Lecture Notes On

GROUP THEORY

By

Ahsan Khan
wolframmath.world

DEPARTEMENT OF MATHEMATICS
Introduction

We begin our study of algebraic structures by investigating sets associated with single operations that satisfy certain reasonable axioms; that is, we want to define an operation on a set in a way that will generalized familiar structures as the integers \( \mathbb{Z} \) together with the single operation of adding or invertible \( 2 \times 2 \) matrices together with the single operation of matrix multiplication. The integers and the \( 2 \times 2 \) matrices, together with their respective single operations, are examples of algebraic structures known as groups.

Group theory is a branch of pure mathematics. The theory of groups occupies a central position in mathematics. Modern group theory arose from an attempt to find the roots of polynomial in term of its coefficients. Groups now play a central role in such areas as coding theory, counting, and the study of symmetries; many areas of biology, chemistry and physics have benefited from group theory.

1.1 Binary Operation

A binary operation \( * \) on a set \( S \) is a function mapping \( S \times S \) into \( S \). For each \( (\mathbf{r}, \mathbf{s}) \in S \times S \), we will denote the element \( * ((\mathbf{r}, \mathbf{s})) \) of \( S \) by \( \mathbf{r} * \mathbf{s} \).

1.1.1 Examples

i. Our usual addition \( + \) is a binary operation on the set \( \mathbb{R} \). Our usual multiplication is a different binary operation on \( \mathbb{R} \). In this example, we could replace \( \mathbb{R} \) by any of the sets \( \mathbb{C}, \mathbb{Z}, \mathbb{R}^+ \) or \( \mathbb{Z}^+ \).

ii. Let \( M(\mathbb{R}) \) be the set of all matrices with real entries. The usual matrix addition \( + \) is not a binary operation on the set since \( A + B \) is not defined for an ordered pair \( (A, B) \) of matrices having different number of rows or of columns.

iii. Let \( * \) be a binary on \( S \) and let \( H \) be a subset of \( S \). The subset \( H \) is closed under \( * \) if for all \( a, b \in H \) we also have \( a * b \in H \). In this case, the binary operation on \( H \) given by restricting \( * \) to \( H \) is the induced operation of \( * \) on \( H \).

Properties

i. Identity element is unique. That is, a binary operation \( (S, *) \) has at most one identity element.

ii. Inverse element is unique.
Note: Remember that in an attempt to define a binary operation \(*\) on a set \(S\) we must make sure that

i. Exactly one element is assigned to each possible ordered pair of element of \(S\),
ii. For each ordered pair of element of \(S\), the element is assigned to it is again in \(S\).

Example

i. Let \(S\) be the set consisting of 20 people, no two of whom are of the same height. Define \(*\) by \(a * b = c\), where \(c\) is the tallest person among the 20 in \(S\). This is a perfectly good binary operation on the set, although not a particularly interesting one.

ii. Let \(S\) be the set consisting of 20 people, no two of whom are of the same height. Define \(*\) by \(a * b = c\), where \(c\) is the shortest person in \(S\) who is taller than both \(a\) and \(b\). This \(*\) is not everywhere defined, since if either \(a\) or \(b\) is the tallest person in the set, \(a * b\) is not determined.

iii. On \(\mathbb{Z}^+\), let \(a * b = \frac{a}{b}\). Since for \(1 * 3\) is not in \(\mathbb{Z}^+\). That is, the element assigned is not again in \(\mathbb{Z}^+\).

Thus \(*\) is not a binary operation on \(\mathbb{Z}^+\), since \(\mathbb{Z}^+\) is not closed under \(*\).

1.2 Groups

A pair \((G, *)\) where \(G\) is a non-empty set and ‘*’ a binary operation in \(G\) is a group if and only if:

i. The binary operation \(*\) closed, i.e.,
\[
a * b = b * a, \forall a, b \in G
\]

ii. The binary operation \(*\) is associative, i.e.,
\[
(a * b) * c = a * (b * c), \forall a, b, c \in G
\]

iii. There is an identity element \(e \in G\) such that for all \(a \in G\)
\[
a * e = e * a = a
\]

iv. For each \(a \in G\) there is an element \(a' \in G\) such that
\[
a * a' = a' * a = e
\]
\(a'\) is called the inverse of \(a\) in \(G\) and its denoted by \(a^{-1}\).

Properties of a Group Let \(G\) be a group, then following are the some important properties of \(G\);

a) Cancelation law holds in \(G\). That is, \(a * b = a * c\) implies \(b = c\), and \(b * a = c * a\) implies \(b = c\) for all \(a, b, c \in G\).

b) Identity element is unique.

c) Inverse of an element is unique.

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

e) \((ab)^{-1} = b^{-1}a^{-1}\)
**Note:** The identity element and inverse of each element are unique in a group.

---

**Historical Note**

There are three historical roots of the development of abstract group theory evident in the mathematical literature of the nineteenth century: the theory of algebraic equations, number theory and geometry. All three of these areas used group theoretic methods of reasoning, although the methods were considerably more explicit in the first area than in the two.

One of the central themes of geometry in the nineteenth century was the search of invariants under various types geometric transformations. Gradually attention became focused on the transformations themselves, which in many cases can be thought of as elements of groups.

In number theory, already in the eighteenth century Leonhard Euler had considered the remainders on division of power $a^n$ by fixed prime $p$. These remainders have “group” properties. Similarly, Carl F. Gauss, in his Disquisitiones Arithmeticae (1800), dealt extensively with quadratic forms $ax^2 + 2bxy + cy^2$, and in particular showed that equivalence classes of these forms under composition possessed what amounted to group properties.

Finally, the theory of algebraic equations provided the most explicit prefiguring of the group concept. Joseph-Louis Lagrange (1736 – 1813) in fact initiated the study of permutations of the roots of an equation as a tool for solving it. These permutations, of course, were ultimately considered as elements of a group.

It was Walter von Dyck (1856 – 1934) and Heinrich Weber (1842 – 1913) who in 1882 were able independently to combine the three roots and give clear definitions of the notion of an abstract group.

---

**Torsion Free And Mixed Group**

A group in which every element except the identity element $e$ has infinite order is known as torsion free ($a$-periodic or locally infinite). A group having elements both of finite as well as infinite order is called a mixed group.

---

**Semigroup And Monoid**

A set with an associative binary operation is called a semigroup. A semigroup that has an identity element for the binary operation is called monoid.

**Note** that every group is both a semigroup and a monoid.

---

**Abelian Group**

A group $G$ is abelian if its binary operation is commutative. That is, let $(G, *)$ be a group. Let $a, b \in G$, then $G$ is called an abelian group iff

$$a * b = b * a$$

---

**1.2.1 Examples**

- The familiar additive properties of integers and of rationals, real and complex numbers show that $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ under addition abelian groups.
b. The set \( \mathbb{Z}^+ \) under addition is not a group. There is no identity element for \( + \) in \( \mathbb{Z}^+ \).

c. The set \( \mathbb{Z}^+ \) under multiplication is not a group. There is an identity 1, but no inverse of 3.

d. The familiar multiplicative properties of rational, real and complex numbers show that the sets \( \mathbb{Q}^+ \) and \( \mathbb{R}^+ \) of positive numbers and the sets \( \mathbb{Q}^* \), \( \mathbb{R}^* \) and \( \mathbb{C}^* \) of nonzero numbers under multiplication are abelian groups.

e. The set \( M_{m \times n}(\mathbb{R}) \) of all \( m \times n \) matrices under addition is a group. The \( m \times n \) matrix with all entries zero is the identity matrix. This group is abelian.

f. The set \( M_n(\mathbb{R}) \) of all \( n \times n \) matrices under matrix multiplication is not a group. The \( n \times n \) matrix with all entries zero has no inverse.

g. The set of all real-valued functions with domain \( \mathbb{R} \) under function addition is an abelian group.

---

**Historical Note**

Commutative groups are called abelian in honor of the Norwegian mathematician Niels Henrik Abel (1802 – 1829). Abel was interested in the question of solvability of polynomial equations. In a paper written in 1828, he proved that if all the roots of such an equation can be expressed as rational functions \( f, g, ..., h \) of one of them, say \( x \), and if for any two of these roots, \( f(x) \) and \( g(x) \), the relation \( f(g(x)) = g(f(x)) \) always holds, then the equation is solvable by radicals. Abel showed that each of these functions in fact permutes the roots of the equation; hence, these functions are elements of the group of permutations of the roots. It was this property of commutativity in these permutation groups associated with solvable equations that led Camille Jordan in his 1870 treatise on algebra to name such groups abelian; the name since then has been applied to commutative groups in general.

1.2.2 Example Let \( * \) be defined on \( \mathbb{Q}^+ \) by \( a * b = \frac{ab}{2} \). Then \((a * b) * c = \frac{ac}{4} \), and likewise \( a * (b * c) = \frac{abc}{4} \).

**SOLUTION** Let \( * \) defined on \( \mathbb{Q}^+ \) by \( * b = \frac{ab}{2} \).

i. Closed property.

For \( a, b \in \mathbb{Q}^+ \), we have \( a * b = \frac{ab}{2} \)

Thus closed property holds.

ii. Associative property.

For \( a, b, c \in \mathbb{Q}^+ \),

\[
(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4} \times \frac{1}{2} = \frac{abc}{4}
\]

\[
a * (b * c) = a * \frac{bc}{2} = \frac{1}{2} \times \frac{abc}{2} = \frac{abc}{4}
\]

Thus associative law holds.

iii. Identity.

