

Unit-04 Algebraic Structure

Binary operation

Let A be a non-empty set, then a function $f: A \times A \rightarrow A$ is called binary operation on A .

A function $g: A \rightarrow A$ is called unary operation on A and a function $h: (A \times A \times A \rightarrow A)$ is called ternary operation on A , or in general, an n -ary operation is a function $\underbrace{A \times A \times A \times \dots \times A}_{n\text{-times}} \rightarrow A$ into A .

Thus binary operation on A is a function that assign each ordered pairs of element of A to an element of A . The symbol $+$, \cdot , $*$, \circ etc.. are used to denote binary operation on a set.

$+$ will be a binary operation on A if and only if

$$a + b \in A \quad \forall a, b \in A \text{ and } \underline{a + b \text{ is unique.}}$$

similarly $*$ will be a binary operation on A if $a * b \in A \quad \forall a, b \in A$ and $a * b$ is unique.

This is said to be the closure property of the binary operation on a set & is said to be the closed with respect to binary operation.

ex: let $A = \{0, 1, -1\}$. then the addition is not a binary operation on A because

$$(-1) + (-1) = -2 \notin A$$

where the multiplication is a binary operation on A .

SBG STUDY

subtraction(-)

ex 2 The operation \wedge on a set A is a binary operation on Z whereas it is not a binary operation on Z^+ .

ex 3 Define $a * b = a|b$ for $a, b \in R$. Then $*$ is not a binary operation on R since $a * b$ ($2 * 0 = 2|0$) is not defined.

ex 3. Let $A = \{0, 1, 2\}$. Define $a * b = a + b$ if $a + b \leq 2$ and $a * b = a + b - 3$ if $a + b > 3$. Then $*$ (binary operator) the table for $*$

| | | | | | |
|----------------|-----|-----------------|---|---|------------------------|
| | | $b \rightarrow$ | | | |
| | $*$ | 0 | 1 | 2 | |
| $a \downarrow$ | 0 | 0 | 1 | 2 | Row $\rightarrow a$ |
| | 1 | 1 | 2 | 0 | Column $\rightarrow b$ |
| | 2 | 2 | 0 | 1 | |

ex 4 If $A = \{a, b\}$, we shall now determine the number of binary operations that can be defined on A . Every binary operation $*$ on A can be described by a table

| | | |
|-----|---|---|
| $*$ | a | b |
| a | . | . |
| b | . | . |

since every blank space can be filled with a and b because it should belong $\{a, b\}$ set.

So there are

$2 \times 2 \times 2 \times 2 = 2^4 = 16$ ways to complete the table. So there are 16 binary operations on A .

Properties of Binary operations

① Commutative Law

A binary operation $*$ on a set A is said to be commutative if

$$a * b = b * a \quad \forall a, b \in A$$

ex: Addition and subtraction are commutative operations on the set Z of integers whereas subtraction is not commutative on the set Z of integers since $3-4 = -1 \neq 4-3$

Ex 6 Consider the binary operation $*$ defined on the set $A = \{a, b, c\}$ by the following table.

| $*$ | a | b | c |
|-----|---|---|---|
| a | b | c | b |
| b | a | b | c |
| c | c | a | b |

then $*$ is not commutative since $a * b = c$ while $b * a = a$

② Associative Law :-

An operation $*$ on a set A is said to be associative or satisfy associative law, if $(a * b) * c = a * (b * c) \quad \forall a, b, c \in A$.

ep. 7 Consider the set \mathbb{Z}^+ of non-negative integers. Check whether the operation $*$ defined by

$a * b = a^2 + b$ for all $a, b \in \mathbb{Z}^+$, is associative or not.

Solⁿ For $a, b, c \in \mathbb{Z}^+$

$$\begin{aligned} (a * b) * c &= \underbrace{(a^2 + b)} * \underbrace{c} \\ &= (a^2 + b)^2 + c \\ &= a^4 + b^2 + 2a^2b + c \end{aligned}$$

$$\begin{aligned} a * (b * c) &= \underbrace{a^2} + \underbrace{(b * c)} \\ &= a^2 + b^2 + c \\ &= a^2 + b^2 + c \end{aligned}$$

thus $(a * b) * c \neq a * (b * c)$ Ans

Q. 8 Consider the operation $*$ defined on \mathbb{Z} , the set of integers, as $a * b = a + b - 3ab$. Determine whether $*$ is commutative or associative.

Solⁿ: Since commutative and associative are both binary operations.

$$\therefore a * b = a + b - 3ab$$

$$b * a = b + a - 3ba$$

$\therefore a * b = b * a$ hence commutative

$$\begin{aligned} \text{(ii)} \quad (a * b) * c &= (a + b - 3ab) * c \\ &= (a + b - 3ab) + c - 3\{a + b - 3ab\} * c \\ &= a + b - 3ab + c - 3ac - 3bc + 9abc \\ &= a + b + c - 3ab - 3bc - 3ca + 9abc \end{aligned}$$

$$\begin{aligned} a * (b * c) &= \underline{a} * (b + c - 3bc) \\ &= a + (b + c - 3bc) - 3a(b + c - 3bc) \\ &= a + b + c - 3ab - 3bc - 3ca + 9abc \end{aligned}$$

$\therefore (a * b) * c = a * (b * c)$ Ans

Q. Consider the operation $*$ defined on the set \mathbb{Z}^+ of non-negative integers as

$$a * b = a + b + 2 \text{ for } a, b \in \mathbb{Z}^+$$

Show that it is commutative as well as associative.

Solⁿ $*$ is commutative

\therefore

$$a * b = a + b + 2$$

$$\& b * a = b + a + 2$$

$$\therefore \boxed{a * b = b * a} \text{ commutative}$$

(ii) Associative

$$\begin{aligned} (a * b) * c &= (a + b + 2) * c \\ &= a + b + 2 + c + 2 \\ &= a + b + c + 4 \end{aligned}$$

Now $a * (b * c) = a * (b + c + 2)$

$$\begin{aligned} &= a + b + c + 2 + 2 \\ &= a + b + c + 4 \end{aligned}$$

$$\therefore \boxed{(a * b) * c = a * (b * c)}$$

Q. Consider the binary operation $*$ defined on the set of integers \mathbb{Z} as

$$a * b = a | b |$$

Determine whether operation $*$ is commutative or not. Check whether it is associative.

Solⁿ. Since $3 * -2 = 3 | -2 | = 3 \times 2 = 6$

Let $a = 3$ $-2 * 3 = -2 | 3 | = (-2)(3) = -6$
 $b = -2$

$\therefore *$ is not commutative.

(ii) $(a * b) * c = (a | b |) | c | = a | b | | c |$

$$a * (b * c) = a * (b | c |) = a | b | | c | = a | b | | c |$$

Thus $*$ is associative.

Q. Consider the set N of Natural numbers, Define an operation $*$ on N as

$$a * b = a^b \quad \forall \text{ all } a, b \in N.$$

Show that $*$ is neither commutative nor associative.

Solⁿ: Let $a=2$ & $b=3$

$$a * b = 2^3 = 8$$

$$\therefore b * a = 3^2 = 9$$

\therefore $a * b \neq b * a$ Hence not Commutative.

(ii) Let $a=2, b=2$ & $c=3$

$$(a * b) * c = (2 * 2) * 3 = (2^2) * 3 = 4 * 3 = 4^3 = 64$$

$$a * (b * c) = 2 * (2 * 3) = 2 * (2^3) = 2 * 8 = 2^8 = 256$$

\therefore $(a * b) * c \neq a * (b * c)$

Q. Show that the binary operation $*$ defined on $(R, *)$, where $x * y = \max(x, y)$ is associative.

Solⁿ: $x * y = \max(x, y)$

$$(x * y) * z = \max(\max(x, y), z)$$

$$= \max(x, y, z)$$

$$= \max(\max(x, y), z)$$

$$= \max(\max(x, y), z)$$

$$= \max(x, y, z) \quad \text{--- ①}$$

~~max~~

$$x * (y * z) = x * (\max(y, z))$$

$$= \max(x, \max(y, z))$$

$$= \max(x, y, z) \quad \text{--- ②}$$

\therefore $(x * y) * z = x * (y * z)$

is associative.

Property

Identity element

Let $*$ be a binary operation on a set A . An element $e \in A$ is called the identity element for $*$ if for any a in A ,

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

if $a * e = a$, then e is called the right identity element for the operation $*$ and if $e * a = a$, then e is called the left identity element for the operation $*$.

ep: Consider the set Z of integers. For the operation of addition defined on Z , the integer 0 is an identity element since

$$0 + a = a + 0 = a \text{ for all } a \in Z.$$

Inverse element

Suppose a binary operation $*$ on a set A have an identity element e . An element $b \in A$ is said to be inverse of a if

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

ep: for the operation of multiplication defined on the set of integers Z , the integer 1 is an identity element since

$$1 \cdot a = a \cdot 1 = a \quad \forall a \in Z.$$

ex. Consider the set Z of integers, for the operation of addition defined on Z , $-a \in Z$ is the inverse element of a since

$$a + (-a) = (-a) + a = 0 \text{ for all } a \in Z.$$

Q. Consider $A = \{1, 2, 3, 4, 5, 6, 7\}$. Define a binary operation $*$ on A as $a * b = \min\{a, b\}$ for all $a, b \in A$.

