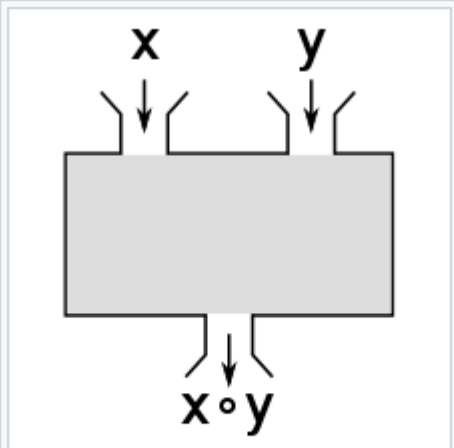
Laws of Binary Operation & Formation of Groups

Binary operations are the keystone of most algebraic structures, that are studied in algebra, in particular in semigroups, monoids, groups, rings, fields, and vector spaces.

In mathematics, a **binary operation** or **dyadic operation** is a calculation that combines two elements (called operands) to produce another element. More formally, a binary operation is an operation of arity two.

More specifically, a binary operation *on a set* is an operation whose two domains and the codomain are the same set. Examples include the familiar arithmetic operations of addition, subtraction, multiplication. Other examples are readily found in different areas of mathematics, such as vector addition, matrix multiplication and conjugation in groups.



A binary operation ∘ is a calculation that combines the arguments x and y to $x \circ y$

1. **Binary operation:** A binary operation on a set S is a function (or mapping) from $S \times S$ into S; that is, if $f: S \times S \to S$, then f is said to be a binary operation on the set S.
   Often we use the symbols $*, \circ, +, \times, \ .$ etc. to denote the binary operation on a set S. Thus $*$ will be a binary operation on S iff $a * b \in S$ for every $a, b \in S$. A binary operation on a set S is also called a binary composition on the set S.

   Examples:

   i) Addition is a binary operation on the set $\mathbb{N}$ of all natural numbers.
   ii) Addition and subtraction are both binary operations on the set $\mathbb{Z}$ of all integers.
   iii) Multiplication is a binary operation on the set of all non-zero rational numbers.
   iv) Division is a binary operation on the set of non-zero real numbers.
   v) The matrix product is a binary operation on the set of all $n \times n$ matrices.
   vi) Vector product is a binary operation on the set of all vectors in space.
   vii) Union and intersection are binary operations in the power set of a given set.

   Non Examples:

   i) Addition is not a binary operation for the set of odd integers because the sum of two odd integers is not an odd integer.
   ii) Subtraction is not a binary operation on $\mathbb{N}$.

iii) Division is not a binary operation on the set of real numbers.

iv) Dot product of two vectors is not a binary operation over the set of all vectors.

v) Scalar multiplication of a vector by a real number is not a binary operation, because the two elements (one a vector and the other a scalar) do not belong to the same set.

2. **Algebraic Structure/ Algebraic System:** A set having one or more binary operations is known as an algebraic structure or an algebraic system.
Thus each one of the systems, $(\mathbb{N},+)$, $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$, $(\mathbb{N},\times),(\mathbb{Z},\times)$, $(\mathbb{Q},\times),(\mathbb{R},\times),(\mathbb{C},\times)$, $(\mathbb{N},+,\times)$, $(\mathbb{Z},+,\times),(\mathbb{Q},+,\times),(\mathbb{R},+,\times),(\mathbb{C},+,\times),(P(A),\cup,\cap)$ is an algebraic structure.

3. **Closure property:** A binary operation $'*'$ over a set G, is said to be defined or G is called closed under the binary operation $'*'$ if $a,b \in G \Rightarrow a*b \in G \; \forall \; a,b \in G$.

Examples:

i) The set of natural numbers, $\mathbb{N}$ is closed for the binary operation addition.

ii) The set of real numbers, $\mathbb{R}$ is closed for the binary operation multiplication.

Non Examples:

i) The set of irrational numbers, $\mathbb{Q}'$ is not closed for the binary operation multiplication.

ii) The set of odd integers is not closed for the binary operation addition.

4. **Associative Law:** A binary operation $*$ over a set G is called associative if
$(a*b)*c = a*(b*c), \forall \; a,b,c \in G$.

Examples:

i) Ordinary addition and multiplication over the sets $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ are associative.

ii) Vector addition over the set of all vectors in space is associative.

Non Examples:

i) Subtraction on the sets $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ is not associative.

ii) Division is not associative on the set of non-zero real numbers.

iii) Cross product of vectors over the set of all vectors in space is not associative.

5. **Identity Law:** There exists an element e in G such that
$e*a = a = a*e, \forall \; a \in G$.

Examples:

i) The set $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and C have 0 as the identity element w.r.to ordinary addition and 1 as the identity element w.r.to ordinary multiplication.

ii) The unit matrix of second order, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element for the set of matrices, $A_\alpha = \begin{pmatrix} cos\alpha & -sin\alpha \\ sin\alpha & cos\alpha \end{pmatrix}$, where α is a real number.

iii) $\emptyset$ is the identity element of the power set, $P(A)$ of A w.r.to the binary operation union.

Non-Examples:

i) The set of natural numbers, $\mathbb{N}$ has no identity element under addition.

6. **Inverse Law:** Each element in G possesses an inverse in G i.e. corresponding to each element $a \in G$ $\exists$ an element $b \in G$ such that $a * b = b * a = e$. The element b is then called the inverse of a and we write, $a^{-1} = b$.

Examples:

i) Inverse law holds for the set of integers, $\mathbb{Z}$ w.r.to addition, where $-a$ is the inverse for each $a \in \mathbb{Z}$.

ii) Inverse law is satisfied by the set $\mathbb{Q}, \mathbb{R}$ and C w.r.to ordinary addition.

Non-Examples:

i) The sets, $\mathbb{N}$, $\mathbb{Q}, \mathbb{R}$ and C don't obey the inverse law w.r.to multiplication.

ii) Inverse law is not satisfied by the power set, $P(A)$ of A w.r.to the binary operation union because for a non- empty subset H of A, we can not find any subset K of A such that $H \cup K = \emptyset$.

7. **Group:** An algebraic structure $(G,*)$ consisting of a non-empty set G together with a binary composition $*$, is called a group if the aforementioned axioms are satisfied by it.

Examples: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}_0, \times)$

Non examples: $(\mathbb{N}, +), (\mathbb{N}, \times), (\mathbb{Z}, \times), (\mathbb{Q}, \times), (\mathbb{R}, \times), (\mathbb{C}, \times)$

8. **Commutative Law:** A binary operation $*$ over a set G is called commutative if $a * b = b * a, \forall\, a, b \in G$.

Examples:

i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}_0, \times)$.

ii) Dot product of vectors over the set of all vectors in space is commutative.

Non-Examples:

i) Subtraction and division on the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are not commutative.

ii) Cross product of vectors over the set of all vectors in space is not commutative.

9. **Abelian group:** A group G is called abelian(or commutative) if for every $a, b \in G$, $a * b = b * a$

Examples:

i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}_0, \times)$.

ii) The set of all vectors in space with respect to vector addition.

iii) Klein's four group.

Non-Examples:

i) The Quaternion group, $S = \{\pm 1, \pm i, \pm j, \pm k\}$ w.r.to multiplication defined by $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$ is a non-abelian group.

ii) The set of all $n \times n$ non-singular matrices having their elements as rational numbers is a non-abelian group w.r.to matrix multiplication.

iii) The symmetric group S_3 of all permutations of degree 3, is a non-abelian group of order 6 with respect to composite composition.

10. **Groupoid:** A groupoid is an algebraic structure $(G, *)$ consisting of a non-empty set G and a binary composition $' * '$ defined on G.

Examples:

i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}_0, \times)$.

ii) The set of all vectors in space with respect to vector addition.

Non-Examples:

i) The set of odd integers w.r.to addition.

ii) The set of irrationals w.r.to multiplication.

iii) The set of all vectors in space with respect to dot product of vectors.

11. **Semi group:** A groupoid is called a semi-group if the binary operation $' * '$ on G is associative.

Examples:

i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{R}_0, \times)$.

ii) The set of all vectors in space with respect to vector addition.

Non-Examples:

i) $(\mathbb{N}, -), (\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{R}, -), (\mathbb{R}_0, \div), (\mathbb{N}, \div)$.

ii) The set of all vectors in space with respect to cross product of vectors.

12. **Monoid:** A semi-group $(G,*)$in which the binary operation $'*'$ on G admits an identity element in G is called a monoid.

Examples:

i) $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+),(\mathbb{R}_0,\times)$.

ii) $(\mathbb{N},\ \times)$.

iii) The power set, $P(A)$ of A w.r.to the binary operation union.

iv) The set $G=\{x: x\in\mathbb{Q}, 0<x\leq 1\}$ with respect to ordinary multiplication.

Non-Examples:

i) $(\mathbb{N},+)$.

ii) The set of even integers under multiplication.

13. **Composition table/ Cayley's Table:** Named after the 19th century British mathematician Arthur Cayley, a **Cayley table** describes the structure of a finite group by arranging all the possible products of all the group's elements in a square table reminiscent of an addition or multiplication table. Many properties of a group – such as whether or not it is closed under the binary operation, whether or not it is abelian, which is the identity element, which elements are inverses of which elements, and the size and contents of the group's center – can be discovered from its Cayley table.

A simple **example** of a Cayley table is the one for the group $\{1,-1\}$ under ordinary multiplication:

×	**1**	**−1**
1	1	−1
−1	−1	1

Rules of Cayley's table:

Let G be a non-empty finite set and the binary composition $*$ be defined on G. Then the Cayley table or composition table, is constructed in the manner indicated below.

Let $G=\{a_1,a_2,a_3,\ldots\ldots\ldots,a_n\}$. We first put down the elements $a_1,a_2,a_3,\ldots\ldots\ldots,a_n$ of the set G in a horizontal row as well as in a vertical column. Now suppose that a_i $(1\leq i\leq n)$ and a_j $(1\leq j\leq n)$ be any two arbitrary elements of G, then we write the element a_i*a_j obtained by operating a_i with a_j at the intersection of row headed by a_i and the column headed by a_j to get the following table.

$*$	a_1	a_2	...	a_i	...	a_j	...	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	...	$a_1 * a_i$	...	$a_1 * a_j$	...	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	...	$a_2 * a_i$	...	$a_2 * a_j$	...	$a_2 * a_n$
...	...	...	...	...	...	...	...	...
a_i	$a_i * a_1$	$a_i * a_2$	...	$a_i * a_i$	...	$a_i * a_j$	...	$a_i * a_n$
...	...	...	...	...	...	...	...	...
a_j	$a_j * a_1$		...		...		...	
...	...	...	...	...	...	...	...	...
a_n	$a_n * a_1$	$a_n * a_2$	...	$a_n * a_i$	...	$a_n * a_j$	...	$a_n * a_n$

From the above table, we infer the following results:-

i) **Closure Law:** If all the entries of the table are the elements of G, then G is closed under the composition $*$ and if there exists even a single entry in the table which doesn't belong to G, then G is not closed for $*$.

ii) **Existence of Identity element:** The meeting point (element), of the row which coincides with the top row and the column which coincides with the extreme left column of the Cayley table, is called the identity element in G for the composition $*$.

iii) **Existence of inverse element:** We consider the position of the identity element e anywhere in the composition table but not in the top row or the column on extreme left. If e is placed at the intersection of the row headed by a_i and the column headed by a_j, then a_i and a_j are the inverse of each other.

iv) **Commutative Law:** If the entries in every row coincide with the corresponding entries in the corresponding column, we say that the composition is commutative, otherwise it is said to be non-commutative.

14. Prepare the Cayley Table for multiplication on $G = \{1, \omega, \omega^2\}$ of cube roots of unity. Show that multiplication on G satisfies the closure property and commutativity. Find the identity element and also find the inverse of each element.

Answer: By the compositions, we obtain the composition table given here with.

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Here we observe that:-

i) All the entries in the composition table are elements of G and therefore G is closed for multiplication.

ii) Here, the row headed by 1 coincides with the top row of the table and the column headed by 1 coincide with the extreme left column of the table, and their meeting point (element) is 1. Therefore, 1 is the identity element for multiplication in G.

iii) Since 1 is the crossing of 1&1, $\omega\&\omega^2$, $\omega^2\&\omega$, so 1, ω and ω^2 are inverses of 1, ω^2 and ω respectively.

iv) Since the entries in first, second and third row of the table coincide with the corresponding entries in first, second and third column respectively, it follows that multiplication on G is commutative.

15. Show that the set $G = \{1, -1, i, -i\}$ of four fourth roots of unity is an abelian group with respect to multiplication composition.

Proof: We construct the composition table/ Cayley's table given below:

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

From this table, we conclude the following results:-

i) **Closure property:** Since all the entries in the composition table are the elements of G, so G is closed under multiplication.

ii) **Associative law:** The elements of G are complex numbers and the multiplication of complex numbers being associative, it follows that multiplication on G is associative.

iii) **Existence of identity element:** Since the first row coincides with the top row and the first column coincides with the column on extreme left and their meeting point (element) is 1, so 1 is the identity element in G for multiplication.

iv) **Existence of inverse:** Since 1 is at the crossing of $1\&1, -1\&-1, i\&-i, -i\&i$. So, the inverse of $1, -1, i$ and $-i$ are $1, -1, -i$ and i respectively.

v) **Commutative law:** Since each row of the table coincides with the corresponding column, it follows that the multiplication on G is commutative.

16. Show that the set of four matrices, $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ forms an abelian group under multiplication of matrices.

Proof: Let $A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, A_4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $G = \{A_1, A_2, A_3, A_4\}$. Then, by taking products of these matrices, taken in pairs, we prepare the composition table given below.

$*$	A_1	A_2	A_3	A_4
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_1	A_4	A_3
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_3	A_2	A_1

From this table, we observe that:

i) All the entries in the composition table are members of G. So, G is closed for multiplication.

ii) Since matrix multiplication is associative in general, so it is associative in G.

iii) Since the first row coincides with the top row and the first column coincides with the column on extreme left and their meeting point (element) is A_1, So A_1 is the identity element in G.

iv) Here, A_1 is at the crossing of $A_1 \& A_1$, $A_2 \& A_2$, $A_3 \& A_3$, $A_4 \& A_4$. It follows that ${A_1}^{-1} = A_1, {A_2}^{-1} = A_2, {A_3}^{-1} = A_3, {A_4}^{-1} = A_4$. So, each member of G possesses an inverse in G.

v) Since each row of the table coincides with the corresponding column, it follows that the multiplication on G is commutative.

Hence, $(G, *)$ is an abelian group.

17. **New compositions on Integers:** Let m be an arbitrary but fixed positive integer. Then, for any integers a and b, we define the following compositions.

a) **Addition modulo m**, to be denoted by $+_m$, is defined, as $a +_m b = r$, where r is the least non-negative remainder obtained by dividing $(a + b)$ by m. Clearly, $0 \leq r < m$. For **example**, $2 +_5 3 = 0$, as the least non-negative remainder obtained by dividing $(2 + 3)$ i.e. 5 by 5, is 0. Similarly, $2 +_4 3 = 1$, $5 +_9 6 = 2$,

$$-24 +_5 9 = 0 \; for \; -24 + 9 = -15 = -3 \times 5 + 0,$$

$$\text{and } -9 +_{12} 7 = 10 \; for \; -9 + 7 = -2 = -1 \times 12 + 10$$

What will you say about the followings?

i) $2 +_4 5 =$?

ii) $7 +_3 3 =$?

iii) $4+_5 9 =$?

iv) $-23+_3 3 =$?

b) **Multiplication modulo m**, to be denoted by $\times_m$ is defined as as $a \times_m b = r$, where r is the least non-negative remainder obtained by dividing ab by m. Clearly, $0 \leq r < m$.
Thus, $2 \times_5 3 = 1, 6 \times_8 3 = 2, 4 \times_7 6 = 3$ and
$-9 \times_4 6 = 2\ for -9 \times 6 = -54 = -14 \times 4 + 2$. What about the followings?
i) $2 \times_4 3 =$? ii) $12 \times_5 4 =$? iii) $4 \times_8 2 =$? iv) $-10 \times_7 9 =$?

18. Show that the set $G = \{0, 1, 2, 3\}$ is a finite abelian group of order four with respect to addition modulo 4.

Proof: We construct the composition table given below:-

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

From this table, we infer the following results:-

i) **Closure property:** All the entries in the composition table are members of G. So, G is closed for $+_4$.

ii) **Associative law:** For any three elements a, b, c of G $(a+_4 b)+_4 c$ and $a+_4(b+_4 c)$ denote the least non-negative remainder obtained by dividing $(a + b) + c$ by 4 and that obtained by dividing $a + (b + c)$ by 4.
But $(a + b) + c = a + (b + c)$.
So, the corresponding remainders will be same.
Hence, $(a+_4 b)+_4 c = (a+_4(b+_4 c) \forall\ a, b, c \in G$.

iii) **Existence of Identity:** Since the first row coincides with the top row and the first column coincides with the column on extreme left and their meeting point (element) is 0, it follows that 0 is the identity element.

iv) **Existence of Inverse:** Clearly, 0 lies at the crossing of 0 and 0, 1 and 3, 2 and 2, 3 and 1. So, the inverses of 0, 1, 2 and 3 are 0, 3, 2 and 1 respectively.

v) **Commutative Law:** Since each row of the table coincides with the corresponding column, So $+_4$ is commutative on G.

Here, G is a non-empty set of 4 elements. Therefore, we may conclude that G is a finite abelian group of order four with respect to addition modulo 4.

19. Show that the set $G = \{1, 5, 7, 11\}$ is a group with respect to multiplication modulo 12.

Proof: We construct the composition table given below:-

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

From this table, we infer the following results:-

i) **Closure property:** All the entries in the composition table are members of G. So, G is closed for $\times_{12}$.

ii) **Associative law:** For any three elements a, b, c of G, $(a \times_{12} b) \times_{12} c$ and $a \times_{12} (b \times_{12} c)$ denote the least non-negative remainder obtained by dividing $(a \times b) \times c$ by 12 and that obtained by dividing $a \times (b \times c)$ by 12.
But $(a \times b) \times c = a \times (b \times c)$.
So, the corresponding remainders will be same.
Hence, $(a \times_{12} b) \times_{12} c = a \times_{12} (b \times_{12} c)\ \forall\ a, b, c \in G$.

iii) **Existence of Identity:** Since the first row coincides with the top row and the first column coincides with the column on extreme left and their meeting point (element) is 1, it follows that 1 is the identity element.

iv) **Existence of Inverse:** Clearly, 1 lies at the crossing of 1 and 1, 5 and 5, 7 and 7, 11 and 11. So, the inverses of 1, 5, 7 and 11 are 1, 5, 7 and 11 respectively.

Therefore, we may conclude that G is a group with respect to multiplication modulo 12.

20. Prove that the operation * on the set $\mathbb{Z}$ of integers defined by $a * b = a + b + 1\ \ \forall\ a, b \in \mathbb{Z}$ satisfies the closure property, the associativity and the commutativity. Find the identity element. What is the inverse of an integer a?

Solution: For all integers a and b, $a + b + 1$ and therefore $a * b$ is clearly an integer. So, closure property is satisfied.

Also, $(a * b) * c = (a + b + 1) * c$
$= (a + b + 1) + c + 1$
$= (a + b + c) + 2$

and $a * (b * c) = a * (b + c + 1)$
$= a + (b + c + 1) + 1$
$= (a + b + c) + 2$

$\therefore (a * b) * c = a * (b * c)\ \forall\ a, b, c \in \mathbb{Z}$.

Thus, the associative law is satisfied.

Again, $a * b = a + b + 1 = b + a + 1 = b * a$

$\therefore a * b = b * a \; \forall \; a, b \in \mathbb{Z}$

Hence, commutative law is satisfied.
Now, if e is the identity element in $\mathbb{Z}$ for *, then $a * e = a \Rightarrow a + e + 1 = a \Rightarrow e = -1$.
So, -1 is the identity for * in $\mathbb{Z}$.
Also, $a * b = -1 \Rightarrow a + b + 1 = -1 \Rightarrow b = -(2 + a)$
So, the inverse of a is $-(2 + a)$.

21. On the set $\mathbb{Q} - \{1\}$ of all rational numbers except 1, define an operation by
$a * b = a + b - ab \; \forall a, b \in \mathbb{Q} - \{1\}$.
Show that $*$ on $\mathbb{Q} - \{1\}$ satisfies the closure property, the associative law and the commutative law. What is the identity element? Also, investigate the value of inverse of an element
$a \in \mathbb{Q} - \{1\}$.

Solution:
Closure property: a, b is clearly a rational number, whenever a and b are in $\mathbb{Q} - \{1\}$. But, $a * b = 1 \Rightarrow a + b - ab = 1 \Rightarrow a(1 - b) = (1 - b) \Rightarrow a = 1$, which is a contradiction, since a is different from 1.
So, $a * b \neq 1 \; i.e., a * b \in \mathbb{Q} - \{1\} \;\; \forall a, b \in \mathbb{Q} - \{1\}$.
$\therefore$ Closure law is satisfied.
Associative law: $\forall \; a, b, c \in \mathbb{Q} - \{1\}$, we have
$(a * b) * c = (a + b - ab) * c$
$= a + b - ab + c - (a + b - ab)c$
$= a + b + c - ab - bc + abc$

Similarly, $a * (b * c) = a + b + c - ab - bc + abc$
$\therefore$ Associative law holds in $\mathbb{Q} - \{1\}$.

Identity Law: If e is the identity element in $\mathbb{Q} - \{1\}$, then $a * e = a \Rightarrow a + e - ae = a \Rightarrow e = 0$.
So, 0 is the identity in $\mathbb{Q} - \{1\}$.
Inverse law: If b is the inverse of a in $\mathbb{Q} - \{1\}$, then $a * b = 0 \Rightarrow a + b - ab = 0 \Rightarrow b = \frac{a}{a-1}$.

Home Work Problems:

22. Prepare the Cayley's table for the followings:

- $(\{-1, 0, 1\}, +)$
- $(\{-1, \; 1\}, \times)$
- $(\{1, -1, i, -i\}, \; \times)$
- The set of four matrices, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ under multiplication of matrices.

23. Determine which of the above sets with operation indicated form a group.
24. Examine whether the set $\{-1, 0, 1\}$ is closed for addition.
25. Does the set of odd integers form a group w.r.to addition? Justify your answer.
26. Does the set of odd integers form a group w.r.to multiplication? Justify your answer.
27. Does the set of even integers form a group w.r.to addition? Justify your answer.
28. Does the set of even integers form a group w.r.to multiplication? Justify your answer.
29. Examine whether the set $\{-2, -1, 0, 1, 2\}$ forms a group w. r. to addition
30. Give an example of a group which consists of i) one element ii) two elements iii) three elements and iv)four elements.
31. None of the algebraic systems, $(\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{R}, -)$, $(\mathbb{N}, -)$ and $(C, -)$ is a group. To What extend do you agree with this?
32. On the set $\mathbb{Q}^+$ of positive rational numbers, define an operation $*$ by $a * b = \frac{ab}{2}, \forall\, a, b \in \mathbb{Q}^+$. Show that
    i) $\mathbb{Q}^+$ is closed for $*$
    ii) $*$ is commutative on $\mathbb{Q}^+$
    iii) $*$ is associative on $\mathbb{Q}^+$

    Also, find the identity element in $\mathbb{Q}^+$ for $*$. What do you say about the inverse of an element $a \in \mathbb{Q}^+$?
33. Show that the set of all matrices of the form $\begin{pmatrix} x & x \\ x & x \end{pmatrix}$, where x is a non-zero real number, is a group of singular matrices for multiplication.
34. Prove that $G = \{1, 2, 3, 4, 5\}$ is a finite abelian group of order 6, relative to multiplication modulo 7.
35. Is the set $\{1, 2, 3, 4, 5\}$ a group under i) addition modulo 6 ii) multiplication modulo 6?

****

Elementary Properties of groups and Order of an element of a Group

Disclaimer: These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.

Theorem 1. (Uniqueness of Identity) The identity element in a group is unique.

