Lecture Notes On

GROUP THEORY

By

MUHAMMAD IFTIKHAR
Sidram0520@gmail.com

DEPARTEMENT OF MATHEMATICS
PMAS ARID AGRICULTURE UNIVERSITY
RAWALPINDI, PAKISTAN

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 2×2 matrices together with the single operation of matrix multiplication. The integers and the 2×2 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×S into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$.

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 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.*,

$$a * b = b * \mathrm{a} \quad ,\forall a, b \in G$$

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 iis 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 is 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 , $b \in G$, then G is called an abelian group iff

$$a * b = b * a$$

1.2.1 Examples

a. 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 $\boldsymbol{M_{m\times n}}(\mathbb{R})$ 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 $\boldsymbol{M_n}(\mathbb{R})$ 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 $f, g, \dots, h$ of one of them, say x, and if for any two of these roots, $f(x)$ and $g(x)$, the relation $f\big(g(x)\big) = g\big(f(x)\big)$ 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 $a * \mathrm{b} = \frac{ab}{2}$. Then $(a * \mathrm{b}) * \mathrm{c} = \frac{ab}{2} * c = \frac{abc}{4}$, and likewise $a * (b * c) = a * \frac{ab}{2} = \frac{abc}{4}$.

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

i. Closed property.

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

Thus closed property holds.

ii. Associative property.
For $a, b, c \in \mathbb{Q}^+$,

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

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

Thus associative law holds.

iii. Identity.

Given that $a * \mathrm{b} = \frac{ab}{2}$.

Let $e \in \mathbb{Q}^+$, since

$$a * e = e * a = a$$

Now $$a * e = \frac{ae}{2}$$

$$\Rightarrow a * 2 = \frac{a \times 2}{2} = a$$

Similarly $$2 * a = \frac{2 \times a}{2} = a$$

Thus $e = 2$ is the identity element.

iv. Inverse.
For $a \in \mathbb{Q}^+$,since

$$a * a' = a' * a = e$$

By computing

$$a * a' = \frac{aa'}{2}$$
$$a * \frac{4}{a} = \frac{a \times 4}{2 \times a} = 2$$

Similarly

$$\frac{4}{a} * a = 2$$

$\Rightarrow a' = \frac{4}{a}$ is the inverse of a. Hence inverse of each element exists. Thus $(\mathbb{Q}^+ ,*)$ is a group.

1.2.3 Example Show that the subset S of $\boldsymbol{M_n}(\mathbb{R})$ 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

$$(AB)(AB)^{-1} = (AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = I_n$$

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.

$\mu : \mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{C} \cup \{\infty\}$ defined by

$$\mu(z) = \frac{az+b}{cz+d} \ , cz+d \neq 0 \ , z \in \mathbb{C} \cup \{\infty\}$$

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

$I : \mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{C} \cup \{\infty\}$ given by

$$I(z) = z \ , \forall\, z \in \ \mathbb{C} \cup \{\infty\}$$

Is the identity element of M. Also for each μ in M, its inverse is the mapping

$\mu' \ : \ \mathbb{C} \cup \{\infty\} \longrightarrow \mathbb{C} \cup \{\infty\}$ 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

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

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

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 $\mathbb{Z} = \{\dots, -3, -2, -1, 0, +1, +2, +3, \dots\}$ 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 $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$.

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

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

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 dnoted 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

$$a.b = c = b.a$$

$$a.c = b = c.a$$

$$b.c = a = c.b$$

The Klien four-group is not cyclic and it is an abelian group. The Cayley's table for K_4 is given by

$\times$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

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

$$H_1 = \{e\}$$

$$H_2 = \{e, a\} \quad , \quad H_4 = \{e, c\}$$

$$H_3 = \{e, b\} \quad , \quad H_5 = K_4$$

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 2*n.* Let

$$A = \{x \in G : x^2 = e\} , \qquad B = \{y \in G : y^2 \neq e\} .$$

Then, we have

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

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

$$y^2 \neq e , \; y^{-1} \neq y$$

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 $H \preccurlyeq G$ or $G \succcurlyeq H$.

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 nth root of unity in $\mathbb{C}_n$ 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 $(H,*)$ 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 $a, b \in H \Rightarrow a, b^{-1} \in H$

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

$$\Rightarrow \quad ab \in H$$

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_α 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, $H \cup K = H \because K \subseteq H$

$$H \cup K = K \because H \subseteq K$$

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

$$H \nsubseteq K\,,\, K \nsubseteq H$$

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

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

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

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

Similarly, suppose $b \in K$, then

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

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
$$\begin{aligned}(ab)^{mn} &= ab.ab.ab\ldots ab \quad (mn \text{ times})\\ &= a^{mn}.b^{mn}\\ &= (a^m)^n.(b^n)^m = e^n.e^m\\ &= e\end{aligned}$$

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

Also, if $b \in H$ and $b^n = e$, then

$$(b^{-1})^n = b^{-1}.b^{-1}.b^{-1} \ldots b^{-1} \quad \text{(n times)}$$

$$= b^{-n} = (b^n)^{-1} = (e)^{-1} = e$$

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

1.5 Cyclic Group

A group G is said to be cyclic if and only qAQWD 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

$$G = < a : a^n = e >.$$

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 $< i >$ 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 , $y \in G$, then there exist integers m and n such that

$$x = a^m \quad , \; y = a^n$$

Now $$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$$

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

$$m = kq + r\ , 0 \le r \le k$$

$$\Rightarrow \quad a^m = a^{kq} + a^r$$

$$= (a^k)^q . a^r$$

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

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

$$m = qk$$

$$\Rightarrow \quad a^m = a^{kq}$$

$$\Rightarrow \quad a^m = (a^k)^q \in H$$

$\Rightarrow a^k$ 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

$$n = mq + r \quad , \quad 0 \le r \le m$$

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 $d = \gcd(r, s)$. 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., $\gcd(42,72) = 6$.

$$\mathrm{d} = \mathrm{nr} + \mathrm{ms}$$

$$6 = (72)(6) + (42)(-5)$$

$$\Rightarrow \mathrm{n} = 6\ ,\ \mathrm{m} = -5$$

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 $n = kd$.

$$\Rightarrow ld = rkd$$

$$\Rightarrow \quad l = rk$$

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

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

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

Let H be a subgroup generated by a^k. Now will prove that $H = G$.
From (A), we have

$$a^{kp+nq} = a^1$$

$$\Rightarrow \quad a^{kp}.a^{nq} = a$$

$$\Rightarrow (a^k)^p.(a^n)^q = a$$

$$\Rightarrow \quad (a^k)^p.(e)^q = a$$

$$\Rightarrow \quad (a^k)^p = a$$

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

$$(a^k)^p = a$$

$$a^{kp} = a$$

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

So $n|kp-1$, because n is the least such integer. So there exist integer q such that

$$\Rightarrow \quad kp - 1 = nq$$

$$\Rightarrow kp - nq = 1$$

$\Rightarrow k$ and n are relatively prime.

b) Let $G =< a >$ be an infinite cyclic group. Let a^k is also the generator of G. Then, there exist an integer p such that

$$(a^k)^p = a$$

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

$\Rightarrow kp - 1 = 0$ or $kp - 1 \neq 0$.

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

$$\Rightarrow \quad kp = 1$$

Since k and p are integers. Therefore, either $k = p = 1$ or $k = p = -1$ ie., a and a^{-1} are the only generators.

Exponent 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 $a \in G$.

1.5.7 Theorem An abelian group G of order n is cyclic if and only if it has exponent n.

Proof Let $G =< a : a^n = e >$ 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

$$(ab)^k = e = a^k . b^k$$

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

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

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

Hence $k|pq$. thus

$$k = pq \qquad\qquad \because (ab)^k = e$$

$\Rightarrow$ 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

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

Where $\alpha_i \geq 0$, $\beta_j \geq 0$, $1 \leq i \leq r$, $1 \leq j \leq s$. If $y^m \neq e$ 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

$$x' = x^{p_1^{\beta 1}} , y' = y^{p_2^{\alpha 2} \dots p_r^{\alpha r}}$$

Then $$(x')^{p_2^{\beta 2} \dots p_s^{\beta s}} = x^m = e$$

and $$(y')^{p_1^{\alpha 1}} = y^{p_1^{\alpha 1}p_2^{\alpha 2}\ldots p_r^{\alpha r}} = y^k = e$$

Since $$\left(\mathrm{p}_1^{\alpha 1}, \mathrm{p}_2^{\beta 2} \ldots \mathrm{p}_s^{\beta_s}\right) = 1,$$

$\mathrm{x}'\mathrm{y}'$ has order $\mathrm{p}_1^{\alpha 1}\, \mathrm{p}_2^{\beta 2} \ldots \mathrm{p}_s^{\beta_s} > m$. This contradicts our choice of x. Hence $y^m = e$, so that m is the 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,

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

$$a^r = e \qquad \because a^k = e$$

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

$\mathrm{h} = 1,2,4,5,7,8$ are all those elements which are relatively prime to 9, so $\mathrm{h}2 = 2,4,8,10,14,16$.

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

$$G = \{a, a^2, a^3, \dots, a^{12} = e\}$$

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

$\cup (12) = \{1,5,7,,11\}$, 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 $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ be a group. Since $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ and

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

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

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

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

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

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

$$\Rightarrow 3 + 3\mathbb{Z} = 3\mathbb{Z}$$

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:

a) **Reflexive:** Let $a \in \mathrm{G}$ then $aa^{-1} = e$, $e \in \mathrm{H}$. since H is a subgroup thus $a \sim_L a$.

b) **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 $b \sim_L a$.

c) **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

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

$\Rightarrow HH^{-1} \subseteq H.$

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

$$xy = y'x' \text{ . i.e., } HK = KH$$

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 amd 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

$$\begin{aligned} xy^{-1} &= hk.(h_1k_1)^{-1} \\ &= hkk_1^{-1}h_1^{-1} \\ &= hk_2h_1^{-1} \quad , kk_1^{-1} = k_2 \in K \because K \text{ is a subgroup} \\ &= hh'k_2' \quad , \qquad \because HK = KH \\ &= h_2'k_2' \quad , hh' = h_2' \in H \quad \because H \text{ is a subgroup.} \end{aligned}$$

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

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

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

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.

