Algebra and Number Theory [MA 8551]

Introduction :

Number System

Natural numbers. $(\mathbb{N}) = \{1, 2, 3, 4, \ldots\}$

Whole numbers $(W) = \{0, 1, 2, 3, 4, \ldots\}$

Integers $(Z) = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$

Rational $(Q) = \left\{ \frac{p}{q} / p \text{ and } q \text{ are integers, } q \neq 0 \right\}$

Irrational = Not rational $= Q^c$

Real numbers = (Rational) $\cup$ (irrational)

$= Q \cup Q^c$

Note :

Rational and irrationals have no number in common.

That is $Q \cap Q^c = \phi$

ϕ means empty set

Q^c means complement of Q.

Set inclusion

Subset If all the elements of the set A are the elements of B then A is a subset of B

We write $A \subseteq B$.

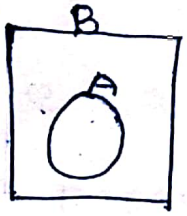
Example

Let $A = \{1, 2, 3\}$

$B = \{1, 2, 3, 4, 5\}$

Hence $A \subseteq B$.

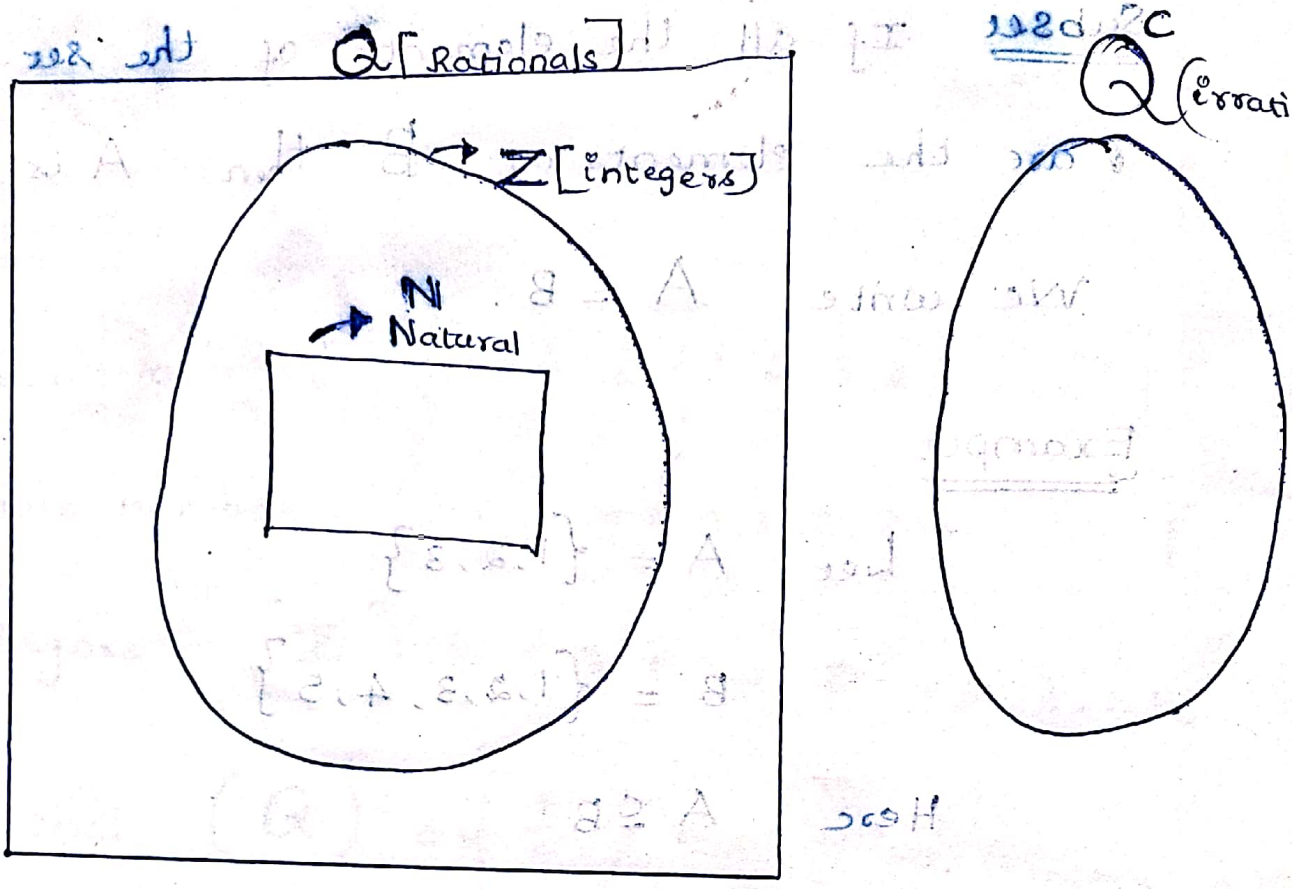
A is a subset of B



Equal Set:

Two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$.

Diagram [Representing Number System]



$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$$

$$\mathbb{Q} \cup \mathbb{Q}^c = \mathbb{R}$$

Here

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

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

$$\mathbb{Q} = \left\{ \frac{p}{q} \;/\; p \text{ and } q \text{ are integers}, q \neq 0 \right\}$$

Unit - I

GROUPS AND RINGS

GROUPS

A non empty set 'G' with binary operation '*' is called a group if it satisfies the following properties.

(i) Closure property:

For any $a, b \in G$, $a * b \in G$.

(ii) Existence of identity:

There exists an identity element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.

(iii) Associative property:

$a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

(iv) Existence of inverse:

For any $a \in G$, there exists $a' \in G$ such that $a * a' = a' * a = e$

Note

Here a' is called inverse of a.

e is identity element.

Notation: If G is a group with respect to $*$ then we denote $(G, *)$ is a group.

Examples

(1) $\mathbb{Z}$ is a group under the binary operation $+$

That is, $(\mathbb{Z}, +)$ is a group.

Proof:

(i) **Closure property**

Let $a, b \in \mathbb{Z}$.

Then obviously $a+b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$

(ii) **Associate property**

Let $a, b, c \in \mathbb{Z}$

Then obviously $a+(b+c) = (a+b)+c$

for all $a, b, c \in \mathbb{Z}$.

(iii) **Existence of identity**

0 is the identity element and $0 \in \mathbb{Z}$

Also for any $a \in \mathbb{Z}$, $0+a = a+0 = a$.

(iv) **Existence of inverse:**

Let $a \in \mathbb{Z}$.

Then $-a \in \mathbb{Z}$ such that

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

Hence $-a$ is inverse of a.

$\therefore (\mathbb{Z}, +)$ is a group.

(2) ~~Prove that~~ $(\mathbb{N}, +)$ is not a group.

Proof

(i) closure property

Let $a, b \in \mathbb{N}$

Then obviously $a+b \in \mathbb{N}$ for all $a, b \in \mathbb{N}$.

(ii) Associative property

Let $a, b, c \in \mathbb{N}$

then obviously $a+(b+c) = (a+b)+c$

for all $a, b, c \in \mathbb{N}$

(iii) Existence of property

Here these does not exists an identity element.

∴ Existence property ~~fails~~ does not hold.

∴ $(\mathbb{N}, +)$ is not a group.

③ Show that Z is not a group under the binary operation '$\cdot$'.

Soln.

To prove $(Z, \cdot)$ is not a group.

(i) closure property:

Let $a, b \in Z$

Then obviously $a \cdot b \in Z$

(ii) Associative property:

Let $a, b, c \in Z$

Then obviously $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(iii) Existence of identity

1 is the identity element and $1 \in Z$

For any $a \in Z$, $1 \cdot a = a \cdot 1 = a$.

(iv) Existence of inverse:

Here elements other than $+1$ and -1 have no inverse

(For example: 2 has no inverse)

$\therefore$ Z is not a group under multiplication.

· Other Examples

(i) $(\mathbb{R}, +)$ is a group.

(ii) $(\mathbb{Q}, +)$ is a group

(iii) $(\mathbb{Q}^c, +)$ is not a group.

(iv) $(\mathbb{R} - \{0\}, \cdot)$ is a group.

(v) $(\mathbb{Q} - \{0\}, \cdot)$ is a group.

Abelian Group

$(G, *)$

A group G is abelian if $a * b = b * a$ for all $a, b \in G$.

Examples

(i) $(\mathbb{R}, +)$ is abelian group

(ii) $(\mathbb{Q}, +)$ is abelian group

(iii) $(\mathbb{R} - \{0\}, \cdot)$ is abelian group.

(iv) $(\mathbb{Q} - \{0\}, \cdot)$ is abelian group.

Problem: Show that the set of all 2×2 non-zero matrices and determinant $\neq 0$ with real entries is a group but not an Abelian group under matrix multiplication.

Soln Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \text{ are real numbers with } a,b,c,d \text{ are not simultaneously zero and } \begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0 \right\}$

(i) **closure property:**

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in G$.

Then $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \in G$.

(ii) **Associate property:**

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \begin{bmatrix} i & j \\ k & l \end{bmatrix} \in G$.

Then $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left[\begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right] \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix}$

(iii) **Existence of identity**

Clearly $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in G$ and it is identity element.

For any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

(iv) **Existence of inverse**

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$.

Then $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$.

$\Rightarrow ad - bc \neq 0$.

$\frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ is the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

$$\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{ad-bc}\begin{bmatrix} ad-bc & -db+db \\ -ac+ac & -ad-bc \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore$ G_S is a group.

To prove G_S is not abelian

Abelian

$a * b = b * a$ for all $a, b \in G_S$.

Let $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix} \in G_S$.

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 8 & 2 \\ 18 & 4 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 6 & 10 \end{bmatrix}$$

Here $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix} \neq \begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$

$\therefore$ G_S is not abelian group.

H.W Determine Which of the following are groups and are not groups. Explain your answer.

① Let $A = \{1, -1, i, -i\}$ where i is a complex number with $i^2 = -1$.

$(A, \cdot)$ is a group or not?

② The set of all whole numbers under the binary operation '+' is a group or not?

③ Let $G = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

ϕ means empty set

Define the binary operation '$\cap$' on G.

$\cap$ means intersection.

$(G, \cap)$ is a group or not?

Order of group The number of elements in a finite group is order of Group. Denoted by $O(G) = |G|$.

Permutation Group.

Permutation

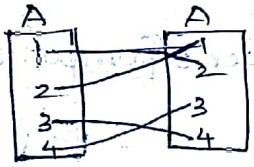
Let 'A' be a finite set. A bijection from 'A' to itself is called a permutation.

[Bijection means 1-1 & onto mapping].

Example Let $A = \{1, 2, 3, 4\}$.

Define a function 'f' from A into A by

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



Then f is bijection.

We write this permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

may be read as "1 goes to 2, 2 goes to 1, 3 goes to 4, 4 goes to 3"

Operation On permutations

Let $A = \{1, 2, 3\}$.

Then there are $3! = 6$ permutations on A.

Let S_3 denote there permutations.

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

Define, a binary operation '$\circ$' [composition] on S_3

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

Take P_1 :
$$\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{matrix}$$

P_2 :
$$\begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{matrix}$$

Then $P_1 \circ P_2$:
$$\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{matrix}$$

Similarly define S_n for $\{1, 2, \ldots, n\}$.

Note

* S_n contains $n!$ elements.
* S_n is a group under $\circ$ [composition of mappings]

Example Let $A = \{1, 2, 3\}$.

