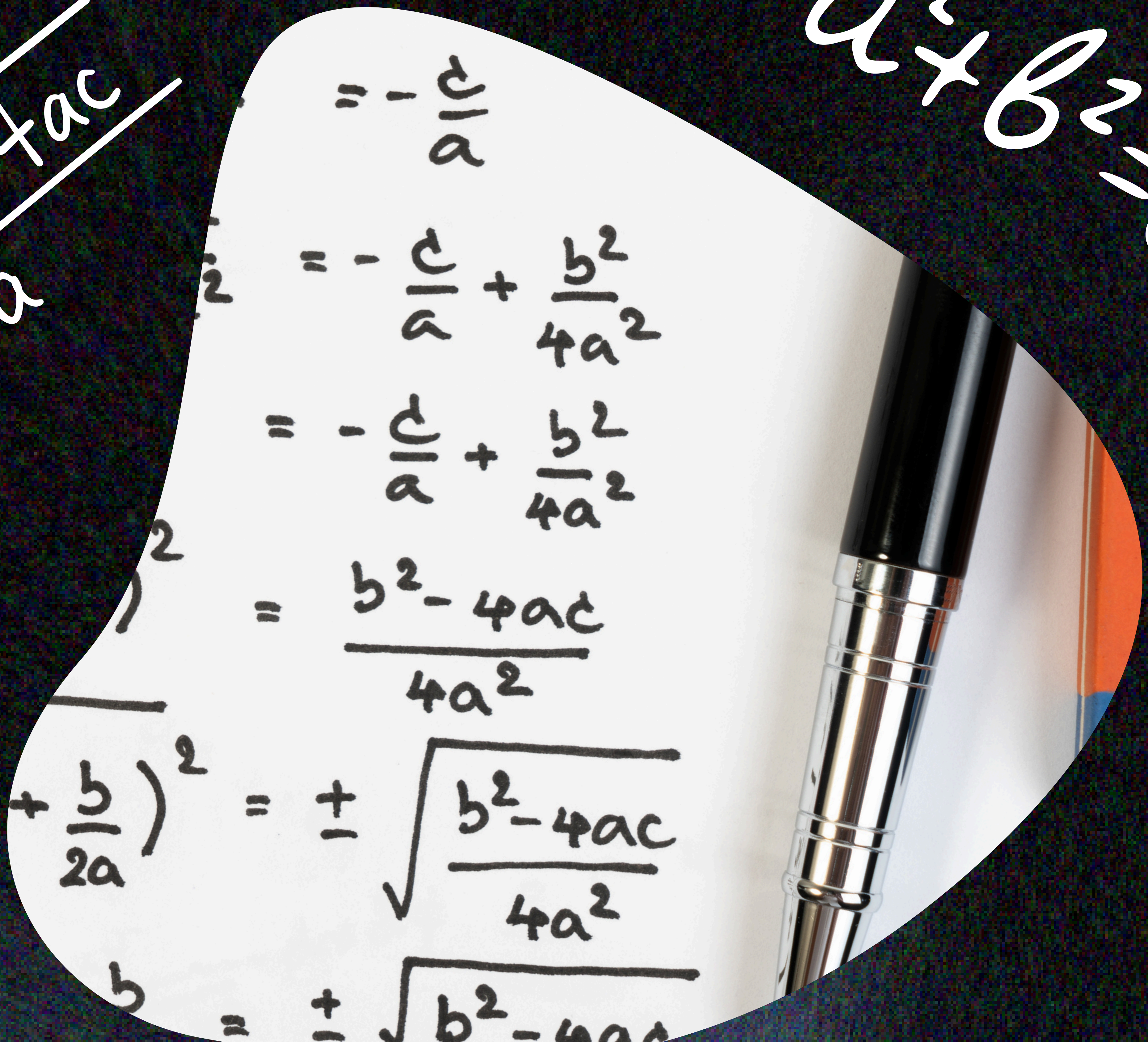
Advanced Modern Algebra

For University Students

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$a^2 + b^2 = c^2$$



Notes

Written BY: Muhibb Ali Raza

Set :-

A collection of well-defined and distinct objects is called set.

Well defined mean that one can easily understand which element belong to set and which element does't.

Distinct mean that an element comes only once in a set.

Number System :-

(i) **Natural Number :-**

$$\mathbb{N} = \{1, 2, 3, \ldots\ldots\}$$

(ii) **Whole Number :-**

$$W = \{0, 1, 2, 3, \ldots\ldots\}$$

(iii) **Integers :-**

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\ldots\}$$

(iv) **Rational Number :-**

The rational number are those number which can be expressed as ratio between two integers.

i.e. $\mathbb{Q} = \{p/q \; ; \; p, q \in \mathbb{Z} \text{ and } q \neq 0\}$

(v) **Real Number :-**

Real number are those number those square is always positive.

(vi) **Complex Number :-**

$$\mathbb{C} = \{a + ib \; ; \; a, b \in \mathbb{R}\}$$

where, $i = \sqrt{-1}$

→ $\boxed{\mathbb{N} \subset W \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}}$

Cartesian Product :-

For two non-empty sets A and B, cartesian is denoted and defined as :

$$A \times B = \{(a,b) \; ; \; a \in A, b \in B\}$$

Binary Relation :-

Any subset of $A \times B$ is called binary relation. from A to B.

i.e. if r is binary relation from A to B, then, $r \subseteq A \times B$ and we write $r : A \rightarrow B$.

Domain :-

let, r be a binary relation from A to B, then domain of r is the set of all first element of ordered pair of r, denoted by Dom r.

Range :-

let, r be a binary relation from A to B, then, range of r is the set of all second elements of ordered pair of r, denoted by Range r.

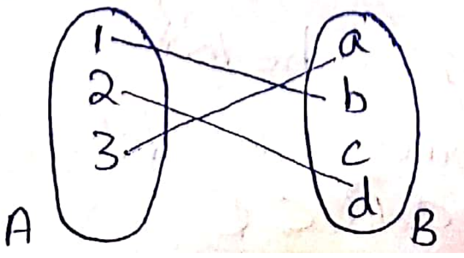
Function :-

A relation of $f : A \rightarrow B$ is said to be a function, if

(i) Dom $f = A$

(ii) first element of ordered pair of f is not repeated.

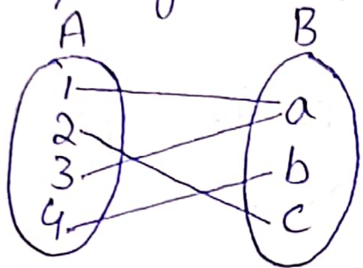
e.g.



Onto Function :-

Let, $f : A \rightarrow B$ be a function, then f is said to be onto/surjective function if Range $f = B$.

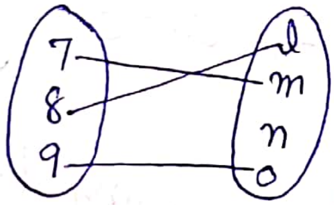
e.g.



One-One Function :-

Let, $f : A \rightarrow B$ be a function, then f is said to be one-one/injective function if different element of A have different images in B.

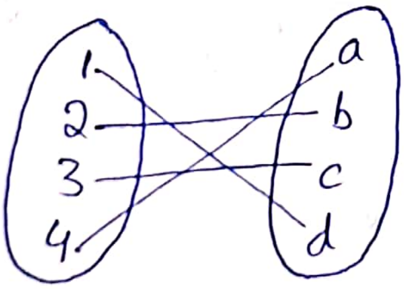
e.g.



Bijective Function :-

Let, $f : A \rightarrow B$ be a function, then, f is said to be bijective function if f is one-one and onto.

e.g.



Relation :-

Let, $A \neq \phi$ be a set and $r \subseteq A \times A$, then r is a relation on set A.

Reflexive Relation :-

A relation r on set A is reflexive relation if $\forall$ $a \in A$ we have $a r a$.

Symmetric Relation :-

A relation r on set A is symmetric relation if whenever $a r b \Rightarrow b r a$ for $a, b \in A$.

Transitive Relation :-

A relation r on set A is transitive relation if whenever $a r b$ and $b r c \Rightarrow a r c$ for $a, b, c \in A$.

Equivalence Relation :-

If a relation is reflexive, symmetric and transitive, then it is called equivalence relation.

Partition :-

Let, $A_1, A_2, \ldots, A_n$ be non-empty subsets of A. Then $A_i (i^n)$ are said to be partition of A if

(i) $\bigcup_{i=1}^{n} A_i = A$

(ii) $A_i \cap A_j = \phi \quad \forall\, i, j$

Equivalence Class :-

An important features of equivalence relation on a set A is that it partitions A into its subsets. These disjoint subset of A are called equivalence class.

Equivalence class determine by a is usully denoted (3) by $[a]$ or, $\bar{a}$, i.e,

$\bar{a} = [a] = \{x \in A ; a \sim x\}$

If C is an equivalence class of any element, then any element of class C is called representative of C.

Quotient Set :-

A quotient set is a set derived from another by equivalence relation.

Let, A be a set and let "$\sim$" be an equivalence relation. The set of equivalence classes of A with respect to "$\sim$" is called quotient of A by "$\sim$". It is denoted by $A/\sim$. (read as "A module $\sim$")

i.e. $A/\sim = \{C_1, C_2, C_3\}$

where, C_1, C_2, C_3 are equivalence classes of A.

The mapping from A to equivalence classes of A i.e. $\phi : A \rightarrow A/\sim$ is surjective.

The mapping $\phi : A \rightarrow A/\sim$ is defined by

$\phi(a) = [a]$ for $a \in A$

where, $[a]$ is equivalence classes of A.

Divisblity :-

let, $a, b \in \mathbb{Z}$, we say that "a" divides "b" if $\exists$ an integer $c \in \mathbb{Z}$, such that,

$$b = ac$$

then, a is called divisor or, factor of b and b is called multiple of a.

Symbolically, it can be written as,

$a|b$ and read as "a" divides "b".

If a does't divides b, then, we write it as $a \nmid b$.

Prime Number :-

A number p is said to be a prime number if it has only two divisor.

e.g. 2, 3, 5, 7, ...

Prime Factorization Theorem :-

This theorem states that "every integer, $n > 1$ can be written uniquely as product of primes."

i.e. $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots\cdots p_n^{\alpha_n}$

Greatest Common Divisor :-

Suppose, the prime factorization of a is

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots\cdots\cdots p_n^{\alpha_n}$$

and, prime factorization of b is

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot p_3^{\beta_3} \cdots\cdots\cdots p_n^{\beta_n}$$

then, the gretest common divisor of a and b is

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots\cdots\cdots p_n^{\min(\alpha_n, \beta_n)}$$

Relatively Prime :-

The two numbers are said to be coprime or, relatively prime if thier gretest common divisor is equal to 1. e.g 2 and 3 are coprime.

Least Common Divisor :-

Suppose, the prime factorization of a is $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_n^{\alpha_n}$ and b is $p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots\cdots p_n^{\beta_n}$, then least common divisor of 'a' and 'b' is

$$lcm(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdots\cdots p_n^{\max(\alpha_n,\beta_n)}$$

Remarks :-

(i) $gcd(a,b) \times lcm(a,b) = ab$

(ii) $lcm(a,b) = ab$ if and only if a, b are coprime.

Example :-

Suppose, we have given two numbers $a = 12$ and $b = 40$, then, thier prime factorization is

$$12 = 2^2 . 3^1 . 5^0$$
$$40 = 2^3 . 3^0 . 5^1$$

then,

$$gcd(12,40) = 2^{\min(2,3)} . 3^{\min(0,1)} . 5^{\min(0,1)}$$
$$= 2^2 . 3^0 . 5^0 = 4$$

and,

$$lcm(12,40) = 2^{\max(2,3)} . 3^{\max(0,1)} . 5^{\max(0,1)}$$
$$= 2^3 . 3^1 . 5^1 = 120$$

Integers Module n :-

Define a relation "$\sim$" on $\mathbb{Z}$ by $a \sim b$, $a, b \in \mathbb{Z}$ if and only if

$$n \mid b-a$$

where, $a, b \in \mathbb{Z}$ and n is fixed positive integer.

Theorem :-

The relation "$\sim$" is an equivalence relation.

Proof :-

(i) Let, $a \in \mathbb{Z}$, then, $n / a-a \Rightarrow n/0$ and $0 \in \mathbb{Z}$

Hence, $a \sim a$

$\Rightarrow$ "$\sim$" is reflexive.

(ii) Let, $a \sim b$ for $a, b \in \mathbb{Z}$, then $n / b-a$

$\Rightarrow n / -(a-b) \Rightarrow n \mid a-b \Rightarrow b \sim a$

$\Rightarrow$ "$\sim$" is symmetric.

(iii) Let,

$a \sim b \Rightarrow n / b-a$ $\quad a, b \in \mathbb{Z}$

and,

$b \sim c \Rightarrow n \mid c-b$ $\quad b, c \in \mathbb{Z}$

then,

$n \mid (b-a)+(c-b) \Rightarrow n \mid c-a \Rightarrow a \sim c$

$\Rightarrow$ "$\sim$" is transitive.

Hence, "$\sim$" is equivalence relation.

Congurent :-

Let, $a, b \in \mathbb{Z}$, and n be a fixed positive integer then, a is congurent to b if and only if $n \mid b-a$.

We can write it as,

$$a \equiv_n b$$

Congruence Class :-

A congruence class $\bar{a}$ or $[a]$ is the set of all integers that have same remainder as "a", when divided by n. (n is fixed positive integer)

$$\bar{a} = [a] = \{a + kn \; ; \; k \in \mathbb{Z}\}$$

$$= \{a, a \pm n, a \pm 2n, a \pm 3n, \ldots\ldots\}$$

Example :-

(i) if we fixed $n = 3$, then congruence classes are

$$\bar{0} = \{\ldots\ldots, -3, 0, 3, 6, 9, \ldots\ldots\}$$

$$\bar{1} = \{\ldots\ldots, -2, 1, 4, 7, \ldots\ldots\}$$

$$\bar{2} = \{\ldots\ldots, -1, 2, 5, 8, 11, \ldots\ldots\}$$

(ii) The congurence classes of integers module n is

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ldots, \overline{n-1}\}$$

Note that,

If $\bar{a}, \bar{b} \in \mathbb{Z}_n$, then

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Binary Operation :-

Let, $X \neq \Phi$ be a set. The $*$ is said to be binary operation on X if

$$* : X \times X \longrightarrow X \quad \text{is a function.}$$

Then for each, $(x_1, x_2) \in X \times X \Rightarrow *(x_1, x_2) \in X$

In our next discussion, instead of writting $*(x_1, x_2)$, we will write $x_1 * x_2$.

If $*$ is binary operation on X, then $*$ is unique and this uniqueness is considered as well defined. We also claim that $(X, *)$ is closed.

For example,

$(\mathbb{N}, +), (\mathbb{N}, \cdot), (\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Z}, -)$ are all closed, But $(\mathbb{N}, -), (\mathbb{Z}, \div)$ are not closed.

Group :-

A set $G \neq \Phi$ is said to be group under binary operation $*$ if

(i) $(G, *)$ is closed.

(ii) $(G, *)$ is associative.

(iii) Identity element exists under $*$.

(iv) Inverse of each element under $*$ exists.

i.e. $\forall a \in G \ \exists \ b \in G$ such that

$$a * b = b * a = e \quad \text{(identity)}$$

Abelian group :-

A group G is said to be abelian group iff $*$ is commutative in G.

Examples :-

(i) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ are abelian group.

(ii) $(\mathbb{Q}\setminus\{0\},\cdot)$ and $(\mathbb{R}-\{0\},\cdot)$ are abelian group.

(iii) $\mathbb{Z}_n-\{0\}=\{\bar{a}\in\mathbb{Z}_n;(a,n)=1\}$ is abelian group.

(iv) $(\mathbb{Z}_n,+)$ is abelian group.

(v) The set $M_{n\times n}$ of all $n\times n$ non-singular matrices forms non-abelian group under "$\circ$".

(vi) The set $M_{m\times n}$ of all $m\times n$ order forms an abelian group under "$+$".

(vii) let, $G=\{\pm 1,\pm i\}$, then, $(G,\cdot)$ is abelian group.

Composition of function :-

let, $f:X\to Y$ and $g:Y\to Z$, then, thier composite $g\circ f:X\to Z$ is defined by

$$(g\circ f)(x)=g(f(x)) \qquad \forall\, x\in X$$

Composition is associative, i.e. if $h:Z\to W$, then,

$$h\circ(g\circ f)=(h\circ g)\circ f$$

Indeed,

$$(h\circ(g\circ f))(x)=h(g(f(x)))=((h\circ g)\circ f)(x) \quad \forall\, x\in X.$$

In particular, if X is a set, then, $\circ$ is an associative binary operation on set of all function $f:X\to X$.

Moreover, this function has an identity. The identity function, $I_X : X \to X$ is defined by

$$I_X(x) = x \quad \forall\ x \in X$$

Then, $I_X \circ f = f = f \circ I_X \quad \forall\ f : X \to X$.

Hence, we say that a function $f' : X \to X$ is an inverse of $f : X \to X$ if

$$f' \circ f = I_X = f \circ f'$$

equivalently, if $f'(f(x)) = x = f(f'(x)) \quad \forall\ x \in X$.

This inverse is unique when it exists.

For if f'' is another inverse of f, then

$$f' = f' \circ I_X = f' \circ (f \circ f'') = (f' \circ f) \circ f'' = I_X \circ f'' = f''$$

When it exists, the inverse of f is denoted by f^{-1}.

Example :-

A translation of plane $\mathbb{R}^2$ in the direction of vectors (a, b) is a function $f : \mathbb{R}^2 \to \mathbb{R}^2$ defined by

$$f(x, y) = (x + a, y + b)$$

The composition of this translation with translation g in direction of (c, d) is function $f \circ g : \mathbb{R}^2 \to \mathbb{R}^2$, where

$$f \circ g(x, y) = f(g(x, y)) = f(x + c, y + d) = (x + c + a, y + d + b)$$

This is translation in direction of $(c + a, d + b)$.

It can easily be verified that set of all translation in $\mathbb{R}^2$ forms an abelian group under composition.

The identity is the identity transformation

$$I_{\mathbb{R}^2} : \mathbb{R}^2 \to \mathbb{R}^2$$

Scanned with CamScanner

The inverse of the translation in the direction (a, b) is the translation in opposite direction $(-a, -b)$.

Symmetric Group :-

If $S(X)$ is the set of bijection from any set X to itself, then, $(S(X), \circ)$ is group under composition. This group is called symmetric group or, permutation group of X.

Since, the composition of two bijection is a bijection thus, $S(X)$ is closed under composition. The composition of function is always associative and identity of $S(X)$ is the identity function $I_X : X \to X$. Also, any bijection function $f \in S(X)$ has an inverse $f^{-1} \in S(X)$.

Therefore, $S(X)$ satisfies all axioms of group.

Since, the composition of function is not generally commutative, i.e. $(f \circ g(x) \neq g \circ f(x))$, $S(X)$ is not usually an abelian group.

Example :-

If $X = \{a, b\}$ is two element set, the only bijection from X to itself are identity I_X and the symmetry $f : X \to X$, defined by $f(a) = b$ and $f(b) = a$

The symmetry group of X is

$S(X) = \{I_X, f\}$

$\circ$	I_X	f
I_X	I_X	f
f	f	I_X

symmetry group of $\{a, b\}$.

Example:-

Consider the element f and g in the permutation group of $\{1,2,3\}$.

where,

$f(1)=2,\ f(2)=3,\ f(3)=1$ and $g(1)=1,\ g(2)=3,\ g(3)=2$

Then, $\{1,2,3\}$ forms non-abelian group under composition $\circ$.

