Groups

Algebraic Structure →

A nonempty set S is called an algebraic structure w.r.t the binary operation '$*$' if $(a*b) \in S$ $\forall$ $a,b \in S$

i.e. $*$ is a closure operation on S.

The algebraic structure is denoted by '$(S,*)$'.

$N = \{1, 2, 3, 4, \ldots \infty\}$

$Z =$ Set of all integers
$= \{0, \pm 1, \pm 2, \pm 3, \ldots \infty\}$

$Q =$ Set of all rational numbers.
$R =$ Set of all real nos.
$C =$ set of all complex nos.

ex → 1) $(N,+)$ is an algebraic structure.
$(a+b) \in N$, $\forall$ $a,b \in N$.

2) $(N, \cdot)$ is an algebraic structure.
$(a \cdot b) \in N$ $\forall$ $a,b \in N$.

3) $(N, -)$ is not an algebraic structure.
$(2-3) \notin N$

4) $(Z, -, +, \cdot)$ is an algebraic structure.
$(2-3) \notin N$ but $(2-3) \in Z$.

5) $(Z, \div)$ is not an algebraic structure.
$(2 \div 3) \notin Z$.

6) $(\mathbb{Q}, \div)$ is not an algebraic structure.
$(1 \div 0) \notin \mathbb{Q}$

So, Let $\mathbb{Q}^* = (\mathbb{Q} - \{0\})$ = set of all nonzero rational nos.

7) $(\mathbb{Q}^*, \div)$ is an algebraic structure.
$(a \div b) \in \mathbb{Q}^*$

Semi-Groups →

An algebraic structure $(S, *)$ is called a semigroup if
$(a*b)*c = a*(b*c) \;\; \forall a, b, c \in S$.
i.e. $*$ is associative on S

ex → 1) $(N, +)$ is a semigroup
$(a+b)+c = a+(b+c) \;\; \forall a, b, c \in N$
i.e. $+$ is associative on N.

2) $(N, *)$ is a semigroup. multiplication $(\cdot)$
$(a \cdot b) \cdot c = a \cdot (b \cdot c) \;\; \forall a, b, c \in N$.

3) $(Z, -)$ is not a semigroup.
$(a-b)-c \neq a-(b-c)$

4) $(\mathbb{Q}^*, +)$ is not a semigroup. (where $\mathbb{Q}^* = \mathbb{Q} - \{0\}$)
$a + (-a) = 0 \notin \mathbb{Q}^* \;\; \forall a \in \mathbb{Q}^*$

5) $(\mathbb{Q}^*, \cdot)$ is a semigroup.

Monoid →

A semigroup $(S,*)$ is called a monoid if there exists an element $e \in S$ such that

$(a*e) = (e*a) = a \quad , \forall a \in S$

The element e is called identity element of S w.r.t. $*$

ex→ 1) $(N, \cdot)$ is a monoid, with identity element $1 \in N$.
$(a \cdot 1) = a \quad \forall a \in N$

2) $(N, +)$ is not a monoid, as $0 \notin N$.

3) $(Z, +)$ is a monoid, as $0 \in Z$.

Group →

A monoid $(S,*)$ with identity element e is called a group if to each element $a \in S$, there exists an element $b \in S$, such that

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

then b is called inverse of a denoted as a^{-1}
$\therefore a^{-1} = b$ and $b^{-1} = a$.

ex → 1) $(Z, +)$ is a group.
$a + (-a) = 0$. So, $a^{-1} = (-a)$.

2) $(Q, \cdot)$ is not a group.

$a \cdot (1/a) \neq 1$ for $a = 0 \in Q$.

So, inverse does not exist for 0.

3) $(Q^*, \cdot)$ is a group. $(\because Q^* = Q - \{0\})$
(with identity element 'e')

→ In a group $(G, *)$; the following properties, with, the following properties must hold good →

1) The identity element of G is unique.

2) The inverse of any element in G is unique.

3) The inverse of identity element e is e itself.

4) Cancellation laws

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

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

5) $(a * b)^{-1} = (b^{-1} * a^{-1})$ $\forall a, b \in G$.

Abelian Group (Commutative Group) →
A group $(G, *)$ is said to be abelian if $(a * b) = (b * a)$ $\forall a, b \in G$.

ex → 1) $(Z, +)$ is an abelian group.
$(a + b) = (b + a)$ $\forall a, b \in Z$.