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

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

$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Cayley table :

$\circ$	e	P_1	P_2	P_3	P_4	P_5
e	e	P_1	P_2	P_3	P_4	P_5
P_1	P_1	e	P_5	P_4	P_3	P_2
P_2	P_2	P_4	e	P_5	P_1	P_3
P_3	P_3	P_5	P_4	e	P_2	P_1
P_4	P_4	P_2	P_3	P_1	P_5	e
P_5	P_5	P_3	P_1	P_2	e	P_4

All properties are clear from above table.

$\therefore S_3$ is a group.

S_3 is non abelian.

U.Q Let G_S be the set of all rigid motions of a equilateral triangle. Identify the elements of G_S. Show that it is a non-abelian group of order 6.

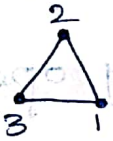
Soln. Let $e =$ 

be equilateral triangle.

Then possible rigid motions are

Rotate 180° anticlockwise 

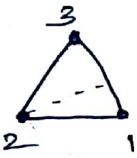
$= P_5$

Rotate 240° anticlockwise 

$= P_4$

Mirrored along axis 

$= P_1$

" " " 

$= P_2$

" " " 

$= P_3$

∴ Set of all rigid motions $= \{e, P_1, P_2, P_3, P_4, P_5\}$.

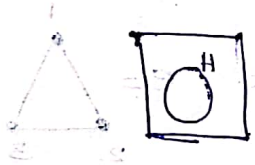
Write cayley Table.

This is non-abelian group of order 6.

It is non-abelian group, since $P_1 \circ P_2 \neq P_2 \circ P_1$

Defn (Subgroup)

A subset 'H' of a group G is called a subgroup of G if H forms a group with respect to the binary operation in G.



Examples

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

② $\{1\}$ is a subgroup of $\{1, -1, i, -i\}$ with respect to the binary operation '.'

③ $\{e, P_1\}$ is a subgroup of S_3 under the binary operation 'o' [composition].

Subgroup Test:

A non-empty subset 'H' of a group $(G, *)$ is a subgroup of G iff $a, b \in H \Rightarrow ab^{-1} \in H$.

Example

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

Proof Let $a, b \in \mathbb{Z}$

Since a, b are integers, $-a, -b$ belong to $\mathbb{Z}$

$\Rightarrow a - b$ is an integer

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

Cyclic Subgroup :

Let G be a group and $a \in G$.

Then $H = \{a^n / n \in \mathbb{Z}\}$ is a subgroup of G.

H is called a cyclic subgroup of G generated by a and is denoted by $\langle a \rangle$.

*) $H = \langle a \rangle$.

Important note

* Suppose G is a group w.r.t '$\cdot$'

Then $H = \{a^n / n \in \mathbb{Z}\}$ is cyclic subgroup.

* Suppose G is a group w.r.t '$+$'

Then $H = \{na / n \in \mathbb{Z}\}$ is cyclic subgroup.

Cyclic Group :

Let G be a group and $a \in G$.

Then G is cyclic if $\langle a \rangle = G$.

Here a is called generator of G.

Examples

① $\{1, -1, i, -i\}$ is a cyclic group w.r.t '$\cdot$'.

Proof

Here i and $-i$ are generators.

$$\langle i \rangle = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}.$$

Similarly $\langle -i \rangle = \{-i, (-i)^2, (-i)^3, (-i)^4\}$

$$= \{-i, -1, i, 1\}.$$

② $(Z, +)$ is a cyclic group.

Proof:

Here 1 and -1 are generators.

$$\langle 1 \rangle = \{n \cdot 1 / n \in Z\} = Z$$

$$\langle -1 \rangle = \{n \cdot (-1) / n \in Z\} = Z$$

This is infinite cyclic group.

③ $(Q, +)$ is not a cyclic group

Since there is no element $a \in Q$ such that $\langle a \rangle = Q$.

④ Let $Z_5 = \{0, 1, 2, 3, 4\}$.

Define a binary operation $\oplus$ in Z_5 such that

$a \oplus b = r$ where r is a remainder when $a+b$ is divided by 5.

For example, $1 \oplus 3 = 4$.

$2 \oplus 4 = 1$

(∵ we get remainder 1 when '2+4' is divided by 5)

$3 \oplus 4 = 2$

$4 \oplus 4 = 3$

$1 \oplus 4 = 0$

Z_5 is a cyclic group.

Proof Here 1 is a generator.

$$\langle 1 \rangle = \{1, 1\oplus 1, 1\oplus 1\oplus 1, 1\oplus 1\oplus 1\oplus 1, 1\oplus 1\oplus 1\oplus 1\oplus 1\}$$

$$= \{1, 2, 3, 4, 0\}.$$

$$= Z_5.$$

Also 3 is a generator

$$\langle 3 \rangle = \{3, 3\oplus 3, 3\oplus 3\oplus 3, 3\oplus 3\oplus 3\oplus 3, 3\oplus 3\oplus 3\oplus 3\oplus 3\}$$

$$= \{3, 1, 4, 2, 0\}$$

$$= Z_5.$$

Home work:

Prove that $\{Z_7, \oplus\}$ is a group. [Write cayley Table].

Also prove it is cyclic group.

Prime Number:

A number is prime if its only divisors are 1 and itself.

Examples

2, 3, 5, 7, 11 are prime numbers.

Question: Prove that $Z_7 - \{0\}$ is a group under multiplication modulo 7. $(\odot)$

Soln

$$Z_7 - \{0\} = \{1, 2, 3, 4, 5, 6\}.$$

Define a binary operation "multiplication modulo 7" on $Z_7 - \{0\}$ by

$a \odot b = r$ where r is a remainder when ab is divided by 7.

For example,

$2 \odot 5 = 3$

$2 \odot 3 = 6.$

Cayley Table

$\odot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

To prove $(Z_7 - \{0\}, \odot)$ is a group

(i) closure property:

It is obvious from cayley table.

(ii) Associative property:

Let $a, b, c \in Z_7 - \{0\}$.

Then clearly $a \odot (b \odot c) = (a \odot b) \odot c$

(iii) Existence of identity

1 is the identity element

and $1 \in Z_7 - \{0\}$ with $1 \odot a = a \odot 1 = a$

for all $a \in Z_7 - \{0\}$.

(iv) Existence of inverse

Inverse of 1 is 1

" " 2 is 4

" " 3 is 5

" " 4 is 2

" " 5 is 3

" " 6 is 6.

∴ All properties of Group are satisfied.

∴ $(Z_7 - \{0\}, \odot)$ is a group.

Also it is abelian group.

(∵ $a \odot b = b \odot a$ for all $a, b \in Z_7 - \{0\}$)

To prove $(Z_7 - \{0\}, \odot)$ is a cyclic group:

Here 3 is a generator.

$$\langle 3 \rangle = \{3, 3\odot3, 3\odot3\odot3, 3\odot3\odot3\odot3, 3\odot3\odot3\odot3\odot3, 3\odot3\odot3\odot3\odot3\odot3\}$$

$$= \{3, 2, 6, 4, 5, 1\}$$

$$= Z_7 - \{0\}$$

$\therefore (Z_7 - \{0\}, \odot)$ is cyclic group.

Note

* Generally $(Z_n - \{0\}, \odot)$ is a group if n is prime.

For example $(Z_6 - \{0\}, \odot)$ is not a group.

Reason: $Z_6 - \{0\} = \{1, 2, 3, 4, 5\}$.

Here $2, 3 \in Z_6 - \{0\}$.

But $2 \odot 3 = 0 \notin Z_6 - \{0\}$.

$\therefore$ closure property is not satisfied

Problem Let $G = \{q \in \mathbb{Q} / q \neq -1\}$

Define a binary operation '$\circ$' on G by

$$x \circ y = x + y + xy.$$

Prove that G is an abelian group.

Soln:

$$G = \{q \in \mathbb{Q} / q \neq -1\}.$$

Let $x, y \in G$.

$$x \circ y = x + y + xy.$$

(i) Closure property:

Let $x, y \in G$.

$\Rightarrow x \neq -1$ and $y \neq -1$.

$x \circ y = x + y + xy$.

To prove: $x + y + xy \neq -1$

Suppose $x + y + xy = -1$

Then $x + y + xy + 1 = 0$

$\Rightarrow (x+1)(y+1) = 0$.

$\Rightarrow (x+1) = 0$ (or) $(y+1) = 0$

$\Rightarrow x = -1$ (or) $y = -1$.

Which is a contradiction to $x \neq -1$ and $y \neq -1$.

$\therefore x + y + xy \neq -1$.

$\therefore x + y + xy \in G$.

Closure property satisfied.

(ii) Associate property

Let $x, y, z \in G$.

To prove $x \circ (y \circ z) = (x \circ y) \circ z$

L.H.S

$$x \circ (y \circ z) = x \circ (y + z + yz)$$

$$= x + y + z + yz + xy + xz + xyz \longrightarrow (1)$$

R.H.S

$$(x \circ y) \circ z = (x + y + xy) \circ z$$

$$= x + y + xy + z + xz + yz + xyz \longrightarrow (2)$$

From (1) and (2), associative property holds good.

(iii) Existence of identity :

$0 \in G_S$ is identity element.

Since, $0 * x = 0 + x + 0.x = x$, for all $x \in G_S$.

(iv) Existence of inverse :

Let $a \in G_S$. $\Rightarrow a \neq -1$.

Let a' be the inverse of a.

Then $a * a' = a' * a$ = identity element

$$a * a' = 0$$

$$a + a' + aa' = 0.$$

$$\Rightarrow a + a'(1+a) = 0.$$

$$\Rightarrow a'(1+a) = 0 - a = -a$$

$$\Rightarrow a' = \frac{-a}{(1+a)} \in G_S$$

$$a * a' = a + \left(\frac{-a}{1+a}\right) + a\left(\frac{-a}{1+a}\right)$$

$$= \frac{a + a^2 - a - a^2}{1+a}$$

$$= \frac{0}{1+a}$$

$$= 0. \quad \text{(identity element)}.$$

Also $a' * a' = 0$. (identity element)

$\therefore$ G_S is a group.

Abelian

$$x * y = x + y + xy$$

$$y * x = y + x + yx = x + y + xy.$$

$\therefore x * y = y * x$ for all $x, y \in G_S$.

$\therefore$ G_S is abelian group.

Notations (Useful in proving theorems)

$\in$: belongs to

$\notin$: does not belongs to

$\Rightarrow$: implies that

$\Leftrightarrow$: if and only if

$\Rightarrow\Leftarrow$: contradiction

$\exists$: there exists

Theorem ① Let G be a group.

(i) identity element of G is unique.

(ii) for any $a \in G$, the inverse of a is unique.

Proof:

Let $(G, *)$ be a group.

(i) T.P : identity element of G is unique.

Suppose e_1 and e_2 are two identity elements of G.

Since e_1 is identity, $e_1 * e_2 = e_2$ ⟶ ①

Since e_2 is identity, $e_1 * e_2 = e_1$ ⟶ ②

From ① and ②, $e_1 = e_2$.

∴ Identity element of G is unique.

(ii) Let $a \in G$ be any arbitrary element.

To prove inverse of a is unique.

Let a' and a'' be two inverses of a.