Example:-

A non-singular linear transformation of plane is a bijective function of form $f: \mathbb{R}^2 \to \mathbb{R}^2$,

where,

$$f(x,y) = (a_{11}x + a_{12}y,\ a_{21}x + a_{22}y)$$

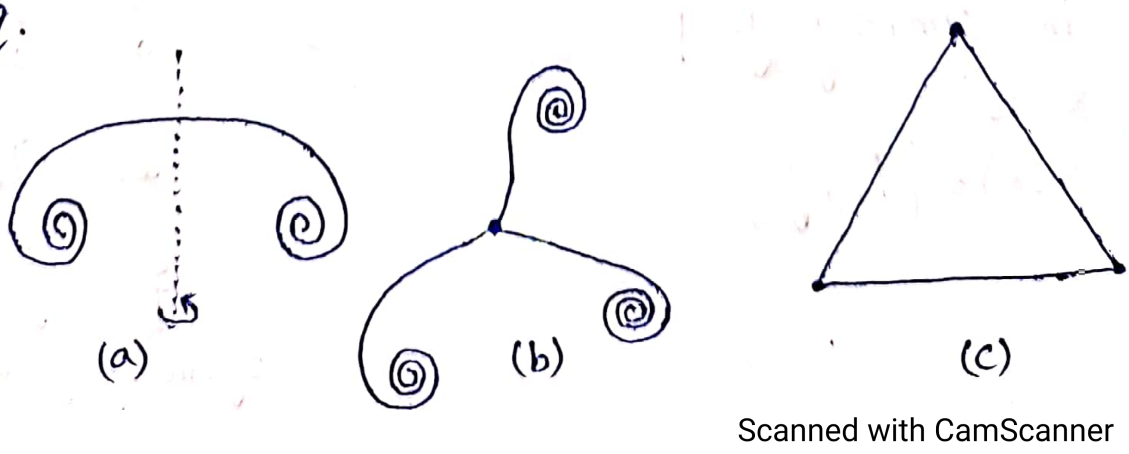
with determinant, $a_{11}a_{22} - a_{12}a_{21} \neq 0$.

The set of all non-singular linear transformation L, forms a non-abelian group, $(L, \circ)$.

Symmetry or, Isometry :-

If F is a figure in plane or in space, a symmetry of figure F is a bijection $f: F \to F$, which preserve distance, i.e. $\forall\ p, q \in F$, the distance from $f(p)$ to $f(q)$ must be same as distance from p to q.

e.g.



(a) (b) (c)

The figure (a) has two symmetries, the identity and a half turn about a vertical axis, called an axis of symmetry.

The figure (b) has 3 symmetries, the identity and rotation of one-third and two-third of revolution about its centre.

Proper Symmetry :-

The rotation can be performed as a physical motion within the plane of object. It is called proper symmetry.

Improper Symmetry :-

The reflection can only be accomplished as physical motion by moving the objects outside the plane. It is called improper symmetry.

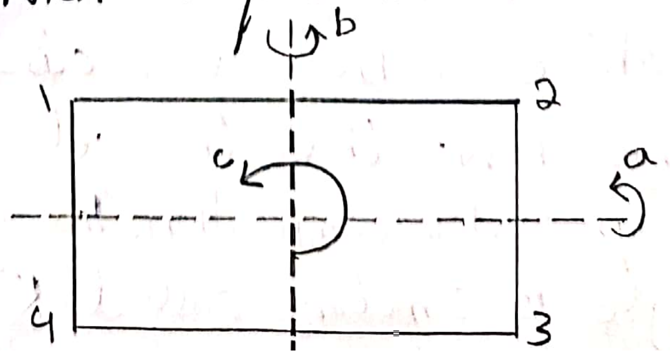
The figure (c) has 6 symmetrices which is obtained by moving the triangle within the plane and moving outside the plane.

Example :-

Write down table for group of symmetrices of rectangle with unequal sides.

Solution :-

symmetries of rectangle



The improper symmetries obtained by reflecting the rectangle in horizontal axis through centre, denoted by "a". Then,

$a(1)=4$, $a(2)=3$, $a(3)=2$, $a(4)=1$

There is a similiar symmetry "b" obtained by reflecting the rectangle in vertical axis, Then,

$b(1)=2$, $b(2)=1$, $b(3)=4$, $b(4)=3$

A third symmetry "c" is obtained by rotating the rectangle in its plane through half a revoulation about its centre.

$c(1)=3$, $c(2)=4$, $c(3)=1$, $c(4)=2$

The table of symmetry group of a rectangle is

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Here, $e.a=a.e=a$, $e.b=b.e=b$, $c.e=e.c=c$
and, $a^2=b^2=c^2=e$, $ab=ba$, $ac=ca$, $bc=cb$.
Further, $ab=c$, $bc=a$, $ca=b$.

All this shows that the set $\{e,a,b,c\}$ forms abelian group under composition. This group of symmetries of rectangle is sometime called <u>Klien 4-group.</u> (K_4)

Proposition :-

Let, $*$ be an binary operation on set S, that has identity e. Then if an element a has an inverse, this inverse is unique.

Proof :-

Suppose, b and c are inverse of a.

Thus, $a*b = b*a = e$ and $a*c = c*a = e$

Now, since, $*$ is associative and e is an identity

So, $b = b*e = b*(a*c) = (b*a)*c = e*c$

$\Rightarrow b = c$

$\Rightarrow$ Inverse is unique.

Proposition :-

If a, b and c are element of group G, Then,

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

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

(iii) $ab = ac$ or $ba = ca \Rightarrow b = c$ (cancellation law)

Proof :-

(i) Let, $a \in G$, Since, G is group, So, $a^{-1} \in G$

Now, $a * a^{-1} = e$ and $a^{-1} * a = e$

We know that inverse is unique, Hence,

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

(ii) Let,

$(ab)(b^{-1}a^{-1}) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$

and, $(b^{-1}a^{-1})(ab) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$

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

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

(iii)

Suppose, $ab = ac$, then, $a^{-1}(ab) = a^{-1}(ac)$

So, $(a^{-1}a)b = (a^{-1}a)c$

$eb = ec \Rightarrow b = c$

Now, suppose, $ba = ca$, then, $(ba)a^{-1} = (ca)a^{-1}$

So, $b(aa^{-1}) = c(aa^{-1})$

$be = ce \Rightarrow b = c$

Hence, proved.

Subgroup :-

If $(G, .)$ is a group and $H \neq \phi$ is a subset of G, then, $(H, .)$ is called a subgroup of $(G, .)$ if following condition hold:

(i) $a.b \in H \quad \forall \; a, b \in H$ (closure property)

(ii) $a^{-1} \in H \quad \forall \; a \in H$ (existence of inverse)

Proposition :-

If H is a subgroup of $(G, .)$, then, $(H, .)$ is also a group.

Proof :-

If H is a subgroup of $(G, .)$, we show that $(H, .)$ satifies all group axioms.

By defination of subgroup, H is closed under "."

i.e. "." is a binary operation on H.

If $a, b, c \in H \subseteq G$,

$(a.b).c = a.(b.c)$ in $(G, .)$

and hence, $(a.b).c = a.(b.c)$ in $H \subseteq G$.
Since, $h \neq \phi$, So, it contain atleast one element, say $h \in H$
Now,

$$h^{-1} \in H \quad \text{(by defination of subgroup)}$$

Then,

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

By defination of subgroup, $(H, .)$ contains inverse.
Therefore, $(H, .)$ satisfies all axioms of group.

Propasition :-

If $H \neq \phi$ is a finite subset of group G and $ab \in H$ for $\forall\, a, b \in H$, then H is subgroup of G.

Proof :-

We have to show that for each element $a \in H$, its inverse is also in H.

All elements, $a, a^2 = a.a, a^3 = a.a.a, \ldots\ldots$ belong to H, So, since H is finite, these cannot all be distinct. Therefore,

$$a^i = a^j \quad \text{for some } 1 \leq i < j$$

By cancelling a^i, we obtain

$$e = a^{j-i} \quad \text{where, } j-i > 0$$

Therefore, $e \in H$ and this equation can be written as

$$e = a(a^{j-i-1}) = (a^{j-i-1})a$$

Hence,

$$a^{-1} = a^{j-i-1}$$

Which belongs to H, since $j-i-1 \geq 0$.

Examples:-

(i) In the group $(\{\pm 1, \pm i\}, \cdot)$, the subset $\{\pm 1\}$ forms a subgroup because this subsets is closed under multiplication.

(ii) The set $\mathbb{N} = \{0, 1, 2, \ldots\ldots\}$ is a subset of $\mathbb{Z}$, but not a subgroup, because inverse of 1 which is -1 is not in $\mathbb{N}$.

(iii) The group $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$, $\mathbb{Q}$ is subgroup of $\mathbb{R}$ and $\mathbb{R}$ is a subgroup of $\mathbb{C}$. Remember that addition is the operation in all these group.

Example:-

Draw the poset diagram of subgroup of the group of symmetries of rectangle.

Solution:-

The group of symmetries of rectangle is

$$V_4 = K_4 = \{e, a, b, c\}$$

We see that "$\circ$" is a binary operation on $\{e, a\}$, thus, $\{e, a\}$ is a subgroup. Also, $\{e, b\}$ and $\{e, c\}$ are subgroup. If a subgroup contain a and b, it must contain $a \circ b = c$, so it is whole group. Similarly, subgroups containing a and c or, b and c must be whole group. The poset diagram of subgroup is given as:

$$\begin{tikzcd}
 & \{e, a, b, c\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{e, a\} \arrow[dr, dash] & \{e, b\} \arrow[d, dash] & \{e, c\} \arrow[dl, dash] \\
 & \{e\} &
\end{tikzcd}$$

Order of group :-

The number of element in a group G is called order of group. It is denoted by $|G|$, or $O(G)$.

Finite and Infinite group :-

G is called finite group if $|G|$ is finite. If $|G|$ is infinite, then, it is called infinite group.

e.g.

The Klein group $K_4 = V_4 = \{e, a, b, c\}$ is finite group and order of this group is 4.

$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ are infinite group.

Order of an Element :-

let, G be a group and g be an element of G then, a least positive integer "n" is called order of g for which $a^n = e$.

Then, we can write, $O(g) = |g| = n$

If no such "n" exists, then the order of "a" is infinite.

Cyclic group :-

→ A group G is said to be cyclic if it is generated by a single element "g".

→ A group $(G, \cdot)$ is said to be cylic if $\exists$ an element $g \in G$, such that:

$$G = \{ g^n \mid n \in \mathbb{Z} \}$$

→ A group $(G, +)$ is said to be cylic if $G = \{ ng \mid n \in \mathbb{Z} \}$ for some $g \in G$.

The cyclic group is denoted by, $G = <g>$ and g is called generator of group G.

Examples :-

(i) The group $(\{\pm 1, \pm i\}, \cdot)$ is cyclic group of order 4 generated by "i", because

$i^4 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = -i$ and so on.

(ii) The group $G = (\mathbb{Z}, +)$, then $G = <1>$ or, $<-1>$.

The group $(\{\pm 1, \pm i\}, \cdot)$ has order 4, the identity 1 has order 1, -1 has order 2 because $(-1)^2 = 1$, i and $-i$ has order 4.

Proposition :-

Let, g be an element of order r in a group, then for $k \in \mathbb{Z}$, $g^k = e$ if and only if r divides k.

Proof :-

Suppose, that r divides k, then $\exists$ a positive fixed integer "m" such that

$$k = rm \quad , \quad m \in \mathbb{Z}, \ m \text{ is fixed}$$

Then,

$$g^k = (g^r)^m = e^m = e$$

Conversely,

Suppose that $g^k = e$, then, we have to show that r divides k.

Consider, the division algorithm

$$k = qr + s \quad \text{where, } q, s \in \mathbb{Z}, \quad 0 \leq s < r$$

Now,

$$g^k = g^{qr+s} = g^{qr} \cdot g^s = (g^r)^q \cdot g^s$$
$$= (e)^q \cdot g^s = e \cdot g^s = g^s$$

$\Rightarrow g^k = g^s$

$\Rightarrow k = s$

Now, if $0 < s < r$, then, $o(g) \neq s$, which is contradiction.

So, $s = 0$

and, $k = qr + s = qr$

$\Rightarrow$ "r" divides "k" which is required.

Hence, proved.

Proposition :-

Every subgroup of a cyclic group is cyclic.

Proof :-

Suppose that G is cyclic with generator "g" and $H \subseteq G$ is a subgroup.

If $H = \{e\}$, it is cyclic with generator "e".

let, $g^k \in H$ with $k \neq 0$. Since $g^{-k} = (g^k)^{-1} \in H$, we have $g^m \in H$ for $m > 0$ and we choose m to be the smallest such positive integer.

Write $h = g^m$, we claim that h generates H. Certainly, $h^k \in H$ for some $k \in \mathbb{Z}$, because $h \in H$. We must show that every element a in H is a power of h. Since, $a \in G$, we have $a = g^s$; $s \in \mathbb{Z}$

By division algorithm, write

$$s = qm + r \qquad 0 \le r < m$$

Now,

$$a = g^s = g^{qm+r} = (g^m)^q \cdot g^r$$

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

$$\Rightarrow g^r = (g^m)^{-q} \cdot a \quad ; \ a \in H \text{ and } (g^m)^{-q} = h^{-q} \in H$$

Since, m is least positive integer for $g^m \in H$, So, it means $0 < r < m$ is not possible. Hence $r = 0$.

Then, the division algorithm becomes

$$s = qm$$

Since, we have, $a = g^s$

$$\Rightarrow a = g^{qm} = (g^m)^q$$

Hence, every element of H is generated by $h = g^m$

Proposition :-

If g is any element of order k in a group $(G, \cdot)$, then, $H = \{g^r \, ; \, r \in \mathbb{Z}\}$ is a subgroup of order k in $(G, \cdot)$. This is called cyclic subgroup generated by g.

Proof :-

We first check that H is a subgroup of $(G, \cdot)$. This follow from fact that

$$g^r \cdot g^s = g^{r+s} \in H \text{ and } (g^r)^{-1} = g^{-r} \in H \quad \forall \ r, s \in \mathbb{Z}$$

If the order of element g is infinite, we show that the element g^r are all distinct.

Suppose, $g^r = g^s$, where $r > s$, then $g^{r-s} = e$ with $r - s > 0$ which contradicts the fact that g has infinite order. In this case $|H|$ is infinite.

If the order of element g is k, which is finite, we show that, $H = \{g^0 = e, g^1, g^2, \ldots, g^{k-1}\}$.

Suppose, $g^r = g^s$ where $0 \le s < r \le k-1$

Multiply both sides by g^{-s}, So that

$$g^{r-s} = e \quad \text{with} \quad 0 < r - s < k$$

This contradicts the fact that k is the order of g.

Hence, the elements $g^0, g^1, g^2, \ldots, g^{k-1}$ are all distinct.

For any other element, g^t, we can write

$$t = qk + r \quad \text{where,} \quad 0 \le r < k$$

Hence,

$$g^t = g^{qk+r} = (g^k)^q \cdot g^r = (e)^q \cdot g^r = g^r$$

Hence,

$$H = \{g^0, g^1, g^2, \ldots, g^{k-1}\} \text{ and } |H| = k$$

Theorem :-

If the finite group G is of order n and has an element g of order n, then, G is a cyclic group generated by g.

Proof :-

From above proposition, we know $H \subseteq G$ generated by g has order n. Therefore, H is subset of finite set G with same number of elements. Hence, $G = H$ and G is cyclic group.

Example:-

Show that Klein 4-group is not cyclic.

Salution:-

$$K_4 = V_4 = \{e, a, b, c\}$$

In this group, the identity has order 1, whereas all orther elements have order 2. As, it has no element of order 4, So, it is not cyclic.

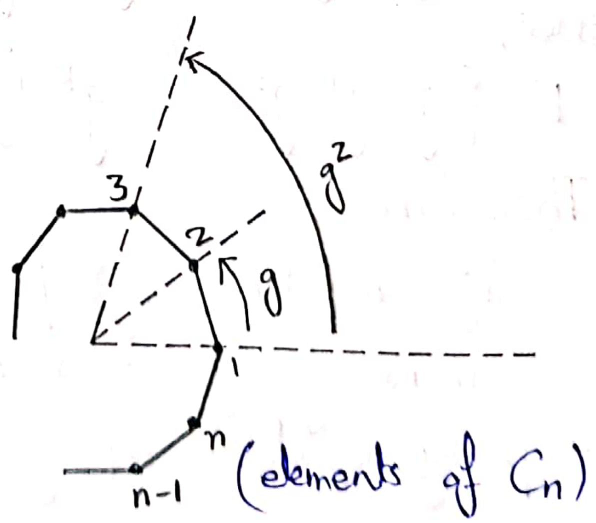
This group can be generated by two elements "a" and "b".

Example:-

Show that the group of proper rotations of regular n-gon in the plane is a cyclic group of order n generated by a rotation of $\frac{2\pi}{n}$ radians. This group is denoted by C_n.

Salution:-

This is the group of those symmetrices of regular n-gon that can be performed in plane, i.e. without turing the n-gon over.



Label the vertices 1 through n. Under any symmetry, the centre must be fixed, and the vertex 1 can be taken to any of n vertices. The image of 1 determine the rotation, hence, the group is of order n.

Let, g be a counter clockwise rotation of n-gon through $2\pi/n$. Then g has order n, So group is cyclic of order n. Hence,

$$C_n = \{e, g^1, g^2, \ldots\ldots, g^{n-1}\}$$

Dihedral group :-

The group of all symmetries (both proper and improper rotation) is called dihedral group. It is denoted by D_n.

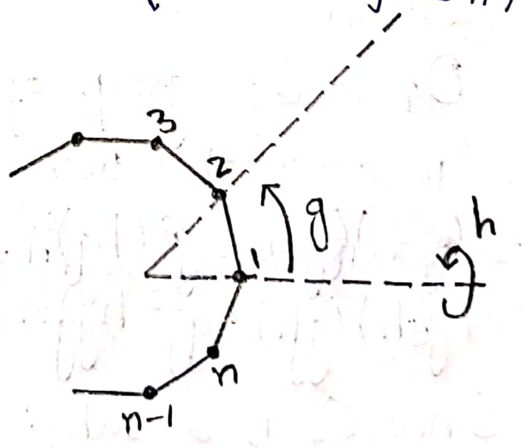
Example :-

Show that the dihedral group D_n, is of order $2n$, and is not cyclic.

Solution :-

Label the vertices 1 to n in a counterclockwise direction around the n-gon. Let, g be rotation by $2\pi/n$ and let h be the improper rotation of n-gon about an axis through the centre and vertex 1. The elements g generates the group C_n, which is cyclic subgroup of D_n.

(elements of D_n)



The element h has order 2 and generates a subgroup $\{e, h\}$. Any symmetry fix the origin and is determined by image of two adjacent vertices, say 1 and 2. The vertex 1 can taken to any of n vertices but 2 must be taken to one of two vertices adjacent to 1.

Hence, D_n has order $2n$.

If the image of 1 is $r+1$ then image of 2 must be 'r' or '$r+2$'. If image of 2 is $r+2$, the symmetry is g^r. If image of 2 is r, the symmetry is $g^r h$.

The symmetries $g^r h$ and hg^{-r} have same effects. and therefore imply the relation.

$$g^r h = hg^{-r} = hg^{n-r}$$

Hence, the dihedral group is

$$D_n = \{e, g, g^2, \cdots, g^{n-1}, h, gh, g^2h, \cdots, g^{n-1}h\}$$

Note that if $n \geq 3$, then $gh \neq hg$; thus D_n is non-abelian group. Therefore, this group cannot be cyclic.

Example:-

Draw the group table for D_4 and C_4.

Solution :-

D_4 is the group of symmetries of square and its table is calculated using the relation : $g^r h = hg^{4-r}$

For example,

$$(g^2h)(gh) = g^2(hg)h = g^2(g^3h)h = g^5h^2 = g$$

Since, C_4 is a subgroup of D_4, the table for C_4 appears inside the dased lines in top left corner.

Note that the order of each elements h, gh, g^2h and g^3h in D_4 is 2. In general, the element $g^r h$ in D_n is a reflection in line through the centre of n-gon bisecting the angle between vertices 1 and $r+1$. Therefore, $g^r h$ always the order 2.