Proof Let G be a group of order n and H be a subgroup of order m in G. Let Ω be the collection of all left cosets of H in G. *i.e.,*

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

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

First we will show that Ω is a partition of G.

Let $a_i \in G$, then $\qquad a_i = a_ie \in a_iH, \ \because \ e \in H$

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

$$\Rightarrow \ G \subseteq \Omega$$

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

$$ah = bh_3h \in bH$$

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

Similarly,

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

Now let $bh \in bH$, then

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

$$\Rightarrow \ bH \subseteq aH \qquad\qquad (2)$$

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 Ω defines a partition of G.

$$\Rightarrow |G| = |a_1 H| + |a_2 H| + \cdots + |a_k H| \qquad (A)$$

To find the number of elements in each coset we define a mapping $\varphi: H \longrightarrow a_i H$ by

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

For $h_1, h_2 \in H$

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

$$\Rightarrow a_i h_1 = a_i h_2$$

$$\Rightarrow \quad h_1 = h_2$$

$\Rightarrow$ φ 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 φ is onto.

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

Since H has m elements, therefore $a_i H$ has m elements.

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

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

$$\Rightarrow n = km$$

$\Rightarrow k|n$ and $m|n$. 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 $\neq e$, $m \neq 1$ 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 ± 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

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

Now

$$bX = Xb$$

$$\Rightarrow b^{-1}bXb^{-1} = b^{-1}Xbb^{-1} = b^{-1}X$$

$$\Rightarrow \qquad b^{-1}X = Xb^{-1}$$

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

$$\Rightarrow b^{-1}bxb^{-1} = b^{-1}xbb^{-1} = b^{-1}x$$

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

$\Rightarrow b^{-1} \in C_G(X)$. 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

$$\zeta(G) \subseteq G, C_G(X) \subseteq G, N_G(X) \subseteq G \qquad \text{(A)}$$

Now it is sufficient to prove that

$$\zeta(G) \subseteq C_G(X) \subseteq N_G(X)$$

Let $y \in \zeta(G)$, then

$$yx = xy \ , \forall\, x, y \in G$$

$$\Rightarrow yx = xy \ , \forall\, x \in X \quad \because X \subseteq G$$

$$\Rightarrow \quad y \in C_G(X)$$

$$\Rightarrow \zeta(G) \subseteq C_G(X) \qquad \textit{(i)}$$

Now, let $y \in C_G(X)$. Then

$$yx = xy \ , \forall\, x \in X$$

As
$$yX = \{yx : \ x \in X\}$$

$$= \{xy : \ x \in X\}$$

$$= Xy$$

$$\Rightarrow \quad y \in N_G(X)$$

$$\Rightarrow C_G(X) \subseteq N_G(X) \qquad \textit{(ii)}$$

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 $G =< a, b: a^4 = b^2 = (ab)^2 = 1 >$ 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

$$(ab)^2 = 1$$

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

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

$$\because a^4 = 1 \therefore a^{-1} = a^3$$

And
$$\because b^2 = 1 \therefore b^{-1} = b$$

$$\Rightarrow ab = ba^3$$

Moreover

$$aba = b\,, ba^2 = a^2b, ba = a^3b.$$

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

$$1a^2 = a^2 1 \quad \Rightarrow a^2 = a^2$$

$$aa^2 = a^2 a \quad \Rightarrow a^3 = a^3$$

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

$$a^3a^2 = a^2a^3 \ \Rightarrow a = a$$

$$ba^2 = a^2b \quad \Rightarrow ba^2 = ba^2$$

$$aba^2 = a^2ab \Rightarrow a^3b = a^3b$$

$$a^2ba^2 = a^2a^2b \Rightarrow b = b$$

$$a^3ba^2 = a^2a^3b \Rightarrow ab = ab.$$

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

$$1X_1 = X_1 1 \Rightarrow X_1 = X_1$$

$$aX_1 = \{a, a^3\} = X_1 a$$

$$a^2X_1 = \{a^2, 1\} = X_1 a^2$$

$$a^3X_1 = \{a^3, a\} = X_1 a^3$$

$$bX_1 = \{b, ba^2\} = \{b, a^2b\} = X_1 b$$

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 $(H\ ,*)$ be two groups. A mapping $\varphi : G \longrightarrow H$ is said to be homomorphism if

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

for $x, y \in G$. The range of φ in H is called the **homomorphic image** of φ.

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

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

Solution Let $x, y \in \mathbb{R}$, then

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

$\Rightarrow$ φ 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 φ.

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

$$\begin{aligned}x &= \varphi(a^k)\\ &= \varphi(a.a \dots a) && (k \text{ times})\\ &= \varphi(a).\varphi(a) \dots \varphi(a) && \because \varphi \text{ is homomorphism}\\ &= b.b \dots b && (k \text{ times})\\ x &= b^k\end{aligned}$$

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

2.2.3 Corollary Let $\varphi : G \longrightarrow G'$ 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 $(H\,,*)$ be two groups. A mapping $\varphi : G \longrightarrow H$ is said to be monomorphism if

a) φ is homomorphism.
b) φ is injective.

2.4 Epimorphism

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

a) φ is homomorphism.
b) φ 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 $(\{1,-1\}\,,\cdot)$ be two groups. Define a mapping $\varphi : \mathbb{Z} \longrightarrow \{1,-1\}$ by

$$\varphi(x) = 1 \text{ , if } n \text{ is even}$$

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

Prove that φ is homomorphism and hence epimorphism.

Proof There are two cases.

Case-1. When n is even.

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

$$\begin{aligned}\varphi(x * y) &= \varphi(x + y)\\ &= 1\\ &= 1 \cdot 1\\ &= \varphi(x) \cdot \varphi(y)\end{aligned}$$

$\Rightarrow \varphi$ is homomorphism.

Case-2. When n is odd.

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

$$= 1$$

$$= -1 \cdot -1$$

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

$\Rightarrow \varphi$ is homomorphism.

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

Endomorphism

Let $(G, *)$ be a group. A homomorphism $\varphi : G \longrightarrow G$ is called endomorphism.

2.5 Isomorphism

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

a) φ is homomorphism.
b) φ is injective.
c) φ 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 $\varphi : \mathbb{Z} \longrightarrow E$ defined by $\varphi(n) = 2n$ is isomorphism.

Solution Let $n_1, n_2 \in \mathbb{Z}$, then

$$\varphi(n_1 + n_2) = 2(n_1 + n_2)$$

$$= 2n_1 + 2n_2$$

$$= \varphi(n_1) + \varphi(n_2)$$

$\Rightarrow \varphi$ is homomorphism.

Now we prove φ is injective.

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

$$\Rightarrow \qquad 2n_1 = 2n_2$$

$$\Rightarrow 2n_1 - 2n_2 = 0$$

$$\Rightarrow 2(n_1 - n_2) = 0$$

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

$$\Rightarrow \qquad n_1 = n_2$$

$\Rightarrow$ φ is injective.

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

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

Solution Let $x, y \in \mathbb{R}^+$, then

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

$$= \log x + \log y$$

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

$\Rightarrow$ φ is homomorphism.

Now we prove φ is injective. Let

$$\varphi(x) = \varphi(y) \ , \ \forall \ x, y \in \mathbb{R}^+$$

$$\Rightarrow \log x = \log y$$

By taking anti-log both sides, we get

$$x = y$$

$\Rightarrow$ φ is injective.

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

Kernel of $\boldsymbol{\varphi}$ Let $(G\ , \ \cdot)$ and $(H\ , *)$ be two groups. Let $\varphi : G \longrightarrow H$ 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 φ and is denoted by $\boldsymbol{Ker\ \varphi}$**.** Thus

$$Ker\ \varphi = \{k \in G : \ \varphi(k) = e\}.$$

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 $\varphi_g : G \longrightarrow G$ by

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

To prove φ_g is a bijective mapping, let

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

$$\Rightarrow gx = gy \qquad\qquad \text{(left cancelation law)}$$

$$\Rightarrow \quad x = y$$

$\Rightarrow \varphi_g$ is one-one.

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

$\Rightarrow \varphi_g$ is a bejective mapping.

Now, put

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

Let $\varphi_g, \varphi_{g'} \in \Phi_g$. Then for any $x \in G$

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

Hence

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

Implies that, Φ_G is a subgroup of the group of all bijective mappings of the set G, as φ_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 Φ_G. For this, define a mapping $\psi: G \longrightarrow \Phi_G$ by

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

To prove ψ is one-one, let

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

$$\Rightarrow \qquad \varphi_{g_1} = \varphi_{g_2}$$

$$\Rightarrow \varphi_{g_1}.\varphi_{g_2^{-1}} = \varphi_e$$

$$\Rightarrow \quad \varphi_{g_1 g_2^{-1}} = \varphi_e \quad , (\Phi_G \text{ is closed})$$

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

$$\Rightarrow \quad g_1 = g_2$$

$\Rightarrow$ ψ is one-one.

Also ψ 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

$$\psi(g_1 g_2) = \varphi_{g_1 g_2}$$

$$= \varphi_{g_1}.\varphi_{g_2}$$

$$= \psi(g_1).\psi(g_2)$$

So that ψ is homomorphism.

Hence G is isomorphic to Φ_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

$$c = g'bg'^{-1} = g'gag^{-1}g'^{-1} = (g'g)a(g'g)^{-1}$$

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 $N = N_G(a)$ i.e the normalizer of a in G. Let Ω be the collection of right cosets of normalizer.

We have to show that number of elements in Ω is equal to the number of elements in C_a.