$\Rightarrow \quad a*a' = a'*a = e$

Also $a * a'' = a'' * a = e$. (identity element)

$\therefore \quad a' = a'*e$

$= a'*(a * a'')$

$= (a' * a) * a''$

$= e * a''$

$a' = a''$

$\therefore$ Inverse of a is unique.

Theorem ② In a group the left and right cancellation laws hold.

i) $a * b = a * c \Rightarrow b = c$.

Proof

Left cancellation Law:

Let $a * b = a * c$

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

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$ (Using Associative Property)

$\Rightarrow e * b = e * c$

$\Rightarrow b = c$.

Hence the left cancellation law.

Right cancellation law

T.P $b * a = c * a \Rightarrow b = c$.

Let $b * a = c * a$

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

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

$\Rightarrow b * e = c * e$

$\Rightarrow b = c$

Hence the right cancellation law

Theorem ③

Let $(H, *)$ be a subgroup of $(G, *)$. Then

ⓐ the identity element of H is the same as that of G.

ⓑ for each $a \in H$ the inverse of a in H is the same as the inverse of a in G.

Proof

ⓐ Let e be an identity element of G and e' be an identity element of H.

Let $a \in H$

Then $a = e'a$ ($\because e'$ is identity in H).

Also $a \in G$. ($\because H \subseteq G$)

Now $a = e * a$.

$\therefore e'a = e * a$. is true in G.

Using right cancellation law, $e' = e$.

$\therefore$ Identity element of H is same as that of G.

(ii) (b) Let a' and a'' be the inverses of a in G in H respectively.

From (a), G and H have same identity element say e.

$\Rightarrow a' * a = e$ and

$a'' * a = e$

$\therefore a' * a = a'' * a$.

Using right cancellation law, $a' = a''$

$\therefore$ Inverse of a in H is same that of G.

Theorem (4) A subset H of a group G is a subgroup of G if and only if

(i) it is closed under the binary operation in G

(ii) the identity e of G is in H

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

Proof:-

Let H be a subgroup of $(G, *)$

Then $(H, *)$ is also a group

$\therefore$ (i), (ii), (iii) are obviously true.

Conversely, let us assume that H is a subset of G satisfying (i), (ii), (iii).

To prove: H is a subgroup.

Closure property:

Let $a, b \in H$.

Then by (i), $a * b \in H$.

Associative property: Let $a, b, c \in H$

$a * (b * c) = (a * b) * c$ for all $a, b, c \in H$.

($\because H \subseteq G$).

Existence of identity

It is obvious from (ii).

Existence of inverse.

It is obvious from (iv).

$\therefore (H, *)$ is a group and $H \subseteq G$.

$\therefore$ H is a subgroup of G.

Theorem 5 Let H be a non-empty finite subset of a group G, then H is a subgroup of G if and only if H is closed under the binary operation in G.

Proof

Let $(G, *)$ be a group.

Let H be a non-empty finite subset of G.

Assume H is closed under $*$

To prove: H is a subgroup of G.

Let $a \in H$

Since H is closed under $*$, a, $a*a$, $a*a*a$, ... are all elements of H.

$\Rightarrow a, a^2, a^3, \ldots, a^n, \ldots$ are all elements of H.

Since H is finite $a, a^2, a^3, \ldots, a^n, \ldots$ cannot all be distinct.

Hence $a^r = a^s$ for some $r < s$.

Then $a^{s-r} = a^r * a^{-r} = e \in H$.

Take $s-r = m$.

Then $a^m = e$.

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

$\Rightarrow a^{m-1}$ is inverse of a

Also $a^{m-1} \in H$.

$\therefore$ H is subgroup [using theorem ④]

Conversely, let H is a subgroup of G.

Then H is closed under the binary operation in G.

Hence the proof.

Theorem ⑥ If H and K are subgroups of a group G then $H \cap K$ is also a subgroup of G.

Proof:-

Let H and K be subgroups of a group $(G, *)$.

Then $e \in H \cap K$.

$\Rightarrow H \cap K$ is non-empty.

To prove: $H \cap K$ is a subgroup.

Let $a, b \in H \cap K$.

$\Rightarrow a, b \in H$ and $a, b \in K$

Since H is a subgroup $a * b^{-1} \in H$

Since K is a subgroup $a * b^{-1} \in K$.

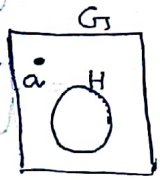
$\Rightarrow a * b^{-1} \in H \cap K$.

$\therefore H \cap K$ is a subgroup.

Defn [coset]

If H is a subgroup of a group G, then for each $a \in G$, the set $aH = \{ah / h \in H\}$ is called a left coset of H in G.

The set $Ha = \{ha / h \in H\}$ is called a right coset of H in G.



Note

* If the operation in G is '+', we write

$a+H$ in place of aH.

$a+H = \{a+h / h \in H\}$.

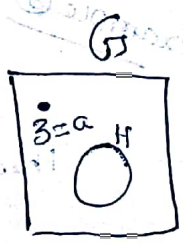
Examples

① Let G be the set of all integers with the binary operation '+'.

$\Rightarrow G = (Z, +)$.

Let $2Z = \{2z / z \in Z\}$

$= \{0, \pm 2, \pm 4, \pm 6, \ldots\}$



Take $H = (2Z, +)$

Then H is a subgroup of G.

$a = 3 \in G$.

Left coset of $H = 3H = 3+H$

$= \{3+h / h \in H\}$.

$= \{3, 5, 1, 7, -1, 9, -3, \ldots\}$.

Example ② Let $G = (Z_{12}, \oplus)$.

$H = \{0, 4, 8\}$ under $\oplus$ [addition modulo 12]

Then H is a subgroup of G.

Take $a = 1 \in G$.

$1 \oplus H = \{1 \oplus h / h \in H\}$

$= \{1 \oplus 0, 1 \oplus 4, 1 \oplus 8\}$

$= \{1, 5, 9\}$.

Take $a = 5 \in G$.

$5 \oplus H = \{5 \oplus h / h \in H\}$

$= \{5 \oplus 0, 5 \oplus 4, 5 \oplus 8\}$

$= \{5, 9, 1\}$

$1 \oplus H$ and $5 \oplus H$ are determine same left coset of H in G.

Example ③ Let $G = (S_3, \circ)$

$H = \{e, P_1\}$ under composition.

Then H is a subgroup of G.

$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Take $a = P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in G$.

Then $aH = a \circ H = \{a \circ h / h \in H\}$.

$= \{a \circ e, a \circ P_1\}$

$= \{P_2, P_2 \circ P_1\}$

Left coset of H $= \{P_2, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\}$.

Right coset of H $= Ha = H \circ a = \{ h \circ a / h \in H \}$.

$= \{ e \circ a, P_1 \circ a \}$

$= \{ e \circ P_2, P_1 \circ P_2 \}$

$= \{ P_2, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \}$.

Note: Here $aH \neq Ha$.

Theorem (7) If H is a subgroup of a finite group G, then for all $a, b \in G$

(i) $|aH| = |H|$

(ii) either $aH = bH$ or $aH \cap bH = \phi$

Proof:-

Let H be a subgroup of a finite group G.

Let $a, b \in G$ be any arbitrary elements.

(i) To prove $|aH| = |H|$.

$aH = \{ ah / h \in H \}$.

$\Rightarrow |aH| \leq |H|$.

$\Rightarrow |aH| < |H|$ or $|aH| = |H|$.

We claim that $|aH| < |H|$ is not possible.

Suppose $|aH| < |H|$ is possible.

Then $\exists$ elements h_1, h_2 with $h_1 \neq h_2$ such that

$ah_1 = ah_2$.

$\Rightarrow h_1 = h_2$ (using cancellation law).

Which is a $\Rightarrow\Leftarrow$ to $h_1 \neq h_2$.

$\therefore |aH| < |H|$ is not possible. $\Rightarrow |aH| = |H|$.

(ii) Let aH and bH be two left cosets.

Suppose aH and bH are not disjoint

$\Rightarrow aH \cap bH \neq \phi$.

We claim that $aH = bH$.

Since $aH \cap bH \neq \phi$, $\exists$ an element $c \in aH \cap bH$.

$\Rightarrow c \in aH$ and $c \in bH$

$\Rightarrow cH = aH$ and $cH = bH$.

Using
$a \in bH \Rightarrow aH = bH$.

$\therefore aH = bH$.

$\therefore$ Either $aH = bH$ or $aH \cap bH = \phi$.

In other words, aH and bH are either identical or disjoint.

Theorem (8) Lagrange's Theorem

If G is a finite group of order n with H a subgroup of order m, then m divides n.

Proof:-

If $H = G$ then the thm is obviously true.

Assume $H \neq G$.

$\Rightarrow m < n$.

$\therefore \exists$ an element $a \in G - H$.

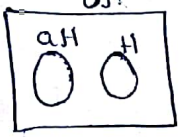
$\Rightarrow a \in G$ but $a \notin H$.

$a \notin H \Rightarrow aH \neq H$

$\therefore aH$ and H are disjoint

$\Rightarrow aH \cap H = \phi$.

G.



If $G = aH \cup H$, then $|G| = |aH| + |H|$

$= |H| + |H|$

$(\because |aH| = |H|)$

$= 2|H|$.

$\Rightarrow n = 2m$

$\Rightarrow m$ divides n.

If $G \neq aH \cup H$, $\exists$ an element $b \in G - (aH \cup H)$.

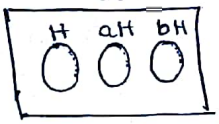
$\Rightarrow b \in G$ but $b \notin aH \cup H$.

Now $b \notin aH \cup H \Rightarrow b \notin aH$ and $b \notin H$.

$\Rightarrow bH \neq aH$ and $bH \neq H$.

$\Rightarrow bH \cap aH = \phi$ and $bH \cap H = \phi$.

G.



If $G = H \cup aH \cup bH$, then $|G| = |H| + |aH| + |bH|$

$= |H| + |H| + |H|$

$= 3|H|$

$n = 3m$

$\Rightarrow m$ divides n.

If $G \neq H \cup aH \cup bH$ then we choose an element $c \in G - (H \cup aH \cup bH)$

Since G is finite group, this process terminates.

$G = a_1H \cup a_2H \cup a_3H \cup \ldots \cup a_kH$ (say)

$|G| = |a_1H| + |a_2H| + |a_3H| + \cdots + |a_kH|$

$= k|H|$

$n = km$.

$\Rightarrow m$ divides n.

Note

* By Lagrange's theorem, $O(H)$ divide $O(G)$.

Suppose 'q' is not a divisor of $O(G)$ then G cannot have a subgroup with order q

Example Let $G = S_3$

$\Rightarrow O(G) = 3! = 6$.

Here 4 does not divide 6.

$\therefore S_3$ cannot have a subgroup of order 4

* Converse of Lagrange's theorem true in finite abelian groups.

U.Q.

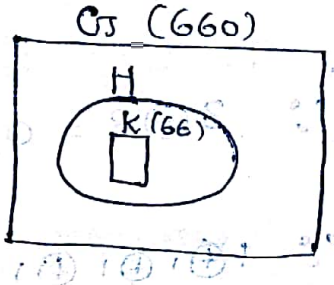
Problem: Let G be a group with subgroups H and K. If $|G| = 660$, $|K| = 66$ and $K \subseteq H \subseteq G$, what are the possible values for $|H|$?

Soln.

Given: G is a group

H and K are subgroups, $K \subseteq H \subseteq G$.