$\cdot$	e	g	g^2	g^3	h	gh	g^2h	g^3h
e	e	g	g^2	g^3	h	gh	g^2h	g^3h
g	g	g^2	g^3	e	gh	g^2h	g^3h	h
g^2	g^2	g^3	e	g	g^2h	g^3h	h	gh
g^3	g^3	e	g	g^2	g^3h	h	gh	g^2h
h	h	g^3h	g^2h	gh	e	g^3	g^2	g
gh	gh	h	g^3h	g^2h	g	e	g^3	g^2
g^2h	g^2h	gh	h	g^3h	g^2	g	e	g^3
g^3h	g^3h	g^2h	gh	h	g^3	g^2	g	e

(group D_4)

DANIYAL ASIF
SP21-RMT-013

Morphism :- (Homomorphism)

Let, $(G, *)$ and $(H, \circ)$ be two groups, then the function $f: G \to H$ is called group morphism if:

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

Isomorphism :-

A group isomorphism is a bijective group morphism. If there is an isomorphism between the group $(G, *)$ and $(H, \circ)$, we say that $(G, *)$ and $(H, \circ)$ are isomorphic and write $(G, *) \cong (H, \circ)$

Examples :-

(1) If G and H are any two groups, the trivial function that maps every element of G to identity of H is always morphism.

(2) If $i: \mathbb{Z} \to \mathbb{Q}$ is the inclusion map, i is group morphism from $(\mathbb{Z}, +)$ to $(\mathbb{Q}, +)$. In fact, if H is subgroup of G, then, inclusion map $i(z) = z$; $z \in \mathbb{Z}$ is always group morphism.

(3) Define $f: (\mathbb{Z}, +) \to (\{\pm 1\}, \cdot)$ by

$$f(n) = 1 \text{ if } n \text{ is odd}, \quad f(n) = -1 \text{ if } n \text{ is even.}$$

Then, f is a group morphism.

(4) Let, $GR(2, \mathbb{R})$ be the set of 2×2 invertible real matrices. The one-to-one correspondence between the set L, of invertible linear transformation of the plane and 2×2 coefficient matrices is an isomorphism

between the groups $(L,\circ)$ and $(GL(2,\mathbb{R}),\cdot)$.

(5) Define $f:(\mathbb{Z}_4,+)\to(\{\pm1,\pm i\},\cdot)$ by $f(\bar{n})=i^n$, then

$$f(\bar{m}+\bar{n})=f(\overline{m+n})=i^{m+n}=i^m\cdot i^n=f(\bar{m})\cdot f(\bar{n})$$

$\Rightarrow f$ is group morphism.

Also, obviously f is bijective, So, f is isomorphism.

Proposition :-

Let, $f:G\to H$ be a group morphism, and, let e_G and e_H be the identity of G and H respectively.

Then,

(i) $f(e_G)=e_H$

(ii) $f(a^{-1})=f(a)^{-1}\quad\forall\ a\in G$

Proof :-

(i) Since, f is morphism, So,

$$f(e_G)\cdot f(e_G)=f(e_G\cdot e_G)=f(e_G)=f(e_G)\cdot e_H$$

By cancellation law,

$$f(e_G)=e_H$$

(ii) Since, f is morphism, So, $\forall\ a\in G$, we have

$$f(a)\cdot f(a^{-1})=f(a\cdot a^{-1})=f(e_G)$$

$\Rightarrow f(a)\cdot f(a^{-1})=e_H$ by part(i)

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

Theorem :-

Cyclic group of same order are isomorphic.

Proof :-

Let,

$G=\{g^r\ ;\ r\in\mathbb{Z}\}$ and $H=\{h^r\ ;\ r\in\mathbb{Z}\}$ be two cyclic groups.

If G and H are infinite, then g has infinite order, So, for $r, s \in \mathbb{Z}$, $g^r = g^s$ if and only if $r = s$. Hence, the function $f: G \to H$ defined by

$$f(g^r) = h^r, \quad r \in \mathbb{Z} \text{ is a bijection, and}$$

$$f(g^r g^s) = f(g^{r+s}) = h^{r+s} = h^r . h^s = f(g^r) . f(g^s)$$

for all $r, s \in \mathbb{Z}$, So, f is isomorphism.

If $|G| = |H| = n$, then,

$$G = \{e, g^1, g^2, \dots, g^{n-1}\} \text{ and } H = \{e, h^1, h^2, \dots, h^{n-1}\}$$

Then, the function $f: G \to H$ defined by

$$f(g^r) = h^r \text{ is again a bijection.}$$

Now, suppose $0 \le r, s \le n-1$ and let $r+s = kn+l$ where, $0 \le l \le n-1$, Then,

$$f(g^r \cdot g^s) = f(g^{r+s}) = f(g^{kn+l}) = f((g^n)^k . g^l)$$
$$= f(e^k . g^l) = f(g^l) = h^l$$

and,

$$f(g^r) . f(g^s) = h^r . h^s = h^{r+s} = h^{kn+l} = (h^n)^k . h^l$$
$$= e^k . h^l = h^l$$

$\Rightarrow f$ is isomorphism.

Hence, cyclic group of same order are isomorphic.

Example:-

Every cyclic group is isomorphic to either $(\mathbb{Z}, +)$ or, $(C_n, \cdot)$ for some n.

The above theorem implies that $(\mathbb{Z}, +) \cong (C_n, \cdot)$

Proposition :-

Corresponding elements under a group isomorphism have the same order.

Proof :-

Let, $f: G \to H$ be an isomorphism and let, $f(g)=h$

Suppose that g and h have same orders 'm' and 'n' respectively, where m is infinite. Then,

$$h^m = f(g)^m = f(g^m) = f(e) = e$$

Since, 'n' is least positive integer with property $h^n = e$

So, n is also finite and $n \leq m$.

On the other hand, if n is infinite, then,

$$f(g^n) = f(g)^n = h^n = e = f(e)$$

Since, f is bijective, So, $g^n = e$

Hence, m is finite and $m \leq n$.

Therefore, either m and n are both finite and $m=n$ or, m and n are both infinite.

Example :-

Is D_2 is isomorphic to C_4 or, Klein 4-group?

Solution :-

D_2		C_4		Klein 4-group	
Elements	order	Elements	order	Elements	order
e	1	e	1	e	1
g	2	g	4	a	2
h	2	g^2	2	b	2
gh	2	g^3	4	c	2

Compare the order of elements in above table.

Since, the corresponding elements under a group isomorphism have same order. Hence, D_2 cannot be isomorphic to C_4, but could possibly be isomorphic to Klein 4-group.

Group D_2				
$\cdot$	e	g	h	gh
e	e	g	h	gh
g	g	e	gh	h
h	h	gh	e	g
gh	gh	h	g	e

Klein 4-Group				
$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

In Klein 4-group, we can write $c = a \cdot b$ and we obtain a bijection, $f: D_2 \to V_4$ defined by

$f(g) = a$ and $f(h) = b$ for $g, h \in D_2$ and $a, b \in V_4$

The above table for two groups show that this is an isomorphism.

Hence, D_2 is isomorphic to V_4, i.e. $D_2 \cong V_4$.

Permutation groups :-

Let, X be any non-empty set, then, any bijective function on X is called permutation on X. The set of all bijective permutation on X, forms non-abelian group under binary operation of composition of function. The permutation of two sets, with same number of elements are isomorphic. We denote the permutation group of $X = \{1, 2, 3, \ldots, n\}$ by $(S_n, \circ)$ and call it the symmetric group on 'n' elements. Hence, $S_n \cong S(X)$ for any 'n' element set X.

Proposition :-

$$|S_n| = n!$$

Proof :-

The order of S_n is the number of bijection from $\{1,2,3,\ldots\ldots,n\}$ to itself. There are 'n' possible choice for image of 1. Once the image of 1 has been choosen, there are 'n-1' choice for image of 2. Then, there are 'n-2' choice for image of 3. Continuing in this way, we see that,

$$|S_n| = n(n-1)(n-2)\cdots\cdots 2.1$$

$$\Rightarrow |S_n| = n!$$

Example :-

(i) For $n=2$, let, $X=\{1,2\}$,

then, $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$

which is of order $2! = 2$

(ii) For $n=3$, let, $X=\{1,2,3\}$, then,

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

which is of order $3! = 3\times2\times1 = 6$

Example :-

If $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ are two elements of S_3, calculate $\pi \circ \rho$ and $\rho \circ \pi$.

Solution :-

$$\pi \circ \rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\boxed{\begin{aligned} \pi \circ \rho(1) &= \pi(\rho(1)) \\ &= \pi(3) = 2 \\ \pi \circ \rho(2) &= \pi(\rho(2)) \\ &= \pi(2) = 1 \\ \pi \circ \rho(3) &= \pi(\rho(3)) \\ &= \pi(1) = 3 \end{aligned}}$$

and,

$$\rho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Since,

$$\boxed{\begin{aligned} \rho \circ \pi(1) &= \rho(\pi(1)) = \rho(3) = 1 \\ \rho \circ \pi(2) &= \rho(\pi(2)) = \rho(1) = 3 \\ \rho \circ \pi(3) &= \rho(\pi(3)) = \rho(2) = 2 \end{aligned}}$$

Hence,

$$\rho \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix}$$

Cycle of length r :-

If $a_1, a_2, \ldots, a_n$ are distinct element of $\{1, 2, 3, \ldots, n\}$, the permutation $\pi \in S_n$, defined by:

$$\pi(a_1) = a_2$$
$$\pi(a_2) = a_3$$
$$\vdots \quad \vdots \quad \vdots$$

$\vdots \quad \vdots \quad \vdots$

$\pi(a_{r-1}) = a_r$

$\pi(a_r) = a_1$

and, $\pi(x) = x$ if $x \notin \{a_1, a_2, \dots, a_r\}$

is called a cycle of length r, or, an r-cycle.

We denote it by $(a_1 \ a_2 \ a_3 \ \dots \ a_r)$.

For Example:-

(i) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (3 \ 2 \ 1)$ is a 3-cycle in S_3.

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1 \ 3 \ 4 \ 2)$ is a 4-cycle in S_4.

(iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix} = (2 \ 5 \ 4)$ is a 3-cycle in S_6.

Proposition:-

An r-cycle in S_n has order r.

Proof:-

If $\pi = (a_1 \ a_2 \ \dots \ a_r)$ is an r-cycle in S_n, then,

$$\pi(a_1) = a_2$$
$$\pi^2(a_1) = a_3$$
$$\pi^3(a_1) = a_4$$
$$\vdots \quad \vdots \quad \vdots$$
$$\pi^r(a_1) = a_1$$

Similarly, $\pi^r(a_i) = a_i$ for $i = 1, 2, 3, \dots, r$

Since, π^r fixed all other elements, it is the identity permutation, But none of the permutation $\pi, \pi^2, ----, \pi^{r-1}$ equal the identity permutation because they all moved element a_1,

Hence, the order of π is r.

Example :-

Write down $\pi = (1\ 3\ 4\ 2)$, $\rho = (1\ 3)$ and $\sigma = (1\ 2) \circ (3\ 4)$ as permutation in S_4. Calculate $\pi \circ \rho \circ \sigma$.

Solution :-

$$\pi = (1\ 3\ 4\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

$$\rho = (1\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\sigma = (1\ 2) \circ (3\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Then,

$$\pi \circ \rho \circ \sigma = (1\ 3\ 4\ 2) \circ (1\ 3) \circ (1\ 2) \circ (3\ 4)$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Since,

$$\boxed{\begin{aligned} \pi \circ \rho \circ \sigma(1) &= \pi \circ \rho(\sigma(1)) = \pi \circ \rho(2) = \pi(2) = 1 \\ \pi \circ \rho \circ \sigma(2) &= \pi \circ \rho(1) = \pi(3) = 4 \\ \pi \circ \rho \circ \sigma(3) &= \pi \circ \rho(4) = \pi(4) = 2 \\ \pi \circ \rho \circ \sigma(4) &= \pi \circ \rho(3) = \pi(1) = 3 \end{aligned}}$$

So, $\pi \circ \rho \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (2\ 4\ 3)$

$\Rightarrow \pi \circ \rho \circ \sigma = (2\ 4\ 3)$ is a 3-cycle in S_4.

Orbit :-

If π is a permutation in S_n and $a \in \{1, 2, ---, n\}$, the orbit of a under π consists of distinct elements

$$a, \pi(a), \pi^2(a), \pi^3(a), -------$$

We can split a permutation up into its different orbit and each orbit will give rise to a cycle.

e.g.

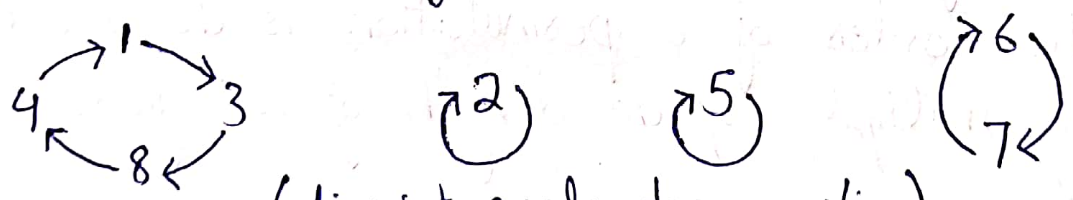
let, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 8 & 1 & 5 & 7 & 6 & 4 \end{pmatrix} \in S_8.$

Here,

$\pi(1) = 3$, $\pi^2(1) = \pi(3) = 8$, $\pi^3(1) = 4$, $\pi^4(1) = 1$

Thus, orbit of 1 is $\{1, 3, 8, 4\}$. This is also the orbit of 3, 4 and 8. This orbit gives rise to cycle $(1\ 3\ 8\ 4)$.

Since, π leaves 2 and 5 fixed. Thier orbits are $\{2\}$ and $\{5\}$. The orbits of 6 and 7 are $\{6, 7\}$, which gives rise to 2-cycle $(6\ 7)$



(disjoint cycle decomposition)

Then, $\pi = (1\ 3\ 8\ 4) \circ (2) \circ (5) \circ (6\ 7)$

These cycle are disjoint. If a permutation is written as a product of disjoint cycle, then, order doesn't mattar. We often omit the 1-cycle and write

$\pi = (1\ 3\ 8\ 4) \circ (6\ 7)$. Identity permutation usually written as (1).

Proposition :-

Every permutation can be written as a product of disjoint cycles.

Proof :-

let, π be a permutation and let, $\gamma_1, \gamma_2, ---, \gamma_k$ be the cycles obtained from orbit of π. let, a_1 be any number in the domain of π and let, $\pi(a_1) = a_2$. If γ_i is the cycle containing a_1, we can write $\gamma_i = (a_1\, a_2 \, ---- a_r)$; the other cycle with not contain any of element $a_1, a_2, ----, a_r$ and hence will leave them all fixed. Therefore, the product $\gamma_1 \circ \gamma_2 \circ ---- \circ \gamma_k$ will maps a_1 to a_2, because the only cycle to move a_1 or a_2 is γ_i. Hence, $\pi = \gamma_1 \circ \gamma_2 \circ --- \circ \gamma_k$, because they both have the same effect on all the numbers in the domain of π.

Corollary :-

The order of a permutation is the least common multiple of the length of its cycle.

Proof :-

If π is written in term of disjoint cycle as $\gamma_1 \circ \gamma_2 \circ ---- \circ \gamma_k$, the order of cycle can be changed because they are disjoint. Therefore, for any integer m,

$$\gamma^m = \gamma_1^m \circ \gamma_2^m \circ \gamma_3^m \circ \cdots\cdots\cdots \circ \gamma_k^m$$

Because the cycle is disjoint, this is the identity if

and only if γ_i^m is the identity for each i.
The least such integer is the least common multiple of the order of cycles.

Example :-

Find order of permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix}$$

Solution :-

We can write this permutation in term of disjoint cycles as:

$$\pi = (1\ 3\ 8\ 2\ 5) \circ (4\ 7\ 6)$$

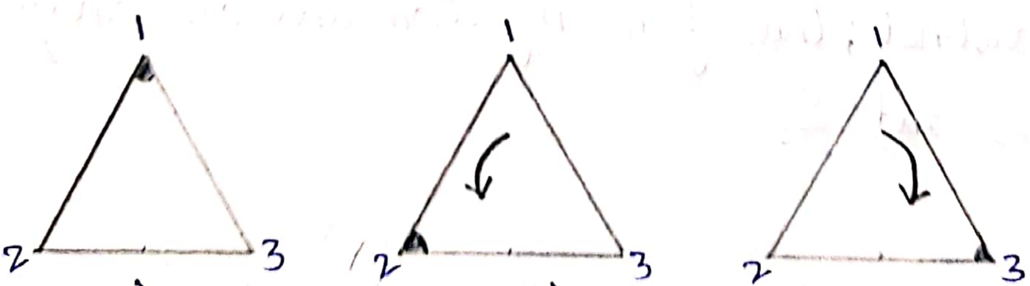
The length of these cycles is 5 and 3.
By corollary, order of permutation is lcm of the length of its cycle, So,

$$\text{order of } \pi = \text{lcm}(5,3) = 15$$

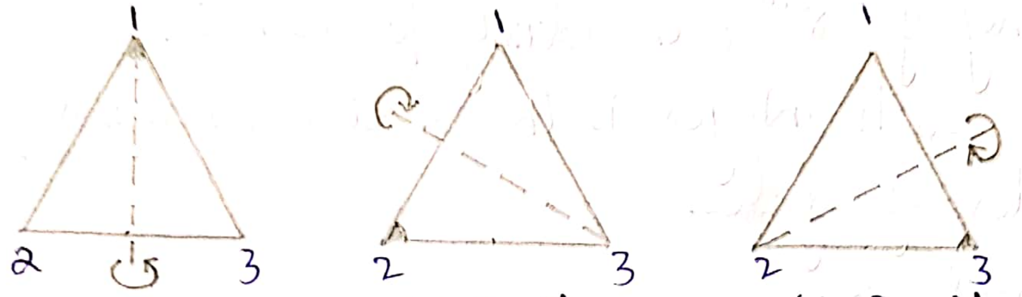
Example :-

Show that D_3 is isomorphic to S_3 and write out table for latter group.

Solution :-



$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) = e, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) = g, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) = g^2$$



$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=(3\ 2)=h;\quad \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=(1\ 2)=gh;\quad \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=(1\ 3)=g^2h$$

(symmetrices of equilateral triangle)

$\circ$	(1)	(123)	(132)	(23)	(12)	(13)
(1)	(1)	(123)	(132)	(23)	(12)	(13)
(123)	(123)	(132)	(1)	(12)	(13)	(23)
(132)	(132)	(1)	(123)	(13)	(23)	(12)
(23)	(23)	(13)	(12)	(1)	(132)	(123)
(12)	(12)	(23)	(13)	(123)	(1)	(132)
(13)	(13)	(12)	(23)	(132)	(123)	(1)

Table (group S_3)

D_3 is the group of symmetries of an equilateral triangle and any symmetry induce a permutation of vertices. This defines a function $f: D_3 \to S_3$. If $\sigma, \tau \in D_3$, then, $f(\sigma \circ \tau)$ is induced permutation on vertices which is same as $f(\sigma) \circ f(\tau)$. Hence, f is morphism. The six permutation are all distinct; thus f is bijection and an isomorphism between D_3 and S_3.

DANIYAL ASIF
SP21-RMT-013

Even and Odd Permutation :-

Every permutation can be given a parity, even or, odd. The defination derives from an action of each permutation σ in S_n on a polynomial $f(x_1, x_2, ----, x_n)$ in n variable by permuting the variables :

$$\sigma f(x_1, x_2, \cdots\cdots, x_n) = f(x_{\sigma 1}, x_{\sigma 2}, ----, x_{\sigma n})$$

e.g. if $\sigma = (1\ 2\ 3)$ in S_4 and

$f(x_1, x_2, x_3, x_4) = 2x_1 x_4 - 3x_2^2 + x_2 x_3^2$, then,

$$\sigma f = 2x_2 x_4 - 3x_3^2 + x_3 x_1^2$$

Ours use of this action involves a particular polynomial $D = D(x_1, x_2, ----, x_n)$ called <u>discriminant</u>, defined to be the product of all terms $(x_i - x_j)$ where $i < j$. More formally,

$$D = \prod_{0 \leq i < j \leq n} (x_i - x_j)$$

e.g. if $n = 3$, then, $D = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$. Given a permutation $\sigma \in S_n$, we have

$$\sigma D = \prod_{0 \leq i < j \leq n} (x_{\sigma i} - x_{\sigma j})$$

Thus, if $n = 3$ and $\sigma = (1\ 2) \in S_3$, then

$$\sigma D = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -D$$

In fact, $\sigma D = \pm D$ for every $\sigma \in S_n$ and we say that

→ <u>σ is even</u> if $\sigma D = D$.

→ <u>σ is odd</u> if $\sigma D = -D$.