Define a mapping $\varphi : \Omega \longrightarrow C_a$ by

$$\varphi(Ng) = g^{-1}ag, \ g \in G.$$

i. φ is well defined.

Let

$$Ng = Ng' \quad , \ g, g' \in G$$

$$\Rightarrow \quad N = Ng'g^{-1}$$

$$\Rightarrow \quad g'g^{-1} \in N \qquad \because \text{if } a \in H \text{ then } aH = H$$

$$\Rightarrow \quad g'g^{-1} = n \qquad (say\ n \in N)$$

$$\Rightarrow \quad g' = ng$$

Now

$$g'^{-1}ag' = (ng)^{-1}a(ng)$$
$$= (g^{-1}n^{-1})a(ng)$$
$$= g^{-1}(n^{-1}an)g$$
$$= g^{-1}ag \qquad \because n^{-1}an = a$$
$$\Rightarrow \varphi(Ng') = \varphi(Ng)$$

$\Rightarrow \varphi$ is well defined.

ii. φ is one-one.

Let

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

But $g' \in Ng'$.

$$\Rightarrow \; Ng' \subseteq Ng$$

Similarly

$$Ng \subseteq Ng'$$

Thus $Ng = \; Ng'$. So φ is one-one.

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

Hence φ is bijective.

Consequently the sets Ω 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 $\varphi: H \longrightarrow K$ is given by $\varphi(h) = ghg^{-1} \in K$. Then

φ is obviously well-defined.

i. φ is one-one.

Let

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

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

$$\Rightarrow \quad h_1 = h_2$$

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

So φ is bijective. Now we will show that φ is homomorphism.

Let $h_1, h_2 \in H$, then

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

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

$$\Rightarrow \varphi(h_1h_2) = \varphi(h_1) \,.\, \varphi(h_2).$$

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 Ω 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 Ω be the collection of all double cosets aK, $a \in G$.

We have to show that Ω 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

$$a = eae \in HaK$$

$$\Rightarrow a \in HaK$$

$$\Rightarrow a \in \bigcup_{a \in G} HaK$$

$$\Rightarrow G \subseteq \bigcup_{a \in G} HaK \qquad \textit{(i)}$$

But

$$\bigcup_{a \in G} HaK \subseteq G \qquad \textit{(ii)}$$

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 $x \in HaK \cap HbK \neq \emptyset$.

$$\Rightarrow \quad x \in HaK \quad , \quad x \in HbK$$

$$\Rightarrow x = h_1ak_1 \quad , \quad x = h_2bk_2$$

Where $h_1, h_2 \in H$, $k_1, k_2 \in K$ *and* $a, b \in G$.

$$\Rightarrow h_1 a k_1 = h_2 b k_2$$

$$\Rightarrow \quad a = {h_1}^{-1} h_2 b k_2 {k_1}^{-1} \qquad (iii)$$

Now, let $y \in HaK$.

$$\Rightarrow \quad y = h_3 a k_3 \quad , h_3 \in H \ , k_3 \in K$$

From equ. *(iii),* we have

$$y = h_3 {h_1}^{-1} h_2 b k_2 {k_1}^{-1} k_3$$

$$\Rightarrow \quad y = h_4 b k_4$$

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

$$\Rightarrow \quad y \in HbK$$

$$\Rightarrow \quad HaK \subseteq HbK \qquad (A)$$

Similarly

$$HbK \subseteq HaK \qquad (B)$$

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 $Qb_i \neq Q$. Also

$$AB = A\bigcup_{i=1}^{r} Qb_i$$

$$= \cup_{i=1}^{r} AQb_i \qquad \textit{(A)}$$

Since Q is the subgroup of A. Therefore

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

So equ. *(A)* becomes

$$AB = \cup_{i=1}^{r} Ab_i$$

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

$$\Rightarrow |AB| = \sum_{i=1}^{r} |Ab_i|$$

$$= |Ab_1| + |Ab_2| + \cdots + |Ab_r|$$

$$= r|A|$$

$$= \frac{n}{q}m$$

$$\Rightarrow |AB| = \frac{mn}{q}.$$

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

Normal Subgroups And Factor Groups

3.1 Normal Subgroups

A subgroup H of a group G is said to be normal if it coincides with all its conjugate subgroups in G. Thus H is normal in G if and only if

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

It is denoted by $H \trianglerighteq G$.

Every group G has at least two normal subgroups namely the identity $\{e\}$ and the group G itself. The normal subgroups which are different from these two subgroups are called proper normal subgroups. All the subgroups of an abelian group are normal. The non-abelian groups all of whose subgroups are normal are called **Hamiltonian Groups.**

3.1.1 Examples

a) The group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ of quaternions is such that it is non-abelian but every subgroup of Q is normal.

b) The centre of any group is normal. Since $\zeta(G) = \{a \in G : ag = ga, \forall\ g \in G\}$, therefore

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

➢ Historical Note

Normal subgroups were introduced by Evarsite Galois in 1831 as a tool for deciding whether a given polynomial equation was solvable by radicals. Galois noted that a subgroup H of a group G of permutations induced two decompositions of G into what we call left cosets and right cosets. If the two decompositions coincide, that is, if left cosets are the same as the right cosets, Galois called the decomposition proper. Thus a subgroup giving a proper decomposition is what we call normal subgroup. Galois stated that if the group of permutations of the roots of an equation has a proper decomposition, then one can solve the given equation if one can first solve an equation corresponding to the subgroup H and then an equation corresponding to the cosets.

One of the main and fundamental properties of normal subgroups is that the give rise to quotient groups. Groups which have no proper normal subgroups are known as simple groups. Finite simple groups have now been all classified. All the finite simple groups are now known their determination was completed in $1980'$s. This classification is one of the greatest achievements in mathematics.

The classification of finite simple groups ahs two aspects. One is the listing of all such groups and the other is the verification that every finite simple group is included in the list.

3.1.2 Theorem

If H is the subgroup of a group G, then the following statements are equivalent;

a) H is a normal subgroup of G.

b) The normalizer of H in G is the whole G. That is, $N_G(H) = G$.
c) $gH = Hg$, $\forall\, g \in G$.
d) $ghg^{-1} \in H$, $h \in H$, $g \in G$.

Proof (a) implies (b).

Assume that H is normal subgroup of G. Then

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

$$\Rightarrow \qquad gH = Hg \ , \forall\, g \in G$$

$$\Rightarrow \qquad g \in N_G(H)$$

$$\Rightarrow \qquad G \subseteq N_G(H) \qquad \textit{(i)}$$

But $$N_G(H) \subseteq G \qquad \textit{(ii)}$$

From *(i)* and *(ii)*, we have

$$N_G(H) = G.$$

(b) implies (c).

Suppose that $N_G(H) = G$. Then

$$N_G(H) = \{gH = Hg : g \in G\}$$

$$\Rightarrow \qquad gH = Hg \ , \forall\, g \in G.$$

(c) implies (d).

Suppose that $gH = Hg$, $\forall\, g \in G$. Then, for given any $h \in H$ there exists $h' \in H$ such that

$$gh = h'g \ , \forall\, g \in G$$

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

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

(d) implies (a).

Suppose that $ghg^{-1} \in H$, $h \in H, g \in G$. Then

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

Hence $gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H$ for all $g \in G$. Also for any $h \in H$

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

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

$$= gh^{'}g^{-1} \in gHg^{-1} \qquad \because g^{-1}hg = h^{'} \in H$$

$$H \subseteq gHg^{-1}$$

Therefore $gHg^{-1} = H$. Hence H is normal subgroup.

3.1.3 Theorem let a be an element of order 2 in a group G. Then

$$H =< a : a^2 = 1 >$$

is normal in G if and only if $a \in \zeta(G)$.

Proof As we know that H is normal if and only if for any $g \in G$,

$$gH = Hg$$

$$\Rightarrow g\{e,a\} = \{e,a\}g$$

$$\Rightarrow \{g,ga\} = \{g,ag\}$$

$$\Rightarrow \quad ga = ag \ ,\forall\, g \in G$$

So $a \in \zeta(G)$.

3.1.4 Theorem Let G and H are two groups and $\varphi: G \longrightarrow H$ is a homomorphism. Then $ker\varphi$ is a normal subgroup.

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

$$\varphi(a) = I_H \quad , \quad \varphi(b) = I_H$$

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

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

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

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

$$= I_H$$

$\Rightarrow ab^{-1} \in ker\varphi$. So $ker\varphi$ is a subgroup.

Now we have to show that $ker\varphi$ is a normal subgroup. Let $k \in ker\varphi$. To prove $g^{-1}kg \in ker\varphi$, $g \in G$

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

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

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

$$= \varphi(gg^{-1}) \qquad \because \varphi \text{ is homomorphism}$$

$$= \varphi(e)$$

$$= I_H$$

Hence $g^{-1}kg \in ker\varphi$, $g \in G$. Thus $ker\varphi$ is a normal subgroup.

3.1.5 Theorem If H, K are normal subgroups of a group G with $H \cap K = \{e\}$. Show that every element of H commute with every element of K. *i.e,* $hk = kh$, $h \in H$, $k \in K$.

Proof For each $h \in H$, $k \in K$ we have to show that $hk = kh$.

For this consider an element $hkh^{-1}k^{-1}$. Since H is a normal subgroup of G. Therefore

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

$$\Rightarrow \; h(kh^{-1}k^{-1}) \in H \,, \; h, h^{-1} \in H \qquad \because H \text{ is a subgroup.}$$

$$\Rightarrow \; hkh^{-1}k^{-1} \in H. \qquad (i)$$

Also K is a normal subgroup of G. Therefore

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

$$\Rightarrow (hkh^{-1})k^{-1} \in K \,, k, k^{-1} \in K \qquad \because K \text{ is a subgroup}$$

$$\Rightarrow \; hkh^{-1}k^{-1} \in K. \qquad (ii)$$

From *(i)* and *(ii)*, we have

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

But since $H \cap K = \{e\}$.