$|G| = 660$, $|K| = 66$.



By Lagranges theorem,

$O(H)$ must divide $O(G)$ and $O(K)$ must divide $O(H)$.

$\therefore$ $O(H)$ must divide $O(G)$ and $O(H)$ = multiple of 66.

$\Rightarrow$ $O(H)$ must divide 660 and $O(H)$ = multiple of 66.

Multiples of 66: 66, 132, 198, 264, 330, 396, 462, 528, 594, 660.

Among there 66, 132, 330, 660. are divisors of 660.

$\therefore$ $O(H)$ can have possible values 66, 132, 330, 660.

Defn [order of an element].

Let G be a group and $a \in G$. Then order of 'a' is the least positive integer 'n' such that $a^n = e$.

Examples ① Let $G = (Z_6, \oplus)$.

Here identity element $= e = 0$

~~Let $a = 3$.~~

Order of 3 is 2. ($\because 3 \oplus 3 = 0$)

Order of 1 is 6 ($\because 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 0$)

Order of 2 is 3 ($\because 2 \oplus 2 \oplus 2 = 0$)

Order of 4 is 3 ($\because 4 \oplus 4 \oplus 4 = 0$)

Order of 5 is 6 ($\because 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 \oplus 5 = 0$)

Order of 0 is 1.

Example ② Let $G = (S_3, \circ)$

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

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

Order of $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ is 1.

order of $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ is 2 ($\because \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$)

order of $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ is 3 ($\because \left[\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right] \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

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

Important Results

① Order of $e = 1$

② Suppose G is a finite cyclic group and 'a' is generator

Then order of $a = O(G) = |G|$.

Example

Let $G = \{1, -1, i, -i\}$.

Then G is a group under multiplication.

$e = 1$

i is generator.

$i.i.i.i = (i)^4 = 1$.

$\therefore$ order of $i = 4 = O(G)$.

③ Order must be least positive integer 'n' such that $a^n = e$.

Example:

Let $G = (Z_3, \oplus)$. $Z_3 = \{0, 1, 2\}$.

Here $e = 0$.

Let $a = 2$.

Order of $a = 3$. ($\because 2 \oplus 2 \oplus 2 = 0$)

At the same time, $2 \oplus 2 \oplus 2 \oplus 2 \oplus 2 \oplus 2 = 0$

(6 times.)

But 3 is least +ve integer.

$\therefore$ Order of 2 is 3.

Theorem ⑨ The order of any element of a finite group G divides the order of G.

Proof:-

Let G be a group of order n.

Let $a \in G$ with $o(a) = m$.

To prove: m divides n.

Since $a \in G$, $\langle a \rangle$ is a subgroup of order m.

By Lagranges theorem, m divides n.

Hence the proof.

Theorem ⑩ Every group of prime order is cyclic.

Proof Let G be a group with $o(G) = p$ where p is a prime number.

Let $a \in G$ with $a \neq e$.

Then $o(a)$ must divide $o(G)$ ($\because$ using thm 9)

$\Rightarrow o(a)$ must divide p. where p is prime

$\Rightarrow o(a) = 1$ or $o(a) = p$ ($\because p$ is prime)

Since $a \neq e$, $o(a) \neq 1$.

$\Rightarrow o(a) = p$.

$\because a \in G$ is an element with $o(a) = p = o(G)$.

$\therefore a$ is a generator.

$\langle a \rangle = G$.

$\therefore G$ is cyclic.

Theorem (11) Let $a \in G$ with $O(a) = n$. If $k \in \mathbb{Z}$ and $a^k = e$, then n divides k.

Proof:- Let G be a group and $a \in G$, $O(a) = n$.

$\therefore$ n is the least positive integer such that $a^n = e$

Let k be any integer with $a^k = e$.

To prove: n divides k.

Suppose n does not divide k.

$\Rightarrow$ $k = qn + r$ where r is a non-zero remainder when k is divided by n.

$0 < r < n$.

$$n \overline{)\, k \,\big|\, q}$$

$r \neq 0$.

$$24 \overline{)\, 100 \,\big|\, 4}$$

$$96$$

$$4$$

Now, $a^k = e$

$\Rightarrow$ $a^{qn+r} = e$

$\Rightarrow$ $a^{qn} \cdot a^r = e$

$\Rightarrow$ $(a^n)^q \cdot a^r = e$

$\Rightarrow$ $(e)^q \cdot a^r = e$

$\Rightarrow$ $e \cdot a^r = e$

$\Rightarrow$ $a^r = e$.

We have $r < n$, with $a^r = e$.

Which is a $\Rightarrow\Leftarrow$ to $O(a) = n$.

$\therefore$ n divides k.

Homomorphism

One to one Function :

A function $f: X \to Y$ is one to one (1–1) if

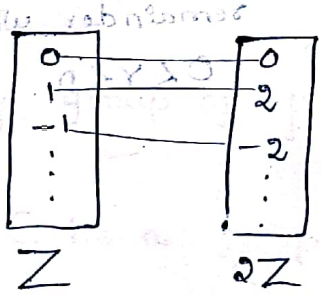
$f(a) = f(b) \Rightarrow a = b$.

In otherwords, f is 1–1 if distinct elements have distinct images.

Example

$f: Z \to 2Z$ defined by,

$f(x) = 2x$ is 1–1 function.



Onto Function :–

A function $f: X \to Y$ is onto if every element in Y has a pre-image in X.

Example

$f: Z \to 2Z$ defined by $f(x) = 2x$ is onto.

Bijection

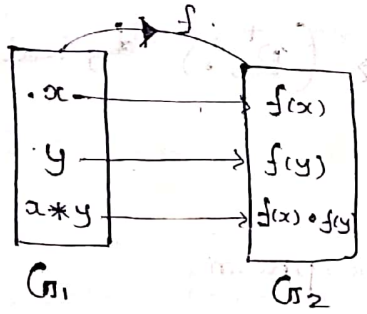
A function $f: X \to Y$ is bijection if it is both 1–1 & onto.

Defn [Group Homomorphism]

Let $(G_1, *)$ and $(G_2, \circ)$ be two groups.

A function $f: G_1 \to G_2$ is a homomorphism if

$$f(x * y) = f(x) \circ f(y) \quad \forall\ x, y \in G_1.$$



Defn [Isomorphism]

Let $(G_1, *)$ and $(G_2, \circ)$ be two groups.

A function $f: G_1 \to G_2$ is an isomorphism if f is homomorphism and bijection.

In this case, we write "G_1 is isomorphic to G_2"

In symbol $G_1 \cong G_2$

Note:

1) Isomorphism is a mapping which preserves algebraic properties.

For example, if $f: G_1 \to G_2$ is an isomorphism

Then G_1 is cyclic $\Rightarrow$ G_2 also cyclic

G_1 is abelian $\Rightarrow$ G_2 also abelian.

Examples

① Let $\mathbb{R}$ denote set of all real numbers.

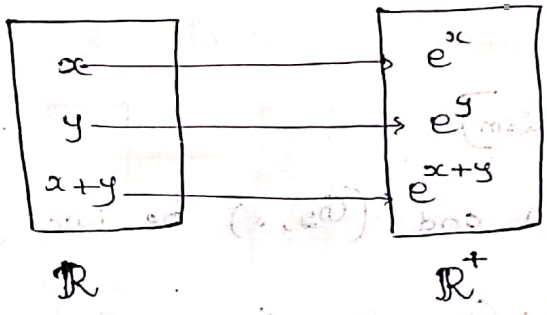
$\mathbb{R}^+$ denote set of all positive real numbers.

Then $(\mathbb{R}, +)$, $(\mathbb{R}^+, \cdot)$ are groups.

Define $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ ~~defined~~ by

$$f(x) = e^x$$

Then f is an isomorphism.



$$f(x+y) = e^{x+y}$$

$$= e^x \cdot e^y$$

$$= f(x) \cdot f(y).$$

$\therefore$ f is homomorphism.

To prove f is 1–1.

Let $f(x) = f(y)$

$\Rightarrow e^x = e^y$

Taking logarithm both sides

$$\log e^x = \log e^y$$

$\Rightarrow x = y.$

$\therefore$ f is 1–1.

To prove f is onto.

Let $r \in \mathbb{R}^+$.

Then $\exists \log r \in \mathbb{R}$ such that

$$f(\log r) = e^{\log r} = r.$$

$\log r$ is the pre-image of r.

$\therefore$ f is onto.

$\therefore$ f is both homomorphism and bijection.

$\therefore$ f is an isomorphism.

$\therefore (\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$

② $f : (\mathbb{Z}, +) \longrightarrow (2\mathbb{Z}, +)$ defined by

$f(x) = 2x$ is an isomorphism.

③ Let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} / a \text{ is non-zero real number} \right\}$

Then G is a group under matrix multiplication.

Let $\mathbb{R}^*$ denote non-zero real numbers.

Then $(\mathbb{R}^*, \cdot)$ is a group.

Define $f : G \to \mathbb{R}^*$ by

$$f \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a.$$

Claim : f is an isomorphism.

To prove f is ~~homomorphism~~ 1–1

Let $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G_S$ such that

$$f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = f\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow a = b$$

$$\Rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

$\therefore f$ is 1–1.

To prove f is onto.

Let $a \in \mathbb{R}^*$

Then $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in G_S$ such that $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$.

$\therefore f$ is onto.

To prove : f is homomorphism.

Let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G_S$

It is enough to prove $f(A \cdot B) = f(A) \cdot f(B)$

$$A \cdot B = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$$

$$f(A \cdot B) = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = ab \quad (\text{by defn})$$

$$= a \cdot b$$

$$= f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot f\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$$

$$= f(A) \cdot f(B)$$

$\therefore$ f is homorphism

$\therefore$ f is isomorphism.

$\Rightarrow (G, \cdot) \cong (\mathbb{R}^*, \cdot)$

Theorem (12) Let $(G, \circ)$, $(H, *)$ be groups with respective identities e_G, e_H. If $f : G \to H$ is a homomorphism, then

(a) $f(e_G) = e_H$

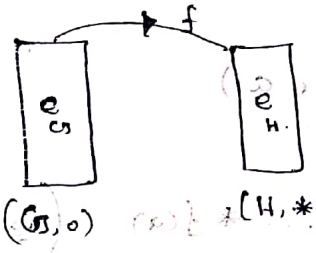
(b) $f(a^{-1}) = [f(a)]^{-1}$ $\forall a \in G$

(c) $f(a^n) = [f(a)]^n$ $\forall a \in G$ and $n \in \mathbb{Z}$

(d) $f(S)$ is a subgroup of H for each subgroup S of G.

Proof:-

Let $(G, \circ)$ and $(H, *)$ be two groups and $f : G \to H$ a homomorphism.



(a) To prove: $f(e_G) = e_H$.

$e_H * f(e_G) = f(e_G)$ ($\because e_H$ is identity in H)

$= f(e_G \circ e_G)$ ($\because e_G \circ e_G = e_G$)

$e_H * f(e_G) = f(e_G) * f(e_G)$ ($\because f$ is homomorphism)

Using right cancellation law, $e_H = f(e_G)$.

(b) To prove: $f(a^{-1}) = [f(a)]^{-1} \quad \forall a \in G$.

Let $a \in G$.