Transposition :-

A 2-cycle is called a <u>transposition</u>.

Proposition :-

Every transposition is odd.

Proof :-

Let, D denote the discriminant in n variables $x_1, x_2, x_3, \ldots\ldots, x_n$, and define

$D_{k/m}$ = product of all terms in D involving x_k, except $(x_k - x_m)$

$D_{k,m}$ = product of all terms in D involving neither 'x_k' nor 'x_m'.

Then, D factors as follow:

$$D = (x_k - x_m) D_{k/m} D_{m/k} D_{k,m}$$

Now, fix a transposition, $\tau = (k\ m)$ in S_n, where $k < m$. Since, τ interchanges k and m, we see that

$$\tau D_{k/m} = u D_{m/k} \quad \text{where, } u = 1 \text{ or } u = -1$$

Since, τ^2 is the identity permutation, we have

$$D_{k/m} = \tau^2 D_{k/m} = \tau(\tau D_{k/m}) = \tau(u D_{m/k}) = u(\tau D_{m/k})$$

Because, $u^2 = 1$, it follows that

$$\tau D_{m/k} = u D_{k/m}$$

Since, $\tau D_{k,m} = D_{k,m}$, appling τ to D gives

$$\tau D = \tau(x_k - x_m) \cdot \tau D_{k/m} \cdot \tau D_{m/k} \cdot \tau D_{k,m}$$

$$= (x_m - x_k) \cdot u D_{m/k} \cdot u D_{k/m} \cdot D_{k,m}$$

$$= -(x_k - x_m) \cdot u^2 . D_{m/k} \cdot D_{k/m} D_{k,m}$$

$$= -(x_k - x_m) D_{m/k} D_{k/m} D_{k,m} \quad \because (u^2 = 1)$$

$$\Rightarrow \tau D = -D$$

Hence, τ is odd and we have proved.

Proposition :-

Every r-cycle is a product of $r-1$ transposition (not necesarily disjoint); in fact,

$$(a_1\ a_2 \cdots a_r) = (a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{r-1}\ a_r)$$

Since, every permutation σ is a product of disjoint cycles, it follows that σ is product of transpositions. This gives us the desired parity test.

Theorem :- (Parity Theorem)

Every permutation $\sigma \in S_n$ is a product of transposition. Moreover, if σ is a product of m transposition in any way at all, the parity of σ equals the parity of m. That is, σ is even if m is even and σ is odd if m is odd.

Proof :-

Write, $\sigma = \tau_1 \tau_2 \cdots \tau_m$, where, τ_i are transposition. If D is the discriminant in n variables, then

$$\tau_i D = -D \text{ for each } i.$$

because, every transposition is odd.

Hence, the effect of $\sigma = \tau_1 \tau_2 \cdots \tau_m$ on D is to change the sign m-times. Thus,

$$\sigma D = (-1)^m D$$

and the results follow.

Corollary :-

An n-cycle is an even permutation if n is odd and an odd permutation if n is even.

Example :-

Write the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 8 & 2 & 7 & 3 & 6 & 5 \end{pmatrix}$$

as a product of disjoint cycles and determine its order and parity.

Solution :-

As disjoint cycles,

$$\pi = (1\ 4\ 2) \circ (3\ 8\ 5\ 7\ 6)$$

Hence, order of π is $\operatorname{lcm}(3,5) = 15$

The parity of the 3-cycle $(1\ 4\ 2)$ is even and the parity of the 5-cycle $(3\ 8\ 5\ 7\ 6)$ is even.

Therefore, the parity of π is (even) $\circ$ (even) $=$ even.

Alternating group :-

Denote the set of even permutation on 'n' elements by A_n. A_n is subgroup of S_n, called the alternating group on 'n' elements.

e.g.

$$A_4 = \left\{ (1), \begin{matrix} (1\ 2)\circ(3\ 4), \\ (1\ 3)\circ(2\ 4), \\ (1\ 4)\circ(2\ 3), \end{matrix} \begin{matrix} (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4) \\ (1\ 3\ 2), (1\ 4\ 2), (1\ 4\ 3), (2\ 4\ 3) \end{matrix} \right\}$$

a group of 12 elements.

Theorem :-

$$|A_n| = \tfrac{1}{2} n! \quad \text{for every } n \geq 2.$$

Proof :-

Let, O_n denote the set of odd permutation in S_n, So,

$$S_n = A_n \cup O_n \quad \text{and} \quad A_n \cap O_n = \Phi.$$

Hence, $n! = |S_n| = |A_n| + |O_n|$, so it suffices to show that $|A_n| = |O_n|$.

We do this by finding a bijection $f : A_n \to O_n$

Let, $\tau = (1 \ 2)$ and define f by $f(\sigma) = \tau \circ \sigma \ \forall \ \sigma \in A_n$.

Since, σ is even and τ is odd, So, $\tau \circ \sigma$ is odd.

Let, $f(\sigma_1) = f(\sigma_2)$, $\sigma_1, \sigma_2 \in A_n$

$\Rightarrow \tau \circ \sigma_1 = \tau \circ \sigma_2$

$\Rightarrow \sigma_1 = \sigma_2$ $\quad \because$ (by cancellation law in S_n)

$\Rightarrow f$ is one-one.

Now, let, $\lambda \in O_n$, then, $\tau \circ \lambda \in A_n$ and

$f(\tau \circ \lambda) = \tau \circ (\tau \circ \lambda) = \lambda$ $\quad \because (\tau \circ \tau = e)$

$\Rightarrow f$ is onto.

Since, f is one-one and onto, So, f is bijective.

$\Rightarrow |A_n| = |O_n|$

$\Rightarrow n! = S_n = 2|A_n|$

$\Rightarrow A_n = \tfrac{1}{2} n!$

Hence, proved.

Proposition :-

Every even permutation can be written as a product of 3-cycles. (not necessarily disjoint).

Proof :-

An even permutation can be written as a product of an even number of transposition. We show that any product of two transposition is a product of 3-cycles. If these transposition are identical, thier product is identity. If the two transposition have one element in common, say $(a\,b)$ and $(b\,c)$, then thier product $(a\,b) \circ (b\,c) = (a\,b\,c)$, a 3-cycle.

If two transposition have no elements in common say $(a\,b)$ and $(c\,d)$, we can write thier product as

$$(a\,b) \circ (c\,d) = (a\,b) \circ (b\,c) \circ (b\,c) \circ (c\,d)$$
$$= (a\,b\,c) \circ (b\,c\,d)$$

a product of two 3-cycle.

Remarks :-

The parity theorem and above proposition show, respectively, that S_n is generated by 2-cycles and A_n is generated by the 3-cycles.

Cayley's Theorem :-

Every group $(G, \cdot)$ is isomorphic to a subgroup of its symmetric group $(S(G), \circ)$.

Proof :-

For each element $g \in G$,

define $\pi_g : G \to G$ by $\pi_g(x) = g \cdot x$.

We show that π_g is bijective.

let, $\pi_g(x) = \pi_g(y)$ for $x, y \in G$

$\Rightarrow g \cdot x = g \cdot y$

$\Rightarrow x = y$ $\therefore$ (by cancellation law)

$\Rightarrow \pi_g$ is one-one.

Now, for any $y \in G$, we have

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

$\Rightarrow \pi_g$ is onto

Hence, $\pi_g \in S(G)$.

let, $H = \{\pi_g \in S(G) \,;\, g \in G\}$. We show that $(H, \circ)$ is a subgroup of $(S(G), \circ)$ isomorphic to $(G, \cdot)$.

In fact we show that the function

$\psi : G \to H$ by $\psi(g) = \pi_g$ is a group isomorphism.

This is clearly surjective.

let, $\psi(g) = \psi(h)$, $g, h \in G$

$\Rightarrow \pi_g = \pi_h$.

and $\pi_g(e) = \pi_h(e) \Rightarrow g = h$

$\Rightarrow \psi$ is also injective.

It remains to show that "ψ" preserves the group operation.

If $g, h \in G$, then,

$$\lambda_{g.h}(x) = (g.h)(x) = g.(h.x) = \lambda_g(h.x)$$
$$= (\lambda_g \circ \lambda_h)(x)$$

$$\Rightarrow \lambda_{g.h} = \lambda_g \circ \lambda_h$$

Also,

$$\lambda_{h^{-1}} \circ \lambda_h = \lambda_{h^{-1}.h} = \lambda_e$$

$$\Rightarrow (\lambda_h)^{-1} = \lambda_{h^{-1}} \in H$$

Hence, H is a subgroup of $S(G)$, and,

$$\psi(g.h) = \psi(g).\psi(h).$$

Hence, every group $(G, .)$ is isomorphic to a subgroup of its symmetric group $(S(G), \circ)$.

Corollary:-

If G is a finite group of order 'n', then, G is isomorphic to a subgroup of S_n.

Daniyal Khuya.

DANIYAL ASIF

SP21-RMT-013

Right Cosets :-

Let, $(G,.)$ be a group with subgroup H. For $a, b \in G$, we say that a is congruent to b module H and write, $a \equiv b \pmod H$
if and only if,

$$ab^{-1} \in H$$

Proposition :-

The relation $a \equiv b \pmod H$ is an equivalence relation on G. The equivalence class containing a can be written in the form

$$Ha = \{ha \; ; \; h \in H\}$$

and, it is called a right coset of H in G. The element a is called a representative of the coset Ha.

Note :-

The equivalence class containing a is

$$\{x \in G \mid x \equiv a \pmod H\} = \{x \in G \mid xa^{-1} = h \in H\}$$
$$= \{x \in G \mid x = ha, \; h \in H\}$$
$$= \{ha, \; h \in H\}$$

Example :-

Find the right cosets of A_3 in S_3.

Solution :-

$S_3 = \{(1), (1\,2\,3), (1\,3\,2), (2\,3), (1\,3), (1\,2)\}$
and, $A_3 = \{(1), (1\,2\,3), (1\,3\,2)\}$

One coset is the group itself, $A_3 = \{(1), (1\,2\,3), (1\,3\,2)\}$

The another right coset is

$$A_3(1\ 2) = \{(1\ 2), (1\ 2\ 3)\circ(1\ 2), (1\ 3\ 2)\circ(1\ 2)\}$$
$$= \{(1\ 2), (1\ 3), (2\ 3)\}$$

Since, the right cosets form a partition of S_3 and these two cosets contains all the elements of S_3, it follows that there is only two cosets.

In fact;

$$A_3 = A_3(1\ 3\ 2) = A_3(1\ 2\ 3)$$

and, $A_3(1\ 2) = A_3(1\ 3) = A_3(2\ 3)$

Example:-

Find the right cosets of $H = \{e, g^4, g^8\}$ in $C_{12} = \{e, g, g^2, \cdots g^{11}\}$.

Solution:-

'H' itself is one coset.

$Hg = \{g, g^5, g^9\}$

$Hg^2 = \{g^2, g^6, g^{10}\}$

$Hg^3 = \{g^3, g^7, g^{11}\}$

Since, $C_{12} = H \cup Hg \cup Hg^2 \cup Hg^3$, these are all the cosets.

Lemma:-

There is a bijection between any right two cosets of H in G.

Proof:-

Let, Ha be a right cosets of H in G. We produce a bijection between Ha and H, from which it follow that there is a bijection between any right two cosets.

Define, $\psi : H \to Ha$ by $\psi(h) = ha$.

Suppose that;

$$\psi(h_1) = \psi(h_2) \qquad h_1, h_2 \in H$$

$$\Rightarrow h_1 a = h_2 a$$

$$\Rightarrow h_1 = h_2$$

$\Rightarrow \psi$ is one-one.

Also, it is clear that ψ is onto.

Hence, ψ is a bijection.

Lagrange's Theorem:-

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

Proof:-

The right cosets of H in G form a partition of G, so G can be written as a disjoint union,

$$G = Ha_1 \cup Ha_2 \cup \cdots\cdots \cup Ha_k$$

for finite set of elements, $a_1, a_2, \ldots, a_k \in G$

Since, there is a bijection between any two right cosets of H in G, So, the number of elements in each cosets is $|H|$.

Hence, counting all the elements in the disjoint union above, we see that $|G| = k|H|$.

Therefore, $|H|$ divides $|G|$.

Index of subgroup H in group G :-

If H is a subgroup of G, the number of distinct right cosets of H in G is called the index of H in G, and is written as $[G : H]$.

Corollary :-

If G is a finite group with subgroup H, then, $[G : H] = \frac{|G|}{|H|}$.

Corollary :-

If 'a' is an element of a finite group G, then, "order of a" divides "order of G."

Proof :-

Let, $H = \{a^r ; r \in \mathbb{Z}\}$ be a cyclic subgroup generated by 'a'. The order of subgroup H is same as the order of 'a'.

Hence, by Langrange theorem, "order of a divides order of G."

Corollary :-

If a is an element of finite group G, then,

$$a^{|G|} = e$$

Proof :-

If m is the order of 'a', then

$|G| = km$, for some integer K.

Hence, $a^{|G|} = a^{mk} = (a^m)^k = e^k = e$

Corollary :-

If G is a group of prime order, then G is cyclic.

Proof :-

Let, $|G| = p$, a prime number

By corollary, every element has order 1 or p, But the only element of order 1 is identity. Therefore, all the other elements have order p, and there is atleast one because $|G| \geq 2$.

Hence, G is cyclic group generated by a prime number 'p'.

Remarks :-

The converse of langarge theorem is not true in general.

Example :-

A_4 is a group of order 12 having no subgroup of order 6.

Solution :-

A_4 = set of all even permutation on 4-elements.

$$= \left\{ \begin{matrix} & (1\,2)\circ(3\,4), & (1\,2\,3), (1\,2\,4), (1\,3\,4), (2\,3\,4) \\ (1), & (1\,3)\circ(2\,4), & \\ & (1\,4)\circ(2\,3), & (1\,3\,2), (1\,4\,2), (1\,4\,3), (2\,4\,3) \end{matrix} \right\}$$

A_4 contains one identity element, eight 3-cycle of the form $(a\,b\,c)$, three pairs of transposition of the form $(a\,b)\circ(c\,d)$, where a, b, c, d are distinct element of $\{1, 2, 3, 4\}$.

If a subgroup contains a 3-cycle $(a\,b\,c)$, it must contains its inverse $(a\,c\,b)$. If a subgroup of order 6 exists, it must contains the identity and product of two transposition, because, odd no. of non-identity cannot be made up of 3-cycles and its inverse. A subgroup of order 6 must also contain atleast two 3-cycle because A_4 only contains four elements that are not 3-cycle.

Without loss of generality, let a subgroup of order 6 contain the elements $(a\,b\,c)$ and $(a\,b)\circ(c\,d)$. Then it must also contain the elements,

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

$$(a\,b\,c)\circ(a\,b)\circ(c\,d) = (a\,c\,d)$$

$$(a\,b)\circ(c\,d)\circ(a\,b\,c) = (b\,d\,c)$$

and, $(a\,c\,d)^{-1} = (a\,d\,c)$

which together with identity, gives more than six elements. Hence, A_4 contains no subgroup of order 6.

Lemma :-

Let, g be an element of order n in a group, and let, $m \geq 1$

(i) if $\gcd(n,m) = d$, then g^m has order n/d.

(ii) In particular, if m divides n, then g^m has order n/m.

Proof:-

(i) We have $(g^m)^{n/d} = (g^n)^{m/d} = (e)^{m/d} = e$

If $(g^m)^k = e$, we must show that n/d divides k.

We have $g^{mk} = e$, So, n divides mk.

Hence, n/d divides $m/d\, k$, But m/d and n/d are relatively prime, So, n/d divides k.

(ii) If m divides n, then, $\gcd(m,n) = m$

So, (i) implies (ii)

Proposition:-

If G is a cyclic group of order n, and if k divides n, then G has exactly one subgroup H of order k. In fact, if g generates G, then H is generated by $g^{n/k}$.

Proof:-

Let, H denote the subgroup generated by $g^{n/k}$. Then, $|H| = k$, because $g^{n/k}$ has order k by above lemma (with $m = \frac{n}{k}$). Now let, K be any subgroup of G of order k, then K is generated by g^m for some $m \in \mathbb{Z}$, then, g^m has order $|K| = k$.

But, if $d = \gcd(m,n)$, then g^m also has order n/d.

Thus, $k = n/d$, so $d = n/k$.

Write, $mx + ny = d$ for $x, y \in \mathbb{Z}$

Then, $g^{n/k} = g^d = g^{mx+ny} = (g^m)^x \cdot (g^n)^y = (g^m)^x \in K$

Since, $g^{n/k}$ generates H, it follow that $H \subseteq K$,
So, $H = K$ because $|H| = |K|$.

Left Cosets :-

Let, G be a group and H be a subgroup of G. We can define a relation L on G so that

aLb if and only if $b^{-1}a \in H$.

This relation L is an equivalence relation and the equivalence class containing a is left cosets.

$$aH = \{ah \,;\, h \in H\}$$

Remarks :-

The left and right cosets may or may not be equal.

Example :-

Find left and right cosets of $H = A_3$ and $K = \{(1), (1\ 2)\}$ in S_3.

$$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$$

$$H = A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$$

$$K = \{(1), (1\ 2)\}$$

Right Cosets of A_3 :-	Left Cosets of A_3
$H = \{(1), (1\,2\,3), (1\,3\,2)\}$	$H = \{(1), (1\,2\,3), (1\,3\,2)\}$
$H(1\,2) = \{(1\ 2), (1\,3), (2\,3)\}$	$(1\,2)H = \{(1), (2\,3), (1\,3)\}$

In this case, left and right cosets are same.

Right Cosets of K :-

$K = \{(1), (1\ 2)\}$

$K(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$

$K(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$

Left Cosets of K :-

$K = \{(1), (1\ 2)\}$

$(1\ 3)K = \{(1\ 3), (1\ 2\ 3)\}$

$(2\ 3)K = \{(2,3), (1\ 3\ 2)\}$

In this case, left and right cosets are not same.

Normal Subgroup :-

A subgroup H of a group G is said to be normal subgroup of G if:

$$g^{-1}hg \in H \quad \forall\ g \in G, h \in H.$$

We can write it by $H \trianglelefteq G$.

Proposition :-

$Hg = gH\ \forall g \in G \Leftrightarrow H$ is normal subgroup of G.

Proof :-

Suppose that, $Hg = gH$, then for any element $h \in H$, $hg \in Hg = Hg$. Hence, $hg = gh_1$ for some $h_1 \in H$ and,
$g^{-1}hg = g^{-1}gh_1 = h_1 \in H$

Therefore, H is normal subgroup.

Conversely,

If H is normal, let, $hg \in Hg$ and $g^{-1}hg = h_1 \in H$

Then, $hg = gh_1 \in gH$

$\Rightarrow Hg \subseteq gH$ ——— (i)

Also,

$ghg^{-1} = (g^{-1})^{-1}hg^{-1} = h_2 \in H$, Since, H is normal, So,

$gh_2 = h_2 g \in Hg$.

$\Rightarrow gH \subseteq Hg$ —— (ii)

from (i) and (ii) : $Hg = gH$

Hence, proved.

Example:-

Since, in A_3,

$A_3(1\ 2) = \{(1\ 2), (1\ 3), (2\ 3)\} = (1\ 2)A_3$

So, A_3 is a normal subgroup of S_3.

Proposition:-

Any subgroup of an abelian group is normal.

Proof:-

Let, G be an abelian group and H be the subgroup of G, then,

$g^{-1}hg = hg^{-1}g = h \in H \quad \forall\ g \in G, h \in H$

$\Rightarrow H$ is normal subgroup.

Theorem :-

If N is normal subgroup of $(G,\cdot)$, the set of cosets $G/N = \{Ng \mid g \in G\}$ forms a group $(G/N, \cdot)$ where the operation is defined by $(Ng_1)\cdot(Ng_2) = N(g_1 \cdot g_2)$. This group is called the quotient group or, factor group of G by N.

Proof :-

→ As, G is a group, So, $e \in G$, then,

$$Ne = N \in G/N \neq \Phi$$

→ We have to show that Multiplication of cosets is well defined.

