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, conjugancy 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 a group if

i) Closure law holds in \( G \).
   i.e. for \( a, b \in G \), \( a \times b \in G \).

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

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

iv) Inverse law holds in \( G \).
    i.e. for \( a \in G \), there exists \( a' \in G \) such that \( a \times a' = a' \times a = e \).

If commutative law holds in \( G \), then \( G \) is called an Abelian group.

Example:

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

\[ A = \{ 1, \pm i, \pm j, \pm k \} \] with the conditions:

\[ i \cdot i = j \cdot j = k \cdot k = 1 \]
\[ i \cdot j = jk, \quad j \cdot k = i, \quad k \cdot i = j \]
\[ j \cdot i = -k, \quad k \cdot j = -i, \quad i \cdot k = -j \]

\[ Ix = x \quad \forall \ x \in A \]

then \( A \) is called a group.

# Question:

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

Solution:

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

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 \( n \), the 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 $a$.

\[ a + (n-a) = n = 0 \]

\[ n \div n = \text{Remainder} \]

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) $(a^{-1})^{-1} = a$, $\forall a \in G$.

v) $(a \cdot b)^{-1} = b^{-1}a^{-1}$.

End of Lesson at 12:16 PM
# Order of Group:

- **def.** The number of elements 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 $a, a^2, a^3, \ldots, a^{n-1}$ are all distinct.

**Solution:**

On the contrary let

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

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

a contradiction \Rightarrow 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 $n \mid k$.

Solution:

Let $n \mid k$ 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 $k = nq + r$; $r < n$.

So

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

Which is only possible if $r = 0$.

Then $k = nq \Rightarrow n \mid k$.

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 $\mid R' = \mathbb{R} - \{0\}$
# Subgroup:

**Def.** Let $H$ be a non-empty subset of a group $G$. Then $H$ is a subgroup of $G$ if $H$ itself is a subgroup with the binary operation defined on $G$.

**Theorem.**

Let $G$ be a group and $H$ a non-empty subset of $G$. Then $H$ is a subgroup if

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

**Proof.**

Suppose that $H$ is a subgroup of $G$. Then $(H, \cdot)$ is a group, if

$$b \in H, \ b^{-1} \in H$$

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

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

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

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

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 $G$.
Let $G$ be an abelian group and $F$ be a subset of all elements 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 $ab^{-1} \in F$.

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

$$= a^{mn} (b^{-1})^{mn} \quad \because G \text{ is abelian}$$

$$= a^{mn} b^{-mn} \quad \because (b^{-1})^m = b^{-m}$$

$$= (a^m)^n (b^n)^{-m}$$

$$= e^n \cdot e^{-m}$$

$$= e \cdot e = e$$

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 $G$. 

[6]
# Note:

Union of two subgroup may not be a subgroup. In general, if \( H_1 \) and \( H_2 \) are subgroups of a group \( G \), then \( H_1 \cup H_2 \) is a subgroup of \( G \) if and only if either \( H_1 \subseteq H_2 \) or \( H_2 \subseteq H_1 \).

\[ Z_1 = \{0, 3, 6\} \quad Z_2 = \{0, 2, 4\} \]

are subgroups of a group \( Z_6 = \{0, 1, 2, 3, 4, 5\} \) but then \( Z_1 \cup Z_2 = \{0, 2, 3, 4, 6\} \) is not a subgroup.

# Theorem:

Let \( H_1 \) and \( H_2 \) are two subgroup of a group \( G \). Then \( H_1 \cup H_2 \) is a subgroup of \( G \) if and only if 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 \( H_1 \cup H_2 = H_1 \).

\( \therefore \) \( H_1 \) and \( H_2 \) are subgroup so \( H_1 \cup H_2 \) is also subgroup.

Conversely:

Let \( H_1 \cup H_2 \) is a subgroup and let \( H_1 \nsubseteq H_2 \) or \( H_2 \nsubseteq H_1 \) then there are a, b \( \in G \) such that:

\[ a \in H_1 \setminus H_2 \quad b \in H_2 \setminus H_1 \]

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

\( \therefore a \cdot b \in H_1 \cup H_2 \) As \( H_1 \cup H_2 \) are subgroup therefore \( a \cdot b \in H_1 \cup H_2 \) so \( a \cdot b \in H_1 \) or \( a \cdot b \in H_2 \) then \( a \cdot (a \cdot b) = a \cdot b \cdot b \in H_1 \) which is a contradiction.

Hence \( H_1 \cup H_2 \) is subgroup iff \( H_1 \subseteq H_2 \) or \( H_2 \subseteq H_1 \).
# Invaluation

Definition: An element $x$ of order 2 in a group $G$ is called invaluation in $G$.

# Theorem:

Every group of even order has at least one invaluation.

Proof:

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

Let $A = \{e, x \mid x^2 = e \land x \in G\}$

and $B = \{y \mid y^2 \neq e \land y \in G\}$

then $A \cup B = G$ and $A \cap B = \emptyset$.

If $B = \emptyset$, then $A = G$.

Then $G$ contains invalidation.

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.

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

$\Rightarrow |A| \geq 2$ $\Rightarrow$ order of $A$ is even, so it contains min. 2 elements.

Since $A \subseteq G$:

$\Rightarrow G$ contains an invaluation.
# Relation between Groups:

- **Homomorphism**
  
def: Let $(G, \cdot)$ and $(H, \cdot)$ be two groups. Define a mapping $\varphi : G \to H$.
  
The $\varphi$ is homomorphism if $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

  \[ e \in (\mathbb{R}, +), \quad (\mathbb{R}, \cdot) \text{ be two groups} \]

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

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

  \[ \varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y) \]

  $\Rightarrow \varphi$ is homomorphism

- **Monomorphism**
  
def: A mapping $\varphi : G \to G'$ is called monomorphism if
  
  i) $\varphi$ is homomorphism
  
  ii) $\varphi$ is injective (one-one)

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

- **Epimorphism**
  
def: A mapping $\varphi : G \to G'$ is epimorphism such that
  
  i) $\varphi$ is homomorphism
  
  ii) $\varphi$ is surjective (onto)

  i.e. $\forall \ b \in G'$ there is $a \in G$ such that $\varphi(a) = b$
Groups: Handwritten notes

- **Isomorphism**
  
  def: A mapping $\phi: G \rightarrow G'$ is an isomorphism if:
  
  i) $\phi$ is homomorphism
  ii) $\phi$ is bijective (one-one and onto)
  (denoted as $G \cong G'$)

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

# Example

- Let $\phi: (\mathbb{R},+) \rightarrow (\mathbb{R}_{>0},\cdot)$, where $\mathbb{R}$ is set of real numbers and $\mathbb{R}_{>0}$ is the set of non-zero positive real numbers.

  define $\phi(x) = e^{x}$ \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 $(\{\pm1\},\cdot)$ be two groups.

  define a mapping $\phi: \mathbb{Z} \rightarrow \{\pm1\}$

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

  prove that $\phi$ 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 $\phi$ is isomorphism.
# Question

Let $G$ and $G'$ be 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 $f(y) = b$.

Or $x = f^{-1}(a)$ and $y = f^{-1}(b)$.

$\therefore f$ is homomorphism

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

as $f(xy) = ab \Rightarrow xy = f(ab)$.

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 $G$, $G'$, $G''$ 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.

And $g \circ f(xy) = g(f(xy))$

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

$\therefore f$ is isomorphism.

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

$= g \circ f(x) \cdot g \circ f(y)$.
Therefore \( \circ \) is homomorphism and hence isomorphism.

**Theorem:**

Prove that isomorphic groups form an equivalence relation.

**Proof:**

1) Reflexive

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

Then \( I \) is one-one and onto

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

2) 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 \( f(xy) = f(x) \cdot f(y) \).

Prove \( f^{-1} \) is homomorphism.

as in previous 'Question.'

3) Transitive (i.e. \( G \sim G' \) and \( G' \sim G'' \) then \( G \sim G'' \))

Suppose \( f : G \to G' \) and \( \hat{f} : G' \to G'' \) are isomorphisms.

then prove \( \hat{f} \circ f \) is isomorphism.

as in previous 'Question.'
# Definition (Kernel):

Let \( \varphi : G \rightarrow G' \) be a homomorphism then kernel of \( \varphi \) is defined by

\[
\ker \varphi = \{ x \in G \mid \varphi(x) = e' \}
\]

where \( e' \) is identity of \( G' \).

# Lemma:

i) If \( \varphi \) 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 \( G' \)

\[
\Rightarrow \varphi(x). e' = \varphi(x)
\]

\[
= \varphi(x.e) \quad \text{\because } x = x.e
\]

\[
= \varphi(x) \cdot \varphi(e)
\]

\[
\Rightarrow e' = \varphi(e) \quad \text{by cancellation law.}
\]

ii) \( \varphi(x) \cdot \varphi(x^{-1}) = \varphi(xx^{-1}) \quad \text{\because } \varphi \text{ 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} \quad \text{as inverse is unique.}
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 \( \phi \).