Given that \( a * b = \frac{ab}{2} \).
Let \( e \in \mathbb{Q}^+ \), since
\[
a \ast e = e \ast a = a
\]
Now
\[
a \ast e = \frac{ae}{2}
\]
\[
\Rightarrow a \ast 2 = \frac{a \times 2}{2} = a
\]
Similarly
\[
2 \ast a = \frac{2 \times a}{2} = a
\]
Thus \( e = 2 \) is the identity element.

**iv. Inverse.**
For \( a \in \mathbb{Q}^+ \), since
\[a \ast a' = a' \ast a = e\]
By computing
\[
a \ast a' = \frac{aa'}{2}
\]
\[
a \ast \frac{4}{a} = \frac{a \times 4}{2 \times a} = 2
\]
Similarly
\[
\frac{4}{a} \ast a = 2
\]
\[
\Rightarrow a' = \frac{4}{a} \text{ is the inverse of } a. \text{ Hence inverse of each element exists. Thus } (\mathbb{Q}^+, \ast) \text{ is a group.}
\]

**1.2.3 Example** Show that the subset \( S \) of \( M_n(\mathbb{R}) \) consisting of all invertible \( n \times n \) matrices under matrix multiplication is a group.

**Solution** we start by showing that \( S \) is closed under matrix multiplication. Let \( A \) and \( B \) in \( S \) so that both \( A^{-1} \) and \( B^{-1} \) exists such that \( AA^{-1} = BB^{-1} = I_n \), then
\[
(AB)(AB)^{-1} = (AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = I_n
\]
So that \( AB \) is invertible, consequently is also in \( S \).

Since matrix multiplication is associative and \( I_n \) acts as the identity element, since each element of \( S \) has an inverse (by definition). We see that \( S \) is indeed a group. This group is not commutative, it is our first example of non abelian group.

**Group of Mobius Transformation**

Let \( \mathbb{C} \cup \{\infty\} \) be the extended complex plane. Consider the set \( M \) of all mappings.
\[
\mu : \mathbb{C} \cup \{\infty\} \rightarrow \mathbb{C} \cup \{\infty\} \text{ defined by}
\]
\[ \mu(z) = \frac{az + b}{cz + d}, \quad cz + d \neq 0, \quad z \in \mathbb{C} \cup \{\infty\} \]

and \(a, b, c, d\) are themselves complex numbers. Multiplication of mappings in \(M\) is their successive application. The mapping

\[ I : \mathbb{C} \cup \{\infty\} \rightarrow \mathbb{C} \cup \{\infty\} \text{ given by} \]

\[ I(z) = z, \quad \forall \ z \in \mathbb{C} \cup \{\infty\} \]

Is the identity element of \(M\). Also for each \(\mu\) in \(M\), its inverse is the mapping

\[ \mu' : \mathbb{C} \cup \{\infty\} \rightarrow \mathbb{C} \cup \{\infty\} \text{ given by} \]

\[ \mu'(z) = \frac{dz - b}{-cz + a} \]

Hence \(M\) is called the group of mobius transformation.

This group is closely related to the groups

\[ M = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{C} \text{ and } ad - bc \neq 0 \right\} \]

And

\[ M^* = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{C} \text{ and } ad - bc = 1 \right\}. \]

Under matrix multiplication.

**1.3 Definitions**

**Order of a Group**

The number of elements in a group is called the order of a group and is denoted by \(|G|\).

**Order of an element**

Let \(a\) be any element of a group \(G\). A non-zero positive integer \(n\) is called the order of \(a\) if \(a^n = e\) and \(n\) is the least such integer.

**Periodic Group**

A group all of whose elements are of finite order is called a periodic group. A finite group is obviously periodic.

**Finite and Infinite Group**
A group $G$ is said to be finite if $G$ consists of the finite number of elements. A group $G$ is said to be an infinite group if $G$ consists of the infinite number of elements.

### 1.3.1 Examples

i. Let $\mathbb{Z} = \{ \ldots, -3, -2, -1, 0, +1, +2, +3, \ldots \}$ is a group under addition, then $|\mathbb{Z}| = \infty$ and for $2 \in \mathbb{Z}$, $|2| = \infty$.

ii. Let $G = \{1, -1, i, -i\}$, then $|G| = 4$.

### 1.3.2 Example

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

**Proof** Let $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$.

a) Let $a, b \in \mathbb{Z}_n$, 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., the binary operation $\oplus$ is defined.

b) The binary operation $\oplus$ is associative in general.

c) $0 \in \mathbb{Z}_n$ is an identity element.

d) For $a \in \mathbb{Z}_n$, $n - a$ is the inverse of $a$. i.e.,

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

All conditions are satisfied. Hence $\mathbb{Z}_n$ under modulo addition $\oplus$ is a group. This group under modulo addition $\oplus$ is also an abelian group.

**Cayley Table:** It is often convenient to describe a group in terms of an addition or multiplication table. Such a table is called **Cayley Table**.

### 1.3.3 Example

Let $G = \{1, -1, i, -i\}$ be a group under multiplication, then the cayley table is given by

$$
\begin{array}{cccc}
\times & 1 & -1 & i & -i \\
1 & 1 & -1 & i & -i \\
-1 & -1 & 1 & -i & i \\
i & i & -i & -1 & 1 \\
-i & -i & i & 1 & -1 \\
\end{array}
$$

**Klien’s Four-Group:** The Klien four-group is group with four elements, in which each element is self-inverse. It was named **Vierergruppe** (four-group) by Felix Klien in 1884. It is also called the Klien group. It is denoted by the letter $V$ or $K_4$ and is given by

\[
K_4 = \{e, a, b, c\}.
\]

Where $a^2 = b^2 = c^2 = (ab)^2 = e$, and
The Klien four-group is not cyclic and it is an abelian group. The Cayley's table for $K_4$ is given by

\[
\begin{array}{ccccc}
\times & e & a & b & c \\
e & e & a & b & c \\
a & a & e & c & b \\
b & b & c & e & a \\
c & c & b & a & e \\
\end{array}
\]

It can be described as the symmetric group of a non-square rectangle (with the three non-identity elements being horizontal and vertical reflection and 180-degree rotation). There are five subgroups of $K_4$ of order 1, 2 and 4. These are

\[H_1 = \{e\}\]
\[H_2 = \{e, a\}\]
\[H_3 = \{e, b\}\]
\[H_4 = \{e, c\}\]
\[H_5 = K_4\]

**Properties**

a) Every non-identity element is of order 2.

b) Any two of the three non-identity element generates the third one.

c) It is the smallest non-cyclic group.

d) All proper subgroups of $K_4$ are cyclic.

**Involution** An element $x$ of order 2 in a group $G$ is called an involution.

**1.3.4 Theorem** Every group of even order has at least one involution.

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

\[A = \{x \in G : x^2 = e\}, \quad B = \{y \in G : y^2 \neq e\}.\]

Then, we have

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

If $B = \emptyset$ then $G = A$. So $G$ contains an involution. Now let $B \neq \emptyset$ and let $y \in B$. Then, as

\[y^2 \neq e, \quad y^{-1} \neq y\]
But since \((y^{-1})^2 \neq e\) so that \(y^{-1} \in B\). So for each \(y \in B\) there exists \(y^{-1} \in B\). Thus the number of elements in \(B\) is even. Since the order of \(G\) is even and

\[ |G| = |A| + |B| \]

So the number of elements in \(A\) is also even. Since \(e^2 = e\), \(e \in A\), \(A \neq \emptyset\). Hence \(|A| \geq 2\). Thus \(A\) and also \(G\) contains an involution.

**1.3.5 Theorem** In a group if every non-identity element is of order 2, then prove that the group is abelian.

**Proof** Let \(G\) be a group and \(a \in G, a \neq e\) such that

\[ a^2 = e \Rightarrow a = a^{-1} \]

Let \(y \in G\), then \(xy = (xy)^{-1} = y^{-1}x^{-1} = yx\).

So \(G\) is abelian.

**1.4 Subgroup**

If a subset \(H\) of a group \(G\) is closed under the binary operation defined on \(G\) and if \(H\) with the induced operation of \(G\) is itself a group, then \(H\) is called a subgroup of \(G\) and is denoted by \(H \leq G\) or \(G \supseteq H\).

OR

A subset \(H\) of a group \(G\) is called a subgroup of \(G\) if and only if \(H\) is itself a group under the same binary operation defined on \(G\).

**1.4.1 Remark** Every group \(G\) has a subgroup \(G\) itself and the identity \(\{e\}\), where \(e\) is the identity element. The subgroup \(G\) itself is the **proper subgroup** and the identity element \(e\) is called **trivial subgroup** of \(G\). All other subgroup of \(G\) are called the **non-trivial subgroup** of \(G\).

**1.4.2 Examples**

i. \((\mathbb{Z}, +)\) is a subgroup of \((\mathbb{Q}, +)\) and \((\mathbb{Q}, +)\) is a subgroup of \((\mathbb{R}, +)\).

ii. The set \(\mathbb{Q}^+\) under multiplication is a subgroup of \(\mathbb{R}^+\) under the algebraic operation multiplication.

iii. The \(n\)th root of unity in \(\mathbb{C}\) form a subgroup \(U_n\) of the group \(\mathbb{C}^*\) of non-zero complex numbers under the algebraic operation multiplication.

**1.4.3 Theorem** A non-empty subset \(H\) of a group \(G\) is a subgroup of \(G\) if and only if for any pair of \(a, b \in H\), \(ab^{-1} \in H\); \(a \neq b \neq e\).
**Proof** Suppose that $H$ is a subgroup of a group $G$, then $(H, \ast)$ is a group.