Since, h_1 is same cosets as g_1, So, $h_1 \equiv g_1 \bmod N$.
Similarly, h_2 is same cosets as g_2, So, $h_2 = g_2 \bmod N$.
We show that, $Nh_1h_2 = Ng_1g_2$.
We have, $h_1g_1^{-1} = n_1 \in N$ and $h_2g_2^{-1} = n_2 \in N$
So, $h_1h_2(g_1g_2)^{-1} = h_1h_2g_2^{-1}g_1^{-1} = n_1g_1n_2g_2g_2^{-1}g_1^{-1}$

$$= n_1g_1n_2g_1^{-1}$$

Now, N is normal subgroup, So,

$$g_1n_2g_1^{-1} \in N \text{ and } n_1g_1n_2g^{-1} \in N$$

Hence,

$$h_1h_2 \equiv g_1g_2 \bmod N \Rightarrow N(h_1h_2) = N(g_1g_2)$$

$\Rightarrow$ operation is well defined.

→ Now, we have to show that operation is associative.

$$(Ng_1 \cdot Ng_2)\cdot Ng_3 = N(g_1g_2)\cdot Ng_3 = N(g_1g_2)g_3$$

and, $Ng_1 \cdot (Ng_2 \cdot Ng_3) = Ng_1 \cdot N(g_2 g_3) = Ng_1(g_2 g_3)$
$= N(g_1 g_2) g_3$

$\Rightarrow$ operation is associative.

$\rightarrow$ Since, $Ng . Ne = Nge = Ng$
and, $Ne . Ng = Neg = Ng$

$\Rightarrow$ The identity is $Ne = N$.

$\rightarrow$ Since, $Ng . Ng^{-1} = N(gg^{-1}) = Ne = N$
and, $Ng^{-1} . Ng = N(g^{-1}g) = Ne = N$

$\Rightarrow$ The inverse of Ng is Ng^{-1}.

Hence, $(G/N, \cdot)$ is a group.

Order of G/N :-

The order of G/N is the number of cosets of N in G. Hence,

$$|G/N| = |G : N| = |G|/|N|$$

Example :-

A_3 is a normal subgroup of S_3.

$A_3(1\ 2) = \{(1\ 2), (1\ 3), (2\ 3)\} = (1\ 2) A_3$

Therefore, S_3/A_3 is a quotient group or, factor group.

If $H = A_3$, then the elements of this group are the cosets H and $H(1\ 2)$, and its multiplication table is

$\circ$	H	$H(1\ 2)$
H	H	$H(1\ 2)$
$H(1\ 2)$	$H(1\ 2)$	H

Example :-

$(\mathbb{Z}_n, +)$ is quotient group of $(\mathbb{Z}, +)$ by the subgroup $n\mathbb{Z} = \{nz \; ; \; z \in \mathbb{Z}\}$

Solution :-

Since, $(\mathbb{Z}, +)$ is abelian, every subgroup is normal. The relationship $a \equiv b \bmod (n\mathbb{Z})$ is equivalent to $a - b \in n\mathbb{Z}$ and to $\frac{a-b}{n}$. Hence, $a \equiv b \bmod (n\mathbb{Z})$ is same relation as $a \equiv b \pmod n$. Therefore, $\mathbb{Z}_n$ is quotient group $\mathbb{Z}/n\mathbb{Z}$' where operation on congurence class is defined by $[a] + [b] = [a+b]$.

$(\mathbb{Z}_n, +)$ is a cyclic group with 1 as generator, and it is isomorphic to C_n.

Proposition :-

If H is a subgroup of index 2 in G, so that $|G : H| = 2$, then, H is normal subgroup of G and G/H is cyclic group of order 2.

Proof :-

Since, $|G : H| = 2$, there are only two cosets of H in G. One must be H and other can be written as $Hg \; ; \; g \in G, \; g \notin H$.

To show H is normal subgroup of G, we need to show that $g^{-1}hg \in H \;\; \forall \; h \in H, \; g \in G$.

If g is an element of H, then, clearly $g^{-1}hg \in H \;\; \forall h \in H$

If g is not an element of H, suppose $g^{-1}hg \notin H$

In this case g must be an element of other eight cosets Hg and we can write $g^{-1}hg = h_1 g$ for some $h_1 \in H$. It fallow that, $g = hh_1^{-1} \in H$, which contradicts the fact that $g \notin H$.

Hence, $g^{-1}hg \in H$ $\forall g \in G$ and $h \in H$

Hence, H is normal subgroup of G.

Theorem :-

If G is finite abelian group and prime p divides order of G, then G contains an element of order p and hence a subgroup of order p.

Proof :-

We prove this result by induction on order of G. For a particular prime p, suppose that all abelian group of order less than K, whose order is divisible by p, contain an element of order p. The result is vacuosly true for groups of order 1. Now suppose that G is a group of order K. If p divides K choose any non-identity element $g \in G$. Let, t be order of the element g.

Case I :-

If p divides t, say $t = pr$, then, g^r is an element of order p. This fallows because g^r is not the identity, but $(g^r)^p = g^t = e$ and p is prime.

Case II :-

If p does not divide t, let K be the subgroup generated by g. Since G is abelian, K is normal and quotient group G/K has order $|G|/t$, which is divisible by p. Therefore by induction hypothesis, G/K has an element of order p, say Kh. If u is the order of h in G, then $h^u = e$ and, $(Kh)^u = Kh^u = K$. Since, Kh has order p in G/K, u is multiple of p and we are back to case I.

The result now follow from the principle of mathematical induction.

Example :-

Show that A_5 has no proper normal subgroups.

Solution :-

A_5 contain three types of non-identity element; 3-cycles, 5-cycles and pairs of disjoint transparition. Suppose, N is normal subgroup of A_5 that contains more than one element.

Case-I :-

Suppose, N contains the 3-cycle $(a\,b\,c)$. from defination of normal subgroup $g^{-1}\circ(a\,b\,c)\circ g \in N$ for all $g \in A_5$. If we take $g = (a\,b)\circ(c\,d)$,

$(a\,b)\circ(c\,d)\circ(a\,b\,c)\circ(a\,b)\circ(c\,d) = (a\,d\,b) \in N$

and also, $(a\,d\,b)^{-1} = (a\,b\,d) \in N$

In a similar way, we can show that N contains every 3-cycles. Therefore, N must be the entire alternating group.

Case-II :-

Suppose, N contains the 5-cycle $(a\,b\,c\,d\,e)$, Then,

$$(a\,b\,c)^{-1} \circ (a\,b\,c\,d\,e) \circ (a\,b\,c) = (a\,c\,b) \circ (a\,b\,c\,d\,e) \circ (a\,b\,c)$$
$$= (a\,b\,d\,e\,c) \in N$$

$$(a\,b\,c\,d\,e) \circ (a\,b\,c\,d\,e)^{-1} = (a\,b\,c\,d\,e) \circ (a\,c\,e\,d\,b) = (a\,d\,c) \in N$$

We are back to case I, and hence $N = A_5$.

Case-III :-

Suppose, N contains the pair of disjoint transposition $(a\,b) \circ (c\,d)$. Then, if e is the element of $\{1, 2, 3, 4, 5\}$ not appearing in these transpositions, we have

$$(a\,b\,e)^{-1} \circ (a\,b) \circ (c\,d) \circ (a\,b\,e) = (a\,e) \circ (c\,d) \in N$$

Also, $(a\,b) \circ (c\,d) \circ (a\,e) \circ (c\,d) = (a\,e\,b) \in N$

and again we are back to case-I

We have shown that any normal subgroup of A_5 containg more than one element must be A_5 itself.

Simple Group :-

Every group G has atleast two normal subgroups namely $\{e\}$ and a group itself. These two are called improper subgroup of G. Any other subgroup is regarded as proper normal subgroup.

A group G is said to be simple if it has no proper normal subgroup.

Examples :-

(1) Every alternating group A_5, $n \geq 5$ is simple.

(2) The cyclic group C_p, where p is prime, is simple.

Morphism Theorem :-

Kernel :- (defination)

Let, G and H be a group and $f: G \to H$ is a group morphism then, kernel of f is denoted and defined as

$$\ker f = \{ g \in G \ ; \ f(g) = e_H \}$$

Proposition :-

Let, G and H be two groups and $f: G \to H$ be a group morphism, Then,

(i) $\ker f$ is normal subgroup of G.

(ii) f is one-one if and only if $\ker f = \{e_G\}$

Proof :-

→ (i) If e_G is identity of G and e_H is identity of H, then, $f(e_G) = e_H \Rightarrow e_G \in \ker f$

$$\Rightarrow \ker f \neq \phi$$

Now, let, $a, b \in \ker f$, then,

$$f(a) = e_H = f(b)$$

Now,

$$f(ab^{-1}) = f(a).f(b^{-1}) = f(a).[f(b)]^{-1}$$
$$= e_H \cdot e_H^{-1} = e_H$$

$$\Rightarrow ab^{-1} \in \ker f$$
$$\Rightarrow \ker f \subseteq G.$$

Now to prove that $\ker f$ is normal subgroup of G.

let, $g \in G$ and $a \in \ker f$, then,

$$f(g^{-1}ag) = f(g^{-1}) f(a) f(g)$$
$$= f(g^{-1}) \cdot e_H \cdot f(g)$$
$$= f(g^{-1}) f(g)$$
$$= f(g^{-1} \cdot g)$$
$$= f(e_G)$$
$$= e_H$$

$\Rightarrow f(g^{-1}ag) = e_H$ for $g \in G, a \in \ker f$

$\Rightarrow f\, g^{-1}ag \in \ker f$

Hence, $\ker f$ is normal subgroup of G.

Proof :-

→ (ii) Let, suppose $\ker f = \{e_G\}$, then to prove f is one-one.
Let, $f(g_1) = f(g_2)$ for $g_1, g_2 \in G$.

$$f(g_1) \cdot [f(g_2)]^{-1} = e_H$$

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

$$f(g_1 \cdot g_2^{-1}) = e_H \qquad \because (f \text{ is group morphism})$$

$$\Rightarrow g_1 \cdot g_2^{-1} \in \ker f$$

$$\Rightarrow g_1 \cdot g_2^{-1} = e_G \qquad \because \ker f = \{e_G\}$$

$$\Rightarrow g_1 = e_G g_2$$

$$\Rightarrow g_1 = g_2$$

$\Rightarrow f$ is one-one.

Conversely, Assume f is one-one, then we have to prove that $\ker f = \{e_G\}$

Let, $a \in \ker f$, then $f(a) = e_H$

But, $f(e_G) = e_H$, Therefore

$$f(a) = f(e_G)$$

Since, f is one-one, So,

$$a = e_G$$

$$\Rightarrow \ker f = \{e_G\}$$

Hence, proved.

Proposition :-

For any group morphism $f : G \to H$, the image of f,

$$Imf = \{ f(g) ; g \in G \}$$ is a subgroup of H.

Proof :-

Let, $f(g_1), f(g_2) \in Imf$ for $g_1, g_2 \in G$.

Then, $e_H = f(e_G) \in Imf$

$$f(g_1) \cdot f(g_2) = f(g_1 g_2) \in Imf$$

and,

$$f(g)^{-1} = f(g^{-1}) \in Imf$$

Hence, Imf is subgroup of H.

First Isomorphism Theorem :-

Statement :-

Let, K be the kernel of group morphism $f : G \to H$. Then $\frac{G}{K}$ is isomorphic to image of f and isomorphism $\psi : \frac{G}{K} \longrightarrow Imf$ is defined by $\psi(Kg) = f(g)$.

Proof :-

Let, $K = \ker f$, then, $\frac{G}{\ker f} = \frac{G}{K} = \{ Kg ; g \in G \}$

Next, $Imf = \{ f(g) ; g \in G \}$

Now define a mapping,

$\psi : \frac{G}{K} \longrightarrow Imf$ by $\psi(Kg) = f(g)$

ψ is well-defined :-

let, $Kg_1 = Kg_2$ for $g_1, g_2 \in G$

$Kg_1 g_2^{-1} = K \Rightarrow g_1 g_2^{-1} \in K \Rightarrow g_1 g_2^{-1} \in \ker f$

So, $f(g_1 g_2^{-1}) = e_H$

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

$\Rightarrow f(g_1) . [f(g_2)]^{-1} = e_H$

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

$\Rightarrow \psi(Kg_1) = \psi(Kg_2)$

$\Rightarrow \psi$ is well-defined.

ψ is a Morphism.

let, $Kg_1, Kg_2 \in G/K$ for $g_1, g_2 \in G$

Now, $\psi[(Kg_1)(Kg_2)] = \psi[K(g_1 g_2)]$

$= f(g_1 g_2)$

$= f(g_1) . f(g_2)$

$= \psi(Kg_1) . \psi(Kg_2)$

$\Rightarrow \psi$ is morphism.

ψ is one-one.

let, $\psi(g_1 K) = \psi(g_2 K)$ then, $f(g_1) = f(g_2)$

$\Rightarrow f(g_1) . [f(g_2)]^{-1} = e_H$

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

$\Rightarrow g_1 g_2^{-1} \in \ker f$

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

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

$\Rightarrow K g_1 = K g_2$

$\Rightarrow \psi$ is one-one.

ψ is onto :-

As for every $f(g) \in \mathrm{Im} f$, we have $g \in G$ and then $Kg \in \frac{G}{K}$ such that $\psi(Kg) = f(g)$.

Hence, ψ is onto.

Hence, ψ is an isomorphism.

Thus, $\frac{G}{K} \cong \mathrm{Im} f$ or, $\frac{G}{\ker f} \cong \mathrm{Im} f$.

Examples :-

(i) The function $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ defined by $f(x) = [x]$, has $n\mathbb{Z}$ as its kernel and therefore, by morphism theorem, $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \mathbb{Z}_n$

$\ker f = \{x \in \mathbb{Z};\ x \equiv 0 \pmod n\} = n\mathbb{Z}$

(ii) If f is identity morphism from a G to itself, the morphism theorem implies that, $\frac{G}{\{e\}} \cong G$.

Proposition :-

A_n is a normal subgroup of S_n, $\frac{S_n}{A_n} \cong C_2$ and $|A_n| = \frac{1}{2} n!$.

Proof :-

The alternating group A_n is of index 2 in S_n i.e. $[S_n : A_n] = 2$

Therefore, by proposition, A_n is normal subgroup of S_n.

Consider, the cyclic group of order 2 i.e. $C_2 = \{-1, +1\}$ under multiplication, and define a function

$$f : S_n \to \{1, -1\} \text{ by } f(\sigma) = \begin{cases} 1 & \text{if } \sigma D = D \\ -1 & \text{if } \sigma D = -D \end{cases}$$

Then, f is surjective morphism and the kernel of f is the group A_n of even permutation.

Since, the order of S_n is 2 and $|A_n| = \frac{1}{2} n!$ (already proved)

So, the morphism theorem is

$$\frac{|S_n|}{|A_n|} = \frac{n!}{\frac{1}{2} n!} = 2$$

Hence, $\frac{S_n}{A_n} \cong C_2$

Example :-

Show that the Quotient group $\mathbb{R}/\mathbb{Z}$ of real numbers module 1 is isomorphic to circle group $W = \{e^{i\theta} \in \mathbb{C} ; \theta \in \mathbb{R}\}$.

Solution :-

The set W consists of point on circle of complex numbers of unit modulus and forms a group under multiplication.

Defined the function $f : \mathbb{R} \to W$ by $f(x) = e^{2\pi i x}$

This is morphism from $(\mathbb{R}, +)$ to $(W, \cdot)$, because

$$f(x+y) = e^{2\pi i(x+y)} = e^{2\pi i x} \cdot e^{2\pi i y} = f(x) \cdot f(y).$$

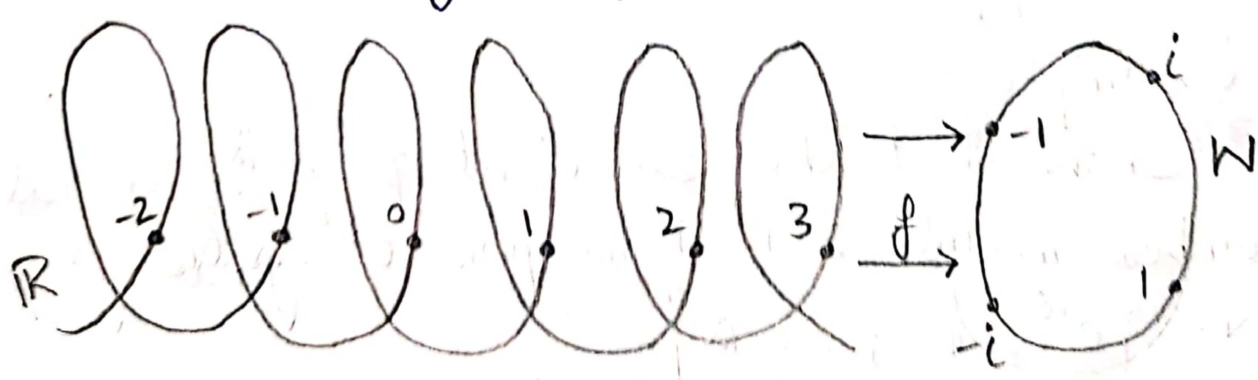
The morphism f is clearly surjective. and

$$\ker f = \{x \in \mathbb{R} ;\ e^{2\pi i x} = 1\} = \mathbb{Z}$$

Therefore, the morphism theorem implies that

$$\frac{\mathbb{R}}{\mathbb{Z}} \cong W.$$

The quotient group $\frac{\mathbb{R}}{\mathbb{Z}}$ is the set of equivalence classes of R under the relation defined by $x \equiv y \pmod{\mathbb{Z}}$ if and only if the real number x and y differ by an integer. This quotient space $\frac{\mathbb{R}}{\mathbb{Z}}$ is called the group of real numbers module 1.



Morphism $f : \mathbb{R} \to W$

Proposition :-

If G and H are finite groups whose order are relatively prime, there is only one morphism from G to H, the trivial one.

Proof :-

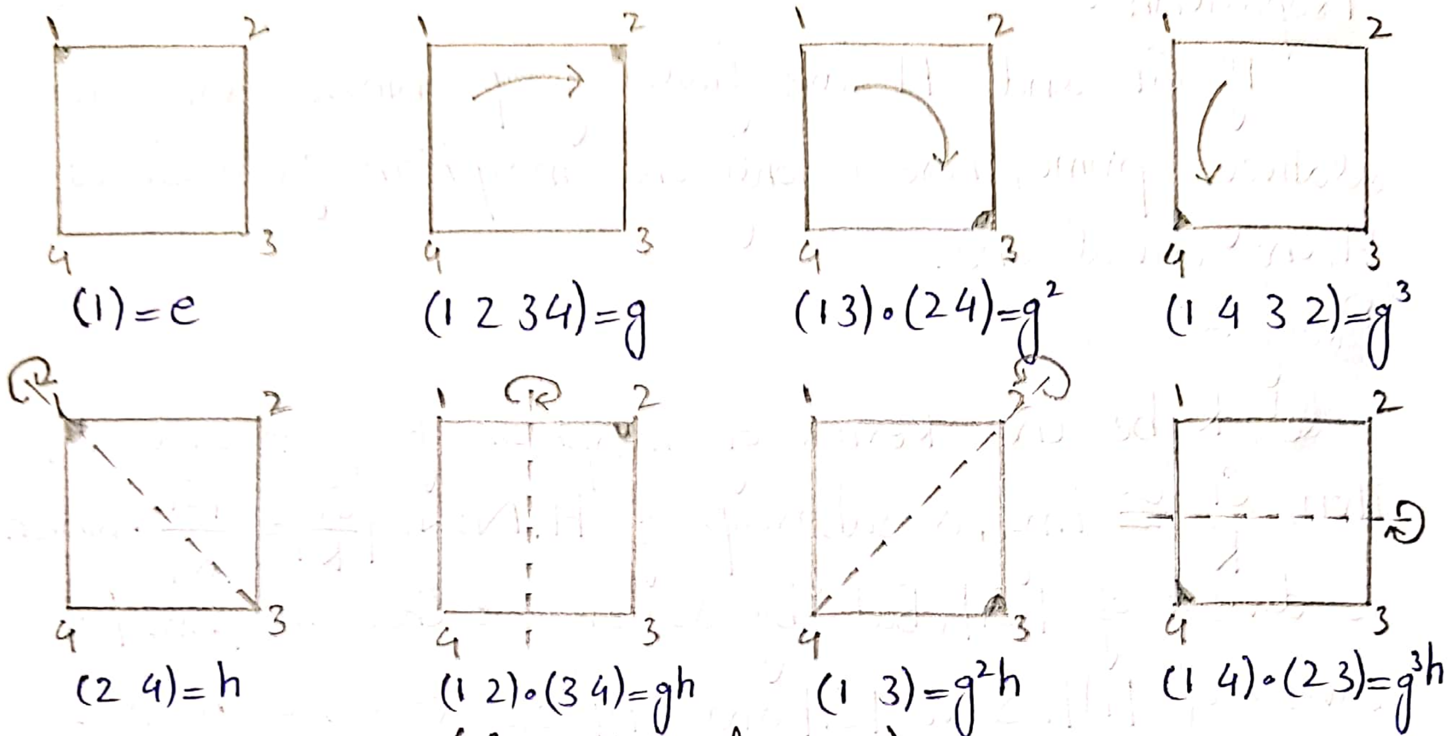
Let, K be the kernel of morphism f from G to H, Then, $\frac{G}{K} \cong Im f$, a subgroup of H. Now, $\left|\frac{G}{K}\right| = \frac{|G|}{|K|}$, which is divisor of $|G|$, But by lagrange's theorem, $|Im f|$ is divisor of $|H|$. Since, $|G|$ and $|H|$ are relatively prime, we must have $\left|\frac{G}{K}\right| = |Im f| = 1$. Therefore $K = G$. So, $f : G \rightarrow H$ is trivial morphism defined by $f(g) = e_H$ for all $g \in G$.

