# MA8551, ALGEBRA AND NUMBER THEORY

## UNIT- I

## Groups And Rings

### Groups:

### Definition:

A non-empty set $G$ with a binary operation $*$, ie., $(G, *)$ is called a group, if $*$ satisfies the following conditions.

(i) closure : For all $a, b \in G$, then $a * b \in G$

(ii) Associative : For all $a, b, c \in G$, we have

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

(iii) Identity : There exists an element $e \in G$ called the identity element such that $a * e = e * a = a$, for all $a \in G$.

(iv) Inverse : There exists an element $a^{-1} \in G$ called the inverse of 'a' such that

$$a * a^{-1} = a^{-1} * a = e \text{ for all } a \in G.$$

### Abelian group (or) commutative :

In a group $(G, *)$, if $a * b = b * a$ for all $a, b \in G$ then the group $(G, *)$ is called an abelian group, otherwise $(G, *)$ is called non-abelian group.

Ex $2 * 3 = 3 * 2$

EX : $(Z, +)$ is an abelian group.

## Order of a group:

The number of elements in a group on $G$ is called the order of the group and it is denoted by $O(G)$ (or) $|G|$ Ex: $G = \{1, 2, 3, 4, 5\}$ $O(G) = 5$

EX: If $G$ has $n$ elements, then $O(G) = n$

## Finite and Infinite group:

If $O(G)$ is finite, then $G$ is called a finite group. $G = \{1, 2, 3\}$

If $O(G)$ is infinite, then $G$ is called an infinite group. $G = \{1, 2, 3, 4, \ldots \infty\}$.

NOTE:

1. $N$ = the set of all positive integers $= \{1, 2, 3, \ldots\}$

whole Numbers $= 0, 1, 2, 3, 4, \ldots\ldots$

$N$ = Natural numbers $= 1, 2, 3, 4, \ldots\ldots$

2. $Z$ = the set of all integers $= \{\cdots, -2, -1, 0, 1, 2, 3, \ldots\}$

3. $Q$ = the set of all rational numbers $= \left\{ \frac{p}{q} \,\middle|\, p, q \in Z,\ q \neq 0 \right\} = \left\{\frac{1}{2}, \frac{2}{3}, \frac{5}{7}, , , \right\}$

Irrational $= \{\sqrt{2}, \sqrt{3}, \pi \ldots\}$

4. $R$ = the set of all real numbers $= \{\cdots -1.5, -1, -0.5\}$

5. $C$ = the set of all complex numbers. $= \{a + ib \mid a, b \in R\}$

6. $(Z, +)$, $(Q, +)$, $(R, +)$ and $(C, +)$ are group or Abelian.

7. $(N, +)$, $(Z, *)$, $(Q, *)$, $(R, *)$, $(C, *)$ are group or Abelian.

Example:

1. Show that set R with the usual addition as a binary operation is an abelian group.

Solution: Given : $(R, +)$, Let $a, b, c \in R$.

(i) Closure : $a + b \in R$

(ii) Associative : $(a+b)+c = a+(b+c)$

(iii) Identity : Since '0' $\in R$ we have $a+0 = 0+a = a$

(iv) Inverse : For $a \in R$, we have $-a \in R$ such that,

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

$\therefore$ The inverse of $a$ is $-a$.

(v) Commutative :

$a + b = b + a$ for all $a, b \in R$

$\therefore (R, +)$ is an abelian group

Since R contains infinite number of elements, $\therefore$ $(R, +)$ is an infinite abelian group.

2. Show that set R with the usual Multiplication as a binary operation is an abelian group.

5. Why $(z, *)$ is not a group?

Solution:

$(z, *)$ is not a group under usual multiplication. Since there is no multiplicative inverse in $z$. [ The multiplicative inverse of 'a' is $\frac{1}{a}$ which is not in $z$ ].

hold.

# Elementary properties of a Group:

Theorem: 1

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

(i) Identity element is unique.

(ii) For each $a \in G$, inverse is unique.

Proof: Given $(G, *)$ is a group

(i) Let $e$ and $e'$ be two identity elements of $G$.

$$e * e' = e' * e = e \quad [\because e' \text{ identity}]$$

$$e' * e = e * e' = e' \quad [\because e \text{ identity}]$$

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

Hence, the identity element is unique.

(ii) Let $e$ be the identity element of $G$.

Let $a \in G$ be any element.

Suppose $a'$ and $a''$ are two inverse of $a$,

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

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

Now, 
$$\begin{aligned} a' &= a' * e \\ &= a' * (a * a'') \\ &= (a' * a) * a'' \\ &= e * a'' \\ a' &= a'' \end{aligned}$$

Hence, the inverse is unique.

Theorem: 2

In a group $(G, *)$ the Cancellation laws hold.

(i) $a * b = a * c \Rightarrow b = c$ [Left Cancellation law]

(ii) $b * a = c * a \Rightarrow b = c$ [Right Cancellation law].

Proof: Given $(G, *)$ is a group.

Let $e$ be the identity element of $G$.

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

Let $a^{-1}$ be the inverse of $a$.

Premultiplying by $a^{-1}$, weget,

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

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

$$e * b = e * c$$

$$b = c$$ which is called L.C.Law.

(ii) Given: $b * a = c * a$ [Post multiplying by $a^{-1}$]

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

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

$$b * e = c * e$$

$$b = c$$

which is Called Right Cancellation Law.

Theorem: 5

In a group $(G,*)$ the equation $a *$

and $y * a = b$ have unique solutions with unk

$x$ and $y$ as $x = a^{-1} * b$, $y = b * a^{-1}$, where $a, b \in G$.

Proof: Given $(G,*)$ is a group.

Let $e$ be the identity element of $G$ and $a^{-1}$ be the inverse of $a$.

Given: $a * x = b$

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

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

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

$$x = a^{-1} * b \in G \text{ is a Solution.}$$

Now prove the uniqueness.

Suppose $x_1, x_2 \in G$ be two solutions of $a * x = b$

then $a * x_1 = b$ and $a * x_2 = b$

$$a * x_1 = a * x_2$$

$$x_1 = x_2 \qquad [\text{by left. c. Law}]$$

Hence the solution is unique and the unique solution is $x = a^{-1} * b$

Illy, Given: $y * a = b$

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

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

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

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

$$y = b * a^{-1} \in G \text{ is a Solution.}$$

Now prove the uniqueness.

Let $y_1, y_2$ be too solutions of $y * a = b$

$$y_1 * a = b \text{ and } y_2 * a = b$$

$$y_1 * a = y_2 * a$$

$$y_1 = y_2$$

Hence the solution is unique and the unique solution is $y = b * a^{-1}$.

Theorem: 4

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

Then (i) For each $a \in G$, $(a^{-1})^{-1} = a$

(ii) For all $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof: Given: $(G, *)$

(i) Let $a \in G$,

Then $a^{-1}$ is the inverse of $a$ and $(a^{-1})^{-1}$ is the inverse of $a^{-1}$

$$\therefore \; a * a^{-1} = a^{-1} * a = e$$

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

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

$$a = (a^{-1})^{-1} \quad [\text{by L.C.L}]$$

(ii) Let $a, b \in G$.

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

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

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

$$= e$$

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

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

$= b^{-1} * b$

$= e$

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

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

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

Problems under group and Abelian group:

1. Show that the set $G = \{1, -1, i, -i\}$ consisting of the 4th roots of unity is a commutative group under multiplication.

Solution: Given $G = \{1, -1, i, -i\}$

Consider the multiplication (Cayley Table).

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

(i) closure: All the elements in this table belongs to G. Hence G is closed.

(ii) Associativity: $1(-1 \cdot i) = (1 \cdot -1) \cdot i$
$= -i \in G$

Hence G is Associative.

(iii) Identity: $1 \cdot 1 = 1$, $-1 \cdot 1 = -1$, $i \cdot 1 = i$, $-i \cdot 1 = -i$

$\therefore$ 1 is the identity element.

(iv) Inverse: Inverse of 1 is 1, Inverse of -1 is -1

Inverse of $i$ is $-i$, Inverse of $-i$ is $i$

Hence $(G, *)$ is a group.

(v) commutative: $1 * -1 = -1 * 1 = -1 \in G$

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

2. verify that set $S = \{-1, 1\}$ is a group or not.
(a) under multiplication (b) under addition.

Solution:

Given : $S = \{-1, 1\}$

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

a) under multiplication:

i) closure property:

$$-1 \cdot 1 = -1 \in S$$
$$1 \cdot -1 = -1 \in S$$

$\therefore$ S is closed.

ii) Associative property:

since there are only two elements in S, the associative property is meaningless.

iii) Existence of identity:

The multiplicative identity $1 \in S$ $[\because ae = ea = a]$

ie., $e = 1$.

iv) Existence of inverse:

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

The inverse of -1 is -1

The inverse of 1 is 1.

which shows that each element has its own inverse.
Hence, S is a group under multiplication.

b) under addition:

i) Closure property:

$$-1 + 1 = 0 \notin S$$

$\therefore$ S is not closed under addition.

$\therefore$ S is not a group under addition.

Ex:

3 verify that the set $= \{-1,0,1\}$ is a group.
* not under addition. [Ans: S is a group]

4. verify that set $= \{10n / n \in z\}$ under addition is a group (or) not.

Solution: Given: $S = \{10n / n \in z\}$

(i) closure property:

Let $n, m \in \mathbb{Z}$

$10n + 10m = 10(m+n) \in S$ since $m+n \in \mathbb{Z}$

$\therefore$ S is closed under addition.

(ii) Associative property:

Let $n, m, p \in \mathbb{Z}$

$$\begin{aligned} 10n + (10m + 10p) &= 10n + 10(m+p) \\ &= 10[n + (m+p)] \\ &= 10[(n+m)+p] \\ &= (10n + 10m) + 10p \end{aligned}$$

Thus S is associative under addition.

(iii) Existence of identity:

The additive identity $0 \in S$

ie, $e = 0 \in S$

$10n + 0 = 0 + 10n = 10n$, since $0 \in \mathbb{Z}$

(iv) Existence of inverse:

Let $k \in \mathbb{Z}$ be the inverse of $10n$

$\therefore 10n + k = 0$ [$\because 0$ is identity of $S$]

$k = 0 - 10n$

$= -10n$

$= 10(-n) \in S$

Hence, $S$ is a group under addition.

AU-2015 5. Show that $M_2$ the set of all $2\times2$ non-singular Matrices over $R$ is a group under usual Matrix Multiplication. Is it abelian?

Solution: Given: $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix}, a,b,c,d \in R \text{ and } ad-bc \neq 0 \right\}$

To prove $(M_2, *)$ is a group.

1. Closure: Let $A, B \in M_2$ then $|A| \neq 0$, $|B| \neq 0$ and $AB$ is a $2\times2$ Matrix.

Then $|AB| = |A||B| \neq 0$

$\therefore AB \in M_2$

So $M_2$ is closed.

2. Associative: We know that Matrix multiplication is associative and hence it is true for $M_2$.

i.e., $A(BC) = (AB)C \quad \forall A, B, C \in M_2$.

$\therefore M_2$ is Associative.

3. Identity: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M_2$ such that,

$AI = IA = A \; \forall \; A \in M_2$

$\therefore$ I is the identity element in $M_2$.

4. Inverse: Let $A \in M_2$ then $|A| \neq 0$ and $A^{-1}$ exists,

$$A^{-1} = \frac{\text{adj} A}{|A|}$$

So inverse exists for every element in $M_2$.

$\therefore (M_2, *)$ is a group

But Matrix multiplication is not commutative.

ie, $AB \neq BA$

$\therefore (M_2, *)$ is not an abelian group.

AU-2007, 2016.

6. Show that the set of all non-zero real numbers is an abelian group under the operation $*$ defined by $a * b = \frac{ab}{2}$.

① SM

Solution: Let G be the set of all non-zero real number

$\therefore G = R - \{0\}$, where R is the set of real numbers.

Given $(G, *)$ is defined by $a * b = \frac{ab}{2}$, $\forall \; a, b \in G$.

1. closure: $a * b = \frac{ab}{2}$.

where a and b are non zero real numbers

so $\frac{ab}{2}$ is non zero real number.

$\therefore \frac{ab}{2} \in G \Rightarrow a * b \in G \; \forall \; a, b \in G$

$\therefore$ G is closed.

2) Associativity: For any $a, b, c \in G$.

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

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

$$\therefore\ a * (b * c) = (a * b) * c \quad \forall\ a, b, c \in G.$$

3) Identity: Suppose $e \in G$ be the identity,

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

$$\Rightarrow \frac{ae}{2} = a \quad \Rightarrow \frac{e}{2} = 1$$

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

4) Inverse: Let $a$ be any element of $G$.

Suppose $a^{-1}$ is its inverse then

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

$$\frac{a a^{-1}}{2} = 2 \quad \Rightarrow a a^{-1} = 4$$

$$\Rightarrow a^{-1} = \frac{4}{a} \in G.$$

Inverse of $a$ is $\frac{4}{a}$.