Then prove that this binary operation $*$ is commutative and associative and also find the identity element.

Solⁿ:

Given ~~that~~ $a * b = \min(a, b) \quad \forall a, b \in A$

Now $a * 7 = \min(a, 7) = a$

$$7 * a = \min(7, a) = a$$

$$\therefore a * 7 = 7 * a = a$$

\therefore Binary operation is commutative and identity element is 7.

(ii)

$$\begin{aligned} (a * b) * c &= \min(a, b) * c \\ &= \min(\min(a, b), c) \\ &= \min(a, b, c) \quad \text{--- (1)} \end{aligned}$$

$$\begin{aligned} a * (b * c) &= a * (\min(b, c)) \\ &= \min(a, \min(b, c)) \\ &= \min(a, b, c) \quad \text{--- (2)} \end{aligned}$$

Now from (1) & (2)

$$\boxed{(a * b) * c = a * (b * c)} \quad \text{Associative.}$$

Group:- Let G be a non-empty set together with some operation $*$ then algebraic structure $(G, *)$ is said to be a group if following 4 conditions are satisfied.

(i) G_1 : Closure Property: If $a \in G, b \in G$ then $a * b \in G \quad \forall a, b \in G$.

(ii) G_2 : Associative Property

If $a, b, c \in G$, then $a * (b * c) = (a * b) * c$
 $\forall a, b, c \in G$.

(iii) G_3 : Existence of identity:-

There exist $e \in G$, such that

$$a * e = e * a = a \quad \forall a \in G.$$

(iv) Existence of Inverse element:-

Every element of G has an inverse i.e. for every $a \in G$ there exist $b \in G$ such that $a * b = b * a = e$, as b is called the inverse of a and b written as $(a^{-1}) = b$.

exp:

Semigroup:

Let A be a non-empty set and $*$ be a binary operation defined on A . The algebraic system $(A, *)$ is called a semigroup if the operation $*$ is associative, that is $(A, *)$ is a semigroup if for any $a, b, c \in A$

$$(i) (a * b) * c = a * (b * c)$$

(ii) closure property.

Note: - A semigroup may or may not have an identity element.

Monoid

An Algebraic system $(A, *)$ is called a monoid if for any $a, b, c \in A$

$$(i) (a * b) * c = a * (b * c)$$

(ii) There exist an identity element $e \in A$ such that for any $a \in A$

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

(iii) closure - for every pair $(a, b) \in S$, $a * b$ must be present in S .

OR A semigroup $(A, *)$ in which the binary operation $*$ has an identity element is called a monoid.

ex. Consider a set of natural nos Then $(\mathbb{N}, +)$ and (\mathbb{N}, \times) are semigroup since addition and multiplication are associative on \mathbb{N}

$a + (b + c) = (a + b) + c$ } but (\mathbb{N}, \times) is monoid
 $\neq a \times (b \times c) = (a \times b) \times c$ } since \mathbb{N} has with identity element 1. whereas

$(\mathbb{N}, +)$ is not monoid, since \mathbb{N} has no zero element.

ex: The algebraic system $(\mathbb{Z}, +)$ is a semigroup as well as monoid, whereas $(\mathbb{Z}, -)$ is not a semigroup & not monoid.

Subsemigroup:-

Consider $(A, *)$ be a semigroup and B is a subset of A . Then $(B, *)$ is called a subsemigroup of $(A, *)$ if B is closed under the operation $*$, i.e. for all $a, b \in B$, $a * b \in B$.

Exp. let consider a semigroup $(N, +)$, where N is the set of natural numbers and $+$ is an addition operation. The algebraic system $(E, +)$ is a subsemigroup of $(N, +)$, where E is the set of even positive numbers

$$N = \{1, 2, 3, 4, 5, \dots\} \quad (N, +) \leftarrow \text{semigroup}$$

$$E = \{2, 4, 6, 8, \dots\} \quad (E, +) \text{ is subsemigroup}$$

because it is also satisfying associative and closure property.

$$(2+4)+8 = (6)+8 = 14$$

$$2+(4+8) = 2+(12) = 14$$

Submonoid:- ~~(M, *)~~, ~~(M, *)~~

with identity element e

Consider a monoid $(M, *)$ and let T be the non-empty subset of M . Then $(T, *)$ is called submonoid of $(M, *)$ if $e \in T$ and T is closed under the operation $*$, i.e. for all $a, b \in T$, $a * b \in T$.

→ Some first few non-negative even integers are $\{0, 2, 4, 6, 8, \dots\}$

→ set of even integers are $= \{-4, -2, 0, 2, 4, \dots\}$

ex: If T be the set of all even integers $T = \{-4, -2, 0, 2, 4, \dots\}$
 then $(T, +)$ is subsemigroup of $(\mathbb{Z}, +)$.

And it is even a submonoid because $(T, +)$ is the submonoid of monoid $(\mathbb{Z}, +)$ with identity element $(e=0)$.

→ Group &

→ Abelian Group - A Group G is said to be abelian group, if it satisfy the commutative property.

G5: Commutative Law: $a \times b = b \times a \quad \forall a, b \in G$

| | |
|---------------|---------------------------|
| Groupoid | G_1 |
| Semi Group | G_1, G_2 |
| Monoid | G_1, G_2, G_3 |
| Group | G_1, G_2, G_3, G_4 |
| Abelian Group | G_1, G_2, G_3, G_4, G_5 |

Q Prove that fourth roots of unity $1, -1, i$ and $-i$ form an abelian ^{multiplicative} group.

Solⁿ: Let $G = \{1, -1, i, -i\}$

* \rightarrow is multiplication

1: $\forall (1, -1, i, -i) \in G$

$a \times b \in G$
also

G2: Associative Law

exp. $1[(-1)i] = -i$
 $= [1(-1)] \cdot i = -i$

| | | | | |
|----|----|----|----|----|
| * | 1 | -1 | i | -i |
| 1 | 1 | -1 | i | -i |
| -1 | -1 | 1 | -i | i |
| i | i | -i | 1 | 1 |
| -i | -i | i | 1 | -1 |

3: Commutative Law

From the table it is clear that elements in each row are the same as element in the corresponding column so that $ab=ba$.

4: Identity element $1 \in G$.

$$\text{as } a \cdot 1 = 1 \cdot a = a \quad \forall a \in G.$$

5: Inverse element

Inverse of 1 is 1, -1 is -1, i is -i
-i is i.

\therefore it is abelian group

Q Show that the set of all positive rational numbers forms an abelian group under the composition defined by $a * b = \left(\frac{ab}{2}\right)$.

Solⁿ

Let \mathbb{Q}^+ be the set of all positive rational numbers. We have to show that $(\mathbb{Q}^+, *)$ is a group with commutative property, under the composition $a * b = \left(\frac{ab}{2}\right)$.

(i) Closure Property.

for all $a, b \in \mathbb{Q}^+$, $\left(\frac{ab}{2}\right)$ is also in \mathbb{Q}^+ , therefore \mathbb{Q}^+ is closed operation
with respect to $*$.

(ii) Associative Property

for every $a, b, c \in \mathbb{Q}^+$

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{abc}{4}$$

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a, bc}{2} = \frac{abc}{4}$$

\therefore therefore it is associative.

(ii) Commutative for any $a, b \in \mathcal{Q}^+$

$$a * b = \frac{ab}{2} = \frac{ba}{2} = (b * a)$$

(iv) Identity element:- let e be the identity element.

such that for all $a \in \mathcal{Q}^+$

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

$$\therefore a * e = a$$

$$\left(\frac{ae}{2}\right) = a$$

$$ae = 2a \Rightarrow ac - 2a = 0$$

$$\Rightarrow a(e - 2) = 0$$

$\therefore a > 0$ (positive rational no. so it can't be zero).

$$\therefore \boxed{e = 2}$$

(v) Inverse element:- let $a \in \mathcal{Q}^+$

let g of b is the inverse of a

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

$$a * b = e$$

$$\left(\frac{ab}{2}\right) = e$$

$$\frac{ab}{2} = e$$

$b = \left(\frac{4}{a}\right)$ is the inverse element of $a \in \mathcal{Q}^+$.

Properties of a Group

① The Identity element in a group is unique.