Example :-

Find all the subgroups and quotient groups of D_4, the symmetery group of a square and draw the posets diagram of its subgroups.

Solution :-

Any symmetry of square induced a permutation of its vertices. This define a group morphism $f : D_4 \rightarrow S_4$ This is not an isomorphism because $|D_4| = 8$ and $|S_4| = 24$ The kerf consists of symmetries fixing the vertices and so consists of identity only. Therefore, by morphism theorem, D_4 is isomorphic to image to f in S_4.

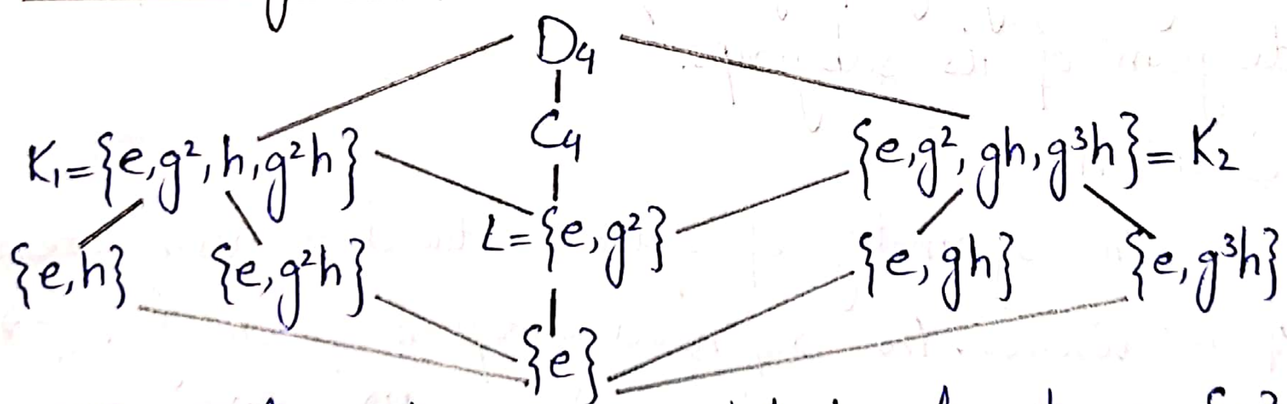


(Symmetries of square)

Order of Symmetries of square :-

Elements of D_4	e	g	g^2	g^3	h	gh	g^2h	g^3h
Order of element	1	4	2	4	2	2	2	2

Posets diagram of D_4 :-



The cyclic subgroups generated by element are $\{e\}$, $C_4=\{e,g,g^2,g^3\}$, $\{e,g^2\}$, $\{e,h\}$, $\{e,gh\}$, $\{e,g^2h\}$ and $\{e,g^3h\}$. By Lagrange's theorem, any proper subgroup must have order 2 or 4. Since any group of order 2 is cyclic, the only proper subgroup that are not cyclic are of order 4.

To find the quotient group, we must determine which subgroups are normal.

The trivial group and whole group, $\{e\}$ and D_4 are normal subgroups, Since, C_4, K_1 and K_2 have index 2 in D_4, So, they are normal. Now,

Subgroup H :-	left cosets gH :-	right cosets Hg :-
$\{e, h\}$	$\{g, gh\}$	$\{g, hg\} = \{g, g^3h\}$
$\{e, g^2h\}$	$\{g, g^3h\}$	$\{g, g^2hg\} = \{g, gh\}$
$\{e, gh\}$	$\{g, g^2h\}$	$\{g, ghg\} = \{g, h\}$
$\{e, g^3h\}$	$\{g, h\}$	$\{g, g^3hg\} = \{g, g^2h\}$

For each of these above subgroups, left and right cosets are different, therefore, none of these are normal.

Left cosets of L :-	Right Cosets of L :-
$L = \{e, g^2\}$	$L = \{e, g^2\}$
$gL = \{g, g^3\}$	$Lg = \{g, g^3\}$
$hL = \{h, hg^2\} = \{h, g^2h\}$	$Lh = \{h, g^2h\}$
$ghL = \{gh, ghg^2\} = \{gh, g^3h\}$	$Lgh = \{gh, g^3h\}$

This shows that $L = \{e, g^2\}$ is normal subgroup.

Hence, $\frac{D_4}{C_4}$, $\frac{D_4}{K_1}$, $\frac{D_4}{K_2}$ and $\frac{D_4}{L}$ are quotient group of D_4.

The multiplication table for D_4/L shows that it is isomorphic to Klein 4-group.

$\circ$	L	Lh	Lg	Lg^2
L	L	Lh	Lg	Lgh
Lh	Lh	L	Lgh	Lg
Lg	Lg	Lgh	L	Lh
Lgh	Lgh	Lg	Lh	L

Direct Product :-

Let, G and H be two groups, then

$$G \times H = \{(g,h) ; g \in G, h \in H\}$$

$G \times H$ is called direct product.

Proposition :-

If $(G,\circ)$ and $(H,*)$ are two group, then $(G\times H, \cdot)$ is a group under the operation '$\cdot$' defined by

$$(g_1,h_1)\cdot(g_2,h_2) = (g_1\circ g_2, h_1 \circ h_2)$$

The group $(G\times H,\circ)$ is called direct product of $(G,\circ)$ and $(H,*)$.

Proof :-

Since, $(G,\circ)$ and $(H,*)$ are groups, So, all axioms of groups follow from the axioms for $(G,\circ)$ and $(H,*)$.

The identity of $G\times H$ is (e_G, e_H) and every $(g,h) \in G\times h$ has inverse in form of (g^{-1}, h^{-1}).

Example :-

Write down the table for direct product of C_2 with itself.

Solution :-

Let, $C_2 = \{e,g\}$

$C_2 \times C_2 = \{(e,e),(e,g),(g,e),(g,g)\}$

The group $C_2\times C_2$ is isomorphic to Klein 4-group.

$\cdot$	(e,e)	(e,g)	(g,e)	(g,g)
(e,e)	(e,e)	(e,g)	(g,e)	(g,g)
(e,g)	(e,g)	(e,e)	(g,g)	(g,e)
(g,e)	(g,e)	(g,g)	(e,e)	(e,g)
(g,g)	(g,g)	(g,e)	(e,g)	(e,e)

Theorem :-

If $\gcd(m,n)=1$, then, $C_{mn} \cong C_m \times C_n$.

Proof :-

let, g, h and k be generators of C_{mn}, C_m and C_n respectively. Define, $f: C_{mn} \to C_m \times C_n$ by

$$f(g^r) = (h^r, k^r) \text{ for } r \in \mathbb{Z}.$$

If $g^r = g^{r'}$ then, $r-r'$ is multiple of mn, So, $r-r'$ is a multiple of m and n. Hence,

$$h^r = h^{r'} \text{ and } k^r = k^{r'}$$

$\Rightarrow f$ is well defined.

Now, $f(g^r \cdot g^s) = f(g^{r+s}) = (h^{r+s}, k^{r+s}) = (h^r \cdot h^s, k^r \cdot k^s)$

$= (h^r, k^r) \cdot (h^s, k^s) = f(g^r) \cdot f(g^s)$

$\Rightarrow f$ is group morphism.

If $g^r \in \ker f$, then $h^r = e$ and $k^r = e$, therefore r is divisible by m and n, and since $\gcd(m,n)=1$, So, r is divisible by mn. Hence, $\ker f = \{e\}$ and image of f is isomorphic to C_{mn}. However, $|C_{mn}| = mn$ and $|C_m \times C_n| = |C_m| \cdot |C_n|$
$= mn$

Hence,

$\operatorname{Im} f = C_m \times C_n$ and f is an isomorphism.

Corollary :-

let, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots\cdots p_r^{\alpha_r}$ where $p_1, p_2, \cdots, p_r$ are distinct primes, Then

$$C_n \cong C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \cdots\cdots \times C_{p_r^{\alpha_r}}$$

Remarks :-

→ (1) If m and n are not coprime, then C_{mn} is never isomorphic to $C_m \times C_n$.

e.g. $C_2 \times C_2$ is not isomorphic to C_4, because $C_2 \times C_2$ contains no element of order 4.

→ (2) The order of element (h,k) in $H \times K$ is l.c.m. of order h and k, because $(h,k)^r = (h^r, k^r) = (e,e)$ if and only if $h^r = e$ and $k^r = e$. Hence, if $\gcd(m,n) > 1$, then, order of (h,k) in $C_m \times C_n$ is less than, mn.

→ (3) Any finite abelian group is isomorphic to direct product of cyclic groups. For example,

$$C_8 \times C_3 \cong C_{24}$$

$$C_2 \times C_4 \times C_3 \cong C_6 \times C_4 \cong C_2 \times C_{12}$$

$$C_2 \times C_2 \times C_2 \times C_3 \cong C_2 \times C_2 \times C_6$$

Theorem :-

If $(G, \cdot)$ is finite group for which every element $g \in G$ satisfies $g^2 = e$, then, $|G| = 2^n$ for some $n \geq 0$ and G is isomorphic to the n-fold direct product

$$C_2^n = C_2 \times C_2 \times \cdots \times C_2$$

Proof :-

Every element in G has order 1 or 2 and the identity is only element of order 1. Therefore, every element has its own inverse. The group G is abelian because, for any $g, h \in G$,

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

Choose, element $a_1, a_2, ----, a_n \in G$, So that $a_i \neq e$ and a_i cannot be written as product of powers of $a_1, a_2, ---, a_{i-1}$. Furthermore, choose n maximal, so that every element can be written in term of elements a_i. If C_2 is generated by g, we define a mapping $f: C_2^n \to G$ by

$$f(g^{r_1}, g^{r_2}, ----, g^{r_n}) = a_1^{r_1} a_2^{r_2} ---- a_n^{r_n}$$

It is an isomorphism. It is well defined for all integers r_i, because if $g^{r_i} = g^{q_i}$, then, $a_i^{r_i} = a_i^{q_i}$.

Now,

$$f((g^{r_1}, g^{r_2}, ---, g^{r_n}) \cdot (g^{s_1}, g^{s_2}, ---, g^{s_n})) = f(g^{r_1+s_1}, ----, g^{r_n+s_n})$$

$$= a_1^{r_1+s_1} ---- a_n^{r_n+s_n}$$

$$= a_1^{r_1} --- a_n^{r_n} \cdot a_1^{s_1} ---- a_n^{s_n} \quad \because (G \text{ is abelian})$$

$$= f(g^{r_1}, ----, g^{r_n}) \cdot f(g^{s_1}, ---, g^{s_n})$$

$\Rightarrow f$ is group morphism.

let, $(g^{r_1}, ---, g^{r_n}) \in \ker f$. Suppose, r_i is last odd exponent, so that $r_{i+1}, r_{i+2}, ----, r_n$ are all even. Then,

$$a_1^{r_1} ---- a_{i-1}^{r_{i-1}} a_i = e \text{ and, } a_i = a_i^{-1} = a_1^{r_1} --- a_{i-1}^{r_{i-1}}$$

which is contradiction.

Therefore, all exponent are even and f is injective. The choice of element a_i guarantees that f is surjective. Hence, f is required isomorphism.

Example :-

Describe all the group morphism from C_{10} to $C_2 \times C_5$. Which of these are isomorphic.

Solution :-

Since, C_{10} is cyclic group, generated by g. let, h and k be generator of C_2 and C_5 respectively. Consider the function, $f_{r,s} : C_{10} \to C_2 \times C_5$ which maps g to element $(h^r, h^s) \in C_2 \times C_5$. Then if $f_{r,s}$ is morphism

$$f_{r,s}(g^n) = (h^{rn}, k^{sn}) \text{ for } 0 \le n \le 9$$

This would be true for all integers n, because if $g^n = g^m$, then, $10 | n-m$. Hence, $2 | n-m$ and $5 | n-m$ and $h^{rn} = h^{rm}$ and $k^{ns} = k^{ms}$.

We now verify that $f_{r,s}$ is morphism for any r, s.

$$f_{r,s}(g^a g^b) = f_{r,s}(g^{a+b}) = (h^{(a+b)r}, k^{(a+b)s}) = (h^{ar}, k^{as})(h^{br}, k^{bs})$$

$$= f_{r,s}(g^a)\, f_{r,s}(g^b)$$

Therefore, there are ten morphism, $f_{r,s}$ from C_{10} to $C_2 \times C_5$ corresponding to the ten elements (h^r, h^s) of $C_2 \times C_5$. Now,

$$\ker f_{r,s} = \{ g^n ; (h^{rn}, k^{sn}) = (e,e) \}$$

$$= \{ g^n ; rn \equiv 0 \pmod 2 \text{ and } sn \equiv 0 \pmod 5 \}$$

Hence, $\ker f_{r,s} = \{e\}$ if $(r,s) = (1,1), (1,2), (1\,3)$ or, $(1,4)$

While, $\ker f_{0,0} = C_{10}$, $\ker f_{1,0} = \{e, g^2, g^4, g^6, g^8\}$,

$\ker f_{0,s} = \{e, g^5\}$ if $s = 1, 2, 3$ or 4.

If $\ker f_{r,s}$ contain more than one element, $f_{r,s}$ is not injective and cannot be an isomorphism. By Morphism theorem,

$$\frac{|C_{10}|}{|\ker f_{r,s}|} = |\mathrm{Im}\, f_{r,s}|$$

and, if $\ker f_{r,s} = \{e\}$, then, $|\mathrm{Im}\, f_{r,s}| = 10$, So, $f_{r,s}$ is surjective also. Therefore, isomorphism are $f_{1,1}, f_{1,2}, f_{1,3}$ and $f_{1,4}$.

Lemma :-

Suppose that a and b are element of coprime order r and s, respectively, in an abelian group. Then ab has order rs.

Proof :-

Let, A and B are groups generated by a and b respectively. Since, $ab = ba$, So, we have,

$$(ab)^{rs} = a^{rs} b^{rs} = (a^r)^s (b^s)^r = e^s e^r = e$$

Suppose, $(ab)^k$, we must show that rs divides k. Observe that, $a^k = b^{-k} \in A \cap B$. Since, $A \cap B$ is subgroup of both A and B, its order divides $|A| = r$ and $|B| = s$. (By Lagrange's theorem)

Since, r and s are coprime, this implies that $|A \cap B| = 1$. It follows that $a^k = e$ and $b^{-k} = e$, So, "r divides k" and "s divides k." Hence, rs divides k.

Hence, ab has order rs.

Groups of Low order :-

→ **Order 1 :-**

Every trivial group is isomorphic to $\{e\}$.

→ **Order 2 :-**

Every group of order 2 is cyclic.

→ **Order 3 :-**

Every group of order 3 is cyclic.

→ **Order 4 :-**

Each element has order 1, 2 or 3.

(i) → If there is an element of order 4, group is cyclic.

(ii) → If not, every element has order 1 or 2, the group is isomorphic to $C_2 \times C_2$.

→ **Order 5 :-**

Every group of order 5 is cyclic.

→ **Order 6 :-**

Each element has order 1, 2, 3 or 6.

(i) → If there is an element of order 6, group is cyclic.

(ii) → If not, every element has order 1, 2 or 3. All element in group of order 6 cannot have order 1 and 2. Hence, there is an element, say 'a', of order 3. The group $H = \{e, a, a^2\}$ has index 2, and if $b \notin H$, the underlying set of group is then, $H \cup Hb = \{e, a, a^2, b, ab, a^2 b\}$. By proposition, H is normal and quotient group of H is cyclic of order 2. Hence,

$$b^r \in Hb^r = (Hb)^r = \begin{cases} H & ; r \text{ is even} \\ Hb & ; r \text{ is odd} \end{cases}$$

Therefore, b has even order. It cannot be 6. So, it must be 2. As, H is normal, $bab^{-1} \in H$. We cannot have $bab^{-1} = e$, because $a \neq e$. If $bab^{-1} = a$, then, $ba = ab$ and the entire group is abelian. This cannot happen because by above lemma, ab would have order 6. So, $bab^{-1} = a^2$ and the group is generated by a and b, with relation $a^3 = b^2 = e$ and $ba = a^2 b$. This group is isomorphic to D_3 and S_3.

→ **Order 7 :-**

Every group of order 7 is cyclic group.

→ **Order 8 :-**

Every element has order 1, 2, 4 or 8.

(i) ⟶ If there is an element of order 8, group is cyclic.

(ii) ⟶ If all element has order 1 or 2, group is isomorphic to $C_2 \times C_2 \times C_2$.

(iii) ⟶ If there is an element of order 4, then the subgroup $H = \{e, a, a^2, a^3\}$ is of index 2 and therefore normal. If $b \notin H$, then, underlying set of group is $H \cup Hb = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Now, $b^2 \in H$, But b^2 cannot have order 4, otherwise, b would have order 8. Therefore, $b^2 = e$ or a^2. As H is normal, $bab^{-1} \in H$ and has same order as 'a' because, $(bab^{-1})^k = ba^kb^{-1}$.

(iii.1) $\rightarrow$ If $bab^{-1}=a$, then, $ba=ab$, and group is abelian. If $b^2=e$, each elements written uniquely in form of $a^r b^s$, where $0 \le r \le 3$ and $0 \le s \le 1$. Hence, group is isomorphic to $C_4 \times C_2$ by mapping $a^r b^s$ to (a^r, b^s). If $b^2=a^2$, let, $c=ab$, so that $c^2=a^2b^2=a^4=e$. Each element of group can now written uniquely in form of $a^r c^s$, where $0 \le r \le 3$ and $0 \le s \le 1$ and group is still isomorphic to $C_4 \times C_2$.

(iii.2) $\rightarrow$ If $bab^{-1}=a^3$ and $b^2=e$, the group is generated by a and b with relations $a^4=b^2=e$, $ba=a^3b$. This is isomorphic to D_4.

(iii.3) $\rightarrow$ If $bab^{-1}=a^3$ and $b^2=a^2$, then, this group is isomorphic to quaterion group Q_8,

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

The isomorphism maps $a^r b^s$ to $i^r j^s$.

Remarks :-

Any group with eight or fewer element is isomorphic to exactly one group in table given as,

Order :	1	2	3	4	5	6	7	8
Abelian groups :	$\{e\}$	C_2	C_3	C_4 $C_2 \times C_2$	C_5	C_6	C_7	C_8 $C_4 \times C_2$ $C_2 \times C_2 \times C_2$
Non-abelian Group :						S_3		D_4 Q_8

Action of a group on a Set :-

The group $(G,\cdot)$ acts on a set X if there is a function,

$$\varphi : G \times X \longrightarrow X.$$

such that, when we write $g(x)$ for $\varphi(g,x)$, we have,

(i) $(g_1 g_2)(x) = g_1(g_2(x)) \ \forall \ g_1, g_2 \in G, \ x \in X$

(ii) $e(x) = x$ if e is identity of G and $x \in X$.