Proof. Let G be a group and if possible, let e and e' be two identity elements in G. Then,

$$e\,e' = e'\,e = e' \qquad [\because e \text{ is identity}]$$

$$\text{and} \quad e\,e' = e'\,e = e \qquad [\because e' \text{ is identity}]$$

$$\therefore \quad e = e'.$$

Hence, the identity in G is unique.

Theorem 2. (Uniqueness of Inverse) Each element of a group has a unique inverse.

Proof. Let G be a group and e be the identity element in G. Let a be an arbitrary element of G and if possible, let b as well as c be an inverse of a. Then,

$$ab = ba = e \text{ and } ac = ca = e.$$

$$\text{Now} \quad ba = e \quad \Rightarrow \quad (ba)\,c = ec = c$$

$$\text{and} \quad ac = e \quad \Rightarrow \quad b\,(ac) = b\,e = b.$$

$$\text{But, by associative law,} \quad (ba)\,c = b\,(ac).$$

$$\therefore \quad b = c, \text{ showing that } a \text{ has a unique inverse.}$$

Thus, each element of the group G has a unique inverse.

Theorem 3. The inverse of the inverse of an element of a group is the element itself.

Proof. Let G be a group and e be the identity element in G. Let a be an arbitrary element of G. Then, $a^{-1}\,a = e$.

Now $$a^{-1}\,a = e$$

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

$$\Rightarrow \quad [(a^{-1})^{-1}\,a^{-1}]\,a = (a^{-1})^{-1} \qquad \text{[by associativity]}$$

$$\Rightarrow \quad e\,a = (a^{-1})^{-1} \qquad [\because (a^{-1})^{-1}\,a^{-1} = e]$$

$$\Rightarrow \quad a = (a^{-1})^{-1}.$$

Hence $(a^{-1})^{-1} = a$.

Theorem 4. Cancellation laws hold in a group.

i.e. in a group G, for all $a, b, c \in G$.

$$a\,b = a\,c \;\Rightarrow\; b = c \quad \text{[Left cancellation law]}$$

and $b\,a = c\,a \;\Rightarrow\; b = c$ [Right cancellation law]

Proof. Let e be the identity element in G. Then,

$a\,b = a\,c \;\Rightarrow\; a^{-1}(a\,b) = a^{-1}(a\,c)$

$\Rightarrow\; (a^{-1}\,a)\,b = (a^{-1}\,a)\,c$ [by associative law]

$\Rightarrow\; e\,b = e\,c$ $[\because\ a^{-1}\,a = e]$

$\Rightarrow\; b = c$.

Again,

$b\,a = c\,a \;\Rightarrow\; (b\,a)\,a^{-1} = (c\,a)\,a^{-1}$

$\Rightarrow\; b\,(a\,a^{-1}) = c\,(a\,a^{-1})$ [by associative law]

$\Rightarrow\; b\,e = c\,e$ $[\because\ a\,a^{-1} = e]$

$\Rightarrow\; b = c$.

Theorem 5.(Reversal law for inverse of the product) Let G be a group, then $(ab)^{-1} = b^{-1}a^{-1}$ $\forall$ a, b $\in$ G .

Proof. Let e be the identity element in G. Then,

$(a\,b)(b^{-1}a^{-1}) = [(a\,b)\,b^{-1}]\,a^{-1}$ [by associative law]

$= [a\,(b\,b^{-1})]\,a^{-1}$ [by associative law]

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

$= a\,a^{-1}$ $[\because\ a\,e = a]$

$= e$.

Also,

$(b^{-1}a^{-1})(a\,b) = [(b^{-1}\,a^{-1})\,a]\,b$ [by associative law]

$= [b^{-1}\ (a^{-1}\ a)]\ b$ [by associative law]

$= (b^{-1}e)\ b$ [$\because\ a^{-1}\ a = e$]

$= b^{-1}\ b$ [$\because\ b^{-1}e = b^{-1}$]

$= e$.

Thus, $(a\ b)\ (b^{-1}a^{-1}) = (b^{-1}a^{-1})\ (a\ b) = e$.

Hence, $(ab)^{-1} = b^{-1}a^{-1}$ [$\because\ x\ y = y\ x = e \Leftrightarrow x^{-1} = y$]

Theorem 6. If a and b are any two elements of a group G, then the equations $ax = b$ *and* $ya = b$, have unique solutions in G.

Proof. If x is an element of G such that $ax = b$, then

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

$\Rightarrow (a^{-1}\ a)\ x = a^{-1}\ b$ [by associative law]

$\Rightarrow e\ x = a^{-1}\ b$ [$\because\ a^{-1}\ a = e$]

$\Rightarrow x = a^{-1}\ b$ [$\because\ e\ x = x$]

More-over, $a \in G, b \in G \Rightarrow a^{-1} \in G, b \in G \Rightarrow a^{-1}\ b \in G$.

Thus, $x = a^{-1}\ b \in G$, is a solution of the equation, $ax = b$.

Now, if possible, let $x = x_1$ and $x = x_2$ be any two solutions of $ax = b$ in G. Then $ax_1 = b$ and $ax_2 = b$.

$\therefore\ ax_1 = ax_2$, which by cancellation law, gives $x_1 = x_2$.

Thus, the equation, $ax = b$ has a unique solution in G. Similarly, it may be proved that the equation, $ya = b$ has a unique solution, $y = ba^{-1} \in G$.

Integral powers of an element of a group:

Let G be a group, whose composition has been denoted multiplicatively. Let $a \in G$. Then, by closure property, a, aa, aaa etc. are all elements of G. Also, the composition being associative on G, the product $aaa\ldots\ \ldots\ \ldots a$ is independent of the manner in which the factors are grouped.

For any positive integer *n*, we use the notation $(aaa \ldots \ldots \ldots \text{ to } n \text{ factors}) = a^n$ and by closure property, $a^n \in G$.

In particular, we write $a = a^1$, $aa = a^2$, $aaa = a^3$ and so on.

Also, if *e* is the identity element in *G*, we write $e = a^0$.

It is conventional to write, $(a^n)^{-1} = a^{-n}$.

Further, $(a^n)^{-1} = (aaa \ldots \ldots \ldots to\ n\ factors)^{-1}$

$= a^{-1}a^{-1}a^{-1} \ldots \ldots \ldots$ to *n* factors

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

$\therefore \quad a^{-n} = (a^n)^{-1} = (a^{-1})^n$.

Remark. For an arbitrary element *a* of a group *G* and for arbitrary integers *m* and *n*, it is easy to verify that

(i) $a^m\, a^n = a^{m+n}$
(ii) $(a^m)^n = a^{mn}$
(iii) $e^n = e$, where *e* is the identity element in *G*.

Order of an element of a group:

Let e be the identity element of a group G, then, an element a ∈ G is said to be of order (or period) m if m is the least positive integer such that $a^m = e$ when G is a group under multiplication or $ma = e$; when G is a group under addition and we write, $\circ(a) = m$. In case, such an m does not exist, we say that a is of infinite or zeroth order.

Examples:

i) Consider the multiplicative group $G = \{1, \omega, \omega^2\}$ of cube roots of unity.
Here, 1 is the least positive integer such that $1^1 = 1$, so $\circ(1) = 1$, 3 is the least positive integer such that $\omega^3 = 1$, So $\circ(\omega) = 3$.
Similarly, $\circ(\omega^2) = 3$.

ii) Suppose $G = \{1, -1, i, -i\}$ is a group under multiplication. Here,
1 is the least positive integer such that $1^1 = 1$, so $\circ(1) = 1$
2 is the least positive integer such that $(-1)^2 = 1$, so $\circ(-1) = 2$
4 is the least positive integer such that $i^4 = 1$, so $\circ(i) = 4$
4 is the least positive integer such that $(-i)^4 = 1$, so $\circ(-i) = 4$

iii) Consider the group $(G = \{0, 1, 2, 3\}, +_4)$.
Since, 0 is the identity element, so $\circ(0) = 1$.
Also, $(1+_4 1+_4 1+_4 1)$ (4 factors) $= 0 \Rightarrow \circ(1) = 4$;
$(2+_4 2)$ (2 factors) $= 0 \Rightarrow \circ(2) = 2$;
$(3+_4 3+_4 3+_4 3)$ (4 factors) $= 0 \Rightarrow \circ(3) = 4$.
Thus, $\circ(0) = 1$, $\circ(1) = 4$, $\circ(2) = 2$, $\circ(3) = 4$.

iv) In the additive group of integers, 0 being the identity element, so its order is 1.
If a be a non-zero integer, then ∃ no positive integer m such that (a+a+… … … m times) = 0.
So, $\circ(a)$ is infinite.

Remark 1. **Clearly, $\circ(e) = 1$.**

If a is an element of G, other than identity such that $\circ(a) = 1$, then by definition, 1 is the least positive integer such that $a^1 = e$. So, $a = e$.

Thus, identity element in a group is the only element whose order is 1.

Remark 2. **If n is a positive integer such that $a^n = e$, then $\circ(a) \leq n$.**

In case, n is the least positive integer for which $a^n = e$, then $\circ(a) = n$. On the other hand, if ∃ a positive integer $m < n$ such that $a^m = e$, then $\circ(a) = m < n$ i.e., $\circ(a) < n$. Therefore, $\circ(a) \leq n$.

Torsion group: A group G is called **a torsion group** or **a periodic group,** if every element of G is of finite order .

Examples:

i) The multiplicative group, $G = \{1, \omega, \omega^2\}$ of cube roots of unity is a torsion group.
ii) The group $(G = \{0, 1, 2, 3\}, +_4)$ is a torsion group.

Non-Examples:

i) $(\mathbb{Z}, +)$ is not a torsion group.
ii) The multiplicative group $(\mathbb{Q}_0, \times)$ of non-zero rational numbers is not a torsion group.

Torsion free group: A group G is called **a torsion free group,** if no element other than the identity element is of finite order .

Examples:

i) $(\mathbb{Z}, +)$ is a torsion free group.
ii) $(\mathbb{R}, +)$ is a torsion free group.

Non-Examples:

i) The multiplicative group, $G = \{1, -1, i, -i\}$ is not a torsion free group.
ii) The multiplicative group, $(\mathbb{Q}_0, \times)$ of non-zero rational numbers is not a torsion free group.

Mixed group: A group *G* is called **a mixed group,** if there exist at least two elements, distinct from the identity element, in such a way that one of them is of finite order and the other one is of infinite order .

Examples:

i) In the multiplicative group $(\mathbb{Q}_0, \times)$ of non-zero rational numbers, 1 is the identity element and so its order is 1.
Also, $\circ(-1) = 2$.
Clearly, no element of $\mathbb{Q}_0$, other than 1 and -1, is of finite order.
So, it is an example of a **mixed group**.
ii) The multiplicative group, $(\mathbb{R}_0, \times)$ of non-zero real numbers is a mixed group.

Non-Examples:

i) The multiplicative group, $G = \{1, \omega, \omega^2\}$ of cube roots of unity is not a mixed group.
ii) $(\mathbb{Q}, +)$ is not a mixed group.

Some results on orders of elements of a group:

Theorem 1: The order of every element of a finite group is finite.

Proof: Let *G* be a finite group whose composition has been denoted multiplicatively. Let *e* be the identity element in *G*. Let *a* be an arbitrary element of *G*.

Consider all positive integral powers of *a i.e.* $a, a^2, a^3, a^4, \ldots\ldots\ldots, a^l, \ldots\ldots\ldots, a^k, \ldots\ldots$

By closure property, these are all elements of *G*.

But, *G* being finite, all these elements cannot be distinct.

Let us suppose that $a^k = a^l$, where $k > l$.

Now, $a^k = a^l \Rightarrow a^k.(a^l)^{-1} = a^l.(a^l)^{-1}$

$\Rightarrow \quad a^k . a^{-l} = e$

$\Rightarrow \quad a^{k-l} = e$

$\Rightarrow \quad a^m = e$, where $m=k-l > 0$, since $k > l$.

Thus, m is a positive integer, such that $a^m = e$.

Since, every set of positive integers has a least member, So the set of all those positive integers m such that $a^m = e$, has a least member n.

Clearly, $\circ(a) = n$, which is finite.

Hence, the order of each element of the finite group G is finite.

Corollary: The order of any element of a finite group can never exceed the order of the group.

Proof. Let G be a finite group and a be an arbitrary element of G. Let $\circ(a) = n$.

Let, if possible, $n > \circ(G)$.

Now, if we consider $a, a^2, a^3, \ldots \ldots \ldots, a^n$, then by closure property, these are all elements of G.

No two of these are equal.

For, if $a^i = a^j$, where $1 \leq j < i \leq n$, then

$a^i = a^j \quad \Rightarrow \quad a^i . (a^j)^{-1} = (a^j)(a^j)^{-1}$

$\Rightarrow \quad a^i . a^{-j} = e$

$\Rightarrow \quad a^{i-j} = e$

$\Rightarrow \quad \circ(a) \leq i - j < n$, which is a contradiction.

Thus, $a, a^2, a^3, \ldots \ldots \ldots, a^n$ are n distinct elements of G.

This shows that $\circ(G) \geq n$.

Thus, the supposition that $\circ(a) = n > \circ(G)$, is wrong.

Hence, $\circ(a) \leq \circ(G)$.

Theorem 2: The order of an element of a group is the same as that its inverse.

Proof. Let $\circ(a) = m$ and $\circ(a^{-1}) = n$.

Then, $\circ(a) = m \Rightarrow a^m = e$

$\Rightarrow (a^m)^{-1} = e^{-1} = e$

$\Rightarrow (a^{-1})^m = e$ $[\because (a^m)^{-1} = (a^{-1})^m]$

$\Rightarrow \circ(a^{-1}) \leq m$

$\Rightarrow n \leq m.$ … … ... (i)

Also,

$\circ(a^{-1}) = n \Rightarrow (a^{-1})^n = e$

$\Rightarrow (a^n)^{-1} = e$

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

$\Rightarrow \circ(a) \leq n$

$\Rightarrow m \leq n$ … … ... (ii)

Thus, from (i) and (ii), we have $m=n$, *i.e.* $\circ(a) = \circ(a^{-1})$.

Now, suppose that order of a is infinite and if possible, let $\circ(a^{-1})$ be finite, say n.

Then, $\circ(a^{-1}) = n \Rightarrow (a^{-1})^n = e$

$\Rightarrow (a^n)^{-1} = e$

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

$\Rightarrow \circ(a) \leq n,$ which is finite.

This contradicts the hypothesis that $\circ(a)$ is infinite.

So, $\circ(a)$ is infinite $\Rightarrow \circ(a^{-1})$ is infinite.

Hence, $\circ(a) = \circ(a^{-1})$.

Theorem 3: If a and b are any two arbitrary elements of a group G, then

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

Proof: Let $\circ(a) = m$. Then, m is the least positive integer, such that $a^m = e$.

Now, $(b^{-1}ab)^m = (b^{-1}ab)\,(b^{-1}ab)$ … … … to m factors

$= b^{-1}ab\; b^{-1}ab$… … … $b^{-1}ab$ [by associativity]

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

$= b^{-1}\,a^m\,b$

$= b^{-1}\,b$ [$\because$ $a^m = e$]

$= e$

Since, by the given hypothesis, m is the least positive integer such that $a^m = e$, so m is the least positive integer such that $(b^{-1}ab)^m = e$.

Hence, $\circ(b^{-1}ab) = m = \circ(a)$.

Theorem 4: For any two elements a, b of a group, the order of ab is the same as that of ba.

Proof: We have

$ba = e\,(ba) = a^{-1}\,a\,(ba) = a^{-1}\,(ab)\,a$

$\therefore\ \circ(ba) = \circ[a^{-1}\,(ab)\,a] = \circ(ab)$.

Theorem 5: The order of any integral power of an element of a group can never exceed the order of the element.

Proof: Let a be an arbitrary element of a group G and let k be any integer positive or negative. Then, we have to show that $\circ(a^k) \leq \circ(a)$.

If $\circ(a)$ is infinite, then the result is obvious.

So, let us suppose that $\circ(a)$ is finite and let $\circ(a) = n$.

Then, $\circ(a) = n \Rightarrow a^n = e$, where e is the identity element in G

$\Rightarrow (a^n)^k = e^k = e$

$\Rightarrow \quad a^{nk} = e$

$\Rightarrow \quad (a^k)^n = e$

$\Rightarrow \quad \circ(a^k) \leq n = \circ(a).$

Hence $\circ(a^k) \leq \circ(a)$.

Theorem 6: If an element a of a group G is of order n and e is the identity element in G, then for some positive integer m,

$a^m = e \quad \Leftrightarrow$ n is a divisor of m.

Proof: Let $\circ(a) = n$ and $a^m = e$ for some positive integer m. Then, we have to show that n is a divisor of m.

Now, $\circ(a) = n$ and $a^m = e \quad \Rightarrow \quad m \geq n$.

If $m = n$, then n is clearly a divisor of m.

So, consider the case, when $m > n$.

In this case, by division algorithm, there exist integers q and r such that

$m = nq + r$, where $0 \leq r < n$.

$\therefore \quad a^m = e \quad \Rightarrow \quad a^{nq+r} = e$

$\Rightarrow \quad a^{nq}\, a^r = e$

$\Rightarrow \quad a^r = e \qquad [\because \quad a^{nq} = (a^n)^q = e^q = e]$

Thus, r is the non-negative integer such that $0 \leq r < n$ and $a^r = e$. But, n being the least positive integer such that $a^n = e$.

So, r cannot be positive.

Consequently, $r = 0$ and therefore $m = nq$.

Accordingly, n is a divisor of m.

Conversely, let n be a divisor of m.

Then, $m = nq$ for some positive integer q.

$\therefore \quad a^m = a^{nq} = (a^n)^q = e^q = e.$

Theorem 7: If the order of an element a of a group G is n and p is an integer relatively prime to n, then $\circ(a^p) = n$.

Proof: Let $\circ(a^p) = m$. Then,

$\circ(a) = n \Rightarrow a^n = e$, where e is the identity element in G.

$\Rightarrow (a^n)^p = e^p = e$

$\Rightarrow a^{np} = e$

$\Rightarrow (a^p)^n = e$

$\Rightarrow \circ(a^p) \leq n$

$\Rightarrow m \leq n$ …… (i) [$\because \circ(a^p) = m$]

Now, by the given hypothesis p and n are relatively prime, so there exist integers q and r such that $pq+nr = 1$.

$\therefore a = a^1 = a^{pq+nr} = (a^p)^q \cdot (a^n)^r = (a^p)^q$ [$\because (a^n)^r = e^r = e$]

So, $a^m = [(a^p)^q]^m = (a^p)^{qm} = [(a^p)^m]^q = e^q = e$ [$\because \circ(a^p) = m$]

Now, $\circ(a) = n$ and $a^m = e \Rightarrow m \geq n$. …… (ii)

Thus, from (i) and (ii), we have $m = n$.

Hence, $\circ(a^p) = n$.

Some Illustrative Examples:

Ex. 1. If any two elements a and b of group G commute, then show that:

(i) $a^{-1} b^{-1} = b^{-1} a^{-1}$
(ii) $a^{-1} b = b a^{-1}$
(iii) $a b^{-1} = b^{-1} a$.

Solution:

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

$\Rightarrow b^{-1} a^{-1} = a^{-1} b^{-1}$ [by reversal law of inverses]

(ii) $ab = ba \Rightarrow b = a^{-1}(ba) = (a^{-1}b)\,a$ [by associative law]

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

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

(iii) $ab = ba \Rightarrow a = (ba)\,b^{-1} = b\,(a\,b^{-1})$ [by associative law]

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

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

Ex. 2. For any two elements a and b of a group G, show that $(ab)^2 = a^2\,b^2$ iff G is abelian.

Solution: Let $(ab)^2 = a^2\,b^2 \quad \forall\, a, b \in G$.

Then, $(ab)^2 = a^2\,b^2 \Rightarrow (ab)\,(ab) = (aa)\,(bb)$

$\Rightarrow (a)\,(ba)\,b = a\,(ab)\,b$ [by associative law]

$\Rightarrow ba = ab$ [by cancellation laws]

Thus, $ab = ba \quad \forall\, a, b \in G$.

Hence, G is abelian.

Conversely, let G be abelian so, that $ab = ba \quad \forall\, a, b \in G$.

Now, $(ab)^2 = (ab)\,(ab)$

$= a\,(ba)\,b$ [by associative law]

$= a\,(ab)\,b$ [$\because$ $ba = ab$]

$= (aa)\,(bb)$ [by associative law]

$= a^2\,b^2$.

Thus, $(ab)^2 = a^2\,b^2 \quad \forall\, a, b \in G$.

Ex. 3. If each element of a group, except the identity element, is of order 2, show that the group is abelian.

Solution: Let G be a group.

Let $a \in G$ and $b \in G$. Then, by closure property, $ab \in G$.

Now, according to given hypothesis

$$\circ(a) = 2, \quad \circ(b) = 2, \quad \circ(ab) = 2$$

i.e. $a^2 = e$, $b^2 = e$, $(ab)^2 = e$, where e is the identity.

Now, $a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$.

Similarly, $b^2 = e \Rightarrow b^{-1} = b$

and $(ab)^2 = e \Rightarrow (ab)^{-1} = ab$

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

$\Rightarrow ba = ab \quad [\because \quad b^{-1} = b \ \& \ a^{-1} = a]$

Thus, $ab = ba \quad \forall\, a, b \in G$.

Hence, G is abelian.

Ex. 4. Let G be a group of even order, then show that there exists an element a, other than the identity element, such that $a^2 = e$.

Solution: Let G be a group of even order, say $2n$. Let $a \in G$.

Now, $a^2 = e \Rightarrow aa = e \Rightarrow a^{-1} = a$.

Thus, we must show that $\exists$ an element $a \neq e$ such that $a^{-1} = a$.

Suppose that no such an element exists.

Now, in a group, every element possesses a unique inverse. The identity element is the only element such that $e^{-1} = e$. The remaining $(2n\text{-}1)$ elements must therefore, be divided into pairs in such a way that each pair consists of two distinct elements, which are inverses of each other.

But, this is impossible, since $(2n\text{-}1)$ is odd.

So, there exists $a \in G$ such that $a \neq e$ and $a^{-1} = a$.

Hence, $\exists\ a \in G$ such that $a \neq e$ and $a^2 = e$.

Ex. 5. If a and b are two arbitrary elements of an abelian group G, then show that for all integers n, $(ab)^n = a^n b^n$.

Solution: **Case *I.*** *When* $n = 0$.

In this case, $a^0 = e$, $b^0 = e$, $(ab)^0 = e$.

$\therefore \quad a^0 b^0 = ee = e = (ab)^0$.

Hence, $(ab)^0 = a^0 b^0$.

Case *II.* *When* $n > 0$. *i.e. n is a positive integer*.

In this case, we shall prove the result by induction.

Clearly, $(ab)^1 = ab = a^1 b^1$.

So, the result is true for $n = 1$.

Let it be true for $n = m$, so that $(ab)^m = a^m b^m$.

Now, $(ab)^{m+1} = (ab)^m (ab)$

$= (a^m b^m)(ab)$ [$\because \quad (ab)^m = a^m b^m$]

$= a^m (b^m a) b$ [by associative law]

$= a^m (ab^m) b$ [$\because$ G being abelian, $b^m a = ab^m$]

$= (a^m a)(b^m b)$ [by associative law]

$= a^{m+1} b^{m+1}$.

Thus, it follows that, if the result is true for $n = m$, then it is also true for $n = (m+1)$.

So, by the principle of mathematical induction, the required result is true for all positive integers.

Case *III*. *When* $n < 0$. *i.e. n is a negative integer.*

Let $n = -m$, where m is a positive integer. Then,

$(ab)^n = (ab)^{-m} = [(ab)^m]^{-1}$

$= (a^m b^m)^{-1}$ [$\because \quad (ab)^m = a^m b^m \quad \forall \ m \in \mathbb{Z}^+$]

$= (b^m a^m)^{-1}$ [$\because$ G being abelian, $a^m b^m = b^m a^m$]

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

$= a^{-m}\, b^{-m}$

$= a^n\, b^n$ [$\because$ $-m = n$]

Hence, $(ab)^n = a^n\, b^n$, for every integer n.

Ex. 6. If G is a group in which $(ab)^i = a^i\, b^i$, for three consecutive integers i and for a, b ∈ G ; show that G is abelian.