1) Let \( g_1, g_2 \in G \) then \( \phi(g_1), \phi(g_2) \in \phi(G) \) and \( \phi(g_1g_2) = \phi(g_1) \cdot \phi(g_2) \in \phi(G) \)

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

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

\[
\phi(g_1) \cdot [\phi(g_2) \cdot \phi(g_3)] = \phi(g_1) \cdot (\phi(g_2) \cdot \phi(g_3))
\]
\[
= \phi(g_1 \cdot (g_2 \cdot g_3))
\]
\[
= \phi((g_1 \cdot g_2) \cdot g_3)
\]
\[
= \phi(g_1 \cdot (g_2 \cdot g_3))
\]
\[
= \phi(g_1) \cdot \phi(g_2) \cdot \phi(g_3)
\]

\( \therefore \) \( \phi(G) \) is associative.

3) If \( e \) is identity of \( G \) then

\[
\phi(x) \cdot \phi(e) = \phi(x \cdot e)
\]
\[
= \phi(x)
\]

\( \therefore \) \( \phi(e) \) is an identity of \( \phi(G) \).

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

\[
\phi(x) \cdot \phi(x^{-1}) = \phi(xx^{-1})
\]
\[
= \phi(e)
\]

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 a homomorphism of a group \( G \) into a group \( H \), then for \( a, b \in G \):

\[ \Phi(a) = \Phi(b) \iff ab^{-1} \in \ker \Phi. \]

Proof:

Suppose \( \Phi(a) = \Phi(b) \)

Now \( \Phi(ab^{-1}) = \Phi(a) \cdot \Phi(b^{-1}) \)

\[ = \Phi(b) \cdot \Phi(b^{-1}) = \Phi(id) = e \]

\[ \Rightarrow ab^{-1} \in \ker \Phi. \]

Conversely, suppose \( ab^{-1} \in \ker \Phi \).

Then \( \Phi(ab^{-1}) = e' \) where \( e' \) is identity of \( H \)

\[ \Rightarrow \Phi(a) \cdot \Phi(b^{-1}) = e' \quad \Phi \text{ is homomorphism} \]

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

\[ \Rightarrow \Phi(a) = \Phi(b) \quad \text{proved} \]

Theorem:

Let \( \Phi : G \rightarrow H \) be a homomorphism then \( \Phi \) is one-one iff \( \ker \Phi = \{ e \} \).

Proof:

Suppose \( \Phi \) is one-one.

It is obvious that \( \{ e \} \subseteq \ker \Phi \)

and let \( a \in \ker \Phi \)

\[ \Rightarrow \Phi(a) = 1_H \]

\[ \Rightarrow \Phi(a) = \Phi(1_G) \]

and \( \Phi \) is one-one.

\[ \therefore a = 1_G \Rightarrow a \in \{ e \} \]

\[ \Rightarrow \ker \Phi \subseteq \{ e \} \text{ and hence } \ker \Phi = \{ e \} \]

[15]
Conversely, let \( \ker \phi = \{ e \} \subset \mathbb{Z} \).

To prove \( \phi \) is one-one.

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

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

\[
\Rightarrow \phi(ab^{-1}) = \phi(b^{-1})
\]

\[
\Rightarrow \phi(ab^{-1}) = \phi(1_\mathbb{Z})
\]

\[
\Rightarrow \phi(ab^{-1}) = 1_\mathbb{Z}
\]

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

\[
\Rightarrow ab^{-1} = 1_\mathbb{Z}
\]

\[
\Rightarrow a = b.
\]

\[
\Rightarrow \phi \text{ is one-one.}
\]
Theorem

Let \( H \) be a subgroup of a group \( G \).
Define a relation over \( G \) such that
\[
\sim \text{ iff } xy^{-1} \in H
\]
then relation \( \sim \) is equivalence relation.

Proof:

i) Reflexive
\[
\because e \in H \Rightarrow xe^{-1} \in H \quad \forall x \in H
\]
\[\Rightarrow x \sim x\]
i.e. this relation is reflexive.

ii) Symmetric

Let \( x \sim y \) then \( xy^{-1} \in H \)
\[\Rightarrow (xy^{-1})^{-1} \in H \because H \text{ is group.}\]
\[\text{i.e. } (xy^{-1})^{-1} = (y^{-1})^{-1} \cdot x^{-1}\]
\[= y \cdot x^{-1}\]
\[\Rightarrow \gamma x^{-1} \in H \quad \text{i.e. } \gamma \sim x\]
\[\therefore \sim \text{ is symmetric.}\]

iii) Transitive

Let \( x \sim y \) then \( xy^{-1} \in H \)
also \( y \sim z \) then \( yz^{-1} \in H \)

Now \( (xy^{-1})(yz^{-1}) \in H \)
\[\text{or } x(y^{-1}y)z^{-1} \in H\]
\[\text{or } x(e)z^{-1} \in H\]
\[\text{or } xz^{-1} \in H\]
\[\Rightarrow x \sim yz \quad \text{i.e. } \sim \text{ is transitive.}\]

Hence the relation \( \sim \) is equivalence.
# Cyclic Group

A group $G$ is called a cyclic group if all of its elements can be expressed as powers of a single element say $a \in G$.

In this case, $a$ is called a generator of $G$. i.e. if $a$ is a 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 $G = \{a, a^2, a^3, \ldots, a^{n-1}, a^n = e_G\}$.

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

E.g.

$$\mathbb{Z}_\pm = \{\pm 1, \pm 2, \ldots\}$$

Let $a = i$, then:

$$a^2 = i^2 = -1$$
$$a^3 = i^3 = i \cdot i^2 = -i$$
$$a^4 = (i^2)^2 = 1$$

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

Any two cyclic group of same order are isomorphic.

Proofs-

1) For finite order:

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

Consider cyclic group \( C_n \) of \( n \) th roots of unity. Consider a mapping \( \Phi : G \rightarrow C_n \) defined by

\[ \Phi(a^k) = e^{\frac{2\pi k}{n}i} \]

- \( \Phi \) is one-one

For \( \Phi(a^k) = \Phi(a^m) \); \( a^k, a^m \in G \)

\[ e^{\frac{2\pi k}{n}i} = e^{\frac{2\pi m}{n}i} \]

\[ \frac{2\pi k}{n} = \frac{2\pi m}{n} \]

\[ k = m \]

Thus \( \Phi \) is one-one

\[ \Phi \] is obviously onto, where

\[ e^{\frac{2\pi k}{n}i} \]

For every \( e^{\frac{2\pi k}{n}i} \), where \( k = 0, 1, 2, \ldots, n-1 \)

\[ a^k \in G \ \forall \ k \]

- Now, \( \Phi(a^k a^m) = \Phi(a^{k+m}) \)

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

\[ = e^{\frac{2\pi k}{n}i} e^{\frac{2\pi m}{n}i} \]

\[ = \Phi(a^k) \cdot \Phi(a^m) \]

\[ \Rightarrow \Phi\] is homomorphism i.e. \( G \subseteq C_n \)

ii) For infinite order:

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

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

$\Rightarrow k = m$

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

And also for each $k \in \mathbb{Z}$ there is an element $a^k \in G$ such that $\phi(a^k) = k$

$\Rightarrow \phi$ is onto.

Also

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

$= k + m$

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

$\Rightarrow \phi$ 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 $G = \langle a : a^n = e \rangle$

$d \mid n \Rightarrow \exists$ 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 that $k \mid n$.

As $K$ has order $d$

$\Rightarrow a^{kd} = a^d = e$

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 subgroup of $G$, and $k$ be the least positive integer such that $a^k \in H$.

We prove that $H$ is generated by $a^k$.

For this, let $x = a^m \in H$ for $m > k$.

Then $x$ and $(a^k)^r$ are in $H$.

We have $a^m = a^{qk + r}$ for some integers $q$ and $r$ such that $0 \leq r < k$.

Thus, $a^m \cdot a^{-qk} = a^r$.

Therefore, $a^r \in H$.

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 $m = qk$.

Thus, $a^m = (a^k)^q$.

Therefore, $a^k$ is generator of $H$, i.e. $H$ is cyclic.

# Theorem:

The homomorphich image of a cyclic group is cyclic.

Proof:

Let $G$ be a cyclic group generated by $a$.

Let $\phi(G)$ be a homomorphich image of $G$ under a homomorphism $\phi$. 

[21]
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

\[
x = \varphi(a^k) = \varphi(a) \cdot \varphi(a) \cdot \varphi(a) \cdots \varphi(a) \quad \text{(k times)}
\]

\[
= b \cdot b \cdot b \cdots b \quad \text{(k times)}
\]

So \( \varphi(G) \) is generated by \( b \).

hence \( \varphi(G) \) is cyclic.
# Theorem:

1) 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.

2) If $G$ is an infinite cyclic group then $a$ and $a^l$ are its generators only.

Proof:

Let $G = \langle a : a^n = e \rangle$ be a 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 $H = G$,

$a^l = a^{pk + qn}$

$= (a^k)^p \cdot (a^n)^q$

$= (a^k)^p \cdot (e)^q$

$= (a^k)^p$

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

$\therefore a^k$ is generator.

So for some integer $p$.

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

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

$\Rightarrow n \mid pk - 1$ $\therefore n$ is least such integer.

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 $p$.
\[ a^{kp-1} = e \]
\[ \Rightarrow kp - 1 = 0 \quad \text{or} \quad kp - 1 = 0 \]
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 $k = p = -1$
\[ \text{i.e. } a, a^{-1} \text{ are only generators.} \]

# Complex in a group:
\[ \text{def.} - \text{A subset } X \text{ of a group } G \text{ is called complex in } G \]

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

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

******************************************************************************

[24]
# Theorem

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

**Proof.**

Let $HK$ be a subgroup.