Proposition :-

If g is an element of G acts on set X, then, the function $g : X \to X$, which maps x to $g(x)$ is a bijection. This defines a morphism

$$\chi : G \to S(X)$$

from group G to the group of symmetries.

Proof :-

for $x, y \in X$, $g(x) = g(y)$, then,

$$g^{-1}g(x) = g^{-1}g(y) \Rightarrow e(x) = e(y)$$
$$\Rightarrow x = y$$

$\Rightarrow g : X \to X$ is injective.

for $z \in X$, we have, $g(g^{-1}(z)) = gg^{-1}(z) = e(z) = z$

$\Rightarrow g : X \to X$ is surjective.

Hence, $g : X \to X$ is bijective, and g can be considered as an element of $S(X)$, the group of symmetries of X. The function $\chi : G \to S(X)$ which takes the element $g \in G$ to the bijection $g : X \to X$ is group morphism because, $\chi(g_1 g_2)$ is function from X to X defined by $\chi(g_1 g_2)(x) = (g_1 g_2)(x) = (g_1(g_2(x)))$

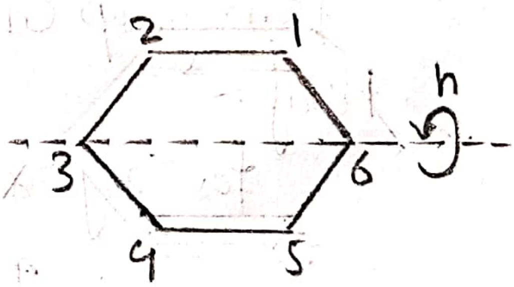
$$= \chi(g_1) \circ \chi(g_2)(x).$$

Thus, $\chi(g_1 g_2) = \chi(g_1) \circ \chi(g_2)$. Hence, Proved.

Def. → If $\ker \chi = \{e\}$, then, χ is injective and group G is said to act faithfully on set X. <u>G acts faithfully on X</u> if only element of G, which fixes every element of X, is the identity $e \in G$. In this case, we identify G with $\mathrm{Im}\chi$ and regareded G as subgroup of $S(X)$.

Examples :-

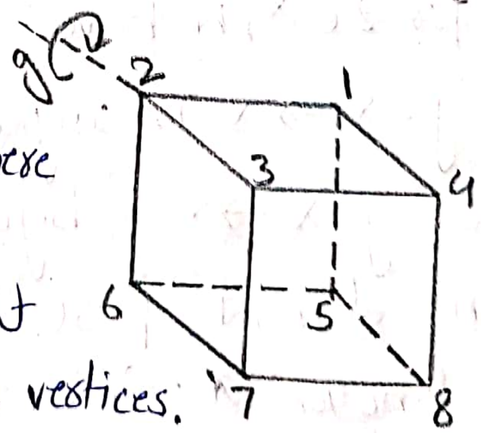
→ **(1)** Consider, $C_2 = \{e, h\}$, acting on regular hexagon, where h reflecting the hexagon about the joining line of vertex 3 to 6.



Then C_2 acts faithfully and can be identified with the subgroup $\{(1), (15)\circ(24)\}$ of D_6.

→ **(2)**

Consider, $C_3 = \{e, g, g^2\}$ acts faithfully on cube, where g rotates the cube through one-third of revoulation about a line joining two opposite vertices.



This group action can be considered as subgroup $\{(1), (163)\circ(457), (136)\circ(475)\}$ of symmetry group.

Stabilizer :-

Let, G be a group and X be a set. If G acts on a set X and $x \in X$, then,

$$Stab\,x = \{g \in G \,;\, g(x) = x\}$$

is a subgroup of G, called stabilizer of x. It is the set of elements of G that fix x.

Proof :-

Let, $g_1, g_2 \in stab\,x$, then,

$$(g_1 g_2)(x) = g_1(g_2(x)) = g_1(x) = x$$

$$\Rightarrow g_1 g_2 \in stab\,x$$

Let, $g \in stab\,x$, then $g^{-1}(x) = x$

$$\Rightarrow g^{-1} \in stab\,x$$

Hence, $stab\,x$ is a subgroup of G.

Orbit :-

The set of all images of an element $x \in X$ under the action of a group G is called the orbit of x under G, and denoted as

$$Orb\,x = \{g(x) \,;\, g \in G\}$$

The orbit of x is the equivalence class of x under the equivalence relation on X in which x is equivalent to y if and only if $y = g(x)$ for some $g \in G$.

For example, the orbit of cyclic group C_2 acting on hexagon are $\{1,5\}, \{2,4\}, \{3\}$ and, $\{6\}$.

Example :- (Special orthogonal group)

$SO(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} ; \theta \in \mathbb{R} \right\}$ is a group under matrix multiplication. This is called special orthogonal group. It is isomorphic to circle group W. $SO(2)$ acts on $\mathbb{R}^2$. The matrix $M \in SO(2)$ takes the vector $x \in \mathbb{R}^2$ to vector Mx. The orbit of any element $x \in \mathbb{R}^2$ is the circle through x with centre at origin. Since the origin is only the fixed for any of non-identity transformation, the stablizer of the origin is the whole group, whereas the stabilizer of any other element is the subgroup consisting of the identity matrix only.

Lemma :-

If G acts on X, then for each $x \in X$,

$$|G : \text{Stab}\, x| = |\text{Orb}\, x|$$

Proof :-

Let, $H = \text{stab}\, x$ and define the function,

$$\xi : \frac{G}{H} \longrightarrow \text{Orb}\, x \quad \text{by} \quad \xi(Hg) = g^{-1}(x).$$

This is well-defined because if $Hg = Hk$, then, $k = hg$ for some $h \in H$, so, $k^{-1}(x) = (hg)^{-1}(x) = g^{-1}h^{-1}(x) = g^{-1}(x)$

Since, $h^{-1} \in H = \text{stab}\, x$.

The function ξ is surjective by definitation of orbit of x. It is also injective because $\xi(Hg_1) = \xi(Hg_2)$ implies that $g_1^{-1}(x) = g_2^{-1}(x)$, So, $g_2 g_1^{-1}(x) = x$ and $g_2 g_1^{-1} \in \text{stab}\, x$

$\Rightarrow \xi : \frac{G}{H} \longrightarrow \text{Orb}\, x$ is bijection, and result follow.

Remarks :-

$\xi : \frac{G}{H} \to Orb\,x$ is not a morphism, $\frac{G}{H = Stab\,x}$ is just a set of cosets because $Stab\,x$ is not necessarily normal. Furthermore, we have placed no group structure on $Orb\,x$.

Theorem :-

If the finite group G acts on a set X, then for each $x \in X$, $\quad |G| = |Stab\,x||Orb\,x|$

Proof :-

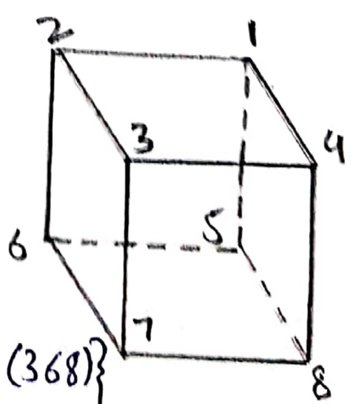
If G is finite group with subgroup H, then by corollary
$$|G : H| = |G|/|H|$$
Since, $Stab\,x$ is subgroup of G, So, we have,
$$|G : Stab\,x| = \frac{|G|}{|Stab\,x|}$$
Also, by above lemma, $|G : Stab\,x| = |Orb\,x|$, Hence,
$$|Orb\,x| = \frac{|G|}{|Stab\,x|}$$
$\Rightarrow \quad |G| = |Orb\,x|.|Stab\,x| \quad$, Hence, proved.

Example :-

Find the number of proper rotations of a cube.

Solution :-

Let, G be a group of proper rotations of a cube, i.e. rotation can be carried out in three dimensions.



The stabilizer of vertex 1 is

$Stab\,1 = \{(1), (2\,4\,5)\circ(3\,8\,4), (2\,5\,4)\circ(3\,6\,8)\}$

The orbit of 1 is the set of all vertices, because there is an element of G that will take 1 to any other vertex. Therefore, $|G| = |\text{Stab}\, x||\text{Orb}\, x|$

$$= |\text{Stab}\, 1||\text{Orb}\, 1| = 3 \times 8 = 24$$

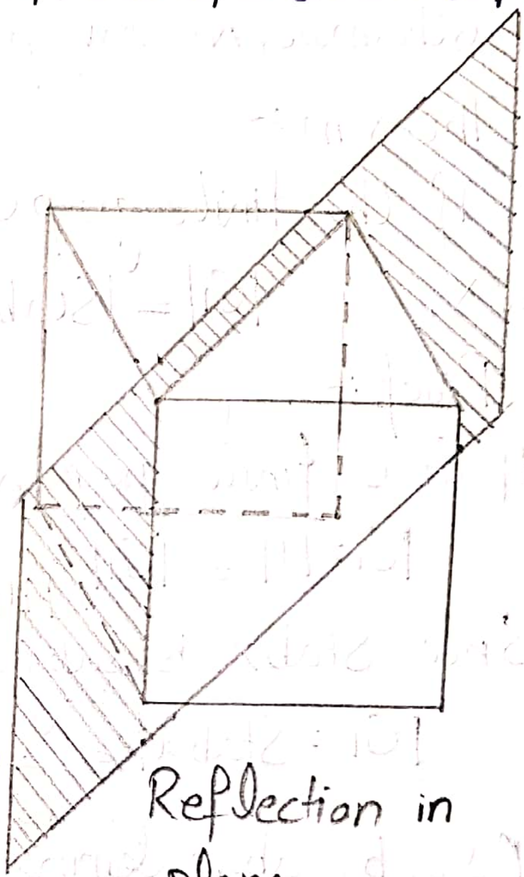
The full symmetry of cube would include improper rotations such as the reflection in plane as shown in figure.

This induce the permutation $(24)\circ(68)$ on vertices.

Under this group,

Stab 1 is

$\{(1), (245)\circ(368), (254)\circ(386), (24)\circ(68), (25)\circ(38), (45)\circ(36)\}$



Reflection in plane.

So, the order of full symmetry group of cube is

$$|\text{Stab}\, 1||\text{Orb}\, 1| = 6 \times 8 = 48.$$

Therefore, there are 24 proper and 24 improper rotations of cube.

Semi-Group :-

Let, $X \neq \phi$ be a set, then X is said to be a semi-group under binary operation '$*$' if

(i) $(X, *)$ is closed.

(ii) $(X, *)$ is associative, i.e. $a*(b*c) = (a*b)*c \ \forall a, b, c \in X$

Monoid :-

Let, $M \neq \phi$ be a set, then M is said to be monoid under binary operation '$*$' if

(i) $(M, *)$ is closed.

(ii) $(M, *)$ is associative,

i.e. $a*(b*c) = (a*b)*c \ \forall \ a, b, c \in M$.

(iii) There exists an identity, $e \in M$, such that,

$$a*e = e*a = a \ \forall \ a \in M.$$

Examples :-

(1) All groups are monoid and semigroup. However, $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$, which do not have inverse are also monoid.

(2) $(\mathbb{P}, +)$ is semigroup, but not monoid, because the set of positive integers $\mathbb{P}$, does not contain 0.

Commutative Monoid :-

A monoid $(M, *)$ is called commutative monoid if the operation $*$ is commutative.

e.g.

$(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}, \cdot)$, $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n, \cdot)$ are all commutative monoid.

Proposition :-

Let, X be any set and let $X^X = \{f : X \to X\}$ be the set of all functions from X to itself. Then, $(X^X, \circ)$ is a monoid, called transformation monoid of X.

Proof :-

Let, $f, g \in X^X$, then, $f \circ g \in X^X \Rightarrow X^X$ is closed.

for, $f, g, h \in X^X$, we have, for $x \in X$

$(f \circ (g \circ h))(x) = f(g(h(x)))$ and, $((f \circ g) \circ h)(x) = f(g(h(x)))$

$\Rightarrow X^X$ is associative.

The identity function $1_x : X \to X$ defined by $1_x(x) = x$ is the identity for composition.

Hence, $(X^X, \circ)$ is monoid.

Example :-

If $X = \{0, 1\}$, write out the table for transformation monoid, $(X^X, \circ)$.

Solution :-

X^X, has four elements, e, f, g, h defined as follow

$e(0) = 0 \quad f(0) = 0$

$g(0) = 1 \quad h(0) = 1$

$e(1) = 1 \quad f(1) = 0$

$g(1) = 0 \quad h(1) = 1$

$\circ$	e	f	g	h
e	e	f	g	h
f	f	f	f	f
g	g	h	e	f
h	h	h	h	h

(Transformation monoid of $\{0, 1\}$.)

The table for $(X^X, \circ)$ is given as:

e.g. $g \circ f(0) = g(f(0))$

$= g(0) = 1$

$g \circ f(1) = g(f(1)) = g(0) = 1$

and, so on.

Example :-

Prove that, $(\mathbb{Z}, *)$ is a commutative monoid, where,

$x * y = 6 - 2x - 2y + xy$ for $x, y \in \mathbb{Z}$.

Solution :-

for any $x * y \in \mathbb{Z}$, $x * y = y * x$ for $x, y \in \mathbb{Z}$

Hence, $*$ is commutative binary operation on $\mathbb{Z}$.

Now, $x*(y*z) = x\,\cancel{6+}*(6-2y-2z+yz)$

$= 6-2x+(-2+x)(6-2y-2z+yz)$

$= -6+4x+4y+4z-2xy-2xz-2yz+xyz$

Also, $(x*y)*z = (6-2x-2y+xy)*z$

$= 6+(-2+z)(6-2x-2y+xy)-2z$

$= -6+4x+4y+4z-2xy-2xz-2yz+xyz$

$= x*(y*z)$

$\Rightarrow$ $*$ is associative.

Suppose, $e*x = x$, then, $6-2e-2x+ex = x$ and $6-2e-2x+ex=0$. This implies $(x-2)(e-3)=0$

Hence, $e*x = x \;\forall\, x \in \mathbb{Z}$ if and only if $\cancel{x}e=3$.

Hence, $(\mathbb{Z}, *)$ is commutative monoid with 3 as identity.

Cyclic Monoid :-

A monoid generated by one element is called cyclic monoid, e.g. $(\mathbb{N}, +)$ is generated by single element 1.

A finite cyclic group is also a cyclic monoid, But the infinite cyclic group is not cyclic monoid, e.g. $(\mathbb{Z}, +)$, it needs atleast two elements to generate, 1 and -1.

Not all finite cyclic monoid are groups, For example, let, $\sigma \in \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 4 & 3 \end{pmatrix} \in X^X$, where $X = \{1, 2, 3, 4\}$

Then, M is $\{\varepsilon, \sigma, \sigma^2, \sigma^3\}$ is a cyclic monoid but not a cyclic group because, $\sigma^4 = \sigma^2$.

Free Monoid :-

A computer recieves its information from an input terminal that feeds in a sequence of symbols, usually binary digits consisting of 0's and 1's. If one sequence is fed in after another, the computer receives one long sequence that is the concatenation of two sequence. These input sequences together with the binary operation of concatenation form a monoid that is called free monoid generated by the input symbols.

let, A be any set and let, A^n be the set of n-tuples of elements in A. The element of A^n is called word of length n from A.

A word of length 0 is called empty string and denoted as Λ. For example, if $A = \{a, b\}$, then, baabbaba$\in A^8$; $A^0 = \{\Lambda\}$, and

$A^3 = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$

Defination :-

let, FM(A) denotes the set of all words from A, more formally,

$$FM(A) = A^0 \cup A \cup A^2 \cup A^3 \cup \cdots = \bigcup_{n=0}^{\infty} A^n.$$

Then, $(FM(A), *)$ is called free monoid generated by A, where, the operation $*$ is concantenation and the identity is the empty word Λ

If we do not include empty word, we obtain free semigroup generated by.

Examples:-

(i) If A consists of a single element, a, then
$FM(A) = \{\Lambda, a, aa, aaa, aaaa, \ldots\}$
and for example, $aaa * aa = aaaaa$.
This free monoid is commutative.

(ii) If $A = \{0, 1\}$, then,
$FM(A) = \{\Lambda, 0, 1, 00, 11, 000, 01, 10, 001, \ldots\}$
We have, $010 * 1110 = 0101110$
and, $1110 * 010 = 1110010$
So, this is not commutative.

Monoid Morphism:-

If $(M, *)$ and $(N, \cdot)$ are two monoids with identities e_M and e_N respectively, Then, $f: M \to N$ is a monoid morphism if

(i) $f(x * y) = f(x) \cdot f(y) \quad \forall x, y \in M$.

(ii) $f(e_M) = e_N$

A monoid isomorphism is a bijective monoid morphism.

For example:

$f: (\mathbb{N}, +) \to (\mathbb{P}, \cdot)$ defined by $f(n) = 2^n$ is monoid morphism because,

$f(m+n) = 2^{m+n} = 2^n \cdot 2^n = f(m) \cdot f(n) \quad \forall m, n \in \mathbb{N}$.

Theorem :-

Let, $FM(A)$ be a free monoid generated by A and let, $i : A \to FM(A)$ be a function that maps each element a of A into corresponding word of length 1, so that $i(a) = a$.

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "\ell"'] & FM(A) \arrow[d, dashed, "h"] \\ & M \end{tikzcd}$$

The function ℓ-factors through free monoid $FM(A)$.

Then, if $\ell : A \to M$ is any function into the underlying set of any monoid $(M, \cdot)$, there is a unique monoid morphism $h : (FM(A), *) \to (M, \cdot)$ s.t. $h \circ i = \ell$

Proof :-

If h satisfies $h \circ i = \ell$, then h must be defined on words of length 1 by $h(a) = \ell(a)$. Once a morphism has been defined on its generator, it is determined completely as follow:

Let, α be a word of length $n \geq 2$ in $FM(A)$. write $\alpha = \beta * c$, where "β" of length "$n-1$" and "c" of length "1". Then, we have

$$h(\alpha) = h(\beta * c) = h(\beta) \cdot h(c) = h(\beta) \cdot \ell(c)$$

Hence, h can be determined by using induction on word length.

In fact, if $\alpha = a_1 a_2 \cdots a_n$ where $a_i \in A$, then

$$h(\alpha) = \ell(a_1)\, \ell(a_2) \cdots \ell(a_n)$$

Finally, let, $h(\Lambda)$ be the identity of M.

Ring :-

A non-empty set R with two binary operations '+' and '.' define on R is said to be ring if following axioms are satisfied:

(i) $(R,+)$ is an abelian group.

(ii) $(R,\cdot)$ is monoid.

(iii) The left and right distributive law is hold.

i.e. $\forall\, a,b,c \in R$, we have,

$a.(b+c) = ab+ac$ and, $(a+b).c = ac+bc$

Remarks :-

If R is a ring under '.' and '+', then, we write it as $(R,+,\cdot)$ or simply R is ring.

Commutative Ring :-

A ring $(R,+,\cdot)$ is said to be commutative ring if '.' is commutative in R.

Unit element :-

Let, $(R,+,\cdot)$ be a ring, then an element $a \in R$ is said to be unit element if a^{-1} exists in R under "." .

If a ring contains unit element, then, it necessary contains unity.

Ring with unity :-

A ring $(R,+,\cdot)$ is said to be ring with unity if multiplicative identity, $1 \in R$,

i.e. $1\cdot a = a\cdot 1 = a$ for $a \in R$.

Division ring :-

A ring $(R, +, \cdot)$ is said to be division ring, if every non-zero element of R is unit element.

It is also called skew-field.

Examples :-

(i) $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Z}_n, +, \cdot)$ are commutative ring with unity.

(ii) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are commutative division ring.

(iii) $(M_n, +, \cdot)$ is non-commutative ring with unity, where M_n is the set of all $n \times n$ matrices with enteries from $\mathbb{R}$.

(iv) The element 'even' and 'odd' forms commutative ring $(\{even, odd\}, +, \cdot)$. 'Even' is zero of ring and 'odd' is multiplicative identity.

+	even	odd
even	even	odd
odd	odd	even

$\cdot$	even	odd
even	even	even
odd	even	odd

(v) $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, where addition and multiplication on congruence classes, modulo n, are defined by

$$[x] + [y] = [x+y] \quad \text{and} \quad [x] \cdot [y] = [xy]$$

(vi) $(\mathcal{P}(X), \Delta, \cap)$ is a commutative ring for any set X. The zero is ϕ and identity is X. In this ring $A \cap A = A$ for every element A in the ring. Such ring is called boolean ring.