Give an example to show that a group is not necessarily abelian, if the relation $(ab)^i = a^i\, b^i$ holds for just two consecutive integers.

Solution: Let $(ab)^i = a^i\, b^i$, $(ab)^{i+1} = a^{i+1}\, b^{i+1}$ & $(ab)^{i+2} = a^{i+2}\, b^{i+2}$.

Then, $(ab)^{i+2} = a^{i+2}\, b^{i+2}$

$\Rightarrow$ $(ab)^{i+1}\,(ab) = (a^{i+1}\, a)\,(b^{i+1}\, b)$

$\Rightarrow$ $(a^{i+1}\, b^{i+1})\,(ab) = (a^{i+1}\, a)\,(b^{i+1}\, b)$ [$\because$ $(ab)^{i+1} = a^{i+1}\, b^{i+1}$]

$\Rightarrow$ $a^{i+1}\,(b^{i+1}\, a)\, b = a^{i+1}\,(a\, b^{i+1})\, b$ [by associative law]

$\Rightarrow$ $b^{i+1}\, a = a\, b^{i+1}$ [by cancellation laws]

$\Rightarrow$ $a^i\,(b^{i+1}\, a) = a^i\,(a\, b^{i+1})$

$\Rightarrow$ $(a^i\, b^i)\,(ba) = (a^i\, a)\, b^{i+1}$

$\Rightarrow$ $(ab)^i\,(ba) = a^{i+1}\, b^{i+1} = (ab)^{i+1} = (ab)^i\,(ab)$

$\Rightarrow$ $ba = ab$ [by cancellation laws]

Thus, $ab = ba \;\forall\; a, b \in G$.

Hence, G is abelian.

For, another part of the problem, consider the Quaternion group, $S = \{\pm 1,\ \pm i,\ \pm j,\ \pm k\}$ with multiplication on S, defined by

$i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

In this group, it is easy to verify that

$(ab)^4 = a^4\, b^4$ and $(ab)^5 = a^5\, b^5$ $\forall\; a, b \in S$.

i.e. $(ab)^i = a^i\, b^i$ holds for two consecutive values 4 and 5 of i.

But, it is clear from the definition of the composition that S is non-abelian.

Ex. 7. Let G be a group. Let a ∈ G such that ∘ (a) = n. Then for any integer m, show that ∘ $(a^m) = \frac{n}{(n,m)}$, where (n, m) denotes the H.C.F. of n and m.

Solution: Let $(n, m) = k$. Then, $n = pk$ *and* $m = qk$ for some integers p and q such that $(p, q) = 1$.

Let, $\circ(a^m) = r$. Then, $(a^m)^r = e$ or $a^{mr} = e$.

Now, $\circ(a) = n$ and $a^{mr} = e \Rightarrow n \mid mr$.

But, $n \mid mr \Rightarrow pk \mid qkr$ [$\because$ $n = pk$ and $m = qk$]

$\Rightarrow p \mid qr$

$\Rightarrow p \mid r$ [$\because$ p and q are relatively prime]

Again, $(a^m)^p = (a^{qk})^p = a^{q(pk)} = a^{qn} = (a^n)^q = e^q = e$.

Now, $\circ(a^m) = r$ and $(a^m)^p = e \Rightarrow r \mid p$.

Thus, $p \mid r$ and $r \mid p \Rightarrow p = r$.

$\therefore \circ(a^m) = r = p = \frac{n}{k} = \frac{n}{(n,m)}$.

Ex. 8. If the elements a, b of a group G commute and ∘ (a) = m, ∘ (b) = n, where m and n are relatively prime, then show that ∘ (ab) = mn.

Solution: Let $\circ(ab) = k$.

Now, $(ab)^{mn} = a^{mn}\, b^{mn} = (a^m)^n\, (b^n)^m = e^n\, e^m = ee = e$.

$\therefore k \mid mn$.

Again, $(ab)^k = e \Rightarrow a^k\, b^k = e$

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

$\Rightarrow \circ(a^k) = \circ[(b^k)^{-1}] = \circ(b^k)$.

Now, $\circ(a^k) \mid \circ(a)$ and $\circ(b^k) \mid \circ(b)$

So, $\circ(a^k) \mid m$ and $\circ(a^k) \mid n$.

But, $\circ(a^k) = \circ(b^k)$.

So, $\circ(a^k) \mid$ (H.C.F. of m and n) *i.e.* $\circ(a^k) = 1$.

Thus, $\circ(a^k) = \circ(b^k) = 1$.

$\therefore \quad a^k = e \quad$ and $\quad b^k = e$

But, $\circ(a) = m,\ a^k = e \Rightarrow m \mid k$
and, $\circ(b) = n,\ b^k = e \Rightarrow n \mid k$ $\}$ $\Rightarrow \quad mn \mid k.$

Now, $mn \mid k \quad$ and $\quad k \mid mn \quad \Rightarrow \quad k = mn.$

Hence, $\circ(ab) = mn.$

Ex. 9: Show that the composition table for a finite group contains each element once and only once in each of its rows and columns.

Solution: Let G be a finite group and let, if possible, an element $x \in G$ be repeated twice in a single row.

Then, an element $a \in G$ operated with distinct elements b and c of G, gives x in each case, *i.e.* $ab = x$ and $ac = x$.

Consequently, $ab = ac$ and therefore, by cancellation law, $b = c$.

This is a contradiction.

So, each row of the table contains each element once and only once.

Similarly, each column of the table contains each element once and only once.

Ex. 10: Show that every group consisting of four or less than four elements is always abelian.

Solution: Let G be a group consisting 4 or less than 4 elements. Then,

Case I. Let $G = \{e\}$, where e is the identity element.

In this case, G is clearly abelian.

Case II. Let $G = \{e, a\}$, where $a \neq e$.

In this case, $ae = ea = a$ and so, G is abelian.

Case III. Let $G = \{e, a, b\}$, where $a \neq b \neq e$.

In this case, we prepare the composition table, given below.

Since, in any row of the composition table of a group, each element occurs only once,

So $a^2 = e$ or $ab = e$ and $ba = e$ or $b^2 = e$.

But $a^2 = e \Rightarrow ab = b$ which is not possible as each element in a row and column occurs only once in the table.

So, $a^2 \neq e$ and therefore, $ab = e$.

Similarly, $b^2 \neq e$ and therefore, $ba = e$.

$\therefore$ $ab = ba = e$.

This shows that G is abelian.

•	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	ba	b^2

Case IV. Let $G = \{e, a, b, c\}$, where, $a \neq b \neq c \neq e$.

In this case, the composition table may be prepared, as given below.

Since, each element in a row occurs only once in the table, so

$ab = e$ or $ab = c$.

Similarly, $ba = e$ or $ba = c$.

Let's consider , ab=e

Since ,each element in a row and column occurs only once in the table.

So, cb=a. Hence, b^2=c. It follows that $ba = e$ as there is no other option for ba. Therefore, ab=e=ba. i.e. , $ab = ba$.

Again, suppose that $ab = c$, then either a^2=e or a^2=b. If a^2=e,

then ba≠e as a^2 and ba belong to the same column, hence ba=c. So, $ab = c = ba$, i.e., $ab = ba$. Hence, G is abelian.

•	e	a	b	c
e	e	a	b	c
a	a	a^2	ab	ac
b	b	ba	b^2	bc
c	c	ca	cb	c^2

****

CYCLIC GROUPS

Cyclic group:

A group is said to be cyclic if it is capable of being generated by a single element i.e., every element of the group can be expressed by a single element. The single element is called the generator of the group. If a cyclic group is generated by an element a, then we can write $G = \{a\}$.

A group $(G,\times)$ is said to be a cyclic group, if there exists an element $a \in G$, such that every element of G is expressible as some integral power of a i.e., every element $x \in G$ can be expressed as $x = a^n$, where $n \in \mathbb{Z}$. Thus, every element of G will be of the form $\ldots\ldots\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 (= e), a^1, a^2, a^3, \ldots\ldots\ldots$

A group $(G,+)$ is said to be cyclic if every $x \in G$ is expressible as $x = na$ for some integer n. The element of $(G,+)$ will be of the form $\ldots\ldots\ldots, -3a, -2a, -a, 0.a\ (= 0), a, 2a, 3a, \ldots\ldots\ldots$

A cyclic group is also known as a **monogenic group.**

Examples:

i) The multiplicative group $\{1, \omega, \omega^2\}$ of cube roots of unity is a cyclic group, generated by ω, since

$$1 = \omega^3, \ \omega = \omega^1 \text{ and } \omega^2 = \omega^2.$$

More-over, $1 = (\omega^2)^3$, $\omega = (\omega^2)^2$ and $\omega^2 = (\omega^2)^1$

i.e. each element of the group is expressible as some integral power of ω^2.

So, ω^2 is also a generator of the group.

ii) The group $(\{0, 1, 2, 3\}, +_4)$ is a cyclic group generated by 1, Since

$$1 +_4 1 = 2, \quad 1 +_4 1 +_4 1 = 3, \quad 1 +_4 1 +_4 1 +_4 1 = 0.$$

iii) The additive group of integers, $(\mathbb{Z},+)$ is a cyclic group whose generators are 1 and -1.

Non-Examples:

i) $(\mathbb{R}_0,\times)$ is not a cyclic group.

ii) Every non abelian group is non cyclic.

iii) The Klein four-group, with four elements, is the smallest group that is not a cyclic group such as the set of four matrices, $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ forms an abelian group under multiplication of matrices but it's not cyclic.

Some results on cyclic groups:

Theorem 1. Every cyclic group is necessarily abelian.

Proof. Let $G = \{a\}$ be a cyclic group generated by an element a. Let x and y be any two arbitrary elements of G, then

$x = a^m$ and $y = a^n$, for some integers m and n.

$\therefore \quad xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx.$

Thus, $xy = yx; \forall \quad x, y \in G.$

Hence, G is an abelian group.

Remark. An abelian group is not always a cyclic group.

For example, the multiplicative group $\mathbb{R}_0$ of non-zero real numbers is clearly an abelian group. Now, if $x \in \mathbb{R}_0$, then $\{x^n : n \in \mathbb{Z}\}$ is a countable subset of $\mathbb{R}_0$ and so it cannot be equal to the uncountable set $\mathbb{R}_0$ *i.e.* all elements of $\mathbb{R}_0$ cannot be expressed as some integral power of a single element of $\mathbb{R}_0$.

So, $(\mathbb{R}_0, \bullet)$ is not a cyclic group.

Theorem 2. If an element a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof. Let $G = \{a\}$ be a cyclic group generated by an element a. Then, each element of G is of the form a^n for some integer n.

Now, we may write, $a^n = a^{-1(-n)} = (a^{-1})^{-n}$.

Thus, every element of G can be expressed as some integral power of a^{-1}.

Theorem 3. The order of a cyclic group is the same as the order of its generator.

Proof. Let $G = \{a\}$ be a cyclic group generated by a. Then

Case I. *When* $\circ(a)$ *is finite.*

Let $\circ(a) = n$, a finite positive integer. Then, $a^n = e = a^0$.

Now, by closure property $a, a^2, a^3, \ldots\ldots\ldots a^n = e$ are elements of G. We show that these elements are distinct and these are only elements of G.

Suppose that for two integers i and j such that $1 \leq j < i \leq n$, we have $a^i = a^j$.

Then, $a^i = a^j \Rightarrow a^i (a^j)^{-1} = e \Rightarrow a^i a^{-j} = e \Rightarrow a^{i-j} = e$.

Clearly, $0 < i - j < n$

So, it shows that $\circ(a) < n$, which is a contradiction.

Thus, $a, a^2, a^3, \ldots\ldots\ldots a^n = e$ are all distinct.

Now, we show that every integral power of a equals some one of these elements.

Consider $a^m \in G$, where m is any integer.

By division algorithm, we have $m = nq+r$, where $0 \leq r < n$

$\therefore \quad a^m = a^{nq+r} = (a^n)^q a^r = ea^r = a^r$, where $0 \leq r < n$.

But a^r is one of $a, a^2, a^3, \ldots\ldots\ldots, a^{n-1}, a^n = e = a^0$.

Thus, every integral power of a is one of $a^0, a^1, a^2, \ldots\ldots\ldots, a^{n-1}$.

Hence G contains n distinct elements $a^0, a^1, a^2, \ldots\ldots\ldots, a^{n-1}$.

i.e. $\circ(G) = n = \circ(a)$.

Case II. When $\circ$(a) is infinite.

In this case, distinct integral powers of a shall give distinct elements of G. For,

if $a^m = a^n$ and $m > n$, then we get $a^{m-n} = e$,

which implies that $\circ(a)$ is finite, a contradiction.

Thus, G will be infinite in this case.

Hence, the order of a cyclic group is the same as the order of its generator.

Problem-1: Show that there exist only two generators of an infinite cyclic group.

Solution: If a is a generator of an infinite cyclic group, then a^{-1} is also a generator. Now, if a^k is any other generator, then $a = (a^k)^m$ for some integer m. But, $a = a^{km} \Rightarrow e = a^{km-1}$. It follows that $k = m = 1$ or $k = m = -1$ as a is of infinite order. Therefore, an infinite cyclic group has two generators only.

Theorem 4. A finite group of order n containing an element of order n must be cyclic.

Proof. Let G be a finite group of order n. Let $a \in G$ such that $\circ(a) = n$.

Let $H = \{a\}$ be a cyclic group generated by a.

Then, clearly $H = \{a, a^2, a^3, \ldots \ldots \ldots a^n = e\}$.

More-over, $a \in G$ and therefore, by closure property, every integral power of a is in G.

Consequently, $H \subseteq G$.

Now, $H \subseteq G$ and $\circ(H) = \circ(G)$, so $H = G$.

But, H being cyclic, so is therefore G.

Theorem 5. If G = {a} be a cyclic group generated by a and $\circ(a) = n$, then for some integer m < n. a^m is a generator $\Leftrightarrow$ m is relatively prime to n.

Proof. Let m be an integer less than n and relatively prime to n. Then, the H.C.F. of m and n is 1. So, $\exists$ integers p and q such that, $mp + nq = 1$.

Let $H = \{a^m\}$ be a cyclic group generated by a^m.

Then, each element of H is some integral power of a^m and therefore of a. So, each element of H is in G.

i.e. $H \subseteq G$.

Now, $a = a^1 = a^{mp+nq} = (a^m)^p (a^n)^q = (a^m)^p$ $[\because a^n = e]$

Thus, each integral power of a is some integral power of a^m.

So, $G \subseteq H$.

Thus, $G = H$.

But, H being the cyclic group generated by a^m, so G is also a cyclic group generated by a^m.

Conversely, let a^m be also a generator of the cyclic group G generated by a, where $\circ(a) = n$ and $m < n$.

Now, each element of G is some integral power of a^m.

In particular, $a = (a^m)^r$, for some integer r.

But, $(a^m)^r = a \Rightarrow a^{mr} = a \Rightarrow a^{mr+ns} = a = a^1$ $[\because a^{ns} = (a^n)^s = e]$

This gives, $mr + ns = 1$, showing that m and n are relatively prime.

Problem: How many generators does a cyclic group of order n have?

Solution: Let G be a cyclic group generated by an element a of order n, then those a^m is a generator of G for which m and n are relatively primes.

If n is a prime number, then the group, G will have $(n-1)$ different generators but when n is a composite number, say $n = 8$, then the number of generators for G, is 4. Similarly, The number of generators of G, for $n = 4, 6, 10$ are $2, 2$ and 4 respectively.

Ex. 1. Find the number of generators of a cyclic group of order 10.

Sol. Let $G = \{a\}$ be a cyclic group of order 10, generated by an element a.

Then, $\circ(a) = \circ(G) = 10$.

$\therefore$ $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10} = e\}$.

Now, a^m is a generator of G, if $m < 10$ and the H.C.F. of m and 10 is 1.

Now, the numbers less than 10 and relatively prime to 10 are 1, 3, 7, 9.

So, a, a^3, a^7, a^9 are generators of G.

Hence, G has four generators.

Ex. 2. Give an example of a finite abelian group, which is not cyclic.

Hints. Consider the multiplicative group G of four matrices

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},\ A_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ A_4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It is easy to verify that G is an abelian group in which

$\circ(A_1) = 1, \quad \circ(A_2) = 2, \quad \circ(A_3) = 2, \quad \circ(A_4) = 2.$

Thus, G is a finite group of order 4 in which no element is of order 4.

So, G is not cyclic.

Ex. 3. Show that the multiplicative group of residue classes $\{[1], [3], [5], [7]\}$ modulo 8 is not cyclic.

Solution: Here, $o([3]) = 2, o([5]) = 2, o([7]) = 2$ and $o([1]) = 1$, so the given group is of order 4 but it has no element of order 4. Therefore, the given group is not cyclic.

Homework:

1. Show that the group $(G, \times_7)$ is cyclic, where $G = \{1, 2, 3, 4, 5, 6\}$. How many generators are there?
2. How many elements of a cyclic group of order 7 can be used as generators of the same.
3. Prove that the group, $[\{1, -1, i, -i\}, \times]$ is cyclic.
4. Show that the group, $[\{1, 2, 3, 4\}, \times_5]$ is a cyclic group.
5. Show that the group $[\{0, 1, 2, 3, \ldots \ldots \ldots, (n-1)\}, +_n]$ is cyclic.
6. Identify whether or not the following groups are cyclic or non cyclic:
   i) The group of non zero residue classes under multiplication modulo 5.
   ii) The group of integers $\{1, 5, 7, 11\}$ under multiplication modulo 12.
7. Give an example of a group which is
   i) Finite and cyclic
   ii) Finite and non cyclic
   iii) Infinite and cyclic
   iv) Infinite and non cyclic
   v) Abelian(finite or infinite) and non cyclic

****

PERMUTATIONS

Disclaimer: These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.

Introduction: A one-one mapping of a set S onto itself is called a *transformation*. However, we are interested in transformations on finite sets, known as permutations. In this chapter, propose to study the groups of permutations.

Permutation: A one-one mapping of a given finite non-empty set S of n distinct elements onto itself, is called a permutation of degree n. We denote a permutation f on S in a two-rowed notation

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots\ldots\ldots & a_n \\ b_1 & b_2 & b_3 & \ldots\ldots\ldots & b_n \end{pmatrix},$$

where, in the first row, all the elements of S are written in a certain order and $f(a_i)=b_i$ is put under a_i for each i. Clearly, each b_i is also a member of S.

Remark. It is immaterial in which order, the elements of S are put in the first row, but image of a_i must be put under a_i.

Examples:

i) Let $S = \{a, b, c, d\}$ and let f be a permutation on S, defined by $f(a) = b$, $f(b) = d$, $f(c) = a$, $f(d) = c$. Then, we write $f = \begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$.

Remark. If S is a finite set containing n elements, then the set S_n of all permutations on S, is called a symmetric set. Clearly, S_n contains $n!$ elements.

ii) Let $S = \{a, b, c\}$. Then, the symmetric set S_3 of all permutations of degree 3 on S contains 3! = 6 elements, given below :-

$$f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, f_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, f_3 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix},$$

$$f_4 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, f_5 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, f_6 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}.$$

Composite of Permutations: Let f and g be two permutations defined on a finite set S. Then, by definition, f as well as g is a one-one mapping of S onto itself. Consequently, the composite mappings $g \circ f$ and $f \circ g$ defined by

$$(g \circ f)(x) = g[f(x)] \quad \forall \ x \in S \quad \text{and} \quad (f \circ g)(x) = f[g(x)] \quad \forall \ x \in S$$

are both one-one mappings of S onto itself.

So, whenever f and g are permutations of degree n, then so are $g \circ f$ and $f \circ g$.

Example:

Let $f = \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix}$ and $g = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$.

Then, $(g \circ f)(a) = g[f(a)] = g(c) = d$;

$(g \circ f)(b) = g[f(b)] = g(a) = b$;

$(g \circ f)(c) = g[f(c)] = g(d) = a$; and

$(g \circ f)(d) = g[f(d)] = g(b) = c$.

$\therefore \quad g \circ f = \begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}$. Similarly, $f \circ g = \begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix}$.

An easy method (Composite of Permutations): To obtain $g \circ f$, we write down the rows of f, as they are. Now under each element of this second row, we put down the image under g, of this element. Then, the third row put under the first row gives $g \circ f$.

Example:

Consider f and g as defined above. Then,

$$g \circ f = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ d & b & a & c \end{pmatrix}.$$

$$\begin{matrix} a & b & c & d \\ \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ c & a & d & b \\ \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ d & b & a & c \end{matrix}$$

Remark. To obtain $f \circ g$, we write down the rows of g, as they are. Now under each element of this second row, we put down the image under f, of this element. Then, the third row put under the first row gives $f \circ g$.

$$f \circ g = \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix}.$$

$$\begin{matrix} a & b & c & d \\ \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ b & c & d & a \\ \Downarrow & \Downarrow & \Downarrow & \Downarrow \\ a & d & b & c \end{matrix}$$

Theorem-1: Let S be a finite set containing n distinct elements. Then, the symmetric set of all permutations of degree n on S, form a finite group of order n! with respect to composite of permutation as the composition.

Proof: Let $S = \{a_1, a_2, \ldots\ldots\ldots, a_n\}$. Then, the composite composition on S_n satisfies the following axioms :-

(i) **Closure property**: Let $f \in S_n$ and $g \in S_n$. Then, f as well as g is a one-one mapping of S onto itself, and therefore, so is $g \circ f$. Consequently, $g \circ f$ is a permutation of degree n, on S. Thus, $f \in S_n,\ g \in S_n \Rightarrow g \circ f \in S_n \quad \forall\ f, g \in S_n$.

(ii) **Associative law**: Since, the composite composition on mappings is associative, so it is associative in case of permutations also.

(iii) **Existence of Identity**: The identity permutation $I = \begin{pmatrix} a_1 & a_2 & \ldots\ldots\ldots & a_n \\ a_1 & a_2 & \ldots\ldots\ldots & a_n \end{pmatrix}$ in S_n, is the identity for composite composition on S_n,

for, if $f = \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots & b_n \end{pmatrix}$, then

$$f \circ I = \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots & b_n \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ a_1 & a_2 & \ldots\ldots & a_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots & b_n \end{pmatrix} = f.$$

Thus, $f \circ I = f$ and similarly, $I \circ f = f$.

(iv) **Existence of inverse**: Corresponding to each permutation $f = \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots & b_n \end{pmatrix} \in S_n$, the permutation, $f^{-1} = \begin{pmatrix} b_1 & b_2 & \ldots\ldots & b_n \\ a_1 & a_2 & \ldots\ldots & a_n \end{pmatrix} \in S_n$ is the inverse of f, since

$$f \circ f^{-1} = \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ b_1 & b_2 & \ldots\ldots & b_n \end{pmatrix} \circ \begin{pmatrix} b_1 & b_2 & \ldots\ldots & b_n \\ a_1 & a_2 & \ldots\ldots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \ldots\ldots & b_n \\ b_1 & b_2 & \ldots\ldots & b_n \end{pmatrix} = I$$ and similarly, $f^{-1} \circ f = I$.

Hence, $(S_n, \circ)$ is a finite group of order $n!$.

Cyclic permutation: Let S be a finite set containing n elements. Then, a permutation f on S is said to be a cyclic permutation of length k, or simply a $k-$cycle, if $(n-k)$ elements of S remain invariant and the variant elements are capable of being expressed in one row, in such a way that the image of each element in this row is the element following it and the image of the last element in the row is the first element with which we started.

Examples: The permutation, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 5 & 6 \end{pmatrix}$ is a cyclic permutation of length 4, denoted by $f = (1\ \ 2\ \ 4\ \ 3)$.

However, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$ is not cyclic, since the elements of g cannot be expressed in the requisite form of one row notation.

Remarks.

(i) Clearly, a cycle of length 1 is the identity permutation.
(ii) A cycle of length 2 is called a transposition.

For example: $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (2, 3)$ is a transposition.

(iii) The inverse of a cyclic permutation is obtained by writing the elements of the row of the cycle in a reverse order. Thus, if $f = (1\ \ 3\ \ 5\ \ 4)$, then $f^{-1} = (4\ \ 5\ \ 3\ \ 1)$.
(iv) Two cycles are said to be disjoint, if when expressed in one-row notation, they have no element in common.