Now $f(a) * f(a^{-1}) = f(a \circ a^{-1})$

$= f(e_G)$

$= e_H$ ... (by (a)) $\longrightarrow$ (1)

Also $f(a^{-1}) * f(a) = f(a^{-1} \circ a)$

$= f(e_G)$

$= e_H$ (by (a)). $\longrightarrow$ (2)

From (1) & (2), $f(a) * f(a^{-1}) = f(a^{-1}) * f(a) = e_H$.

$\Rightarrow$ $f(a^{-1})$ is the inverse of $f(a)$.

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

(c) To prove $f(a^n) = [f(a)]^n \quad \forall a \in G$ and $n \in Z$.

Let $a \in G$ and $n \in Z$.

$f(a^n) = f(\underbrace{a \circ a \circ \dots \circ a}_{n \text{ times}})$

$= \underbrace{f(a) * f(a) * \dots * f(a)}_{n \text{ times}}$ (∵ f is homo)

$= [f(a)]^n$.

(d) Let $(S, \circ)$ be a subgroup of G.

To prove: $f(S)$ is a subgroup of H.

$f(S) = \{ f(a) / a \in H \}$.

Subgroup Test

$$x, y \in S \Rightarrow x \circ y^{-1} \in S.$$

Let $x, y \in f(S)$

To prove: $x \circ y^{-1} \in f(S)$.

$\therefore x = f(a)$, $y = f(b)$ for some $a, b \in S$.

$$x \circ y^{-1} = f(a) \circ [f(b)]^{-1}$$

$$= f(a) \circ f(b^{-1}) \quad (\because f(b^{-1}) = [f(b)]^{-1})$$

$$x \circ y^{-1} = f(a \circ b^{-1}) \longrightarrow (1)$$

Since S is a subgroup $a, b \in S \Rightarrow a \circ b^{-1} \in S$.

$\therefore$ From (1) $x \circ y^{-1} \in f(S)$.

$\therefore f(S)$ is a subgroup of H.

Hence the proof.

Theorem (13) Let G be a cyclic group.

(a) $|G|$ is infinite then $G \cong (Z, +)$

~~(b) $|G|$ is finite then $G \cong$~~

(b) $|G| = n$ where $n > 1$ then $G \cong (Z_n, \oplus)$

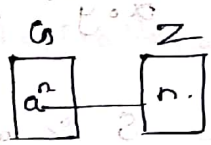
Proof:-

Let G be a cyclic group with generator 'a'

$\Rightarrow G = \{a^n / n \in Z\}$.

(a) Suppose $|G|$ is infinite.

To prove: $G \cong (Z, +)$.



Define $f : G \to Z$ by $f(a^n) = n$. $\forall a^n \in G$.

Claim: f is an isomorphism.

f is 1-1: Let $f(a^n) = f(a^m)$

$\Rightarrow n = m$

$\Rightarrow a^n = a^m$.

$\therefore f$ is 1-1.

f is onto: For any $n \in Z$, $\exists$ $a^n \in G$

such that $f(a^n) = n$.

$\therefore f$ is onto.

f is homomorphism:

$$f(a^n . a^m) = f(a^{n+m})$$

$$= n + m$$

$$= f(a^n) + f(a^m)$$

$\therefore f$ is homomorphism.

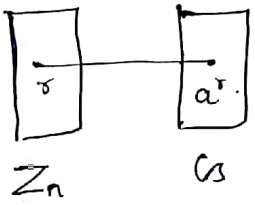
$\therefore f$ is an isomorphism. $\Rightarrow G \cong (Z, +)$.

(b) If $|G| = n$ with $n > 1$.

Then $G = \{a, a^2, a^3, \ldots, a^{n-1}, e\}$.

To prove $Z_n \cong G$.

Define $f : Z_n \to G$ by $f(r) = a^r$



(i) f is 1-1

Let $f(r) = f(s)$

$\Rightarrow a^r = a^s$

$\Rightarrow r = s$

$\therefore f$ is 1-1.

(ii) f is onto: For any $a^r \in G$, $\exists\ r \in Z_n$ with

$f(r) = a^r$. $\therefore f$ is onto.

(iii) f is homomorphism:

To prove $f(r \oplus s) = f(r) \cdot f(s)$.

Let $r \oplus s = t$.

$\Rightarrow r + s$ leaves the remainder t when it divided by n.

$\Rightarrow r + s = qn + t, \quad 0 \le t < n.$

$\Rightarrow f(r \oplus s) = f(t) = a^t \longrightarrow (1)$

Also $f(r) \cdot f(s) = a^r \cdot a^s = a^{r+s} = a^{qn+t} = a^{qn} \cdot a^t$

$= (a^n)^q \cdot a^t$

$= (e)^q \cdot a^t$

$f(r) \cdot f(s) = a^t \longrightarrow (2)$.

From (1), (2), $f(r \oplus s) = f(r) \cdot f(s)$

$\therefore f$ is isomorphism.

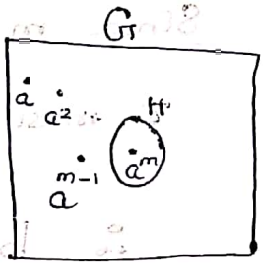
Theorem (1A) Every subgroup of a cyclic group is cyclic.

Proof: Let G be a cyclic group generated by a.

i) $\langle a \rangle = G$.

Every element of G is some powers of a.

Let H be a subgroup of G.



To prove: H is cyclic.

Let m be the least +ve integer such that $a^m \in H$.

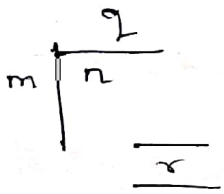
We claim that a^m is the generator of H.

It is enough to prove, every element of H is some power of a^m.

Let $b \in H$.

$\therefore b = a^n$ $\left(\because b \in G, G \text{ is cyclic}\right)$

Dividing n by m



$n = mq + r \quad ; \quad 0 \leq r < m.$

Consider $b = a^n = a^{mq+r}$

$$b = a^{mq} \cdot a^r$$

Operate $(a^{mq})^{-1}$ both sides

$$b \cdot (a^{mq})^{-1} = (a^{mq}) \cdot (a^{mq})^{-1} \cdot a^r$$

$$b \cdot (a^{mq})^{-1} = e \cdot a^r$$

$$b \cdot (a^{mq})^{-1} = a^r \longrightarrow (1)$$

We have $b, a^{mq} \in H$.

Since H is a subgroup $b.(a^{mq})^{-1} \in H$.

From ①, $a^r \in H$.

We have $0 \leq r < m$ with $a^r \in H$.

Since m is least +ve integer such that $a^m \in H$,

r must be zero.

$\therefore b = a^{mq+r} \Rightarrow b = a^{mq+0}$

$\Rightarrow b = a^{mq}$

$\Rightarrow b = (a^m)^q$

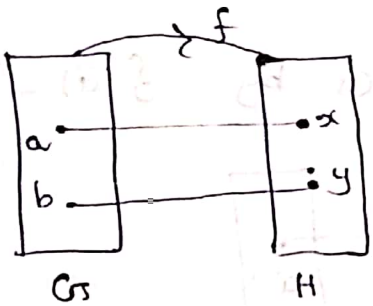
$\therefore$ Every element of H is some power of a^m.

$\Rightarrow$ H is cyclic.

Hence the proof.

Problem: Let $f: G \to H$ be a group homomorphism onto H. If G is abelian then prove H is abelian.

Soln: Given $f: G \to H$ is a homomorphism and onto.



Assume that G is abelian.

To prove: H is abelian

Let $x, y \in H$.

It is enough to prove $x \cdot y = y \cdot x$.

Since f is onto, x & y have pre-images.

$\Rightarrow x = f(a)$ & $y = f(b)$ for some $a, b \in G$.

$$x \cdot y = f(a) \cdot f(b)$$
$$= f(a \cdot b) \quad (\because f \text{ is homo})$$
$$= f(b \cdot a) \quad (\because G \text{ is abelian}, a \cdot b = b \cdot a)$$
$$= f(b) \cdot f(a)$$
$$x \cdot y = y \cdot x$$

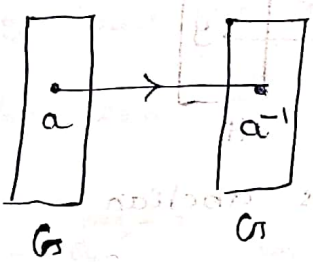
This is true for every $x, y \in H$.

$\therefore$ H is abelian.

Problem For a group G, prove that $f: G \to G$, $f(a) = a^{-1}$ is an isomorphism iff G is abelian.

Proof:- Let G be a group.

Define $f: G \to G$ by $f(a) = a^{-1}$.



Assume that $f(a) = a^{-1}$ is an isomorphism.

To prove: G is abelian

Let $a, b \in G$.

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

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

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

Formula

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

$$(b^{-1})^{-1} \cdot (a^{-1})^{-1} = (a^{-1})^{-1} \cdot (b^{-1})^{-1} \longrightarrow (1).$$

a is the inverse of a^{-1} & vice-versa

b " " b^{-1} a ".

$\therefore$ From (1), $b \cdot a = a \cdot b$.

$\therefore G$ is abelian.

Conversely assume that G is abelian.

To prove: $f(a) = a^{-1}$ is an isomorphism.

(i) f is 1–1

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

$\therefore f$ is 1–1.

(ii) f is onto

Let $a \in G$

Then $\exists\ a^{-1} \in G$ such that $f(a^{-1}) = (a^{-1})^{-1} = a$

(a) a^{-1} is the pre-image of a.

$\therefore f$ is onto.

(iii) f is homomorphism

$$f(a.b) = (a.b)^{-1}$$
$$= b^{-1}.a^{-1}$$
$$= a^{-1}.b^{-1} \quad (\because G \text{ is abelian})$$
$$= f(a).f(b)$$

$\Rightarrow f$ is homomorphism.

$\therefore f$ is an isomorphism.

Hence the proof.

Rings

Defn (Ring)
A non-empty set R with two binary operations $+$ and $\cdot$ is called a ring if it satisfies the following

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

(ii) $\cdot$ is associative.

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

(iii) Distributive law holds

Left distributive law

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

Right distributive law

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

Ring denoted by $(R, +, \cdot)$.

Defn (Commutative ring)
A ring $(R, +, \cdot)$ is commutative ring if

$$a \cdot b = b \cdot a \quad \forall a, b \in R.$$

Defn (Ring with Identity)

A ring $(R, +, \cdot)$ is called a ring with identity element if it has the identity with respect to the binary operation $\cdot$

Notes

* In a ring additive identity element called zero element. Denoted by '0'.

  Multiplicative identity element called "identity".

* A ring may and may not have identity element.

  But a ring must have zero element.

* $+$ → First binary operation

  $\cdot$ → Second binary operation

  These binary operations can be changed.

* Additive inverse of a is denoted by $-a$.

Examples

① $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.

② $(2\mathbb{Z}, +, \cdot)$ is a ring.

Also it is commutative ring.

But it has no identity element.

③ $(\mathbb{Q}, +, \cdot)$ is a commutative ring with identity

④ $(\mathbb{R}, +, \cdot)$ is a commutative ring with identity.

$\mathbb{R} \rightarrow$ Set of all real numbers.

⑤ $(\mathbb{C}, +, \cdot)$ is a commutative ring with identity

$\mathbb{C} \rightarrow$ set of all complex numbers.

⑥ Let $M_2(R)$ be the set of all 2×2 matrices with real entries.

Then $M_2(R)$ is a ring under matrix addition and matrix multiplication.