Therefore if $b \in H$, $b^{-1} \in H \Rightarrow a, b^{-1} \in H$ and $ab^{-1} \in H$ (closed property)

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

To prove $H$ is a subgroup, put $b = a \Rightarrow a, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$.

$\Rightarrow$ identity element exists.

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

$\Rightarrow$ inverse of each element exists in $H$.

Again, let $a, b \in H \Rightarrow a, b^{-1} \in H$

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

$\Rightarrow ab \in H$

Thus $H$ is closed under the induced algebraic operation. The associative law holds in $H$ as it holds in $G$.

Therefore $H$ is a subgroup.

1.4.4 Theorem Prove that the intersection of family of subgroups of a group $G$ is a subgroup of $G$.

**Proof** Let $\{H_\alpha\}_{\alpha \in I}$ be a family of subgroups of $G$. We have to show that $H = \bigcap_{\alpha \in I} H_\alpha$ is a subgroup of $G$.

Let $a, b \in H$, then $a, b \in H_\alpha$ for each $\alpha \in I$. Since $H_\alpha$ is a subgroup of $G$, so $ab^{-1} \in H_\alpha$ for each $\alpha \in I$.

Therefore,

$$ab^{-1} \in \bigcap_{\alpha \in I} H_\alpha = H$$

$\Rightarrow H$ is a subgroup of $G$. Hence the intersection of family of subgroups of $G$ is a subgroup of $G$.

1.4.5 Theorem The union $H \cup K$ of two subgroups $H, K$ of a group $G$ is a subgroup of $G$ if and only if either $H \subseteq K$ or $K \subseteq H$.

**Proof** Suppose that either $H \subseteq K$ or $K \subseteq H$. We have to show that $H \cup K$ is a subgroup of $G$.

Now,

$$H \cup K = H \quad \therefore K \subseteq H$$

$$H \cup K = K \quad \therefore H \subseteq K$$
Thus $H \cup K$ is a subgroup of $G$ as $H, K$ are subgroups of $G$.

Conversely, suppose that $H \cup K$ is a subgroup of $G$. To prove either $H \subseteq K$ or $K \subseteq H$, suppose on contrary that

$$H \not\subseteq K, K \not\subseteq H$$

Let $a \in H \setminus K, b \in K \setminus H$. Since, $b \in H \cup K$, therefore

$$ab \in H \cup K \implies H \cup K \text{ is a subgroup}$$

$\Rightarrow$ either $ab \in H$ or $ab \in K$. Suppose that $b \in H$, then

$$b = a^{-1}(ab) \in H \implies H \text{ is a subgroup}$$

Similarly, suppose $b \in K$, then

$$a = (ab)b^{-1} \in K \implies K \text{ is a subgroup}$$

This is contradiction to our supposition so either $H \subseteq K$ or $K \subseteq H$.

**1.4.6 Theorem** Show that $\mathbb{Z}_p$ has no proper subgroup if $P$ is a prime number.

**Proof** As number of subgroups of $\mathbb{Z}_p$ is the same as the number of distinct divisors of $P$ which are $1$ and $P$ itself. Hence the number of distinct subgroups of $\mathbb{Z}_p$ are two $\{1\}$ and $\mathbb{Z}_p$ itself. Thus the number of proper subgroups is zero (no proper subgroup), as we can say that $\mathbb{Z}_p$ has no proper subgroup.

**1.4.7 Theorem** Let $G$ be an abelian group and $H$ be the set consisting of the elements of finite order in $G$. Then $H$ is a subgroup of $G$.

**Proof** Let $a, b \in H$, then there exist integers $m, n$ such that

$$a^m = b^n = e, (e \text{ is the identity of } H)$$

So

$$(ab)^mn = ab \cdot ab \cdot ab \ldots ab \ (mn \text{ times})$$

$$= a^m \cdot b^n$$

$$= (a^m)^n \cdot (b^n)^m = e^n \cdot e^m$$

$$= e$$

$\Rightarrow ab$ has finite order, so $ab \in H$.

Also, if $b \in H$ and $b^n = e$, then
\[(b^{-1})^n = b^{-1} \cdot b^{-1} \cdot b^{-1} \ldots b^{-1} \quad (\text{n times})\]
\[= b^{-n} = (b^n)^{-1} = (e)^{-1} = e\]

\(\Rightarrow b^{-1} \in H\). Hence \(H\) is a subgroup of \(G\).

### 1.5 Cyclic Group

A group \(G\) is said to be cyclic if and only if it generates by a single element. i.e., a group \(G\) is cyclic if there is some element \(a \in G\) that generates \(G\). If \(G\) is finite cyclic group of order \(n\), then

\[G = \langle a : a^n = e \rangle.\]

If an element of \(G\) is the generator of \(G\) then its inverse is also the generator of \(G\).

### 1.5.1 Examples

i. A group \(G = \{1, -1, i, -i\}\) is cyclic group as \(\langle i \rangle\) is its generator.

ii. A group \(\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}\) under modulo addition is cyclic group. Since every element of \(\mathbb{Z}_5\) is in the power of a single element that is 1. Therefore 1 is the generator of \(\mathbb{Z}_5\).

iii. A set \(\{1, -1\}\) is a cyclic group under multiplication.

iv. The group \(\mathbb{Z}\) under addition is a cyclic group. Both 1 and \(-1\) are generators of this group, and they are the only generators. Also, for \(n \in \mathbb{Z}^+\), the group \(\mathbb{Z}_n\) under addition modulo \(n\) is cyclic. If \(n > 1\), then both 1 and \(n - 1\) are generators, but there may be others.

### 1.5.2 Theorem

Every cyclic group is abelian.

**Proof** Let \(G\) be a cyclic group and let \(a\) be a generator of \(G\).

Let \(x, y \in G\), then there exist integers \(m\) and \(n\) such that

\[x = a^m \quad y = a^n\]

Now

\[xy = a^m a^n = a^{m+n} = a^{n+m} = a^na^m = yx\]

So \(G\) is abelian.

### 1.5.3 Theorem

Every subgroup of a cyclic group is cyclic.

**Proof** Let \(G\) be 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 have to prove that \(H\) is generated by \(a^k\).

For this, let \(a^m \in H\), \(\forall m > k\), then there exist integers \(q\) and \(r\) such that
\[ m = kq + r, \ 0 \leq r \leq k \]
\[ \Rightarrow \ a^m = a^{kq} + a^r \]
\[ = (a^k)^q \cdot a^r \]
\[ \Rightarrow a^m \cdot (a^k)^{-q} = a^r \]

Sine \( a^m \) and \( (a^k)^{-q} \) are in \( H \). Therefore, \( a^r \in H \). But since \( k \) is the smallest integer for which \( a^k \in H \) and \( r < k \), so \( a^k \in H \) is possible only if \( r = 0 \). But if \( r = 0 \), then
\[ m = qk \]
\[ \Rightarrow \ a^m = a^{kq} \]
\[ \Rightarrow \ a^m = (a^k)^q \in H \]
\[ \Rightarrow a^k \] is the generator of \( H \).

Hence \( H \) is cyclic subgroup of \( G \).

**Division algorithm for \( \mathbb{Z} \)**  If \( m \) is a positive integer and \( n \) is any integer such that \( n > m \), then there exist unique integer \( q \) and \( r \) such that
\[ n = mq + r, \quad 0 \leq r \leq m \]
Where \( q \) is the quotient and \( r \) is the remainder when \( n \) divided by \( m \).

**1.5.4 Corollary**  The subgroups of \( \mathbb{Z} \) under addition are precisely the groups \( n\mathbb{Z} \) under addition for \( n \in \mathbb{Z} \). This corollary gives the greatest common divisors of two positive integers \( r \) and \( s \).

**Greatest Common Divisor**  Let \( r \) and \( s \) be two positive integers. The positive generator \( d \) of the cyclic group \( G = \{ nr + ms \mid n, m \in \mathbb{Z} \} \) under addition is the greatest common divisor of \( r \) and \( s \). We write \( d = \text{gcd}(r, s) \). If two positive integers are relatively prime then their greatest common divisor is 1.

**Note:** If \( r \) and \( s \) are relatively prime and if \( r \) divides \( ms \), then \( r \) must divide \( m \).

**Question**  Find the greatest common divisor of 42 and 72.

**Solution**  The positive divisors of 42 are 1,2,3,6,7,21,42. The positive divisors of 72 are 1,2,3,4,6,8,9,12,18,24,36,72. This implies that the greatest common divisor of 42 and 72 is 6. i.e., \( \text{gcd}(42,72) = 6 \).

\[ d = nr + ms \]
\[ 6 = (72)(6) + (42)(-5) \]
\[ \Rightarrow n = 6, \ m = -5 \]
1.5.5 Theorem Let $G$ be a cyclic group of order $n$. Then $G$ contains one and only one subgroup of order $d$ if and only if $d | n$.

**Proof** Let $G$ be a cyclic group generated by $a \in G$ such that $a^n = e$. Suppose that $d > 0$ divides $n$, then $n = kd$ for some integer $k$. So

$$a^n = a^{kd} = (a^k)^d \in H$$

$$\Rightarrow H = \{a^k : k = \frac{n}{d}\}$$

is a subgroup of order $d$. To prove $H$ is unique subgroup of order $d$ in $G$, let $K$ be another subgroup of order $d$ in $G$ and generated by $a^l$, $l > 0$. then

$$(a^l)^d = a^{ld} = e$$

So $n$ divides $ld$. Thus $ld = rn$ for some integer $r$. But $n = kd$.

$$\Rightarrow ld = rkd$$

$$\Rightarrow l = rk$$

$$\Rightarrow a^l = a^{rk} = (a^k)^r \in H$$

Therefore $K \subseteq H$. Since $H$ and $K$ are subgroups of $G$ having same order, so $H = K$.