Some results on composite of permutations:

Theorem-1: The product of disjoint cycles is commutative.

Proof: Let f and g be any two disjoint cycles, defined on a given finite set. Then, f and g, when expressed in one-row notation have no common element.

So, the elements permuted by f are left unchanged by g and those permuted by g remain invariant under f.

Consequently, $f \circ g = g \circ f$.

Ex. Let $f = (1\ \ 2\ \ 5)$ and $g = (3\ \ 4\ \ 6)$ be two disjoint cycles, defined on six symbols 1, 2, 3, 4, 5, 6.

Then, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 4 & 1 & 6 \end{pmatrix}$ & $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{pmatrix}$.

$\therefore\ g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 4 & 1 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix}$; and

$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 4 & 1 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix}$.

$\therefore\ g \circ f = f \circ g$.

Theorem-2: Every permutation can be expressed as a composite of disjoint cycles.

Proof: Let f be a given permutation of degree n, defined on S. First we take up all the cycles of length one, each determined by the invariant element.

Then, we take an element, which is non-invariant and construct a row starting with the same and putting after each element its image under f.

Since, the number of elements in S is finite, after a finite number of steps, we arrive at an element whose image under f is the one with which we started.

This row represents a cycle.

Now, if all the elements of S have not been contained in the cycles, so far obtained, then we start with one such element and obtain another cycle in the above manner.

Continuing in this way, each and every element of S will be included in one or the other cycle.

Clearly, these cycles have no element in common and So they are disjoint.

Thus, f can be expressed as a composite of disjoint cycles.

Ex. Express the permutation , f $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix}$ as a Composite of disjoint cycles. Also, verify the answer.

Solution: We may write

$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix} = (1) \circ (2\ \ 6) \circ (3\ \ 5\ \ 4)$.

Verification: $(1) \circ (2\ \ 6) \circ (3\ \ 5\ \ 4)$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 3 & 4 & 6 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix} = f$.

Theorem-3: Every permutation can be expressed as a composite of transpositions.

Proof: By preceding theorem, every permutation can be expressed as composite of disjoint cycles.

Now, it is easy to verify that

$(a_1 \quad a_2 \ldots\ldots\ldots \quad a_k) = (a_1 \quad a_k) \circ (a_1 \quad a_{k-1}) \circ \ldots\ldots\ldots \circ (a_1 \quad a_2)$, when $k > 1$ *i.e.* every cycle other than the identity permutation can be expressed as a composite of transpositions.

Also, $\begin{pmatrix} a_1 & a_2 & \ldots\ldots\ldots & a_n \\ a_1 & a_2 & \ldots\ldots\ldots & a_n \end{pmatrix} = (a_1 \quad a_2) \circ (a_2 \quad a_1)$

i.e. the identity permutation can also be expressed as a composite of transpositions.

Thus, every cycle and therefore, every permutation can be expressed as the product of transpositions.

Ex. Express the permutation, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix}$ as a product of transpositions.

Solution: $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix} = (1) \circ (2 \quad 6) \circ (3 \quad 5 \quad 4)$

$= (1 \quad 2) \circ (2 \quad 1) \circ (2 \quad 6) \circ (3 \quad 4) \circ (3 \quad 5)$.

[$\because$ $(1) = (1 \quad 2) \circ (2 \quad 1)$ and $(3 \quad 5 \quad 4) = (3 \quad 4) \circ (3 \quad 5)$]

Even and odd Permutations: A permutation is said to be even or odd according as it is expressible as the product of an even or an odd number of transpositions.

Examples:

i) The permutation, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 3 & 4 & 2 \end{pmatrix}$ is an odd permutation.

ii) The permutation, $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 5 & 3 \end{pmatrix}$ is an even permutation.

Some results on even and odd Permutations:

Theorem-5: A cycle of length n is an even or an odd permutation according as n is odd or even.

Proof: Let $f = (a_1 \quad a_2 \ldots\ldots\ldots \quad a_n)$ be a cycle of length *n*.

Then, $f = (a_1 \quad a_2 \ldots\ldots\ldots \quad a_n) = (a_1 \quad a_n) \circ (a_1 \quad a_{n-1}) \circ \ldots\ldots\ldots \circ (a_1 \quad a_2)$.

i.e. f is expressible as the product of $(n-1)$ transpositions.

Clearly, when *n* is odd, $(n-1)$ is even and so f is even.

And, when *n* is even, $(n-1)$ is odd and so f is odd.

Corollary. Every transposition is always an odd permutation.

Proof: Since a transposition is a cycle of length 2, So by preceding theorem, it is an odd permutation.

Theorem-6: Identity permutation is always an even permutation.

Proof: We have, $I = \begin{pmatrix} a_1 & a_2 & \ldots\ldots & a_n \\ a_1 & a_2 & \ldots\ldots & a_n \end{pmatrix} = (a_1 \quad a_2) \circ (a_2 \quad a_1)$.

i.e. the identity permutation is expressible as the product of two transpositions. Hence, it is an even permutation.

Theorem-7:

(i) The product of two even permutations is an even permutation.
(ii) The product of two odd permutations is an even permutation.
(iii) The product of an even permutation and an odd permutation is an odd permutation.

Proof: (i) Let f and g be two even permutations so that each one is expressible as a product of an even number of transpositions say m and n respectively.

Then, $g \circ f$ is the product of $(m+n)$ transpositions.

But, $(m+n)$ being the sum of two even numbers, it is even.

Hence, $g \circ f$ is an even permutation.

Similarly, (ii) and (iii) may be proved.

Theorem-8:

(i) The inverse of an even permutation is even ;
(ii) The inverse of an odd permutation is odd.

Proof: (i) Let f be even and if possible, f^{-1} be odd.

Then, $f \circ f^{-1} = I$ is odd, which contradicts the fact that identity permutation is always even.

Hence, whenever f is even, then f^{-1} is even.

Similarly, (ii) follows.

Theorem-9: Of the n! permutations on n symbols, n! / 2 are even and n! / 2 are odd.

Proof: Let the symmetric group S_n of all $n!$ permutations of degree n consist of even permutations $f_1, f_2, \ldots\ldots\ldots f_k$ and odd permutations $g_1, g, \ldots\ldots\ldots g_m$ so that $(k+m) = n!$.

Now, let f be any transposition in S_n. Then, f is an odd permutation.

By closure property, $f \circ f_i \in S_n$ for $1 \leq i \leq k$ and

$$f \circ g_j \in S_n \quad \text{for} \quad 1 \leq j \leq m.$$

Since, f is odd and f_i is even, so $f \circ f_i$ is odd, for each i.

Again, f is odd and g_j is odd, so $f \circ g_j$ is even, for each j.

Also, $f \circ f_i = f \circ f_p \Rightarrow f_i = f_p$ (by cancellation law)

and $f \circ g_j = f \circ g_l \Rightarrow g_j = g_l$ (by cancellation law)

Thus, $f \circ f_1$, $f \circ f_2$, $\ldots\ldots\ldots$, $f \circ f_k$ are k distinct odd permutations and,

$f \circ g_1$, $f \circ g_2$, $\ldots\ldots\ldots$, $f \circ g_m$ are m distinct even permutations.

This shows that S_n contains k odd permutations and m even permutations.

But, a permutation cannot be both even and odd.

$\therefore \quad m = k = \frac{n!}{2}$.

Hence, S_n contains $(\frac{n!}{2})$ even permutations and $(\frac{n!}{2})$ odd permutations.

Theorem-10 (Alternating Group):The set A_n of all even permutations of degree n, defined on a set S, forms a finite group of order $(\frac{n!}{2})$ with respect to composite composition.

Proof: It has already been shown that the composite of two even permutations is even, the identity permutation is even, and the inverse of an even permutation is even.

We also know that the composite composition on permutations is associative, so it is associative on A_n.

More-over, out of $n!$ permutations in S_n, $\frac{n!}{2}$ are even.

Hence, $(A_n , \circ)$ is a group of order $\frac{n!}{2}$.

Some Illustrative Examples:

Ex.1. Show that the four permutations I, (ab), (cd), $(ab) \circ (cd)$ on four symbols a, b, c, d form a finite abelian group with respect to the composite composition.

Solution: Let $f_1 = I = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$, $f_2 = (ab) = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$,

$f_3 = (cd) = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}$ and

$f_4 = (ab) \circ (cd) = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$.

Let $G = \{f_1, f_2, f_3, f_4\}$.

By computing the various products, we get the table, given below :

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Clearly, all the entries in the table are members of G, f_1 is the identity and

$f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$ and $f_4^{-1} = f_4$.

Also, composite composition on G is associative.

More-over, each row of the table coincides with the corresponding column.

Hence, $(G, \circ)$ is an abelian group.

Ex.2. In the symmetric group S_4 of all permutations of degree 4, find which permutations are even.

Solution: It is clear that S_4 contains 4! *i.e.* 24 permutations.

Let $S = \{a, b, c, d\}$. Then,

$S_4 = \{ I, (ab), (ac), (ad), (bc), (bd), (cd), (abc), (acb), (abd), (adb), (acd), (adc), (bcd), (bdc), (ab) \circ (cd), (bc) \circ (ad), (ca) \circ (bd), (abcd), (abdc), (acbd), (acdb), (adbc), (adcb) \}$

Now, we know that identity permutation, I is even.

Also, each cycle of length 3 being expressible as the product of 2 transpositions, is even.

Also, the composite of two transpositions gives even permutation.

Again, every transposition is an odd permutation and each cycle of length 4 being expressible as the product of 3 transpositions, is odd.

So, the set of even permutations in S_4 is given by,

A_4 = { I, (abc) , (acb) , (abd) , (adb) , (acd) , (bcd) , (bdc) , (adc) , $(ab) \circ (cd)$,

$(bc) \circ (ad)$, $(ca) \circ (bd)$ }.

Ex.3. Prove that every even permutation of degree n ($n \geq 3$) can be expressed as the product of cycles, each of length 3.

Solution: Let f be an even permutation of degree n, where $n \geq 3$. Let it be expressible as the product of r transpositions. Then, r is even. We can divide r into $(r/2)$ pairs. Now,

Case. **I**: When a pair of transpositions has no common element.

In this case, the product of these two transpositions may be expressed as the product of two cycles, each of length 3.

For example, $(ab) \circ (cd) = (ab) \circ (ac) \circ (ca) \circ (cd) = (acb) \circ (cda)$.

Case. **II**.When a pair of transpositions has some common element.

In this case, also the product of two transpositions may be expressed as a cycle of length 3.

For example, $(ab) \circ (ac) = (acb)$.

Thus, in both cases, the permutation f can be expressed as a composite of $(r/2)$ cycles, each of length 3.

Exercise

1. If $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$, then compute (i) $g \circ f$ (ii) $f \circ g$ (iii) $f^{-1} \circ g^{-1}$ (iv) $g^{-1} \circ f^{-1}$.

2. Show that the set S_3 of all permutations of degree 3, defined on three symbols a, b, c is a finite non-abelian group of order 6 with respect to composite composition.

3. Express the following permutations each defined on five symbols 1, 2, 3, 4, 5 as the product of disjoint cycles :

(i) $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$

(ii) $I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$;

(iii) $g = (1\ \ 3\ \ 2\ \ 5) \circ (1\ \ 4\ \ 3) \circ (2\ \ 5\ \ 1)$;

(iv) $h = (1\ \ 4\ \ 3\ \ 2) \circ (2\ \ 4\ \ 1) \circ (1\ \ 3\ \ 5)$.

4. Express each of the following permutations, defined on five symbols 1, 2, 3, 4, 5 as the product of transpositions :

(i) $f = (2\ \ 3\ \ 4\ \ 5)$;

(ii) $g = (1)$;

(iii) $h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$;

(iv) $k = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$;

(v) $\circ = (4\ \ 5) \circ (1\ \ 2\ \ 3)$.

5. Show that the eight permutations I, $(abcd)$, $(ac) \circ (bd)$, $(adcb)$, $(ab) \circ (cd)$, $(bc) \circ (ad)$, $(bd) \circ (ac)$ on four symbols a, b, c, d form a finite non-abelian group with respect composite composition.

6. Prove that the set $A_3{}'$ of all even permutations (a) , (abc) , (acb) on three symbols a, b, c is a finite abelian group with respect to composite composition.

7. Determine, which of the following permutations are even ;

(i) $f = (1\ \ 2\ \ 3) \circ (1\ \ 2)$;

(ii) $g = (1\ \ 2\ \ 3\ \ 4\ \ 5) \circ (1\ \ 2\ \ 3) \circ (4\ \ 5)$;

(iii) $h = (1\ \ 2) \circ (1\ \ 3) \circ (1\ \ 4) \circ (2\ \ 5)$;

(iv) $\circ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 9 & 8 \end{pmatrix}$.

****

Homomorphisms and Isomprphisms of Groups

Homomorphism: Let $(G,\circ)$ and $(G', *)$ be two groups. Then, a mapping f from G to G' is called a homomorphism, if f is **composition preserving**, i.e.

$$f\ (a \circ b) = f\ (a) * f\ (b) \quad \forall\ a, b \in G.$$

Examples:

i) Let G be a multiplicative group and f be a mapping, $f: G \to G$ defined by $f(x) = x; x \in G$, then f is a homomorphism of G onto itself.

ii) Let $\emptyset: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ such that $\emptyset(x) = 5x;\ \forall x \in \mathbb{Z}$, then $\emptyset$ is a homomorphism of $\mathbb{Z}$ onto itself.

iii) Let $\mathbb{Z}$ be the group of integers under addition and H be the multiplicative group whose elements are 1 and -1, then the mapping $f: (\mathbb{Z},\ +) \to (H,\ \times)$ defined by
$f(x) = \begin{cases} 1; if\ x\ is\ even \\ -1; if\ x\ is\ odd \end{cases}$
is a homomorphism of $\mathbb{Z}$ onto H.

Non Examples:

i) Let $f: (\mathbb{Z},\ +) \to (\mathbb{R}_0,\ \times)$ be a mapping defined by $f(x) = x^2$, then for $1, 2 \in \mathbb{Z}$, $f(1) = 1, f(2) = 4$ and $f(3) = 9$
However, $f(1+2) = f(3) = 9$ and $f(1) \times f(2) = 4$ i.e. $f(1+2) \neq f(1) \times f(2)$.
Thus, f is not a homomorphism of $\mathbb{Z}$ onto $\mathbb{R}_0$.

ii) Let $f: (G,\ +) \to (\mathbb{R}, +)$ be a mapping, where G is a group of matrices such that $f(A) = \det(A)$ for $A \in G$. Consider $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 6 \\ 2 & 5 \end{pmatrix}$,
then $A + B = \begin{pmatrix} 4 & 8 \\ 5 & 9 \end{pmatrix}$
Now, $f(A) = |A| = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 4 - 6 = -2$
$f(B) = |B| = \begin{vmatrix} 3 & 6 \\ 2 & 5 \end{vmatrix} = 15 - 12 = 3$
$f(A+B) = |A+B| = \begin{vmatrix} 4 & 8 \\ 5 & 9 \end{vmatrix} = 36 - 40 = -4$
Here, clearly, $f(A+B) \neq f(A) + f(B)$which implies f is not a homomorphism of G onto $\mathbb{R}$.

Isomorphism: Let $(G,\circ)$ and $(G', *)$ be two groups. Then, a one-one onto, composition preserving mapping f from G to G', is called an **isomorphism**.

In this case, we say that $(G,\circ)$ is isomorphic to $(G', *)$ and we write,

$$(G,\circ) \cong (G', *).$$

Examples:

i) The additive group $(\mathbb{Z}, +)$ of integers is isomorphic to the additive group $(G = \{ma : a \in \mathbb{Z}\}, +)$.

ii) The additive group $(\mathbb{R}, +)$ of all real numbers and the multiplicative group $(\mathbb{R}^+, \times)$ of all positive real numbers, are isomorphic.

Non Examples:

i) Let $f: (\mathbb{Z}, +) \to (\mathbb{R}_0, \times)$ be a mapping defined by $f(x) = x^2$, then for $1, 2 \in \mathbb{Z}$, $f(1) = 1, f(2) = 4$ and $f(3) = 9$
However, $f(1+2) = f(3) = 9$ and $f(1) \times f(2) = 4$ i.e. $f(1+2) \neq f(1) \times f(2)$.
Thus, f is not an isomorphism of $\mathbb{Z}$ onto $\mathbb{R}_0$.

ii) Let $f: (G, +) \to (\mathbb{R}, +)$ be a mapping, where G is a group of matrices such that $f(A) = \det(A)$ for $A \in G$. Consider $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 6 \\ 2 & 5 \end{pmatrix}$,
then $A + B = \begin{pmatrix} 4 & 8 \\ 5 & 9 \end{pmatrix}$
Now, $f(A) = |A| = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 4 - 6 = -2$

$$f(B) = |B| = \begin{vmatrix} 3 & 6 \\ 2 & 5 \end{vmatrix} = 15 - 12 = 3$$

$$f(A+B) = |A+B| = \begin{vmatrix} 4 & 8 \\ 5 & 9 \end{vmatrix} = 36 - 40 = -4$$

Here, clearly, $f(A+B) \neq f(A) + f(B)$ which implies f is not a isomorphism of G onto $\mathbb{R}$.

Remarks:

(i) A one-one homomorphism is called a **monomorphism**.
(ii) An onto homomorphism is called an **epimorphism**.
(iii) An isomorphism of a group onto itself is called an **automorphism**.
(iv) A homomorphism of a group into itself is called an **endomorphism**.

Illustrative Examples:

Ex.1. The additive group $(\mathbb{Z}, +)$ of integers is isomorphic to the additive group

$(G = \{ma : a \in \mathbb{Z}\}, +)$.

Proof. Consider the mapping $f: \mathbb{Z} \to G : f(a) = ma \quad \forall\, a \in \mathbb{Z}$.

Now, f is one-one, since $f(a) = f(b) \Rightarrow ma = mb \Rightarrow a = b$.

Also, corresponding to each $ma \in G$, there exists an element $a \in \mathbb{Z}$ such that

$f(a) = ma$. So, f is onto.

More-over, $\forall\ a, b \in \mathbb{Z}$, we have

$f\ (a+b) = m\ (a+b) = ma + mb = f\ (a) + f\ (b)$.

This shows that f is composition preserving.

Hence, f is an isomorphism, *i.e.* $(\mathbb{Z}, +) \cong (G, +)$.

Ex-2: Let $\mathbb{Z}$ be the group of integers under addition and H be the multiplicative group whose elements are 1 and -1, then the mapping $f: (\mathbb{Z},\ +) \to (H,\ \times)$ defined by

$$f(x) = \begin{cases} 1; if\ x\ is\ even \\ -1; if\ x\ is\ odd \end{cases}$$

is a homomorphism of $\mathbb{Z}$ onto H.

Proof: We have $f(x) = 1$ or -1 according as f is even or odd integer. Our work is to show that $f(ab) = f(a)f(b);\ \forall a, b \in \mathbb{Z}$.

Sum of two integers is even when both of them are even integers or odd integers, otherwise the sum will be odd.

There are four cases arise here, as follows:

i) If a, b are both even, the $f(a+b) = 1 = 1.1 = f(a)f(b)$
ii) If a, b are both odd, the $f(a+b) = 1 = (-1).(-1) = f(a)f(b)$
iii) If a is even and b is odd, then $f(a+b) = -1 = (+1).(-1) = f(a)f(b)$
iv) If a is odd and b is even, then $f(a+b) = -1 = (-1).(+1) = f(a)f(b)$
In every case, $f(a+b) = f(a)f(b)$.

Therefore, f is a homomorphism, here but f is not isomorphism as it is not a ono-one mapping.

Some Results on Isomorphism:

Theorem-1: Let $\emptyset: G \to H$ be an isomorphism of two groups. Then the following statements are true.

i) $\emptyset^{-1}: H \to G$ is an isomorphism
ii) $|G| = |H|$
iii) If G is abelian, then H is abelian
iv) If G is cyclic, then H is cyclic
v) If G has a subgroup of order n, then H has a subgroup of order n.

Theorem -2. Let G and G' be two isomorphic groups whose compositions have been denoted multiplicatively and let f be the corresponding isomorphism. Then,

(i) if e is the identity in G, then f (e) is identity in G';
(ii) $f\ (a^{-1}) = [f\ (a)]^{-1} \quad \forall\ a \in G$;
(iii) $\circ\ (a) = \circ\ [f\ (a)] \quad \forall\ a \in G$.

Proof.

(i) Let a' be an arbitrary element of G'. Then, f being one-one onto $\exists$ a unique element $a \in G$, such that $f(a) = a'$.

Now, $ae = ea = a$

$\Rightarrow f(ae) = f(ea) = f(a)$

$\Rightarrow f(a)\, f(e) = f(e)\, f(a) = f(a)$ [by composition preserving property]

$\Rightarrow a'\, f(e) = f(e)\, a' = a' \quad \forall\ a' \in G'$.

This shows that $f(e)$ is the identity in G'.

(ii) $a\, a^{-1} = a^{-1}\, a = e$

$\Rightarrow f(a\, a^{-1}) = f(a^{-1}\, a) = f(e)$ [where $f(e)$ is identity in G']

$\Rightarrow f(a)\ f(a^{-1}) = f(a^{-1})\ f(a) = f(e)$ [by composition preserving property]

$\Rightarrow [f(a)]^{-1} = f(a^{-1}) \quad \forall\ a \in G.$

(iii) Let $a \in G$ and let $\circ(a) = m$.

Then, m is the least positive integer, such that $a^m = e$.

Now, $a^m = e$

$\Rightarrow f(a^m) = f(e)$

$\Rightarrow f(aaa \ldots\ldots\ldots m \text{ times}) = f(e)$

$\Rightarrow f(a)\ f(a)\ f(a) \ldots\ldots\ldots m \text{ times} = f(e)$ [$\because$ f is composition preserving]

$\Rightarrow [f(a)]^m = f(e)$

$\Rightarrow \circ[f(a)] \leq m.$

Let, if possible, $\circ[f(a)] = k < m.$

Then, $\circ[f(a)] = k$

$\Rightarrow [f(a)]^k = f(e)$

$\Rightarrow f(a)\ f(a)\ f(a) \ldots\ldots\ldots k \text{ times} = f(e)$

$\Rightarrow f(aaa \ldots\ldots\ldots k \text{ times}) = f(e)$ [$\because$ f is composition preserving]

$\Rightarrow \quad f(a^k) = f(e)$

$\Rightarrow \quad a^k = e \qquad [\because \quad f \text{ is one-one}]$

$\Rightarrow \quad \circ(a) \leq k < m, \qquad$ which is a contradiction, since $\circ(a) = m$.

Since, the contradiction arises by assuming that $\circ[f(a)] < m$.

So, $\circ[f(a)] \not< m$.

Hence, $\circ[f(a)] = m = \circ(a)$.

Again, let $\circ(a)$ be infinite and if possible, let $\circ[f(a)]$ be finite, say k.

Then, as proceeded above, $\circ[f(a)] = k \quad \Rightarrow \quad \circ(a) \leq k$, leading us to conclude that $\circ(a)$ is finite.

This contradicts the hypothesis that $\circ(a)$ is infinite.

Thus, whenever, $\circ(a)$ is infinite, then $\circ[f(a)]$ is also infinite.

Hence, $\circ(a) = \circ[f(a)]$.

Theorem-3: (Transference of group structures) Suppose G is a group and $(G', *)$ is an algebraic structure. Also, suppose that there exists one-one map $f: G \to G'$ such that $f(xy) = f(x) * f(y); x, y \in G$, then G' is a group and $G \cong G'$.

Theorem-4: (Cayley's theorem) Every finite group is isomorphic to a permutation group.

Proof: Let $(G, *)$ be a finite group of order n. For each $a \in G$, consider a mapping

$f_a : G \to G : f_a(x) = a * x \qquad \forall \quad x \in G.$

Then, f_a is one-one, since

$f_a(x) = f_a(y) \quad \Rightarrow \quad a * x = a * y \quad \Rightarrow \quad x = y \qquad$ [by left cancellation law].