Proof:-

$$M_2(R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / \; a, b, c, d \text{ are real numbers} \right\}.$$

First binary operation $(+)$: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$

Second binary operation $(\cdot)$: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$

(i) $(M_2(R), +)$ is an abelian group.

$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is zero element.

(ii) '$\cdot$' is associative :

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \begin{bmatrix} i & j \\ k & l \end{bmatrix} \in M_2(R)$

Take $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, $C = \begin{bmatrix} i & j \\ k & l \end{bmatrix}$.

To prove

Left dist. law $A \cdot [B+C] = A \cdot B + A \cdot C$

$$A \cdot (B+C) = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right)$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix}$$

$$= \begin{bmatrix} a(e+i)+b(g+k) & a(f+j)+b(h+l) \\ c(e+i)+d(g+k) & c(f+j)+d(h+l) \end{bmatrix}$$

$$A \cdot (B+C) = \begin{bmatrix} ae+ai+bg+bk & af+aj+bh+bl \\ ce+ci+dg+dk & cf+cj+dh+dl \end{bmatrix} \longrightarrow (1)$$

$$A \cdot B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

$$A \cdot C = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} i & j \\ k & l \end{bmatrix} = \begin{bmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{bmatrix}$$

$$A \cdot B + A \cdot C = \begin{bmatrix} ae+ai+bg+bk & af+aj+bh+bl \\ ce+ci+dg+dk & cf+cj+dh+dl \end{bmatrix} \longrightarrow (2)$$

From (1), (2) $A \cdot [B+C] = [A \cdot B] + [A \cdot C]$.

Similarly, we can prove right distributive law.

$\therefore (M_2(R), +, \cdot)$ is a ring.

But it is not a commutative ring.

Since $\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}5&6\\7&8\end{pmatrix} \neq \begin{pmatrix}5&6\\7&8\end{pmatrix}\begin{pmatrix}1&2\\3&4\end{pmatrix}$.

But it has an identity element $\begin{bmatrix}1&0\\0&1\end{bmatrix}$.

∴ $(M_2(R), +, \cdot)$ is a non-commutative ring with an identity element.

Problem U.Q. Prove that $(Q, \oplus, \circ)$ is a ring on the set of all rational numbers under the binary operations

$$x \oplus y = x + y + 7$$
$$x \circ y = x + y + \left(\frac{xy}{7}\right) \quad \text{for } x, y \in Q.$$

Soln:-

To prove: $(Q, \oplus, \circ)$ is a ring

(i) **claim:** $(Q, \oplus)$ is an abelian group.

Closure property. Let $x, y \in Q$

$$x \oplus y = x + y + 7 \in Q.$$

Associate property: Let $x, y, z \in Q$

To prove: $x \oplus (y \oplus z) = (x \oplus y) \oplus z$

L.H.S $x \oplus (y \oplus z) = x \oplus (y + z + 7)$

$$= x + y + z + 7 + 7. \longrightarrow (1)$$

R.H.S $(x \oplus y) \oplus z = (x + y + 7) \oplus z$

$$= x + y + 7 + z + 7. \longrightarrow (2)$$

From (1) and (2), $x \oplus (y \oplus z) = (x \oplus y) \oplus z$

Existence of identity:

-7 is an identity element.

$-7 \in \mathbb{Q}$ such that, $x \oplus -7 = x + (-7) + 7$

$= x$.

Also $-7 \oplus x = -7 + x + 7$.

$= x$.

Existence of inverse:

Let $x \in \mathbb{Q}$, and x' be the inverse of x.

Then $x \oplus x' = x + x' + 7 = -7$. (identity element).

$\Rightarrow x' = -7 - x - 7$.

$\Rightarrow x' = -x - 14$.

For any $x \in \mathbb{Q}$, $x' = -x - 14$ is the inverse of x and $x' \in \mathbb{Q}$.

Abelian:

Let $x, y \in \mathbb{Q}$.

Then $x \oplus y = x + y + 7$

Also $y \oplus x = y + x + 7$

$= x + y + 7$.

$\therefore x \oplus y = y \oplus x \quad \forall x, y \in \mathbb{Q}$.

$\therefore (\mathbb{Q}, \oplus)$ is an abelian group.

(ii) Claim: '$\circ$' is associative.

(a) To prove $x \circ (y \circ z) = (x \circ y) \circ z$.

L.H.S $x \circ (y \circ z) = x \circ \left(y + z + \frac{yz}{7} \right)$

$= x + y + z + \frac{yz}{7} + \frac{xyz}{49} + \frac{xy}{7} + \frac{xz}{7}$.

Q.11.5

$$(x \circ y) \circ z = \left(x + y + \frac{xy}{7}\right) \circ z = x + y + \frac{xy}{7} + z + \frac{\left(x + y + \frac{xy}{7}\right) z}{7}$$

$$= x + y + \frac{xy}{7} + z + \frac{xyz}{49} + \frac{xz}{7} + \frac{yz}{7}$$

$\therefore x \circ (y \circ z) = (x \circ y) \circ z \quad \forall x, y, z \in Q$

$\therefore$ '$\circ$' is associative.

(iii) Distributive Laws

Left Distributive Law : $x \circ (y \oplus z) = (x \circ y) \oplus (x \circ z)$

$$x \circ (y + z) = x \circ (y + z + 7)$$

$$= x + y + z + 7 + \frac{x(y + z + 7)}{7}$$

$$= x + y + z + 7 + \frac{xy}{7} + \frac{xz}{7} + \frac{yx}{7}$$

$$= 2x + y + z + 7 + \frac{xy}{7} + \frac{xz}{7} \quad \longrightarrow (3)$$

$$x \circ y = x + y + \frac{xy}{7}$$

$$x \circ z = x + z + \frac{xz}{7}$$

$$(x \circ y) \oplus (x \circ z) = \left(x + y + \frac{xy}{7}\right) \oplus \left(x + z + \frac{xz}{7}\right)$$

$$= x + y + \frac{xy}{7} + x + z + \frac{xz}{7} + 7$$

$$= 2x + y + z + 7 + \frac{xy}{7} + \frac{xz}{7} \quad \longrightarrow (4)$$

From (3) & (4)

$$x \circ (y \oplus z) = (x \circ y) \oplus (x \circ z)$$

Right Distributive Law : $(x \oplus y) \circ z = (x \circ z) \oplus (y \circ z)$

$$(x \oplus y) \circ z = (x + y + 7) \circ z$$

$$= x + y + 7 + z + \frac{(x + y + 7) z}{7}$$

$$= x + y + 7 + z + \frac{xz}{7} + \frac{yz}{7} + z$$

$$= x + y + 2z + 7 + \frac{xz}{7} + \frac{yz}{7} \longrightarrow (5)$$

$$x \circ z = x + z + \frac{xz}{7}$$

$$y \circ z = y + z + \frac{yz}{7}$$

$$(x \circ z) \oplus (y \circ z) = \left(x + z + \frac{xz}{7}\right) \oplus \left(y + z + \frac{yz}{7}\right)$$

$$= x + z + \frac{xz}{7} + y + z + \frac{yz}{7} + 7$$

$$= x + y + 2z + 7 + \frac{xz}{7} + \frac{yz}{7} \longrightarrow (6)$$

From (5) & (6), $(x \oplus y) \circ z = (x \circ z) \oplus (y \circ z)$

∴ Distributive law holds.

∴ $(Q, \oplus, \circ)$ is a ring.

Defn: [Zero divisor]

Let $(R, +, \cdot)$ be a commutative ring with identity. A non-zero element $a \in R$ is said to be a zero-divisor if there exists a non-zero element $b \in R$ such that $ab = 0$ or $ba = 0$.

Examples

$(Z_{12}, \oplus, \odot)$ is a commutative ring with identity.

$\oplus \rightarrow$ addition modulo 12

$\odot \rightarrow$ multiplication modulo 12.

Here zero element is 0

3 is a zero divisor.

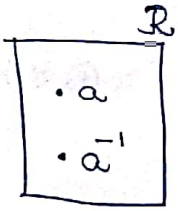
Since $3 \odot 4 = 0$

Also 2, 6, 4 are zero divisors.

Since $2 \odot 6 = 0$ and $4 \odot 3 = 0$.

Defn:- [Unit]

Let $(R, +, \cdot)$ be a commutative ring with identity. An element $a \in R$ is called a unit in R if it has a multiplicative inverse in R



Example:

$(Z_5, \oplus, \odot)$ is a commutative ring with identity.

$\oplus \rightarrow$ addition modulo 5

$\odot \rightarrow$ multiplication modulo 5

Here identity element is '1'.

Here 3 is a unit.

Since $2 \in Z_5$ such that $2 \odot 3 = 3 \odot 2 = 1$.

This means that 2 is multiplicative inverse of 3.

Also 4 is a unit.

Since $4 \odot 4 = 1$, inverse of 4 is 4.

Defn:- [Field]

A commutative ring with identity is called a Field if every non zero element has a multiplicative inverse.

Example $(Z_5, \oplus, \odot)$ is a Field.

$\oplus \rightarrow$ addition modulo 5

$\odot \rightarrow$ multiplication modulo 5

Here identity element is 1.

$Z_5 = \{0, 1, 2, 3, 4\}$.

Cayley Table for Z_5 under $\odot$

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Multiplia-Inverse of 1 is 1

Multiplicative inverse of 2 is 3

" " of 3 is 2

" " of 4 is 4.

Defn:- [Integral domain]

A commutative ring with identity having no zero divisors is called an integral domain.

Examples:

(i) $(Z, +, .)$ is an integral domain

(ii) $(Z_3, \oplus, \odot)$ is an integral domain

(iii) $(Z_6, \oplus, \odot)$ is not an integral domain.

Since 2 and 3 are zero divisors.

$2 \odot 3 = 0$.

Notes

* Every field is an integral domain.

But every integral domain need not be field.

For example, $(Z, +, .)$ is an integral domain.

But $(Z, +, .)$ is not a field.

Since 2 has no multiplicative inverse.

Defn: [Relatively prime]

A positive integer 'a' is relatively prime to 'n' if g.c.d of a and n is '1'.

g.c.d of a and n is denoted by (a, n)

Example

① 10 is relatively prime to 13.

Since g.c.d of 10 and 13 is 1.

i.e., $(10, 13) = 1$.

② 15 is relatively prime to 16.

Since $(15, 16) = 1$.

③ 2 is not relatively prime to 4

$(2, 4) = 2 \neq 1$.

Formula [Finding how many integers relatively prime to n]

Let n be given positive integer.

Aim: To find number of +ve integers $\leq n$ and relatively prime to n.

Express n as product of prime powers.

Say $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$.

Then number of +ve integers $\leq n$ and relatively prime to $n = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right)$

This is denoted by $\phi(n)$

$\therefore \phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_k}\right)$

Examples

① Find how many +ve integers are ≤ 100 and relatively prime to 100.

Soln :-

$$\begin{array}{r|l} 2 & 100 \\ 2 & 50 \\ 5 & 25 \\ & 5 \end{array}$$

$\therefore 100 = 2 \times 2 \times 5 \times 5$

$100 = 2^2 \times 5^2$.

The number of +ve integers ≤ 100 and relatively prime to 100 $= \phi(100)$

$\phi(100) = 100 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$= 100 \times 1/2 \times 4/5$

$= 40.$

∴ There are 40 integers which are ≤ 100 and relatively prime to 100.