Let $h, k_1 \in HK$ for $h \in H$, $k_1 \in K$.

Then $(h^{-1} k_1)^{-1} \in HK$ i.e. $HK$ is a subgroup.

Now $(h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$.

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

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

$kh = (k^{-1})^{-1}(h^{-1})^{-1} = (h^{-1} k^{-1})^{-1} \in HK$ as $HK$ is subgroup.

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

From \(\text{(i)}\) and \(\text{(ii)}\).

$HK = KH$.

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

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

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

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

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

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

$= (h_1 h_2^{-1}) k_2$ for $h_1, h_2 \in H$, $h_3 = h_1 h_2^{-1} \in H$

$= h_3 k_2 \in HK$.

Therefore $HK$ is a subgroup.

**Question.** If $H$ is a subgroup of group $G$ then

i) Prove that $H^2 = H$

ii) Prove that $H^{-1} = H$ \(\text{Do yourself}\)
Theorem: -

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

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

Proof:

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

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

$$h_1 k_1 = h_2 k_2$$

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

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

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

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

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

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

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

$$\Rightarrow g = e$$

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

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

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

which is a contradiction.

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

Or

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

\[ H = \{ 1, \omega, \omega^2 \} \]

\[ k = \{ \pm 1, \pm i \} \text{ are two subgroups of } G \]

\[ HNK = \{ 1 \} \]

Then

\[ HK = \{ \pm 1, \pm i, \pm \omega, \pm \omega^2, \pm \omega^3, \pm \omega^4 \} \]

Question:

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

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

prove that \( G \) is a group.
# Theorem:

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

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

**Proof:**

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

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

$$= \{x_1, x_2, x_3, \ldots, x_r\} \quad \text{(say)}$$

Also $O(HNK) = r$

so let $HNK = \{y_1, y_2, y_3, \ldots, y_r\}$

- Each $y_i \in HNK \quad \forall i = 1, 2, \ldots, r$

and $HNK$ is a subgroup of $G$.

- $y_i^{-1} \in HNK \quad \forall i = 1, 2, \ldots, r$

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

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

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

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

but $(hy_i)(y_i^{-1}k) = (hy_1)(y_1^{-1}k) = (hy_2)(y_2^{-1}k) = \ldots \ldots \ldots$ $= (hy_r)(y_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. $rm = pq$

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

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

proved.
# Corollary:

Let $H$ and $K$ are subgroups 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:**

\[ o(H) \geq \sqrt{o(G)}, \quad o(K) \geq \sqrt{o(G)} \]

as $H$ and $K$ are subgroups of $G$

\[ H \subseteq G, \quad K \subseteq G \]

\[ HK \subseteq G \]

\[ o(HK) < o(G) \]

i.e.

\[ o(G) > o(HK) \]

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

\[ > \sqrt{o(G) \cdot \frac{o(G)}{o(H \cap K)}} \]

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

\[ \Rightarrow o(H \cap K) \geq 1 \]

\[ \Rightarrow H \cap K \neq \{e\} \]
Groups: Handwritten notes

# Coset:

defn: Let $H$ be a subgroup of a group $G$, then the set $Ha = \{aha : h \in H\}$ 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 $G = \{e, f, g, g^2, f^2, g^3\}$ be a group where $f^3 = e$, $g^3 = e$, $(fg)^2 = e$.

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

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

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

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

As $(fg)^2 = e$

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

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

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

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

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

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

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

i.e. we have only two disjoint right coset.

# Index of Subgroup:

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

[30]
Index of subgroup:

**Definition:** 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:** \( [G : H] = \frac{|G|}{|H|} \) (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 \( a_1H, a_2H, \ldots, a_kH \) be the distinct left cosets of \( H \) in \( G \).

We prove
\[
G = \bigcup_{i=1}^{k} a_iH \quad \text{and} \quad a_iH \cap a_jH = \emptyset, \quad i \neq j
\]

and \( i, j = 1, 2, \ldots, k \).

Let \( a_i \in G \),
then \( a_i = a_1e \in a_1H \) because \( e \in H \).

So, \( G \subseteq \bigcup_{i=1}^{k} a_iH \) (i)

Also, each \( a_iH \) is a subset of \( G \).

\[
\therefore \bigcup_{i=1}^{k} a_iH \subseteq G \quad \text{(ii)}
\]

From (i) and (ii),
\[
G = \bigcup_{i=1}^{k} a_iH.
\]

Next, let \( aH \) and \( bH \) be distinct left cosets and \( x \in aH \cap bH \).

Then \( x = ah_1 = bh_2 \) for some \( h_1, h_2 \in H \).

\[
\Rightarrow a = bh_2h_1^{-1} = bh_3, \quad \text{where} \quad h_3 = h_2h_1^{-1} \quad \text{(say)}.
\]

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.

\[ aH \cap bH = \emptyset, \]
\[ \Rightarrow \text{all left cosets of } H \text{ in } G \text{ define a partition.} \]
\[ \Rightarrow |G| = |a_1H| + |a_2H| + \ldots + |a_kH| \quad (iii) \]

To find the number of elements in each coset, we define a mapping \( \varphi : H \rightarrow a_iH \) by
\[ \varphi(h) = a_\varphi h, \quad h \in H. \]

for \( h_1, h_2 \in H \)
\[ \varphi(h_1) = \varphi(h_2) \]
\[ \Rightarrow a_\varphi h_1 = a_\varphi h_2 \]
\[ \Rightarrow h_1 = h_2 \]
\[ \Rightarrow \varphi \text{ is one-one.} \]

Also for each \( a_iH \in \{ a_iH \} \), \( \exists h \in H \)
so \( \varphi \) 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
\[ n = m + m + \ldots + m \quad (k \text{ times}) \]
\[ \Rightarrow n = km \]
\[ \Rightarrow k \mid n \text{ and } m \mid n \]
i.e. order and index of subgroup divides
order of group.
Double Cosets:

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

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

is called coset of module $(H, K)$.

Theorem:

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

Proof:

Let $H_aK$ be a collection of all double cosets of $H$ and $K$ in $G$.

We have to prove

$$G = \bigcup (H_aK) \text{ and } H_aK \cap H_bK = \emptyset.$$ 

Since each $H_aK \subseteq G$,

$$\Rightarrow \bigcup (H_aK) \subseteq G \quad (i)$$

If $a \in G$ then $eae \in H_aK$

$$\Rightarrow a \in H_aK$$

i.e.

$$\Rightarrow G \subseteq \bigcup (H_aK) \quad (ii)$$

From (i) and (ii)

$$G = \bigcup (H_aK)$$

Now consider $H_aK$ and $H_bK$ are two distinct double cosets.

Let $x \in (H_aK) \cap (H_bK)$.

$$\Rightarrow x \in H_aK \text{ and } x \in H_bK$$

$$\therefore x = hak \text{ and } x = h_bk_l$$

$$\Rightarrow hak = h_bk_l$$

$$\Rightarrow ak = h^{-1}h_bk_l$$

$$\Rightarrow a = h^{-1}h_bk_lk_1$$
if \( \gamma \in H a K \)
then \( \gamma = h_2 a k_2 \)
\[ = h_2 h' h_1 b k_1 k' k_2 \in H b K \]
\[ \Rightarrow \gamma \in H b K \]
\[ \Rightarrow H a K \subseteq H b K \]

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 \( H a K \cap H b K = \phi \)

The proof is complete.

# Normalizer

**Definition:** Let \( X \) be a subset of a group \( G \), then the set \( N_g(X) = \{ a : a \in G, ax = xa \} \)

is called the 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 \( bx = xb \).

\[ bx = xb \]
\[ \Rightarrow (bx)b^{-1} = (xb)b^{-1} \]
\[ \Rightarrow b(xb^{-1}) = x(bb^{-1}) \]
\[ b(xb^{-1}) = x \]
\[ xb^{-1} = b^{-1}x \]
\[ b^{-1} \in N_G(x) \]

Now
\[ a b^{-1}(x) = a(b^{-1}x) = a(x b^{-1}) \]
\[ = a(x b^{-1}) = (a x) (b^{-1}) = (xa) b^{-1} = x (ab^{-1}) \]
\[ \Rightarrow ab^{-1} \in N_G(x). \]

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 \( hH = H = Hh \) \( \Rightarrow aH = H \Leftrightarrow a \in H \)

i.e. \( hH = Hh \)

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

So \( H \subseteq N_G(H) \).

**Note:**
The above corollary can also be stated as

"Normalizer of a subgroup contains that subgroup."

Also converse of above corollary may not be true.
**Centralizer**

Let \( X \) be a subset of a group \( G \) and \( \forall x \in X \), then the set

\[
C_G(X) = \{ a : a \in G \land ax = xa \}
\]

is called the centralizer of \( X \) in \( G \).