2) $(R^*, \cdot)$ is an abelian group. (where $R^* = R - \{0\}$)

1) Set of all nonsingular matrices of order $n \times n$ is a group w.r.t. matrix multiplication, but not an abelian group because matrix multiplication is not commutative.

$(A \cdot B)$ and $(B \cdot A)$ may or may not be equal.

2) Set of all bijections on a finite set A is a group w.r.t. function composition $\circ$, but not an abelian group because function composition is not commutative.

$I : A \to A$ so, $(f \circ I) = f$ so identity funcn exists.

$(f \circ g) = A \to A$ it is associative also.

But, in general, $\boxed{(f \circ g) \neq (g \circ f)}$. So, it is not commutative.

Q. which of the following is/are true?

S1) In a group $(G, *)$ with an identity element 'e', if $a * a = a$, then $a = e$ true

→ suppose, $a * a = a$

$\Rightarrow \cancel{a} * a = \cancel{a} * e$ $(\because a = e)$

$\therefore \boxed{a = e}$ (by left cancellation law).

S2) In a group $(G, *)$, if $x^{-1} = x \ \forall x \in G$, then G is abelian group. true.

→ we have, $(a * b)^{-1} = (b^{-1} * a^{-1}) \ \forall a, b \in G$

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

$(a+b)^2$
$(a \cdot b)^2$
$a^2 \cdot b^2$

7/11/13

$\therefore$ G is abelian group.

Q) In a group $(G, *)$, if $(a*b)^2 = a^2 * b^2$ $\forall a, b \in G$, then G is abelian group: true

$\rightarrow$ $a^2 = a*a$, $a^3 = a*a*a$

Given that $(a*b)^2 = a^2 * b^2$ $\forall a, b \in G$

$\Rightarrow$ $(a*b)*(a*b) = (a*a)*(b*b)$

$\Rightarrow$ $\cancel{a}*(b*a)*\cancel{b} = \cancel{a}*(a*b)*\cancel{b}$ (by associative law)

$\Rightarrow$ $(b*a) = (a*b)$

$\therefore$ G is an abelian group.

3.2. If $A = \{1, 3, 5, 7, 8, \ldots \infty\}$ and $B = \{2, 4, 6, 8, 10, \ldots \infty\}$. which of the following is not a semigroup?

✓a) $(A, +)$ b) $(A, \cdot)$ c) $(B, +)$ d) $(B, \cdot)$

(ex. $1+3=4 \notin A$)

$\rightarrow$ closure property fails for a. i.e. $(a+b) \in A$ $\forall a, b \in A$.
$\therefore$ $(A, +)$ is not a semigroup and also not a algebraic structure.

Q.3. Let $A = \{1, 2, 3, 4, 5, 6, \ldots \infty\}$, then and a binary operation $*$ is defined by $a*b = a^b$ $\forall a, b \in A$: which of the foll. is true?

a) $(A, *)$ is a semigroup but not a monoid.

b) $(A, *)$ is a monoid but not a group.

c) $(A, *)$ is a group

✓d) $(A, *)$ is not a semigroup. ✓(Associative prop. fails).

→ we have, $(a*b) = a^b \ \forall\ a,b \in A$.
and $*$ is a closed operation on A.

$(a*b)*c = (a^b)*c = (a^b)^c = a^{bc}$ $\quad a*(b*c) = a*(b^c)$
$= d^c \quad (\because a^b = d)$ $\quad = (a)^{(b^c)} = a^{b^c}$
$= a^e \quad \because e = b^c)$

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

$\therefore *$ is not associative operation on A.

$\therefore$ (A,*) is not a semigroup.

Q.4. Let $A = \{x \mid 0 < x \leq 1$ and x is a real no.$\}$, then A w.r.t. multiplication is

a) A semigroup but not a monoid.

✓b) A monoid but not a group.

c) A group.

d) Not a Semigroup.

→ • is a closed operation on A.
• is an associative operation on A.
1 is an identity element in A

$\therefore$ (a monoid but not a group)

w.r.t. multiplication, inv. of any element of A except 1 does not exist.

a * 0.1 (10) $\frac{1}{10.1}$ 0.1 (a * b)(b * a) = (1) $\frac{1}{0.1}$ * 0.1 = 0.1

-5. Let A = set of all integers and a binary operation * is defined by (a * b) = min (a, b). Then (A, *) is

Same options.