Let us suppose that $a \in G$ and e, e' be the two identities in G .

$$\therefore e \in G \text{ and } a \in G \Rightarrow ae = a \text{ --- ①}$$

$$e' \in G \text{ and } a \in G \Rightarrow ae' = a \text{ --- ②}$$

From ① and ②

$$ae = ae'$$

$$\therefore \boxed{e = e'}$$

② The inverse of each element in a group is unique.

Let $a \in G$ and $e \in G$

Let b and c be the two inverse of a in G .

$$\therefore a \in G \text{ and } b \in G \Rightarrow ab = e \text{ --- ①}$$

$$\therefore a \in G \text{ and } c \in G \Rightarrow ac = e \text{ --- ②}$$

From eqⁿ ① and ②

$$ab = ac$$

$$\Rightarrow \boxed{b = c}$$

③ For every element 'a' in a Group G , prove that $(a^{-1})^{-1} = a$

Proof: Let e be the identity element of the group G .

For each element $a \in G$, there exist an element $b \in G$

such that $a * b = b * a = e$ (if b is the inverse of a)

\exists \forall $a \in G$ inverse $b \in G$

$$b = a^{-1} \text{ --- ①}$$

$$a = b^{-1} \text{ --- ②}$$

\forall both inverse

$b^{-1} \in G$

put value of b from ① in ②

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

4. The inverse of the product of two elements of a group G is the product of the inverse taken in the reverse order i.e. $(a * b)^{-1} = b^{-1} * a^{-1}$ for a Group $(G, *)$
 Solⁿ Prove that $(a * b)^{-1} = b^{-1} * a^{-1}$

Take $a, b \in G \Rightarrow (a * b)^{-1} \neq$

Let $a, b \in G$ and suppose a^{-1} and b^{-1} are the inverse of a and b respectively.

$$\left. \begin{aligned} a \cdot a^{-1} &= e \\ b \cdot b^{-1} &= e \end{aligned} \right\} \text{ where } e \text{ is the identity.}$$

$$\begin{aligned} (a * b) \cdot (b^{-1} * a^{-1}) &= (a(b * b^{-1})) * a^{-1} && \text{Apply Associative Law} \\ &= a * e * a^{-1} \\ &= a * a^{-1} = e \end{aligned}$$

$$\begin{aligned} (b^{-1} * a^{-1}) (a * b) &= b^{-1}(a^{-1} * a) * b \\ &= b^{-1} * e * b \\ &= b^{-1} * b = e \end{aligned}$$

$\therefore b^{-1} * a^{-1}$ is the inverse of $a * b$.

$$\therefore \boxed{a * b = b^{-1} * a^{-1}}$$

⑤ Cancellation Law: If $a, b, \text{ and } c$ are any elements of $(G, *)$ then

More detailed Solution (i) $a * c = b * c \Rightarrow \boxed{a = b}$ Right cancellation Law.

let $x = b^{-1} * a^{-1}$. then we will prove that x is the inverse of $a * b$.

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

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

$$= a * [(b * b^{-1}) * a^{-1}] \text{ " "}$$

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

$$\because a * e = a \quad = (a * e) * a^{-1} \Rightarrow a * a^{-1} = e \quad \text{--- (1)}$$

Similarly we have to show that

$$x * (a * b) = e$$

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

$$\Rightarrow [(b^{-1} * a^{-1}) * a] * b \quad \text{by associative law}$$

$$\Rightarrow [b^{-1} * (a^{-1} * a)] * b \quad \text{" "}$$

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

$$\Rightarrow b^{-1} * (e * b) \quad \text{by associative}$$

$$\Rightarrow b^{-1} * b \quad e * b = b$$

$$\Rightarrow e \quad \text{--- (2)}$$

from eqⁿ (1) and (2)

$$\boxed{(a * b)^{-1} = b^{-1} * a^{-1}}$$

(5) Cancellation Law

If a, b and c are any three element of G , then

$$(i) \quad ab = ac \Rightarrow b = c \quad \text{Left cancellation law}$$

$$(ii) \quad ba = ca \Rightarrow b = c \quad \text{Right cancellation law}$$

Proof (i) let $a \in G \Rightarrow a^{-1} \in G$

Now

$$ab = ac$$

$$\because a^{-1} \in G$$

$$\therefore a^{-1} * (ab) \in G$$

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

$$(a^{-1}a) \cdot b = (a^{-1}a) c \quad (\text{associative Law})$$

$$e \cdot b = e \cdot c$$

$$\boxed{b = c}$$

$$(ii) \quad ba = ca$$

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

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

$$\boxed{b = c}$$

associative

⑥ If G is a group and $a, b \in G$ be any element, then

(i) The equation $a * x = b$ has a unique solution
 $x = a^{-1} * b$ in G .

(ii) The equation $y * a = b$ has a unique solution
 $y = b * a^{-1}$ in G .

Proof: (i) $a * x = b$ — ①
 \Rightarrow Premultiply by a^{-1} on both side of eqⁿ — ②

$$a^{-1} * (a * x) = a^{-1} * b \quad (\because a^{-1} \in G)$$

$$(a^{-1} * a) * x = a^{-1} * b \quad \text{associative.}$$

$$e * x = a^{-1} * b$$

$$x = a^{-1} * b \in G \quad (\because a^{-1} \& b \in G)$$

therefore, the equation $a * x = b$ has a solution
 $x = a^{-1} * b$ in G .

Uniqueness:- let if possible x_1 and x_2 be any two
solution of the equation $a * x = b$, so that

$$a * x_1 = b \quad \text{and} \quad a * x_2 = b$$

$$\Rightarrow a * x_1 = a * x_2$$

$$\Rightarrow x_1 = x_2 \quad (\text{by left cancellation law})$$

therefore the equation $a * x = b$ has
a unique solution.

Q. let G be a group with identity element e , show that if $a^2 = e$ for all $a \in G$, then G is abelian.

Solⁿ. Given $a^2 = e$ for all $a \in G$

$$a * a = e$$

Pre-multiply by a^{-1} on both side

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

$$(a^{-1} * a) * a = a^{-1} \quad \text{by associativity}$$

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

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

i.e every element is inverse itself.

Now for $a, b \in G$

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

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

$$\boxed{a * b = b * a}$$

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

every element is inverse itself.

which is commutative

Q. For any Group G , prove that G is abelian if and only if $(ab)^2 = a^2 * b^2 \quad \forall a, b \in G$

Solⁿ. Suppose G is a abelian then $ab = b * a \quad \forall a, b \in G$

$$(a * b)^2 = (b * a) (b * a) (a * b) (a * b)$$

$$= a * [b * (a * b)]$$

$$= a * [(b * a) * b]$$

$$= a * [(a * b) * b]$$

$$= a * [a * (b * b)]$$

$$= (a * a) * (b * b)$$

$$(a * b)^2 = a^2 * b^2$$

Q. For any group G , prove that G is abelian if and only if

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

solⁿ Suppose G is abelian then
 $ab = ba \quad \forall a, b \in G$.

Now

$$\begin{aligned} (ab)^2 &= (ab)(ab) \\ &= a[b(ab)] \\ &= a[(ba)b] && \because G \text{ is abelian.} \\ &= a[(ab)b] \\ &= a[a(bb)] \\ &= (a \cdot a)(b \cdot b) \\ &= a^2 \cdot b^2 \quad \text{proven.} \end{aligned}$$

Q. Let $G = \{(a,b) \mid a, b \in \mathbb{R}, a \neq 0\}$. Define a binary operation $*$ on G by $(a,b) * (c,d) = (ac, bc+ad)$ for all $(a,b), (c,d) \in G$. Show that $(G, *)$ is a group.

Solⁿ

(i) Close Property:-

Let (a,b) and (c,d) be any two member (element) of G .
Then $a \neq 0$ and $c \neq 0$
therefore $ac \neq 0$.

Now for all $(a,b) * (c,d) = (ac, bc+ad)$ is also a member of G . Hence G is closed with respect to given composition.

(ii) G Associative Law

Let $(a,b), (c,d)$ and (e,f) be any three member of S . Then

$$\begin{aligned} ((a,b) * (c,d)) * (e,f) &= (ac, bc+ad) * (e,f) \\ &= ([ac]e, [bc+ad]e+f) \\ &= (ace, bce+de+f) \end{aligned}$$

$$\begin{aligned} \therefore (a,b) * ((c,d) * (e,f)) &= (a,b) * [ce, de+f] \\ &= (a[ce], bce+dc+f) \\ &= (ace, bce+dc+f) \end{aligned}$$

(iii) Identity Element. Suppose (x,y) is an element of G such that

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

then $(xa, ya+b) = (a,b) \quad \forall (a,b) \in G_1$

Hence $xa = a$ and $ya+b = b$

$$x = 1 \quad \text{and} \quad y = 0$$

$\therefore (1, 0) \in G_1$ is an identity element

(iv) Inverse Element:-

Let $(a, b) \in G$ be any member of G . Let (x, y) be a member of G such that

$$(x, y) * (a, b) = (1, 0)$$

$$xa, ya + b = 1, 0$$

$$\Rightarrow xa = 1 \quad \text{and} \quad ya + b = 0$$

$$\Rightarrow x = \frac{1}{a} \quad \text{and} \quad y = \frac{-b}{a}$$

$\therefore \left(\frac{1}{a}, -\frac{b}{a}\right)$ is the inverse of (a, b) . Hence G is a group.