Now, f_a is a one-one mapping of a finite set into itself, so it is onto.

Thus, f_a is a permutation of degree n, defined on G.

In this way, for each $a \in G$, we can define a permutation f_a on G.

Let, $G' = \{ f_a : a \in G \}$.

We assert that $(G', \circ)$ is a group isomorphic to $(G, *)$.

Define a mapping $\phi : G \to G' : \phi(a) = f_a \qquad \forall \quad a \in G.$

Now, ϕ is one-one, since

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

$\Rightarrow f_a(x) = f_b(x) \quad \forall\ x \in G$

$\Rightarrow a * x = b * x$

$\Rightarrow a = b$ [by right cancellation law].

Now, ϕ being a one-one mapping from G to G' and both of these being finite sets containing same number of elements, so ϕ is onto.

More-over, $\forall\ a, b \in G$, we have $\phi(a * b) = f_{a*b}$.

But, $f_{a*b}(x) = (a * b) * x \quad \forall\ x \in G$

$= a * (b * x)$ [by associativity]

$= f_a(b * x)$

$= f_a[f_b(x)] = (f_a \circ f_b)(x)$.

$\therefore \quad f_{a*b} = f_a \circ f_b$.

Consequently, $\phi(a * b) = f_{a*b} = f_a \circ f_b = \phi(a) \circ \phi(b)$.

Thus, ϕ is one-one mapping from G onto G' and it preserves the composition.

So, by the theorem of **transference of group structure**, it follows that $(G', \circ)$ is a group isomorphic to $(G, *)$.

Thus, for each finite group, we can always find a permutation group, isomorphic to the given group. Hence the theorem follows.

Regular permutation group: The permutation group which is isomorphic to a given finite group is called the regular permutation group of the given group.

Illustrative Examples:

Ex.1. Show that the group $(G = \{0, 1, 2, 3\}, +_4)$ is isomorphic to the group $(G' = \{1, 2, 3, 4\}, \times_5)$.

Solution: The requisite isomorphism will be a mapping f from G to G', defined in such a way that $\circ(a) = \circ[f(a)] \quad \forall\ a \in G$.

It is easy to verify that : in group G,

$\circ(0) = 1, \quad \circ(1) = 4, \quad \circ(2) = 2 \quad \& \quad \circ(3) = 4.$

Also, in group G', $\quad \circ(1) = 1, \quad \circ(2) = 4, \quad \circ(3) = 4 \quad \& \quad \circ(4) = 2.$

Thus, we define $f : G \to G'$ by

$f(0) = 1, \quad f(1) = 2, \quad f(2) = 4$ and $f(3) = 3,$

which is clearly *one-one* and *onto*.

Now, let $a_1 = 0, \quad a_2 = 1, \quad a_3 = 2, \quad a_4 = 3, \quad b_1 = 1, \quad b_2 = 2, \quad b_3 = 4, \quad b_4 = 3.$

Then, $f(a_1) = b_1, \quad f(a_2) = b_2, \quad f(a_3) = b_3$ and $f(a_4) = b_4.$

More-over, the composition tables for G and G' are

$+_4$	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_3	a_4	a_1
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_1	a_2	a_3

$\times_5$	b_1	b_2	b_3	b_4
b_1	b_1	b_2	b_3	b_4
b_2	b_2	b_3	b_4	b_1
b_3	b_3	b_4	b_1	b_2
b_4	b_4	b_1	b_2	b_3

respectively.

Clearly, the above composition tables are identical *i.e.* replacing each a_i in the table for G by b_i, we get the table for G'.

So, $f(a_i +_4 a_j) = b_i \times_5 b_j = f(a_i) \times_5 f(a_i) \quad \forall \quad a_i, a_j \in G.$

This shows that f is composition preserving.

Thus, f is an isomorphism and hence $(G, +_4) \cong (G', \times_5).$

Remark: However, if we define a mapping

$g : G \to G' : \; g(0) = 1, \; g(1) = 3, \; g(2) = 4 \; \& \; g(3) = 2.$

Then, g is also an isomorphism.

Ex.2. Show that the multiplicative group $G = \{1, -1, i, -i\}$ is isomorphic to the permutation group $G' = \{I, (abcd), (ac) \circ (bd), (adcb)\}$ on 4 symbols a, b, c, d.

Solution: It is easy to verify that

$\circ (1) = 1, \quad \circ (-1) = 2, \quad \circ (i) = 4, \quad \circ (-i) = 4$ and

$\circ (I) = 1, \quad \circ (abcd) = 4, \quad \circ [(ac) \circ (bd)] = 2$ and $\circ (adcb) = 4$.

So, consider a mapping $f : G \to G'$, defined by

$f(1) = I, \quad f(-1) = (ac) \circ (bd), \quad f(i) = (abcd) \quad \& \quad f(-i) = (adcb)$.

This mapping is clearly **one-one** and **onto**.

Now, let $A_1 = 1, \quad A_2 = -1, \quad A_3 = i \quad \& \quad A_4 = -i$

and, let $B_1 = I, \quad B_2 = (ac) \circ (bd), \quad B_3 = (abcd) \quad \& \quad B_4 = (adcb)$.

Now, if we prepare the composition tables for G and G', then we shall find that the two composition tables are identical *i.e.* by replacing each A_i in the composition table for G by B_i, we get the composition table for G'.

Consequently, $\forall \; A_i, A_j \in G$, we have

$f(A_i \times A_j) = B_i \circ B_j = f(A_i) \circ f(A_j)$.

This shows that f is composition preserving.

Thus, f is an isomorphism and hence $(G, \times) \cong (G', \circ)$.

Home work:

1. Write a short note on the following:

i) Quotient group
ii) Kernel of homomorphism
iii) Fundamental Theorem of Homomorphism (First law of Isomorphism)
iv) Second law of Isomorphism
v) Third law of Isomorphism

****

Subgroups

Disclaimer: These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.

Complexes and sub-groups

Let G be a group whose composition has been denoted multiplicatively. Let $H \subseteq G$. Then, the composition on G, restricted only on points of H is called an **induced composition**. Also, we say that H is stable for the induced composition, if

$$a \in H,\ b \in H \quad \Rightarrow \quad ab \in H \qquad \forall \quad a, b \quad \in \quad H.$$

Sub-group: A non-empty subset H of a group G is said to be its **sub-group** if H is stable for the composition in G and H itself is a group with respect to the induced composition.

OR

If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

Complex: Any non-empty subset H of a group G, whether a sub-group or not is called a **complex** of G.

Examples:

i) Let $G = \{1, -1, \iota, -\iota\}$ and $H = \{-1, 1\}$.

Then, clearly $(H, \times)$ is a subgroup of $(G, \times)$.

ii) Let E be the set of all even integers and $\mathbb{Z}$ be the set of all integers. Then, $(E, +)$ is a subgroup of $(\mathbb{Z}, +)$.

iii) Let S be a finite set containing n distinct elements. Let the symmetric set of all permutations on S be denoted by S_n and the alternating set of all even permutations on S be denoted by A_n. Then, $(A_n, \circ)$ is a subgroup of $(S_n, \circ)$.

Non examples:

i) Let $H = \{1, \omega, \omega^2\}$ be the set of cube-roots of unity. Then, $(H, \times)$ is a group. Again, if $\mathbb{C}$ denotes the set of all complex numbers. Then, $(\mathbb{C}, +)$ is a group. Though, $H \subseteq \mathbb{C}$, yet $(H, \times)$ is not a sub-group of $(\mathbb{C}, +)$.
Note that the composition must be the same on both the sets.

ii) Let G be the group of nonzero real numbers under multiplication, $H = \{x \in G : x = 1 \text{ or } x \text{ is irrational}\}$ and $K = \{x \in G : x \geq 1\}$. Then H is not a subgroup of G, since $\sqrt{2} \in H$ but $\sqrt{2}.\sqrt{2} = 2 \notin H$. Also, K is not a subgroup, since $2 \in K$ but $2^{-1} \notin K$.

Remark: Every group G has surely two sub-groups namely G and $\{e\}$, where e is the identity element in G. These sub-groups are called **trivial** or **improper sub-groups**. A sub-group, other than trivial ones is called a **proper sub-group**.

Properties of a sub-group

Theorem-1:

(i) The identity of a subgroup is the same as that of the group.
(ii) The inverse of any element of a subgroup is the same as the inverse of the element regarded as a member of the group.
(iii) The order of any element of a subgroup is the same as the order of that element regarded as a member of the group.

Proof: Let H be a subgroup of a group G, whose composition has been denoted multiplicatively. Now,

(i) Let e and e' be the identity elements in G and H respectively.

Let a be an arbitrary element of H. Then, $a \in G$.

Now, $a \in G$ and e is identity element in G $\Rightarrow$ $ae = a$.

Also, $a \in H$ and e' is identity element in H $\Rightarrow$ $ae' = a$.

$\therefore$ $ae = ae'$ and so by cancellation law, $e = e'$.

(ii) Let e be the identity element in H and therefore in G.

Let a be an arbitrary element of H. Then, clearly $a \in G$.

Let b and c be the inverses of a regarded as e member of H and G respectively. Then, $ab = ba = e$ and $ac = ca = e$.

Thus, $ab = ac$ and therefore, by cancellation law, $b = c$.

(iii) Let a be an arbitrary element of H. Then, $a \in G$.

Let m and n be the orders of a regarded as a member of G and H respectively. Then, m and n are the least positive integers such that $a^m = e$ and $a^m = e$. Clearly, such a least positive integer must be unique. Hence $m = n$.

Remark: It is clear that every subgroup of an abelian group is always abelian. However, a non-abelian group may have an abelian subgroup.

For example, $(S_3, \circ)$ is non-abelian and its subgroup , $(A_3, \circ)$ is abelian.

More-over, a non-abelian group may have a non-abelian subgroup.

For example, the non-abelian group $(S_4, \circ)$ has a non-abelian subgroup $(A_4, \circ)$.

Theorem-2 (**Criterion for a complex to be a subgroup**):A necessary and sufficient condition for a complex H of a group G to be a subgroup is that

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

Proof: Let H be a subgroup of a group G. Then, H is a group in its own right. Let a and b be arbitrary elements of H.

Then, $a \in H,\ b \in H$

$\Rightarrow \quad a \in H,\ b^{-1} \in H \qquad [\because\ H$ being a group, $b \in H \ \Rightarrow \ b^{-1} \in H\ ]$

$\Rightarrow \quad ab^{-1} \in H \qquad [$ by closure property in group $H\ ]$

Thus, $a \in H,\ b \in H \quad \Rightarrow \quad ab^{-1} \in H \qquad \forall \quad a, b \in H.$

Conversely, Let H be a complex of a group G, given in such a way that

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

Then, using the given condition, we have

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

$$e \in H,\ a \in H \quad \Rightarrow \quad ea^{-1} \in H \quad \Rightarrow \quad a^{-1} \in H;$$

Thus, the identity element e exists in H and every element in H has its inverse in H.

More-over, $a \in H,\ b \in H \quad \Rightarrow \quad a \in H,\ b^{-1} \in H$

$$\Rightarrow \quad a\,(b^{-1})^{-1} \in H \qquad [\text{by given property}]$$

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

This shows that H is stable for the composition in G.

Also, $H \subseteq G$. So, all elements of H are in G and since the composition is associative for elements of G, it is therefore, associative for elements of H.

Hence H is a subgroup of G.

Remark: If G is an additive group and $H \subseteq G$, then H is a subgroup of G iff

$$a \in H,\ b \in H \quad \Rightarrow \quad (a - b) \in H \qquad \forall \quad a, b \in H.$$

Theorem-3: The intersection of an arbitrary collection of subgroups of a group is again a subgroup of the group.

Proof: Let $\{H_\alpha : \alpha \in \Delta\}$ be an arbitrary collection of subgroups of a group G. Then, the identity element e in G is contained in each H_α. Consequently,

$\cap \{H_\alpha : \alpha \in \Lambda\} \neq \phi$. Let a and b be arbitrary elements of $\cap \{H_\alpha : \alpha \in \Lambda\}$.

Then, $a, b \in \cap \{H_\alpha : \alpha \in \Lambda\}$

$\Rightarrow$ $a, b \in H_\alpha$ for each α

$\Rightarrow$ $ab^{-1} \in H_\alpha$ for each α [$\because$ each H_α is a sub-group]

$\Rightarrow$ $ab^{-1} \in \cap \{H_\alpha : \alpha \in \Lambda\}$.

Hence, $\cap \{H_\alpha : \alpha \in \Lambda\}$ is also a sub-group of G.

Remark: The union of any two subgroups of a group is not necessarily a subgroup of the same. For example, consider the symmetric group S_3 of all permutations of degree 3 defined on three symbols a, b, c.

Let $H_1 = \{I, (ab)\}$ and $H_2 = \{I, (bc)\}$ be any two complexes of S_3. It is easy to verify that H_1 as well as H_2 is a subgroup of S_3.

More-over, $H_1 \cup H_2 = \{ I, (ab), (bc)\}$.

Now, $(ab) \circ (bc) = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \circ \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = (abc)$.

Clearly, $(ab) \in H_1 \cup H_2$, $(bc) \in H_1 \cup H_2$.

But, $(ab) \circ (bc) = (abc) \notin H_1 \cup H_2$.

Thus $H_1 \cup H_2$ is not closed for the composite composition.

Hence $H_1 \cup H_2$ is not a sub-group.

Theorem-4: Every subgroup of a cyclic group is cyclic.

Proof: Let $G = \{a\}$ be a cyclic group generated by a and let H be any subgroup of G.

If $H = G$ or $H = \{e\}$, where e is the identity element, then H is clearly cyclic.

So, consider the case, when H is a proper subgroup of G.

Since, $H \subset G$, so each element of H is some integral power of a.

Let m be the least positive integer such that $a^m \in H$.

Now, if a^s be an arbitrary element of H, then by division algorithm, $s=mq+r$, where $0 \leq r < m$.

But, H being a subgroup,

$$a^s \in H,\ a^m \in H \Rightarrow a^s \in H,\ a^{-m} \in H$$
$$\Rightarrow a^s \in H,\ (a^{-m})^q \in H$$
$$\Rightarrow a^{s-mq} \in H$$
$$\Rightarrow a^r \in H \quad \text{where} \quad 0 \leq r < m.$$

But, m being the least positive integer such that

$a^m \in H$ and $0 \leq r < m$, so $r = 0$. $s = mq$.

$\therefore \quad a^s = a^{mq} = (a^m)^q$.

Thus, each element of H is some integral power of a^m and hence, H is a cyclic group generated by a^m.

Theorem-5: Every proper subgroup of an infinite cyclic group is always infinite.

Proof: Let $G = \{a\}$ be an infinite cyclic group, generated by an element a and let H be a proper subgroup of G. Now if m is the least positive integer such that $a^m \in H$, then as shown in the preceding theorem, H is a cyclic group generated by a^m.

Now, if possible, let H be finite and let $\circ(H) = n$.

Then, the order of any generator of a finite cyclic group being the same as the order of the group, it follows that $\circ(a^m) = \circ(H) = n$.

Consequently $(a^m)^n = e$ or $a^{mn} = e$.

So, $\circ(a) \leq mn$ *i.e.* $\circ(a)$ is finite and therefore, G is finite, which contradicts the hypothesis that G is infinite.

Since, the contradiction arises by assuming that H is finite,

So H is infinite.

Some Results on Complexes

Theorem 1: If H is a subgroup of a group G, then H^{-1}= H. The converse, however is not true.

Proof: Let H be a subgroup of a group G. Then, H being a group,

$h \in H \Rightarrow h^{-1} \in H \Rightarrow (h^{-1})^{-1} \in H^{-1} \Rightarrow h \in H^{-1}$.

$\therefore H \subseteq H^{-1}$.

Again, if x is an arbitrary element of H^{-1}, then

$x \in H^{-1} \Rightarrow x = h^{-1}$ for some $h \in H$

$\Rightarrow x = h^{-1} \in H \quad [\because h \in H \Rightarrow h^{-1} \in H]$

$\therefore H^{-1} \subseteq H$.

Thus, $H^{-1} = H$.

To show that the converse is not always true, consider the multiplicative group $G = \{1, -1\}$ and its complex $H = \{-1\}$.

Clearly, $H^{-1} = \{-1\} = H$.

But, H is not a subgroup of G.

Theorem 2: A necessary and sufficient condition for a complex H of a group G to be a subgroup is that, $H H^{-1} = H$.

Proof: Let H be a subgroup of a group G.

Let x be an arbitrary element of $H H^{-1}$. Then,

$x \in H H^{-1} \Rightarrow x = ab^{-1}$ for some $a \in H, \quad b^{-1} \in H^{-1}$

$\Rightarrow x = ab^{-1}$, where $a \in H, \quad b \in H$

$\Rightarrow x = ab^{-1} \in H$

[$\because$ H being a subgroup, $a \in H, \ b \in H \Rightarrow ab^{-1} \in H$]

$\therefore H H^{-1} \subseteq H$.

Again, if y is an arbitrary element of H, then we may write

$y = ye = y e^{-1} \in H H^{-1} \quad [\because e \in H \Rightarrow e^{-1} \in H^{-1}]$.

$\therefore H \subseteq H H^{-1}$.

Hence, $H H^{-1} = H$.

Conversely, let H be a complex of a group G, given in such a way that $H H^{-1} = H$. Then,

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

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

$\Rightarrow a b^{-1} \in H \quad [\because H H^{-1} = H]$.

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

But, this is the necessary and sufficient condition for H to be a subgroup.

Hence, H is a subgroup of G.

Theorem 3: If H and K are subgroups of a group G, then HK is a subgroup if and only if HK = KH.

Proof: Let H and K be two subgroups of a group G, given in such a way that HK is also a subgroup of G. Then,

HK is a subgroup

$\Rightarrow (HK)^{-1} = HK \quad [\because A \text{ is a subgroup} \Rightarrow A^{-1} = A]$

$\Rightarrow \quad K^{-1}\ H^{-1} = HK \qquad [\because \quad (HK)^{-1} = K^{-1}\ H^{-1}]$

$\Rightarrow \quad KH = HK \qquad [\because \quad H^{-1} = H \quad \text{and} \quad K^{-1} = K\ ]$

$\therefore \quad HK = KH.$

Conversely, let H and K be two subgroups of a group G such that $HK = KH$. Then, in order to prove that HK is a subgroup, it is sufficient to show that

$(HK)\ (HK)^{-1} = HK.$

Now, $(HK)\ (HK)^{-1}$

$= (HK)\ (K^{-1}\ H^{-1}) \qquad [\because \quad (HK)^{-1} = K^{-1}\ H^{-1}]$

$= H\ (K\ K^{-1})\ H^{-1} \qquad$ [by associativity]

$= (HK)\ H^{-1} \qquad [\because \quad K$ being a subgroup, $K\ K^{-1} = K\ ]$

$= (KH)\ H^{-1} \qquad [\because \quad HK = KH\ ]$

$= K\ (H\ H^{-1}) \qquad$ [by associativity]

$= KH \qquad [\because \quad H$ being a subgroup, $H\ H^{-1} = H\ ]$

$= HK \qquad [\because \quad KH = HK\ ].$

Thus, $(HK)\ (HK)^{-1} = HK.$

Hence, HK is a subgroup.

Corollary: If H and K are two subgroups of an abelian group G, then HK is also a subgroup of G.

Theorem 4: A necessary and sufficient condition for a complex H of a finite group G to be a subgroup is that HH =H.

Proof: Let H be a subgroup of a finite group G.

Now, if x be an arbitrary element of HH, then

$x \in HH \quad \Rightarrow \quad x = ab \quad \in \quad HH \qquad$ for some $\quad a \in H, \quad b \in H$

$\Rightarrow \quad x = ab \quad \in \quad H$

$[\because \quad H$ being a subgroup, $\quad a \in H, \quad b \in H \quad \Rightarrow \quad ab \in H\ ]$

$\therefore \quad HH \quad \subseteq \quad H$

Again, if y is an arbitrary element of H, then we can write

$y = ye \in HH$.

So, $H \subseteq HH$.

Hence, $HH = H$.

Conversely, let H be a complex of a finite group G, given in such a way that $HH = H$. Then, in order to prove that H is a subgroup of G, it is sufficient to show that H is stable for the composition in G.

Now, $a \in H, \quad b \in H \quad \Rightarrow \quad ab \in HH \quad \Rightarrow \quad ab \in H \quad [\because HH = H]$.

Hence, H is a subgroup of G.

COSETS

Coset: Let H be a subgroup of a group $(G,*)$. Let $a \in G$. Then, the complexes $H * a = \{h * a : h \in H\}$ and $a * H = \{a * h : h \in H\}$ *of* G are respectively known as the right coset and the left coset of H in G, determined by a.

Examples:

i) Consider the multiplicative group, $G = \{1, -1, i, -i\}$. Let $H = \{-1, 1\}$ be a subgroup of G. Now, the right coset determined by i is given by
$H \bullet i = \{(-1) \bullet i, 1 \bullet i\} = \{-i, i\}$.

Similarly, the other right cosets are

$H \bullet 1 = H, \quad H \bullet (-1) = H \quad \& \quad H \bullet (-i) = \{-i, i\}$.

In a similar fashion, we can say that the various left cosets are

$1 \bullet H = H, \quad (-1) \bullet H = H, \quad i \bullet H = \{-i, i\} \quad \& \quad (-i) \bullet H = \{-i, i\}$.

ii) Consider the additive group $(\mathbb{Z}, +)$ of all integers.

Let $H = \{3a : a \in \mathbb{Z}\} = \{\ldots\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\ldots\}$.

Then, it is easy to verify that H is a subgroup of $\mathbb{Z}$. Now,

$H + 0 = \{\ldots\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\ldots\} = H$;

$H + 1 = \{\ldots\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\ldots\}$; and

$H + 2 = \{ \ldots \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \ldots \}$.

Clearly, $\mathbb{Z} = (H + 0) \cup (H + 1) \cup (H + 2)$.

Similarly, $\mathbb{Z} = (0 + H) \cup (1 + H) \cup (2 + H)$.

iii) Consider the symmetric group S_3 of all permutations of degree 3, defined on three symbols a, b, c and given by $f_1 = (a)$, $f_2 = (ab)$, $f_3 = (bc)$, $f_4 = (ca)$, $f_5 = (abc)$ & $f_6 = (acb)$.

Let $H = \{f_1, f_5, f_6\}$.

Then, H is clearly a subgroup of S_3.

It is easy to verify that each right coset of H in G, is equal to the corresponding left coset.

However, if $H^* = \{f_1, f_2\}$, then H^* is also a subgroup of G.

But, $H^* \circ f_3 \neq f_3 \circ H^*$.

Remarks:

i) H itself is a right as well as a left coset, determined by the identity element e, since $He = \{he : h \in H\} = \{h : h \in H\} = H$ and similarly, $eH = H$.

ii) Since, $e \in H \Rightarrow ea \in Ha \Rightarrow a \in Ha$. It follows that every right coset Ha is non-empty and it contains at least one element, namely, a. Similarly, $a \in Ha$ and therefore, $aH \neq \phi$.

iii) In general, $aH \neq Ha$. But, if the group G is abelian, then $aH = Ha \quad \forall\, a \in G$. However, even when G is non-abelian, we may have $aH = Ha$ for each $a \in G$.

Properties of Cosets

Theorem 1: If H is a subgroup of a group G, then h ∈ H ⇔ Hh = H and hH = H.

Proof: Let $h \in H$. Now, if $x \in Hh$, then

$x \in Hh \Rightarrow x = h'h$ for some $h' \in H$

$\Rightarrow x = h'h \in H \quad [\because h' \in H, h \in H \Rightarrow h'h \in H]$

$\therefore Hh \subseteq H \quad \ldots\ldots\ldots$ (i)

Again, if $y \in H$, then

$y = ye = y(h^{-1}h) = (yh^{-1})h \in Hh$ $[\because\ yh^{-1} \in H]$

$\therefore\ H \subseteq Hh$ … … … (ii)

Thus, from (i) and (ii) we have, $Hh = H$.

Similarly, $h \in H \Rightarrow hH = H$.

Conversely, let $Hh = H$.

Then, $eH \in Hh \Rightarrow h \in Hh \Rightarrow h \in H$ $[\because\ Hh = H]$.