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

5) commutative: Let $a, b$ be any two elements of $G$.

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

$$= b * a$$

$$a * b = b * a$$

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

7. If $G = \{1, \omega, \omega^2\}$ is the set of cube roots of unity, the prove that $G$ is group under Multiplicab,

Solution: Given : $G = \{1, \omega, \omega^2\}$ and $\omega^3 = 1$.

The Cayley Table is,

| $*$ | $1$ | $\omega$ | $\omega^2$ |
|---|---|---|---|
| $1$ | $1$ | $\omega$ | $\omega^2$ |
| $\omega$ | $\omega$ | $\omega^2$ | $1$ |
| $\omega^2$ | $\omega^2$ | $1$ | $\omega$ |

1. closure :

The body of the table contains all the elements of $G$ only. $\therefore$ $G$ is closed.

2. Associative :

$$(1 * \omega) * \omega^2 = 1 * (\omega * \omega^2) = \omega^3 = 1.$$

3. Identity : wehave,

$$1 * 1 = 1$$
$$\omega * 1 = \omega$$
$$\omega^2 * 1 = \omega^2$$

$\therefore$ 1 is the identity element of $G$.

4. Inverse : $1 * 1 = 1$ $\therefore$ The inverse of 1 is 1

$\omega * \omega^2 = 1$ The inverse of $\omega$ is $\omega^2$

$\omega^2 * \omega = 1$ The inverse of $\omega^2$ is $\omega$.

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

5) Commutativity: For $1, \omega, \omega^2 \in G$.

$$1 * \omega = \omega * 1 = \omega \in G$$

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

Scanned with CamScanner

8. Show that $\{R-\{-1\}, *\}$ is an abelian group under the binary operation $*$ defined by $a*b = a+b+ab$, $\forall\ a,b \in R-\{-1\}$.

Solution: $\text{Given:}\ \underset{(G,*)=}{G=a} * b = a+b+ab,\ \forall\ a,b \in R-\{-1\}$.

1. closure: since $a,b$ are real numbers $\overset{\text{and } a*b\neq -1}{,} \neq -1$,

$a+b+ab$ is a real number and $a+b+ab \neq -1$.

if, $a+b+ab = -1$,

$1 + a + b + ab = 0 \Rightarrow (1+a) + b(1+a) = 0$

$(1+a)(1+b) = 0$

$\Rightarrow a = -1$ (or) $b = -1$, which is a contradiction.

$\therefore\ a+b+ab \neq -1$

so $a+b+ab \in G$.

$G$ is closed.

2) Associativity: Let $a,b,c \in G$.

Then $(a*b)*c = (a+b\overset{a}{+}ab) * \overset{b}{c}$.

$= a+b+ab+c + (a+b+ab)c$

$= a+b+ab+c + ac+bc+abc$

$= a+b+c+ab+bc+ca+abc.$ $\to (1)$

and $(a)*(b*c) = a*(b+c+bc)$

$= a+b+c+bc+a(b+c+bc)$

$= a+b+c+bc+ab+ac+abc$

$= a+b+c+ab+bc+ca+abc.$ $\to (2)$

From (1) & (2), $(a*b)*c = a*(b*c)$, $\forall\ a,b,c \in G$.

Scanned with CamScanner

3. Identity: suppose $e \in G$ be the identity, then

$$a * e = a$$

$$a + e + ae = a$$

$$e + ae = a - a$$

$$e(1+a) = 0$$

$$\boxed{e = 0}$$

Identity element is 0.

4) Inverse: Let $a \in G$ be any element

$$\therefore a \neq -1$$

If $a^{-1}$ is the inverse of $a$, then

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

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

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

$$a^{-1} = \frac{-a}{1+a} \neq -1 \in G.$$

5. Commutativity: Let $a, b \in G$,

$$a * b = a + b + ab$$

$$= b + a + ba$$

$$= b * a$$

$\therefore (G, *)$ is an abelian group.

9. Show that if every element in a group $G$ is its own inverse, then the group $G$ must be abelian. AU-2005 2006.

(OR)

In a group $G$, if $a^2 = e \ \forall a \in G$, then $G$ is abelian.

7 2m

Solution: Let $a, b \in G$ be any two elements,

then $a * b \in G$.

Given every element is its own inverse.

$$a^{-1} = a \ , \ b^{-1} = b \text{ and } (a*b)^{-1} = a*b$$

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

$$b * a = a * b \quad \forall a, b \in G.$$

Hence $G$ is abelian.

10. In a group $(G, *)$, if $(a*b)^2 = a^2 * b^2 \ \forall a, b \in G$ then show that $(G, *)$ is abelian. * AU-2012.

Solution: Given : $(G, *)$ is a group

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

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

$$a*(b*a)*b = a*(a*b)*b \quad [\text{by } L \,\&\, R \text{ C. Law}]$$

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

This is true for all $a, b \in G$.

Hence $(G, *)$ is abelian.

AU-2017.

11. Examine $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \neq 0 \in R \right\}$ is a commutai group under Matrix multiplication, where R is the set of all real numbers.

Solution: Given: $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \neq 0 \in R \right\}$

1. closure: Let $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix} \in G, a \neq 0, b \neq 0.$

Then $AB = \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} \in G$

So, closure is satisfied.

2. Associative: since Matrix Multiplication is associative, i.e., $A(BC) = (AB)C \ \forall \ A, B, C \in G.$

3. Identity: Let $I = \begin{bmatrix} x & x \\ x & x \end{bmatrix}$, $x \neq 0$ is the identity element in G.

Then for any $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $a \neq 0$ in G

Now $AI = A$

$$\Rightarrow \begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} x & x \\ x & x \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$$

$$\begin{bmatrix} 2ax & 2ax \\ 2ax & 2ax \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$$

$$2ax = a$$

$$\Rightarrow x = \tfrac{1}{2}$$

$$I = \begin{bmatrix} \tfrac{1}{2} & \tfrac{1}{2} \\ \tfrac{1}{2} & \tfrac{1}{2} \end{bmatrix}$$ is the identity element

4. Inverse:

Let $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$ $a \neq 0$ in $G$

if $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$ is the inverse then $AB = I$

$$AB = I$$

$$\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} \tfrac{1}{2} & \tfrac{1}{2} \\ \tfrac{1}{2} & \tfrac{1}{2} \end{bmatrix}$$

$$\begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix} = \begin{bmatrix} \tfrac{1}{2} & \tfrac{1}{2} \\ \tfrac{1}{2} & \tfrac{1}{2} \end{bmatrix}$$

$$2ab = \tfrac{1}{2}$$

$$\Rightarrow b = \frac{1}{4a}$$

Inverse of $B = A^{-1} = \begin{bmatrix} \tfrac{1}{4a} & \tfrac{1}{4a} \\ \tfrac{1}{4a} & \tfrac{1}{4a} \end{bmatrix}$ exists.

$\therefore$ $G$ is a group.

5. Commutative: Since $ab = ba$ $\forall$ $a, b \in R$ for any

$A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $B = \begin{bmatrix} b & b \\ b & b \end{bmatrix}$ we have $AB = BA$

$\therefore$ $G$ is an abelian group under Multiplication.

12. prove that $(A, *)$ is a non-abelian group.

* where $A = R^{+} \times R$ and $(a,b) * (c,d) = (ac, bc+d)$.

Solution:

Given: $(A, *) = (a,b) * (c,d) = (ac, bc+d)$.

i) closure:

Let $(a,b)\ (c,d) \in A$

Then $(a,b) * (c,d) = (ac, bc+d) \in A$.

$\therefore$ A is closed.

(ii) Associative:

Let $(a,b), (c,d), (e,f) \in A$

To prove: $(a,b) * [(c,d) * (e,f)] = [(a,b) * (c,d)] * (e,f)$

consider, $(a,b) * [(c,d) * (e,f)] = (a,b) * [ce, de+f]$

$= ace, bce+de+f \longrightarrow ①$

$[(a,b) * (c,d)] * (e,f) = (ac, bc+d) * (e,f)$

$= [ace, bce+de+f] \rightarrow ②$

From ① & ② weget, A is associative.

(iii) Identity:

Let $(a,b) \in A$ and $(e_1, e_2) \in A$.

$\Rightarrow (a,b) * (e_1, e_2) = (a,b)$

$\Rightarrow (ae_1, be_1 + e_2) = (a,b)$

$\Rightarrow ae_1 = a \qquad be_1 + e_2 = b$

$e_1 = 1 \qquad b + e_2 = b \Rightarrow e_2 = 0.$

Hence identity is $(1,0)$.

iv) Inverse:

Let $(a,b) \in A$, $(c,d) \in A$

$\Rightarrow (a,b) * (c,d) = (e_1, e_2)$

$\Rightarrow (ac, bc+d) = (1,0)$

$\rightarrow ac = 1, \; bc+d = 0$

$\Rightarrow c = a^{-1}, \; d = -bc$

$= -ba^{-1}$

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

Hence $(A, *)$ is a group

v) Commutative:

Let $(a,b), (c,d) \in A$

To prove $(a,b) * (c,d) \neq (c,d) * (a,b)$

$(a,b) * (c,d) = (ac, bc+d) \rightarrow ①$

$(c,d) * (a,b) = (ca, da+b) \rightarrow ②$

From ① & ② weget,

$(a,b) * (c,d) \neq (c,d) * (a,b)$

$\therefore (A, *)$ is a non-abelian group.

Sub group:

Let $(G, *)$ is a group and $\phi = H \subset G$.

If $(H, *)$ is a group under the binary operation of $G$, then $(H, *)$ is a subgroup of $(G, *)$

i.e, $(H, *)$ is said to be a subgroup of $(G, *)$ if

1) $e \in H$ where $e$ is the identity in $G$

2) For any $a \in H$, $a^{-1} \in H$. 3) for $a, b \in H$, $a * b \in H$.

NOTE:

1. Every group $G$ $(G, *)$ has $[e]$ $(\{e\}, *)$ and $G$ as subgroups. These are called trivial sub-groups of $G$. All others are termed non-trivial (or) proper.

2. The non-trivial subgroups are also known as proper Subgroups.

3. The group $(Z, +)$ is a subgroup of $(Q, +)$, which is a sub-grouph of $(R, +)$. Yet $Z^*$ under multiplication is not a sub group of $(Q^*, \cdot)$

Theorem: 2

If $H$ is a non-empty subset of a group $G$. then $H$ is a subgroup of $G$ if and only if,

a) For all $a, b \in H$, $ab \in H$ and

b) For all $a \in H$, $a^{-1} \in H$.

proof:

If part:

Given: $H$ is a subgroup of $G$ $\Rightarrow$ $H$ is a group under the same binary operation.

To prove: a) For all $a, b \in H$, $ab \in H$

b) For all $a \in H$, $a^{-1} \in H$

For, $a, b \in H \Rightarrow a * b \in H$ (closure)

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

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

$\Rightarrow a * b^{-1} \in H$ ($\because$ H is a subgroup)

Sufficient condition:

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

To prove that H is a subgroup of G.

i) Closure:

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

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

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

$\Rightarrow a * b \in H$

H is closed.

ii) Identity: Let $a \in H \Rightarrow a^{-1} \in H$

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

$\Rightarrow e \in H.$

$\therefore$ The identity element is $e \in H$.

(iii) Inverse:

Let $e \in H$.

Choose, $a = e$ in $a * b^{-1} \in H$

$e * b^{-1} \in H$

$b^{-1} \in H$

$\therefore$ The inverse $b^{-1}$ is in H.

$\therefore$ H is a subgroup of G.

## SUBGROUPS:

Let $(G,*)$ be a group. Then $(H,*)$ is said to be subgroup of $(G,*)$ if $H \subseteq G$ and $(H,*)$ itself a group under the operation $*$.

i.e., $(H,*)$ is said to be a subgroup of $(G,*)$ if

(i) $e \in H$, where $e$ is the identity in $G$.

(ii) For any $a \in H$, $a^{-1} \in H$

(iii) For $a,b \in H$, $a*b \in H$.

Ex: (1) $(Q,+)$ is a subgroup of $(R,+)$

(2) $(R,+)$ is a subgroup of $(C,+)$.

Define proper and improper Subgroups:

1) The subgroups $(G,*)$ and $(\{e\},*)$ are called improper (or) trivial subgroups.

2) All the other groups are called the proper (or) non-trivial subgroups.

Theorem: 1

The necessary and sufficient condition that a non-empty subset $H$ of a group $G$ to be a subgroup is $a,b \in H \Rightarrow a*b^{-1} \in H$, for all $a,b \in H$.

Proof: Necessary condition:

Let us assume that $H$ is a subgroup of $G$.

since $H$ itself is a group,

Proof: $\forall\ a,b \in H$

$\Rightarrow$ a) For all $a,b \in H \Rightarrow ab \in H$

b) for all $a \in H \Rightarrow a^{-1} \in H$ [$\because$ by the definition of subgroup, Here $H$ is a subgroup of $G$]

only if part:

Given: a) For all $a,b \in H$, $ab \in H$

b) For all $a \in H$, $a^{-1} \in H$

To prove: $H$ is a subgroup of $G$

proof: $\forall\ a,b,c \in H$. Since $H \subseteq G$

$\Rightarrow a,b,c \in G$

$\therefore\ a(bc) = (ab)c$ ( Associative law holds in $H$)

$\forall\ a \in H,\ a^{-1} \in H$

$\Rightarrow aa^{-1} \in H$ [by (a)]

$\Rightarrow e \in H$

So $H$ is a group

Hence, $H$ is a subgroup of $G$.