**Centre of \( G \)**

The centralizer of \( G \) in \( G \) is called the 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, \( \forall x \in X \)

\[
ax = xa \quad (i)
\]

\[
bx = xb \quad (ii)
\]

From (ii)

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

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

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

\[
\Rightarrow xb^{-1} = b^{-1}x \quad (iii)
\]

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:

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) Reflexive
\[ a = ea = eae^{-1}, e \in G \Rightarrow a \sim a. \]

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 \( g^{-1} \in G \).
\[ \Rightarrow b \sim a \Rightarrow \sim \text{ is symmetric}. \]

iii) Transitive
Let \( a \sim b \) and \( b \sim c \)
\[ \Rightarrow b = g_{1}a(g_{1})^{-1} \] and \( c = g_{2}b(g_{2})^{-1} \) for \( g_{1}, g_{2} \in G \).
Since
\[ c = g_{2}b(g_{2})^{-1} \]
\[ = g_{2}(g_{1}a(g_{1})^{-1})g_{2}^{-1} \]
\[ = (g_{2}g_{1})a(g_{1}g_{2})^{-1} \]
\[ = (g_{2}g_{1})a(g_{2}g_{1})^{-1} \]
\[ \Rightarrow a \sim c. \]

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 subsets i) \( X = \{1, a^2 \} \) ii) \( X = \{1, a, a^2, a^3 \} \)

Find centralizer of \( X \).

Solution:

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

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

\[ a^4 = 1 \quad b^2 = 1 \]

\[ a^4 = a^3 \quad \Rightarrow \quad b^{-1} = b \]

\[ (ab)^2 = 1 \quad \Rightarrow \quad (ab)^2 = 1 \]

\[ (ab)(ab) = 1 \quad \Rightarrow \quad (ab)(ab) = 1 \]

\[ ab = b^{-1}a^{-1} \quad \Rightarrow \quad a(ba)b = 1 \]

\[ = ba = a^3b \]

\( C_G(X) \) 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 \( b \)

\[ b \cdot 1 = b = 1 \cdot b \]

\[ b \cdot a^2 = a^2 b \quad (ba) \quad a = (a^2 b) a = a^3 (ba) \]

\[ a = a^3 (a^2 b) = a^4 b = a^4 (a^2 b) = a^4 b \]

For \( ab \)

\[ (ab) \cdot 1 = ab = 1 \cdot (ab) \]
(ab).a^2 = (ba^3).a^2 = ba^5 = (ba).a^4 = ba

= a^3b = a^2(ab).

For a^3b

(a^3b).a^2 = (ba).a^2 = ba^3 = ab

a^2.(a^3b) = a^5b = a^4(ab) = ab

\Rightarrow (a^3b)a^2 = a^2.(a^3b)

For a^2b

(a^2b).1 = 1.(a^2b)

(a^2b).a^2 = a(ab)a^2 = a(ba^3)a^2

= a(ba) = a(a^3b) = a^4b = a^2.(a^2b)

As all element of G commute with element of X therefore Cg(x) = G.

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

ba \neq ab \text{ so } b \text{ does not commute with } a.

a^2(ab) = a^3b \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)^3 = e \rangle

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

# Exercise.

Find NG(G) \cap N_G(x) \text{ if } G = D_8

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

Ans: i) G

ii) \{1, a, a^2, a^3\}
# Remarks

- Let \( b = g a g^{-1} \Rightarrow a = g^{-1} b (g^{-1})^{-1} \)
  \[ b^m = (g a g^{-1})^m = g a^m g^{-1} \quad \text{and} \quad a^m = g^{-1} b^m (g^{-1})^{-1} \]

\[ \text{i.e.} \quad a^m = e \iff b^m = e \]
\[ \text{i.e. order of} \quad a \quad \text{and} \quad b \quad \text{is same.} \]

- If \( \exists x \in \{ x \} = \text{singleton set} \)
  then \( C_G(x) = N_G(x) \).

# Self-Conjugate:

- An element \( a \in G \) is called self-conjugate if for \( g \in G \), \( a = g a g^{-1} \).
  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 \( x = g a g^{-1} \),

\[ xg = gx \]
\[ \Rightarrow x \in C_G(G). \]

Conversely,

Let \( x \in C_G(G) \),

\[ xg = gx \]
\[ \Rightarrow x = g^{-1} x g^{-1} \]
\[ \Rightarrow x \text{ is self conjugate.} \]

# Conjugancy Class

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

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

Then we have to prove that the number of elements in $A$ is equal to the number of elements in $C_a$.

Define a mapping

$$\varphi: A \rightarrow C_a$$

by $\varphi(Ng) = g'ag$, $g \in G$.

i) $\varphi$ is well defined

Let $N_1 = N_{g_1}$ where $g_1, g_2 \in G$

$$\Rightarrow N = \bigoplus N_{g_2}$$

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

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

Now

$$g_2 a g_2 = (ng_1^{-1})a (ng_1)$$

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

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

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

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

$$\Rightarrow \varphi$$ is well defined.

ii) $\varphi$ is onto as to every $g'ag \in C_a$, we have right coset $Ng$. 

[41]
\[ \text{iii), } \phi \text{ is one-one} \]
\[ \phi(Ng_1) = \phi(Ng_2) \]
\[ \Rightarrow g_1\phi g_1 = g_2\phi g_2 \]
\[ \Rightarrow g_1 (g_1^{-1} a g_1) g_2 = a \]
\[ \Rightarrow (g_2 g_1^{-1}) a (g_1 g_2^{-1}) = a \]
\[ \Rightarrow (g_2 g_1^{-1}) a (g_1 g_2^{-1}) = a \]
\[ \Rightarrow g_1 g_2 \in N \]
\[ \Rightarrow g_1 \in Ng_2 \text{ but } g_1 \notin Ng_1 \]
\[ \Rightarrow Ng_1 \subseteq Ng_2 \]

Similarly
\[ Ng_1 \subseteq Ng_1 \]
\[ \Rightarrow Ng_1 = Ng_2 \text{ so } \phi \text{ is one-one} \]
\[ \Rightarrow \phi \text{ is bijective} \]

i.e. no. of elements in \( A \) = no. of elements in \( Ca \)
\[ \Rightarrow \text{no. of elements in } Ca \text{ is equal to the no. of right cosets of normalizer of } z \text{, and since by Lagrange's theorem index (no. of right cosets) divides order of the group } G. \]

+ Review:

Let \( a \in G \), then the subset of all elements of \( G \) conjugate to \( a \) is called conjugacy class
i.e. \( Ca = \{ b \in G \mid b = g a g^{-1}, g \in G \} \).

If \( X = \{ a \} \) then
\[ Ng(X) = C(a)(X) \]
i.e. Normalizer of \( X \) in \( G \) = Centralizer of \( X \) in \( G \).
\# Class Equation

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 \( n = |C_1| + |C_2| + \cdots + |C_r| \) \( \quad (i) \)

i.e. \( n = m_1 + m_2 + \cdots + m_r \)

where each \( m_i \) divides \( n \).

Then equation \((i)\) is called class equation.

\# P-Group

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 \( p^k \).

i.e. \( p^k, p^{k+1}, \ldots, p^n \)

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 only that element i.e. \( a \) is self-conjugate then \( C_a = \{a\} \)
but if \( b \in C_a \), then \( b = g a g^{-1} \)
\[ \Rightarrow b g = g a \]
\[ \Rightarrow b g = a g \quad \therefore \text{a is self-conjugate} \]
\[ \Rightarrow b = a \]

Let such classes of the above two types be \( k \).
Without loss of generality these are
\[ m_1, m_2, \ldots, m_k \]

Now
\[ p^n = m_1 + m_2 + \ldots + m_k + m_{k+1} + m_{k+2} + \ldots + m_r \]
\[ = 1 + 1 + \ldots + 1 + m_{k+1} + m_{k+2} + \ldots + m_r \]
\[ k = p^n - (\sum_{z=k+1}^{r} p^\alpha_z) \]
\[ \Rightarrow k = p^n - \sum_{z=k+1}^{r} p^\alpha_z \]

Now \( p \mid p^n \) and \( p \mid p \alpha_z \) for each \( z = k+1, k+2, \ldots, r \)
\[ \Rightarrow p \mid p^n - \sum_{z=k+1}^{r} p^\alpha_z \]
\[ \text{i.e. } p \mid k \]
\[ \Rightarrow \text{centre of } p\text{-group is non-trivial} \]

# Alternative Statement
\[ \text{Order}_{p^n} \]
- Every group of \( p^n \) has non-trivial centre.
- Every finite \( p \)-group has non-trivial centre.
Conjugate Subgroup

Let $H$ be a subgroup of a group $G$. Define a set

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

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 a 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

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

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

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

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

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

$\therefore h_1, h_2 \in H$ and $H$ is a 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 a subgroup

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

[45]
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 \( \phi \) :
\[
\phi : H \to K \quad \text{by} \quad \phi(h) = k
\]

i) Then \( \phi \) is onto
\[ k \in K \quad \text{is image of} \quad h \in H \quad \text{as} \quad k = ghg^{-1} \]

ii) \( \phi \) is one-one
\[
\phi(h_1) = \phi(h_2) \implies k_1 = k_2 \implies gh_1g^{-1} = gh_2g^{-1} \implies h_1 = h_2 \implies \phi \text{ is bijective mapping.}
\]

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

\[
\phi(h_1h_2) = gh_1h_2g^{-1}
\]
\[
= (gh_1)(h_2)g^{-1}
\]
\[
= (gh_1)g^{-1}g(h_2)g^{-1}
\]
\[
= (gh_1)g^{-1}(gh_2)g^{-1}
\]
\[
= \phi(h_1)\phi(h_2)
\]

\( \implies \phi \text{ is homomorphism} \)

\( \therefore \phi \text{ is bijective} \)

\( \therefore H \text{ and } K \text{ are isomorphism.} \)
# Theorem

If $H$ and $K$ are finite subgroups of a group $G$, then each double coset $H a K$ contains $\frac{m n}{q}$ number of elements,

where $\theta(H) = m$, $\theta(K) = n$ and $\theta(G) = q$

with $Q = H n a K$.