(2) How many +ve integers are ≤ 23 and relatively prime to 23.

Soln:-

23 is a prime number.

∴ $23 = 23^1$.

∴ $\phi(23) = 23 \times (1 - 1/23)$

$= 23 \times \frac{22}{23}$

$= 22.$

Notes

* If p is a prime number then

$\phi(p) = (p-1)$.

Important Result:

Let $(Z_n, \oplus, \odot)$ be a ring.

$\oplus \rightarrow$ addition modulo n

$\odot \rightarrow$ multiplication modulo n.

Then the number of elements in Z_n which have multiplicative inverse is $\phi(n)$.

(or) The number of units in Z_n is $\phi(n)$.

Example: Compute how many elements in $(Z_{12}, \oplus, \odot)$ are units and list out them.

Soln:-

$$Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

The number of units in Z_{12} is $\phi(12)$.

$$\begin{array}{r|l} 2 & 12 \\ \hline 2 & 6 \\ \hline & 3 \end{array}$$

$\therefore 12 = 2 \times 2 \times 3$

$= 2^2 \times 3.$

$\therefore \phi(12) = 12 \times (1 - 1/2) \times (1 - 1/3)$

$= 12 \times 1/2 \times 2/3$

$\phi(12) = 4.$

$(1,12) = 1$.

$(5,12) = 1$

$(7,12) = 1$.

$(11,12) = 1$.

$\therefore$ 1, 5, 7, 11 are units.

Verification :-

Cayley Table Z_{12} under $\odot$

$\odot$	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11
2	2	4	6	8	10	0	2	4	6	8	10
3	3	6	9	0	3	6	9	0	3	6	9
4	4	8	0	4	8	0	4	8	0	4	8
5	5	10	3	8	1	6	11	4	9	2	7
6	6	0	6	0	6	0	6	0	6	0	6
7	7	2	9	4	11	6	1	8	3	10	5
8	8	4	0	8	4	0	8	4	0	8	4
9	9	6	3	0	9	6	3	0	9	6	3
10	10	8	6	4	2	0	10	8	6	4	2
11	11	10	9	8	7	6	5	4	3	2	1

Multiplicative inverse of 1 is 1

" " 5 is 5

" " 7 is 7.

" " 11 is 11.

$\therefore$ 1, 5, 7, 11 are units in $(Z_{12}, \oplus, \odot)$

Theorem ① Let $(R, +, \cdot)$ be a commutative ring with identity. Then R is an integral domain iff for all $a, b, c \in R$ where $a \neq 0$, $ab = ac$ implies that $b = c$.

(OR)

A commutative ring with identity is an integral domain iff the cancellation law of multiplication holds in R.

Proof:

Assume that R is an integral domain

Claim: For all $a, b, c \in R$ where $a \neq 0$

$$ab = ac \Rightarrow b = c.$$

Let $a, b, c \in R$ where $a \neq 0$.

Now $ab = ac$

$\Rightarrow ab - ac = 0$

$\Rightarrow a(b - c) = 0$

Since R is an integral domain, R has no zero divisor.

$\therefore$ Either $a = 0$ (or) $b - c = 0$.

But $a \neq 0$.

$\therefore b - c = 0$

$\Rightarrow b = c$.

$\therefore$ Cancellation law holds good in R.

Conversely assume that for all $a, b, c \in R$ with $a \neq 0$, $ab = ac \Rightarrow b = c$.

Claim: R is an integral domain.

i) To prove R has no zero divisor.

ii) To prove $ab = 0 \Rightarrow a = 0$ (or) $b = 0$.

Let $ab = 0$ with $a \neq 0$.

$ab = a \cdot 0$ $(\because a \cdot 0 = 0)$

Using cancellation law, $b = 0$.

$\therefore$ R is an integral domain.

Theorem ② Let $(F, +, \cdot)$ be a field. Then it is an integral domain.

Proof:-

Let $(F, +, \cdot)$ be a field.

Claim: $(F, +, \cdot)$ is an integral domain.

i) To prove F has no zero divisor.

Let $ab = 0$ with $a \neq 0$.

Since $a \neq 0$, $a^{-1} \in F$. $(\because F$ is a field$)$.

Now $ab = 0$.

Operate a^{-1} on both sides

$a^{-1}ab = a^{-1}0$

$\Rightarrow eb = 0$ where e is identity

$\Rightarrow b = 0$.

$\therefore$ R is an integral domain.

Theorem ③ Any finite integral domain is a field.

Proof: Let $(R, +, \cdot)$ be finite integral domain.

$\therefore$ By defn, R is a commutative ring with identity.

$\therefore R = \{0, 1, a_1, a_2, \ldots a_n\}$.

($\because$ R is finite, 1 = identity, 0 = zero element).

Let $a \in R$ with $a \neq 0$.

Then $\{a1, aa_1, aa_2, \ldots, aa_n\}$ is a set of distinct elements and none of them is zero.

Hence $aa_i = 1$ for some $a_i \in R$

Also $a_i a = 1$

$\therefore$ $aa_i = a_i a = 1$.

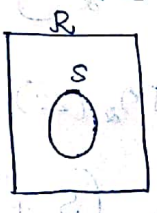
$\Rightarrow$ a_i is multiplicative inverse of a

$\therefore$ Every non-zero element has a multiplicative inverse in R.

$\therefore$ $(R, +, \cdot)$ is a field.

Subring : Let $(R, +, \cdot)$ be a ring.

A non-empty subset S of R is called a subring of R if $(S, +, \cdot)$ is a ring



Subring Test :

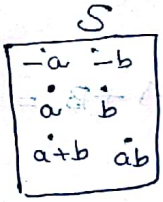
Given a ring $(R, +, \cdot)$

Let S be a non-empty subset of R

Then S is a subring of R if it satisfies the following

(i) For all $a, b \in S$, $a+b \in S$ and $ab \in S$

(ii) For all $a \in S$, $-a \in S$.



Examples

(i) $(2\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Z}, +, \cdot)$

(ii) $(\mathbb{Q}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$

$\mathbb{Q} \rightarrow$ set of all rationals

$\mathbb{R} \rightarrow$ set of all real numbers.

(iii) $(\mathbb{R}, +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$

$\mathbb{C} \rightarrow$ set of all complex numbers.

$\mathbb{R} \rightarrow$ set of all real numbers.

Problem: Let $M_2(\mathbb{Z})$ be the set of all 2×2 matrices with integer entries.

Let $S = \left\{ \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} / x, y \in \mathbb{Z} \right\}$.

be the subset of $M_2(\mathbb{Z})$.

(For example $\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \in S$, $\begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} \notin S$)

Then prove that $(S, +, \cdot)$ is a subring of $(M_2(\mathbb{Z}), +, \cdot)$

Soln:-

S

$-A$	$-B$
A	B
$A+B$	AB

Subring Test:

(i) Let $A = \begin{bmatrix} x_1 & x_1+y_1 \\ x_1+y_1 & x_1 \end{bmatrix}$, $B = \begin{bmatrix} x_2 & x_2+y_2 \\ x_2+y_2 & x_2 \end{bmatrix} \in S$

$$A+B = \begin{bmatrix} x_1+x_2 & x_1+y_1+x_2+y_2 \\ x_1+y_1+x_2+y_2 & x_1+x_2 \end{bmatrix}$$

$$= \begin{bmatrix} x_1+x_2 & x_1+x_2+y_1+y_2 \\ x_1+x_2+y_1+y_2 & x_1+x_2 \end{bmatrix}$$

$A+B \in S$.

$$AB = \begin{bmatrix} x_1 & x_1+y_1 \\ x_1+y_1 & x_1 \end{bmatrix} \cdot \begin{bmatrix} x_2 & x_2+y_2 \\ x_2+y_2 & x_2 \end{bmatrix}$$

$$= \begin{bmatrix} x_1x_2 + x_1x_2 + x_1y_2 + x_2y_1 + y_1y_2 & x_1x_2 + x_1y_2 + x_1x_2 + x_2y \\ x_1x_2 + x_2y_1 + x_1x_2 + x_1y_2 & x_1x_2 + x_1y_2 + x_2y_1 + y_1y_2 \end{bmatrix}$$

$AB \in S$.

(ii) Let $A = \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}$

$$-A = \begin{bmatrix} -x & -(x+y) \\ -(x+y) & -x \end{bmatrix}$$

$\therefore -A \in S.$

$\therefore (S, +, \cdot)$ is a subring of $(M_2(\mathbb{Z}), +, \cdot)$

Homework

① Let $R = M_2(\mathbb{Z})$ and S be the subset of R where $S = \left\{ \begin{bmatrix} x & x-y \\ x-y & y \end{bmatrix} / x, y \in \mathbb{Z} \right\}$.

Prove S is a subring of R.

Integers modulo n

Defn [congruence]

Let n be any positive integer and $n > 1$.

We say that "a is congruent to b modulo n" and we write $a \equiv b \pmod{n}$ if n divides $(a-b)$

Examples

① $17 \equiv 2 \pmod{5}$

Because 5 divides $(17-2)$.

② $-7 \equiv -49 \pmod{6}$

Since 6 divides $-7-(-49)$

i.e. 6 divides 42.

③ $11 \equiv -5 \pmod{8}$

Since 8 divides $11-(-5)$

8 divides 16.

Notes Suppose a, b, n are +ve integers.

* If $a \equiv b \pmod{n}$ then 'a' leaves the remainder 'b' when a is divided by n.

If we subtract the remainder 'b' from 'a' then the resulting number is the multiple of n.

i.e. $a-b$ = multiple of n.

For example,

$$17 \equiv 2 \pmod 5$$

$\therefore$ 17 leaves the remainder 2 when 17 is divided by 5.

Also $17 - 2 = 3(5)$.

* Suppose any one of a and b is -ve

Then $a \equiv b \pmod n$ means that

$a - b$ = multiple of n.

For example; $-7 \equiv -49 \pmod 6$

Here $-7 - (-49)$ = multiple of 6.

i.e., $42 = 7(6)$.

* Congruence will help to find the inverse of any unit in $(Z_n, \oplus, \odot)$.

Theorem ④ $(Z_n, \oplus, \odot)$ is a field iff n is prime.

Proof:- We know that $(Z_n, \oplus, \odot)$ is a commutative ring with identity.

Assume that n is prime.

Claim: Z_n is a field.

Let a be any non-zero element in Z_n.

To prove: $a^{-1} \in Z_n$.

Now g.c.d $(a, n) = 1$.

> **Result** If g.c.d $(x, y) = m$ then $\exists$ s, t such that $m = sx + ty$.
> s, t are integers.

$\therefore \exists$ integers s, t such that

$$1 = as + tn.$$

~~$\Rightarrow as + tn = 1$.~~

$$\Rightarrow -tn = as - 1.$$

$\Rightarrow$ multiple of n $= as - 1$.

$$\Rightarrow as \equiv 1 \pmod{n}$$

$$\Rightarrow s = a^{-1} \in Z_n.$$

$\therefore Z_n$ is a field.

Conversely assume that Z_n is a field.

$\Rightarrow Z_n$ is an integral domain.

Claim: n is prime

Suppose n is not a prime number.

Then $n = kl$ where $1 < k, l < n$.

But $k, l \in Z_n$.

$k \cdot l = n$ = zero element

$\Rightarrow$ k, l are zero divisors

$\Rightarrow Z_n$ is not an integral domain.