Theorem:

If $G$ is a group $\phi \neq H \subseteq G$, with $H$ finite, then $H$ is a subgroup of $G$ if and only if $H$ is closed under the binary operation of $G$.

Proof: If part:

Given: $H$ is a subgroup of $G$

$\Rightarrow H$ is a group

To prove: $H$ is closed under the binary operation of $G$

proof: $\forall\ a, b \in H$

$\Rightarrow ab \in H$ [$\because$ H is a subgroup of G]

only if part:

Given: H is closed under the binary operation of G.

ie, $\forall\ a, b \in H \Rightarrow ab \in H$

To prove: H is a subgroup of G.

proof: (i) closure property:

$\forall\ a, b \in H \Rightarrow ab \in H$ [$\because H \leq G$]

(ii) Associative law:

Associative law holds in G it holds in H as well.

(iii) Existence identity:

If $a \in H$, then $aH = \{ah \mid h \in H\} \subseteq H$, because of the closure condition, By left-cancellation in G.

$ah_1 = ah_2$

$\Rightarrow h_1 = h_2$

So $|aH| = |H|$. with $aH \subseteq H$ and $|aH| = |H|$, it follows from H being finite that $aH = H$. As $a \in H$, there exists $b \in H$ with $ab = a$. But (in G)

$ab = a = ae$, so $b = e$ and H contains the identity.

(iv) Existence of Inverse:

since $e \in H = aH$, there is an element $c \in H$ such that $ac = e$, Then $(ca)^2 = (ca)(ca) = c(ac)a = (ce)a = ca = (ca)e$, so $ca = e$ and $c = a^{-1} \in H$.

consequently by thm(I), H is a subgroup of G.

Theorem : 3

AU- 2008, 2013, 2014, 2015. (5) 2m.

If $H_1$ & $H_2$ are subgroups of a Group $(G,*)$ then $H_1 \cap H_2$ is a subgroup of $(G,*)$.

proof: Given: $H_1, H_2$ are two subgroups of $(G,*)$

To prove: $H_1 \cap H_2$ is a subgroups.

Let $a,b \in H_1 \cap H_2 \Rightarrow a,b \in H_1$ and $a,b \in H_2$.

Since $H_1$ and $H_2$ are subgroups of $G$.

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

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

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

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

Hence, $H_1 \cap H_2$ is a subgroup of $(G,*)$.

Theorem: 4

* If $G$ is a group, let $H = \{a \in G / ag = ga,$ for all $g \in G\}$ then $H$ is a subgroup of $G$.

proof: Given: $G$ is a group

$H = \{a \in G / ag = ga,$ for all $g \in G\}$

To prove: $H$ is a subgroup of $G$.

i.e., To prove: $\forall a,b \in H \Rightarrow ab \in H$ and $a^{-1} \in H$

proof: Since $e \in G$ and $eg = ge = e$ for all $g \in G$

$\Rightarrow e \in H$

$\therefore$ $H$ is non empty.

$\forall \; a, b \in H$

$\Rightarrow ag = ga \rightarrow$ ①

and $bg = gb \rightarrow$ ② for all $g \in G$.

(i) To prove: $ab \in H$

proof: $(ab)g = a(bg)$

$= a(gb)$ [by ②]

$= (ag)b$

$= (ga)b$

$= g(ab)$

$\Rightarrow ab \in H$

(ii) To prove: $a^{-1} \in H$

ie., To prove: $a^{-1} g = g a^{-1}$ for all $g \in G$

Proof: $a^{-1}(ga)\, a^{-1} = a^{-1}(ag)\, a^{-1}$

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

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

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

Hence, $H$ is a subgroup of $G$.

problems based on subgroups:

1. Find all subgroups of $(\mathbb{Z}_6, +)$ group.

Solution:

To determine all subgroups of the grou $(\mathbb{Z}_6, +)$.

since $\{e\}$ and $G$ are the trivial subgroups of the group $G$.

$\{0\}$ and $\mathbb{Z}_6$ are the trivial subgroups of $(\mathbb{Z}_6, +$

If $G$ is a group and $\phi \neq H \subseteq G$, with $H$ is finite, then $H$ is a subgroup of $G$ iff $H$ is closed under the binary operation of $G$.

$\therefore$ clearly $\{0, 3\}$, $\{0, 2, 4\}$ are proper subsets of group $(\mathbb{Z}_6, +)$. $\{0,1,2,3,4,5\}$

| + | 0 | 3 |
|---|---|---|
| 0 | 0 | 3 |
| 3 | 3 | 0 |

| + | 0 | 2 | 4 |
|---|---|---|---|
| 0 | 0 | 2 | 4 |
| 2 | 2 | 4 | 0 |
| 4 | 4 | 0 | 2 |

From the tables we observe that $\{0, 3\}$, $\{0, 2, 4\}$ are closed under the binary operation $+$.

Hence, all subgroups of $(\mathbb{Z}_6, +)$ are $\{0\}$, $\{0, 3\}$, $\{0, 2, 4\}$, $\mathbb{Z}_6$

2. Find all the subgroups of $\{Z_{11}^{*}, \cdot\}$ group.

* Solution:

To determine all subgroups of the group $(Z_{11}^{*}, \cdot)$.

Since $\{e\}$ and $G$ are the trivial subgroups of the Group $G$. and $\{1\}$ and $Z_{11}^{*}$ are the trivial sub-groups of $\{Z_{11}^{*}\}$.

If $G$ is a group and $\phi \neq H \subseteq G$, with $H$ is finite, then $H$ is a subgroup of $G$ if and only if $H$ is closed under the binary operation of $G$.

clearly $\{1, 10\}, \{1, 3, 4, 5, 9\}$ are proper subsets of group $(Z_{11}^{*}, *)$

| * | 1 | 10 |
|---|---|---|
| 1 | 1 | 10 |
| 10 | 10 | 1 |

| * | 1 | 3 | 4 | 5 | 9 |
|---|---|---|---|---|---|
| 1 | 1 | 3 | 4 | 5 | 9 |
| 3 | 3 | 9 | 1 | 4 | 5 |
| 4 | 4 | 1 | 5 | 9 | 3 |
| 5 | 5 | 4 | 9 | 3 | 1 |
| 9 | 9 | 5 | 3 | 1 | 4 |

From the table we observe that $\{1, 10\}, \{1, 3, 4, 5, 9\}$ are closed under the binary operation.

Hence, all sub groups of $(Z_{11}, \cdot)$ are $\{1\}, \{1, 10\}, \{1, 3, 4, 5, 9\}, Z_{11}^{*}$.

H.10

1. Find all the subgroups of $(Z_{12}, +)$ group. Sol: $\{0, 6\}, \{0, 3, 6, 9\}$ $\{0, 4, 8\}$ $\{0, 2, 4, 6, 8, 10\}$

2. Find all the subgroups of $(Z_5, *)$ group. Sol = $\{1, 4\}$ $\{1, 3, \}$

Permutation:

Let $S$ be a non-empty set. A bijective function: $f: S \to S$ is called a permutation. If $S$ has $n$ elements, then the permutation is said to be of degree $n$.

Let $S = \{1, 2, 3, \dots n\}$.

The group $S_n$ is called the permutation group on $n$ symbols.

Definition:

A symmetry of a rigid body is a one to one distance preserving Mapping (or) transformation of the body onto itself.

1. Find all the subgroups of $S_3$ group.

Solution:

To determine all subgroups of the group $S_3 = \{1, 2, 3\}$.

Since $\{e\}$ and $G$ are the trivial subgroups of the group $G$.

$\pi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ and $S_3$ are the trivial subgroups of $S_3 = \{1, 2, 3\}$.

The group $S_3$ is symmetric group with three symbols $\{1, 2, 3\}$ and the group of all permutations of the set under the binary operation function composition. The elements of $S_3$ are,

$\pi_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $\pi_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $\pi_2 = \begin{pmatrix}1&2\\2&3\end{pmatrix}$,

(Identity element)

$\gamma_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $\gamma_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $\gamma_3 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

clearly $\{\pi_0, \pi_1, \pi_2\}$, $\{\pi_0, \gamma_1\}$, $\{\pi_0, \gamma_2\}$, $\{\pi_0, \gamma^3\}$ are the proper subsets of group $S_3$.

| * | $\pi_0$ | $\gamma_1$ |
|---|---|---|
| $\pi_0$ | $\pi_0$ | $\gamma_1$ |
| $\gamma_1$ | $\gamma_1$ | $\pi_0$ |

Let

$$\gamma_1\gamma_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

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

$$\gamma_1\gamma_1 = \pi_0$$

| * | $\pi_0$ | $\gamma_2$ |
|---|---|---|
| $\pi_0$ | $\pi_0$ | $\gamma_2$ |
| $\gamma_2$ | $\gamma_2$ | $\pi_0$ |

| * | $\pi_0$ | $\gamma_3$ |
|---|---|---|
| $\pi_0$ | $\pi_0$ | $\gamma_3$ |
| $\gamma_3$ | $\gamma_3$ | $\pi_0$ |

| * | $\pi_0$ | $\pi_1$ | $\pi_2$ |
|---|---|---|---|
| $\pi_0$ | $\pi_0$ | $\pi_1$ | $\pi_2$ |
| $\pi_1$ | $\pi_1$ | $\pi_2$ | $\pi_0$ |
| $\pi_2$ | $\pi_2$ | $\pi_0$ | $\pi_1$ |

| * | $\pi_0$ | $\pi_1$ | $\pi_2$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ |
|---|---|---|---|---|---|---|
| $\pi_0$ | $\pi_0$ | $\pi_1$ | $\pi_2$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ |
| $\pi_1$ | $\pi_1$ | $\pi_2$ | $\pi_0$ | $\gamma_3$ | $\gamma_1$ | $\gamma_2$ |
| $\pi_2$ | $\pi_2$ | $\pi_0$ | $\pi_1$ | $\gamma_2$ | $\gamma_3$ | $\gamma_1$ |
| $\gamma_1$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ | $\pi_0$ | $\pi_1$ | $\pi_2$ |
| $\gamma_2$ | $\gamma_2$ | $\gamma_3$ | $\gamma_1$ | $\pi_2$ | $\pi_0$ | $\pi_1$ |
| $\gamma_3$ | $\gamma_3$ | $\gamma_1$ | $\gamma_2$ | $\pi_1$ | $\pi_2$ | $\pi_0$ |

$$\pi_1\pi_1 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

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

$$= \pi_2$$

Scanned with CamScanner

$$\pi_1\pi_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = \pi_0$$

$$\pi_2\pi_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = \pi_0$$

$$\pi_2\pi_2 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \pi_1$$

From the composition table,

$\{\pi_0\}$, $\{\pi_0, \pi_1, \pi_2\}$, $\{\pi_0, r_1\}$, $\{\pi_0, r_2\}$, $\{\pi_0, r^3\}$ and $S_3$ are the proper sub-groups of $S_3$.

2. In the group $S_6$, Let

$$\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 6 & 2 & 5\end{pmatrix} \text{ and } \beta = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 2 & 6 & 1 & 3 & 5\end{pmatrix}$$

Determine $\alpha\beta$, $\beta\alpha$, $\alpha^3$, $\beta^4$, $\alpha^{-1}$, $\beta^{-1}$, $(\alpha\beta)^{-1}$, $(\beta\alpha)^{-1}$ and $\beta^{-1}\alpha^{-1}$.

Solution:

(i) $$\alpha\beta = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 6 & 2 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 2 & 6 & 1 & 3 & 5\end{pmatrix}$$

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

Route map:
1 → 3 → 6, 2 → 1 → 4
3 → 4 → 1, 4 → 6 → 5
5 → 2 → 2, 6 → 5 → 3.

(ii) $$\beta\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 2 & 6 & 1 & 3 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 6 & 2 & 5\end{pmatrix}$$

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

(iii) $$\alpha^3 = \alpha\alpha\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 6 & 2 & 5\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 6 & 2 & 5\end{pmatrix}$$

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

(iv) $\beta^4 = \beta\beta\beta\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 1 & 3 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \\ 4 & 2 & 6 & 1 & 3 & 5 \end{pmatrix} S_5,$

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

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

(v) $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 2 & 5 \end{pmatrix}^{-1}$

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

Route Map:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 3 & 1 & 4 & 6 & 2 & 5 \end{pmatrix}^{-1}$$

4)

(vi) $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 1 & 3 & 5 \end{pmatrix}^{-1}$

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

(vii) $(\alpha\beta)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 5 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 2 & 4 & 1 \end{pmatrix}$

(viii) $(\beta\alpha)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 3 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & \end{pmatrix}$

(ix) $\beta^{-1}\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 6 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 3 & 6 & 4 \end{pmatrix}$

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

$$\therefore \beta^{-1}\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 2 & 4 & 1 \end{pmatrix}.$$

H.W

* In a group $S_5$, Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ & $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$

Find $\alpha\beta$, $\beta\alpha$, $\alpha^3$, $\beta^4$, $\alpha^{-1}$. $\beta^{-1}$. $(\alpha\beta)^{-1}$; $(\beta\alpha)^{-1}$ and $\beta^{-1}\alpha^{-1}$.