Proof:

If $H$ and $K$ are finite subgroups of $G$, so number of elements in $H a K$ is also finite.

Let $H a K = \bigcup_{i=1}^{r} g_i a K = \bigcup_{i=1}^{r} g_i a K$, $r < n$.

Then $H a K \subseteq G$

Then each $g_i a K$ is distinct but for $i \neq j$ if $g_i a K = g_j a K$.

Define mapping $\phi: H a K \rightarrow H a K$

by $\phi(h a k) = h a k$.

$\Rightarrow |H a K| = |H a K| \quad (i)$

Also let $a K = K'$ then number of elements in $K$, being conjugate to $K$, is $n$.

Now $|H a K| = |H K'|$

$\Rightarrow \frac{|H| \cdot |K'|}{|H a K|} = \frac{m n}{q}$

where $|H n K| = |Q| (\text{say})$; $|Q| = q \quad (\text{say})$

where $Q = H n K = H n a K$.

By (i) and (ii)

$|H a K| = \frac{m n}{q}$ proved.
# Theorem

- Let $H$ and $K$ be subgroups of a group $G$, $HAK$ is a double coset and $Q = HAK\bar{a}_{1}$

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 $H$,

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

Then $\phi$ is well defined.

As $hAK = h'K$,

$\Rightarrow hAK = h'AK$ for $k, k' \in K$.

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

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

$\Rightarrow h \in h'Q$ 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 $\phi$ is well defined.

$\phi$ 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

$\Rightarrow h^{-1}h = aK\bar{a}_{1}$

$\Rightarrow h = hAK \in hAK$.

*Also $h = hae \in hAK$.

$\Rightarrow hAK$ and $h'AK$ are not disjoint.

$\Rightarrow hAK = h'AK$.

Also $\phi$ is onto obviously.

So there is one-one correspondence between

$Q = HNK\bar{a}_{1}$ elements of $A$ and $B$. 

[48]
# Normal Subgroup

Define: Let $H$ be a subgroup of a group $G$. If $a'Ha = H$ for $a \in G$, or $a'ha \in H$ for $h \in H$, $a \in G$, then $H$ is called normal subgroup.

and we write $H \triangleleft G$.

Note: If $a'ha \in H$ then $a'ha = h_1 \Rightarrow ha = ah_1$.

# 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 $ab' \in \ker \phi$.

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

$\phi$ is homomorphism,

$= I_H \cdot (\phi(b'))^{-1}$.

$= \phi(a) \cdot I_H$.

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

$= I_H$.

$\Rightarrow ab' \in \ker \phi$.

Let $k \in \ker \phi$.

To prove $gkg' \in \ker \phi$, $g \in G$,

$\phi(gkg') = \phi(g) \cdot \phi(k) \cdot \phi(g')$.

$\phi$ is homomorphism,

$= \phi(g) \cdot I_H \cdot \phi(g')$.

$= \phi(g) \cdot \phi(g')$.

$= \phi(gg')$.

$= \phi(e) = I_H$.

$\Rightarrow gkg' \in \ker \phi$.

$\Rightarrow \ker \phi$ is normal subgroup.
Theorem

: If \( H \) and \( K \) are normal subgroups of \( G \) with \( HK = \{ e \} \), show that every element of \( H \) commutes 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 \( hk h^{-1} k^{-1} \).

As \( H \) is normal subgroup of \( G \),

\[ hk h^{-1} k^{-1} \in H \quad \text{for} \quad h \in H, \quad k \in K \subseteq G, \]

\[ h(kh h^{-1} k^{-1}) \in H \quad \text{by closure law as} \quad h \in H, \]

or \( hk h^{-1} k^{-1} \in H \).

Also \( K \) is normal subgroup of \( G \),

\[ hk h^{-1} k^{-1} \in K \quad \text{for} \quad k \in K, \quad h \in H \subseteq G. \]

\[ (hk h^{-1} k^{-1}) k \in K \quad \text{by closure law as} \quad k \in K, \]

\[ hk h^{-1} k^{-1} \in K. \]

\[ \therefore hk h^{-1} k^{-1} \in H \quad \text{and} \quad hk h^{-1} k^{-1} \in K. \]

\[ \therefore hk h^{-1} k^{-1} \in HK = \{ e \} \]

\[ \therefore hk h^{-1} k^{-1} = e \]

\[ \therefore hk = kh \quad \text{proved} \]

---

Corollary:

: Let \( G \) be an abelian group then each subgroup of \( G \) is normal in \( G \).

Proof:

Let \( H \) is a subgroup of \( G \),

\[ G \text{ is abelian} \quad \therefore ab = ba \quad \forall \ a, b \in G. \]

\[ \therefore ah = ha \quad \forall \ h \in H \text{ and } a \in G. \]

\[ \therefore h = a'ha \in H \]

Hence \( H \) is normal in \( G \).
Theorem

Let $H$ be a subgroup of a group $G$. Then the following are equivalent:

i) $H$ is a normal subgroup of $G$.

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

iii) $gH = Hg$.

Proof:

(i) $\Rightarrow$ (ii)

Let $H$ be a normal subgroup of $G$. Then $gHg^{-1} \subseteq H$, $g \in G$

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

If $h \in H$,

$h = (gg')h(gg')^{-1}
= g(g'hg)g'
= ghg' \in gHg'$

$\Rightarrow H \subseteq gHg' \quad (B)$

From (A) and (B)

$gHg' = H$

Now (ii) $\Rightarrow$ (iii)

i.e. $gHg' = H$

$\Rightarrow \forall g' h \in H', h, h' \in H$

or $h = g'h'g$

For $gh \in gH$,

$gh = g(g'hg')
= (gg'hg')g = eh'g
= h' \in Hg$

$\Rightarrow gH \subseteq Hg \quad (C)$

Likewise $gHg \subseteq gH \Rightarrow gH = Hg$.
(iii) \implies (i)

\[ gH = Hg \]

\[ gh = h'g \quad \text{for} \quad h, h' \in H \]

\[ ghg'^{-1} = h' \in H \]

\[ \Rightarrow H \text{ is normal subgroup of group } G. \]

\[ \text{Theorem} \]

\[ \Rightarrow \text{Every subgroup of index two is a normal subgroup.} \]

OR Let \( G \) be a group and \( H \) a subgroup of index two then \( H \triangleleft G \).

\[ \text{Proof:} \]

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 \( a \notin H \Rightarrow \) 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

\[ i.e. \quad G = H \cup Ha = H \cup aH \]

and

\[ H \cap Ha = aH \cap H = \emptyset. \]

\[ \Rightarrow aH = Ha \]

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

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

\[ \Rightarrow ahha'^{-1} = h' \in H \]

\[ \Rightarrow ahha'^{-1} \in H \]

\[ \Rightarrow H \triangleleft G. \]
# 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 $G$.

\[
Q = G/H = \{ Ha : a \in G \}
\]

is called the quotient group of $G$ by $H$.

We define multiplication in $Q$ by

\[
Ha \cdot Hb = Hab.
\]

This multiplication is well defined for $h_a, h_b \in H$.

For $h_1, h_2 \in H$,

\[
h_1h_2 = h_1(h_2a) = \begin{align*}
&= (h_1h_2) \cdot (ab) \quad \Rightarrow h_1h_2 \in H \\
&= h_1 \cdot (ah_2) \quad aH = Ha \\
&= h_1 \cdot h_a \quad \Rightarrow \alpha h_2 = h_2 \beta, h_1h_2 \in H
\end{align*}
\]

\[\Rightarrow Ha \cdot Hb = Hab.
\]

Also, $Q$ is a group:

- 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 $Q$

\[
\Rightarrow Ha \cdot H = Ha, He = Hae = Ha
\]

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

- iv) For $a \in G$ exists $a' \in G$ such that $Ha \cdot H a' = Ha a' = He = H$

also $H a' \cdot Ha = H a' a = He = H$

\[\Rightarrow Q \text{ contains inverse of each right coset}
\]

\[
\Rightarrow Q = G/H = \{ Ha : a \in G \}
\]

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

Proof:

\( \phi : G \to G/H \) is defined as

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

i) \( \phi \) is well defined as

\[ a = b, \quad a, b \in G \]

\[ Ha = Hb \]

\[ \Rightarrow \phi(a) = \phi(b) \]

ii) \( \phi \) is onto as

\( Ha \in G/H \) is an image of \( a \in G \) under \( \phi \).

iii) \( \phi \) 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 \( a \in H \subseteq G \)

\[ \phi(a) = Ha \]

\[ = H \]

\[ \therefore \text{identity of Quotient Group} \]

\[ \Rightarrow a \in \ker \phi \]

\[ \Rightarrow H \subseteq \ker \phi \quad \text{(i)} \]

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)

\[ \ker \phi = H \quad \text{proved} \]
Ist Isomorphism Theorem

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

**Proof:**

$\varphi : G \rightarrow G'$

$\Rightarrow \varphi(g) = g'$ for $g \in G$, $g' \in G'$

Define a mapping $\psi$ such that

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

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

then $\psi$ is well defined.