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

$$\Rightarrow \qquad hk = kh.$$

Hence every element of H commute with every element of K.

3.1.5 Theorem Let G be an abelian group. Then each subgroup of G is normal in G.

Proof Let H be a subgroup of G. We have to show that H is normal in G.

Since G is abelian. So $ab = ba$, $\forall\, a, b \in G$.

$$\Rightarrow \quad ah = ha \ , \forall\, h \in H \, , g \in G$$

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

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

Hence H is a normal subgroup of G.

3.1.6 Theorem

Every subgroup of index 2 in a group G is a normal subgroup.

OR

Let G be a group and H be a subgroup of index 2. Then H is a normal subgroup of G.

Proof Let H be a subgroup of index 2. Then H has two distinct left and right cosets in G.

One of the left coset is $H = eH$, $e \in G$ and the other left coset is aH , $a \in G$. Similarly one of the right coset is $H = He$ and the other right coset is Ha , $a \in G$.

By Lagrange's theorem (all the left and right cosets defines a partition).

$$G = eH \cup aH = He \cup Ha$$

And
$$eH \cap aH = He \cap Ha = \emptyset$$

$$\Rightarrow \quad aH = Ha$$

$$\Rightarrow \quad ah = h'a \ , h, h' \in H$$

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

Hence $a^{-1}h'a \in H$, $h' \in H$, $a \in G$. Thus H is normal in G.

Corollary: If H, K are normal subgroups of G. Then HK is a normal subgroup of G.

3.2 Factor Group OR Quotient Group

Let H be a normal subgroup of a group G and consider the collection Q of all left cosets of aH of H, $a \in G$.

$$\text{i.e } Q = \frac{G}{H} = \{aH : \ a \in G\}.$$

is called a factor group of G by H. Define a multiplication in Q by

$$aH.bH = abH, \text{ For } aH, bH \in Q$$

3.2.1 Theorem Prove that a factor group $Q = \frac{G}{H} = \{aH : a \in G\}$ form a group.

Proof Since the factor group is $Q = \frac{G}{H} = \{aH : a \in G\}$. We define a multiplication in Q by

$$aH.bH = abH\,, aH, bH \in Q \text{ and } a, b \in G.$$

First we check the multiplication is well-defined. For $ah_1 \in aH\,, bh_2 \in bH$, we have

$$\begin{aligned} ah_1\, bh_2 &= a(h_1\, b)\, h_2 \\ &= a(bh_3)h_2 \qquad \because H \text{ is normal} \quad \therefore aH = Ha\ \ , h_3 \in H \\ &= abh_3h_2 \\ &= abh_4 \in abH \quad , \quad \text{where } h_4 = h_3h_2 \in H \end{aligned}$$

$\Rightarrow aH.bH = abH$. Hence multiplication is well-defined.

Now we have to show that Q forms a group.

a) Q is closed because $aH.bH = abH \in Q$.

b) Q is associative because

$$\begin{aligned} (aH.bH).cH &= abH.cH \\ &= abcH \\ &= aH.bcH \\ &= aH.(bH.cH). \end{aligned}$$

c) H is the identity of Q because

$$aH.H = aH.eH = aeH = aH$$

And $$H.aH = eH.aH = eaH = aH.$$

d) Since G is group, therefore for each $a \in G$ there exists $a^{-1} \in G$ such that

$$aH.a^{-1}H = aa^{-1}H = eH = H$$

And $$a^{-1}H.aH = aa^{-1}H = eH = H.$$

So Q contains inverse of each left coset. Hence $Q = \frac{G}{H} = \{aH : a \in G\}$ form a group.

3.2.2 Theorem Let H be a normal subgroup of a group G and $\varphi: G \longrightarrow \frac{G}{H}$ is a mapping given by $\varphi(a) = aH\,, \forall\, a \in G$. Then φ is epimorphism and $ker\varphi = H$.

Proof The mapping $\varphi: G \longrightarrow \frac{G}{H}$ is defined by

$$\varphi(a) = aH \text{ , } \forall\, a \in G$$

First we will show that φ is well-defined. Let

$$a = b$$

$$\Rightarrow \quad aH = bH$$

$$\Rightarrow \quad \varphi(a) = \varphi(b)$$

Implies that φ is well-defined.

Now we have to show that φ is epimorphism. For this we have to show that φ is homomorphism and surjective.

φ is surjective because for each $H \in \frac{G}{H}$ is the image of $a \in G$. Also for $a, b \in G$

$$\begin{aligned} \varphi(a).\varphi(b) &= aH.bH \\ &= abH \\ &= \varphi(ab) \end{aligned}$$

Implies that φ is homomorphism. Hence φ is epimorphism.

To prove $ker\varphi = H$, let $a \in H \subseteq G$. Then

$$\begin{aligned} \varphi(a) &= aH \\ &= H \qquad \because H \text{ is a subgroup and } a \in H, aH = H \end{aligned}$$

Since H is the identity of quotient group $\frac{G}{H}$. Therefore $a \in ker\varphi$.

$$\Rightarrow \qquad H \subseteq ker\varphi \qquad\qquad \textit{(i)}$$

Let $a \in ker\varphi$, then

$$\varphi(a) = H$$

$$\Rightarrow \quad aH = H$$

$$\Rightarrow \quad a \in H \qquad (H \text{ is a subgroup})$$

$$\Rightarrow \quad ker\varphi \subseteq H \qquad\qquad \textit{(ii)}$$

From *(i)* and *(ii),* we have

$$ker\varphi = H.$$

Quaternion Group: The quaternion group Q_8 is a non-abelian group of order 8, isomorphic to the certain eight elements subset of the quaternions under multiplication. It is given by

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Where $i^2 = j^2 = k^2 = -1$, and

$$i.j = k = -j.i$$

$$j.k = i = -k.j$$

$$k.i = j = -i.k.$$

Since $i.j \neq j.i$, therefore it is non-abelian. There are 6 subgroups of Q_8 of order 1,2,4 and 8. These are

$$H_1 = \{1\} \quad , \quad H_4 = \{\pm 1, \pm j\}$$

$$H_2 = \{1, -1\} \quad , \quad H_5 = \{\pm 1, \pm k\}$$

$$H_3 = \{\pm 1, \pm i\} \quad , \quad H_6 = \{\pm 1, \pm i, \pm j, \pm k\} = Q_8$$

All these subgroups are cyclic and abelian. The Cayley's table for Q_8 is given by

$\times$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Properties

a) The quaternion group Q_8 has the same order as the dihedral group
$$D_4 = < a, b : a^4 = b^2 = (ab)^2 = 1 >.$$
b) Every subgroup of Q_8 is a normal subgroup.
c) The center and the commutator subgroup of Q_8 is the subgroup $\{1, -1\}$.
d) The factor group $\frac{Q_8}{\{1,-1\}}$ is isomorphic to the Klien four group K_4.

3.3 The Isomorphism Theorems

Although it is not evident at first, factor groups correspond exactly to homomorphic images, and we can use factor group to study homomorphism. We already know that every group homomorphism $\varphi: G \longrightarrow H$ we can associate a normal subgroup of G, $ker\varphi$. The converse is also true; that is, every normal subgroup of a group G gives rise to homomorphism of groups.

The following theorems describe the relationship between homomorphisms, normal subgroups and the factor groups.

3.3.1 First Isomorphism Theorem

Let $\varphi: G \longrightarrow G'$ be an epimorphism from G to G'. Then:

a) The $K = ker\varphi$ is a normal subgroup of G.
b) The factor group $\frac{G}{K}$ is isomorphic to G'.
c) A subgroup H' of G' is normal in G' if and only if its inverse image $H = \varphi^{-1}(H')$ is normal in G.
d) There is one-one correspondence between the subgroups of G' and those subgroups of G which contain $ker\varphi$.

Proof The mapping $\varphi: G \longrightarrow G'$ is given by

$$\varphi(g) = g' \text{, For all} \in G \text{, } g' \in G'$$

a) If K is the kernel of φ and $k_1, k_2 \in K$ then

$$\varphi(k_1) = \varphi(k_2) = e' \text{ and } \varphi({k_2}^{-1}) = (\varphi(k_2))^{-1} = e'$$

Now

$$\begin{aligned}\varphi\left(k_1{k_2}^{-1}\right) &= \varphi(k_1).\varphi\left({k_2}^{-1}\right) \qquad \because \ \varphi \text{ is homomorphism}\\ &= \varphi(k_1).(\varphi(k_2))^{-1}\\ &= e'.e'\\ &= e'\end{aligned}$$

$\Rightarrow k_1{k_2}^{-1} \in K$. So K is a subgroup.

Now we have to show that K is a normal subgroup of G. Since for each $k \in K$ and $g \in G$ we have

$$\begin{aligned}\varphi(gkg^{-1}) &= \varphi(g)\varphi(k)\varphi(g^{-1}) \qquad \because \ \varphi \text{ is homomorphism}\\ &= \varphi(g).e'.(\varphi(g))^{-1}\end{aligned}$$

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

$$= e^{'}$$

Thus $gkg^{-1} \in K$ for each $k \in K$ and $g \in G$. Hence K is a normal subgroup of G.

b) Define a mapping $\psi : \frac{G}{K} \longrightarrow G^{'}$ by

$$\psi(gK) = g^{'} = \varphi(g) \quad , gK \in \frac{G}{K} , g^{'} \in G^{'}.$$

To prove ψ is isomorphism, first we will prove that ψ is well-defined.