→ * is a closed operation on A.

also * is an associative operation on A.

→ ∵ (a * b) * c = a * (b * c)

Let e be the identity element

∴ a * e = a (by defn of identity element).

min (a, e) = a ∀ a, e ∈ A

Here, e should be a greatest integer. But the greatest integer does not exist.

∴ (A, *) is a semigroup but not a monoid.

-6. Let S = set of all bit strings including the null string ε. '+' denotes string concatenation. (S, +) is

a) a semigroup but not a monoid.

b) a monoid but not a group.

c) a group.

d) not a semigroup.

→ + is a closed operation on S. (∵ 101 + 1101 = 1011101.)

$a+(b+c) = (a+b)+c$ ($\because$ $101 + 1101 = 101\,1101 + 11 = \underline{10111011}$ } same.
& $101 + (1101+11) = 101 + 110111 = \underline{10111011}$)

$\therefore$ + is associative on S.

ϵ is the identity element in S.

But inverse of a nonempty bit string does not exist w.r.t. '+'.
($\because$ String + String $\neq \epsilon$ for any string).

$\therefore$ (S,+) is a monoid but not a group.

7. Let A = set of all +ve rational pos. and a binary operation * is defined by $(a*b) = \frac{a \cdot b}{3}$ $\forall a,b \in A$. then which of the foll. statements are true?

✓S1) (A, *) is a group.

✓S2) The identity element of A w.r.t * is 3

✓S3) The inverse of $a = \frac{3}{a}$ $\forall a \in A$.

→. We have, $(a*b) = \frac{a \cdot b}{3} \in A$ $\forall a,b \in A$.

$\therefore$ * is a closed operation on A.

$a*(b*c) = a * \frac{bc}{3} = \frac{abc}{9}$. $\quad (a*b)*c = \frac{ab}{3} * c = \frac{abc}{9}$.

$\therefore$ * is an associative operation on A.

Let e be the identity element.
$\therefore a*e = a$ $\forall a \in A$. $\therefore \frac{a \cdot e}{3} = a$ $\therefore \boxed{e = 3}$.

$a \times 14 .$ 379

$\frac{9}{3/2}$ $a * c\ b+c+bc)$ $a+b+c+bc+abc.$ $a = 3/a.$

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

$\frac{a \cdot a^{-1}}{3} = 3.$ $\therefore \boxed{a^{-1} = \frac{9}{a}} \in A.$

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

Q.8. Let A = set of all real nos. $*$ be a binary operation $(a*b) = a+b+ab$ then which of the foll. are true?

S1) $(A,*)$ is a group.

S2) The identity element of A w.r.t. $*$ is -1.

S3) The inverse of $2 = -2/3$.

→ $*$ is a closed operation on A.

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

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

$a*(b*c)$

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

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

$\therefore$ $*$ is an associative operation on A.

Let e be the identity element.

$\therefore a*e = a. \quad \forall a \in A. \quad \cancel{a}+e+a\cdot e = \cancel{a}. \quad \forall a \in A$

$e(1+a) = 0.$

$\therefore \boxed{e=0}$

Let a^{-1} = inv. of a $\forall a \in A.$

$\therefore a * a^{-1} = e$ $\therefore a * a^{-1} = 0.$

$\therefore a + a^{-1} + a \cdot a^{-1} = 0.$

$\therefore \boxed{a^{-1} = \frac{-a}{a+1}}$

But (it is not true for $a = -1$.)
(inv. for -1 does not exist).
$\therefore (A,*)$ is not a group.

9. which of the following is not a group?

a) $\{0, \pm 2, \pm 4, \pm 6, \dots \infty\}$ wrt '+'.

→ The set is abelian group wrt '+'.

b) $\{0, \pm k, \pm 2k, \pm 3k, \dots \infty\}$ wrt '+'

→ This set is an abelian group wrt '+'.

c) $\{2^n : n$ is an integer $\}$ wrt multiplication '($\cdot$)'

→ $2^a \cdot 2^b = 2^{a+b} = 2^c$. ∴ is closed on given set.

$2^a \cdot (2^b \cdot 2^c) = (2^a \cdot 2^b) \cdot 2^c$ ∴ is associative on given set.

$2^0 = 1$ e identity element ∈ set.