Subgroup:-

Let G be a group then any non-empty subset H of G is called the complex of the group G .

A non-empty subset H of a group $(G, *)$ is said to be a subgroup if $(H, *)$ is also a group i.e. if $(G, *)$ is a group then complex which satisfy all the axioms of the group is said to be subgroup i.e. all subgroups are complexes but all complexes are not subgroups.

Any Group $(G, *)$ has at least two subgroups

- (i) Trivial subgroup $\{e, *\}$ as we know that
- (ii) G at self. (because, every set is a subset of itself.)

Therefore, if G is a group, then G is also a subgroup of itself.

Examples

① $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$

② $(\mathbb{Q}, +)$ " " " $(\mathbb{R}, +)$

$\{(1, +), *\}$ is " " " $\{(1, -1, -i, i), *\}$

Trivial subgroup

Consider a subgroup S of $(\mathbb{Z}, +)$. Then 0 must be in S , as 0 is the identity of $(\mathbb{Z}, +)$. If S does not contain any element other than 0 , then S is the trivial (improper) subgroup. Otherwise, suppose S contains another elements are called proper or non-trivial subgroups.

therefore every group $(G, *)$ contain at least two subgroups $(G, *)$ and $\{e, *\}$. And these two subgroups are called trivial subgroups.

Theorem ① The identity element of a subgroup is the same as that of the group.

Proof: let H be the subgroup of the group G and suppose e and e' be the identity elements of G and H respectively.

Now, if $a \in H$ then $a \in G$ then $ae = a$ — ①
since $e \in G$

and, $a \in H$ and $e' \in H \Rightarrow ae' = a$ as $e' \in H$ — ②

$$\begin{aligned} \text{①} \& \text{②} \Rightarrow ae = ae' \\ & \Rightarrow \boxed{e = e'} \end{aligned}$$

After theorem 2

② The necessary and sufficient condition for a non-empty subset H of a group $(G, *)$ to be a subgroup is

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

where b^{-1} is the inverse of b in G .

Theorem 2 A non-empty subset H of a group G is a subgroup of G if and only if:

(i) $a \in H, b \in H \Rightarrow a * b \in H$

(ii) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G .

Proof:- Suppose H is a subgroup of G , then H must be closed with respect to operation $*$ i.e.

$$a \in H, b \in H \Rightarrow a * b \in H.$$

Let $a \in H$ and a^{-1} be the inverse of a in G . Then the inverse of a in H is also a^{-1} . As H itself is a group, each element of H will possess inverse in it, i.e. $a \in H \Rightarrow a^{-1} \in H$.

Thus the condition is necessary. Now let us examine the sufficiency of this condition.

As we have been given in condition (i)
(i) Closure Property:- $a \in H, b \in H \Rightarrow a * b \in H$
this shows that H is closed under the operation $*$.

(ii) Associative Property:- As the elements of H are also the elements of G and the elements of G satisfy the associative law for the binary operation, therefore, the elements of H will also satisfy the associative law.

(iii) Existence of Inverse Identity

from (ii) $a \in H$ and $a^{-1} \in H$

from (i) $a \in H, a^{-1} \in H \Rightarrow a a^{-1} \in H$
 $\Rightarrow e \in H$.

e is the identity of H .

(iv) Inverse:- from (ii) $a \in H \Rightarrow a^{-1} \in H, \forall a \in H$.
therefore each element possesses an inverse.

Theorem-3 A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that

$$a \in H, b \in H \Rightarrow a * b^{-1} \in H \text{ where } b^{-1} \text{ is the inverse of } b \text{ in } G.$$

Proof: For necessary condition

Suppose H is a subgroup of G and let $a \in H, b \in H$. Since H is a group itself so each element of H must possess inverse in it.

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

Also, H is closed under the operation $*$ in G .

Therefore

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

The condition is sufficient. If it is given that $a \in H, b^{-1} \in H \Rightarrow a * b^{-1} \in H$ then we have to prove that H is a subgroup.

(i) closure Property:-

$$\text{let } a, b \in H$$

$$\text{then } b \in H \Rightarrow b^{-1} \in H \text{ (as above)}$$

therefore by the given condition

$$\begin{aligned} a \in H, b^{-1} \in H &\Rightarrow a * (b^{-1})^{-1} \in H \\ &\Rightarrow a * b \in H. \end{aligned}$$

Thus, H is closed with respect to the binary operation $*$.

(ii) Associative Property: Since the elements of H are also the elements of G , then the binary operator $*$ is associative in H .

(iii) Existence of identity:- Since

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

(iv) Existence of Inverse:-

Let $a \in H$, then

$$e \in H, a \in H \Rightarrow e * a^{-1} \in H \text{ (by given condition)} \\ \Rightarrow a^{-1} \in H \text{ [} e * a = a * e = a \text{]}$$

then each element of H posses inverse.

Hence H itself is a group for binary operation $*$ in G .

Q. The interseccion of any two subgroup of a Group $(G, *)$ is again a subgroup of $(G, *)$.

Proof. Let H_1 and H_2 form any two subgroup of $(G, *)$. We have $H_1 \cap H_2 \neq \emptyset$. Since at least the identity element is common to both H_1 & H_2 .

Now Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$

$$\Rightarrow a \in H_1 \text{ and } a \in H_2 \text{ \& } b \in H_1 \text{ and } b \in H_2$$

Since H_1 and H_2 form sub-groups under the group $(G, *)$, we have

$$a \in H_1, b \in H_1 \Rightarrow a * b^{-1} \in H_1$$

$$a \in H_2, b \in H_2 \Rightarrow a * b^{-1} \in H_2$$

$$\text{Finally, } a * b^{-1} \in H_1, a * b^{-1} \in H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$$

thus

$$a \in H_1 \cap H_2, b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$$

therefore, $H_1 \cap H_2$ forms a sub-group under $(G, *)$.

Cyclic Group

A group G is called cyclic group if for some $a \in G$, every element $x \in G$ is of the form a^n , where n is some integer. The element ' a ' is then called a generator of G .

For example: The multiplicative group $G = \{1, -1, i, -i\}$ is cyclic.

We can write $G = \{i, i^2, i^3, i^4\}$

Thus G is cyclic group and i is a generator.

Similarly we can also write

$$G = \{-i, (-i)^2, (-i)^3, (-i)^4\}$$

Thus $-i$ also generator of G .

So there may be more than one generator of a cyclic group.

If G is a cyclic group generated by ' a ' it is denoted by $G = \langle a \rangle$. The elements of G are in the form of

$$\dots a^{-3}, a^{-2}, a^{-1}, a^0, a, a^2, a^3 \dots$$

0. The Group $(G, +_6)$ is a cyclic group where $G = \{0, 1, 2, 3, 4, 5\}$

sdⁿ $+_6$ is modulo 6 operator.

| $+_6$ | 0 | 1 | 2 | 3 | 4 | 5 |
|-------|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

Proof:

$$1^1 = 1$$

$$1^2 = 1 +_6 1 = 1 +_6 1 = 2$$

$$1^3 = 1 +_6 1^2 = 1 +_6 2 = 3$$

$$1^4 = 1 +_6 1^3 = 1 +_6 3 = 4$$

$$1^5 = 1 +_6 1^4 = 1 +_6 4 = 5$$

$$1^6 = 1 +_6 1^5 = 1 +_6 5 = 0 \text{ (e)}$$

$$\text{Thus } G = \{1^6, 1^5, 1^4, 1^3, 1^2, 1^1\}$$

Hence G is a cyclic group and 1 is generator. Similarly, it can be shown that 5 is another generator.

Q Every cyclic group is an abelian group.
Proof:

Let G be a cyclic group and let a be a generator of G so that

$$G = \{a^n : n \in \mathbb{Z}\}$$

If g_1 and g_2 be the two element of G , there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$.

$$\text{Then } g_1 g_2 = a^r \cdot a^s = a^{r+s} = a^s \cdot a^r = g_2 g_1$$

$\therefore G$ is abelian.

Theorem

Q. If a is a generator of a cyclic group G , then a^{-1} is also generator of G .

Solⁿ. Let $G = \langle a \rangle$ be a cyclic group generated by a .

Take x be any integer, then a^x be any element of G for some integer x .

$$\text{So we can write } a^x = (a^{-1})^{-x} \\ = (a^{-1})^{-x}$$

Since $-x$ is also some integer, therefore each element of G , is generated by a^{-1} . Thus a^{-1} is also a generator of G .