Thus, $Hh = H \Rightarrow h \in H$.

Similarly, $hH = H \Rightarrow h \in H$.

Theorem 2: Let H be a subgroup of a group G and let a, b ∈ G. Then,
Ha = Hb ⇔ $ab^{-1} \in H$ and aH = bH ⇔ $a^{-1}b \in H$.

Proof: $Ha = Hb \Rightarrow a \in Hb$ $[\because\ a = ea \in Ha]$

$\Rightarrow a = hb$ for some $h \in H$

$\Rightarrow ab^{-1} = h \in H$.

Again, $ab^{-1} \in H \Rightarrow ab^{-1} = h$ for some $h \in H$

$\Rightarrow a = hb$

$\Rightarrow Ha = H(hb) = (Hh)b = Hb$ $[\because h \in H \Rightarrow Ha = H]$

Hence, $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Similarly, $aH = bH \Leftrightarrow a^{-1}b \in H$.

Theorem 3: Any two right (left) cosets of a subgroup are either disjoint or identical.

Proof: Let H be a subgroup of a group G. Let Ha and Hb be any two right cosets of H in G.

If $Ha \cap Hb \neq \phi$, then we are done.

So, let $Ha \cap Hb \neq \phi$. Then, at least one element of Ha must be equal to some elements of Hb.

Let $h_1 a = h_2 b$ for some $h_1, h_2 \in H$.

Now $h_1 a = h_2 b \Rightarrow b = h_2^{-1}(h_1 a) = (h_2^{-1} h_1) a$

$\Rightarrow Hb = H(h_2^{-1} h_1) a$

$\Rightarrow Hb = [H(h_2^{-1} h_1)] a$

$\Rightarrow Ha = Hb. \quad [\because h_2^{-1} h_1 \in H \Rightarrow H(h_2^{-1} h_1) = H]$

Thus, either $Ha \cap Hb = \phi$ or $Ha = Hb$.

Similarly, either $aH \cap bH = \phi$ or $aH = bH$.

Theorem 4: If H is a subgroup of a group G, then G is the union of all right (left) cosets of H in G.

Proof: Since, every right coset of H in G is a subset of G, the union of all right cosets of H in G is therefore, a subset of G.

On the other hand, if a ∈ G, then a ∈ Ha.

i.e. each element of G is contained in some right coset of H in G.

Consequently, G is contained in the union of all right cosets of H in G.

Thus, G is the union of all right cosets of H in G.

Similarly, G is the union of all left cosets of H in G.

Theorem 5: Let H be a subgroup of a group G. Then, there is a one to one correspondence between the set of all distinct left cosets and the set of all distinct right cosets of H in G.

Proof: Let us denote by G' and G'', the sets of all distinct left cosets and that of all distinct right cosets respectively.

Consider the mapping $f: G' \longrightarrow G'' : f(aH) = Ha^{-1} \quad \forall\ a \in G.$

This mapping is well defined, since

$aH = bH \Rightarrow a^{-1} b \in H$

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

$\Rightarrow Ha^{-1} = Hb^{-1}$

$\Rightarrow f(aH) = f(bH).$

Also, f is one-one, since

$f(aH) = f(bH) \Rightarrow Ha^{-1} = Hb^{-1}$

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

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

$\Rightarrow aH = bH.$

Now, for each $Ha \in G'' \quad \exists \quad a^{-1}H \in G''$ such that $f(a^{-1}H) = Ha.$

So, f is onto.

Thus, f is a one-one mapping from G' to G'' and hence the theorem follows.

Remark: As a consequence of the above theorem, it follows that the number of distinct right cosets of H in G, is the same as the number of distinct left cosets of H in G.

Index of a subgroup: Let H be a subgroup of a group G. Then the number of distinct right (left) cosets of H in G, is called the index of H in G and it is denoted by [G : H].

Examples:

i) Consider the multiplicative group, $G = \{1, -1, i, -i\}$. Let $H = \{-1, 1\}$ be a subgroup of G. Now, the right coset determined by i is given by
$H \bullet i = \{(-1) \bullet i, 1 \bullet i\} = \{-i, i\}$.

Similarly, the other right cosets are

$H \bullet 1 = H, \quad H \bullet (-1) = H \quad \& \quad H \bullet (-i) = \{-i, i\}$.

In a similar fashion, we can say that the various left cosets are

$1 \bullet H = H, \quad (-1) \bullet H = H, \quad i \bullet H = \{-i, i\} \quad \& \quad (-i) \bullet H = \{-i, i\}$.

As the number of distinct right (left) cosets of H in G, is 2, so the index of H in G,

[G : H]=2, here.

ii) Consider the additive group $(\mathbb{Z}, +)$ of all integers.

Let $H = \{3a : a \in \mathbb{Z}\} = \{ \dots \dots, -9, -6, -3, 0, 3, 6, 9, \dots \dots \}$.

Then, it is easy to verify that H is a subgroup of $\mathbb{Z}$. Now,

$H + 0 = \{ \dots \dots, -9, -6, -3, 0, 3, 6, 9, \dots \dots \} = H$;

$H + 1 = \{ \dots \dots, -8, -5, -2, 1, 4, 7, 10, \dots \dots \}$; and

$H + 2 = \{ \dots \dots, -7, -4, -1, 2, 5, 8, 11, \dots \dots \}$;

$H + 3 = \{ \dots \dots, -9, -6, -3, 0, 3, 6, 9, \dots \dots \} = H$;

$H + 4 = \{ \dots \dots, -8, -5, -2, 1, 4, 7, 10, \dots \dots \}$=H+1 ;

$H + 5 = \{ \dots \dots, -7, -4, -1, 2, 5, 8, 11, \dots \dots \}$=H+2;

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

and so on.

Here, the distinct right cosets of H in G are $H, H + 1, H + 2$, Thus, the index of H in G are, $[G, H] = 3$.

Theorem 6: Let H be a subgroup of a group G. Then, there exists a one to one correspondence between any two right (left) cosets of H in G.

Proof: Let Ha and Hb be any two right cosets of H in G. Consider the mapping

$f : Ha \longrightarrow Hb : f(ha) = hb \quad \forall\ h \in H.$

f is one-one, since

$f(h_1 a) = f(h_2 a) \quad \Rightarrow \quad h_1 b = h_2 b \quad \Rightarrow \quad h_1 = h_2.$

Also, f is onto, since for each $hb \in Hb$ $\exists$ an element ha of Ha such that $f(ha) = hb$.

Remark: As a consequence of the above theorem, it follows that any two distinct right cosets of H in G contain the same number of elements.

Similarly, any two distinct left cosets of H in G contain the same number of elements.

Theorem 7 (**Lagrange's theorem**): The order of each subgroup of a finite group, is a divisor of the order of the group.

Proof: Let H be a subgroup of a finite group G. Then, clearly H is also finite.

Let, $\circ(H) = m$ and $\circ(G) = n$.

Let, $H = \{h_1, h_2, \ldots\ldots\ldots, h_m\}$, where h_i's are distinct.

Now, let a be an arbitrary element of G. Then,

$Ha = \{h_1 a, h_2 a, h_3 a, \ldots\ldots\ldots, h_m a\}.$

All these elements in Ha are distinct, for, if h_i and h_j are two distinct elements of H, then $h_i a = h_j a \quad \Rightarrow \quad h_i = h_j$ (by cancellation law), which contradicts the hypothesis that $h_i \neq h_j$.

This shows that Ha consists of m distinct elements.

Since, any two distinct right cosets of H in G contain the same number of elements, it follows that every right coset of H in G contains exactly m distinct elements.

Now, let the right coset decomposition of G relative to H contain k cosets *i.e.*, G is the union of k distinct right cosets of H in G.

Since every right coset contains m distinct elements, the union of k cosets will therefore contain mk distinct elements.

Consequently, G contains mk distinct elements.

$\therefore \quad n = mk \quad$ or $\quad \frac{n}{m} = k. \quad i.e. \quad \frac{\circ(G)}{\circ(H)} = k.$

Accordingly, the order of H is a divisor of order of G.

Remark 1. Since $n = mk$, we have $\frac{n}{k} = m$. *i.e.* $\frac{\circ(G)}{[G:H]} = m.$

Thus, the index of any subgroup of a finite group is the divisor of the order of the group.

Remark 2. **The converse of Lagrange's theorem is always true**, *i.e.* if G is a finite group of order n and m is a positive integer such that m is a divisor of n, then it is not necessary that G must have a subgroup of order m.

For example, if we consider the alternating group A_4 of all even permutations of degree 4, defined on a set S containing 4 elements. Then,

$\circ(A_4) = \frac{1}{2} \times \circ(S_4) = 12 \qquad [\because \quad \circ(S_4) = 4! = 24]$

Now, 6 is clearly a divisor of 12, but $\exists$ no subgroup of A_4 of order 6.

We shall show further that the inverse of Lagrange's theorem holds in case of finite cyclic groups.

Deduction from Lagrange's Theorem

Corollary 1: The order of every element of a finite group is a divisor of the order of the group.

Proof: Let G be a finite group of order n and let a be an arbitrary element of G. Since, the order of every element of a finite group is finite, so $\circ(a)$ is finite. Let $\circ(a) = m$.

Let H be the cyclic group generated by the element a.

Then, $H = \{ a, a^2, a^3, \ldots\ldots\ldots, a^m = e \}$, where all a_i's are distinct.

So, $\circ(H) = m$.

Now, by Lagrange's theorem, $\circ(H)$ is a divisor of $\circ(G)$.

So, $\exists$ a positive integer k such that $\frac{n}{m} = k.$

$\therefore \quad \frac{\circ(G)}{\circ(a)} = k. \quad i.e. \quad \circ(a)$ is a divisor of $\circ(G)$.

Theorem 1: A finite group of prime order does not have any proper subgroups.

Proof: Let G be a finite group of order n, where n is prime. If possible, let H be a subgroup of G, such that $\circ(H) = m \leq n$.

Then, by Lagrange's theorem m is a divisor of n. But, n being prime, so either $m = 1$ or $m = n$. This shows that H is an improper subgroup of G.

Thus, a finite group of prime order does not have any proper subgroup.

Theorem 2: Converse of Lagrange's theorem always holds in case of finite cyclic groups. i.e. If G is a finite cyclic group of order n . Then for any divisor m of n, there exits a unique subgroup of G, of order m.

Proof: Let G be a finite cyclic group of order n, generated by a. Then, $\circ(a) = n$.

Let, m be a divisor of n so that $n = mk$ for some positive integer k.

Now, if H is a cyclic group generated by a^k, then each element of H is some integral power of a^k and therefore, of a. Consequently, each element of H is in G. So, H is a subgroup of G.

Clearly, $\circ(H) = \circ(a^k)$. We now show that $\circ(a^k) = m$.

Now, $\circ(a) = n \Rightarrow a^n = e \Rightarrow a^{mk} = e \Rightarrow (a^k)^m = e$

$\therefore \quad \circ(a^k) \leq m.$

If possible, let $\circ(a^k) = p < m$. Then,

$\circ(a^k) = p \Rightarrow (a^k)^p = e$

$\Rightarrow a^{kp} = e$

$\Rightarrow \circ(a) \leq kp$

$\Rightarrow \circ(a) < n \quad [\because p < m \Rightarrow kp < km = n]$

This contradicts the fact that $\circ(a) = n$. So, $\circ(a^k) \not< m$.

Accordingly, $\circ(a^k) = m$.

Thus, $\circ(H) = \circ(a^k) = m$. *i.e.* H is a subgroup of order m.

To prove uniqueness, let H' be another cyclic subgroup of G, of order m, generated by say a^l.

Then, by division algorithm $\exists$ integers q and r such that

$l = kq+r$, where $0 \leq r < k$. $ml = mkq+mr$, where $0 \leq mr < mk$.

Now, $a^{ml} = a^{mkq+mr} = (a^{mk})^q \cdot a^{mr} = a^{mr}$ [$\because$ $mk = n$ & $a^n = e$]

Since, H' is a cyclic group of order m, generated by a^l, so $\circ(a^l) = m$ and therefore, $a^{ml} = e$.

Consequently, $a^{mr} = e$, where $0 \leq mr < mk = n$.

This is possible only, when $mr = 0$ and therefore, $r = 0$ [$\because m \neq 0$], $l = kq$.

Consequently, $H' = \{a^l\} \subseteq \{a^k\} = H$.

But, $\circ(H') = \circ(H)$. So, $H = H'$.

Theorem 3: Every finite group of prime order is cyclic.

Proof: Let G be a finite group of order n, where n is prime. Since n is prime, so $n > 1$. It follows, therefore, that G contains at least two elements.

So, $\exists$ $a \in G$ such that $a \neq e$.

Now, since $a \neq e$, so $\circ(a) \geq 2$.

Let, $\circ(a) = m$, where $m \geq 2$.

Now, let H be a cyclic group generated by a. Then, $\circ(H) = \circ(a) = m$.

So, by, Lagrange's theorem m is a divisor of n.

But, n being prime and $m \neq 1$, so $m = n$.

Now, $H \subseteq G$ and $\circ(H) = \circ(G)$, so $H = G$.

But, H being cyclic, so is therefore G.

Thus, every finite group of prime order is cyclic.

Theorem 4: Every finite group of composite order possesses proper subgroups.

Proof: Let G be a finite group of composite order.

Let $\circ(G) = mn$, where $m > 1$ and $n > 1$.

Case I. When G is cyclic.

Let G be a cyclic group, generated by an element a.

Then, $\circ(a) = \circ(G) = mn$. Consequently, $\circ(a^m) = n$.

Let H be a cyclic group generated by a^m.

Then, $H = \{ a^m , a^{2m} , a^{3m} , \ldots\ldots\ldots , a^{mn} = e \}$

i.e. H is a subgroup of G, of order n.

Also, since $2 \leq n < mn$, it follows that H is a proper subgroup of G.

Case II. When G is not cyclic.

In this case, the order of each element of G is less than mn.

So, $\exists$ an element $a \in G$ such that $\circ(a) = k$, where $2 \leq k < mn$.

Now, if H is a cyclic group generated by a, then $\circ(H) = \circ(a) = k < mn$.

i.e. H is a proper subgroup of G.

Illustrative Examples

Ex-1. Let H be a subgroup of a group G and let a, b $\in$ H. Show that

$Ha \neq Hb \quad \Leftrightarrow \quad a^{-1}H \neq b^{-1}H.$

Solution: Let $Ha \neq Hb$ and if possible, let $a^{-1}H = b^{-1}H$. Then,

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

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

$\Rightarrow \quad Ha = Hb,$ which is a contradiction.

So, $Ha \neq Hb \quad \Rightarrow \quad a^{-1}H \neq b^{-1}H.$

Similarly, $a^{-1}H \neq b^{-1}H \quad \Rightarrow \quad Ha \neq Hb.$

Hence, the result follows.

Ex-2. If H is a subgroup of a group G and a $\in$ G, then $(Ha)^{-1} = a^{-1}H$.

Solution: Let $x \in (Ha)^{-1}$, then $x = (ha)^{-1}$ for some $h \in H$.

$\therefore \quad x = (ha)^{-1} = a^{-1}h^{-1} \in a^{-1}H \qquad [\because \quad h \in H \Rightarrow h^{-1} \in H]$

So, $(Ha)^{-1} \subseteq a^{-1}H \quad \ldots\ldots\ldots$ (i)

Again, let $y \in a^{-1}H$, then $y = a^{-1}h$ for some $h \in H$.

$\therefore \quad y = a^{-1}h = (h^{-1}a)^{-1} \in (Ha)^{-1} \qquad [\because \quad h \in H \Rightarrow h^{-1} \in H]$

So, $a^{-1}H \subseteq (Ha)^{-1} \quad \ldots\ldots\ldots$ (ii)

Thus, from (i) & (ii), we have $(Ha)^{-1} = a^{-1}H$.

NORMAL SUB-GROUPS

Normal sub-groups: A sub-group H of a group G is said to be a normal sub-group of G, if Ha = aH $\forall$ a $\in$ G.

A normal sub-group is also known as an **invariant sub-group** or a **self-conjugate sub-group** or a **normal divisor** of the group.

For a group G, G and {e} are always normal sub-groups of G and these are called trivial normal sub-groups.

Examples:

i) The alternating group A_3 of all even permutations of degree 3 is a normal sub-group of the symmetric group S_3 of all permutations of degree 3.
Here $S_3 = \{(a), (bc), (ab), (ac), (abc), (acb)\}$ and $A_3 = \{(a), (abc), (acb)\}$.
It is easy to verify that $A_3 \circ f = f \circ A_3 \quad \forall \ f \in S_3$.
However, $\boldsymbol{H = \{(a), (bc)\}}$ is a sub-group of $\boldsymbol{S_3}$, which is not normal, since $H \circ (ab) \neq (ab) \circ H$.

ii) Let G be the multiplicative group of all n × n non-singular matrices. Let H be the set of all those matrices from G, the value of those determinant is 1. Then, H is a normal sub-group of G.

Proof: Let $A \in H$, $B \in H$. Then, $|A| = 1$ and $|B| = 1$.

$\therefore \quad |AB^{-1}| = |A|\,|B^{-1}| = |A|\,|B| = 1.1 = 1.$

Thus, $A \in H$, $B \in H \quad \Rightarrow \quad AB^{-1} \in H \quad \forall\ A, B \in H.$

This shows that H is a sub-group of G.

Now, if $B \in H$, then $|B| = 1 \neq 0$, so $AB = BA \quad \forall\ A \in G.$

Consequently, $AH = HA \qquad \forall\ A \in G.$

Hence, H is a normal sub-group of G.

iii) Every sub-group of an abelian group is normal.

Proof:

Since, every left coset of a sub-group of an abelian group is equal to the corresponding right coset, so it follows that every sub-group of an abelian group is normal.

Remark: Every cyclic group being an abelian group, it follows that every sub-group of a cyclic group is normal.

Hamiltonian Groups: A non-abelian group, each of whose sub-groups is normal, is known as a Hamiltonian group.

Example: The Quaternion group is a Hamiltonian group.

Proof: We know that the set $S = \{ \pm 1 , \pm i , \pm j , \pm k \}$ is a group with respect to multiplication on S, defined by

$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i \qquad$ and $\qquad ki = -ik = j.$

The possible sub-groups of S are

$H_1 = \{1\}, \qquad H_2 = \{1, -1\}, \qquad H_3 = \{ \pm 1 , \pm i \}, \qquad H_4 = \{ \pm 1 , \pm j \},$

$H_5 = \{ \pm 1 , \pm k \} \qquad$ and $\qquad H_6 = \{ \pm 1 , \pm i , \pm j , \pm k \}.$

It is easy to verify that each one of these sub-groups is a normal sub-group.

Thus, each sub-group of the non-abelian Quaternion group is normal and therefore, it is an example of a Hamiltonian group.

Non-Example: The symmetric group, S_3 of all permutations of degree 3.

Simple groups: A group G ≠ {e} is said to be a simple group, if it has no proper normal sub-groups.

Example: Every group of prime order is simple.

Since a group of prime order has no proper sub-group, so it has no proper normal sub-group. Hence, it is simple.

Non-Example: A cyclic group of composite order is never a simple group.

Since, every cyclic group of composite order surely possesses a proper sub-group and every sub-group of a cyclic group being normal, so the result follows.

Similarly, an abelian group of composite order is never a simple group.

Results on Normal sub-groups

Theorem 1: A sub-group H of a group is normal iff

$xhx^{-1} \in H \quad \forall\ x \in G$ and $\forall\ h \in H$.

Proof: Let H be normal subgroup of a group G.

Then, $xH = Hx \quad \forall\ x \in G$.

Now, if h is an arbitrary element of H, then

$xh = h'x$ for some $h' \in H$ [$\because\ xH = Hx$].

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

Conversely, let H be a subgroup of G such that

$xhx^{-1} \in H \quad \forall \quad x \in G,\ h \in H$.

Now, if a be an arbitrary element of G and h be any element of H, then $aha^{-1} \in H$.

Now, $ah \in aH$.

But, $ah = aha^{-1}a = (aha^{-1})\, a \in Ha$ [$\because\ aha^{-1} \in H$].

Thus, each element of aH is in Ha. *i.e.* $aH \subseteq Ha$ … … … (i)

Again, let $ha \in Ha$.

But, $ha = aa^{-1}ha = a\,(a^{-1}ha) \in aH$.

[$\because\ a \in G \Rightarrow a^{-1} \in G \Rightarrow a^{-1}h\,(a^{-1})^{-1} \in H \Rightarrow a^{-1}ha \in H$].

$\therefore\ Ha \subseteq aH$ … … … (ii)

Thus, form (i) and (ii), we have $Ha = aH \quad \forall\ a \in G$.

This shows that H is a normal subgroup of G.

Theorem 2: A subgroup H of a group G is normal iff

$xHx^{-1} = H \quad \forall\ x \in G$.

Proof: Let $xHx^{-1} = H \qquad \forall\ x \in G.$

Then, for any element $h \in H$, $xhx^{-1} \in xHx^{-1}$ and therefore,

$xhx^{-1} \in H \qquad \forall \qquad h \in H,\ x \in G.$

This shows that H is normal.

Conversely, let H be a normal subgroup of G.

Then, $xhx^{-1} \in H \qquad \forall \qquad h \in H$ and $x \in G.$

$\therefore \qquad xHx^{-1} \subseteq H \qquad \ldots\ldots\ldots$ (i)

Again, let h be an arbitrary element of H. Then, $\forall\ x \in G$, we have

$h = xx^{-1}hxx^{-1} = x(x^{-1}hx)x^{-1} \in xHx^{-1}$ [$\because$ H being normal, $x^{-1}hx \in H$]

$\therefore \qquad H \subseteq xHx^{-1} \qquad \ldots\ldots\ldots$ (ii)

Thus, from (i) and (ii), we have $xHx^{-1} = H.$

Theorem 3: A subgroup H of a group G is normal if and only if the product of two right cosets of H in G is again a right coset of H in G.

Proof: Let H be a normal subgroup of G and let $a, b \in G.$

Then, $Ha = aH$ and $Hb = bH.$

$\therefore \quad (Ha)(Hb) = H(aH)b = H(Ha)b = HHab = Hab.$

[$\because$ $aH = Ha$ and H being a subgroup, $HH = H$]

Thus, the product of two right cosets is a right coset.

Conversely, let H be a subgroup of a group G such that the product of any two right cosets of H in G, is a right coset.

Now, if $x \in G$, then $x^{-1} \in G.$

$\therefore$ Hx and Hx^{-1} are two right cosets of H in G and according to the given hypothesis $(Hx)(Hx^{-1})$ is a right coset of H in G.

Now, $e = xx^{-1} = (ex)(ex^{-1}) \in (Hx)(Hx^{-1})$ [$\because$ $e \in H$].

Thus, $(Hx)(Hx^{-1})$ and H are two right cosets of H in G, having a common element e. But, any two right cosets having a common element are identical.

So, $(Hx)\,(Hx^{-1}) = H$.

Consequently, $(h_1 x)\,(hx^{-1}) \in H \quad \forall\, x \in G$ and $h_1, h \in H$

$\therefore \quad h_1^{-1} h_1\,(xhx^{-1}) \in h_1^{-1} H \quad$ or $\quad xhx^{-1} \in H$.

$[\because \quad h_1^{-1} \in H \quad \Rightarrow \quad h_1^{-1} H = H\,]$

Hence, H is normal.

Remark. A similar result holds for left cosets.

Theorem 4: The product of any two normal subgroups of a group is again a normal subgroup of the same.

Proof: Let H and K be two normal subgroups of a group G. Then, $e \in H$ and $e \in K$ and therefore, $e = ee \in HK$. Thus, $HK \neq \phi$.

Now, let h_1k_1 and h_2k_2 be any two arbitrary elements of HK so that $h_1, h_2 \in H$ and $k_1, k_2 \in K$.

Then,

$(h_1k_1)\,(h_2k_2)^{-1} = (h_1k_1k_2^{-1}h_2^{-1}) = h_1h_2^{-1}\,[h_2\,(k_1k_2^{-1})\,h_2^{-1}] \in HK$.