$2^a \cdot 2^{-a} = 1$. ∴ ∀ a ∈ set, inverse exists.

∴ The given set $(S, \cdot)$ is a group

Also, $(2^a \cdot 2^b) = (2^b \cdot 2^a)$. ∴ S is an abelian group.

d) Set of all complex nos. wrt. multiplication.

→ S = $\{a+ib \mid a$ and b are real nos.$\}$.

0 is also complex no. Inv. of $(a+ib) = \frac{1}{a+ib}$

∴ Inv. of 0 does not exist.

∴ S is not a group.

(a+1))
(a+ib) (a+ib)
a + b +

Finite Groups →

A group with finite no. of elements is called a finite group.

Order of a finite group $(G, *)$ denoted by $O(G)$ is "no of elements in (G)".

e.g. 1) If a group has only one element, then it is the identity element of the group.

ex → $S = \{0\}$ is a group of order 1 w.r.t addition operation because 0 is identity element w.r.t addition.

2) The only finite group of real nos. w.r.t addition is the $S = \{0\}$.

3) $S = \{1\}$ is a group of order 1 w.r.t multiplication because 1 is identity element w.r.t multiplication.

Also, $S = \{1, -1\}$ is a finite group w.r.t multiplication.

4) composition table →

$\cdot$	1	-1
1	1	-1
-1	-1	1

Identity element. entries.

Inv. of $1 = 1$
Inv. of $-1 = -1$

5) In general, For a group of order 2, $G = \{a, b\}$.

com position table →

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

Identity element.

Inv of $a = a$
Inv. of $b = b$.

∴ For a group G of order 2, Inv. of $a = a$ $\forall a \in G$.

6) The only finite groups of reals nos. w.r.t multiplication are $\{1\}$ and $\{1,-1\}$.

ex→1) The cuberoots of unity, $G = \{1, \omega, \omega^2\}$ is an abelian group w.r.t multiplication.

→ $\omega = \left(\frac{-1+\sqrt{3}i}{2}\right)$. $\omega^2 = \left(\frac{-1-\sqrt{3}i}{2}\right)$

$\omega^3 = 1$

Composition table →

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	ω^3 1
ω^2	ω^2	1	ω

Identity element → 1

Inv. of $1 = 1$
Inv of $\omega = \omega^2$
Inv of $\omega^2 = \omega$

2) The fourth roots of unity $G = \{1, -1, i, -i\}$ is a group. w.r.t multiplication.

→

composition table →

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	+1	$-i$	i
i	i	$-i$	$i^2 = -1$	$-i^2 = 1$
$-i$	$-i$	i	$-i^2 = 1$	$i^2 = -1$

identity element → 1

$i^2 = -1$
$-i^2 = 1$

∴ Inv. of $1 = 1$
Inv. of $-1 = -1$
Inv. of $i = -i$
Inv. of $-i = i$

* Note→ The nth roots of unity is a group w.r.t. multiplication ∵ $n = 1, 2, 3, \ldots$

Addition Modulo m ($\oplus_m$) →

$\oplus_m$, where, 'm' is +ve integer.

If a and b are any two +ve integers, then $a \oplus_m b$ is given as,

$a \oplus_m b = a+b$, if $(a+b) < m$

$= r$, if $(a+b) \geq m$ where r is the remainder obtained by $\frac{(a+b)}{m}$.

Ex → $m = 6$

1) $2 \oplus_6 3 = 5$ 2) $4 \oplus_6 3 = 7 \% 6 = 1$ 3) $5 \oplus_6 1 = 6 \% 6 = 0$.

4) $4 \oplus_6 5 = 9 \% 6 = 3$.

Ex → Set $S = \{0, 1, 2, \dots, m-1\}$ is a group w.r.t. $\oplus_m$.

Multiplication modulo m $\otimes_m$ →

If a and b are any two +ve integers, then $a \otimes_m b$,

$a \otimes_m b = a \cdot b$, if $a \cdot b < m$

$= r$, if $a \cdot b \geq m$ where $r = \frac{a \cdot b}{m}$

The set $S = \{1, 2, 3, 4, 5, 6\}$ is a group wrt $\otimes_7$

2 If n is a +ve integer, then the set 'S_n' is defined as,

S_n = set of +ve integers which are $\leq n$ and relatively prime to n.