Theorem - If a cyclic group G is generated by a . Let a^x be any element of G , where x is some integer. We can write

Theorem:- If a cyclic group G is generated by an element a of order n , then a^m is a generator of G if and only if the greatest common divisor of m and n is 1 i.e. if and only if m and n are relative primes.

Q. How many generators are there of the cyclic group G of order 8.

Solⁿ let a be the generator of G . Then $o(a) = 8$ and we can write $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$

7 is prime to 8, therefore a^7 is also a generator of G

5 " " " 8, " a^5 " " " " " "

3 " " " " " a^3 " " " " " "

1 " " " " " a^1 " " " " " "

Thus there are only 4 generator of G
i.e. a, a^3, a^5, a^7

Cosets

Suppose G is a group and H is any subgroup of G .
Let a be any element of G , then the set

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

is called a right coset of H in G generated by a .

Similarly, the set $aH = \{ah; a \in H\}$

is called left coset of H in G generated by a .

If e is the identity element of G then $He = eH = H$.
Therefore, H itself is right as well as left coset.

If the group G is abelian, then we have
 $ah = ha \quad \forall a \in H$.

therefore right coset Ha will be equal to the
corresponding left coset aH .

If the group operation be addition, then the
right coset of H in G generated by ' a ' is
defined as

$$H+a = \{h+a; h \in H\}$$

and left coset is

$$(a+H) = \{a+h; h \in H\}$$

If H is a subgroup of group G the number of
distinct left or right cosets of H in G is
called the index of H in G and is denoted by
 $[G:H]$ or $i_G(H)$.

Properties of Cosets: Let H be a subgroup of G , \therefore
and $a \neq b$ belongs to G , then

1. $a \in aH$
2. $aH = H$ if and only if $a \in H$.
3. $aH = bH$ or $aH \cap bH = \emptyset$
4. $aH = bH$ if and only if $a^{-1}b \in H$.

Proof: (i) $a = ae \in aH$, $\therefore e$ is identity element of G .

(ii) $aH = H$ if and only if $a \in H$.

If e be the identity in G and so is in H , then

$$\begin{aligned} aH = H &\Rightarrow ae \in H \\ &\Rightarrow a \in H \quad \because e \in H. \quad \text{--- (1)} \end{aligned}$$

Now $a \in H$ and $h \in H$, then

$$a \in H \Rightarrow ah \in H \quad \forall h \in H$$

$$\therefore aH \subset H \quad \text{--- (2) } \checkmark$$

Also $a \in H \Rightarrow a^{-1} \in H$
 $\Rightarrow a^{-1}h \in H \quad \forall h \in H$

$$a^{-1}H \subset H$$

$$a^{-1}h \in H \quad \forall h \in H \text{ by closure law in } H$$

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

$$a(a^{-1}h) \in H \quad \forall h \in H \text{ by closure law in } H$$

$$h \in aH \quad \forall h \in H$$

$$H \subseteq aH. \quad \text{--- (3) } \checkmark$$

So by ② and ③ $aH \subset H$ & $H \subset aH$.
 $\boxed{aH = H}$

Now $a \in H \Rightarrow aH = H$

Hence $aH = H \Leftrightarrow a \in H$

$\boxed{aH = H}$ if and only if $a \in H$.

③ $aH = bH$ OR $aH \cap bH = \emptyset$
(Any two left cosets of a subgroup are either identical or disjoint)

Let H be a subgroup of a group G and let aH and bH be two of its left cosets. Assume that $aH \cap bH \neq \emptyset$ and let c be the common element of the two cosets.

Then we may write $c = ah$ and $c = bh'$
for $h, h' \in H$.

Therefore $ah = bh'$, giving $a = bh'h^{-1}$

Since H is a subgroup, we have $h'h^{-1} \in H$

~~Let~~

Now $aH = (bh'h^{-1})H = b(h'h^{-1}H) = bH$

\rightarrow necessary & sufficient condition

$\because h'h^{-1} \in H$ $\frac{\text{of a subgroup}}$

$aH = bH$ $aH \neq bH$

Hence two cosets are identical if $aH \cap bH \neq \emptyset$

Thus two ^{left} cosets aH & bH are identical if they are ^{not} disjoint $aH \cap bH \neq \emptyset$.

Thus $aH \cap bH = \emptyset$ or $aH = bH$.

Therefore, we have shown that any two left cosets which are not disjoint are identical. if they will be disjoint then they will not be identical.

④ If a and b are arbitrary distinct elements of a group G and H is any subgroup of G , then

Solⁿ.

$$\begin{aligned} Ha = Hb &\Leftrightarrow ab^{-1} \in H \\ aH = bH &\Leftrightarrow b^{-1}a \in H \end{aligned}$$

Let a and b be arbitrary elements of a group G such that $a \neq b$.

Let e be the identity element of G
then $e \in H$.

Now

$$\begin{aligned} Ha &= Hb \\ \Rightarrow (Ha)b^{-1} &= (Hb)b^{-1} \\ \Rightarrow H(ab^{-1}) &= H(bb^{-1}) \\ \Rightarrow H(ab^{-1}) &= He = H \quad (\because He = eH = H) \\ \Rightarrow H(ab^{-1}) &= H \\ \Rightarrow ab^{-1} &\in H \quad \because [Ha = H \text{ if and only if } a \in H] \end{aligned}$$

Conversely:-

$$\begin{aligned} ab^{-1} &\in H \\ \Rightarrow H(ab^{-1}) &= H \\ \Rightarrow H(ab^{-1})b &= Hb \\ \Rightarrow Ha(b^{-1}b) &= Hb \\ \Rightarrow (Ha)e &= Hb \\ \Rightarrow \boxed{Ha = Hb} \end{aligned}$$

Therefore we have $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Lagrange's Theorem:-

The order of each subgroup of a finite group is a divisor (factor) of the group.

Proof. Let H be a subgroup of a finite Group G & let $O(G) = n$ and $O(H) = m$.

To show that m is a divisor of n , we have to show the $n = mp$ for some $p \in \mathbb{N}$.

Let Ha be any right coset of H in G .

Then $O(H) = m \Rightarrow \exists m$ distinct elements $h_1, h_2, \dots, h_m \in H$.

\Rightarrow there exist m distinct elements $ha, h_2a, \dots, h_ma \in Ha$.

\Rightarrow Every right coset of H in G has m distinct elements.

Since, G is finite and therefore, number of distinct right coset of H in G will be finite say p .

Also, we know that any two right cosets of H in G will be disjoint. Hence p distinct right cosets of H in G will contain mp distinct elements.

$\therefore G = Ha \cup Hb \cup Hc \cup \dots$

$\therefore G = Ha \cup Hb \cup Hc \cup \dots$ where $a, b, c, \dots \in G$.

$$O(G) = O(Ha) + O(Hb) + O(Hc) + \dots$$

$$= m + m + m + \dots \text{ } p \text{ times}$$

$$= mp$$

$$O(G) = mp$$

$$\Rightarrow \boxed{n = mp}$$

Order of an Element of a Group

Let G be a group under multiplication. Let e be the identity element in G . Suppose a is any element of G then the least positive integer n , if exist such that $a^n = e$ is said to be the order of an element $a \in G$, and can be written as

$$O(a) = n$$

In case, such a positive integer n does not exist, we say that the element a is of infinite or zero order.

If $a \in G$, n be a positive integer such that $a^n = e$, then $O(a) \leq n$.

exp. Consider a multiplicative group $G = \{1, -1, i, -i\}$ of cube root of unity. find the order of each element of G .

Solⁿ: Since 1 is the identity element, therefore

$$O(1) = 1$$

$$(-1)^2 = 1 \Rightarrow O(-1) = 2$$

$$(i)^4 = 1 \Rightarrow O(i) = 4$$

$$(-i)^4 = 1 \Rightarrow O(-i) = 4.$$

Theorem - 1

The order of every element of a finite group is finite and less than or equal to the order of the group.

$$\text{i.e. } O(a) \leq O(G) \quad \forall a \in G.$$

multiplicative.

Proof. Let G be a finite group of order n and $a \in G$.

Now consider the elements $a^0 = e, a, a^2, a^3, \dots, a^{n-1}, a^n$.

By closure property, all these elements belong to G .
These are $n+1$ numbers.

Since G is finite, therefore, all these elements cannot be distinct.

Suppose

$$a^r = a^s, \text{ where } r > s$$

then,

$$a^r = a^s \Rightarrow a^r \cdot a^{-s} = a^s \cdot a^{-s}$$

multiply by a^{-s} on both sides

$$a^{r-s} = a^0 = e$$

$$a^{r-s} = e$$

$$a^m = e \text{ where } m = r - s.$$

Let $\exists a \in G$ such that $a^k \neq e$

$\forall k \in \mathbb{N}$.