For $g_1K, g_2K \in \frac{G}{K}$ and $g_1, g_2 \in G$. Let

$$g_1K = g_2K$$

$$\Rightarrow \quad K = {g_1}^{-1}g_2K$$

$$\Rightarrow \quad {g_1}^{-1}g_2 \in K$$

$$\Rightarrow \quad \varphi({g_1}^{-1}g_2) = e^{'} \qquad \because K \text{ is kernel of } \varphi$$

$$\Rightarrow \quad \varphi({g_1}^{-1}).\varphi(g_2) = e^{'} \qquad \because \varphi \text{ is homomorphism}$$

$$\Rightarrow (\varphi(g_1))^{-1}.\varphi(g_2) = e^{'}$$

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

$$\Rightarrow \quad \psi(g_1K) = \psi(g_2K).$$

Hence ψ is well-defined.

For each $g_1K, g_2K \in \frac{G}{K}$. Let

$$\psi(g_1K) = \psi(g_2K)$$

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

$$\Rightarrow (\varphi(g_1))^{-1}.\varphi(g_2) = e^{'}$$

$$\Rightarrow \quad \varphi({g_1}^{-1}).\varphi(g_2) = e^{'}$$

$$\Rightarrow \quad \varphi({g_1}^{-1}g_2) = e^{'} \qquad \because \varphi \text{ is homomorphism}$$

$$\Rightarrow \quad {g_1}^{-1}g_2 \in K \qquad \because K \text{ is kernel of } \varphi$$

$$\Rightarrow \quad K = {g_1}^{-1}g_2K$$

$$\Rightarrow \quad g_1K = g_2K.$$

Therefore ψ is one-one (injective).

Also ψ is onto (surjective) because each $g' = \varphi(g) \in G'$ is the image of $gK \in \frac{G}{K}$.

Now, to prove ψ is homomorphism, let $g_1K, g_2K \in \frac{G}{K}$. Then

$$\psi(g_1Kg_2K) = \psi(g_1g_2K)$$

$$= \varphi(g_1g_2)$$

$= \varphi(g_1).\varphi(g_2) \quad \because \varphi$ is homomorphism

$$= \psi(g_1K).\psi(g_2K)$$

$\Rightarrow \psi$ is homomorphism.

Hence ψ is an isomorphism between $\frac{G}{K}$ and G'.

c) Suppose that H' is a normal subgroup of G' and

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

To prove H is normal in G, Consider an element ghg^{-1}, for $h \in H$ and $g \in G$. Now

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

$$= \varphi(g).\varphi(h).(\varphi(g))^{-1} \in H'$$

$\Rightarrow \varphi(ghg^{-1}) \in H' \quad \because H'$ is normal subgroup

Hence $ghg^{-1} \in H$ for each $g \in G$, $h \in H$ and so H is normal subgroup of G.

Conversely, suppose that $H = \varphi^{-1}(H')$ is normal in G. To prove H' is normal in G', consider an element $g'h'g'^{-1}$, for $h' \in H'$ and $g' \in G'$.

Since $\varphi(H) = H'$, let $g \in G$, $h \in H$ are the pre-images of $h' \in H'$, $g' \in G'$. Then

$$g'h'g'^{-1} = \varphi(g).\varphi(h).(\,\varphi(g))^{-1}$$

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

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

Since H is normal in G, $ghg^{-1} \in H$. Therefore

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

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

Hence $H^{'}$ is normal in $G^{'}$.

d) Let Ω be the collection of subgroups of G containing K and ω be the collection of all subgroups of $G^{'}$.

Define a mapping $\alpha:\ \Omega \longrightarrow \omega$ by

$$\alpha(H) = H^{'} = \varphi(H)\ \text{, where } H \in \Omega \text{ and } H^{'} = \varphi(H) \in \omega.$$

Now, for $H_1, H_2 \in \Omega$, let

$$\alpha(H_1) = \alpha(H_2)$$

$$\Rightarrow\ \varphi(H_1) = \varphi(H_2).$$

Let $H_1 = \varphi^{-1}(H^{'})$, then $H_1 \subseteq H$ because $H = \varphi^{-1}(H^{'})$. Next let $h \in \mathrm{H}$, then

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

$$\Rightarrow \varphi(h) = h^{'} = \varphi(h_1) \qquad\qquad \because\ \alpha(H) = H^{'} = \varphi(H_1)$$

$$\Rightarrow \varphi(h) = \varphi(h_1)$$

$$\Rightarrow\ \varphi\left({h_1}^{-1}h\right) = e$$

$$\Rightarrow {h_1}^{-1}h \in K \subseteq H_1$$

$$\Rightarrow\quad h \in h_1K \subseteq H_1$$

$$\Rightarrow\quad H \subseteq H_1$$

$$\Rightarrow\quad H = H_1.$$

Similarly $H = H_2$. Hence α is injective.

Also α is surjective because each $H^{'} \in \omega$ is the image of $H \in \Omega$ and therefore α bijective. Hence there is a one-one correspondence between the subgroups of G containing K and the subgroups of $G^{'}$.

Define the **natural** or **canonical homomorphism** $\mu : G \longrightarrow \frac{G}{K}$ by

$$\mu(g) = gK\ \ , g \in G.$$

Then μ is an epimorphism of G to $\frac{G}{K}$. Moreover the mapping $\psi:\ \frac{G}{K} \longrightarrow G^{'}$ defined by

$$\psi(gK) = g^{'} = \varphi(g)\ \ , g^{'} \in G^{'}$$

is a homomorphism. Since the product of two homomorphisms is again a homomorphism, we have $\varphi = \psi\mu$.

Mathematician often use diagrams called **commutative diagrams** to describe such relations. The following diagram "commutes" since $\varphi = \psi\mu$

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\mu"'] & & G' \\ & \frac{G}{K} \arrow[ur, "\psi"'] & \end{tikzcd}$$

Note: There is a one-one correspondence between the normal subgroup of a group and the number of homomorphisms of that group.

Example let G be a cyclic group with generator g. Define a mapping $\varphi : \mathbb{Z} \longrightarrow G$ by

$$\varphi(n) = g^n \ , n \in \mathbb{Z} \, , g \in G.$$

Then φ is surjective and homomorphism since for $m, n \in \mathbb{Z}$

$$\varphi(m+n) = g^{m+n} = g^m . g^n = \varphi(m).\varphi(n)$$

Clearly φ is onto because each $g^n \in G$ is the image of $n \in \mathbb{Z}$. if $|g| = m$, then $g^m = e$.
Hence $ker\varphi$ =m $\mathbb{Z}$ and

$$\frac{\mathbb{Z}}{ker\varphi} = \frac{\mathbb{Z}}{m\mathbb{Z}} \cong G$$

On the other hand if the order of g is infinite, then $ker\varphi = 0$ and φ is an isomorphism of G and $\mathbb{Z}$. Hence, two cyclic groups are isomorphic exactly when they have the same order. Up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}^n$.

3.3.2 Second Isomorphism Theorem

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

a) HK is a subgroup of G,
b) $H \cap K$ is normal in H, and
c) $\frac{HK}{K} \cong \frac{H}{H \cap K}$.

Proof

a) To prove HK is a subgroup of G. Let $x_1, x_2 \in HK$, then

$$x_1 = h_1 k_1 \quad , \quad x_2 = h_2 k_2 \text{ for } h_1, h_2 \in H \text{ and } k_1, k_2 \in K.$$

Now
$$\begin{aligned} x_1 {x_2}^{-1} &= (h_1 k_1)(h_2 k_2)^{-1} \\ &= h_1 k_1 {k_2}^{-1} {h_2}^{-1} \\ &= h_1 k_3 {h_2}^{-1} \qquad \because k_1 {k_2}^{-1} = k_3 \in K \text{ is a subgroup} \\ &= h_1 ({h_2}^{-1} h_2)\, k_3 {h_2}^{-1} \\ &= \left(h_1 {h_2}^{-1}\right)(h_2\, k_3 {h_2}^{-1}) \in HK \end{aligned}$$

because $h_1 {h_2}^{-1} \in H$ and $h_2\, k_3 {h_2}^{-1} \in K$ (K is normal subgroup of G).

$$\Rightarrow x_1 {x_2}^{-1} \in HK$$

Hence HK is a subgroup of G.

b) To prove $H \cap K$ is normal in H, let $x \in H \cap K$ $i.e(x \in H, x \in K)$ and $h \in H$. Then

$$\Rightarrow hxh^{-1} \in K \qquad \because K \text{ is a normal subgroup and } h \in H \subseteq G$$

Also $$hxh^{-1} \in H \qquad \because H \text{ is a subgroup and } x, h \in H.$$

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

Hence $H \cap K$ is a normal subgroup of H.

c) To prove $\frac{HK}{K} \cong \frac{H}{H \cap K}$, define a mapping $\varphi : H \longrightarrow \frac{HK}{K}$ by

$$\varphi(h) = hkK \ , h \in H, k \in K$$

$$= hK \quad \because K \text{ is a subgroup and } kK = K, k \in K$$

Then φ is obviously well-defined. Also φ is onto because each $hK \in \frac{HK}{K}$ is the image of $h \in H$. Moreover,

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

$$= h_1 K . h_2 K$$

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

$\Rightarrow \varphi$ is homomorphism.

Hence φ is an epimorphism.

Now, by first isomorphism theorem

$$\frac{HK}{K} \cong \frac{H}{ker\varphi}$$

To prove $ker\varphi = H \cap K$, let $h \in ker\varphi$, then

$$\varphi(h) = K \ \text{, where } K \text{ is the identity of quotient group}$$

$$\Rightarrow hK = K$$

$$\Rightarrow h \in K \, , h \in H$$

$$\Rightarrow h \in H \cap K \ , \Rightarrow ker\varphi \subseteq H \cap K$$

Conversely, let $x \in H \cap K$

$$\Rightarrow x \in H, x \in K$$

Since $$\varphi(x) = xK$$

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

$$\Rightarrow x \in ker\varphi \qquad \because K \text{ is the identity of quotient group.}$$

$$\Rightarrow H \cap K \subseteq ker\varphi$$

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

Hence $\frac{HK}{K} \cong \frac{H}{H \cap K}$.