3. For all $2 \leq n \leq 5$, find an element of order $n$ in $S_5$. Also determine the (cyclic) subgroup of $S_5$ that each of these elements generates.

2 8m. Solution: Cyclic subgroup:

For an $a \in a$ cyclic group $G$

$\langle a \rangle = \{a, a^2, \ldots a^{n-1}, a^n = e\}$ is cyclic subgroup generated by $a$.

Now in $S_5$, For $n = 2$, $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$ has order 2 and generates cyclic subgroup of $S_5$ given by the Set $\left\{ a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}, a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e \right\}$

For $n = 3$, $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ has order 3 and generates cyclic subgroup of $S_5$ given by the Set,

$$\left\{ a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}, a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}, a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e \right\}$$

For $n = 4$, $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$ has order 4 and generates cyclic subgroup of $S_5$ given by the Set,

$$\left\{ a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}, a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}, a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}. a^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e \right\}$$

For $n=5$,

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$ has order 5 and generates the cyclic subgroup of $S_5$ given by,

$$\left\{ a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}, \right.$$

$$a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}, a^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix},$$

$$\left. a^5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e \right\}.$$

4. Let $V = \frac{1+\sqrt{3}\,i}{2}$ and Let $A_6 = \{1, V, V^2, V^3, V^4, V^5\}$.

③ 8m

a) show that $(A_6, \cdot)$ is a group

b) For each $x$ in $A_6$, list the elements of the Carrier $[x]$ of the cyclic subgroup $([x], \cdot)$ and give the order of $x$.

c) Is $(A_6, \cdot)$ cyclic. If so name each generator of $G$.

d) Is $(A_6, \cdot)$ abelian.

Solution:

Given: $V = \frac{1+\sqrt{3}\,i}{2}$

$$V^2 = \left(\frac{1+\sqrt{3}i}{2}\right)\left(\frac{1+\sqrt{3}\,i}{2}\right) = \frac{1}{4}\left[1-3+2\sqrt{3}\,i\right]$$

$$= \frac{-1+\sqrt{3}i}{2}$$

$$V^2 = \frac{-1+\sqrt{3}\,i}{2}$$

$$v^3 = v^2 v = \left(\frac{-1+\sqrt{3}\,i}{2}\right)\left(\frac{1+\sqrt{3}\,i}{2}\right) = -\frac{4}{4} = -1$$

$v^3 = -1.$

$v^6 = v^3 v^3 = (-1)(-1) = 1.$

Multiplication table for $A_6$.

| $\circ$ | $1$ | $v$ | $v^2$ | $v^3$ | $v^4$ | $v^5$ |
|---|---|---|---|---|---|---|
| $1$ | $1$ | $v$ | $v^2$ | $v^3$ | $v^4$ | $v^5$ |
| $v$ | $v$ | $v^2$ | $v^3$ | $v^4$ | $v^5$ | $i$ |
| $v^2$ | $v^2$ | $v^3$ | $v^4$ | $v^5$ | $1$ | $v$ |
| $v^3$ | $v^3$ | $v^4$ | $v^5$ | $1$ | $v$ | $v^2$ |
| $v^4$ | $v^4$ | $v^5$ | $1$ | $v$ | $v^2$ | $v^3$ |
| $v^5$ | $v^5$ | $1$ | $v$ | $v^2$ | $v^3$ | $v^4$ |

From this table $1$ is the identity.

Table of inverses.

| | | | | | | |
|---|---|---|---|---|---|---|
| $x$ : | $1$ | $v$ | $v^2$ | $v^3$ | $v^4$ | $v^5$ |
| $x^{-1}$ : | $1$ | $v^5$ | $v^4$ | $v^3$ | $v^2$ | $v$ |

The binary operation $\circ$ which is multiplication of complex numbers is closed and associative.

Hence $(A_6, *)$ is a group.

b) $[1] = \{1\}, [v] = A_6 = [v^5]$

$[v^2] = \{1, v^2, v^4\} = [v^4], [v^3] = \{1, v^3\}.$

| $x$ : | $1$ | $v$ | $v^2$ | $v^3$ | $v^4$ | $v^5$ |
|---|---|---|---|---|---|---|
| order of $x$: | 1 | 6 | 3 | 2 | 3 | 6 |

(c) Yes. $(A_6, *)$ is a cyclic group and each of $V^1$ and $V^5$ is a generator.

(d) Yes, abelian group, since $x * y = y * x$ for any $x, y \in A_6$.

5. Show that the set of rigid Motions (symmetries) of a square with the binary operation of composition is a non-abelian group.

*

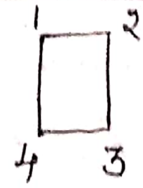
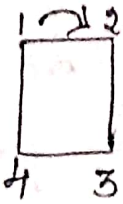
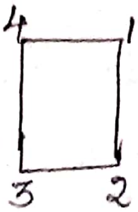
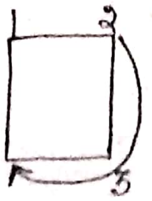
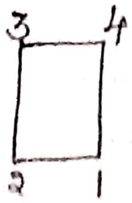
Solution:

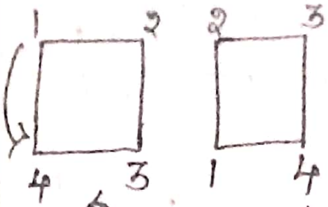
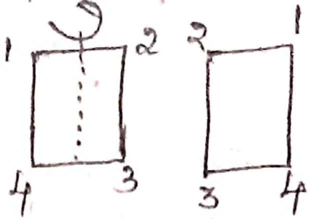
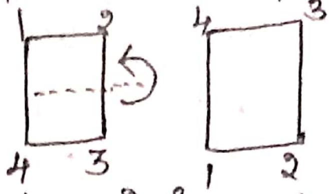
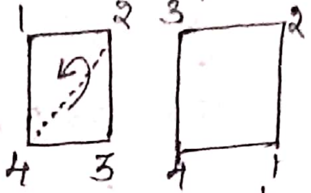
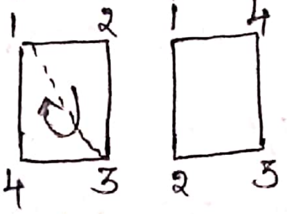
The set of all symmetries (rigid motion) of a square is $F = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$.

Let $*$ be the binary operation of $F$ (which is a set of 8 functions) defined as composition

$$(f \circ g)(x) = f(g(x)).$$

The symmetries (rigid motion) of a square.

| S. NO | Name | Rigid Motion | | Permutation of vertices. |
|---|---|---|---|---|
| | | Before | After | |
| 1. | $f_1$ identity | |  | $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ |
| 2. | $f_2$ rotate 90° clockwise |  |  | $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ |
| 3. | $f_3$ rotate 180° clockwise |  |  | $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ |

| | | | |
|---|---|---|---|
| 4. | $f_4$ rotate $\overset{270}{90^\circ}$ Counter-clockwise |  | $\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$ |
| 5. | $f_5$ reflect |  | $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ |
| 6. | $f_6$ reflect |  | $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$ |
| 7. | $f_7$ reflect |  | $\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$ |
| 8. | $f_8$ reflect |  | $\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$ |

To composition table is,

| * | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ |
|---|---|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ |
| $f_2$ | $f_2$ | $f_3$ | $f_4$ | $f_1$ | $f_7$ | $f_8$ | $f_6$ | $f_5$ |
| $f_3$ | $f_3$ | $f_4$ | $f_1$ | $f_2$ | $f_6$ | $f_5$ | $f_8$ | $f_7$ |
| $f_4$ | $f_4$ | $f_1$ | $f_2$ | $f_3$ | $f_8$ | $f_7$ | $f_5$ | $f_6$ |
| $f_5$ | $f_5$ | $f_8$ | $f_6$ | $f_7$ | $f_1$ | $f_3$ | $f_4$ | $f_2$ |
| $f_6$ | $f_6$ | $f_7$ | $f_5$ | $f_8$ | $f_3$ | $f_1$ | $f_2$ | $f_4$ |
| $f_7$ | $f_7$ | $f_5$ | $f_8$ | $f_6$ | $f_2$ | $f_4$ | $f_1$ | $f_3$ |
| $f_8$ | $f_8$ | $f_6$ | $f_7$ | $f_5$ | $f_4$ | $f_2$ | $f_3$ | $f_1$ |

Example: $f_3 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = f_2$$

$$f_3 \circ f_4 = f_2.$$

Hence the composition $\circ$ binary is a closure operation and is associative.

For example: $f_8 \circ (f_3 \circ f_6) = f_8 \circ (f_5) = f_4$ and

$(f_8 \circ f_3) f_6 = f_7 \circ f_6 = f_4.$

Hence, $f_8 \circ (f_3 \circ f_6) = (f_8 \circ f_3) \circ f_6$

The identity e is $f_1$ as is evident from the elements of the first row and first column of the composition table.

Inverse Table is,

| $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ |
|---|---|---|---|---|---|---|---|
| $f_1$ | $f_4$ | $f_3$ | $f_2$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ |

Hence, $(F, \circ)$ is a group. But it is not an abelian group since for example,

$$f_5 \circ f_2 = f_8 \neq f_7 = f_2 \circ f_5.$$

6. Find the elements in the groups $U_{20}$ and $U_{24}$ - the groups of units for the rings $(Z_{20}, +, \cdot)$ and $(Z_{24}, +, \cdot)$ respectively.

Solution: To find the elements in the groups $U_{20}$ and $U_{24}$ which are the groups of units for the rings $(Z_{20}, +, \cdot)$ and $(Z_{24}, +, \cdot)$ respectively.

Since units of the rings $(Z_n, +, \cdot)$ are defined as,

$U_n = \{ a \in Z / \gcd(a, n) = 1 \text{ and } 1 \le a \le n-1 \}$.

$\therefore U_{20} = \{ a \in Z / \gcd(a, 20) = 1 \text{ and } 1 \le a \le 19 \}$

$= \{1, 3, 7, 9, 11, 13, 17, 19\}$

Also, $U_{24} = \{ a \in Z / \gcd(a, 24) = 1 \text{ and } 1 \le a \le 23 \}$

$= \{1, 5, 7, 11, 13, 17, 19, 23\}$.

7. Find $x$ in $(U_{16}, \cdot)$ where $x \neq 1, x \neq 15$ but $x = x^{-1}$.

Solution:

To find $x$ in $(U_{16}, \cdot)$ where $x \neq 1, x \neq 15$ but $x = x^{-1}$.

W.K.T $(U_{16}, \cdot)$ is a group under the closed binary operation of Multiplication Modulo 16.

To find the inverse of each the elements.

| $\cdot$ | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 |
| 3 | 3 | 9 | 15 | 5 | 11 | 1 | 7 | 13 |
| 5 | 5 | 15 | 9 | 3 | 13 | 7 | 1 | 11 |
| 7 | 7 | 5 | 3 | 1 | 15 | 13 | 11 | 9 |
| 9 | 9 | 11 | 13 | 15 | 1 | 3 | 5 | 7 |
| 11 | 11 | 1 | 7 | 13 | 3 | 9 | 15 | 5 |
| 13 | 13 | 7 | 1 | 11 | 5 | 15 | 9 | 3 |
| 15 | 15 | 13 | 11 | 9 | 7 | 5 | 3 | 1 |

we observe that $7^2 = 1$ and $9^2 = 1$,

$\therefore \quad 7 = 7^{-1}$ and $9 = 9^{-1}$

Hence $x = 7$ and $9$.

HW:

Find $x$ in $(U_8, *)$ where $x \neq 1$ and $x \neq 7$ but $x = x^{-1}$.

8. State and prove Wilson's Theorem (or) prove that $(p-1)! \equiv -1 \pmod p$, for $p$ a prime.

Solution:

To prove that $(p-1)! \equiv -1 \pmod p$, for $p$ a prime

The result is true for $p = 2$.

Assume that result is true for $p \geq 3$.

Since $(Z_p^*, *)$ is group, every non-zero element 'a' has a unique multiplication say $a^{-1}$.

[Lagrange's theorem says that the only values of 'a' for which $a = a^{-1} \pmod p$ are $a \equiv \pm 1 \pmod p$ because the congruence $a^2 \equiv 1$ can have at most two roots (mod p)]

$\therefore$ with the exception of $\pm 1$, the factor of $(p-1)!$ can be arranged in unequal pairs, where the product of each pair is $\equiv -1 \pmod p$.

Thus, $(p-1)! \equiv -1 \pmod p$.