(इस एक element दिया group में जिसका कोई power k करने पर e नहीं आता $k \in \mathbb{N}$)

then we can write $k = k_1 - k_2$

where $k_1, k_2 \in \mathbb{Z}$

$$\Rightarrow a^{k_1 - k_2} \neq e \Rightarrow a^{k_1} \neq a^{k_2} \forall$$

So all powers of a are distinct $k_1, k_2 \in \mathbb{Z}$.

$$\{a, a^2, a^3, \dots, a^n, \dots\}$$

hence Group is infinite.

Since $r > s$, therefore m is a positive integer less than or equal to n . Thus there exist a positive integer m such that

$$a^m = e$$

Hence the $O(a)$ is finite and less than or equal to $O(G)$.

Theorem 2

The order of an element a of group G is the same as that of its inverse a^{-1} .

Solⁿ:

$$\text{let } o(a) = n \text{ and } o(a^{-1}) = m$$

Now $o(a) = n$

$$\therefore a^n = e \quad (\text{identity element})$$

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

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

$$\Rightarrow o(a^{-1}) \leq n \quad \left[\text{If } a \in G \text{ and } n \text{ be a positive integer such that } a^n = e, \text{ then } o(a) \leq n \right]$$

$$\Rightarrow m \leq n \quad \text{--- ①}$$

Also $o(a^{-1}) = m$

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

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

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

$$\Rightarrow a^m = e$$

$$\Rightarrow o(a) \leq m$$

$$\Rightarrow n \leq m \quad \text{--- ②}$$

from ① & ② $\boxed{n = m}$

Theorem-3 If the element a of group G is of order n , then $a^k = e$ iff n is a divisor of k .

Proof Let $a^k = e$ $o(a) = n$

Since k is an integer such that either $k = n$ or $k > n$.

(i) If $k = n$ then n is a divisor of k .

(ii) If $k > n$, then by division algorithm, there exist two integers p and q such that $k = np + q$ where $0 \leq q < n$

$$\begin{aligned}
 \text{Now, } a^k &= a^{np+q} \\
 &= a^{np} \cdot a^q \\
 &= (a^n)^p \cdot a^q \\
 &= (e)^p \cdot a^q \\
 &= a^q
 \end{aligned}$$

$$\text{Therefore } a^k = a^q = e$$

Since $0 \leq q < n$ and $a^n = e$
 then $a^q \neq e$ unless $q=0$

$\therefore k=np$ or n is a divisor of k when $q=0$.

Conversely, let n is a divisor of k , then there exist an integer p such that

$$\begin{aligned}
 \text{Now } k &= np \\
 a^k &= a^{np} \\
 &\Rightarrow (a^n)^p \\
 &= (e)^p \\
 &= e
 \end{aligned}$$

Hence $a^k = e$ iff n is a divisor of k .

Normal Subgroup :-

Let G be a group and H is a subgroup of G . Subgroup H is called normal subgroup (or self conjugate subgroup or invariant subgroup) of G if and only if for every $x \in G$ and all $h \in H$, $xhx^{-1} \in H$.

clearly every subgroup of an abelian group is a normal subgroup.

Theorem 1 Every subgroup of an abelian group is normal.

Proof

Let G be an abelian group & H be a subgroup of G .

let $h \in H$ and $x \in G$

then $xh = hx$ ($\because G$ is abelian)

$$\begin{aligned}\Rightarrow xhx^{-1} &= (hx)x^{-1} \\ &= h \cdot e \\ &= h\end{aligned}$$

Now $h \in H$

$$\therefore \boxed{xhx^{-1} \in H}$$

Hence H is a normal subgroup of G .

Theorem 2 A subgroup H of a group G is normal subgroup if and only if for every x in G , $xHx^{-1} = H$.

Proof let H be a normal subgroup of G . Then we have to show that

$$xHx^{-1} = H \quad \forall x \in G.$$

Now $x \in G$ and $h \in H \Rightarrow xhx^{-1} \in H$ (from theorem)
 $\Rightarrow xHx^{-1} \subseteq H$ — ①

Again $xHx^{-1} \subseteq H \quad \forall x \in G$.

$$\Rightarrow x^{-1}H(x^{-1})^{-1} \subseteq H \quad [\because x^{-1} \in G]$$

$$\Rightarrow x^{-1}Hx \subseteq H$$

$$\Rightarrow x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$$

$$\Rightarrow (xx^{-1})H(xx^{-1}) \subseteq xHx^{-1}$$

$$\Rightarrow eHe \subseteq xHx^{-1}$$

$$\Rightarrow H \subseteq xHx^{-1} \text{ — ②}$$

from eqⁿ ① & ②

$$\boxed{xHx^{-1} = H}$$

Conversely:- Suppose that $xHx^{-1} = H \quad \forall x \in G$. Then we have to show that H is a normal subgroup of G .

Now $xHx^{-1} = H$

$$\Rightarrow xHx^{-1} \subseteq H$$

$$\Rightarrow xhx^{-1} \in H \quad \forall h \in H \text{ \& } \forall x \in G.$$

It is the definition of normal subgroup, H is a normal subgroup of G . Thus a subgroup H is normal iff it is self conjugate.

Theorem The intersection of any two normal subgroups of a group is a normal subgroup

Proof Let G be a group & H_1 & H_2 be any two normal subgroups of a group G . Then $H_1 \cap H_2$ is a subgroup of G .

Now let $x \in G$ and $h \in H_1 \cap H_2$. Then $h \in H_1 \cap H_2$
 $\Rightarrow h \in H_1$ and $h \in H_2$

But H_1 is a normal subgroup of G , then by definition

$$x h x^{-1} \in H_1 \quad \forall x \in G \text{ and } h \in H_1 \quad \text{--- (1)}$$

Also H_2 is a normal subgroup of G . then

$$x h x^{-1} \in H_2 \quad \forall x \in G \text{ and } h \in H_2 \quad \text{--- (2)}$$

Now from (1) and (2) we get

$\forall x \in G, h \in H_1 \cap H_2 \Rightarrow x h x^{-1} \in H_1 \cap H_2$
thus $H_1 \cap H_2$ is a normal subgroup of G .

Homomorphism of a Group

(G, \circ) & $(G', *)$

Suppose G and G' be any two groups and let \circ and $*$ be the respective binary operations. Then a mapping $f: G \rightarrow G'$ is called a homomorphism if $f(a \circ b) = f(a) * f(b) \quad \forall a, b \in G$.

Thus if f is a homomorphism from G to G' then f preserves the composition in G and G' i.e.

image of the composition = composition of images

A group G' is said to be a homomorphic of a group G , if there exists a homomorphism f of G onto G' .

Isomorphism

A homomorphism f of a group (G, \circ) into $(G', *)$ is an isomorphism from G to G' if

(i) f is one-one i.e.

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

(ii) f is onto means every $b \in G'$ there exist $a \in G$ such that $f(a) = b$.

Q. let $(I, +)$ be a group, Prove that the mapping $f: I \rightarrow I$ defined by $f(x) = 5x \quad \forall x \in I$ is homomorphism from I to itself.

Solⁿ The mapping $f: I \rightarrow I$ will be homomorphism if it preserves the composition in I .

$$\begin{aligned} f(x_1 + x_2) &= 5(x_1 + x_2) \\ &= 5x_1 + 5x_2 \\ &= f(x_1) + f(x_2) \end{aligned}$$

Thus f preserves compositions in I and hence homomorphism

Q: Show that the mapping $f: G \rightarrow G'$ given by $f(x) = 2x$ $\forall x \in G$ is an isomorphism of G onto G' where G is the additive group of integers and G' is the additive groups of even integers including zero.

Solⁿ The mapping $f: G \rightarrow G'$ will be an isomorphism if it is

(i) one-one

(ii) Onto

(iii) preserves composition in G & G' .

Let $x_1, x_2 \in G$ then $f(x_1) = f(x_2) \Rightarrow 2x_1 = 2x_2$

$$\Rightarrow x_1 = x_2$$

(by cancellation law)

Thus two elements in G have the same f -image in G' only if they are equal.

Therefore, distinct elements in G have distinct f -images in G' . Hence f is one-one.

f is onto:-

Let y is an element of G' i.e y is an even integer, then $\frac{y}{2} \in G$.

(For exp - $\frac{6}{2} = 3 \in G, \frac{8}{2} = 4 \in G, \frac{2}{2} = 1 \in G, \dots$)

$$f(x) = 2x$$

$$f\left(\frac{y}{2}\right) = 2 \cdot \left(\frac{y}{2}\right) = y$$

So, there exist $\frac{y}{2} \in G$ such that $f\left(\frac{y}{2}\right) = y$. Thus each element of G' is the f -image

Thus f is onto.

f preserves the composition in G & G'

Let $x_1, x_2 \in G$

$$f(x_1 + x_2) = 2(x_1 + x_2) = 2x_1 + 2x_2$$

$$= f(x_1) + f(x_2)$$

Thus f preserves the composition in G & G' .