3.3.3 Third Isomorphism Theorem

Let H,K be normal subgroups of a group G and $H \subseteq K$. Then

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

Proof Since H, K are normal subgroups of G and $H \subseteq K$. Therefore H is normal in K.

To prove $\frac{K}{H}$ is normal in $\frac{G}{H}$, consider the element $(gH)kH(gH)^{-1}$, for $gH \in \frac{G}{H}$ and $kH \in \frac{K}{H}$.

Now $$(gH)kH(gH)^{-1} = gHkH(g^{-1}H)$$

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

$$= gkg^{-1}H \quad \text{(by multiplication of quotient group)}$$

$$\Rightarrow \qquad gkg^{-1}H \in \frac{K}{H} \qquad \because K \text{ is normal in } G$$

$\Rightarrow \frac{K}{H} \trianglelefteq \frac{G}{H}$. That is, $\frac{K}{H}$ is normal in $\frac{G}{H}$.

To prove $(G/H)/(K/H) \cong G/K$. Define a mapping $\varphi : \frac{G}{H} \longrightarrow \frac{G}{K}$ by

$$\varphi(gH) = gK, g \in G.$$

Then φ is obviously well-defined. Also φ is surjective because each $gK \in \frac{G}{K}$ is the image of $gH \in \frac{G}{H}$. Moreover, for $g_1H, g_2H \in \frac{G}{H}$

$$\varphi(g_1Hg_2H) = \varphi(g_1g_2H)$$

$$= g_1g_2K$$

$$= g_1K.g_2K$$

$$= \varphi(g_1H).\varphi(g_2H)$$

$\Rightarrow \varphi$ is homomorphism. Hence φ is an epimorphism.

Now, by first isomorphism theorem

$$(G/H)/ker\varphi \cong G/K.$$

To prove $ker\varphi = \frac{K}{H}$, let $gH \in ker\varphi$ then

$\varphi(gH) = K$, where K is the identity of quotient group.

$\Rightarrow \quad gK = K$

$\Rightarrow \quad g \in K$

$\Rightarrow \; gH \in \frac{K}{H}$

$\Rightarrow ker\varphi \subseteq \frac{K}{H}$ *(i)*

Conversely, let $kH \in \frac{K}{H}$ then

$\varphi(kH) = kK$

$= K$ $\because k \in K$ is a subgroup

$\Rightarrow \quad kH \in ker\varphi$ $\because K$ is the identity of quotient group.

$\Rightarrow \quad \frac{K}{H} \subseteq ker\varphi$ *(ii)*

From *(i)* and *(ii)*, we have

$$\frac{K}{H} = ker\varphi.$$

Hence

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

3.4 Automorphism

Let G be a group. Then a mapping $\alpha : G \longrightarrow G$ is called an automorphism if and only if

a) α is bijective,
b) $\alpha(g_1g_2) = \alpha(g_1).\alpha(g_2)$, $\forall \; g_1, g_2 \in G$.

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

3.4.1 Theorem The set $A(G)$ of all automorphism of G form a group.

Proof Let G be group and $A(G)$ be the set of all automorphism of G. We have to show that $A(G)$ forms a group.

i. Let $\alpha, \beta \in A(G)$. Then the product $\beta\alpha$ of bijective mapping α and β is also bijective. Moreover, for $g_1, g_2 \in G$

$$\beta\alpha(g_1g_2) = \beta(\alpha(g_1g_2))$$
$$= \beta(\alpha(g_1).\alpha(g_2)) \quad \because \alpha \text{ is an automorphism}$$
$$= \beta(\alpha(g_1).\beta(\alpha(g_2) \quad \because \beta \text{ is an automorphism}$$
$$= (\beta\alpha)(g_1).(\beta\alpha)(g_2)\text{ , } \forall\, g_1, g_2 \in G$$

$\Rightarrow \beta\alpha \in A(G)$.

Thus $A(G)$ is closed under the usual multiplication of mappings.

ii. Also the associative law holds in $A(G)$. It follows from the associativity of mappings of a set.

iii. The identity mapping $I: G \longrightarrow G$ is defined by

$$I(g) = g \ \ , g \in G$$

is bijective. Moreover, for $g_1, g_2 \in G$

$$I(g_1g_2) = g_1g_2$$
$$= I(g_1).I(g_2).$$

$\Rightarrow I$ is homomorphism.

Also $$\alpha I(g) = \alpha o I(g) = \alpha\big(I(g)\big) = \alpha(g)$$

and $$I\alpha(g) = I o \alpha(g) = I\big(\alpha(g)\big) = \alpha(g)$$

Hence I is the identity in $A(G)$.

iv. Now we have to show that for each $\alpha \in A(G)$ there exist $\alpha^{-1} \in A(G)$. Since α bijective, so α^{-1} is also bijective (inverse of bijective mappings is also bijective). Also for all $g_1, g_2 \in G$

$$\alpha^{-1}(g_1g_2) = \alpha^{-1}(I(g_1g_2))$$
$$= \alpha^{-1}\big(I(g_1).I(g_2)\big)$$
$$= \alpha^{-1}(\alpha\alpha^{-1}(g_1).\alpha\alpha^{-1}(g_2))$$
$$= \alpha^{-1}(\alpha\big(\alpha^{-1}(g_1).\alpha^{-1}(g_2)\big)) \quad \because \alpha \text{ is an homomorphism}$$

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

Hence α^{-1} is homomorphism. Thus $\alpha^{-1} \in A(G)$.
Therefore $A(G)$ forms a group.

3.4.2 Inner And Outer Automorphism

Let a be a fixed element of G then the mapping $I_a: G \longrightarrow G$ given by

$$I_a(g) = aga^{-1} \quad , g \in G$$

is called an inner automorphism of G. The set of all inner automorphism of G is denoted by $I(G)$. For $a, b \in G$

$$I_a.I_b = I_a[(bgb^{-1})]$$
$$= a(bgb^{-1})a^{-1}$$
$$= (ab)g(ab)^{-1}$$
$$I_a.I_b = I_{ab}.$$

An automorphism of G which is not an inner automorphism is called an oiter automorphism of G. Every automorphism of an abelian group except the identity automorphism is an outer automorphism.

3.4.3 Theorem Let G be a group. The mapping $\varphi : G \longrightarrow G$ defined by

$$\varphi(g) = g^{-1} \quad , g \in G$$

is an automorphism if and only if G is abelian.

Proof Suppose that G is abelian. Then, for $g_1, g_2 \in G$

$$g_1g_2 = g_2g_1.$$

Define a mapping $\varphi : G \longrightarrow G$ by

$$\varphi(g) = g^{-1} \quad , g \in G.$$

Then $\qquad \varphi(g_1) = g_1{}^{-1} \;,\; \varphi(g_2) = g_2{}^{-1}$

Now $\qquad \varphi(g_1g_2) = (g_1g_2)^{-1}$

$$= g_2{}^{-1}g_1{}^{-1}$$
$$= g_1{}^{-1}g_2{}^{-1} \qquad \because G \text{ is abelian}$$
$$= \varphi(g_1).\varphi(g_2)$$

$\Rightarrow \varphi$ is homomorphism. Also φ is bijective (Do it).

Hence φ is an automorphism.

Conversely, let $\varphi : G \longrightarrow G$ given by

$$\varphi(g) = g^{-1} \quad , g \in G$$

be an automorphism. Then, for $g_1, g_2 \in G$

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

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

Also

$$\varphi(g_1 g_2) = \varphi(g_1).\varphi(g_2) \qquad \because \varphi \text{ is homomorphism}$$

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

From *(i) and (ii), we have*

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

$$\Rightarrow (g_1 g_2)^{-1} = (g_2 g_1)^{-1} \text{ or } g_1 g_2 = g_2 g_1 \quad , g_1, g_2 \in G$$

Hence G is abelian.

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

Proof First we will show that $I(G)$ is a subgroup of $A(G)$. Let $I_a, I_b \in I(G)$, then

$$I_a(g) = aga^{-1} \quad , I_b(g) = bgb^{-1} \text{ for all } g \in G$$

And

$$I_{b^{-1}}(g) = b^{-1}gb$$

Also

$$I_b.I_{b^{-1}}(g) = I_b(b^{-1}gb)$$

$$= bb^{-1}gbb^{-1} = g$$

$$= I_e(g)$$

$$\Rightarrow I_{b^{-1}} = (I_b)^{-1}$$

Now

$$I_a.I_{b^{-1}}(g) = I_a(b^{-1}gb)$$

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

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

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

$$= I_{ab^{-1}}(g) \in I(G) \text{ , for all } g \in G.$$

Hence $I(G)$ is a subgroup of $A(G)$.

To prove $I(G)$ is a normal subgroup of $A(G)$. Let $I_a \in I(G)$ and $\alpha \in A(G)$, then

$$(\alpha I_a \alpha^{-1})(g) = \alpha I_a(\alpha^{-1}(g))$$

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

$$= \alpha(a).\alpha\big(\alpha^{-1}(g)\big).\alpha(a^{-1}) \qquad \because \alpha \text{ is homomorphism}$$

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

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

$$= I_{\alpha(a)}(g) \in I(G) \text{ , } \forall\, g \in G$$

Therefore $I(G)$ is a normal subgroup of $A(G)$.

3.4.5 Theorem Let $\zeta(G)$ be the centre and $I(G)$ be the inner automorphism of a group G. Then $\frac{G}{\zeta(G)} \cong I(G)$.

Proof Define a mapping $\varphi : G \longrightarrow I(G)$ by

$$\varphi(a) = I_a \text{ , } a \in G.$$

First we will show that φ is well-defined. For $a, b \in G$, let

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

$$\Rightarrow \quad ag = bg$$

$$\Rightarrow aga^{-1} = bga^{-1}$$

$$\Rightarrow aga^{-1} = bgb^{-1}$$

$$\Rightarrow \quad I_a = I_b$$

Then φ is surjective because each $I_a \in I(G)$ is the image of $a \in G$. Moreover, for $a, b \in G$

$$\varphi(ab) = I_{ab}$$

$$= I_a.I_b$$

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

Hence φ is homomorphism. Thus φ is epimorphism.