$[\because \quad H \;\&\; K$ being subgroups, $h_1h_2^{-1} \in H \quad \&\quad k_1k_2^{-1} \in K$ and K being normal in G, $h_2\,(k_1k_2^{-1})\,h_2^{-1} \in HK\,]$

Thus, $h_1k_1 \in HK, \quad h_2k_2 \in HK \quad \Rightarrow \quad (h_1k_1)\,(h_2k_2)^{-1} \in HK$.

So, HK is a subgroup of G.

Now, H and K are normal in G.

$\Rightarrow \quad xhx^{-1} \in H \quad \&\quad xkx^{-1} \in K \qquad \forall\, x \in G \quad \&\quad h \in H,\ k \in K$

$\Rightarrow \quad (xhx^{-1})\,(xkx^{-1}) \in HK \qquad \forall\, x \in G\,,\ h \in H \;\&\; k \in K$

$\Rightarrow \quad x\,(hk)\,x^{-1} \in HK \qquad \forall\, x \in G \quad \&\quad hk \in HK$.

This shows that HK is normal in G.

Theorem 5: Let H and K be two normal subgroups of a group G such that

$H \cap K = \{e\}$, then every element of H commutes with every element of K.

Proof: Let $h \in H$ and $k \in K$.

Then, in order to show that $hk = kh$, it is sufficient to show that $hkh^{-1}k^{-1} = e$.

Now, by the normality of K and H in G, we have $hkh^{-1} \in K$ & $kh^{-1}k^{-1} \in H$

[$\because$ $h \in H \Rightarrow h \in G$ & $k \in K \Rightarrow k \in G$]

Also, H and K being subgroups of G, we have

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

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

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

$\therefore$ $hkh^{-1}k^{-1} = e$ [$\because$ $H \cap K = \{e\}$]

Hence, $hk = kh$ $\forall\, h \in H$, $k \in K$.

Theorem 6: If a cyclic subgroup N of G is normal in G, then every subgroup of N is normal in G.

Proof: Let a be a generator of a cyclic and normal subgroup N of a group G. Let H be a subgroup of N. Let m be the least positive integer such that $a^m \in H$. Then, H is a cyclic group generated by a^m.

Now, if h is an arbitrary element of H, then $h = (a^m)^k$ for some integer k.

Thus, $\forall\, x \in G$, we have $xhx^{-1} = x\,(a^m)^k\,x^{-1} = (xa^kx^{-1})^m$.

But, N being normal, $xa^kx^{-1} \in N$.

Consequently, $xa^kx^{-1} = a^p$ for some integer p.

$\therefore$ $xhx^{-1} = (a^p)^m = (a^m)^p \in H$.

This shows that H is normal in G.

Thus, every subgroup of N is normal in G.

Theorem 7: If G is a group and H is a subgroup of index 2 in G, then H is a normal subgroup of G.

Proof: Let H be a subgroup of index 2 in G. Then G is the union of two distinct right (or left) cosets of H in G.

Now, let x be an arbitrary element of G.

Then, there are only two possibilities, $x \in H$ or $x \notin H$.

If $x \in H$, then $xH = H = Hx$ and so $xH = Hx$.

Again, if $x \notin H$, then $Hx \neq H$ and $xH \neq H$.

$\therefore$ $G = H \cup Hx$ and $G = H \cup xH$.

Consequently, $Hx = xH$ [each equal to $(G - H)$]

Thus, in either case, $Hx = xH$ $\forall\, x \in G$.

Hence, H is normal in G.

Illustrative Examples

Example-1: Let G be a group of order 2p, where p is prime. Then, show that G has a normal subgroup of order p.

Solution: Let G be a group of order $2p$, where p is prime.

Then, G being a finite group of composite order, it must have proper subgroups. Let, H be a proper subgroup of G.

Now, by Lagrange's theorem, $\circ(H)$ must divide $\circ(G)$.

$\therefore$ either $\circ(H) = 2$ or $\circ(H) = p$.

Now, if $\circ(H) = p$, then $[G : H] = \frac{\circ(G)}{\circ(H)} = \frac{2p}{p} = 2$.

Thus, H is a subgroup of index 2 in G.

Hence, H is normal in G.

Example-2: Give an example to show that, if H is a normal subgroup of G and K is a normal subgroup of H, then K may not be a normal subgroup of G.

Solution: Consider the following sets of permutations of degree 4, defined on four symbols a, b, c, d.

$G = \{ I , (ab) \circ (cd) , (ac) \circ (bd) , (ad) \circ (bc) , (ac) \circ (bd) , (abcd) , (adcb) \}$;

$H = \{ I , (ab) \circ (cd) , (ac) \circ (bd) , (ad) \circ (bc) \}$ and

$K = \{ I , (ab) \circ (cd) \}$.

It is easy to verify that G is a group and each one of H and K is a subgroup of G.

More-over, $[\, G : H \,] = \frac{\circ(G)}{\circ(H)} = \frac{8}{4} = 2.$

Thus, H is a subgroup of index 2 in G and therefore, H is a normal subgroup of G.

Also, $[\, H : K \,] = \frac{\circ(H)}{\circ(K)} = \frac{4}{2} = 2.$

So, K is a subgroup of index 2 in H and therefore, K is a normal subgroup of H.

But, $(abcd) \in G$, $(ab) \circ (cd) \in K$, and

$(abcd) \circ [(ab) \circ (cd)] \circ (abcd)^{-1} = (ad) \circ (bc) \notin K.$

This shows that K is not normal in G.

****

QUOTIENT GROUPS

Quotient group: Let H be a normal subgroup of a group G and let a be any element of G, then the set G/H of all right (left) cosets of H in G, is a group (called the quotient group or the factor group) under the binary composition, defined by

$(Ha)(Hb) = Hab \; ; \forall \; Ha, Hb \in G/H.$

G/H can be read in any of the following ways

i) G over H
ii) G factor H
iii) Factor group of G by H
iv) Quotient group of G by H

Examples:

i) Consider the multiplicative group, $G = \{1, -1, i, -i\}$. Let $H = \{-1, 1\}$ be a subgroup of G. Here, H is a normal subgroup of G as $G$is abelian and the distinct cosets of H are H and $\{-i, i\}$. Hence, H and $\{-i, i\}$ are only elements of the quotient group, G/H.

ii) Consider the additive group $(\mathbb{Z}, +)$ of all integers.

Let $H = \{3a : a \in \mathbb{Z}\} = \{ \ldots \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \ldots \}$.

Then, it is easy to verify that H is a normal subgroup of $\mathbb{Z}$. Now,

$H + 0 = \{ \ldots \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \ldots \} = H$;

$H + 1 = \{ \ldots \ldots, -8, -5, -2, 1, 4, 7, 10, \ldots \ldots \}$; and

$H + 2 = \{ \ldots \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \ldots \}$;

$H + 3 = \{ \ldots \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \ldots \} = H$;

$H + 4 = \{ \ldots \ldots, -8, -5, -2, 1, 4, 7, 10, \ldots \ldots \}$=H+1 ;

$H + 5 = \{ \ldots \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \ldots \}$=H+2;

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

and so on.

Here, the distinct right cosets of H in G are $H, H+1, H+2$,

Thus, ${}^{\mathbb{Z}}/_{H} = \{H, H+1, H+2\}$.

iii) Consider the symmetric group S_3 of all permutations of degree 3, defined on three symbols a, b, c and given by $f_1 = (a)$, $f_2 = (ab)$, $f_3 = (bc)$, $f_4 = (ca)$, $f_5 = (abc)$ & $f_6 = (acb)$. Then, it is easy to verify that the complex $A_3 = \{f_1, f_5, f_6\}$ of all even permutations is a normal subgroup of S_3 and the distinct cosets of A_3 in S_3 are A_3 and $A_3 \circ f_2$. Hence, $S_3/A_3 = \{A_3, A_3 \circ f_2\}$.

iv) Consider the group of integers $\boldsymbol{Z}$ (under addition) and the subgroup $2\boldsymbol{Z}$ consisting of all even integers. This is a normal subgroup, because $\boldsymbol{Z}$ is abelian. There are only two cosets: the set of even integers and the set of odd integers, and therefore the quotient group $\boldsymbol{Z}/2\boldsymbol{Z}$ is the cyclic group with two elements.

Theorem 1: Let H be a normal subgroup of a group G, then the set ${}^{G}/_{H}$ of all right (left) cosets of H in G, is a group (called the quotient group or the factor group) under the binary composition, defined by

$(Ha)(Hb) = Hab \; ; \forall \; Ha, Hb \in {}^{G}/_{H}$.

Theorem 2: If H is a normal subgroup of a finite group G, then $\circ\left({}^{G}/_{H}\right) = \frac{\circ(G)}{\circ(H)}$.

Theorem 3: If H is a normal subgroup of a group G such that the index of H in G is a prime number, then the quotient group ${}^{G}/_{H}$ is cyclic.

Theorem 4: Every quotient group of an abelian group is abelian, but the converse is not necessarily true.

Theorem 5: Every quotient group of a cyclic group is cyclic, but the converse is not necessarily true.

Homework:

i) If $G = (a)$ is a cyclic group of order 8, then find the quotient group corresponding to the subgroups generated by a^2 and a^4 respectively.

****

RING

Ring:

An algebraic structure $(R,+,\times)$, consisting of a non-empty set R with two binary compositions (to be denoted additively and multiplicatively), is called a ring, if the following properties are satisfied :

(i) $(R,+)$ is an abelian group;

(ii) Multiplication is associative, i.e., $(ab)c = a(bc)\ \forall\, a,b,c \in R$;

(iii) Multiplication distributes addition, i.e.,

$$a(b+c) = ab + ac \text{ and } (a+b)c = ac + bc;\ \forall\, a,b,c \in R.$$

Examples:

i) $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ are rings of numbers.

ii) Let M be the set of all $n \times n$ matrices, having their elements as integers (or rational or real or complex numbers). Then, $(M,+,\times)$ is a ring.

iii) The algebraic structure, $(R = \{0,1,2,3,4,5\}, +_6, \times_6)$ is a ring.

iv) Let $\boldsymbol{J}$ be the set of all **Gaussian integers**, i.e., the complex numbers of the form $a + ib$, where a and b are integers. $(\boldsymbol{J},+,\times)$ is a ring.

Remarks:

i) When there is no confusion about the operations on R, we simply say that R is a ring.

ii) In a ring R, the additive identity is called the **zero** of the ring and the additive inverse of a $\in R$ is called the negative of a, to be denoted by –a. Also, we define, $a - b = a + (-b);\ \forall\, a,b \in R$.

iii) A ring having multiplicative identity element (called unit element) is called a ring with unity.

Various types of Rings

Commutative ring: A ring $(R,+,\times)$ is called a **commutative ring**, if multiplication on R is commutative.

Examples:

i) Each one of the algebraic systems $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ is a commutative ring.

ii) Let $\boldsymbol{J}$ be the set of all **Gaussian integers**, i.e., the complex numbers of the form $a+ib$, where a and b are integers. $(\boldsymbol{J},+,\times)$ is a commutative ring.

Non Examples:

i) Let $M=\{\begin{bmatrix}0 & a\\ 0 & b\end{bmatrix}$: a and b are real numbers$\}$.Then, $(M,+,\times)$ is a non-commutative ring.

ii) The set of 2×2 matrices of the form $\begin{pmatrix}z_1 & z_2\\ -\overline{z_2} & \overline{z_1}\end{pmatrix}$;where z_1, z_2 are complex numbers, is a non-commutative ring.

Ring with unity: A ring $(R,+,\times)$ is called a **ring with unity**, if multiplicative identity (called, the unity of R and denoted by 1) exists in R.

Examples:

i) Each one of the algebraic systems $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ is a ring with unity.

ii) Let $\boldsymbol{J}$ be the set of all **Gaussian integers**, i.e., the complex numbers of the form $a+ib$, where a and b are integers. $(\boldsymbol{J},+,\times)$ is a ring with unity.

Non Examples:

i) Let $M=\{\begin{bmatrix}0 & a\\ 0 & b\end{bmatrix}$: a and b are real numbers$\}$.Then, $(M,+,\times)$ is a ring without unity.

ii) The ring of even integers is a ring without unity.

A ring without zero divisors: A ring $(R,+,\times)$ is called a ring without zero divisors if it is not possible to find two non-zero elements of R, whose product is zero, i.e., R is without zero divisors, when

$$[\,ab = 0 \;\Leftrightarrow\; a = 0 \;\; or \;\; b = 0\,].$$

Examples:

i) Each one of the algebraic systems $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ is a ring without zero divisors.

ii) If m is an arbitrary but fixed positive integer, then the set $S = \{ma : a \in \mathbb{Z}\}$ forms a ring, without zero divisors, with respect to addition and multiplication compositions.

iii) Let $\boldsymbol{J}$ be the set of all **Gaussian integers**, i.e., the complex numbers of the form $a + ib$, where a and b are integers. $(\boldsymbol{J},+,\times)$ is a ring without zero divisors.

Non Examples:

i) Let M be the set of all $n \times n$ matrices, having their elements as integers (or rational or real or complex numbers). Then, $(M,+,\times)$ is a ring with zero divisors, since we can find two $n \times n$ non-zero matrices, whose product is an $n \times n$ null matrix.

ii) Let $M = \{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a \text{ and } b \text{ are real numbers}\}$. Then, $(M,+,\times)$ is a ring, with zero divisors.

A ring with zero divisors: A ring $(R,+,\times)$ is called a ring with zero divisors if it is possible to find at least two elements a and b of R such that, $a \neq 0$, $b \neq 0$ and $ab = 0$.

Examples:

i) Let M be the set of all $n \times n$ matrices, having their elements as integers (or rational or real or complex numbers). Then, $(M,+,\times)$ is a ring with zero divisors, since we can find two $n \times n$ non-zero matrices, whose product is an $n \times n$ null matrix.

ii) Let $M = \{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a \text{ and } b \text{ are real numbers}\}$. Then, $(M,+,\times)$ is a ring, with zero divisors.

Non Examples:

i) Each one of the algebraic systems $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ is a ring without zero divisors.

ii) If m is an arbitrary but fixed positive integer, then the set $S = \{ma : a \in \mathbb{Z}\}$ forms a ring, without zero divisors, with respect to addition and multiplication compositions.

iii) Let $\boldsymbol{J}$ be the set of all **Gaussian integers**, i.e., the complex numbers of the form $a+ib$, where a and b are integers. $(\boldsymbol{J},+,\times)$ is a ring without zero divisors.

Integral domain: A ring $(R,+,\times)$ is called an Integral domain if it is a commutative ring, with unity and without zero divisors.

Examples:

i) Each one of the algebraic systems $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ is an Integral domain.

ii) Let $\boldsymbol{J}$ be the set of all **Gaussian integers**, i.e., the complex numbers of the form $a+ib$, where a and b are integers. $(\boldsymbol{J},+,\times)$ is a commutative ring, with unity and without zero divisors. Therefore, $(\boldsymbol{J},+,\times)$ is an Integral domain.

Non Examples:

i) If m is an arbitrary but fixed positive integer, then the set $S = \{ma : a \in \mathbb{Z}\}$ forms a commutative ring, without unity and without zero divisors, with respect to addition and multiplication compositions. Hence, S is not an Integral domain with respect to the operations provided here.

ii) Let M be the set of all n×n matrices, having their elements as integers (or rational or real or complex numbers). Then, $(M,+,\times)$ is a commutative ring with unity. Also, M is with zero divisors, since we can find two n×n non-zero matrices, whose product is an n×n null matrix. So, $(M,+,\times)$ is not an Integral domain.

iii) Let $M = \{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a \text{ and } b \text{ are real numbers}\}$. Then, $(M, +, \times)$ is a non-commutative ring, without unity and with zero divisors. So, $(M, +, \times)$ is not an Integral domain.

iv) The ring of even integers is not an integral domain. For it does not contain unity element.

Division ring or a skew-field: A ring $(R, +, \times)$ is called a Division ring or a skew-field if it's a ring with unity in which every non-zero element has a multiplicative inverse.

Examples:

i) Each one of the algebraic systems $(\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ is a Division ring or a skew-field.

ii) The set of 2×2 matrices of the form $\begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix}$; where z_1, z_2 are complex numbers, forms a division ring.

Non Examples:

i) $(\mathbb{Z}, +, \times)$ is a commutative ring, with unity and without zero divisors but it's not a skew-field.

ii) Let $\boldsymbol{J}$ be the set of all **Gaussian integers**, i.e., the complex numbers of the form $a + ib$, where a and b are integers. $(\boldsymbol{J}, +, \times)$ is a commutative ring, with unity and without zero divisors. But, this system is not a skew-field, for, if $(a + ib)$ is non-zero Gaussian integer, then

$(a + ib)^{-1} = \frac{1}{(a+ib)} = \frac{a}{(a^2+b^2)} + i\left(\frac{-b}{a^2+b^2}\right)$ is not necessarily a Gaussian integer, as $a/(a^2 + b^2)$ and $(-b)/(a^2 + b^2)$ are not necessarily integers.

Field: A ring $(R, +, \times)$ is called a Field if it is a commutative ring with unity in which every non-zero element has a multiplicative inverse.

Examples:

i) Each one of the algebraic systems $(\mathbb{Q},+,\times),(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ is a field.

ii) Let p be an arbitrary but fixed prime number. Then, the set $Z_p = \{0,1,2,3,\ldots\ldots\ldots,(p-1)\}$ forms a field with respect to $+_p$ and $\times_p$.

Non Examples:

i) The set of 2×2 matrices of the form $\begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix}$;where z_1, z_2 are complex numbers, forms a division ring which is not a field.

ii) Let M be the set of all n×n matrices, having their elements as integers (or rational or real or complex numbers). Then, $(M,+,\times)$ is a commutative ring with unity. Also, M is with zero divisors, since we can find two n×n non-zero matrices, whose product is an n×n null matrix. So, $(M,+,\times)$ is not a field.

iii) The algebraic structure, $(R=\{0,1,2,3,4,5\},+_6,\times_6)$, is a commutative ring with unity and with zero divisors. So, it's not a field.

Boolean ring: A ring $(R,+,\times)$ is called a **Boolean ring** if every element of R is idempotent, i.e.,

$x^2 = x\,;\ \forall\ x \in R.$

Examples:

i) The ring of integers modulo 2.

ii) One example of a Boolean ring is the power set of any set *X*, where the addition in the ring is symmetric difference, and the multiplication is intersection.

iii) As another example, we can also consider the set of all finite or cofinite subsets of *X*, again with symmetric difference and intersection as operations. More generally with these operations any field of sets is a Boolean ring.

Non Examples:

i) None of the algebraic systems $(\mathbb{Q},+,\times),(\mathbb{R},+,\times)$ and $(\mathbb{C},+,\times)$ is a Boolean ring.

Theorem 1: A ring is without zero divisors if and only if the cancellation laws hold in it.

Proof: Let us first suppose a ring R to be without zero divisors. Let $a,b,c \in R$ such that $a \neq 0$ and $ab = ac$. Then,

$a \neq 0,\ ab = ac \Rightarrow a \neq 0,\ ab - ac = 0$

$\Rightarrow a \neq 0,\ a.(b - c) = 0$

$\Rightarrow b - c = 0$ [$\because$ R is without zero divisors]

$\Rightarrow b = c.$

Thus, $a \neq 0$ and $ab = ac \Rightarrow b = c.$

Similarly, $a \neq 0$ and $ba = ca \Rightarrow b = c.$

Accordingly, the cancellation laws hold in R.

Conversely,

Let the cancellation laws hold in R. Let $a,b \in R$ such that $ab = 0$.

Let $ab = 0$ and $a \neq 0$. Then,

$ab = 0,\ a \neq 0 \Rightarrow ab = a.0$ & $a \neq 0$ [$\because$ $0 = a.0$]

$\Rightarrow b = 0$ [by left cancellation law]

Thus, $ab = 0$ and $a \neq 0 \Rightarrow b = 0.$

Similarly, $ab = 0$ and $b \neq 0 \Rightarrow a = 0.$

Consequently, $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0.$

Hence, R is without zero divisors.

Theorem 2: A field has no zero divisors.

Proof: Let R be a field. Then, it is a commutative ring with unity and every non-zero element in R has a multiplicative inverse.

Let $a,b \in R$ such that $ab = 0$ and if possible, let $a \neq 0$. Then, a^{-1} exists and therefore, in this case,

$ab = 0,\ a \neq 0 \Rightarrow a^{-1}(ab) = a^{-1}.0$

$\Rightarrow (a^{-1}a)b = 0$

$\Rightarrow eb = 0$

$\Rightarrow b = 0.$

Thus, ab = 0, a ≠ 0 ⇒ b = 0.

Similarly, ab = 0, b ≠ 0 ⇒ a = 0.

Hence, R is without zero divisors.

Remark: As a consequence of the above theorem, it follows that every field is an integral domain.

Theorem 3: A finite integral domain is a field.

Proof: Let D be a finite integral domain containing n elements.

Then, it is a commutative ring, with unity and without zero divisors. Let a be an arbitrary non-zero element of D.

Consider the set, $D^* = \{ax : x \in D \text{ and } x \neq 0\}$.

By closure property of multiplication on D and the fact that D is a ring without zero divisors, it follows that each element of D^* is a non-zero element of D.

More-over, $ax = ay, \ a \neq 0 \Rightarrow x = y$ [by cancellation law]

This shows that all the elements of D^* are distinct.

Consequently, D^* consists of all $(n-1)$ non-zero elements of D.

Now, D being a ring with unity, i.e. $1 \in D$.

So, one of the $(n-1)$ elements in D^* must coincide with 1.

i.e., $ax = 1$ for some $x \in D$

$\therefore \ a^{-1} = x \in D$ [$\because$ D being commutative, $ax = 1 \Rightarrow xa = 1$]

Thus, each non-zero element in D has its multiplicative inverse in D.

Hence, D is a field.

Theorem 4: A finite commutative ring without zero divisors is a field.

Proof: Let D be a finite commutative ring without zero divisors and let D contain n distinct elements. Let $0 \neq a \in D$.

Now, if $D^* = \{ax : x \neq 0\}$, then D^* consists of $(n-1)$ non-zero elements of D.

So, $ax = a$ for some $x \in D$. [$\because \ a \in D$]

But, $ax = a \Rightarrow ax = a.1 \Rightarrow x = 1 \in D$.

[$\because$ D has no zero divisors, so cancellation laws hold in D]

Now, since $1 \in D$, $ax' = 1$ for some $x' \in D$.

$\therefore$ $ax' = x'a = 1$ [$\because$ D is commutative].

So, $a^{-1} = x' \in D$

Thus, $1 \in D$ and each non-zero element in D has its multiplicative inverse in D.

Hence, D is a field.

Ex.1: If each element of a ring R is idempotent, show that R must be a commutative ring. What can you say about the converse?

Proof: Let R be a ring such that $x^2 = x \quad \forall\, x \in R$.

First we show that, $x + x = 0 \quad \forall\, x \in R$.

Now, $x \in R \Rightarrow (x + x) \in R \Rightarrow (x + x)^2 = (x + x)$.

Now, $(x + x)^2 = (x + x)$

$\Rightarrow$ $(x + x)(x + x) = (x + x)$

$\Rightarrow$ $(x + x)x + (x + x)x = (x + x)$ [by distributive law]

$\Rightarrow$ $(x^2 + x^2) + (x^2 + x^2) = (x + x)$ [by distributive law]

$\Rightarrow$ $(x + x) + (x + x) = (x + x) = (x + x) + 0$ [$\because$ $x^2 = x$]

$\Rightarrow$ $(x + x) = 0$.

Thus, $x + x = 0 \quad \forall\, x \in R$.

Now, let a and b be any arbitrary elements of R so that $a^2 = a$ and $b^2 = b$.

Also, $a \in R, b \in R \Rightarrow (a + b) \in R \Rightarrow (a + b)^2 = (a + b)$.