$\therefore f$ is homomorphism of G & G' .

Endomorphism:-

A homomorphism of a Group G into itself, is called endomorphism of G .

Monomorphism:-

A homomorphism f from a group G to a group G' is said to be monomorphism if f is one-one.

Epimorphism:-

A homomorphism f from a group G to a group G' is said to be epimorphism if f is onto.

Automorphism:-

An isomorphism of a group G onto itself is called an automorphism of G .

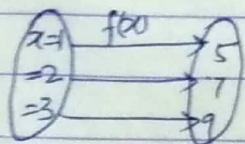
Exp let a be an element of a group G . Then the mapping $f_a: G \rightarrow G$ given by $f_a(x) = axa^{-1}$, $\forall x \in G$ is an automorphism.

Solⁿ let $a \in G$ and $x \in G$.

$$\therefore a \cdot x \in G \Rightarrow a \cdot x \cdot a^{-1} \in G.$$

hence f_a is a mapping from G to G .

Because if we take $y = 2x + 3$



but in the above case

$$a \in G, x \in G$$

$$axa^{-1} \in G \text{ so it}$$

the mapping from G to G .

f_a is one-one.

$$\text{let } x_1, x_2 \in G, \text{ then } f_a(x_1) = f_a(x_2)$$

$$\Rightarrow ax_1a^{-1} = ax_2a^{-1}$$

$$\Rightarrow x_1a^{-1} = x_2a^{-1} \text{ (By left cancellation Law)}$$

$$\Rightarrow x_1 = x_2 \text{ (By Right cancellation Law)}$$

$\therefore f_a$ is one-one.

f_a is onto

For every $y \in G$, there exist $a^{-1}ya \in G$
 $f_a(x) = y = axa^{-1}$
 $\Rightarrow \boxed{a^{-1}ya = x}$

such that $f(x) = y$

$$f_a(x) = a(a^{-1}ya)a^{-1} = (aa^{-1})y(aa^{-1}) \quad (\text{ASSO})$$

$$\Rightarrow f_a \text{ is onto. } \boxed{f_a(x) = y}$$

f_a preserve the composition in G .

\Rightarrow let $x_1, x_2 \in G$ then

$$\begin{aligned} f_a(x_1 x_2) &= a(x_1 x_2)a^{-1} \\ &= ax_1 x_2 a^{-1} \\ &= ax_1 e x_2 a^{-1} \\ &= ax_1 \underline{a^{-1}a} x_2 a^{-1} \\ &= (ax_1 a^{-1}) (ax_2 a^{-1}) \\ &= f_a(x_1) \cdot f_a(x_2) \end{aligned}$$

$\therefore f_a$ preserve the composition in G . Hence f_a is isomorphism.

Theorem 1

Let $(G, *)$ and (G', \circ) be groups with respective identities e and e' . If $f: G \rightarrow G'$ is a homomorphism, then

- (i) $f(e) = e'$
- (ii) $f(a^{-1}) = [f(a)]^{-1} \quad \forall a \in G$.
- x(iii) $f(a^n) = [f(a)]^n \quad \forall a \in G$ and all $n \in \mathbb{Z}$.
- x(iv) $f(S)$ be a subgroup of G' for ~~the~~ each subgroup S of G .

Solⁿ

(i) We know that $e \in G$ then $f(e) \in G'$

$\therefore f$ is a mapping from $G \rightarrow G'$.

Now since $e' \in G'$ & $f(e) \in G'$

$$e' \circ f(e) = f(e) \quad \because e' \text{ is identity element of } G'$$

$$e' \circ f(e) = f(e * e) \quad \because e \text{ is the identity element of } G$$
$$= f(e) \circ f(e)$$

$\therefore f$ is homomorphic

$\Rightarrow \boxed{e' = f(e)}$ By Right cancellation Law.
(e is the identity of G then $f(e)$ is the identity of G')

(ii) We know that $aa^{-1} = a^{-1} * a = e \quad \forall a \in G$
from ①

$$e' = f(e)$$

$$= f(aa^{-1}) = f(a) \circ f(a^{-1}) \quad \because f \text{ is homomorphism} \quad \text{--- ①}$$

$$\text{and } e' = f(e) = f(a^{-1} * a) = f(a^{-1}) \circ f(a) \quad \text{--- ②}$$

thus From ① & ②

$$f(a) \circ f(a^{-1}) = f(a^{-1}) \circ f(a) = e'$$

Hence, $f(a^{-1})$ is the inverse of $f(a)$

$$\therefore f(a^{-1}) = [f(a)]^{-1}$$

Q. If R be the additive group of real numbers and R^+ the multiplicative group of positive real numbers show that the following mapping are isomorphism.

Solⁿ. (i) $f: R \rightarrow R^+$ $f(x) = e^x$, $x \in R$ (ii) $f: R^+ \rightarrow R$ i.e. $f(x) = \log x$, $x \in R^+$

For f is one-one. $| (R^+) \& (R, x)$

Let $x_1, x_2 \in G$

then $f(x_1) = f(x_2)$

$$e^{x_1} = e^{x_2}$$

$$\Rightarrow x_1 = x_2$$

Hence two elements in G have same image only if they are same.

For onto let $y = e^x \Rightarrow x = \log_e y$

$$f(x) = e^{\log_e y} = y$$

$\therefore f$ is onto.

f preserves the composition

$$f(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2} = f(x_1) \times f(x_2)$$

Hence f preserves the composition in G & G'

(ii) $f(x) = \log x$ $\forall x \in R^+$

Since any two distinct real positive number have two different logarithms as real numbers

$\therefore f$ is one-one.

For $x_1 \neq x_2 \Rightarrow \log x_1 \neq \log x_2$ $\forall x_1, x_2 \in R^+$

For

f is onto let $y \in R$

$$\text{let } y = \log_e x \Rightarrow x = e^y$$

For every $y \in R$, there exist a $x \in R^+$ such that

$$f(x) = y$$

$$f(x) = \log_e e^y = y \quad \therefore f \text{ is onto.}$$

f preserve the composition $f: R^+ \rightarrow R$

$$f(x_1 \cdot x_2) = \log(x_1 \cdot x_2) = \log x_1 + \log x_2 = f(x_1) + f(x_2)$$

Hence f is homomorphism.

Ring - An algebraic structure $(R, +, \cdot)$, where R is a non-empty set and $+$ and \cdot are two binary operations known as addition and multiplication respectively, is called a ring if the following properties are satisfied:

(i) $(R, +)$ is an abelian group

(ii) (R, \cdot) is semi-group

(iii) Multiplication is distributive with respect to Addition.

OR

① Closed under addition

$$a+b \in R \quad \forall a, b \in R$$

② Associative under addition

$$a+(b+c) = (a+b)+c \quad \forall a, b, c \in R$$

③ Existence of identity

$$0+a = a \quad \forall a \in R$$

0 is the additive identity of R .

④ Existence of inverse

there exist an element $-a \in R$ such that

$$-a+a = 0 = e \quad \forall a \in R.$$

⑤ Commutative under addition

$$a+b = b+a \quad \forall a, b \in R$$

⑥ closed under multiplication

$$a, b \in R \quad a \cdot b \in R$$

⑦ Associative under multiplication

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in R$$

⑧ Multiplication is distributed over addition

(i) Left distributive law $a \cdot (b+c) = a \cdot b + a \cdot c$

(ii) Right " " $(b+c) \cdot a = b \cdot a + c \cdot a$

An algebraic structure $(R, +, \cdot)$ is said to be a ring provided $a, b \in R, c, d \in R, \forall a, b \in R$

Commutative Ring:-

A ring $(R, +, \cdot)$ is called a commutative ring if $a \cdot b = b \cdot a \quad \forall a, b \in R$.

Ring with unity (if multiplicative semi-group (R, \cdot) has identity element) (such an identity element is called unity)

A ring $(R, +, \cdot)$ is said to be ring with unity if R has the identity element for its multiplicative composition. If there exists $e \in R$ such that

$$a \cdot e = e \cdot a = a \quad \forall a \in R \quad (\text{here } e=1) \text{ for multiplicative composition.}$$

Some Examples:-

① Null Ring (or Zero Ring) - A set R having a single element 0 with two binary operations addition and multiplication defined by $0+0=0$ & $0 \cdot 0=0$ is called Null Ring.

② The set $R = \{a, b\}$ with addition and multiplication defined by the following table

| | | |
|---|---|---|
| + | a | b |
| a | a | b |
| b | b | a |

| | | |
|---|---|---|
| • | a | b |
| a | a | a |
| b | a | b |

is commutative ring because

$$a \cdot b = b \cdot a = a$$

It has an identity element $e=b$ such that

$$a \cdot e = e \cdot a = a$$

put $e=b$

$a \cdot b = b \cdot a = a$ hence $e=b$ is the identity element. Hence it is commutative ring with unity.

ex. The set I of integers is a ring under addition and multiplication of integers. This ring is said to be the ring of Integers.