By First Isomorphism Theorem

$$\frac{G}{ker\varphi} \cong I(G)$$

Now we have to show that

$$\zeta(G) = ker\varphi$$

Let $z \in ker\varphi$, then

$$\varphi(z) = I_z \quad , \text{ by definition of } \varphi$$

$$= I_e \quad , \text{by assumption that } z \in ker\varphi$$

$$\Rightarrow I_z(g) = I_e(g)$$

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

$$\Rightarrow zg = gz$$

$$\Rightarrow z \in \zeta(G)$$

$$\Rightarrow ker\varphi \subseteq \zeta(G) \qquad (i)$$

Conversely, let $z \in \zeta(G)$. Then

$$\varphi(z) = I_z \quad , \text{ by definition of } \varphi$$

$$= zgz^{-1} = gzz^{-1} = g = I_e(g)$$

$$\Rightarrow I_z(g) = I_e(g) \qquad \because z \in \zeta(G) \therefore zg = gz$$

$$\Rightarrow z \in ker\varphi$$

$$\Rightarrow \zeta(G) \subseteq ker\varphi \qquad (ii)$$

From *(i) and (ii),* we have $\zeta(G) = ker\varphi$.

Hence $\frac{G}{\zeta(G)} \cong I(G)$.

Complete Group: if the centre $\zeta(G)$ of a group G is trevial and very automorphism of G is an inner automorphism, G is called a complete group.

3.4.6 Conjugation as an Automorphism

Let G be a group, $a \in G$. Define a mapping $I_a : G \longrightarrow G$ by

$$I_a(g) = aga^{-1} \text{ , for all } g \in G.$$

Then I_a is an automorphism.

Proof First we will show that I_a is bijective. For $g_1, g_2 \in G$, let

$$\begin{aligned} & I_a(g_1) = I_a(g_2) \\ \Rightarrow\ & ag_1a^{-1} = ag_2a^{-1} \\ \Rightarrow\ & g_1 = a^{-1}ag_2a^{-1}a \\ \Rightarrow\ & g_1 = g_2 \end{aligned}$$

$\Rightarrow I_a$ is one-one.

Also I_a is onto because each $a^{-1}ga \in G$ is the image of $g \in G$ under I_a.

$$i.e,\ I_a(a^{-1}ga) = a(a^{-1}ga)a = (aa^{-1})g(aa^{-1}) = g.$$

Hence I_a is bijective.

Now we have to show that I_a is homomorphism. For $g_1, g_2 \in G$, let

$$\begin{aligned} I_a(g_1g_2) &= ag_1g_2a^{-1} \\ &= ag_1a^{-1}ag_2a^{-1} \\ &= (ag_1a^{-1})(ag_2a^{-1}) \\ &= I_a(g_1).I_a(g_2) \end{aligned}$$

$\Rightarrow I_a$ is an homomorphism.

Thus $I_a \in A(G)$. That is, I_a is an automorphism.

3.5 Commutator

Let G be a group and $a, b \in G$. Then the element

$$x = aba^{-1}b^{-1}$$

Is called the commutator of a, b and it is denoted by $[a, b]$.

3.5.1 Theorem Let G be a group. Then for $a, b, c \in G$, the following commutator identities hold in G;

a) $[b, a] = [a, b]^{-1}$
b) $[ab, c] = [b, c]^a [a, c]$
c) $[a, bc] = [a, b][a, c]^b$
d) $[a, b^{-1}] = [b, a]^{b^{-1}}$ *and* $[a^{-1}, b] = [b, a]^{a^{-1}}$.

Proof

a) Since $[b, a] = bab^{-1}a^{-1}$. Now

$$\begin{aligned}[a, b][b, a] &= (aba^{-1}b^{-1})(bab^{-1}a^{-1}) \\ &= (aba^{-1})(b^{-1}b)(ab^{-1}a^{-1}) \\ &= (ab)(a^{-1}a)(b^{-1}a^{-1}) \\ &= (ab)(ab)^{-1} \\ &= e\end{aligned}$$

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

b) For $a, b, c \in G$,

$$\begin{aligned}[ab, c] &= abc(ab)^{-1}c^{-1} \\ &= abcb^{-1}a^{-1}c^{-1} \\ &= abcb^{-1}(c^{-1}c)a^{-1}c^{-1} \\ &= a(bcb^{-1}c^{-1})a^{-1}(aca^{-1}c^{-1}) \\ &= a[b, c]a^{-1}[a, c]\end{aligned}$$

$$\Rightarrow [ab, c] = [b, c]^a [a, c].$$

c)

$$\begin{aligned}[a, bc] &= abca^{-1}(bc)^{-1} \\ &= abca^{-1}c^{-1}b^{-1} \\ &= aba^{-1}aca^{-1}c^{-1}b^{-1} \\ &= (aba^{-1}b^{-1})b(aca^{-1}c^{-1})b^{-1}\end{aligned}$$

$$\Rightarrow [a, bc] = [a, b][a, c]^b.$$

d)

$$\begin{aligned}[a, b^{-1}] &= ab^{-1}a^{-1}(b^{-1})^{-1} \\ &= ab^{-1}a^{-1}b \\ &= b^{-1}(bab^{-1}a^{-1})b \\ &= b^{-1}[b, a](b^{-1})^{-1}\end{aligned}$$

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

and $[a^{-1}, b] = [b, a]^{a^{-1}}$. (do it yourself).

Note:

a. A group G abelian if and only if for any two elements $a, b \in G$, $[a,b] = e$.
b. The product of two commutators may not b a commutator.

Derived Group OR Commutator Subgroup: Let G be a group and G' be a subgroup of G. Then G' is said to be a commutator subgroup, if it is generated by a set of commutators of G.

3.5.2 Theorem let G be a group. Then

a) the derived group G' is normal subgroup of G,
b) the factor group $\frac{G}{G'}$ is abelian,
c) if K is a normal subgroup of G such that $\frac{G}{K}$ is abelian then $G' \subseteq K$.

Proof

a) Since G' is generated by the commutators $[a,b], a, b \in G$. To prove G' is normal in G, consider

$$\begin{aligned} g[a,b]g^{-1} &= g(aba^{-1}b^{-1})g^{-1} \quad , \quad \text{for } [a,b] \in G' \text{ and } g \in G \\ &= gag^{-1}.gbg^{-1}.ga^{-1}g^{-1}.gb^{-1}g^{-1} \\ &= gag^{-1}.gbg^{-1}.(gag)^{-1}.(gbg)^{-1} \\ &= a^g b^g (a^g)^{-1}(b^g)^{-1} \qquad \because a^g = gag^{-1} \text{ is the conjugate of } a \\ &= [a^g, b^g] \in G' \quad , \text{for all } g \in G \end{aligned}$$

$$\Rightarrow g[a,b]g^{-1} \in G'$$

Hence G' is a normal subgroup of G.

b) Let $aG', bG' \in \frac{G}{G'}$, $a, b \in G$, then

$$\begin{aligned} [aG', bG'] &= aG'bG'(aG')^{-1}(bG')^{-1} \\ &= aG'bG'a^{-1}G'b^{-1}G' \\ &= (aba^{-1}b^{-1})G' \qquad \text{(by quotient multiplication)} \\ &= G' \qquad \because [a,b] \in G' \\ &= \text{identity of factor group.} \end{aligned}$$

Hence the factor group $\frac{G}{G'}$ is abelian.

c) Let K be a normal subgroup of G such that $\frac{G}{K}$ is abelian and $K, bK \in \frac{G}{K}$. Then

$$\begin{aligned} [ak, bK] &= aKbK(aK)^{-1}(bK)^{-1} \\ &= aKbKa^{-1}Kb^{-1}K \\ &= (aba^{-1}b^{-1})K \\ &= [a,b]K = K \qquad \because \frac{G}{K} \text{ is abelian} \end{aligned}$$

Hence $[a,b] \in K$. But since $[a,b] \in G'$. Therefore $G' \subseteq K$.

Product Of Groups

4.1 Direct Product

If G and H are two groups (finite or infinite). Then the direct product of G and H is a new group, denoted by $G \times H$ and is defined by

$$G \times H = \{(x, y) | x \in G, y \in H\}.$$

The group operation defined is multiplication. Let $a, b \in G$ and $x, y \in H$, then

$$(a, b).(x, y) = (a.x, b.y).$$

It is also called the external direct product.

Properties

a) **Identity:** The direct product $G \times H$ has an identity element, namely $\{e_1, e_2\}$, where $e_1 \in G$ and $e_2 \in H$.

b) **Inverse:** The inverse of each element $(x, y) \in G \times H$ is (x^{-1}, y^{-1}), where $x^{-1} \in G$ and $y^{-1} \in H$.

c) **Associativity:** The associative law holds in $G \times H$. That is, for $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in G \times H$
$$((x_1, y_1).(x_2, y_2)).(x_3, y_3) = (x_1, y_1).((x_2, y_2).(x_3, y_3)).$$

4.1.1 Example

Let $G = \mathbb{Z}$ under addition, $H = \{\pm 1, \pm i\}$ under multiplication be two groups. Then the direct product of G and H is

$$G \times H = \{(x, y) | x \in \mathbb{Z}, y = \pm 1 \text{ } or \pm i\}.$$

Now to identify the group operation, let $(6, -1), (-3, i) \in G \times H$. Then

$$(6, -1).(-3, i) = (6 - 3, -1.i)$$

(because $\mathbb{Z}$ under addition is a group and $\{\pm 1, \pm i\}$ under multiplication is a group)

$$= (3, -i).$$

The identity element is $(0,1)$, because

$$(7, -i).(0,1) = (7 + 0, -i.1) \quad , (7, -i) \in G \times H$$

$$= (7, -i) = (0,1).(7, -i)$$

Let $(13, -i) \in G \times H$, then

$$(13, -i).(-13, i) = (13 - 13, -i.i)$$
$$= (0,1) = (-13, i).(13, -i)$$

$\Rightarrow (-13, i) \in G \times H$ is an inverse. Hence inverse of each element of $G \times H$ exists.