Scanned with CamScanner

Proposition :-

If $(R,+,\cdot)$ is a ring with additive identity "0", then, for any $a,b,c \in R$,

(i) $a\cdot 0 = 0\cdot a = 0$

(ii) $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$

(iii) $(-a)\cdot(-b) = a\cdot b$

(iv) $(-1)\cdot a = -a$

(v) $(-1)\cdot(-1) = 1$

Proof :-

(i) $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$ (by distributivity)

$a\cdot 0 - a\cdot 0 = a\cdot 0 + a\cdot 0 - a\cdot 0$

$0 = a\cdot 0$

Similarly, $0\cdot a = 0$

(ii) $a\cdot(-b) + a\cdot b = a\cdot(-b+b) = a\cdot 0 = 0$ (using (i))

Therefore, $a\cdot(-b) = -(a\cdot b)$

Similarly, $(-a)\cdot b = -(a\cdot b)$

(iii) $(-a)(-b) = -(a(-b))$ $\quad\therefore$ by (ii)

$= a\cdot b$

(iv) $(-1)\cdot a = -(1\cdot a) = -a$ $\quad\therefore$ by (ii)

(v) $(-1).(-1) = 1\cdot 1 = 1$ $\quad$ by (ii)

Proposition :-

If $0=1$, the ring only contains one element and is called trivial ring. All other rings are called non-trivial.

Proof :-

for any element $a \in R$ in which $0=1$, we have,

$$a = a \cdot 1 = a \cdot 0 = 0$$

Therefore, the ring contain only the element 0.

Zero Divisor :-

Let, $(R,+,\cdot)$ be a commutative ring, a non-zero element $a \in R$ is called a zero divisor if $\exists$ non-zero element $b \in R$ such that

$$a \cdot b = 0 \quad \text{and} \quad b \cdot a = 0$$

Integral Domain :-

A nontrivial commutative ring is called an integral domain if it has no zero divisor.

Non-zero divisor :-

A ring R is said to be non-zero divisor if for $a,b \in R$, we have,

$a \cdot b = 0$ always implies that $a=0$ or, $b=0$.

Examples :-

(i) The ring $(\mathbb{Z}_n,+,\cdot)$ has zero divisor iff n is composite, e.g. $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

then, $\bar{2} \neq \bar{0}$ and $\bar{3} \neq 0$ But $\bar{2} \cdot \bar{3} = \bar{3} \cdot \bar{2} = 0$.

(ii) If p is prime, then $(\mathbb{Z}_p,+,\cdot)$ has no zero divisor. Hence, $(\mathbb{Z}_p,+,\cdot)$ is an integral domain.

The ring $(M_n,+,\cdot)$ has zero divisor, Hence, it is not an integral domain

Consider,

$$M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \ a,b,c,d \in \mathbb{R} (\text{or}, \mathbb{C}) \right\}$$

then,

$$\begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & -2 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

But,

$$\begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & -2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -2 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 0 \end{bmatrix}$$

Proposition :-

If a is a non zero element of an integral domain R and $a.b = a.c$, then $b = c$.

Proof :-

If $a.b = a.c$, then, $a.(b-c) = a.b - a.c = 0$

Since, R is an integral domain, it has no zero divisor.

Since, $a \neq 0$, So, $b - c = 0 \Rightarrow b = c$.

Field :- (defination)

A commutative division ring is called field.

In other words, A non-empty set F is said to be a field under binary operation '+' and '.' if fallowing axioms are hold:

(1) $(F, +)$ is abelian group.

(2) $(F - \{0\}, \cdot)$ is abelian group.

(3) The left and right distributive laws are hold.

i.e. $\forall a,b,c \in F$, we have,

$a.(b+c) = ab + ac$ and, $(a+b).c = ac + bc$

Examples :-

(i) $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields, but $\mathbb{Z}$ is not field because, $(\mathbb{Z}-\{0\}, \cdot)$ is not abelian.

(ii) $\mathbb{Z}_n$ is a field if and only if n is prime.

Proof :-

Suppose, n is prime and that $[a]\cdot[b]=[0]$ in $\mathbb{Z}_n$.

Then, $n|ab$, So, $n|a$ and $n|b$.

Hence, $[a]=[0]$ and $[b]=[0]$ and $\mathbb{Z}_n$ is an integral domain. Since, $\mathbb{Z}_n$ is also finite, So, $\mathbb{Z}_n$ is a field.

Suppose, n is not prime. Then, we can write $n=rs$, where, r and s are integers such that $1<r<n$ and $1<s<n$.

Now, $[r]\neq[0]$ and $[s]\neq[0]$, But $[r]\cdot[s]=[rs]=[0]$

Therefore, $\mathbb{Z}_n$ has zero divisor and hence is not a field.

Proposition :-

Every field is an integral domain.

Proof :-

Let, F be a field and for $a,b\in F$, we have

$a.b=0$

If $a\neq 0$, $\exists$ $a^{-1}\in F$ and $a^{-1}(a.b)=a^{-1}.0$

$\Rightarrow (a^{-1}.a).b=0 \Rightarrow e.b=0 \Rightarrow b=0$

Hence, either $a=0$ or, $b=0$

$\Rightarrow$ no zero divisor. Hence, F is an integral domain.

Remarks:-

Converse of above proposition is not true in general.
e.g. $(\mathbb{Z}, +, \cdot)$ is an integral domain but not field.

Theorem:-

A finite integral domain is a field.

Proof:-

Let, $D = \{x_0, x_1, ----, x_n\}$ be a finite integral domain, with x_0 as 0 and x_1 as 1. We have to show that every non-zero element of D has multiplicative inverse.
If x_i is non-zero, then $x_i D = \{x_i x_0, x_i x_1, ----, x_i x_n\}$ is same as set D.
If $x_i x_j = x_i x_k$, then, $x_j = x_k$. Hence, all element $x_i x_0, x_i x_1, -----, x_i x_n$ are distinct and $x_i D$ is a subset of D with same number of elements. Therefore, $x_i D = D$
But then there is some elements x_j, such that

$$x_i x_j = x_1 = 1 \Rightarrow x_j = x_i^{-1}$$

Hence, D is a field.

Example:-

Is $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ an integral domain or, field.

Solution:-

Let, $a, b, c, d \in \mathbb{Q}$, then, we have,

$(a + b\sqrt{2}) + (c + \sqrt{2}d) = (a+c) + \sqrt{2}(b+d) \in \mathbb{Q}(\sqrt{2})$
since, $(a+c) \in \mathbb{Q}$ and $(b+d) \in \mathbb{Q}$

Also,

$$(a+b\sqrt{2})\cdot(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}\sqrt{2}$$

because, $(ac+2bd)\in\mathbb{Q}$ and $(ad+bc)\in\mathbb{Q}$

Now,

→ Addition is associative.

→ Addition is commutative.

→ The zero is $0=0+0\sqrt{2}\in\mathbb{Q}(\sqrt{2})$

→ The additive inverse of $a+b\sqrt{2}$ is $(-a)+(-b)\sqrt{2}\in\mathbb{Q}(\sqrt{2})$.

⇒ $(\mathbb{Q}\sqrt{2},+)$ is abelian.

Also,

→ Multiplication of $\mathbb{Q}$ is associative.

→ Multiplicative identity is $1=1+0\sqrt{2}\in\mathbb{Q}\sqrt{2}$

→ Let, $a+b\sqrt{2}$ be a non-zero element, then the multiplicative inverse is

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{(a+b\sqrt{2})^2}=\left(\frac{a}{a^2-2b^2}\right)-\left(\frac{b}{a^2-2b^2}\right)\sqrt{2}\in\mathbb{Q}\sqrt{2}$$

→ Multiplication in $\mathbb{Q}$ is commutative.

⇒ $(\mathbb{Q}(\sqrt{2})-\{0\},\cdot)$ is abelian.

⇒ The distributive axioms hold for $\mathbb{R}$ and hence, hold for elements of $\mathbb{Q}(\sqrt{2})$.

Hence,

$(\mathbb{Q}(\sqrt{2}),+,\cdot)$ is a field (and, an integral domain).

Subring :-

let, $(R,+,\cdot)$ be a ring and S be a non-empty subset of R, then, S is said to be subring of R if for $\forall\, a,b \in S$, we have,

(i) $a-b \in S$ (ii) $ab \in S$

(iii) $1 \in S$

Proposition :-

If S is a subring of $(R,+,\cdot)$, then, $(S,+,\cdot)$ is a ring.

Proof :-

let, S be a subring, then, $a-b \in S$ and $ab \in S$, So, S is closed under addition and multiplication.
Since, $(S,+) \subseteq (R,+)$ and '$+$' is commutative in R, So, it is also commutative in S, So, $(S,+)$ is abelian.
Since, '$\cdot$' is associative in R, So, it is also associative in S. So, $(S,\cdot)$ is semi group.
Further, '$\cdot$' is distributive under '$+$' in R, So, it is also distribute in S.
Hence,
$(S,+,\cdot)$ is a ring.

for example :-

(i) $(E,+,\cdot)$ is a subring of $(\mathbb{Z},+,\cdot)$.
(ii) $(\mathbb{Z},+,\cdot)$ is a subring of $(\mathbb{Q},+,\cdot)$.
(iii) $(\mathbb{Q},+,\cdot)$ is a subring of $(\mathbb{R},+,\cdot)$.
(iv) $(\mathbb{R},+,\cdot)$ is a subring of $(\mathbb{C},+,\cdot)$.
(v) let, D be set of $n \times n$ real diagonal matrices.

Then, D is subring of the ring of all n×n real matrices, $M_n(\mathbb{R})$, because the sum, difference and product of two diagonal matrices is another diagonal matrix. Note that, D is commutative even through $M_n(\mathbb{R})$ is not.

Example:-

Show that $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,;\, a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{R}$.

Solution:-

Let, $a+b\sqrt{2}$, $c+d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, Then,

(i) $(a+b\sqrt{2}) - (c+d\sqrt{2}) = (a+c) - (b+d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

(ii) $(a+b\sqrt{2}) . (c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

(iii) $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

Hence,

$\mathbb{Q}(\sqrt{2})$ is subring of $\mathbb{R}$.

Ring Morphism:-

Let, $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be a two rings. The function $f : R \to S$ is called ring morphism if for all $a, b \in R$, we have

$$f(a+b) = f(a) \oplus f(b)$$
$$f(a.b) = f(a) \odot f(b)$$
$$f(I_R) = I_S, \text{ where, } I_R \text{ and } I_S \text{ are respective identities.}$$

Pradeep Khuja.
SP21-RMT-013

Ring Isomorphism :-

A morphism $f: R \to S$ is said to ring isomorphism iff $f: R \to S$ is bijective.

If there is an isomorphism between the rings R and S, we say R and S are isomorphic rings and write it as $R \cong S$.

Examples :-

(1) The function $f: \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = [x]$, which map an integer to its equivalence class module n, is a ring morphism from $(\mathbb{Z}, +, \cdot)$ to $(\mathbb{Z}_n, +, \cdot)$.

(2) The inclusion function $i: S \to R$ of any subring S into a ring R is always is ring morphism.

(3) The linear transformation from $\mathbb{R}^n$ to itself form a ring $(\mathcal{L}(\mathbb{R}^n, \mathbb{R}^n), +, \circ)$ under addition and composition. The function, $f: \mathcal{L}(\mathbb{R}^n, \mathbb{R}^n) \to M_n(\mathbb{R})$ is a ring morphism where, f assigns each linear transformation its standard matrix, i.e. $n \times n$ coefficient matrix with respect to the standard basis of $\mathbb{R}^n$.

Solution :-

If α is linear transformation from $\mathbb{R}^n$ to itself, then,

$$\alpha \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n \end{bmatrix} \text{ and, } f(\alpha) = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$$

Matrix addition and multiplication is defined, So that $f(\alpha+\beta) = f(\alpha) + f(\beta)$ and, $f(\alpha \circ \beta) = f(\alpha) \cdot f(\beta)$

Any matrix defines a linear transformation, so that f is surjective. Furthermore, f is injective, because, j^{th} column of matrix must be the image of j^{th} basis vector. Hence, f is an isomorphism.

Example :-

Show that $f: \mathbb{Z}_{24} \to \mathbb{Z}_4$, defined by $f([x]_{24}) = [x]_4$ is ring morphism.

Solution :-

Let, $[x]_{24} = [y]_{24}$, then, $x \equiv y \pmod{24}$ and $24 | (x-y)$

Hence, $4 | (x-y)$ and $[x]_4 = [y]_4$.

$\Rightarrow f$ is well-defined.

We now check the conditions for ring morphism.

(i) $f([x]_{24} + [y]_{24}) = f([x+y]_{24})$

$$= [x+y]_4$$

$$= [x]_4 + [y]_4$$

(ii) $f([x]_{24} \cdot [y]_{24}) = f([xy]_{24})$

$$= [xy]_4$$

$$= [x]_4 \cdot [y]_4$$

(iii) $f([1]_{24}) = [1]_4$

Hence, f is ring morphism.

New rings from old :-

If $(R,+,\cdot)$ and $(S,+,\cdot)$ are two rings, their product is the ring $(R\times S,+,\cdot)$, whose underlying set is cartesian product of R and S and whose operation are defined by

$(r_1,s_1)+(r_2,s_2)=(r_1+r_2, s_1+s_2)$ and $(r_1,s_1)\cdot(r_2,s_2)=(r_1\ , s_1s_2)$

Example :-

Write down the addition and multiplication table for $\mathbb{Z}_2\times\mathbb{Z}_3$.

Solution :-

let, $\mathbb{Z}_2=\{0,1\}$ and $\mathbb{Z}_3=\{0,1,2\}$, then,

$\mathbb{Z}_2\times\mathbb{Z}_3=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$

+	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

·	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,0)	(0,1)	(0,2)
(0,2)	(0,0)	(0,2)	(0,1)	(0,0)	(0,2)	(0,1)
(1,0)	(0,0)	(0,0)	(0,0)	(1,0)	(1,0)	(1,0)
(1,1)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(1,2)	(0,0)	(0,2)	(0,1)	(1,0)	(1,2)	(1,1)

Theorem :-

$\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic as a ring to $\mathbb{Z}_{mn}$ if and only if $\gcd(m,n)=1$.

Proof :-

If $\gcd(m,n)=1$, then $C_{mn} \cong C_m \times C_n$.

Since, we know the cyclic groups of same order are isomorphic.

Hence, the function $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ defined by

$$f([x]_{mn}) = ([x]_m, [x]_n)$$ is a group morphism.

However, this function also preserve multiplication because,

$$f([x]_{mn} \cdot [y]_{mn}) = f([xy]_{mn}) = ([xy]_m, [xy]_n)$$
$$= ([x]_m \cdot [y]_m, [x]_n \cdot [y]_n)$$
$$= ([x]_m, [x]_n) \cdot ([y]_m \cdot [y]_n)$$
$$= f([x]_{mn}) \cdot f([y]_{mn})$$

Also, $f([1]_{mn}) = f([1]_m, [1]_n)$

Thus, $f: \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ is ring isomorphism.

and, $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

If $\gcd(m,n) \neq 1$, $\mathbb{Z}_m \times \mathbb{Z}_n$ are not isomorphic as groups, Hence, they cannot be isomorphic as rings.

Theorem :-

Let, $m = m_1 . m_2 \cdots m_r$ where, $\gcd(m_i, m_j) = 1$ if $i \neq j$. Then, $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ is a ring isomorphic to $\mathbb{Z}_m$.

Corollary :-

Let, $n = p_1^{\alpha_1} p_2^{\alpha_2} \text{-----} p_r^{\alpha_r}$ be a decomposition of integers n into powers of distinct primes. Then,

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \text{------} \times \mathbb{Z}_{p_r^{\alpha_r}} \text{ as rings.}$$

Ring of nxn Matrices :-

If R is commutative ring, we can construct the ring of nxn matrices with entrices from R, $(M_n(R), +, \cdot)$. Addition and multiplication performed as in real matrices.

For example, $(M_n(\mathbb{Z}_2), +, \cdot)$ is a ring of nxn matrices with 0 and 1 entries. This is noncommutative rings with $2^{(n^2)}$ elements.

Polynomial Ring :-

If R is a commutative ring, a polynomial $p(x)$ in the indeterminate x over the ring R is an expression of the form, $p(x) = a_0 + a_1 x + a_2 x^2 + \text{----} + a_n x^n$

where, $a_0, a_1, a_2 \text{---} a_n \in R$ and $n \in \mathbb{N}$.

The element a_i is called the coefficient of x^i in $p(x)$.

Let, $f(x)$ and $g(x)$ be two polynomials, s.t.

$f(x) = a_0 + a_1 x + \text{---} + a_n x^n$ and $g(x) = b_0 + b_1 x + \text{----} + b_n x^n$

then, $f(x) = g(x)$ if and only if $a_n = b_n \ \forall n$

The polynomial, $a_0 + a_1 x + \text{---} + a_n x^n$ is called zero polynomial if and only if $a_0 = a_1 = a_2 = \text{----} = a_n = 0$

If n is the largest integer for which $a_n \neq 0$, we say $p(x)$ has degree n and write $\deg p(x) = n$.

The polynomial of degree '0' is called constant polynomial.

Examples :-

→ $4x^2 - \sqrt{3}$ is a polynomial over $\mathbb{R}$ of degree 2.

→ $ix^4 - (2+i)x^3$ is a polynomial over $\mathbb{C}$ of degree 4.

→ $x^7 + x^5 + x^4 + 1$ is a polynomial over $\mathbb{Z}_2$ of degree 7.

→ The number 5 is constant polynomial over $\mathbb{Z}$.

Defination :-

The set of all polynomials in x with coefficients from commutative ring R is denoted by $R[x]$. That is,

$$R[x] = \{a_0 + a_1x + a_2x^2 + \text{-----} + a_nx^n \; ; \; a_i \in \mathbb{R}, n \in \mathbb{N}\}$$

This forms a ring $(R[x], +, \cdot)$ called the polynomial ring with coefficient from R, when addition and multiplication of polynomials

$f(x) = \sum_{i=0}^{n} a_i x^i$ and, $g(x) = \sum_{i=0}^{m} b_i x_i$ are defined by

$$f(x) + g(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i$$

and, $f(x) \cdot g(x) = \sum_{k=0}^{m+n} c_k x^k$, where $c_k = \sum_{i+j=k} a_i b_j$

The zero is zero polynomial and multiplicative identity is constant polynomial.

For example :- In $\mathbb{Z}_5[x]$, the polynomial ring with coefficients in the integers modulo 5, we have

$$(2x^3 + 2x^2 + 1) + (3x^2 + 4x + 1) = 2x^3 + 4x + 2$$

and, $(2x^3+2x^2+1)\cdot(3x^2+4x+1) = x^5+4x^4+4x+1$

Theorem :-

If R is an integral domain, then, So, $R[x]$.

Solution :-

Since, $R[x]$ is a commutative ring. We only prove that $R[x]$ has no-zero divisor.

Let, $f(x) = a_0x^0 + a_1x + --- + a_nx^n \in R[x]$

$g(x) = b_0x^0 + b_1x + --- + b_nx^n \in R[x]$

Let, $f(x)\cdot g(x) = 0$. To prove, $f(x)=0$ or, $g(x)=0$

Suppose, $f(x)\cdot g(x) = 0$

$\Rightarrow a_0b_0 = 0$

$a_0b_1 + a_1b_0 = 0$

$a_0b_2 + a_1b_1 + a_2b_0 = 0$

and, so on

If $a_0b_0 = 0$, then, since R is an integral domain,

So, $a_0 = 0$ or $b_0 = 0$

We say $a_0 = 0$ $(b_0 \neq 0)$

If $a_0b_1 + a_1b_0 = 0$, then, $0 + a_1b_0 = 0$ $\because (a_0 = 0)$

$\Rightarrow a_1 = 0$ because $b_0 \neq 0$.

Similarly, $a_0b_2 + a_1b_1 + a_2b_0 = 0$ gives us $a_2 = 0$.

Similarly, continuing the process, we get $f(x) = 0$.

$\Rightarrow R[x]$ has no zero divisor.

$\Rightarrow R[x]$ is an integral domain.