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

if $\bar{g}K = \bar{g}_1K$

$\Rightarrow K = \bar{g}_1g_1K$

$\Rightarrow \bar{g}_1g_1 \in K$

$\Rightarrow \varphi(g_1g_1) = e'$

$\Rightarrow \varphi(g_1) \varphi(g) = e'$ \quad \because \varphi$ is homomorphism

$\Rightarrow \varphi(g) \varphi(g_1) \varphi(g) = \varphi(g) e'$

$\Rightarrow \varphi(gg_1) \varphi(g) = \varphi(g) g'$

$\Rightarrow \varphi(e) \cdot g' = g'$

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

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

$\Rightarrow \psi$ is well defined.

ii) For $g' \in G'$

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

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

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

$\Rightarrow \psi$ is onto.
(iii) $\psi$ is one-one

As $\psi(gk) = \psi(g, k)$

$\Rightarrow \Phi(g) = \Phi(g)$

$\Rightarrow \Phi(g') \cdot \Phi(g) = \Phi(g') \cdot \Phi(g)$

$\Rightarrow \Phi(g'g) = \Phi(g'g)$ \quad \because \Phi \text{ is homomorphism}

$\Rightarrow \Phi(e') = \Phi(g'g)$

$\Rightarrow e' = \Phi(g'g)$ \quad \text{where } \Phi(e) = e'$

$\Rightarrow g'g \in K$

$\Rightarrow g'g, g \in G \Rightarrow g'g, g \in g'k$

$\Rightarrow gk = g'k$

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

(iv) To prove $\psi$ is homomorphism

For $gk, g', k \in G/K$

$\psi(gk \cdot g', k) = \psi(gg', k)$ \quad \text{by multiplication of quotient group}

$= \Phi(gg')$

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

$= \psi(gk) \cdot \psi(g')$

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

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

*******************************************************************************

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

*******************************************************************************

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

*******************************************************************************
# Theorem

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

**Proof:**

Let \( H' \) be normal subgroup of \( G' \) and \( H = \Phi^{-1}(H') = \{ h : \Phi(h) = h' \} \). Let \( h \in H, g \in G \) to prove \( ghg^{-1} \in H \)

\[
\Phi(ghg^{-1}) = \Phi(g) \cdot \Phi(h) \cdot \Phi(g^{-1}) = \Phi(ghg^{-1}) \in H' \quad \therefore H' \text{ is normal}
\]

\[ \Rightarrow \Phi(ghg^{-1}) \in H' \]

\[ \Rightarrow ghg^{-1} \in \Phi^{-1}(H') = H \quad \therefore \Phi \text{ is onto} \]

\[ \Rightarrow H \text{ is normal subgroup of } G \]

Conversely, let \( H \) is normal subgroup of \( G \).

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

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

\[ g' h' g'^{-1} = \Phi(g') \cdot \Phi(h') \cdot \Phi(g'^{-1}) = \Phi(ghg^{-1}) \]

\[ \therefore H \Delta G \Rightarrow ghg^{-1} \in H \]

\[ \Rightarrow \Phi(ghg^{-1}) \in H' \]

\[ \therefore g' h' g'^{-1} \in H' \]

\[ \Rightarrow H' \Delta G' \]

-------------------------------------------------------------------------------------

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

-------------------------------------------------------------------------------------
# 2nd Isomorphism Theorem

- Let $G$ be a group, $H$ a subgroup, and $K$ a normal subgroup of $G$ then,
  
  i) $HNK$ is a normal subgroup of $H$.
  
  ii) $HK$ is a subgroup of $G$.
  
  iii) $H/\text{HNK} \cong HK/K$.

**Proof:**

i) To prove $HNK$ is a normal subgroup

Let $x \in HNK$.

\[ \Rightarrow x \in H \text{ and } x \in K. \]

:: $K$ is normal subgroup.

\[ \Rightarrow hxh^{-1} \in K \text{ for } h \in H \subseteq G. \]

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

\[ \Rightarrow hxh^{-1} \in HNK. \]

\[ \Rightarrow HNK \text{ is normal subgroup}. \]

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

Note:

\[ x_1x_2^{-1} = (h_1k_1)(h_2k_2)^{-1} \]

\[ = (h_1k_1)(k_2^{-1}h_2) = h_1(k_1^{-1}k_2^{-1})h_2^{-1} \]

\[ = h_1k_3h_2^{-1} \text{ where } k_1k_2^{-1} \in K \]

\[ \Rightarrow \text{HK is subgroup of } G. \]

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

Define a mapping

\[ \varphi : H \rightarrow HK/K \]

by \[ \varphi(h) = hK \] (i)
then $\varphi$ is obviously well defined and onto.

Now

$$\varphi(h_1h_2) = h_1h_2K$$

$$= (h_1K)(h_2K) \quad \text{by multiplication in quotient group.}$$

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

i.e. $\varphi$ is homomorphism.

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

By 1st isomorphism theorem

$$H/\ker \varphi \cong \varphi(H) \quad \text{1st Isomorphism Th.}$$

$\varphi : G \to G'$ is epimorphism

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

then. $G/K \cong G'$

i.e. $G/\ker \varphi \cong \varphi(G)$

Now to prove $\ker \varphi = HNK$

Let $h \in \ker \varphi$

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

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

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

$\Rightarrow h \in HNK$ \quad \text{(ii)}

$\Rightarrow \ker \varphi \subseteq HNK$ \quad \text{(iii)}

Now let $x \in HNK$

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

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

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

$\Rightarrow x \in \ker \varphi$

$\Rightarrow HNK \subseteq \ker \varphi$ \quad \text{(iii)}

From (ii) and (iii)

$\ker \varphi = HNK$

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

$\Rightarrow H/HNK \cong HK/K$ \quad Q.E.D.
3rd Isomorphism Theorem

Let $H$ and $K$ are two normal subgroups of $G$ with $H \subseteq K$ then 
\[
\frac{G/H}{(K/H)} \cong \frac{G/K}{K/H}
\]

Proof

Since $H \triangleleft G$ and $H \subseteq K$ 
\[\Rightarrow H \triangleleft K\]

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

For $kH \in K/H$ and $gH \in G/H$ 
\[
(gH)kH(gH)^{-1} = (gH)(kH)(gH)^{-1}
\]
\[
= (gkH)(g'H)
\]
\[
= gkg'H \quad \text{by multiplication of quotient group.}
\]

\[\therefore K \triangleleft G \implies gkg \in K\]

so $gkg'H \in K/H$ 
\[\Rightarrow K/H \triangleleft G/H\]

Define a mapping $\varphi : G/H \rightarrow G/K$ 
by $\varphi(gH) = gK$ 
then $\varphi$ is clearly onto

Also $\varphi(g_1H, g_2H) = \varphi(g_1, g_2H)$
\[
= g_1, g_2K
\]
\[
= g_1K \cdot g_2K
\]
\[
\Rightarrow \varphi \text{ is homomorphism.}
\]

$\varphi$ is epimorphism as it is onto and homomorphism.

by 1st isomorphism theorem 
\[
\frac{G/H}{\ker \varphi} \cong G/K
\]
if $\varphi : G \rightarrow G'$ is epimorphism then 
\[
G/\ker \varphi \cong G'
\]
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)

$\ker \phi = K/H$

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

$\therefore (G/H)_{(K/H)} \cong G/K$

proved
Groups: Handwritten notes

# Endomorphism:

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

The set of all 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 a homomorphism, if the mapping $\alpha$ is bijective then $\alpha$ is called an automorphism.

i.e. $\alpha : G \rightarrow G$ is an automorphism if
i) $\alpha$ is a homomorphism
ii) $\alpha$ 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) Let $\alpha, \beta \in A(G)$, then since $\alpha, \beta$ are bijective mappings, so their product (composition) $\alpha \beta$ is also bijective mapping.

and for $g_1, g_2 \in G$

$$\alpha \beta(g_1g_2) = \alpha (\beta(g_1)\beta(g_2))$$

$\because \beta$ is hom. 

$= \alpha (\beta(g_1)) \cdot \alpha (\beta(g_2))$ \because $\alpha$ is hom.

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

$\Rightarrow \alpha \beta$ is homomorphism $\Rightarrow \alpha \beta \in A(G)$.
ii) Since mappings are associative in general, therefore associative property holds in $A(G)$.

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

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

i.e. $\alpha I = \alpha$.

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

iv) To prove for $\alpha \in A(G)$ $\exists \tilde{\alpha}' \in A(G)$

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

i.e. $\tilde{\alpha}' : G \rightarrow G$ is also bijective.

$$\tilde{\alpha}' (g_1, g_2) = \tilde{\alpha}' (I(g_1, g_2))$$

$$= \tilde{\alpha}' (I(g_1) \cdot I(g_2))$$

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

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

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

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

$\Rightarrow \tilde{\alpha}'$ is homomorphism $\Rightarrow \tilde{\alpha}' \in A(G)$.

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 \( \Phi_a : G \rightarrow G \) by

\[
\Phi_a(g) = a^{-1}ga
\]

then \( \Phi_a \) is automorphism.

Proof:

i) \( \Phi \) is onto.