Which is a $\Rightarrow\Leftarrow$ to Z_n is an integral domain.

$\therefore$ n is a prime number.

H/P.

Theorem ⑤ In $(Z_n, \oplus, \odot)$ a is a unit iff

g.c.d $(a, n) = 1$.

Proof:-

Assume that g.c.d $(a, n) = 1$.

Claim: a is a unit.

Since g.c.d $(a, n) = 1$, $\exists$ Integers s and t

such that $1 = as + tn$.

$\Rightarrow -tn = as - 1$.

$\Rightarrow$ multiple of $n = as - 1$.

$\Rightarrow as \equiv 1 \pmod{n}$

$\Rightarrow s = a^{-1} \in Z_n$.

$\therefore$ a is a unit.

Conversely assume that a is a unit.

$\Rightarrow a^{-1} \in Z_n$.

Claim : $g.c.d(a,n) = 1$.

Let $a^{-1} = s$.

$\Rightarrow as = 1$

$\Rightarrow as \equiv 1 \pmod{n}$

$\Rightarrow as - 1 =$ multiple of n.

$\Rightarrow as - 1 = tn$. for some $t \in Z$.

$\Rightarrow as = 1 + tn$.

$\Rightarrow 1 = as - tn$.

$\Rightarrow 1 = as + n(-t)$.

$\Rightarrow g.c.d(a,n) = 1$.

H/p.

Procedure for finding inverse in Z_n.

To find a^{-1}

Step(1) Check if g.c.d $(a, n) = 1$.

If g.c.d $(a, n) = 1$, $a^{-1} \in Z_n$.

Otherwise not exists.

Step(2) Write g.c.d $(a, n) = 1$ as a linear combination of a and n.

Step(3) Suppose $1 = as + tn$.

Then $as - 1 = -tn$

$as - 1 =$ multiple of n.

$\Rightarrow as \equiv 1 \pmod{n}$.

Step(4) We have $as \equiv 1 \pmod{n}$.

Case (i) Suppose s is +ve, $a^{-1} = s$.

Case (ii) Suppose s is -ve, $a^{-1} = s + n$

Problem Find $(25)^{-1}$ in Z_{72}.

Soln. We know that $(Z_{72}, \oplus, \odot)$ is a commutative ring with identity.

Aim: To find multiplicative inverse of 25.

Now g.c.d $(25, 72) = 1$.

$\therefore$ By thm (5), $(25)^{-1}$ exists in Z_{72}.

Divide 72 by 25

$72 = 2(25) + 22$ → ① , $0 < 22 < 25$.

Divide 25 by 22.

$25 = 1(22) + 3$ → ② , $0 < 3 < 22$.

Divide 22 by 3.

$22 = 7(3) + 1$ → ③ , $0 < 1 < 3$.

Divide 3 by 1.

$3 = 3(1) + 0$.

The last non zero remainder is 1.

$1 = g.c.d\ (25, 72)$.

From ③, $1 = 22 - 7(3)$.

$= 22 - 7(25 - 22)$ (using ②)

~~$= 22 - 7(72 - 2(25))$~~

~~$= 22 - 7(72 - 50)$~~

~~$= 22 - 7(22)$~~

~~$= 22$~~

$= 22 - 7(25) + 7(22)$

$= 8(22) - 7(25)$

$= 8(72 - 2(25)) - 7(25)$

$= 8(72) - 16(25) - 7(25)$

$= 8(72) - 23(25)$

$\Rightarrow -23(25) - 1 = 8(72)$

$\Rightarrow -23(25) - 1 =$ multiple of 72

$\Rightarrow -23(25) \equiv 1 \pmod{72}$.

$-23(25) \equiv 1 \pmod{72}$.

$\Rightarrow$ inverse of 25 is $(-23+72)$.

$\Rightarrow$ inverse of 25 is 49.

Problem ②

U.Q. : Find $(100)^{-1}$ in Z_{1009}.

Soln. We know that $(Z_{1009}, \oplus, \odot)$ is a Commutative ring with identity.

Aim: To find $(100)^{-1}$

Since g.c.d $(100, 1009) = 1$, $(100)^{-1} \in Z_{1009}$.

Divide 1009 by 100.

$1009 = 10(100) + 9 \rightarrow ①$, $0 < 9 < 100$.

Divide 100 by 9

$100 = 11(9) + 1 \rightarrow ②$, $0 < 1 < 9$.

Divide 9 by 1

$9 = 9(1) + 0$.

The last non-zero remainder is 1.

$\therefore$ g.c.d $(100, 1009) = 1$.

$\therefore \quad 1 = 100 - 11(9)$ (using ②)

$= 100 - 11\left[1009 - 10(100)\right]$

$= 100 - 11(1009) + 110(100)$

$1 = 111(100) - 11(1009)$

$\Rightarrow \quad 11(1009) = 111(100) - 1$

$\Rightarrow$ multiple of $1009 = 111(100) - 1$.

$\Rightarrow \quad 111(100) \equiv 1 \pmod{1009}$

$\Rightarrow$ 111 is inverse of 100.

Homework

① Find $(98)^{-1}$ in Z_{101}.

② Find $(17)^{-1}$ in Z_{625}.

Homomorphism

Defn Let $(R,+,\cdot)$ and $(S,\oplus,\odot)$ be two rings.

The function $f:(R,+,\cdot)\longrightarrow(S,\oplus,\odot)$ is a homomorphism if it satisfies the following.

(i) $f(x+y) = f(x)\oplus f(y)$

(ii) $f(x\cdot y) = f(x)\odot f(y) \quad \forall\, x,y \in R$.

Defn [Isomorphism]

A homomorphism $f:(R,+,\cdot)\to(S,\oplus,\odot)$ is an isomorphism if it is 1-1 & onto.

Example

① Let $\mathbb{C}$ be the ring of complex numbers.

a) $(\mathbb{C},+,\cdot)$ is a ring.

Let S be the set of all matrices of the form

$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where $a,b \in R$.

b) $S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \Big/ \; a,b \text{ are real numbers} \right\}$.

S is a ring under matrix addition and matrix multiplication.

Define $f: \mathbb{C} \to S$ by $f(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

Then f is an isomorphism.

Proof:-

$f : C \to S$ by $f(a+ib) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

Let $x = a_1 + ib_1$

$y = a_2 + ib_2 \in C$.

(i) claim: $f(x+y) = f(x) + f(y)$.

L.H.S $f(x+y) = f[(a_1+ib_1) + (a_2+ib_2)]$

$= f[(a_1+a_2) + i(b_1+b_2)]$

$= \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ -(b_1+b_2) & a_1+a_2 \end{bmatrix}$

$= \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$

$= f(x) + f(y)$

(ii) claim $f(x.y) = f(x) \cdot f(y)$

$f(x.y) = f\left[\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}\right]$

$= f\begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -a_2b_1 - a_1b_2 & -b_1b_2 + a_1a_2 \end{bmatrix}$

L.H.S $f(x.y) = f[(a_1+ib_1)\cdot(a_2+ib_2)]$

$= f[(a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)]$

$f(x.y) = \begin{bmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix}$ → (1)

$$f(x) = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \quad ; f(y) = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$$

$$f(x) \cdot f(y) = \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 - b_1 b_2 & a_1 b_2 + a_2 b_1 \\ -a_2 b_1 - a_1 b_2 & a_1 a_2 - b_1 b_2 \end{bmatrix} \longrightarrow (2)$$

From (1) & (2), $f(x.y) = f(x) \cdot f(y)$

$\therefore$ f is an homomorphism.

Claim f is 1-1.

Let $f(x) = f(y)$

$$\Rightarrow \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} = \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix}$$

$$\Rightarrow a_1 = a_2 \ \& \ b_1 = b_2$$

$$\Rightarrow a_1 + ib_1 = a_2 + ib_2$$

$$\Rightarrow x = y.$$

$\therefore$ f is 1-1.

Claim: f is onto.

For any $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in S$, $\exists$ $a+ib \in C$ such that

$$f[a+ib] = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

$\therefore$ f is onto.

Theorem ⑥: Let $f : (R, +, \cdot) \to (S, \oplus, \odot)$ be a ring homomorphism, then

ⓐ $f(0_R) = f(0_S)$.

where $0_R \to$ zero element in R

$0_S \to$ zero element in S

ⓑ $f(-a) = -f(a)$ for all $a \in R$.

ⓒ $f(na) = n f(a)$ $\forall\ a \in R, n \in Z$.

ⓓ $f(a^n) = [f(a)]^n$ for all $a \in R$, $n \in Z^+$

ⓔ if A is a subring of R, it follows that $f(A)$ is a subring of S.

Proof:-

ⓐ **Claim** $f(0_R) = f(0_S)$.

$0_S + f(0_R) = f(0_R)$ ($\because 0_S$ is zero element in S)

$= f(0_R + 0_R)$ ($\because 0_R + 0_R = 0_R$)

$0_S + f(0_R) = f(0_R) + f(0_R)$ ($\because f$ is homo)

Using right cancellation law, $0_S = f(0_R)$.

ⓑ **Claim**: $f(-a) = -f(a)$. $\forall a \in R$.

From ⓐ $f(0_R) = 0_S$

$f(a - a) = 0_S$ ($\because a - a = 0_R$).

$f(a + (-a)) = 0_S$.

$f(a) \oplus f(-a) = 0_S$.

$\Rightarrow f(-a)$ is additive inverse of $f(a)$.

But additive inverse of $f(a)$ is $-f(a)$

$\therefore f(-a) = -f(a)$.

(c) $f(na) = n f(a)$. $\forall a \in R, n \in Z$.

Let $a \in R$ and $n \in Z$.

$$f(na) = f(a+a+\cdots+a) \quad (n \text{ times})$$

$$= f(a) \oplus f(a) \oplus \cdots + f(a) \quad (n \text{ times})$$

$$= n f(a).$$

(d) $f(a^n) = [f(a)]^n$ $\forall a \in R, n \in Z^+$.

Let $a \in R$ and n be any +ve integer.

$$f(a^n) = f(a.a\ldots a)$$

$$= f(a) \odot f(a) \odot \cdots \odot f(a) \quad (n \text{ times})$$

$$= [f(a)]^n.$$

(e). Let A be a subring of R.

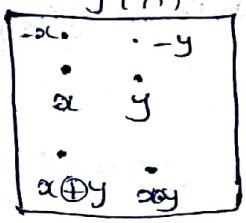
Claim $f(A)$ is a subring of S.

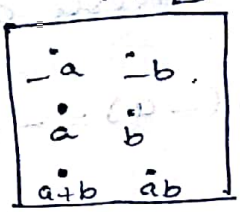
$$f(A) = \{ f(a) / a \in A \}.$$

Let $x, y \in f(A)$.

$\Rightarrow x = f(a)$

$y = f(b)$ for some $a, b \in A$.





Claim: $x \oplus y \in f(A)$.

$$x \oplus y = f(a) \oplus f(b)$$
$$= f(a+b)$$

$\therefore x \oplus y \in f(A)$.

Claim: $x \odot y \in f(A)$.

$$x \odot y = f(a) \odot f(b)$$
$$= f(ab)$$

$\therefore x \odot y \in f(A)$.

Let $x \in f(A)$

$\Rightarrow x = f(a)$ for some a.

$$-x = -f(a)$$
$$= f(-a)$$

$\Rightarrow -x \in f(A)$.

$\therefore$ By subring test, $f(A)$ is a subring of S.