Also, for $(6, -1), (-3, i), (12,1) \in G \times H$

$$(6, -1).\big((-3, i).(12,1)\big) = (6, -1).(-3 + 12, i.1)$$
$$= (6, -1).(9, i)$$
$$= (6 + 9, -1.i)$$
$$= (15, -i)$$

and $$\big((6, -1).(-3, i)\big).(12,1) = (6 - 3, -1.i).(12,1)$$
$$= (3, -i).(12,1)$$
$$= (3 + 12, -i.1)$$
$$= (15, -i)$$

$$\Rightarrow (6, -1).\big((-3, i).(12,1)\big) = \big((6, -1).(-3, i)\big).(12,1)$$

Hence the associative law holds in $G \times H$.

Internal Direct Product: let G be group and H, K be two subgroups of G. Then G is said to be internal direct product of H, K if and only if

a) G is generated by H, K,
b) H, K are normal subgroups of G,
c) $H \cap K = \{e\}$ is the identity in G.

Note: We can take the direct product of finitely or infinitely many groups. For example, if $G_1, G_2, \dots, G_n$ are n groups. Then the direct product

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \dots \times G_n$$

is finite. But if G_i for all $i = 1,2, \dots$ is infinite, then the direct product is also infinite.

4.1.2 Theorem

Let G be a direct product of its two normal subgroups H, K with $H \cap K = \{e\}$ and $G = HK$. Then

i. Each element of H is permutable with every element of K. *i.e,* $hk = kh$, for all $h \in H, k \in K$

ii. Every element of G is uniquely expressible as $g = hk$, for all $h \in H, k \in K$

iii. $G \cong H \times K$.

Proof

i. Let $h \in H, k \in K$ and consider the commutator $hkh^{-1}k^{-1}$. Then

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K \qquad (K \text{ is normal in } G)$$

$$= h(kh^{-1}k^{-1}) \in H \qquad (H \text{ is normsl in } G)$$

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

But since $H \cap K = \{e\}$.

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

$$\Rightarrow \quad hk = kh$$

Hence each element of H is permutable with every element of K.

ii. Since G is generated by its subgroups H, K. Let

$$g = h_1k_1 \ , \ g = h_2k_2 \text{ for } h_1, h_2 \in H, k_1, k_2 \in K$$

$$\Rightarrow \quad h_1k_1 = h_2k_2$$

$$\Rightarrow h_2{}^{-1}h_1 = k_2k_1{}^{-1} \in H, K$$

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

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

$$\Rightarrow \quad h_1 = h_2 = h \in H \ (say)$$

Also $\quad k_2k_1{}^{-1} \in H \cap K$

$$\Rightarrow k_2k_1{}^{-1} = e$$

$$\Rightarrow \quad k_1 = k_2 = k \in K \ (say)$$

$$\Rightarrow \quad h_1k_1 = h_2k_2 = hk$$

Hence every $g \in G$ is uniquely expressible as $g = hk$, for all $h \in H, k \in K$.

iii. To prove $G \cong H \times K$. Define a mapping $\varphi : G \longrightarrow H \times K$ by

$$\varphi(g) = (h, k) \ , g \in G \, , (h, k) \in H \times K.$$

First we will show that φ is well-defined. For $g_1, g_2 \in G$, let

$$g_1 = g_2$$

$$\Rightarrow h_1k_1 = h_2k_2 \qquad \because G = HK$$

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

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

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

$\Rightarrow \varphi$ is well-defined.

For one-one, let

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

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

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

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

$$\Rightarrow \quad g_1 = g_2 \qquad \because G = HK$$

$\Rightarrow \varphi$ is one-one.

Also φ is onto because each $(h, k) \in H \times K$ is the image of $g \in G$ under φ.

Now for $g_1, g_2 \in G$

$$\begin{aligned}
\varphi(g_1 . g_2) &= \varphi(h_1 k_1 . h_2 k_2) \\
&= \varphi(h_1 (k_1 h_2) k_2) \\
&= \varphi(h_1 h_2 . k_1 k_2) \qquad \because hk = kh \\
&= (h_1 h_2, k_1 k_2) \\
&= (h_1, k_1).(h_2, k_2) \\
&= \varphi(g_1).\varphi(g_2)
\end{aligned}$$

Hence φ is homomorphism. Thus $G \cong H \times K$.

4.1.3 Theorem

If $G = H \times K$ and $\zeta(G), \zeta(H), \zeta(K)$ are the centre of G, H and K respectively, then

$$\zeta(G) = \zeta(H) \times \zeta(K).$$

Proof To prove $\zeta(G) = \zeta(H) \times \zeta(K)$. Let $x \in \zeta(H) \times \zeta(K)$, then

$$x = z_1 z_2 \text{ , where } z_1 \in \zeta(H) \text{ and } z_2 \in \zeta(K)$$

Let $g \in G$, then $g = hk$, for $h \in H$, $k \in K$ (by theorem 4.1.2(ii)). Now

$$xg = z_1 z_2 hk$$

$$= z_1(z_2h)k \qquad \because hk = kh$$

$$= (z_1h)(z_2k)$$

$$= h(z_1k)z_2 = hkz_1z_2$$

$$\Rightarrow xg = gx$$

$$\Rightarrow \quad x \in \zeta(G)$$

$$\Rightarrow \ \zeta(H) \times \zeta(K) \subseteq \zeta(G) \qquad \textit{(i)}$$

Now, let $a \in \zeta(G)$, then

$$ag = ga \text{, for } g \in G$$

$$\Rightarrow ah = ha \,, h \in H \subseteq G$$

And $$ak = ka, k \in K \subseteq G$$

Let $a = h'k'$, $h' \in H, k' \in K$. Then

$$ah = h'k'h = h'(k'h) = h'hk' \qquad \because hk = kh$$

And $$ha = hh'k'$$

but since $ah = ha$

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

$$\Rightarrow \quad h'h = hh' \qquad \text{(right cancelation law)}$$

$$\Rightarrow \qquad h' \in \zeta(H).$$

Also $$ak = h'k'k$$

and $$ka = kh'k' = (kh')k' = h'kk' \qquad \because hk = kh$$

$$\Rightarrow h'k'k = h'kk' \qquad \because ak = ka$$

$$\Rightarrow \quad k'k = kk' \qquad \text{(left cancelation law)}$$

$$\Rightarrow \qquad k' \in \zeta(K)$$

$$\Rightarrow \quad h'k' \in \zeta(H) \times \zeta(K)$$

$$\Rightarrow \qquad a \in \zeta(H) \times \zeta(K)$$

$$\Rightarrow \zeta(G) \subseteq \zeta(H) \times \zeta(K) \qquad \textit{(ii)}$$

From *(i) and (ii),* we have $\zeta(G) = \zeta(H) \times \zeta(K)$.

4.1.4 Theorem Let $G = H \times K$. Then the factor group $\frac{G}{K} \cong H$.

Proof The factor group

$$\frac{G}{K} = \{gK : g \in G\}$$

$$\frac{G}{K} = \{hkK = hK, h \in H\} \qquad \because g = hk$$

To prove $\frac{G}{K} \cong H$. Define a mapping $\varphi : \frac{G}{K} \longrightarrow H$ by

$$\varphi(gK) = \varphi(hK) = h.$$

First we will show that φ is well-defined. For $g_1K, g_2K \in \frac{G}{K}$, let

$$g_1K = g_2K$$

$$\Rightarrow \quad h_1K = h_2K$$

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

$$\Rightarrow \quad h_2{}^{-1}h_1 \in K$$

But also $h_2{}^{-1}h_1 \in H$.

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

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

$$\Rightarrow \quad h_1 = h_2$$

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

$\Rightarrow \varphi$ is well-defined.

For one-one, let

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

$$\Rightarrow \quad h_1 = h_2$$

$$\Rightarrow \quad h_1K = h_2K$$

$\Rightarrow \varphi$ is one-one.

Also φ is onto because each $h \in H$ is the image of $gK \in \frac{G}{K}$. Moreover, for $g_1K, g_2K \in \frac{G}{K}$

$$\varphi(g_1Kg_2K) = \varphi(h_1Kh_2K)$$

$$= \varphi(h_1h_2K)$$

$$= h_1h_2$$

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

Hence φ is homomorphism. Thus $\frac{G}{K} \cong H$.

4.1.5 Theorem Let $G = H \times K$ and H_1 be a normal subgroup of H. Then H_1 is normal in G.

Proof Since $G = H \times K$, therefore for each $g \in G$

$$g = hk.$$

To prove H_1 is normal in G. Consider an element gh_1g^{-1}, for each $h_1 \in H_1$, $g \in G$. Then

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

$$= hkh_1k^{-1}h^{-1}$$

$$= h(kh_1)k^{-1}h^{-1} \qquad \because hk = kh$$

$$= hh_1(kk^{-1})h^{-1}$$

$$= hh_1h^{-1} \in H_1 \qquad \because H_1 \text{ is normal in } H$$

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

Hence H_1 is normal in G.

4.1.6 Theorem Let H, K be cyclic groups of order m, n respectively, where m, n are relatively prime. Then $H \times K$ is a cyclic group of order mn.

Proof Let $=< a : a^m = e >$, $K =< b : b^n = e >$. Let $G = H \times K$, then ab is an element of $H \times K$.

Also $(ab)^k = a^kb^k = e$ if and only if $m|k, n|k$. But since $(m, n) = 1$, therefore $mn|k$. Moreover

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e.e = e$$

Hence ab has order mn. As $H \times K$ has mn elements.

$$\Rightarrow G =< a, b : (ab)^{mn} = e >$$

Hence G is cyclic group of order mn.