$\Rightarrow$ there is one and only one subgroup of order $d$ in $G$.

Conversely, suppose that $H$ is a subgroup of order $d$. Then $d$ being the order of subgroup divides the order of group $G$ i.e., $d | n$.

1.5.6 Theorem Let $G$ be a cyclic group of generated by $a$,

a) If $G$ is of finite order $n$ then an element $a^k \in G$ is a generator of $G$ if and only if $k$ and $n$ are relatively prime.

b) If $G$ is of infinite order, then $a$ and $a^{-1}$ are the only generator of $G$.

**Proof**

a) Let $G = \langle a : a^n = e \rangle$ be a finite cyclic group. Consider $k$ and $n$ are relatively prime, then there exist integers $p$ and $q$ such that

$$kp + nq = 1 \quad \rightarrow (A)$$

Let $H$ be a subgroup generated by $a^k$. Now will prove that $H = G$.

From (A), we have

$$a^{kp + nq} = a^1$$
\[ a^{kp} . a^{nq} = a \]
\[ (a^k)^p . (a^n)^q = a \]
\[ (a^k)^p . (e)^q = a \]
\[ (a^k)^p = a \]

Since \((a^k)^p\) is an element of \(H\). So \(a \in H\)

Also \(a \in G\), therefore \(H = G\).

\(\Rightarrow G\) is generated by \(a^k\).

Conversely, suppose \(a^k\) is the generator of \(G\), so for some integer \(p\) we have

\[ (a^k)^p = a \]
\[ a^{kp} = a \]
\[ \Rightarrow a^{kp - 1} = e \]

So \(n \mid kp - 1\), because \(n\) is the least such integer. So there exist integer \(q\) such that

\[ \Rightarrow kp - 1 = nq \]
\[ \Rightarrow kp - nq = 1 \]

\(\Rightarrow k\) and \(n\) are relatively prime.

b) Let \(G = \langle a \rangle\) be an infinite cyclic group. Let \(a^k\) is also the generator of \(G\). Then, there exist an integer \(p\) such that

\[ (a^k)^p = a \]
\[ \Rightarrow a^{kp - 1} = e \]

\(\Rightarrow kp - 1 = 0\) or \(kp - 1 \neq 0\).

If \(kp - 1 \neq 0\), then order of \(G\) is finite, which is contradiction. Therefore \(kp - 1 = 0\)

\[ \Rightarrow kp = 1 \]

Since \(k\) and \(p\) are integers. Therefore, either \(k = p = 1\) or \(k = p = -1\) i.e., \(a\) and \(a^{-1}\) are the only generators.

<table>
<thead>
<tr>
<th>Exponent</th>
<th>Let (G) be a group of order (n). If the order of its generator is (n) then (G) has exponent (n). i.e., (a^n = e) for some (a \in G).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1.5.7 Theorem</strong></td>
<td>An abelian group (G) of order (n) is cyclic if and only if it has exponent (n).</td>
</tr>
</tbody>
</table>
Proof Let $G = \langle a : a^n = e \rangle$ be a cyclic group, then clearly $G$ has an exponent $n$.

Conversely, suppose that $G$ is an abelian group of order $n$ and has exponent $n$. We have to show that $G$ is cyclic.

First we show that for any $a, b \in G$ of order $p$ and $q$ respectively with $(p, q) = 1$, the order or $ab$ is $pq$.

Let the order of $ab$ is $k$, then we have

$$(ab)^k = e = a^k \cdot b^k$$

$$\Rightarrow a^k = b^{-k} = c \text{ (say)}$$

Let $m$ be the order of $c$. Then $m$ divides the order of $a$ and $b$.

So $m|(p, q)$. since $(p, q) = 1, m = 1$. Hence $c = e$ so that

$$a^k = b^k = e$$

But then $p|k, q|k$. Hence $pq|k$. Also

$$(ab)^{pq} = (a^p)^q \cdot (b^q)^p = e$$

Hence $k|pq$. thus

$$k = pq \quad \therefore (ab)^k = e$$

$\Rightarrow$ the order of $ab$ is $pq$.

Next let $x$ be an element of maximal order in $G$ so that

$$x^m = e$$

We show that for each $y \in G$, $y^m = e$.

Since $G$ is finite, let $k$ be the order of $y$, and

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

Where $\alpha_i \geq 0, \beta_j \geq 0, 1 \leq i \leq r, 1 \leq j \leq s$. If $y^m = e$ then $k$ does not divide $m$. So for some $i, \alpha_i > \beta_i$.

suppose that $i = 1$, so that $\alpha_1 > \beta_1$.

Take

$$x' = x^{p_1^{\beta_1}}, y' = y^{p_2^{\beta_2} \cdots p_r^{\beta_r}}$$

Then

$$(x'^{p_2^{\beta_2} \cdots p_s^{\beta_s}} = x^m = e$$
and \((y^r)^{p_1^{a_1}} = y^{p_1^{a_1} + p_2^{a_2} \ldots p_s^{a_s}} = y^k = e\)

Since
\[
\left( p_1^{a_1}, p_2^{a_2} \ldots p_s^{a_s} \right) = 1,
\]
x has order \(p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s} m > m\). This contradicts our choice of \(x\). Hence \(y^m = e\), so that \(m = \text{exponent of } G\). But then \(m = n\). Thus \(x\) has order \(n\) in \(G\) which also has order \(n\). Hence \(G\) is cyclic group generated by \(x\).

**1.5.8 Proposition** Let \(G\) be a cyclic group of order \(n\) and suppose that \(a\) is a generator for \(G\). Then \(a^k = e\) if and only if \(n\) divides \(k\).

**Proof** First suppose that \(a^k = e\). By the division algorithm, \(k = nq + r\) where \(0 \leq r < n\). Hence,
\[
a^k = a^{nq+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r
\]
\[
a^r = e
\]
\[
\therefore a^k = e
\]

Since \(n\) is the least such integer for which \(a^n = e\), \(r < n\). So it is possible only if \(r = 0\).
\[
\Rightarrow k = nq
\]
This implies that \(n|k\).

Conversely, if \(n\) divides \(k\), then \(k = nq\) for some integer \(q\). Consequently, we have
\[
a^k = a^{nq} = (a^n)^q = e
\]
\[
\Rightarrow a^k = e.
\]

**Corollary** If \(a\) is a generator of a finite cyclic group \(G\) of order \(n\), then the other generators of \(G\) are the elements of the form \(a^r\), where \(r\) is relatively prime to \(n\).

**1.5.9 Example** Find all the subgroups of \(\mathbb{Z}_{18} = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17\}\).

**Solution** The number 2 is the generates a subgroup consists of 9 number of elements.
\[
< 2 > = \{0,2,4,6,8,10,12,14,16\}
\]
by using previous corollary the elements 1,5,7,11,13,17 are all the generators of \(\mathbb{Z}_{18}\) and
\[
h = 1,2,4,5,7,8\text{ are all those elements which are relatively prime to } 9,\text{ so } h2 = 2,4,8,10,14,16.
\]
The element 6 of \(< 2 >\) generates a subgroup \(\{0,6,12\}\) and 12 also is the generator of this subgroup.

We have thus found all subgroups generated by \(0,1,2,4,5,6,7,8,10,11,12,13,14,16,17\). this leaves just 3,9 and 15.
Since the element 3 generates a subgroup consisting of 6 elements,

\[ < 3 > = \{0,3,6,9,12,15\} \]

Therefore, 15 = 5.3 also generates a subgroup of order 6, as 5 and 6 are relatively prime.

Finally, \( < 9 > = \{0,9\} \).

**1.5.10 Theorem** Every non-identity element in an infinite cyclic group is of infinite order.

**Proof** Let \( G =< a > \) be an infinite cyclic group. Let \( a^k \in G, m \neq 0 \) such that \( |a^k| \) is finite.

i.e \((a^k)^m = e\) for some integer \( m \).

\[ \Rightarrow a^{km} = e \]

This implies \( |a| \) is finite, which is contradiction to that \( G \) is infinite. Hence order of \( a \) is infinite.

**1.5.11 Theorem** A non-trivial subgroup of an infinite cyclic group is an infinite cyclic.

**Proof** Let \( G =< a > \) be an infinite cyclic group and \( H \) be a non-trivial subgroup of \( G \).

Since \( H \) is cyclic, so that \( H =< a^k > \) for some integer \( k > 0 \) (the subgroup of an infinite cyclic group is cyclic). By theorem (every non-identity element of an infinite cyclic group is of infinite order) \( |a^k| \) is infinite. Hence \( H \) is an infinite cyclic subgroup of \( G \).

**Definition** Let \( G \) be a group and let \( a_i \in G \) for \( i \in I \). The smallest subgroup of \( G \) containing \( \{a_i : i \in I\} \) is the **subgroup generated** by \( \{a_i : i \in I\} \). If this subgroup is all of \( G \), then \( \{a_i : i \in I\} \) generates \( G \) and the \( a_i \) are **generators of \( G \)**. If there is a finite set \( \{a_i : i \in I\} \) that generates \( G \), then \( G \) is **finitely generated**.