But, $(a + b)^2 = (a + b)$

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

$\Rightarrow$ $(a + b)a + (a + b)b = (a + b)$ [by distributive law]

$\Rightarrow$ $(a^2 + ba) + (ab + b^2) = (a + b)$ [by distributive law]

$\Rightarrow$ $(a + ba) + (ab + b) = (a + b)$

$\Rightarrow$ $(a + b) + (ba + ab) = (a + b) = (a + b) + 0$

[by commutativity & associativity of addition in R]

$\Rightarrow$ $ba + ab = 0$ [by cancellation law of addition]

$\Rightarrow$ $ba + ab = ba + ba$ [$\because$ $x + x = 0 \quad \forall\, x \in R$ & $ba \in R$]

$\Rightarrow$ $ab = ba$ [by left cancellation law of addition in R]

Hence, R is a commutative ring.

The converse of the above statement is not true, since the ring $\mathbb{Z}$ of all integers is a commutative ring but each of its elements is not idempotent.

Sub-ring: Let $(R, +, \times)$ be a ring. Then, a non-empty subset S of R is called a sub-ring of R, if S is stable for the compositions in R, and S itself is a ring with respect to the induced compositions.

If S is a sub-sing of R, then R is called an *over ring* of S.

Examples:

(i) $\mathbb{Z}$ is a sub-ring of $\mathbb{Q}$;

(ii) $\mathbb{Q}$ is a sub-ring of $\mathbb{R}$; and

(iii) $\mathbb{R}$ is a sub-ring of $\mathbb{C}$.

(iv) The set $S = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} : a, b, c \in \mathbb{Z} \right\}$ is a sub-ring of the ring M of all 2×2 matrices over $\mathbb{Z}$.

(v) The set of all real valued differentiable functions on [0,1] is a sub-ring of the ring of all real valued continuous functions on [0,1].

Remark: Every ring R has surely two sub-rings, namely R and {0}. These sub-rings are called trivial or improper sub-rings.
A sub-ring other than these sub-rings is called a proper sub-ring.

Results on Sub-rings of a ring

Theorem-1: The necessary and sufficient conditions for a non-empty subset S of a ring R to be a sub-ring there-of are that

$a \in S, \; b \in S \Rightarrow a - b \in S$ and $ab \in S \quad \forall\, a, b \in S$.

Proof: First suppose that S is a sub-ring of a ring R.

Then, $a \in S, \; b \in S \Rightarrow a \in S, \; -b \in S$

$\Rightarrow a + (-b) \in S \quad [\because$ S is stable for $+]$

$\Rightarrow a - b \in S$.

Also, $a \in S, \; b \in S \Rightarrow ab \in S \quad [\because$ S is stable for $\times]$.

Thus, $a \in S, \; b \in S \Rightarrow a - b \in S$ and $ab \in S$.

Again, let S be a non-empty sub-set of a ring R such that

$a \in S, \quad b \in S \quad \Rightarrow \quad a - b \in S \quad$ and $\quad ab \in S.$

Then, $\quad a \in S, \quad a \in S \quad \Rightarrow \quad a - a \in S \quad \Rightarrow \quad 0 \in S$;

$0 \in S, \quad a \in S \quad \Rightarrow \quad 0 - a \in S \quad \Rightarrow \quad -a \in S$;

$a \in S, \quad b \in S \quad \Rightarrow \quad a \in S, \; -b \in S$

$\Rightarrow \quad a - (-b) \in S \quad \Rightarrow \quad a + b \in S$;

And $\quad a \in S, \quad b \in S \quad \Rightarrow \quad ab \in S.$

This shows that S is stable for addition as well as multiplication; the additive identity exists in S and every element in S has its negative in S.

Also, $S \subseteq \mathbb{R}$. Now, since the commutativity of addition, the associativity of addition, the associativity of multiplication and the distributive laws hold in R, so they hold in S also.

Hence, S is a sub-ring of R.

Ideals: A sub-ring S of a ring R is called a

(i) **right ideal** of R, if $a \in S, \; r \in R \quad \Rightarrow \quad ar \in S$;

(ii) **left ideal** of R, if $a \in S, \; r \in R \quad \Rightarrow \quad ra \in S$;

(iii) **both sided idea** or simply an **ideal**, if S is a right ideal as well as a left ideal, i.e., if $a \in S, \; r \in R \Rightarrow ar \in S \;\&\; ra \in S$.

Examples:

i) Obviously, {0} and R are ideals of any ring R. These are referred to as 'trivial' or 'improper' ideals. All ideals of R, other than {0} and R are called proper ideals. A ring having no proper ideals is called a **simple ring**.

ii) Let m be an arbitrary but fixed positive integer and $S = \{ma : a \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the ring of all integers, then S is an ideal of $\mathbb{Z}$.

Non Examples:

i) $\mathbb{Z}$ is neither a left ideal nor a right ideal of $\mathbb{Q}$.

ii) $\mathbb{Q}$ is neither a left ideal nor a right ideal of $\mathbb{R}$.

iii) Let $\mathbb{R}$ be ring of all 2×2 matrices with their elements as integers. Let $S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathbb{Z} \right\}$. Then, S is a left ideal but not a right ideal of R.

iv) Let R be the ring of all 2×2 matrices with their elements as integers.

Let $S = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Z} \right\}$. Then, S is a right ideal but not a left ideal of R.

Remark: It is clear from the above definitions that the left ideal of a commutative ring is also the right ideal of the ring.

Theorem-1: The necessary and sufficient conditions for a non-empty subset of S of a ring R to be an ideal of R are :

(i) $a \in S, \ b \in S \Rightarrow a - b \in S$;

(ii) $a \in S, \ r \in R \Rightarrow ar \in S$ and $ra \in S$.

Proof: Let S be an ideal of a ring R. Then, S is a sub-ring of R. In particular, S is a subgroup of additive group of R.

So, $a \in S, \ b \in S \Rightarrow a - b \in S$.

Also, by definition of an ideal, $a \in S, r \in R \Rightarrow ar \in S$ and $ra \in S$.

Conversely, let S be a non-empty subset of a ring R such that conditions (i) and (ii) are satisfied.

Now, $a \in S, \ b \in S \Rightarrow a - b \in S$ [from (i)]

Also, $a \in S, \ b \in S \Rightarrow a \in S, \ b \in R \Rightarrow ab \in S$ [from (i)]

Thus, $a \in S, \ b \in S \Rightarrow a - b \in S$ & $ab \in S$. S is a sub-ring of R, satisfying (ii). Hence, S is an ideal of R.

Ex-1: We know that, $\mathbb{Z} \subset \mathbb{Q}$. Since the difference of two integers is an integer and the product of two integers is an integer, so $\mathbb{Z}$ is a sub-ring of $\mathbb{Q}$.

But, $\mathbb{Z}$ is neither a left ideal nor a right ideal of $\mathbb{Q}$.

Since, $a \in \mathbb{Z}, r \in \mathbb{Q}$ not necessarily implies that $ra \in \mathbb{Z}$ and $a \in \mathbb{Z}, r \in \mathbb{Q}$ not necessarily implies that $ar \in \mathbb{Z}$.

[For example, $3 \in \mathbb{Z}$ & $\frac{2}{5} \in \mathbb{Q}$ while neither $3.\frac{2}{5} \in \mathbb{Z}$ nor $\frac{2}{5}.3 \in \mathbb{Z}$]

Similarly, $\mathbb{Q}$ is a sub-ring of $\mathbb{R}$, but $\mathbb{Q}$ is neither a left ideal nor a right ideal of $\mathbb{R}$.

Ex-2: Let $\mathbb{R}$ be ring of all 2×2 matrices with their elements as integers.

Let $S = \{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathbb{Z} \}$.

Then, for any two matrices $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$ & $B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ in S,

$A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \in S$ $[\because (a_1 - a_2), (b_1 - b_2) \in \mathbb{Z}]$ and $AB = \begin{bmatrix} a_1a_2 & 0 \\ b_1b_2 & 0 \end{bmatrix} \in S$ $[\because a_1a_2, b_1b_2 \in \mathbb{Z}]$.

Thus, $A \in S, B \in S \Rightarrow A - B \in S$ & $AB \in S$;

So, S is a sub-ring of R.

More-over, if $A = \begin{bmatrix} p & 0 \\ q & 0 \end{bmatrix} \in S$ and $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$ be arbitrary, then $TA = \begin{bmatrix} ap + bq & 0 \\ cp + dq & 0 \end{bmatrix} \in S$ $[\because ap + bq , cp + dq \in \mathbb{Z}]$

Thus, $A \in S, T \in R \Rightarrow TA \in S$.

This shows that S is a left ideal of R. However, it is clear that $B = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \in S$ and $C = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} \in R$.

But, $BC = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 1 & 3 \end{bmatrix} \notin S$. This shows that S is not a right ideal of R. Hence, S is a left ideal but not a right ideal of R.

Ex-3: Let R be the ring of all 2×2 matrices with their elements as integers.

Let $S = \{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Z} \}$. Then, it is easy to verify that S is a right ideal but not a left ideal of R.

Ex-4: Let m be an arbitrary but fixed positive integer and $S = \{ma : a \in \mathbb{Z}\}$, where $\mathbb{Z}$ is the ring of all integers.

Then, for any two elements ma and mb of S, we have

$ma - mb = m(a - b) \in S$ $[\because a - b \in \mathbb{Z}]$ and

$ma \cdot mb = m(mab) \in S$ $[\because mab \in \mathbb{Z}]$

$\therefore$ S is a sub-ring of $\mathbb{Z}$.

Also, for arbitrary elements $ma \in S$ and $b \in \mathbb{Z}$, we have

$(ma)b = m(ab) \in S$ and $b(ma) = m(ba) \in S$.

Hence, S is a both sided ideal of $\mathbb{Z}$.

Theorem-1: Arbitrary intersection of ideals of a ring $R$is an ideal of R.

Proof: Let $\{S_\alpha : \alpha \in \Lambda\}$ be any collection of ideals of a ring R. Then, the intersection of any number of sub-rings being a sub-ring, it follows that $\cap\{S_\alpha : \alpha \in \Lambda\}$ is a sub-ring of R.

Now, $a \in \cap\{S_\alpha : \alpha \in \Lambda\}$ and $r \in R$

$\Rightarrow$ $a \in$ each S_α and $r \in R$

$\Rightarrow$ $ar \in$ each S_α and $ra \in$ each S_α [$\because$ each S_α is an ideal of R]

$\Rightarrow$ $ar \in \cap\{S_\alpha : \alpha \in \Lambda\}$ and $ra \in \cap\{S_\alpha : \alpha \in \Lambda\}$.

$\therefore$ $\cap\{S_\alpha : \alpha \in \Lambda\}$ is an ideal of R.

Theorem-2: Let M be a non-empty subset of a ring R, then the intersection of all ideals of R containing M is the smallest ideal of R containing M.

Proof: Let $\{S_\alpha : \alpha \in \Lambda\}$ be the collection of ideals of a R, each containing M.

Then, $\cap\{S_\alpha : \alpha \in \Lambda\}$ is clearly an ideal of R containing M.

Now, if S is any ideal of R containing M, then it is clearly a member of $\{S_\alpha : \alpha \in \Lambda\}$ and therefore, $\cap\{S_\alpha : \alpha \in \Lambda\} \subseteq S$.

Hence, $\cap\{S_\alpha : \alpha \in \Lambda\}$ is the smallest ideal of R containing M.

Remark: The smallest ideal of R containing M is called the **ideal** generated by M and it is denoted by (M).

Principal ideal: An ideal of a ring R, generated by a single element a of R, is called a **principal ideal** of the ring and we write, R = (a).

Examples:

i) The principal ideal generated by 0 is the ring $\{0\}$.

ii) The principal ideal generated by the unity element 1 is the ring R.

iii) Let $S = \{\cdots\cdots -3m, -2m, -m, 0, m, 2m, 3m, \cdots\cdots\}$be an ideal of the ring $\mathbb{Z} = \{\cdots\cdots -3, -2, -1, 0, 1, 2, 3, \cdots\cdots\}$. Then S is generated by the single integer m i.e. $S = (m)$. Therefore, S is a principal ideal of the ring $\mathbb{Z}$.

Principal ideal ring: A commutative ring R without zero divisors and with unity is called a principal ideal ring, if every ideal of R is a principal ideal.

Examples:

i) The commutative rings are examples of principal ideal rings.

ii) Every field is a principal ideal ring.

Maximal ideal: A non-zero ideal S of a ring R such that $S \neq R$ is called a maximal ideal of R, if there exists no proper ideal of R containing S.

Examples:

i) Consider the ring $\mathbb{Z}$ of integers:

$(2) = \{2x : x \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \cdots\cdots\cdots\}$

$(3) = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \pm 15, \cdots\cdots\cdots\}$

$(4) = \{0, \pm 4, \pm 8, \pm 12, \pm 16, \pm 20, \cdots\cdots\cdots\}$

$(5) = \{0, \pm 5, \pm 10, \pm 15, \pm 20, \pm 25, \cdots\cdots\cdots\}$

$(6) = \{0, \pm 6, \pm 12, \pm 18, \pm 24, \pm 30, \cdots\cdots\cdots\}$

Evidently $(6) \subseteq (2), (6) \subseteq (3)$

Hence if m is composite, say $m = ab$, then

$$(m) \subseteq (a), (m) \subseteq (b)$$

$(3), (5), (7)$ are maximal ideals of the ring of integers but (4) and (6) are not maximal ideal of the ring of integers.

Theorem-3: A field has no proper ideals.

Proof: Let S be a non-zero ideal of a field F and let a be an arbitrary non-zero element of S, then S being a subset of F,

$$a \in S \quad \Rightarrow \quad a \in F \quad \Rightarrow \quad a^{-1} \in F.$$

Now, S being an ideal of F,

$$a \in S, \; a^{-1} \in F \quad \Rightarrow \quad a.a^{-1} \in S \quad \Rightarrow \quad 1 \in S.$$

Now, let x be an arbitrary element of F. Then,

$$x \in F \quad \Rightarrow \quad 1.x \in S \quad \Rightarrow \quad x \in S$$

$[\because$ S being an ideal, $1 \in S, x \in F \Rightarrow 1.x \in S]$

This shows that each element of F is contained in S and therefore, $F \subseteq S$.

But $S \subseteq F$. So, $S = F$.

Thus, every non-zero ideal of the field F coincides with F and therefore, the only ideals of F are {0} and F.

Hence, a field has no proper ideals.

Theorem-4: If R is a commutative ring and $a \in R$, then $Ra = \{ra : r \in R\}$ is an ideal of R.

Proof: It is evident that every element of Ra is of the form ra, where $r \in R$ and by closure property of multiplication in R, each such element is contained in R. So, $Ra \subseteq R$.

Now, let r_1a and r_2a be any two elements of R a so that $r_1, r_2 \in R$.

$\therefore$ $r_1a - r_2a = (r_1 - r_2)\, a \in R$ a $[\because r_1 - r_2 \in R]$ and $(r_1a)\,(r_2a) = [(r_1a)\, r_2]\, a \in R$ a $[\because (r_1a)\, r_2 \in R]$

So, R a is a sub-ring of R.

More-over, if $r_1a \in R$ a and $r \in R$, then

$r\,(r_1a) = (r\, r_1)\, a \in R$ a $[\because r\, r_2 \in R]$ and

$(r_1a)\, r = (r_1r)\, a \in R$ a $[\because r_1r \in R]$

Hence, R a is an ideal of R.

Theorem-5: A commutative ring with unity is a field, if it has no proper ideals.

Proof: Let R be a commutative ring with unity having no proper ideals. i.e., the only ideals of R are {0} and R.

Now, let a be an arbitrary non-zero element of R.

Then, clearly R a is a non-zero ideal of R. Consequently, R a = R. Now, since $1 \in R$, it follows that $1 \in R$ a and therefore, 1 = ba for some $b \in R$.

And, since R is a commutative ring, so ab = 1.

Thus, $a^{-1} = b \in R$.

Accordingly, every non-zero element in R has its multiplicative inverse in R.

Hence, R is a field.

Theorem-6: Let R be a commutative ring with unity and let $a \in R$. Then, Ra is a principal ideal of R, generated by a.

Proof: It has already been shown that Ra is an ideal of R.

Also, $a \in Ra$ $[\because 1 \in R \Rightarrow 1.a \in Ra]$

Thus, Ra is an ideal of R containing a.

Now, let S be any ideal of R containing a.

Now, if $ra \in Ra$, then $r \in R$ and therefore,

$a \in S, r \in R \Rightarrow ra \in S$ [$\because$ S is an ideal containing a]

Consequently, $ra \in Ra \Rightarrow ra \in S$ and therefore, $Ra \subseteq S$.

Thus, Ra is contained in every ideal containing a and therefore, it is the smallest ideal containing a. Hence, Ra is the principal ideal, generated by a.

Theorem-7: The ring of integers is a principal ideal ring.

Proof: We know that $\mathbb{Z}$ is a commutative ring with unity. Now, in order to prove the required result, we must show that every ideal of $\mathbb{Z}$ is a principal ideal.

Let S be any ideal of $\mathbb{Z}$.

If $S = \{0\}$, then it is clearly a principal ideal.

If $S \neq \{0\}$, it must contain at least one non-zero integer a.

But, S being a sub-ring of $\mathbb{Z}$, $a \in S \Rightarrow -a \in S$.

Thus, S contains at least one positive integer.

Now, let s be the least positive integer in S.

As shown earlier, it is easy to verify that $\mathbb{Z}s$ is a principal ideal of $\mathbb{Z}$. We claim that $\mathbb{Z}s = S$.

Clearly, $\mathbb{Z}s \subseteq S$ [$\because as \in \mathbb{Z}s \Rightarrow a \in \mathbb{Z}, s \in S \Rightarrow as \in S$]

Again, let $n \in S$.

Then, by division algorithm, $\exists$ integers q and r such that $n = qs + r$, where $0 \leq r < s$

Now, $s \in S$, $q \in \mathbb{Z} \Rightarrow qs \in S$ [$\because$ S is an ideal of $\mathbb{R}$] and $n \in S$, $qs \in S \Rightarrow n - qs \in S \Rightarrow r \in S$ [$\because$ $n - qs = r$]

But, $0 \leq r < s$ and s is the least positive integer such that $s \in S$. Consequently, $r = 0$ and so $n = qs \in \mathbb{Z}s$. Thus, $n \in S \Rightarrow n \in \mathbb{Z}s$. $\therefore$ $S \subseteq \mathbb{Z}s$.

Thus, $\mathbb{Z}s = S$.

But, $\mathbb{Z}s$ being the principal ideal generated by s, it follows that every ideal of $\mathbb{Z}$ is a principal ideal.

Hence, $\mathbb{Z}$ is a principal ideal ring.

Theorem-8: Let S_1 and S_2 be any two ideals of a ring R, then $S_1 + S_2$ is the ideal generated by $S_1 \cup S_2$.

Proof: Clearly, $0 = 0 + 0 \in S_1 + S_2$. So, $S_1 + S_2 \neq \emptyset$.

Let, $a_1 + a_2$, $b_1 + b_2 \in S_1 + S_2$ so that $a_1, b_1 \in S_1$ & $a_2, b_2 \in S_2$. Then, $(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in S_1 + S_2$ and $(a_1 + a_2)(b_1 + b_2) = (a_1b_1 + a_1b_2 + a_2b_1 + a_2b_2)$

$= (a_1b_1 + a_1b_2) + (a_2b_1 + a_2b_2) \in S_1 + S_2$

[$\because$ S_1 being an ideal, $a_1 \in S_1$, $b_2 \in S_2 \Rightarrow a_1 \in S_1$, $b_2 \in \mathbb{R} \Rightarrow a_1b_2 \in S_1$ and similarly, $a_2b_1 \in S_2$]

More-over, each element of $S_1 + S_2$ is of the form $r_1 + r_2$, where $r_1 \in S_1$ and $r_2 \in S_2$.

But, $r_1 \in S_1$ and $r_2 \in S_2 \Rightarrow r_1, r_2 \in R \Rightarrow r_1 + r_2 \in R$.

$S_1 + S_2 \subseteq R$. Consequently, $S_1 + S_2$ is a sub-ring of R.

Now, if $a_1 + a_2 \in S_1 + S_2$, then $a_1 \in S_1$ and $a_2 \in S_2$.

So, for an arbitrary $r \in R$, we have

$r(a_1 + a_2) = ra_1 + ra_2 \in S_1 + S_2$ and $(a_1 + a_2)r = a_1r + a_2r \in S_1 + S_2$.

$\therefore$ $S_1 + S_2$ is an ideal of R.

Now, $S_1 \subseteq S_1 + S_2$, since $a_1 \in S_1 \Rightarrow a_1 = a_1 + 0 \in S_1 + S_2$. Similarly, $S_2 \subseteq S_1 + S_2$.

$\therefore$ $S_1 \cup S_2 \subseteq S_1 + S_2$.

Thus, $S_1 + S_2$ is an ideal containing $S_1 \cup S_2$.

Now, if $\mathbb{R}$ is an ideal containing $S_1 \cup S_2$, then $\mathbb{R}$ contains each element of S_1 as well as that of S_2 and it being an ideal, it will contain each element of $S_1 + S_2$.

Consequently, $S_1 + S_2$ is the smallest ideal containing $S_1 \cup S_2$.

Hence, $S_1 + S_2 = \{S_1 \cup S_2\}$.

Prime ideal: An ideal S of a ring $\mathbb{R}$ is said to be a prime ideal of $\mathbb{R}$, if $ab \in S \Rightarrow a \in S$ or $b \in S$.

Examples:

i) In the ring $\mathbb{Z}$ of integers, the ideal $\mathbb{Z}p$, generated by $p \in \mathbb{Z}$ is a prime ideal iff p is a prime, for, if p is prime, then $ab \in \mathbb{Z}p \Leftrightarrow p \mid ab \Leftrightarrow p \mid a$ or $p \mid b$ [$\because$ p is prime] $\Leftrightarrow a \in \mathbb{Z}p$ or $b \in \mathbb{Z}p$.

ii) In the ring $\mathbb{Z}$ of integers, $S = \{3r : r \in \mathbb{Z}\}$ is a prime ideal of R generated by 3 and we write $S = (3)$.

Here, $ab \in S \Rightarrow 3|ab$

$\Rightarrow 3|a$ or $3|b$ as 3 is prime

$\Rightarrow a \in S$ or $b \in S$

$\Rightarrow S$ is prime

Similarly, $(5), (7), (11)$ etc. are examples of prime ideals. Therefore, the set $\{mr : r \in \mathbb{Z}\}$ is a prime ideal of the ring of integers for every prime integer m.

Non Examples:

i) The ideal $\{4r : r \in \mathbb{Z}\} = (4)$ is not prime.

For $ab \in (4) \Rightarrow 4|ab$. Again, since 4 is a composite integer, it does not imply $4|a$ or $4|b$

$\Rightarrow a \in (4)$ or $b \in (4)$

Hence $ab \in (4)$ does not imply $a \in (4)$ or $b \in (4)$.

Therefore, (4) is not prime.

For example, $6.2 \in (4)$ but neither 6 nor 2 belongs to (4).

Theorem-9: Let S be an ideal of a commutative ring $\mathbb{R}$ with unity. Then, $\mathbb{R}/S$ is an integral domain, if and only if S is a prime ideal of $\mathbb{R}$.

Proof: Since S is an ideal of a commutative ring $\mathbb{R}$ with unity, so $\mathbb{R}/S$ is also a commutative ring with unity.

Now, first suppose that S is a prime ideal. Then,

$(S+a)(S+b) = S \Rightarrow S+ab = S \Rightarrow ab \in S \Rightarrow a \in S$ or $b \in S$ [$\because$ S is prime] $\Rightarrow S+a = S$ or $S+b = S$.

This shows that $\mathbb{R}/S$ is without zero divisors and hence it is an integral domain.

Again, suppose that $(S+a)(S+b) = S \Rightarrow S+a = S$ or $S+b = S$. Then, $S+ab = S \Rightarrow S+a = S$ or $S+b = S$.

i.e., $ab \in S \Rightarrow a \in S$ or $b \in S$.

This proves that S is prime.

Theorem-10: If $\mathbb{R}$ is a commutative ring with unity, then every maximal ideal of $\mathbb{R}$ is a prime ideal.

Proof: Let S be a maximal ideal of a commutative ring $\mathbb{R}$ with unity.

Then, $\mathbb{R}/S$ is a field and therefore, an integral domain.

Hence, by the preceding theorem (**Theorem-9**), it follows that S is a prime ideal.

****