For \( g \in G \), \( a \in G \) we have \( aga^{-1} \in G \)

then \( g \) is image of \( aga^{-1} \) under \( \Phi \)

\[
\Phi_a(aga^{-1}) = a^{-1}(aga^{-1})a
\]

\[
= (a^{-1}a)g(a^{-1}a)
\]

\[
= g
\]

\( \Rightarrow \ \Phi \) is onto.

ii) \( \Phi \) is one-one

\[
\Phi_a(g_1) = \Phi_a(g_2)
\]

\( \Rightarrow \ a^{-1}g_1a = a^{-1}g_2a \)

\( \Rightarrow \ g_1 = g_2 \)

iii) \( \Phi \) is homomorphism

\[
\Phi_a(g_1g_2) = \Phi_a(g_1)\Phi_a(g_2)
\]

\[
= a^{-1}g_1(a^{-1}g_2)a
\]

\[
= (a^{-1}g_1a)(a^{-1}g_2a)
\]

\[
= \Phi_a(g_1)\Phi_a(g_2)
\]

Hence \( \Phi_a \) is automorphism.
# Inner and Outer automorphism

The set $I(G)$ or $\text{Inn}(G)$ 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 $\text{Aut}(G)$.

**Proof**

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

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

Now

$\phi_b \cdot \phi_b^{-1}(g) = \phi_b \left( b^{-1}g \left( b^{-1}\right)^{-1} \right)$

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

$= b \left( b^{-1}gb \right) b^{-1}$

$= (bb^{-1})g \left( b^{-1}b^{-1} \right)$

$= e \cdot e^{-1}$

$= \phi_e$

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

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

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

$= \phi_a \phi_b^{-1}(g) = \phi_a \left( b^{-1}gb \right)$

$= a \left( b^{-1}gb \right) a^{-1}$

$= (ab^{-1})g \left( ba^{-1} \right)$

$= (ab^{-1})g \left( ab^{-1} \right)^{-1}$

$= \phi_{ab^{-1}} \in I(G)$

$\Rightarrow I(G)$ is a subgroup.
Let \( \varphi_a \in I(G) \), \( \alpha \in A(G) \).

Now
\[
\alpha \varphi_a \alpha^{-1}(g) = \alpha \varphi_a (\alpha^{-1}(g)) = \alpha \left( \varphi_a (\alpha^{-1}(g)) \right) = \alpha (\alpha^{-1}(g)) \cdot \alpha^{-1} = \alpha \cdot \alpha^{-1} = 1 \text{, since } \alpha \text{ is } \text{hom}. \]
\[
= \alpha (\alpha) \cdot g \cdot (\alpha(g))^{-1} \quad \text{since } \alpha \text{ is } \text{bijective}.
\]
\[
\varphi_{\alpha(g)} \in I(G) \quad \text{i.e. } \alpha \varphi_a \alpha^{-1} \in I(G).
\]

Hence \( I(G) \subseteq A(G) \).

*****************************************************************************

Available online 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 $\psi(a) = \phi_a$ where $a \in G$, $\phi_a \in I(G)$.

i) Then $\psi$ is well defined.

If $a = b$, then $\phi_a = \phi_b$.

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

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

Therefore, $\psi(a) = \psi(b)$.

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

iii) $\psi$ is homomorphism as $\psi(ab) = \phi_{ab}$

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

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

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

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

$= \phi_a(\phi_b) = \phi_a \circ \phi_b$ (composite function)

$\Rightarrow \psi(a) \circ \psi(b) = \psi(ab)$.

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

Now by first isomorphism theorem $G/\ker\psi \cong I(G)$. If $\psi : G \rightarrow G'$ is epimorphism then $G'/\ker\psi \cong G'$. 

[67]
To prove \( \ker \psi = e(G) \).

Let \( \ker \psi = \{ a : a \in G \land \psi(a) = e_{F} \} \)

\[ = \{ a : a \in G \land \varphi_{a} = e_{F} \} \]

\[ = \{ a : a \in G \land aga^{-1} = eg e^{-1} \} \]

\[ = \{ a : a \in G \land aga^{-1} = g \} \]

\[ = \{ a : a \in G \land ag = ga \} \]

\[ = e(G) \]

\[ \Rightarrow \frac{G}{e(G)} \cong I(G) \]

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
  - Check out all these at

[68]
# Theorem:

Let \( \phi : G \to G \) by \( \phi(x) = x' \) then \( \phi \) is an automorphism iff \( G \) is abelian.

**Proof.**

Let \( G \) be abelian

\[
\phi(g_1g_2) = (g_1g_2)^{-1}
\]

\[
= g_2^{-1}g_1^{-1}
\]

\[
= g_1^{-1}g_2^{-1} \quad \therefore G \text{ is abelian}
\]

\[
= \phi(g_1) \cdot \phi(g_2)
\]

\( \Rightarrow \phi \) is homomorphism

\( \phi \) is onto because each \( g \in G \) we have

\[
\phi(g') = (g')^{-1} = g
\]

\( \phi \) is one-one

\[
\phi(g_1) = \phi(g_2)
\]

\( \therefore g_1^{-1} = g_2^{-1} \quad \therefore g_1 = g_2 \)

\( \Rightarrow \phi \) is an automorphism.

Conversely, let \( \phi \) is automorphism i.e. \( \phi \) is homomorphism

\[
\phi(g_1g_2) = \phi(g_1) \cdot \phi(g_2)
\]

\( \Rightarrow (g_1g_2)^{-1} = g_1^{-1}g_2^{-1} \)

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

\( \Rightarrow g_1g_2 = g_2g_1 \)

\( \Rightarrow G \) is abelian.
Groups: Handwritten notes

# 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 the 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) $[ab, c] = [b, c]^a [a, c]$ \[ [b, c]^a = a [b, c] a^{-1} \]

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

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

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

Proof:

$[a, b] [b, a] = (ab a^{-1} b') (ba b' a^{-1})$

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

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

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

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

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

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

ii) $[ab, c] = (ab) c (ab)^{-1} c^{-1}$

$= a b c b' a^{-1} c^{-1}$

$= a b c b' c^{-1} e a^{-1} c^{-1}$

$= a b c b' c^{-1} e c a^{-1} c^{-1}$

$= a b c b' c^{-1} a^{-1} a c^{-1} c^{-1}$

$= a b c b' c^{-1} a^{-1} c^{-1} c^{-1}$

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

$= [b, c]^a [a, c]^{-1}$ proved

iii) $[a, bc] = a (bc) a^{-1} (bc)^{-1}$

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

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

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

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

[70]
\[ (a \bar{a}' b') b (a c \bar{a}' c') b^{-1} = [a, b][a, c]^b \quad \text{proved} \]

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

And
\[ [\bar{a}', b] = \bar{a}' b (\bar{a}')^{-1} b^{-1} \]
\[= \bar{a}' b a b' \bar{a}' \bar{a} \]
\[= \bar{a}' b (b a b' \bar{a}') a \]
\[= \bar{a}' (b a b' \bar{a}') (\bar{a}')^{-1} \]
\[= [b, a] \bar{a}' \quad \text{proved} \]

---

# 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.

\[ G' = \langle x_1, x_2, \ldots, x_n \rangle \]

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 \( G/K \)

\[ \text{is abelian then } G \leq K. \]

Proof:

To prove \( G' \triangleleft G \), let for \( g \in G \)
\[ g [a; b] g' = g (a b \bar{a}' b') g' \]
\[ = g a b a^l b^l g^{-1} \]
\[ = g a g^{-1} g b g^{-1} g a^l g^{-1} g b^l g^{-1} \]
\[ = (g a g^{-1})(g b g^{-1})(g a^l g^{-1})(g b^l g^{-1}) \]
\[ = (g a g^{-1})(g b g^{-1})(g a g^{-1})^{-1}(g b g^{-1})^{-1} \]
\[ = a g b a^l (a g^{-1})^{-1} (b g^{-1})^{-1} = [a g, b g] \in G' \]
\[ \Rightarrow G' \text{ is normal subgroup of } G. \]

ii) Let \( a G' , b G' \in G / G' \) where \( a, b \in G \)

\[ [a G', b G'] = (a G')(b G')(a G')^{-1}(b G')^{-1} \]
\[ = (a G')(b G')(a^{-1} G')(b^{-1} G') \]
\[ = (a b a^{-1} b^{-1}) G' \text{ by multiplicative of quotient group} \]
\[ = [a, b] G' \]
\[ = G' \quad \therefore [a, b] \in G' \]
\[ = \text{Identity of Quotient group} \]
\[ \Rightarrow a b a^{-1} b^{-1} = e \]
\[ \Rightarrow a b = ba \]
\[ \Rightarrow G / G' \text{ is abelian} \]

iii) Since \( a K, b K \) \( (a K)^{-1} (b K)^{-1} = K \) \( \therefore G / K \) is abelian

\[ \Rightarrow a K, b K, a^l K, b^l K = K \]
\[ \Rightarrow (a b a^{-1} b^{-1}) K = K \]
\[ \Rightarrow [a, b] K = K \quad \therefore \text{if } a H = H \]
\[ \Rightarrow [a, b] \in K \]
\[ \Rightarrow a \in H \]
\[ \Rightarrow G' \subseteq K. \]
# Direct Product of Groups

Let $H$ and $K$ be two subgroups of a group $G$. We define the direct product of these two groups by:

$$H \times K = \{(h, k) : h \in H \land k \in K\}$$

under multiplication:

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1h_2, k_1k_2)$$

**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 $HNK = \{e, e'\}$, then:

1. Every element of $H$ is permutable (commute) with every element of $K$.
2. Every element of $G$ is uniquely expressible as $g = hk$.
3. $G \cong H \times K$, i.e., $HK \cong H \times K$.