This proves the wilson's Theorem.

# Homomorphism - Isomorphism - cyclic groups:

Homomorphism :

If $(G, *)$ and $(H, *)$ are groups and $f: G \to H$, then $f$ is called a group homomorphism if for all $a, b \in G$, $f(a \circ b) = f(a) * f(b)$.

Isomorphism:

If $: (G, *) \to (H, *)$ is a homomorphism, then $f$ is an isomorphism, if it is one-to-one and onto. In this case, $G$, $H$ are said to be isomorphism groups.

Cyclic: A group $G$ is called cyclic, if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in \mathbb{Z}$.

Properties of Homomorphism:

Let $(G, \circ)$, $(H, *)$ be groups with respect identities $e_G$ $e_H$.

If $f: G \to H$ is a homomorphism, then

a) $f(e_G) = e_H$

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

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

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

Theorem : 1

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

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

(c) $f(a^n) = [f(a)]^n$ for all $e \in G$ and all $n \in \mathbb{Z}$.

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

proof: $[\because a.e = a]$

(a) $e_H * f(e_G) = f(e_G) = f(e_G * e_G)$

$= f(e_G) * f(e_G)$

$\Rightarrow e_H = f(e_G)$ by [Right - cancellation law]

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

(b) $f(a) * f(a^{-1}) = f(a * a^{-1}) = f(e_G) = e_H$ and

$f(a^{-1}) * f(a) = f(a^{-1} * a) = f(e_G) = e_H$,

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

(a) Let $e_G \in G$ and $e_H \in H$ be the identity elements.

Let $e_G * e_G = e_G$

$\Rightarrow f(e_G * e_G) = f(e_G)$

$\Rightarrow f(e_G) * f(e_G) = f(e_G) * e_H$ $[\because e_H$ is identity$]$

$\Rightarrow f(e_G) = e_H \rightarrow ①$ (by left Cancellation law)

b) Let $a \in G$, then $a^{-1} \in G$ and $a * a^{-1} = e_G = a^{-1} * a$

$f(a * a^{-1}) = f(e_G) = f(a^{-1} * a)$.

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

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

(c) Let $n$ be a positive integer and $a \in G$.

$f(a^n) = f(a * a * a * a \ldots$ n times).

$= f(a) * f(a) * f(a) * f(a) \ldots$ n times.

$f(a^n) = [f(a)]^n$, for any $n \in Z^+, a \in G$ → ②

Let us assume that the result in true for $n = k(\geq 1)$. ∴ $n = k+1$ wehave,

$f(a^n) = f(a^{k+1}) = f(a^k . a^1) = f(a^k) * f(a)$

$= [f(a)]^k * f(a)$ by ②

$= [f(a)]^{k+1}$

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

So by the principal of Mathematical induction the result is true for all $n \geq 1$.

For $n < 1$, we have $-n \geq 1$,

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

$f(a^n) = [[f(a)]^{-1}]^{-n}$ [∵ $f(a^{-1}) = [f(a)]^{-1}$] for all $a \in G$.

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

Hence, $f(a^n) = [f(a)]^n$ for all $a \in G$ and for all $n \in Z$.

d) If $S$ is a subgroup of $G$, then $S \neq \phi$, so $f(S) \neq \phi$.

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

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

Since $S$ is a subgroup of $G$, it follow that $a * b \in S$,

so $x * y = f(a) * f(b) = f(a * b) \in f(S)$.

$x^{-1} = [f(a)]^{-1} = f(a^{-1}) \in f(S)$ because $a^{-1} \in S$ when $a \in S$.

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

Theorem: 2.

Let $a \in G$ with $O(a) = n$, if $k \in \mathbb{Z}$ and $a^k = e$, then $n/k$.?

proof: Let $\boxed{k = qn + r}$ [by division algorithm] $0 \leq r < n$.

$$e = a^k = a^{qn+r} = a^{qn}\, a^r = (a^n)^q (a)^r$$
$$= e^q (a^r) = a^r$$

If $0 < r < n$, we get contradiction to $O(a) = n$.

Hence $r = 0$ and $k = qn$

$\Rightarrow n/k$.

$n/k$ $k = qn + r$

$\boxed{k = qn}$ $3/12$ $3/14$

$12 = (3 \times 4) + 0$ $14 = (3 \times 4) + 2$

$3/12$

Theorem: 3

Let $G$ be a cyclic group.

(a) If $|G|$ is infinite, then $G$ is isomorpic to $(\mathbb{Z}, +)$.

(b) If $|G| = n$, where $n > 1$, then $G$ is isomorphic to $(\mathbb{Z}_n, +)$.

solution:

(a) Let $a$ be a generator of $G$

$$G = \langle a \rangle = \{a^k, k \in \mathbb{Z}\}$$

Let $f : G \to \mathbb{Z}$ by $f(a^k) = k$.

(i) To prove : $f$ is homomorphism

For $a^m, a^n \in G$.

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

$\Rightarrow$ $f$ is a homomorphism.

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

(ii) To prove : $f$ is one-to-one.

Then, let $f(a^m) = f(a^n)$

$\Rightarrow m = n$

$\Rightarrow a^m = a^n$

Hence, $f$ is one-to-one.

(iii) To prove : $f$ is onto.

For any $k \in \mathbb{Z}$, we have $a^k \in G$ and $f(a^k) = k$.

$\therefore$ $f$ is onto.

Hence, there exists an isomorphism from $G$ onto $(\mathbb{Z}, +)$.

This means that $G$ and $(\mathbb{Z}, +)$ are isomorphic.

b) If $G = \langle a \rangle = \{ a, a^2, \dots, a^{n-1}, a^0 = e \}$

$f : G \to \mathbb{Z}_n$ by $f(a^k) = [k]$, $k = 1, 2, \dots, n$.

(i) To prove : $f$ is homomorphism.

Let $a^r, a^s \in G$, $1 \leq r \leq n$, $1 \leq s \leq n$.

$f(a^r a^s) = f(a^{r+s}) = [r+s]$

$= [r] + [s]$

$= a^r + a^s$ in $\mathbb{Z}_n$

$\Rightarrow$ $f$ is a homomorphism.

(ii) To prove : $f$ is one - to one.

$f(a^r) = f(a^s) \Rightarrow [r] = [s]$

$\Rightarrow r \equiv s \pmod{n}$.

$\Rightarrow (r-s)$ is a multiple of $n$

$\Rightarrow (a^{r-s}) = e$

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

$\Rightarrow a^r = a^s$

$10 \equiv 2 \pmod 8$

$10 - 2 = 8$

(iii) To prove : $f$ is onto.

$G$ and $Z_n$ are finite sets.

$\Rightarrow f$ is onto.

Hence, there exists an isomorphism from $G$ onto $(Z_n, +)$. This means that $G$ and $(Z_n, +)$ are isomorphic.

Theorem: 4

Every subgroup of a cyclic group is cyclic.

proof:

Let $G = \langle a \rangle$

Let $H$ be a subgroup of $G$

If $H = \{e\}$, then the result is trivial.

If $H \neq \{e\}$.

Let $t$ be the smallest positive integer such that $a^t \in H$. we claim $H = \langle a^t \rangle$. Since $a^t \in H$, by the closure property for the subgroup $H$. $\langle a^t \rangle \subseteq H$.

Let $b \in H$, then $b = a^s$ for some $s \in Z$.

By division algorithm, For the opposite inclusion.

$s = qt + r$ where $q, r \in G$ and $0 \leq r < t$. —①

Consequently $a^s = a^{qt+r}$

$\Rightarrow r = s - qt \rightarrow (1)$

$\Rightarrow a^r = a^{s-qt} = a^s a^{-qt} = a^s (a^t)^{-q}$

H is a subgroup of G, so $a^t \in H$

$= b(a^t)^{-q} \in H \quad [\because b \in H \text{ and } (a^t)^{-q} \in H]$

$\Rightarrow a^r \in H$ with $r > 0$, which is contradiction to mini... malit... of t.

But t is the smallest positive integer such that $a^t \in H$. $\Rightarrow r = 0$.

Hence, $s = qt$

$\Rightarrow b = a^s = a^{qt} = (a^t)^q \in \langle a^t \rangle$.

So $H = \langle a^t \rangle$, a cyclic group.

Theorem: 5

For a group G, prove that the function $f: G \to G$ defined by $f(a) = a^{-1}$ is an isomorphism if and only if G is abelian.

proof:

If part:

Assume that f is an isomorphism

To prove that G is abelian.

For $a, b \in G$

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

$\Rightarrow (a^{-1} b^{-1})^{-1} = ((ab)^{-1})^{-1}$, by taking inverse of both sides.

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

$\Rightarrow$ G is abelian.

Only if part:

Assume that $G$ is abelian

To prove that $f$ is an isomorphism.

(i) To prove $f$ is a homomorphism:

For $a, b \in G$,

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

Since $G$ is abelian.

$\therefore$ $f$ is a homomorphism.

(ii) To prove $f$ is one-to-one:

Let $f(a) = f(b)$.

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

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

$\Rightarrow a = b$

$\Rightarrow$ $f$ is one-to-one.

(iii) To prove $f$ is onto:

Let $a \in G$, Then $a^{-1} \in G$ and wehave,

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

$\Rightarrow$ $f$ is onto.

$\therefore$ $f$ is an isomorphism.

Theorem:6

Let $f: G \to H$ be a group Homomorphism onto $H$. If $G$ is abelian, prove that $H$ is abelian.

proof: Let $x, y \in H$, Then

$f$ is onto $\Rightarrow$ there exist $a, b \in G$ such that $f(a) = x$ and $f(b) = y$.

$G$ is abelian $\Rightarrow ab = ba$

$\Rightarrow f(ab) = f(ba)$

$\Rightarrow f(a)\,f(b) = f(b)\,f(a)$, since $f$ is a homomorphism.

$\Rightarrow xy = yx, \ \forall\, x, y \in H$

$\therefore$ $H$ is abelian.

1. Define $f: U_9 \to \langle Z_6, + \rangle$ as follows:

$f(1) = f(2^0) = 0$, $f(2) = f(2^1) = 1$

$f(4) = f(2^2) = 2$, $f(5) = f(2^5) = 5$

$f(7) = f(2^4) = 4$, $f(8) = f(2^3) = 3$

where $U_9 = \{1, 2, 4, 5, 7, 8\}$, the set of all units in $Z_9$.
Then $f$ is an isomorphism.

Solution: Let $a, b \in U_9$

Then $a = 2^m$ and $b = 2^n$ for $0 \le m, n \le 5$.

$\therefore$ $f(ab) = f(2^m 2^n) = f(2^{m+n}) = [m+n] = [m] + [n]$

$= f(2^m) + f(2^n)$

$f(ab) = f(a) + f(b)$

$\Rightarrow f$ is a homomorphism.

Clearly, $f$ is both one to one and onto.

Hence, $f$ is an isomorphism.

2. Show that $f:(R^+,\cdot)\rightarrow(R,+)$, where $f(x)=\log_{10}x$. $\forall x\in R^+$ is an isomorphism.

Solution: If $x\in R^+$ then $\log x\in R$

Also $\log x$ is unique.

$\therefore$ If $f(x)=\log x$ then $f:(R^+,\cdot)\rightarrow(R,+)$

(i) To prove $f$ is one-to-one:

Let $x_1, x_2\in R^+$ then $f(x_1)=f(x_2)$

$\Rightarrow \log x_1 = \log x_2$

$\Rightarrow e^{\log x_1} = e^{\log x_2}$

$\Rightarrow x_1 = x_2$

$\therefore f$ is one-to one.

(ii) To prove $f$ is onto:

Suppose $y\in R$ i.e., $y\in R^+$

$\Rightarrow e^y\in R^+$

$f(e^y)=\log e^y = y$

Thus $y\in R \Rightarrow \exists\, e^y\in R^+$

such that $f(e^y)=y$

$\therefore$ each element of $R$ is the $f$ image of some element of $R^+$

$\Rightarrow g$ is onto.

(iii) To prove $f$ preserves compositions in $R^+$ and $R$.

Let $x_1, x_2\in R^+$ then

$f(x_1, x_2) = \log(x_1 x_2)$.

Scanned with CamScanner

$$= \log x_1 + \log x_2$$

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

$\Rightarrow$ f is an isomorphism of $R^+$ onto R.

Hence, $R^+ \approx R$.

3. Show that $(M, *)$ is an abelian group where $M = \{A, A^2, A^3, A^4\}$ with $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $*$ is ordinary Matrix Multiplication. Further prove that $(M, *)$ is isomorphic to the abelian group $(G, *)$ where $G = \{1, -1, i, -i\}$ and $*$ is ordinary Multiplication.

Solution :

(a) Given: $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$,

$$A^2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

$$M = \{A, A^2, A^3, A^4\}$$

To prove: $(M, *)$ is an abelian group.

proof: (i) Closure property:

$$A^2 A^3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0+0 & -1+0 \\ 0-1 & 0+0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

For all $1 \le m, n \le 4$

$$A^m \cdot A^n = A^{m+n} = A^r, \quad 1 < r < 4$$

$$m+n = r \pmod 4$$

$$2+3 \quad 5 = 1 \pmod 4$$

$\Rightarrow$ $*$ is a closure.