**Question** Find the generators of a finite cyclic group of order 12.

**Solution** Let \( G =< a > \) be a cyclic group of order 12, then

\[ G = \{a, a^2, a^3, ..., a^{12} = e\} \]

To find the generators of \( G \), the smallest subgroup of \( G \) generated by \( a^k, k \in \cup(12) \). Where

\[ \cup(12) = \{1,5,7,11\}, \text{i.e } a, a^5, a^7, a^{11}. \]

But since 1,5,7,11 are relatively prime to 12. Therefore \( a, a^5, a^7, a^{11} \) are the generators of \( G \).

**1.6 Cosets**

Let \( H \) be a subgroup of a group \( G \) which may be finite or infinite. We exhibit two partitions of \( G \) by two equivalence relation (left \( \sim_L \) and right \( \sim_R \)) on \( G \).
Let $H$ be a subgroup of a group $G$ then the subset $aH = \{ah : h \in H, a \in G\}$ of $G$ is the left cosets of $H$ containing $a$, while the subset $Ha = \{ha : h \in H, a \in G\}$ is the right cosets of $H$ containing $a$.

### 1.6.1 Example

Exhibit the left and right cosets $3\mathbb{Z}$ of $\mathbb{Z}$.

#### Solution

Let $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ be a group. Since $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ and $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

Now the left cosets $3\mathbb{Z}$ are

$$0 + 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$1 + 3\mathbb{Z} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$$

$$2 + 3\mathbb{Z} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

$$3 + 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

⇒ $3 + 3\mathbb{Z} = 3\mathbb{Z}$

It is clear that there are three left cosets we are found do exhaust. So they constitute the partition of $\mathbb{Z}$ into the left cosets of $3\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, therefore there left cosets $3 + 3\mathbb{Z}$ and the right cosets $3\mathbb{Z} + 3$ are the same. Since the partition of $\mathbb{Z}$ into the right cosets of $3\mathbb{Z}$ is the same.

#### Equivalence Relation:

- **Reflexive:** Let $a \in G$ then $aa^{-1} = e$, $e \in H$. Since $H$ is a subgroup thus $a \sim_L a$.
- **Symmetric:** Suppose $a \sim_L b$ then $a^{-1}b \in H$. Since $H$ is a subgroup of $G$, therefore $(a^{-1}b)^{-1}$ is in $H$ and hence $b \sim_L a$.
- **Transitive:** Let $a \sim_L b$ and $b \sim_L c$ then $a^{-1}b \in H$ and $b^{-1}c \in H$. Since $H$ is a subgroup, therefore $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = a^{-1}c \in H$.

Hence $a \sim_L c$.

The equivalence relation is used for the partition of a group.

**Note** Every left and right cosets of a subgroup $H$ of a group $G$ has the same number of elements.

#### 1.6.2 Theorem

A non-empty subset $H$ of a group $G$ is a subgroup of $G$ if and only if $HH^{-1} \subseteq H$.

#### Proof

Suppose that $H$ is a subgroup. Then

$$HH^{-1} = \{ab^{-1} : a, b \in H\} \subseteq H$$ (by closure law)

⇒ $HH^{-1} \subseteq H$.

Conversely, suppose that $HH^{-1} = \{ab^{-1} : a, b \in H\} \subseteq H$, then $ab^{-1} \in H$. So by theorem (a non-empty subset $H$ of a group $G$ is a subgroup of $G$ if and only if, for any pair $a, b \in H$, $ab^{-1} \in H$) $H$ is a subgroup.
**Permutable** The two subgroups $H$ and $K$ of a group $G$ are said to be permutable if and only if for any $x \in H$ and $y \in K$ there exist $x' \in H$ and $y' \in H$ such that $xy = y' x'$, i.e., $HK = KH$

1.6.3 **Theorem** Let $H$ and $K$ be subgroups of a group $G$. The product $HK$ of $H$ and $K$ is a subgroup of $G$ if and only if $H$ and $K$ are permutable.

**Proof** Let $H$ and $K$ be permutable. Then, for any $h \in H$ and $k \in K$, there exist $h' \in H$ and $k' \in K$ such that

$$hk = k'h'$$

To prove $HK$ is a subgroup, let $x, y \in HK$ and $= hk, y = h_1k_1$. Then

$$xy^{-1} = hkk_1^{-1}h_1^{-1} = hkk_1^{-1}h_1^{-1} = h_2k_2^{-1}, k_1^{-1}k_2 \in K \therefore K \text{ is a subgroup}$$

$$= hh'k_2', \quad \therefore HK = KH$$

$$= h_2'k_2', \text{ and } hh' = h_2' \in H \quad \therefore H \text{ is a subgroup.}$$

Hence $xy^{-1} \in HK$ and $HK$ is a subgroup.

Conversely, suppose that $HK$ is a subgroup. To prove $HK = KH$, let $hk \in HK, h \in H, k \in K$. Then

$$(hk)^{-1} \in HK \quad \therefore HK \text{ is a subgroup}$$

Now

$$(hk)^{-1} = k^{-1}h^{-1} = k'h' \in KH, k' = k^{-1} \in K, h' = h^{-1} \in H$$

Hence $HK \subseteq KH$.

Also for any $kh \in KH$ being the product of two elements $ek$ and $he$ of the subgroup $HK$, is in $HK$, so that $KH \subseteq HK$.

By combining the two inclusion relation we have

$$HK = KH.$$  

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

1.7 **Lagrange’s Theorem**

Let $H$ be a subgroup of a finite group $G$. Then the order and index of $H$ divides the order of $G$. 

20
Proof  Let $G$ be a group of order $n$ and $H$ be a subgroup of order $m$ in $G$. Let $\Omega$ be the collection of all left cosets of $H$ in $G$, i.e.,

$$\Omega = a_1H \cup a_2H \cup \ldots \cup a_kH \quad (k \text{ is the index of subgroup})$$

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

First we will show that $\Omega$ is a partition of $G$.

Let $a_i \in G$, then

$$a_i = a_i e \in a_iH, \quad \because e \in H$$

$$\Rightarrow a_i \in \bigcup_{i=1}^{k} a_iH$$

$$\Rightarrow G \subseteq \Omega$$

Also each $a_iH$ is a subset of $G$, therefore

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

$$\Rightarrow \Omega \subseteq G$$

By combining the two inclusion we get

$$G = \Omega$$

Now, let $aH$ and $bH$ are distinct left cosets and $x \in aH \cap bH$, then

$$x = ah_1 = bh_2 \text{ for some } h_1, h_2 \in H$$

$$\Rightarrow a = bh_2 h_1^{-1} = bh_3, h_3 = h_2 h_1^{-1} \in H$$

Now let $ah \in aH$, then

$$ah = bh_3h \in bH$$

$$\Rightarrow aH \subseteq bH \quad (1)$$

Similarly,

$$\Rightarrow b = bh_1 h_2^{-1} = bh', h' = h_2 h_1^{-1} \in H$$

Now let $bh \in bH$, then

$$bh = a h'h \in bH$$

$$\Rightarrow bH \subseteq aH \quad (2)$$
From (1) and (2), we have

\[ aH = bH \]

Contradicting the fact that \( aH \) and \( bH \) are distinct left cosets. Thus \( aH \cap bH = \emptyset \). This implies that \( \Omega \) defines a partition of \( G \).

\[ \Rightarrow |G| = |a_1 H| + |a_2 H| + \cdots + |a_k H| \quad (A) \]

To find the number of elements in each coset we define a mapping \( \varphi : H \rightarrow a_i H \) by

\[ \varphi(h) = a_i h, \quad h \in H \]

For \( h_1, h_2 \in H \)

\[ \varphi(h_1) = \varphi(h_2) \]

\[ \Rightarrow a_i h_1 = a_i h_2 \]

\[ \Rightarrow h_1 = h_2 \]

\[ \Rightarrow \varphi \text{ is one one.} \]

Also for each \( a_i h \in a_i H \) there exist \( h \in H \) such that \( \varphi(h) = a_i h \). So \( \varphi \) is onto.

Hence the number of elements in \( H \) and \( a_i H \) is the same for \( i = 1, 2, \ldots, k \).

Since \( H \) has \( m \) elements, therefore \( a_i H \) has \( m \) elements.

So from equ. \( (A) \), we have

\[ n = m + m + \cdots + m \quad (k \text{ times}) \]

\[ \Rightarrow n = km \]

\[ \Rightarrow k|n \text{ and } m|n. \text{ That is, the order and index of a subgroup divides the order of group.} \]

**Corollary**

a) Two left or right cosets of a subgroup \( H \) in a group \( G \) are either identical or disjoint.

b) Every element of \( G \) belong to one and only one left or right coset of \( H \).

**1.7.1 Theorem** Every group whose order is prime number is necessarily cyclic.

**Proof** Let \( G \) be a group of order \( p \) where \( p \) is a prime number and \( a \in G \) be a non-identity element.

Then the order \( m \) of the cyclic group \( H \) generated by \( a \) is a factor of \( p \). As \( e \neq e, m \neq 1 \) and so \( m = p \).

Thus \( H \) coincides with \( G \). Therefore \( G \) is cyclic.
RELATIONS BETWEEN GROUPS

2.1 Definitions

Normalizers

Let $X$ be an arbitrary subset of a group $G$. The set of those elements of $G$ which permute with $X$ is called normalizer of $X$ in $G$ and is denoted by $N_G(X)$. That is:

$$N_G(X) = \{ a \in G : aX = Xa \}.$$

Centralizers

The centralizers of a subset $X$ in a group $G$ is the set of those elements of $G$ which are permutable with every element of $X$. It is denoted by $C_G(X)$. That is:

$$C_G(X) = \{ a \in G : ax = xa, \forall x \in X \}.$$

The centralizer of the whole group $G$ is called the centre of $G$.