It is a commutative ring with unity because multiplication of integers is commutative and 1 is the unity element in I .

D Show that the set $R = \{0, 1, 2, 3, 4, 5\}$ form a commutative ring with respect to $+_6$ and \times_6 as two binary composition.

Solⁿ

$$R = \{0, 1, 2, 3, 4, 5\} \quad a \pm_6 b = (a \pm b) \text{ mod } 6$$

| $+_6$ | 0 | 1 | 2 | 3 | 4 | 5 | \times_6 | 0 | 1 | 2 | 3 | 4 | 5 |
|-------|---|---|---|---|---|---|------------|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 5 | 4 | 3 | 2 | 1 |

① Addition Modulo 6 is closed.

$$\text{for } \forall a, b \in R \quad a \pm_6 b \in R.$$

② $+_6$ is associative. let $a, b, c \in R \mid a \pm_6 b = (a \pm b) \text{ mod } 6$

$$a \pm_6 (b \pm_6 c) = (a \pm_6 b) \pm_6 c$$

non-negative
= a remainder when $a + (b+c)$ is divided by 6

= a remainder when $(a+b) + c$ " " " " " "

$$= (a \pm_6 b) \pm_6 c$$

∴ Hence associative.

3. Existence of identity:- From the composition table 0 is the additive identity.

4. Existence of additive Inverse:- From the composition table

| |
|-------------------|
| inverse of 0 is 0 |
| " " 1 " 5 |
| " " 2 " 4 |
| " " 3 " 3 |
| " " 4 " 2 |
| " " 5 " 1 |

Hence the inverse axiom is true for \oplus_6 .

5) \oplus_6 is commutative.

Let $a, b \in R$

$a \oplus_6 b = a$ non negative remainder when $a+b$ is divided by 6.

= " non-negative remainder when $b+a$ is divided by 6.

= $b \oplus_6 a$.

\therefore Commutative

Thus the algebraic structure (R, \oplus_6) is abelian group.

Now (6) \times_6 is closed

(Multiplication Modulo 6 \times_6) is closed.

$\because a, b \in R, a \times_6 b \in R$.

(7) \times_6 is associative. let $a, b, c \in R$

$a \times_6 (b \times_6 c) = a$ non-negative remainder when $a \times (b \times c)$ is divided by 6.

= a non-negative remainder when $(a \times b) \times c$ is divided by 6.

= $(a \times_6 b) \times_6 c$

= associative

8) \times_6 is distributive over $+_6$.

Let $a, b, c \in R$, then

$$\begin{aligned} a \times_6 (b +_6 c) &= (a \times_6 b) +_6 (a \times_6 c) && \text{[Left Dist Law]} \\ (b +_6 c) \times_6 a &= (b \times_6 a) +_6 (c \times_6 a) && \text{[Right " "]} \end{aligned}$$

(i) $a \times_6 (b +_6 c) = a$ non-negative remainder when $a(b+c)$ is divided by 6.

$$\begin{aligned} &= a \text{ non-negative remainder when } ab+ac \text{ is divided by 6.} \\ &= (a \times_6 b) +_6 (a \times_6 c) \end{aligned}$$

Similarly $(b +_6 c) \times_6 a = (b \times_6 a) + (c \times_6 a)$

9) \times_6 is commutative

Let $a, b \in R$

$$a \times_6 b = a \text{ non-negative remainder when } a \times b \text{ is divided by 6.}$$

$$= a \text{ non-negative remainder when } b \times a \text{ is divided by 6}$$

$$= b \times_6 a$$

Hence \times_6 is commutative.

Hence $(R, '+_6, \times_6)$ is a commutative Ring.

~~Q~~ If R is a Ring such that $a^2 = a \forall a \in R$ prove that

(i) $a + a = 0 \forall a \in R$ (ii) $a + b = 0 \Rightarrow a = b$

(iii) $a + b = 0 \forall a = b$

(iii) R is a commutative Ring.

$$a \cdot b = a \cdot c \quad \text{Left cancel} \\ \Rightarrow b = c \\ b \cdot a = c \cdot a \Rightarrow b = c \quad \text{(Right cancellation)}$$

(i) Since $a \in R \Rightarrow a+a \in R$ (By closure Property)

$$a^2 = a \quad \text{(given)} \quad \text{--- ①}$$

Now $(a+a)^2 = a+a$ put $a = a+a$ in eqⁿ ①

$$(a+a) \cdot (a+a) = (a+a)$$

$$(a+a) \cdot a + (a+a) \cdot a = a+a \quad \text{(By left Distributed Law)}$$

$$(a^2+a^2) + (a^2+a^2) = a+a \quad \text{(By Right Distributed Law)}$$

$$(a+a) + (a+a) = (a+a) \quad (\because a^2 = a)$$

$$(a+a) + (a+a) = (a+a) + 0$$

$$a+a = 0 \quad \text{(By left cancellation Law)}$$

Hence prove.

(iii) If $a, b \in R$ then $a+b \in R$

Now $(a+b)^2 = a+b$ ($\because a^2 = a$)

$$(a+b) \cdot (a+b) = (a+b)$$

$$(a+b)a + (a+b)b = (a+b) \quad \text{(By Left Distributive Law)}$$

$$a^2 + ba + ab + b^2 = a+b \quad \text{(By Right " " " ")}$$

$$\underline{a + ba + ab + b = a + b}$$

$$a + ba + ab = a \quad \text{(By Right cancellation Law)}$$

$$\underline{ba + ab = 0} \quad \text{(By Left " " " ")}$$

$$\boxed{ab = ba}$$

[If $a+b=0$
then $a=b$]

(ii) $a+b=0$

$$a+b = a+a \quad \text{from (i) } (a+a=0)$$

$$\boxed{b=a} \quad \text{(By left cancellation Law)}$$

R is a commutative Ring.

(ii) $a+b=0 \Rightarrow a+b = a+a \quad \because a+a=0$

$b=a$ from left cancellation Law from eq ①
① post

Special kind of Rings

① Integral Domain - A ring is called an integral domain if it is commutative has unit element and is without zero divisor.

Field:- A ring $(F, +, \cdot)$ is said to be a field if it
(i) has unity
(ii) has commutative
(iii) has every non-zero element has multiplicative
inverse.

Note:- Let R be a ring with unity 1 . If $a \in R$ and
there exist $b \in R$ such that $a \cdot b = b \cdot a = 1$,
then b is called the multiplicative inverse
of a and a is called unit of R .

exp $(\mathbb{Z}, +, \cdot)$ is a ring with unity, 1 being
the unity of the ring

Zero Divisor

→ If in a Ring R , there exist element a & b
such that $a \cdot b = 0$ when neither $a = 0$ nor
 $b = 0$. Then, the element a and b are
called zero divisors.

→ A ring $(R, +, \cdot)$ is said to be a ring without
zero divisor if for all $a, b \in R$, $ab = 0 \Rightarrow$
 $a = 0$ or $b = 0$, where 0 is the additive
identity of the ring R .

Exp The Ring $(\mathbb{Z}, +, \cdot)$ is a ring without
zero divisor since the product of two
non-zero integers cannot be equal to zero.

Q. Show that $(\mathbb{Z}_6, +_6, \times_6)$ is a ring with zero divisors.

Ans:

| \times_6 | 0 | 1 | 2 | 3 | 4 | 5 |
|------------|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Note that $3 \times_6 2 = 0$

$3 \times_6 4 = 0$

the product of two non-zero elements are zero.
hence zero divisors are = 2, 3, 4.

BY - KKV SIR

Field

- A ring $(F, +, \cdot)$ is said to be a field if
- It is commutative
 - It has unity
 - It is such that every non-zero element has multiplicative inverse.

OR

- which is closed
- ✓ A field is a set F under two operations $+$ and \times such that
- F is an abelian group under $+$ &
 - $F - \{0\}$ (the set F without the additive identity) is an abelian group under \times .

Exp The ring $(\{0, 1, 2, 3, 4\}, +_5, \times_5)$ is an example of finite field.

Ans.

| $+_6$ | 0 | 1 | 2 | 3 | 4 | \times_6 | 0 | 1 | 2 | 3 | 4 |
|-------|---|---|---|---|---|------------|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 2 | 3 | 4 | 0 | 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 2 | 3 | 4 | 0 | 1 | 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 3 | 4 | 0 | 1 | 2 | 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 | 4 | 0 | 4 | 3 | 2 | 1 |

- $\{0, 1, 2, 3, 4\}$ is an abelian group for $+_5$.
 0 is the additive identity and each element is invertible.
- $\{1, 2, 3, 4\}$ is an abelian group for \times_5 .
 1 is the unity and each element has its multiplicative inverse.