(ii) Associative property:

Since Matrix multiplication is associative.

so $*$ is associative.

(iii) Existence of identity:

$$A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e \text{ is the identity.}$$

(iv) Existence of Inverse:

$$A^{-1} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = A^3$$

$$A^{-2} = (A^2)^{-1} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = A^2$$

$$A^{-3} = (A^3)^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = A^1$$

$$A^{-4} = (A^4)^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = A^0$$

Hence every element in M has a multiplicative inverse.

(v) Abelian property: For all $1 \leq m, n \leq 4$

$$A^m \cdot A^n = A^{m+n} = A^{n+m} = A^n \cdot A^m$$

so $*$ is commutative.

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

(b) Define $f : M \to G$ such that,

$$f(A) = i, \quad f(A^2) = -1 = i^2$$

$$f(A^3) = -i = i^3, \quad f(A^4) = 1 = i^4$$

Then $f$ is 1-1, onto and preserves the operation.

Hence, $f$ is an isomorphism from M to G.

Observe that $g : M \to G$ defined by,

$g(A) = -i$, $g(A^2) = -1$, $g(A^3) = i$, $g(A^4) = 1$ is also isomorphism.

# COSETS AND LAGRANGE'S THEOREM:

**Left coset:**

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

**Right coset:**

If $H$ is a subgroup of $G$, then for each $a \in G$, the set $Ha = \{ha / h \in H\}$ is called a right co-set of $H$ in $G$.

**Lemma:**

If $H$ is a subgroup of the finite group $G$, then for all $a, b \in G$

a) $|aH| = |H|$

b) either $aH = bH$ (or) $aH \cap bH = \phi$.

**proof:**

Given: $H$ is a subgroup of $G$.

a) Since $aH = \{ah / h \in H\} \Rightarrow |aH| \leq |H|$.

If $|aH| < |H|$, we have $ah_i = ah_j$ with $h_i, h_j$ distinct elements of $H$

$x.2 \neq x.3$ $h_i, h_j \in H, h_i \neq h_j$

By left-cancellation in $G$ we then get the contradiction $h_i = h_j$, so $|aH| = |H|$.

$a = bh_2h_1^{-1}$, $b = ah_1h_2^{-1}$ $x = ah$ $= (bh_2h_1^{-1})h$ $= b(h_2h_1^{-1}h) \in H$

b) If $aH \cap bH \neq \phi$, let $c = ah_1 = bh_2$, for some $h_1, h_2 \in H$

If $x \in aH$, then $x = ah_3$ for some $h_3 \in H$ and so,

$x = (bh_2h_1^{-1})h_3 = b(h_2h_1^{-1}h) \in bH$ and $aH \subseteq bH$

III^ly, $y \in bH \Rightarrow y = bh_3$ for some $h_3' \in H$

$b = ah_1h_2^{-1}$ $y = bh$ $= (ah_1h_2^{-1})h$ $= a\, h_1h_2^{-1}h \in aH$

$\Rightarrow y = (ah_1 h_2^{-1})h_3 = a(h_1 h_2^{-1} h_3) \in aH.$

So $bH \subseteq aH$.

Therefore $aH$ and $bH$ are either disjoint or identical.

Theorem: Lagrange's Theorem:

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

Proof: Let $|G| = o(G) = n$ and $o(H) = m$.

Since $G$ is a finite group, $H$ is finite.

$\therefore$ The number of co-sets of $H$ in $G$ is finite

Let $Ha_1, Ha_2, \ldots, Ha_r$ be the distinct right co-sets of $H$ in $G$.

Then by the right co-set decomposition of $G$, we have

$$G = Ha_1 \cup Ha_2 \cup Ha_3 \cup \ldots \cup Ha_r$$

So that, $o(G) = o(Ha_1) + o(Ha_2) + \ldots + o(Ha_r)$

But $o(Ha_1) = o(Ha_2) = \ldots = o(Ha_r) = o(H)$ (by Lemma (ii))

$\therefore o(G) = o(H) + o(H) + o(H) + \ldots + o(H)$ ($r$ terms)

$o(G) = r\, o(H) \Rightarrow n = rm$

This shows that $o(H)$ divides $o(G)$.

$\Rightarrow m/n$

Hence the Lagrange's Theorem.

Corollary : 1

If $G$ is a finite group and $a \in G$, then $o(a)$ divides $|G|$.

proof: Let, $o(a) = m$,

Then the subgroup $H$, of $G$, generated by 'a' is given by, $H = [a] = \{a, a^2, \ldots, a^m = e\}$

$\Rightarrow |H| = m$. [Since: if $a^i = a^j$, for $1 \le i, j \le m$, then $a^{j-i} = e$, with $0 < j-i < m$, contradicting the minimality of $m$).

$\Rightarrow$ By Lagrange's theorem, $|H|$ divides $|G|$

$\Rightarrow m / |G|$

$\Rightarrow o(a) / |G|$.

$a^2 = a^3$

$a^{2-3} = a^{-1} \neq e$

Corollary: 2.

Every group of prime order is cyclic.

proof:

Let $G$ be a group of prime order $p$, and $a \in G$.

w.k.T, If $G$ is finite group and $a \in G$, then $o(a)$ divides $|G|$.

$\therefore$ weget $o(a)$ divides $p$.

Since $p$ is prime, then $o(a) = p$

Hence, $G = \langle a \rangle$ and $G$ is a cyclic group.

Theorem:

Let $H$ and $k$ be subgroups of a group $G$, where $e$ is the identity of $G$.

If $|H| = m$ and $|k| = n$ with $\gcd(m, n) = 1$, prove that $H \cap k = \{e\}$.

Proof:

Given: If $H$ and $K$ are subgroups of $G$.
and $|H| = m$ and $|K| = n$.

Suppose $H \cap k$ is a subgroup of $H$

$\Rightarrow |H \cap k|$ divides $|H| = m$.

and $H \cap k$ is a subgroup of $k$

$\Rightarrow |H \cap k|$ divides $|k| = n$.

$|H \cap k|$ divides both $m$ and $n$ and given $\gcd(m, n) = 1$.

$\Rightarrow |H \cap k| = 1$

$\Rightarrow H \cap k = \{e\}$

since $e \in H \cap k$.

1. For the group $G = (Z_{12}, +)$ and the subgroup, $H = \{[0], [4], [8]\}$ of $G$, find all the left co-sets of $H$ in $G$. Also, obtain the corresponding co-set decomposition of $G$.

5 8M

Solution:

Let $Z_{12} = \{[0], [1], [2], \ldots, [11]\}$

The left co-sets of the given $H$ w.r.to $[a] \in Z_{12}$ is given by.

$$[a] + H = \{[a] + [h] \mid [h] \in H\}$$

$$= \{[a] + [0], [a] + [4], [a] + [8]\}$$

varying $[a]$ over the elements of $Z_{12}$, weget the left co-sets of $H$ as given below:

$$[0]+H = \{[0]+[0], [0]+[4], [0]+[8]\}$$

$$= \{[0], [4], [8]\}$$

$$[4]+H = \{[4], [8], [0]\}$$

$$[8]+H = \{[8], [0], [4]\}$$

$$\therefore [0]+H = [4]+H = [8]+H = H.$$

$$[1]+H = \{[1]+[0], [1]+[4], [1]+[8]\}$$

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

$$[5]+H = \{[5], [9], [1]\}$$

$$[9]+H = \{[9], [1], [5]\}$$

$$\therefore [1]+H = [5]+H = [9]+H.$$

$$[2]+H = \{[2]+[0], [2]+[4], [2]+[8]\}$$

$$= \{[2], [6], [10]\}$$

$$[6]+H = \{[6], [10], [2]\}$$

$$[10]+H = \{[10], [2], [6]\}$$

$$\therefore [2]+H = [6]+H = [10]+H.$$

$$[3]+H = \{[3]+0, [3]+[4], [3]+[8]\}$$

$$= \{[3], [7], [11]\}$$

$$[7]+H = \{[7], [11], [3]\}$$

$$[11]+H = \{[11], [3], [7]\}.$$

$$\therefore [3]+H = [7]+H = [11]+H.$$

$(\mathbb{Z}_{12}, +) = ([0]+H) \cup ([1]+H) \cup [[2]+H) \cup ([3]+H)$ is a partition of $G$.

2. a) For $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ find the subgroup $k = \langle \beta \rangle$.

b) Determine the left co-sets of k in $G = S_4$.

Solution:

a) $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ has order 4 and generates the cyclic subgroup,

$$k = \langle \beta \rangle = \left\{ \overset{\beta^1}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}}, \overset{\beta^2}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}}, \overset{\beta^3}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}}, \overset{\beta^4}{\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}} = \beta^4 = e \right\} \text{ of } S_4.$$

b) Let co-sets of k in $G = S_4$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} k = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \right\}$$

$$= \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} k = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} k = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} k = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} k = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} k = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} K = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} K = K.$$

# RINGS

## Definition : Ring

Let $R$ be a non-empty set on which we have two closed binary operations, denoted by $+$ and $\cdot$
Then $(R, +, \cdot)$ is a ring if for all $a, b, c \in R$,
The following conditions are satisfied.

a) $a+b = b+a$ Commutative law of +

b) $a+(b+c) = (a+b)+c$. Associative law of +

c) There exists $z \in R$ such that $a+z = z+a = a$ for every $a \in R$. Existence of identity +

d) For each $a \in R$ there is an element $b \in R$ with $a+b = b+a = z$ Existence of inverse +

e) If $a, b \in R \Rightarrow a * b \in R$ Closure *

f) $a*(b*c) = (a*b)*c$ Associative law of *

g) $a*(b+c) = a*b + a*c$
$(b+c)*a = b*a + c*a$ } Distributive laws of * over +.

## Definition:

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

a) If $a * b = b * a$ for all $a, b \in R$, then $R$ is called a commutative ring

b) The Ring $R$ is said to have no proper divisors of zero if for all $a, b \in R$, $ab = z \Rightarrow a = z$ (or) $b = z$.

c) A ring with unity, if there is an element $1 \in R$ such that $a*1 = 1*a = a$ $\forall a \in R$. Then $1$ is called a unity or multiplicative identity.

d) Let R be a ring with unity $u$. if $a \in R$ and there exists $b \in R$ such that $ab = ba = u$ then $b$ is called a Multiplicative inverse of 'a' and 'a' is called a unit of R.

## Integral domain & Field:

Let R be a commutative ring with unity.

Then:

a) R is said to be an integral domain, if it has no zero divisors. (ie, $ab = z \Rightarrow a = z$ or $b = z$).

b) R is said to be a field, if every non-zero element in R is a unit.

## Subring:

Let $(R, +, \cdot)$ be a ring. Then a non-empty subset S, of R is said to be a subring of R, if $(S, +, \cdot)$ itself is a ring.

Ex: 1) $\{z\}$ and R are subrings of $(R, +, \cdot)$

2) $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Q}, +, \cdot)$, which is a subring of $(\mathbb{R}, +, \cdot)$.

## Ideal:

A non-empty subset I of a ring R is called an Ideal of R, if for all $a, b \in I$ and all $r \in R$, we have,

a) $a - b \in I$

b) $ar, ra \in I$.

## Properties of Rings:

In any ring $(R, +, \cdot)$

1) The zero element $z$ is unique. [i.e. $0 = 0'$]

2) The additive inverse of every element is unique. [$b = c$

3) The Cancellation law's of Addition are valid.

a) $a + b = a + c \Rightarrow b = c$

b) $b + a = c + a \Rightarrow b = c$.

### Theorem: 1

For any ring $(R, +, \cdot)$ and any $a \in R$, we have

$az = za = z$.

Proof: If $a \in R$ then $az = a(z+z)$, [$\because z + z = z$]

Hence, $z + az = az = a(z+z)$

$z + az = az + az$ [by Right C. Law]

$z = az$

Illy, $za = z$.

Hence, $az = za = z$.

### Theorem: 2

If $(R, +, \cdot)$ is a ring and if $a, b \in R$ then

a) $-(-a) = a$

b) $a(-b) = (-a)b = -(ab)$

c) $(-a)(-b) = ab$.

proof:

a) $(-a) + a = z$ and $(-a) + (-(-a)) = z$

Since $-a$ is the additive inverse of $a$ and $-(-a)$ is the additive inverse of $-a$.

$\Rightarrow (-a)+a = (-a)+(-(-a))$

$\Rightarrow a = -(-a)$, by left cancellation.

b) $(ab+a(-b) = a(b+(-b)) = az = z)$

$\Rightarrow a(-b+b) = a(-b)+a.b$

$\Rightarrow a.0 = a(-b)+a.b$

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

Illy, $(-a).b = -(ab)$.

Hence $(-a)b = a(-b) = -(ab)$.

c) we know that $a(-b) = -(a.b)$

Replacing $a$ by $-a$ weget,

$(-a)(-b) = -(-a.b) = -[-(a.b)] = a.b.$

Hence, $(-a)(-b) = ab$.