Centre Of A Group

The centre of a group $G$ is the set of those elements of $G$ which commute with every element of $G$. The centre of $G$ is denote by $\zeta(G)$. That is:

$$\zeta(G) = \{ a \in G : ag = ga, \forall g \in G \}.$$

The centre of a group $G$ is its subgroup.

Examples

a) The centre of the quaternion group $Q_8 = \{ \pm 1, \pm i, \pm j, \pm k \}$ is $\pm 1$.

b) The centre of the groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of integers, rational, real and of complex numbers under their usual addition are the corresponding groups themselves.

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

Proof Let $a, b \in N_G(X)$. Then

$$aX = Xa \text{ and } bX = Xb.$$

23
Now
\[ bX = Xb \]
\[ \Rightarrow b^{-1}bXb^{-1} = b^{-1}Xbb^{-1} = b^{-1}X \]
\[ \Rightarrow b^{-1}X = Xb^{-1} \]
\[ \Rightarrow b^{-1} \in N_G(X). \]
Hence
\[ (ab^{-1})X = a(b^{-1}X) = a(Xb^{-1}) = (aX)b^{-1} = X(ab^{-1}) \]
Therefore \( ab^{-1} \in N_G(X). \) So \( N_G(X) \) is a subgroup.

2.1.2 Theorem The centralizer \( C_G(X) \) of a subset \( X \) in a group \( G \) is a subgroup of \( G \).

Proof Let \( a, b \in C_G(X) \). Then
\[ ax = xa \text{ and } bx = xb \]
Now
\[ a^{-1}b^{-1}bxb^{-1} = b^{-1}xbb^{-1} = b^{-1}x \]
\[ \Rightarrow b^{-1}x = xb^{-1} \]
\[ \Rightarrow b^{-1} \in C_G(X). \]
Hence
\[ (ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = x(ab^{-1}) \]
Therefore \( ab^{-1} \in C_G(X). \) So \( C_G(X) \) is a subgroup.

2.1.3 Theorem Let \( G \) be a group and \( X \) be a non-empty subset of \( G \). Then prove that
\[ \zeta(G) \subseteq C_G(X) \subseteq N_G(X) \subseteq G. \]

Proof As we have already prove that
\[ \zeta(G) \subseteq G, C_G(X) \subseteq G, N_G(X) \subseteq G \]
(A)
Now it is sufficient to prove that
\[ \zeta(G) \subseteq C_G(X) \subseteq N_G(X) \]
Let \( y \in \zeta(G) \), then
\[ yx = xy, \forall x, y \in G \]
\[ yx = xy, \forall x \in X \therefore X \subseteq G \]
\[ \Rightarrow y \in C_G(X) \]
\[ \Rightarrow \zeta(G) \subseteq C_G(X) \quad (i) \]

Now, let \( y \in C_G(X) \). Then
\[ yx = xy, \forall x \in X \]
As
\[ yX = \{yx : x \in X\} = \{xy : x \in X\} = Xy \]
\[ \Rightarrow y \in N_G(X) \]
\[ \Rightarrow C_G(X) \subseteq N_G(X) \quad (ii) \]

From (i) and (ii), we have
\[ \zeta(G) \subseteq C_G(X) \subseteq N_G(X) \]

By equ. (A), we have
\[ \zeta(G) \subseteq C_G(X) \subseteq N_G(X) \subseteq G. \]

**2.1.4 Question**  Let \( G = \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle \) be the dihedral group of order 8. Its elements are \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}. The two non-empty sets of \( G \) are given below

i. \( X_1 = \{1, a^2\} \)
ii. \( X_2 = \{1, a, a^2, a^3\} \).

Find the \( \zeta(G) \), centralizers of \( X_1, X_2 \) and normalizers of \( X_1, X_2 \) in \( G \).

**Solution**  Given that

\[ (ab)^2 = 1 \]
\[ \Rightarrow (ab) = (ab)^{-1} \]
\[ \Rightarrow ab = b^{-1}a^{-1} \]
\[ \therefore a^4 = 1 \therefore a^{-1} = a^3 \]

And
\[ b^2 = 1 \therefore b^{-1} = b \]
\[ \Rightarrow ab = ba^3 \]
Moreover

\[ ab = b, ba^2 = a^2b, ba = a^3b. \]

i. Now let \( X_1 = \{1, a^2\} \). Then

\[ \zeta(G) = \{1\} \]

Because there is only the identity element \( \{1\} \) of \( G \) which commute with every element of \( G \).

Now we are to find the \( C_G(X_1) \). Since

\[ 1a^2 = a^21 \Rightarrow a^2 = a^2 \]
\[ aa^2 = a^2a \Rightarrow a^3 = a^3 \]
\[ a^2a^2 = a^2a^2 \Rightarrow a^4 = a^4 = 1 \]
\[ a^3a^2 = a^2a^3 \Rightarrow a = a \]
\[ ba^2 = a^2b \Rightarrow ba^2 = ba^2 \]
\[ aba^2 = a^2ab \Rightarrow a^3b = a^3b \]
\[ a^2ba^2 = a^2a^2b \Rightarrow b = b \]
\[ a^3ba^2 = a^2a^3b \Rightarrow ab = ab. \]

Hence \( C_G(X_1) = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\} \).

Now we are to find \( N_G(X_1) \). Since

\[ 1X_1 = X_11 \Rightarrow X_1 = X_1 \]
\[ aX_1 = \{a, a^3\} = X_1a \]
\[ a^2X_1 = \{a^2, 1\} = X_1a^2 \]
\[ a^3X_1 = \{a^3, a\} = X_1a^3 \]
\[ bX_1 = \{b, ba^2\} = \{b, a^2b\} = X_1b \]

Similarly \( ab, a^2b, a^3b \) permute with \( X_1 \). So

\[ N_G(X_1) = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}. \]

\[ \Rightarrow C_G(X_1) = N_G(X_1) = G. \]

ii. \( X_2 = \{1, a, a^2, a^3\} \).

**Solution** Do it by yourself.
2.2 Homomorphism

Let \((G, \cdot)\) and \((H, \ast)\) be two groups. A mapping \(\varphi : G \rightarrow H\) is said to be homomorphism if
\[
\varphi(x \cdot y) = \varphi(x) \ast \varphi(y)
\]
for \(x, y \in G\). The range of \(\varphi\) in \(H\) is called the homomorphic image of \(\varphi\).

**Endomorphism:** Let \((G, \ast)\) be a group. A homomorphism \(\varphi : G \rightarrow G\) is called endomorphism.

**2.2.1 Example** Let \((\mathbb{R}, +)\) and \((\mathbb{R}', \cdot)\) be two groups and \(\varphi : \mathbb{R} \rightarrow \mathbb{R}'\) be a mapping defined by \(\varphi(x) = e^x\), \(x \in \mathbb{R}\). Show that \(\varphi\) is homomorphism.

**Solution** Let \(x, y \in \mathbb{R}\), then
\[
\varphi(x + y) = e^{x+y}
\]
\[
= e^x \cdot e^y
\]
\[
= \varphi(x) \cdot \varphi(y)
\]
\[\Rightarrow \varphi \text{ is homomorphism.}\]

**2.2.2 Theorem** The homomorphic image of a cyclic group is cyclic.

**Proof** Let \(G\) be a cyclic group generated by \(a \in G\). Let \(\varphi(G)\) be a homomorphic image of \(G\) under a homomorphism of \(\varphi\).

We show that \(\varphi(G)\) is cyclic. Take, \(\varphi(x) = b\)

Let \(\in \varphi(G)\), then there is an element \(a^k \in G\) such that
\[
x = \varphi(a^k)
\]
\[
= \varphi(a \cdot a \ldots a) \quad (k \text{ times})
\]
\[
= \varphi(a) \cdot \varphi(a) \ldots \varphi(a) \quad : \varphi \text{ is homomorphism}
\]
\[
= b \cdot b \ldots b \quad (k \text{ times})
\]
\[
x = b^k
\]

So \(\varphi(G)\) is generated by \(b\). Therefore the homomorphic image of a cyclic group is cyclic.

**2.2.3 Corollary** Let \(\varphi : G \rightarrow G'\) be a homomorphism of \(G\) into \(G'\), where \(G\) and \(G'\) are groups. Then
i. The image of the identity of $G$ is the identity element in $\varphi(G)$.

ii. The image of the inverse $g^{-1}$ of $g \in G$ is the inverse of the image. That is, $\varphi(g^{-1}) = [\varphi(g)]^{-1}$.

### 2.3 Monomorphism

Let $(G, \cdot)$ and $(H, \ast)$ be two groups. A mapping $\varphi : G \to H$ is said to be monomorphism if

a) $\varphi$ is homomorphism.

b) $\varphi$ is injective.

### 2.4 Epimorphism

Let $(G, \cdot)$ and $(H, \ast)$ be two groups. A mapping $\varphi : G \to H$ is said to be epimorphism if

a) $\varphi$ is homomorphism.

b) $\varphi$ is surjective. i.e., for all $b \in H$, there is an element $a \in G$ such that $\varphi(a) = b$.

### 2.4.1 Example

Let $(\mathbb{Z}, +)$ and $\{(1, -1), \ast\}$ be two groups. Define a mapping $\varphi : \mathbb{Z} \to \{1, -1\}$ by

\[
\varphi(x) = \begin{cases} 
1 & \text{if } x \text{ is even} \\
-1 & \text{if } x \text{ is odd}
\end{cases}
\]

Prove that $\varphi$ is homomorphism and hence epimorphism.