**Proof:**

Consider an element $hk h'^{-1}k'^{-1}$, then $hk h'^{-1}k' \in H$ if $H \triangleleft G$.

$$h(k h'^{-1}k') \in H \quad \therefore h \in H$$

Also $hk h'^{-1} \in K$ if $K \triangleleft G$.

$$(hk h'^{-1})k' \in K \quad \therefore k' \in K$$

i.e., $hk h'^{-1}k' \in H \cap K = \{e, e\}$ (given).

$$hk h'^{-1}k' = e$$

$$hk = kh$$

Thus, every element of $H$ is permutable with every element of $K$. 

[73]
ii) Let if possible, \( g \) has two expressions
\[
g = h_1k_1 \quad \& \quad g = h_2k_2
\]
for \( h_1, h_2 \in H \Rightarrow k_1, k_2 \in K \\
\text{such that } h_1 \neq h_2 \Rightarrow k_1 \neq k_2
\]
\[\Rightarrow h_1k_1 = h_2k_2\]
\[\Rightarrow h_1^{-1}h_1 = k_2k_1^{-1} \in K \text{ and } H\]
\[\Rightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K\]
\[\Rightarrow h_2^{-1}h_1 = e \quad \& \quad k_2k_1^{-1} = e\]
\[\Rightarrow h_1 = h_2 \quad \& \quad k_1 = k_2\]
which is a contradiction.
hence \( g = h_1k_1 \) is a unique representation.

iii) To prove \( G \cong H \times K \)
Define a mapping \( \varphi : G \rightarrow \mathbb{Q} \times \mathbb{R} \times H \times K \)
by \( \varphi(g) = (h, k) \)

a) The mapping is well defined as:
\[\text{for } g_1 = g_2\]
\[\Rightarrow h_1k_1 = h_2k_2 \quad \therefore g_1 = g_2\]
\[\Rightarrow h_1 = h_2 \quad \& \quad k_1 = k_2\]
\[\Rightarrow (h_1, k_1) = (h_2, k_2)\]
\[\Rightarrow \varphi(g_1) = \varphi(g_2)\]

b) \( \varphi \) is onto as:
\((h, k) \in H \times K \) is image of \( g = hk \in H \times K = G\)
\[\therefore (h, k) \in H \times K\]
\[\Rightarrow h \in H, \quad k \in K \Rightarrow hk \in HK\]

c) \( \varphi \) is one-one:
\[\varphi(g_1) = \varphi(g_2)\]
\[\Rightarrow (h_1, k_1) = (h_2, k_2)\]
Groups: Handwritten notes

\[ h_1 = h_2, \quad k_1 = k_2 \]
\[ h_1k_1 = h_2k_2 \]
\[ g_1 = g_2 \quad \therefore g = hk \]

d) \( \varphi \) is homomorphism

\[ \varphi (g_1 \cdot g_2) = \varphi (h_1 \cdot k_1 \cdot h_2 \cdot k_2) \]
\[ = \varphi (h_1 (k_1 h_2) \cdot k_2) \]
\[ = \varphi (h_1 (h_2 k_1) \cdot k_2) \quad \text{by (1)} \]
\[ = \varphi (h_1 h_2 \cdot k_1 k_2) \]
\[ = (h_1, k_1 \cdot h_2, k_2) \]
\[ = \varphi (h_1 k_1) \cdot \varphi (h_2 k_2) \]
\[ = \varphi (g_1) \cdot \varphi (g_2) \]

i.e \( \varphi \) is homomorphism.

and hence \( \varphi \) is isomorphism as it is also one-one and onto.

\[ G \cong H \times K \quad \text{or} \quad HK \cong H \times K \]

# Note: \( G \) is abelian group if \( H=\text{se} \) is derived group.

**************************************************************

- FSc
- BSc
- MSc / BS
- MPhil / MS
- PhD
- Old Papers / Entry Test
  - Check out all these at

***************************************************************
Lemma

Let $G$ be a direct product of two subgroups $H$ and $K$ and $H, K \triangleleft G$ then prove that $H \triangleleft G$.

Proof

Let $h_1 \in H$ and $g \in G$ then $g = h_k$ for $h \in H$, $k \in K$.

Now

$$gh_1g^{-1} = (hk)h_1(hk)^{-1}$$

$$= (hk)h_1(k'h^{-1})$$

$$= h(kh_1)(k'h^{-1})$$

$$= h(h_1k)(k'h^{-1})$$

$$= h h_1 (k k' h^{-1})$$

$$= h h_1 k h^{-1} \in H_1 \Rightarrow H \triangleleft H_1.$$

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

$\Rightarrow H_1 \triangleleft G$ 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 $g = h_k$ for $h \in H, k \in K, g \in G$ then

$$gx = (hk)(z_1 z_2)$$

$$= h(k z_1) z_2$$

$$= h(z_1 k) z_2$$

[76]
\[
\begin{align*}
&= (h z_1) (k z_2) \\
&= (z_1 h) (z_2 k) \\
&= z_1 (h z_2) k \\
&= (z_1 z_2) (h k) \\
&= z g \\
&\Rightarrow x \in C(G)
\end{align*}
\]

Hence
\[
C(H) \times C(K) \subseteq C(G) \quad \text{(i)}
\]

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

Let \( z \in C(G) \)

\[
\Rightarrow g z = z g \quad \text{for} \ g \in G.
\]

In particular

\[
zh = h z, \quad zk = k z \quad \forall h \in H \subseteq G, \ k \in K \subseteq G
\]

Let \( z = h' k' \) for \( h' \in H, \ k' \in K \)

So

\[
zh = (h' k') h = h'(k'h) = h' k
\]

and

\[
hz = h' k'
\]

\[
\Rightarrow h z = zh
\]

\[
\Rightarrow h h' k' = h' h k'
\]

\[
\Rightarrow h h' = h' h \quad \Rightarrow h' \in C(H)
\]

Similarly

\[
k' \in C(K)
\]

Hence

\[
h' k' \in C(H) \times C(K)
\]

\[
\Rightarrow z \in C(H) \times C(K) \quad \Rightarrow z = h' k'
\]

\[
\Rightarrow C(G) \subseteq C(H) \times C(K) \quad \text{(ii)}
\]

From (i) and (ii)

\[
C(G) = C(H) \times C(K) \quad \text{proved.}
\]
# Theorem

If \( G = H \times K \), then the factor group \( G/K \) is isomorphic to \( H \).

**Proof:**

\[ G/K = \{ gK : g \in G \} \]

Define a mapping

\[ \phi : G/K \to H \] by \[ \phi(gK) = \phi(hK) \]

then \( \phi \) is well defined as

\[ g_1 K = g_2 K \]

\[ \implies h_1 K = h_2 K \]

\[ h_2^{-1} h_1 K = K \]

\[ h_2^{-1} h_1 \in K \] but also \( h_2^{-1} h_1 \in H \)

\[ \implies h_2^{-1} h_1 \in H \cap K = \{ e \} \]

\[ \implies h_2^{-1} h_1 = e \implies h_1 = h_2 \]

\[ \implies \phi(h_1 K) = \phi(h_2 K) \]

\( \phi \) is onto and one-to-one as

For \( h \in H \) there is a coset \( hK \in G/K \) i.e. \( \phi(hK) = h \)

and \( \phi(h_1 K) = \phi(h_2 K) \)

\[ \implies h_1 = h_2 \]

\[ \implies h_1 K = h_2 K \]

Now,

\[ \phi(g_1 K \cdot g_2 K) = \phi(h_1 K \cdot h_2 K) \]

\[ = \phi(h_1 h_2 K) \]

\[ = h_1 h_2 \]

\[ = \phi(h_1 K) \cdot \phi(h_2 K) \]

\[ = \phi(g_1 K) \cdot \phi(g_2 K) \]

\[ \implies \phi \text{ is homomorphism} \]

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

$(a, b)^{mn} = (a^{mn}, b^{mn}) = ((a^m)^n, (b^n)^m) = (e, e)$

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

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

# Invariant Subgroup

**Definition:** 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 $[x, y] \in G'$

$\phi([x, y]) = \phi(xy, x', y')$

$= \phi(x) \cdot \phi(y) \cdot \phi(x') \cdot \phi(y')$

$= \phi(x) \cdot \phi(y) \cdot (\phi(x))' \cdot (\phi(y))'$

$\Rightarrow [\phi(x), \phi(y)] \in G'$

$\Rightarrow G'$ is fully invariant.
Groups: Handwritten notes

# Characteristic Subgroup:

A subgroup $H$ of $G$ is characteristic subgroup if it remains fully invariant under all automorphism, i.e. for all $h \in H$, for all $\phi \in \text{Aut}(G)$,

$\phi(h) \in H$ or $\phi(H) = H$.

# Question

$: Centre of G is characteristic subgroup of G.$

Solution:

Let $x \in C(G)$

$\Rightarrow gx = xg$ \hspace{0.5cm} \forall g \in G$

Let $\phi: G \rightarrow G$ be an automorphism

$\phi(gx) = \phi(xg)$

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

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 $\phi(H) = H$ \hspace{0.5cm} \forall \phi \in \text{Aut}(G)$

In particular

$\phi_g(H) = H$ \hspace{0.5cm} $: \phi_g$ is an inner automorphism.

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

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

******************************************************************************

={ The End =}

******************************************************************************