Theorem:3

Let $(R,+,\cdot)$ be a commutative ring with unity. Then $R$ is an integral domain if and only if, for all $a,b,c \in R$ where $a \neq z$, $ab = ac \Rightarrow b = c$.

(OR)

A commutative ring with unity is an integral domain if & only if the cancellation laws holds in R.

Proof: If R is an integral domain.

Let $x, y \in R$

$\Rightarrow xy = z$

$x = z$ or $y = z$

Now $ab = ac$

$\Rightarrow ab - ac = a(b-c) = z$

$\Rightarrow b - c = z \quad [\because a \neq z]$

(or) $b = c$.

Converse part:

R is commutative with unity and R satisfies Multiplicative cancellation.

Let $a, b \in R$

$ab = z$

If $a = z$ the result holds good.

If $a \neq z$

$az = z$

$\Rightarrow ab = az$

$\Rightarrow b = z$

So there are no proper divisors of zero and R is an integral domain.

Theorem: 4

If $(F, +, \cdot)$ is a field, then it is an integral domain.

proof: Let $a, b \in F$ with $ab = z$.

If $a = z$, then the result holds good.

If not, 'a' has a multiplicative inverse $a^{-1}$ because F is a field.

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

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

Hence, F has no proper divisors of zero and is an integral domain.

Theorem: 5

A finite Integral domain $(D, +, \cdot)$ is a field.

Proof: To prove $D$ is a field.

we need to prove that every non-zero element in $D$ has a multiplicative inverse.

Let $a \neq z$ be in $D$.

Since $D$ is finite, Let $\{a_1, a_2, .., a_n\}$ be the only distinct elements of $D$.

consider, $A = \{a a_1, a a_2, \dots, a a_n\}$ in $D$.

we claim that they are all distinct elements.

To prove this claim assume the contrary that,

$$a a_i = a a_j \quad \text{with } a_i \neq a_j$$

$$\Rightarrow a(a_i - a_j) = z \quad \text{with } a_i - a_j \neq z$$

$$\not\Rightarrow \quad a = z \quad (\text{Since}, F \text{ is an I.D})$$

This is a contradiction.

$\therefore$ our claim is proved.

Hence $A = \{a a_1, .., a a_n\} = D$

Since $1 \in D$, $1 = a a_j$ for some $j$ with $1 \leq j \leq n$.

$\Rightarrow a_j \in D$ is the multiplicative inverse of $a$

$\Rightarrow D$ is a field.

Theorem: 6

Given a ring $(R, +, \cdot)$ a non-empty subset $S$ of $R$ is a subring of $R$ if and only if,

1) For all $a, b \in S$, we have $a+b$, $ab \in S$. and.

2) For all $a \in S \Rightarrow -a \in S$.

Proof :

a) Let $(S, +, \cdot)$ is a subring of $R$ for all $a, b \in S$

$\Rightarrow ab \in S$ by definition of ring

$\Rightarrow a \in S$ and $b \in S$ $[\because (S, +)$ is a group$]$

$\Rightarrow a+b \in S$

Hence, $(S, +, \cdot)$ is a subring of $R$ then $a+b, ab \in S$ for all $a, b \in S$.

Converse part :

Let $a+b, ab \in S$ for all $a, b \in S$

To prove : $(S, +, \cdot)$ is a subring of $R$

b) Let $a \in S$

$\Rightarrow a - a = z \in S$ and $z + a = a \in S$

Also if $b \in S$ then,

$a + (b) = a+b \in S$

Hence, $a - (-b) = a+b \in S$.

Hence, $a+b, ab \in S$ for all $a, b \in S$.

Then $(S, +, \cdot)$ is a subring of $R$.

Problems based on Rings:

1. Consider the set $\mathbb{Z}$ together with the binary operations of $\oplus$ and $\odot$, which are defined by,

$$x \oplus y = x+y-1 \quad \text{and} \quad x \odot y = x+y-xy$$

For $x, y \in \mathbb{Z}$. prove that $(\mathbb{Z}, \oplus, \odot)$ is a ring.

Solution:

(i) Closure axiom under $\oplus$:

Let $x, y \in \mathbb{Z}$. Then

$$x \oplus y = x + y - 1 \in \mathbb{Z}$$

$\Rightarrow$ closure is true.

(ii) Associative axiom under $\oplus$:

Let $x, y, z \in \mathbb{Z}$. Then

$$(x \oplus y) \oplus z = (x+y-1) \oplus z$$
$$= x+y-1+z-1$$
$$= x+y+z-2$$

$$x \oplus (y \oplus z) = x \oplus (y+z-1)$$
$$= x+y+z-1-1$$
$$= x+y+z-2$$

$\therefore (x \oplus y) \oplus z = x \oplus (y \oplus z) \ \forall x, y, z \in \mathbb{Z}$.

Hence, $\oplus$ is associative in $\mathbb{Z}$.

(iii) Existence of zero element:

Let $x \in \mathbb{Z}$ and let $x \oplus e = x$

Then $x + e - 1 = x$

$\Rightarrow e = 1 \in \mathbb{Z}$.

$\therefore 1 \in \mathbb{Z}$ is the zero element under $\oplus$

$x + z = \mathbb{Z}$.
$x + z - 1 = x$
$\cancel{x} + z = \cancel{x} + 1$
$z = 1 \in \mathbb{Z}$

(iv) Existence of additive inverse:

Let $x \in \mathbb{Z}$ and Let $x \oplus x' = 1$

Then $x + x' - 1 = 1$

$\Rightarrow x' = 2 - x \in \mathbb{Z}$.

$\therefore 2 - x \in \mathbb{Z}$ is the additive inverse of $x$.

$x \oplus -x = \mathbb{Z}$.
$x - x - 1 = 1$

$x \oplus x' = \mathbb{Z}$
$x + x' = 1$
$x + x' - 1 = 1$
$x' = -x + 1 + 1$
$x' = 2 - x \in \mathbb{Z}$

(v) Commutative axiom under $\oplus$ :

Let $x, y \in \mathbb{Z}$. Then,

$x \oplus y = x+y-1$ and $y \oplus x = y+x-1 = x+y-1$

$\Rightarrow x \oplus y = y \oplus x, \forall x, y \in \mathbb{Z}$

$\Rightarrow \oplus$ is commutative in $\mathbb{Z}$.

(vi) closure axiom under $\odot$ :

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

$x \odot y = x+y-xy \in \mathbb{Z}$

Thus, $x, y \in \mathbb{Z} \Rightarrow x \odot y \in \mathbb{Z}$

$\Rightarrow$ closure axiom is true under $\odot$

(vii) Associative axiom under $\odot$ :

Let $x, y, z \in \mathbb{Z}$, Then

$$\begin{aligned}(x \odot y) \odot z &= (x+y-xy) \odot z \\ &= x+y-xy+z-(x+y-xy)z \\ &= x+y+z-xy-yz-zx+xyz\end{aligned}$$

$$\begin{aligned}x \odot (y \odot z) &= x \odot (y+z-yz) \\ &= x+y+z-yz-x(y+z-yz) \\ &= x+y+z-yz-xy-zx+xyz \\ &= x+y+z-xy-yz-zx+xyz\end{aligned}$$

$\Rightarrow (x \odot y) \odot z = x \odot (y \odot z), \forall x, y, z \in \mathbb{Z}$.

$\Rightarrow \odot$ is associative.

(viii) Distributive axiom:

Let $x, y, z \in \mathbb{Z}$, Then

$x \odot (y \oplus z) = x \odot (y+z-1)$

$$= x+y+z-1-x(y+z-1)$$
$$= x+y+z-1-xy-xz+x$$
$$= 2x+y+z-xy-xz-1$$

$$(x \odot y) \oplus (x \odot z) = (x+y-xy) \oplus (x+z-xz)$$
$$= x+y-xy+x+z-xz-1$$
$$= 2x+y+z-xy-xz-1$$

$\Rightarrow x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

$\Rightarrow$ $\odot$ is distributive with respect to $\oplus$

$\therefore \langle \mathbb{Z}, \oplus, \odot \rangle$ is a Ring.

H.W.

2. Define the binary operations $\oplus$ and $\odot$ on $\mathbb{Z}$ by, $x \oplus y = x+y-7$, $x \odot y = x+y-3xy$, for all $x, y \in \mathbb{Z}$. Explain why $(\mathbb{Z}, \oplus, \odot)$ is not a ring

3. Let $k, m$ be fixed integers, Find all values for $k, m$ for which $(\mathbb{Z}, \oplus, \odot)$ is a ring under the binary operations $x \oplus y = x+y-k$, $x \odot y = x+y-mxy$, where $x, y \in \mathbb{Z}$.

Solution:

$(\mathbb{Z}, \oplus, \odot)$ is a ring. for $x, y, z \in \mathbb{Z}$, we have

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

Using $x \oplus y = x+y-k$, $x \odot y = x+y-mxy$ weget,

$$x \odot (y+z-k) = (x+y-mxy) \oplus (x+z-mxz)$$

$$(x)+(y+z-k)-mx(y+z-k) = (x+y-mxy)+(x+z-mxz)-k$$

$x+y+z-k-mxy-mxz+mkx = x+y-mxy+x+z-mxz$ $-k.$

on cancelling the like terms on both the sides, we get

$$mkx = x$$

$$\Rightarrow mk = 1$$

Since $mk = 1$, and $k, m$ are integers, we have,

$$m = k = 1$$

(or)

$$m = k = -1$$

Hence the values of $m$ and $k$ are $\pm 1$.

4. Let $(Q, \oplus, \odot)$ denote the field where $\oplus$ and $\odot$ are defined by,

$$a \oplus b = a+b-k \quad , \quad a \odot b = a+b+(ab/m)$$

For fixed elements $k, m (\neq 0)$ of $Q$. Determine the value for $k$ and the value for $m$ in each of the following,

(a) The zero elements for the field is 3.

(b) The additive inverse of the element 6 is $-9$.

(c) The multiplicative inverse of 2 is $1/8$.

Solution:

$$\text{Given: } a \oplus b = a+b-k \rightarrow ①$$

$$a \odot b = a+b+\frac{ab}{m} \rightarrow ②$$

(a) Given: The zero element for the field is 3.

W.k.T $\quad a+0 = a$

$$① \Rightarrow a \oplus 3 = a \quad \forall a \in Q$$

$$\Rightarrow k = 3$$

W.k.T, $\quad a \cdot 0 = 0$

$$\Rightarrow a \odot 3 = 3$$

② ⇒ $a + 3 + \frac{(a)(3)}{m} = 3$

⇒ $a + \frac{(a)(3)}{m} = 0$

⇒ $a\left[1 + \frac{3}{m}\right] = 0$

⇒ $1 + \frac{3}{m} = 0$ ⇒ $1 = -3/m$

⇒ $m = -3$

$\therefore$ $k = 3$ , $m = -3$.

(b) Given: The additive inverse of 6 is −9.

Let b be the zero of the field.

W.K.T $a + b = a$

$a \oplus b = a$

① ⇒ $a + b - k = a$

⇒ $\boxed{b = k}$

So, k is the zero of the field $(Q, \oplus, \odot)$

$6 \oplus (-9) = k$ //

$6 + (-9) - k = k$

$-3 - k = k$

$-3 = 2k$

$k = -3/2$

W.K.T, $a \odot k = k$

② ⇒ $a + k + \frac{(a)(k)}{m} = k$

⇒ $a + \frac{(a)(k)}{m} = 0$ ⇒ $a(1 + k/m) = 0$

$1 + k/m = 0$

⇒ $m = -k = -(-3/2) = 3/2$.

$\therefore\ k = -3/2\ ,\ m = 3/2.$

(c) Given: Multiplicative inverse of 2 is $\frac{1}{8}$.

W.k.T, $a \cdot e = a\ ,\ a \in Q$

$a \odot e = a$

② $\Rightarrow a + e + \frac{ae}{m} = a$

$\Rightarrow e + \frac{ae}{m} = 0 \Rightarrow e\left[1 + \frac{a}{m}\right] = 0$ $\quad \Rightarrow e = 0,\ 1 + \frac{a}{m} = 0.$

$\Rightarrow e = 0$

So the multiplicative identity is 0.

$2 \odot \frac{1}{8} = 0$

② $\Rightarrow 2 + \frac{1}{8} + \frac{2(1/8)}{m} = 0$

$\Rightarrow \frac{17}{2} + \frac{1}{4m} = 0$

$\Rightarrow m = -2/17.$

$a = 1$

$b = k.$

$1 + k + k/m.$

W.k.T , $\boxed{1 + \frac{k}{m} = 0} \Rightarrow m + k = 0$

$m = -k.$

$\therefore\ k = -m = 2/17.$

$\therefore\ k = 2/17\ ,\ m = -2/17.$

The solutions are,

(a) $k = 3,\ m = -3.$

(b) $k = -3/2\ ,\ m = 3/2$

(c) $k = 2/17\ ,\ m = -2/17.$

5. Let $A = \left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} / a, b, c \in Z \right\}$ be the subset of the ring $R = M_2(Z)$. prove that A is a subring but not an ideal.