**Proof** There are two cases.

**Case-1.** When $n$ is even.

Let $x, y \in \mathbb{Z}$, then

\[
\varphi(x \ast y) = \varphi(x + y)
\]

\[
= 1
\]

\[
= 1 \cdot 1
\]

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

$\Rightarrow \varphi$ is homomorphism.

**Case-2.** When $n$ is odd.

\[
\varphi(x \ast y) = \varphi(x + y)
\]
\[ \begin{align*}
&= 1 \\
&= -1 \cdot -1 \\
&= \varphi(x) \cdot \varphi(y)
\end{align*} \]

\[ \Rightarrow \varphi \text{ is homomorphism.} \]

\( \varphi \text{ is surjective:} \) since for every \( y \in \{1, -1\} \) there exist a pre-image \( \varphi(y) \in \mathbb{Z} \) such that \( \varphi(y) = y \).

\[ \text{Hence } \varphi \text{ is epimorphism.} \]

**Endomorphism**

Let \((G, \ast)\) be a group. A homomorphism \( \varphi : G \rightarrow G \) is called endomorphism.

**2.5 Isomorphism**

Let \((G, \cdot)\) and \((H, \ast)\) be two groups. A mapping \( \varphi : G \rightarrow H \) is said to be isomorphism if

a) \( \varphi \) is homomorphism.

b) \( \varphi \) is injective.

c) \( \varphi \) is surjective.

The isomorphism between two groups is denoted by " \( \cong \) " i.e., the isomorphism between \( G \) and \( H \) is denoted by \( G \cong H \).

**2.5.1 Example** Let \((\mathbb{Z}, +)\) and \((E, +)\) be two groups under addition. Then the mapping \( \varphi : \mathbb{Z} \rightarrow E \) defined by \( \varphi(n) = 2n \) is isomorphism.

**Solution** Let \( n_1, n_2 \in \mathbb{Z} \), then

\[ \varphi(n_1 + n_2) = 2(n_1 + n_2) \]
\[ = 2n_1 + 2n_2 \]
\[ = \varphi(n_1) + \varphi(n_2) \]

\[ \Rightarrow \varphi \text{ is homomorphism.} \]

Now we prove \( \varphi \) is injective.

Let \( \varphi(n_1) = \varphi(n_2) \), \( \forall n_1, n_2 \in \mathbb{Z} \)

\[ \Rightarrow 2n_1 = 2n_2 \]
\[ \Rightarrow 2n_1 - 2n_2 = 0 \]
\[ \Rightarrow 2(n_1 - n_2) = 0 \]

But since \(2 \neq 0\), so \(n_1 - n_2 = 0\)

\[ \Rightarrow n_1 = n_2 \]

\(\Rightarrow \phi\) is injective.

Also \(\phi\) is surjective (onto), for \(2n \in E\), there exist a pre-image \(n \in \mathbb{Z}\) such that \(\phi(n) = 2n\). Hence \(\phi\) is isomorphism.

**2.5.2 Example**  Let \((\mathbb{R}^+, \cdot)\) and \((\mathbb{R}, +)\) be two groups, then the mapping \(\phi : \mathbb{R}^+ \rightarrow \mathbb{R}\) defined by \(\phi(x) = \log x\) is isomorphism.

**Solution**  Let \(x, y \in \mathbb{R}^+\), then

\[
\phi(x \cdot y) = \log(xy) \\
= \log x + \log y \\
= \phi(x) + \phi(y)
\]

\(\Rightarrow \phi\) is homomorphism.

Now we prove \(\phi\) is injective. Let

\[
\phi(x) = \phi(y), \; \forall \; x, y \in \mathbb{R}^+ \\
\Rightarrow \log x = \log y
\]

By taking anti-log both sides, we get

\[ x = y \]

\(\Rightarrow \phi\) is injective.

Also \(\phi\) is surjective (onto), for \(\log x \in \mathbb{R}\) there exist a pre-image \(x \in \mathbb{R}^+\) such that \(\phi(x) = \log x\). Hence \(\phi\) is isomorphism. That is \(\mathbb{R}^+ \cong \mathbb{R}\).

**Kernel of \(\phi\)**  Let \((G, \cdot)\) and \((H, \ast)\) be two groups. Let \(\varphi : G \rightarrow H\) be a homomorphism of group.

The set of those elements of \(G\) which are mapped on the identity \(e\) of \(H\) is called the kernel of \(\varphi\) and is denoted by \(\text{Ker} \, \varphi\). Thus

\[ \text{Ker} \, \varphi = \{k \in G : \varphi(k) = e\}. \]

**Embedding:** An embedding of a group \(G\) into a group \(G'\) is simply a monomorphism of \(G\) into \(G'\). In other words, if \(G\) is embedded in a group \(G'\) then \(G'\) contains a subgroup \(H'\) isomorphic to \(G\).
**Cayley’s Theorem**

**Statement:** Any group $G$ can be embedded in a group of bijective mappings of a certain set.

**Proof:** Let $G$ be a group. For each $g \in G$, define a mapping $\varphi_g : G \to G$ by

$$\varphi_g(x) = gx, \quad \forall x \in G.$$  

To prove $\varphi_g$ is a bijective mapping, let

$$\varphi_g(x) = \varphi_g(y)$$

$$\Rightarrow gx = gy$$  \hspace{1cm} \text{(left cancelation law)}

$$\Rightarrow x = y$$

$\Rightarrow \varphi_g$ is one-one.

Also $\varphi_g$ is onto because each $y \in G$ is the image of $g^{-1}y \in G$.

$\Rightarrow \varphi_g$ is a bijective mapping.

Now, put

$$\Phi_G = \{ \varphi_g : g \in G \}$$

Let $\varphi_g, \varphi_g' \in \Phi_G$. Then for any $x \in G$

$$(\varphi_g \varphi_g')(x) = \varphi_g(\varphi_g'(x)) = \varphi_g(g'x) = gg'x = \varphi_{gg'}(x), \forall \ g, g' \in G.$$  

Hence

$$\varphi_g \cdot \varphi_g' = \varphi_{gg'} \in \Phi_G.$$  

Implies that, $\Phi_G$ is a subgroup of the group of all bijective mappings of the set $G$, as $\varphi_e$ for $e \in G$ is the identity element and for each $g \in G$, $\varphi_g^{-1}$ is the inverse of $\varphi_g \in \Phi_G$.

Now we show that $G$ is isomorphic to $\Phi_G$. For this, define a mapping $\psi : G \to \Phi_G$ by

$$\psi(g) = \varphi_g, \forall g \in G.$$  

To prove $\psi$ is one-one, let

$$\psi(g_1) = \psi(g_2), \ g_1, g_2 \in G$$

$\Rightarrow \quad \varphi_{g_1} = \varphi_{g_2}$
\[ \Rightarrow \varphi_{g_1} \cdot \varphi_{g_2}^{-1} = \varphi_e \]
\[ \Rightarrow \varphi_{g_1g_2^{-1}} = \varphi_e \ (\Phi_G \text{ is closed}) \]
\[ \Rightarrow g_1g_2^{-1} = e \]
\[ \Rightarrow g_1 = g_2 \]

\[ \Rightarrow \psi \text{ is one-one.} \]

Also \( \psi \) is onto because each \( \varphi_g \in \Phi_G \) is the image of \( g \in G \).

Moreover if \( g_1, g_2 \in G \), then

\[ \psi(g_1g_2) = \varphi_{g_1g_2} = \varphi_{g_1} \cdot \varphi_{g_2} = \psi(g_1) \cdot \psi(g_2) \]

So that \( \psi \) is homomorphism.

Hence \( G \) is isomorphic to \( \Phi_G \). Therefore \( G \) is embedded in a group of all bijective mappings of a set namely \( G \).

**Corollary:** Every finite group of order \( n \) can be embedded in a group of bijective mappings of a set consisting of \( n \) elements.

### 2.6 Conjugacy Relation In Groups

Let \( G \) be a group. For any \( a \in G \), the element \( gag^{-1}, g \in G \) is called the conjugate or transform of \( a \) by \( g \).

Two elements \( a, b \in G \) are said to be conjugate if and only if there exists an element \( g \in G \) such that

\[ b = gag^{-1} \]

**2.6.1 Theorem** The relation of conjugacy between elements of a group is an equivalence relation.

**Proof** Let us denote the relation of conjugacy between elements of a group by \( R \), then

i. **Reflexive:** \( R \) is reflexive i.e \( aRa \) because the identity element \( e \in G \) and \( eae^{-1} = a \).

ii. **Symmetric:** \( R \) is symmetric because if \( aRb \) for \( a, b \in G \), then there exists \( g \in G \) such that \( b = gag^{-1} \)

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

So that \( bRa \).
iii. **Transitive**: Let \( aRb \) and \( bRc \), then there exists \( g, g' \in G \) such that
\[
b = gag^{-1}, c = g'bg'^{-1}
\]
Now
\[
c = g'bg'^{-1} = g'gag^{-1}g'^{-1} = (g'g)(g'g)^{-1}
\]
Thus \( aRc \), so \( R \) is transitive.
Hence \( R \) is an equivalence relation in \( G \).

**Conjugacy Class**

An equivalence class determined by the conjugacy relation between elements in \( G \) is called conjugacy class. A conjugacy class consisting of elements conjugate to an element \( a \) of \( G \) is denoted by \( C_a \).

**Self Conjugate**

An element \( a \in G \) is called self conjugate if for any \( g \in G \), \( a = gag^{-1} \). This element is also called a central element.

