automorphism

$$\phi(gx) = \phi(xg)$$

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

$$\text{As } g \in G \Rightarrow \phi(g) \in G$$

$$\text{so } \phi(x) \in C(G)$$

$$\Rightarrow C(G) \text{ is characteristic}$$

Question

$\therefore$ Every characteristic subgroup is normal.

Solution:

Let H is a characteristic subgroup of G ,

$$\text{then } \phi(H) = H \quad \forall \phi \in \text{aut}(G)$$

In particular

$$\phi_g(H) = H \quad \because \phi_g \text{ is an inner automorphism,}$$

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

$$\Rightarrow H \text{ is normal subgroup of } G.$$

= { The End } =