Solution:

For any $B = \begin{bmatrix} d & 0 \\ e & f \end{bmatrix}, C = \begin{bmatrix} g & 0 \\ h & i \end{bmatrix} \in A$

we have $B + C = \begin{bmatrix} d+g & 0 \\ e+h & f+i \end{bmatrix} \in A$ and

$B.C = \begin{bmatrix} dg & 0 \\ eg+fh & fi \end{bmatrix} \in A$

Since $d+g, e+h, f+i, dg, eg+fh, fi \in Z$.

For any $A = \begin{bmatrix} a & 0 \\ b & c \end{bmatrix}$, the additive inverse is

$-A = \begin{bmatrix} -a & 0 \\ -b & -c \end{bmatrix}$.

So that $A + (-A) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Hence A is a subring of $M_2(Z)$.

For $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in A$ and $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in M_2(Z)$.

wehave, $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 2 & 1 \end{bmatrix} \notin A$.

So A is not an ideal.

6. Let $R = M_2(Z)$ and Let $S$ be the Subset of $R$ where $S = \left\{ \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} / x, y \in Z \right\}$ prove that $S$ is a subring of $R$.

Solution: If $R = M_2(Z)$ and $S = \left\{ \begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} / x, y \in Z \right\}$ is the subset of $R$.

To prove that $S$ is a subring of $R$.

Consider, $x = 0$, $y = 0$ in $S$, it follows that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$.

$\therefore S \neq \phi$.

Let $\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}$ and $\begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix}$ are two elements of $S$, where, $x, y, v, w \in Z$.

Consider, $\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} - \begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix} = \begin{bmatrix} x-v & (x-v)+(y-w) \\ (x-v)+(y-w) & x-v \end{bmatrix}$

we observe that is the form of $\begin{bmatrix} x & x+y \\ x+y & y \end{bmatrix}$ with $x = x-v$ and $y = y-w$.

$$\therefore \begin{bmatrix} x-v & (x-v)+(y-w) \\ (x-v)+(y-w) & x-v \end{bmatrix} \in S.$$

Then $S$ is closed under Subtraction.

Let $\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix} \begin{bmatrix} v & v+w \\ v+w & v \end{bmatrix}$

$$= \begin{bmatrix} xv+(x+y)(v+w) & x(v+w)+(x+y)v \\ (x+y)v+x(v+w) & (x+y)(v+w)+xv \end{bmatrix}$$

$$= \begin{bmatrix} xv+xv+yv+xw+yw & xv+xw+xv+yv \\ xv+yv+xv+xw & xv+yw+xw+yv+xv \end{bmatrix}$$

$$= \begin{bmatrix} 2xv + vy + xw + yw & 2xv + xw + yv \\ 2xv + xW + yv & 2xv + yv + xw + yw \end{bmatrix}$$

we observe that is of the form of $\begin{bmatrix} x & x+y \\ x+y & x \end{bmatrix}$

with $x = 2xv + yv + xw + yw$ and $y = -yw$

$$\Rightarrow \begin{bmatrix} 2xv + yv + xw + yw & (2xv + yv + xw + yw) + (-yw) \\ (2xv + yv + xw + yw) + (-yw) & 2xv + yv + xw + yw \end{bmatrix} \in S.$$

Hence, $S$ is closed under multiplication.

weget $S$ is closed under subtraction and multiplication.

Hence $S$ is a subring of $R$.

H/W

7. Let $R = M_2(\mathbb{Z})$ and let $S$ 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 that $S$ is a subring of $R$.

The integers Modulo $n$:

Let $n \in \mathbb{Z}^+$ and $n > 1$. For $a, b \in \mathbb{Z}$

$a \equiv b \pmod n \iff a - b$ is devisible by $n \iff n / (a-b)$

$\iff a = b + tn$, for some $t \in \mathbb{Z}$.

Theorem: $\mathbb{Z}_n$ is a field iff $n$ is a prime.

proof: Let $n$ be a prime, $0 < a < n$

then $\gcd(a, n) = 1$.

$\therefore$ There exists integers $s, t$ with $as + tn = 1$

$\Rightarrow as - 1 = (-t) + n$

$\Rightarrow as - 1$ is divisible by $n$.

$\Rightarrow as \equiv 1 \pmod n$.

(or) $[a][s] = [1]$,

and $[a]$ is a unit of $\mathbb{Z}_n$

Hence $\mathbb{Z}_n$ is a field.

conversely, If $n$ is not a prime,

then $n = n_1 n_2, 1 < n_1, n_2 < n$

so, $[n_1] \neq [0]$ and $[n_2] \neq [0]$

but $[n_1][n_2] = [n_1 n_2] = [0]$

$\mathbb{Z}_n$ is not even an Integral domain.

so it Cannot be a field.

Hence $n$ is a prime.

Theorem:

In $\mathbb{Z}_n$, $[a]$ is a unit iff $\gcd(a,n)=1$.

proof: Given: $\gcd(a,n)=1$

$\Rightarrow as+tn=1$

$\Rightarrow as-1=(-t)n$

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

$\Rightarrow [a][s]=[1]$

$\Rightarrow [a]^{-1}=[s]$

Hence, $[a]$ is a unit of $\mathbb{Z}_n$.

Converse part, Let $[a] \in \mathbb{Z}_n$.

$\Rightarrow [a]^{-1}=[s]$

$\Rightarrow [as]=[a][s]=[1]$

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

$\Rightarrow as = 1+tn, \ t \in \mathbb{Z}$.

But $1 = as + n(-t)$

$\Rightarrow \gcd(a,n)=1$.

1. Determine whether each of the following pairs of integers is congruent Modulo 8. (i) 62, 118 (ii) $-43$, $-237$ (iii) $-90$, $230$.

Solution:

(i) $118-62=56$ is divisible by 8

$\Rightarrow 118 \equiv 62 \pmod{8}$.

(ii) $-43-(-237) \equiv 194$ is not divisible by 8

$\Rightarrow -43 \not\equiv -237 \pmod{8}$

(iii) $230-(-90) = 320$ is divisible by 8

$\Rightarrow 230 \equiv -90 \pmod 8$.

2. Determine the values of the integer $n>1$ for which the congruence is true:

(a) $28 \equiv 6 \pmod n$ (b) $68 \equiv 37 \pmod n$ (c) $301 \equiv 233 \pmod n$

(d) $44 \equiv 3 \pmod n$.

2M

Solution;

a) $28 \equiv 6 \pmod n \Leftrightarrow 28-6$ is divisible by $n$.

$\Leftrightarrow 22 = 2 \times 11$ is divisible by $n$.

$\Leftrightarrow n = 2, 11, 22$.

(b) $68 \equiv 37 \pmod n \Leftrightarrow n$ divides 31 (Prime)

$\Leftrightarrow n = 31$.

(c) $301 \equiv 233 \pmod n \Leftrightarrow n$ divides $301-233 = 68$

$68 = 2 \times 2 \times 17 \Rightarrow n = 2, 17, 4, 34, 68$.

(d) $49 \equiv 2 \pmod n \Leftrightarrow 47$ is divisible by $n$.

$\therefore n = 47$.

3. Determine the last digit of $3^{55}$?

Solution:

$$3^{55} = 3^{32+16+4+2+1}$$

$$3^1 \equiv 3 \pmod{10}$$

$$3^2 \equiv 9 \pmod{10}$$

$$3^4 = 81 \equiv 1 \pmod{10}$$

$$3^{16} = (3^4)^4 \equiv 1^4 \pmod{10}$$

$$3^{32} = (3^{16})^2 = 1^2 \pmod{10}$$

$\Rightarrow 3^1 . 3^2 . 3^4 . 3^{16} . 3^{32} \equiv 3 \times 9 \times 1 \times 1 \times 1 \pmod{10}$.

$\equiv 27 \pmod{10} \equiv 7 \pmod{10}$.

$\therefore$ The last digit of $3^{55}$ is 7.

4. Solve for $x$ the Linear congurence

(i) $3x \equiv 7 \pmod{31}$

(ii) $5x \equiv 8 \pmod{37}$

(iii) $6x \equiv 97 \pmod{125}$

Solution: $3x \equiv 7 \pmod{31}$.

(i) $\gcd(3,31)=1 \Rightarrow [3]^{-1}$ exists in $\mathbb{Z}_{31}$

$$31 = 10\times 3+1 \Rightarrow 1 = 31-10\times 3$$

$$\Rightarrow [1] = [31-10\times 3] = [-10\times 3] = [21\times 3]$$

$$= [21][3]$$

$$\Rightarrow [3]^{-1} = [21]$$

$\therefore$ $3x \equiv 1 \pmod{31} \Rightarrow x \equiv 21 \pmod{31}$

Hence, $3x \equiv 7 \pmod{31} \Rightarrow x \equiv 147 \pmod{31}$

$\Rightarrow x \equiv 23 \pmod{31}$.

(ii) $5x \equiv 8 \pmod{37}$.

$\gcd(5,37)=1 \Rightarrow [5]^{-1}$ exists in $\mathbb{Z}_{37}$.

We have: $\left.\begin{array}{l} 37 = 7\times 5+2 \\ 5 = 2\times 2+1 \end{array}\right\} \Rightarrow 1 = 5-2\times 2$

$$= 5-2(37-7\times 5)$$

$$= 15\times 5 - 3\times 37$$

$$\Rightarrow [1] = [15\times 5 - 3\times 37] = [15\times 5] = [15][5]$$

$$\Rightarrow [5]^{-1} = [15]$$

$\therefore$ $5x \equiv 1 \pmod{37} \Rightarrow x \equiv 15 \pmod{37}$.

Hence, $5x \equiv 8 \pmod{37} \Rightarrow x \equiv 120 \pmod{37}$

$\equiv 9 \pmod{37}$

(iii) $6x \equiv 97 \pmod{125}$:

$\gcd(6,125)=1 \Rightarrow [6]^{-1}$ exists in $\mathbb{Z}_{125}$

$$\begin{array}{r|l} & \;\;3 \\ 37 & 120 \\ & 111 \\ \hline & \;\;9 \end{array}$$

We have,

$$\left.\begin{array}{l} 125 = 20\times 6+5 \\ 6 = 1\times 5+1 \end{array}\right\} \Rightarrow 1 = 6-1\times 5$$

$$= 6-1(125-20\times 6)$$

$$= 21\times 6-125$$

$$\Rightarrow [1] = [21\times 6-125] = [21\times 6]$$

$$= [21][6]$$

$$\Rightarrow [6]^{-1} = [21].$$

$$\begin{array}{r|l} & 16 \\ \hline 125 & 2037 \\ & \underline{125} \\ & 787 \\ & \underline{750} \\ & 37 \end{array}$$

$\therefore$ $6x \equiv 1 \pmod{125} \Rightarrow x \equiv 21 \pmod{125}$.

Hence, $6x \equiv 97 \pmod{125} \Rightarrow x \equiv 21\times 91 \pmod{125}$

$$\equiv 2037 \pmod{125}$$

$$x \equiv 37 \pmod{125}$$

5. Find $[25]^{-1}$ in $\mathbb{Z}_{72}$.

Solution:

25 and 72 are prime numbers.

$\therefore$ The gcd $(25, 72) = 1$.

By Euclidean algorithm,

$72 = 2(25)+22, \quad 0<22<25 \rightarrow ①$

$25 = 1(22)+3, \quad 0<3<22 \rightarrow ②$

$22 = 7(3)+1, \quad 0<1<3. \rightarrow ③.$

As 1 is the last non-zero remainder,

$1 = 22-7(3)$ by (3)

$= 22-7[25-1(22)]$ by ②

$= 22-7(25)+7(22)$

$= 8(22)-7(25)$

$= 8[72-2(25)]-7(25)$ by ①

$= 8(72)-23(25).$

$\Rightarrow 1-[-23(25)] = 8(72).$

⇒ L.H.S is divisible by 72.

$\Rightarrow 1 \equiv (-23)(25)$

$\equiv (-23+72)(25) \bmod 72$ [∵ −23 is negative]

$\Rightarrow \quad \equiv (49)(25) \bmod 72.$

$\Rightarrow [1] = [49][25].$

$\Rightarrow [25]^{-1} = [49]$ in $\mathbb{Z}_{72}$.

H.W

1. Find $[17]^{-1}$ in the ring $\mathbb{Z}_{1009}$
2. Find $[100]^{-1}$ in the ring $\mathbb{Z}_{1009}$
3. Find $[777]^{-1}$ in the ring $\mathbb{Z}_{1009}$.

Ring Homorphorphism:

Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be rings.

A function $f : R \to S$ is called a ring homomorphism if for all $a, b \in R$.

(a) $f(a+b) = f(a) \oplus f(b)$ and

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

When the function $f$ is onto we say that $S$ is a homomorphic image of $R$.

A homomorphism which is both one-one and onto is called an isomorphism.

Scanned with CamScanner