**2.6.2 Theorem** The number of elements in a conjugacy class \( C_a \) of an element \( a \) in a group \( G \) is equal to the index of its normalizer in \( G \). Thus
\[
|C_a| = |G : N_a(x)|.
\]

**Proof** Let \( G \) be group and \( a \in G \). Let \( C_a \) be the conjugacy class of \( G \) containing \( a \). Let \( N = N_a(a) \) i.e the normalizer of \( a \) in \( G \). Let \( \Omega \) be the collection of right cosets of normalizer.

We have to show that number of elements in \( \Omega \) is equal to the number of elements in \( C_a \).

Define a mapping \( \varphi: \Omega \rightarrow C_a \) by
\[
\varphi(Ng) = g^{-1}ag, \ g \in G.
\]

i. \( \varphi \) is well defined.

Let
\[
Ng = Ng', \ g, g' \in G
\]
\[
\Rightarrow N = Ng'g^{-1}
\]
\[
\Rightarrow g'g^{-1} \in N \quad \because \text{if } a \in H \text{ then } aH = H
\]
\[
\Rightarrow g'g^{-1} = n \quad \text{(say } n \in N)\]
\[
\Rightarrow g' = ng
\]
Now
\[
g^{-1}a g' = (ng)^{-1}a(n g) = (g^{-1}n^{-1})a(n g) = g^{-1}(n^{-1}a)g = g^{-1} a \quad \because n^{-1}a = a
\]
\[
\Rightarrow \varphi(Ng') = \varphi(Ng)
\]
\[
\Rightarrow \varphi \text{ is well defined.}
\]

ii. \( \varphi \) is one-one.

Let
\[
\varphi(Ng') = \varphi(Ng)
\]
\[
\Rightarrow \quad g^{-1}a g' = g^{-1}ag
\]
\[
\Rightarrow \quad g(g^{-1}ag')g^{-1} = a
\]
\[
\Rightarrow \quad (g'g)^{-1}a(g'g^{-1}) = a
\]
\[
\Rightarrow \quad g'g^{-1} \in N
\]
\[
\Rightarrow \quad g' \in Ng
\]

But \( g' \in Ng' \).

\[
\Rightarrow \quad Ng' \subseteq Ng
\]

Similarly
\[
Ng \subseteq Ng'
\]

Thus \( Ng = Ng' \). So \( \varphi \) is one-one.

iii. Also \( \varphi \) is onto because each \( g^{-1}ag \in C_a \) is the image of a right coset \( Ng \).

Hence \( \varphi \) is bijective.

Consequently the sets \( \Omega \) and \( C_a \) have the same number of elements. Therefore the number of elements in \( C_a \) is equal to the index of the normalize of \( a \). That is
\[
|C_a| = |G : N_a(x)|.
\]
Corollary:
- Let $G$ be a finite group and $a \in G$. Then the number elements in the conjugacy class $C_a$ divides the order of $G$.
- The number of elements in a conjugacy class of an element in a group is finite if and only if the index of the normalizer of that element is finite.

Conjugate Subgroup

Let $G$ be a group and $H$ be a subgroup of $G$. Then for each $g \in G$, the set

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

is a subgroup of $G$ and it is called a conjugate subgroup of $G$.

A conjugacy class of a subgroup $H$ is a collection of all subgroups of $G$ which are conjugate to $H$.

2.6.3 Theorem Any two conjugate subgroups of a group $G$ are isomorphic.

Proof Let $H, K$ are two conjugate subgroups of $G$. Then for some $g \in G$

$$K = gHg^{-1}.$$ 

The mapping $\varphi : H \rightarrow K$ is given by $\varphi(h) = ghg^{-1} \in K$. Then $\varphi$ is obviously well-defined.

i. $\varphi$ is one-one.

Let

$$\varphi(h_1) = \varphi(h_2), \quad h_1, h_2 \in H$$

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

$$\Rightarrow h_1 = h_2$$

ii. Also $\varphi$ is onto because each $ghg^{-1} \in K$ is the image of $h \in H$.

So $\varphi$ is bijective. Now we will show that $\varphi$ is homomorphism.

Let $h_1, h_2 \in H$, then

$$\varphi(h_1h_2) = gh_1h_2g^{-1}$$

$$= gh_1g^{-1}gh_2g^{-1}$$
\[ \Rightarrow \varphi(h_1h_2) = \varphi(h_1) \cdot \varphi(h_2). \]

Hence \( H \) and \( K \) are isomorphic.

**Note:** Two conjugate subgroups of a group have the same order.

### 2.7 Double cosets

Let \( H, K \) be two subgroups of a group \( G \) and \( a \) be an arbitrary element of \( G \). Then the set

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

is called a double coset in \( G \) modulo \((H, K)\) determine by \( a \).

**2.7.1 Theorem** Let \( H, K \) be two subgroups of a group \( G \). Then the collection \( \Omega \) of all double cosets \( HaK, a \in G \) is a partition of \( G \).

**Proof** Let \( H, K \) be two subgroups of a group \( G \) and \( \Omega \) be the collection of all double cosets \( aK, a \in G \).

We have to show that \( \Omega \) defines a partition of \( G \). For this we will show that

i. \( \bigcup_{a \in G} HaK = G \)

ii. \( HaK \cap HbK = \emptyset \).

First we will prove \( \bigcup_{a \in G} HaK = G \). Let \( a \in G \), then

\[ a = eae \in HaK \]

\[ \Rightarrow a \in HaK \]

\[ \Rightarrow a \in \bigcup_{a \in G} HaK \]

\[ \Rightarrow G \subseteq \bigcup_{a \in G} HaK \quad (i) \]

But

\[ \bigcup_{a \in G} HaK \subseteq G \quad (ii) \]

From (i) and (ii), we have

\[ \bigcup_{a \in G} HaK = G. \]

Now we will prove that \( HaK \cap HbK = \emptyset \). Let \( HaK \) and \( HbK \) be distinct double cosets in \( G \) and suppose that \( x \in HaK \cap HbK \neq \emptyset \).

\[ \Rightarrow x \in HaK, x \in HbK \]

\[ \Rightarrow x = h_1ak_1, x = h_2bk_2 \]
Where \( h_1, h_2 \in H, k_1, k_2 \in K \) and \( a, b \in G \).

\[
\Rightarrow h_1 ak_1 = h_2 bk_2
\]

\[
\Rightarrow a = h_1^{-1} h_2 bk_2 k_1^{-1} \quad (iii)
\]

Now, let \( y \in HaK \).

\[
\Rightarrow y = h_3 ak_3, \ h_3 \in H, k_3 \in K
\]

From equ. \((iii)\), we have

\[
y = h_3 h_1^{-1} h_2 bk_2 k_1^{-1} k_3
\]

\[
\Rightarrow y = h_4 bk_4
\]

Where \( h_4 = h_3 h_1^{-1} h_2 \in H \) and \( k_4 = k_2 k_1^{-1} k_3 \in K \).

\[
\Rightarrow y \in HbK
\]

\[
\Rightarrow HaK \subseteq HbK \quad (A)
\]

Similarly

\[
HbK \subseteq HaK \quad (B)
\]

From \((A)\) and \((B)\), we have

\[
HaK = HbK
\]

This is contradiction to our supposition. Hence \( HaK \) and \( HbK \) are disjoint i.e \( HaK \cap HbK = \emptyset \).

Therefore the double cosets of \( G \) modulo \((H, K)\) define a partition of \( G \).

**Complexes In A Group:** An arbitrary subset \( X \) of a group \( G \) is called a complex in \( G \). For two complexes \( X \) and \( Y \) in \( G \) we define their product as a complex \( XY \) given by

\[
XY = \{xy : x \in X, y \in Y\}.
\]

**2.7.2 Theorem** let \( A \) and \( B \) be finite subgroups of a group \( G \). Then the complex \( AB \) contains exactly \( mn/q \), where \( m, n \) and \( q \) are respectively the orders of \( A, B \) and \( Q = A \cap B \).

**Proof** Since \( Q \) is the intersection of the subgroups \( A \) and \( B \) of a group \( G \). Therefore \( Q \) is also a subgroup of \( G \).

Since \( A \) and \( B \) are finite subgroups of \( G \), therefore the order \( q \) of \( Q \) and the index \( r = n/q \) in \( B \) is finite. Let \( B = \bigcup_{i=1}^{r} Qb_i \) be a right coset decomposition of \( B \). Then only one \( b_i = e \) and \( b_i \notin Q \) for \( i > 1 \) so that the set \( Qb_1 \neq Q \). Also
\[ AB = A \bigcup_{i=1}^{r} Qb_i \]
\[ = \bigcup_{i=1}^{r} AQb_i \quad (A) \]

Since \( Q \) is the subgroup of \( A \). Therefore

\[ AQ = \{ Ax : x \in Q \} = A. \]

So eqn. (A) becomes

\[ AB = \bigcup_{i=1}^{r} Ab_i \]

As \( b_i \in B \) and \( b_i \notin Q \), which shows that \( b_i \notin A \) for \( i > 1 \), the cosets \( Ab_i, i = 1, 2, \ldots, r \), are all distinct. Each of these cosets contains exactly \( m \) elements and there are \( r \) such cosets.

\[ \Rightarrow |AB| = \sum_{i=1}^{r} |Ab_i| \]
\[ = |Ab_1| + |Ab_2| + \cdots + |Ab_r| \]
\[ = r|A| \]
\[ = \frac{n}{q} \cdot m \]
\[ \Rightarrow |AB| = \frac{mn}{q}. \]

Hence the complex \( AB \) contains exactly \( \frac{mn}{q} \) elements.