GCD of $\{a, b\} = 1$ ⇒ a, b are relatively prime.

ex →
∴ $S_6 = \{1, 5\}$ $S_8 = \{1, 3, 5, 7\}$. $S_{15} = \{1, 2, 4, 7$

euler function

$5\times3 = 15$

$5\times5 \to 25\%8 = 1$

If n is a positive integer then S_n is a group w.r.t. $\otimes_m$

Q. If $G = \{1, 3, 5, 7\}$ is a group w.r.t. $\otimes_8$, which of the following is not true?

a) The inv of 1 is 1. true

b) The inv of 3 is 3. true

c) The inv of 5 is 7 false.

d) The inv of 7 is 7. true.

If and

given as,

-12.

13. which of the following is a group ?

a) $\{1,2,3,4,5\}$ w.r.t. $\otimes 6$.

→ It is not a group because the binary operation is not a closure operation. $2 \otimes_6 3 = \underline{0} \notin$ set.

b) $S = \{0,1,2,3,4,5\}$ w.r.t. $\otimes 6$.

→ In the given set, inv. of 0 does not exist. w.r.t. $\otimes 6$.
$\therefore S$ is not a group.

c) $S = \{\cancel{0},1,2,3,4,5,6\}$ w.r.t. $\otimes 7$.

→ It is a group.

d) $S = \{1,2,3,4,5,6\}$ w.r.t. $\oplus 7$.

→ not a group. No identity element.

Order of an element of a group →

Let $(G, *)$ be a group. And $a \in G$, then

order of element a = $O(a)$ = the smallest +ve integer n such that a^n = identity element.

In a group, order of identity element is always ①

Ex. → 1) $G = \{1, -1\}$ is a group w.r.t multiplication.

→ $O(1) = 1$ $\quad 1^n = 1$

$O(-1) = 2$. $\quad (-1)^n = (-1)^2 = 1$

2) $G = \{1, \omega, \omega^2\}$ is a group w.r.t multiplication.

→ $O(1) = 1$

$O(\omega) \Rightarrow (\omega)^n = 1 \quad \therefore n = 3$.

$O(\omega^2) \rightarrow (\omega^2)^n = 1 \quad \therefore n = 3$.

3) $G = \{1, -1, i, -i\}$ is a group w.r.t multiplication.

→ $O(1) = 1$

$O(-1) = 2$

$O(i) \Rightarrow (i)^n = 1 \quad \therefore n = 4$.

$O(-i) = 4$.

$\therefore \boxed{O(G) = 4.}$

Note → 1) In a finite group $(G, *)$, $O(a)$ is a divisor of $O(G)$ $\forall a \in G$.

2) $O(a) = O(a^{-1}) \quad \forall a \in G$.

$\oplus_m$ $-1+1$ 2×2 $3+3$ $3\,3\,3\,3$ $1 \oplus 1 \oplus 1 \oplus 1 \oplus 1$ $2\times2\times2\times2$ $4 \oplus 3 \oplus_m^2$ 8^n

Q.14. Set $S = \{0, 1, 2, 3\}$ is a group w.r.t. $\oplus_4$.

→ $O(0) = 1$

$O(1) = 4$ $\quad 1 \oplus_4 1 \oplus_4 1 \oplus_4 1$

$O(2) = 2$ $\quad 2 \oplus_4 2$

$O(3) = 4.$ $\quad 3 \oplus_4 3 \oplus_4 3 \oplus_4 3.$

Q.15. Set $S = \{1, 2, 3, 4\}$ is a group w.r.t. $\otimes_4$.

→ $O(1) = 1$ $\quad 1^n = 1$ $\quad n = 1$

$O(2) = 4$ $\quad 2^n = 1$ $\quad 2 \otimes_4 2 \otimes_4 2 \otimes_4 2 = 1.$

$O(3) = 4$

$O(4) = 2$

Q.16. which of the foll. statements is/are true ?

S1) In the group $(Z, +)$, the order of any element except 0 does not exist. true.

→ $a^n = a$. i.e. $\underbrace{a + a + a + \cdots + a}_{n \text{ times}} = 0$. ∈ not possible for any $a \neq 0$.

S2). In the group $(Q^*, \cdot)$ where Q^* is a set of all nonzero rational nos. i.e $Q^* = Q - \{0\}$, the order of any element except 1 does not exist. False.

→ $O(-1) = 2$ it exists. So, the given statement is false.

Subgroups →

Let $(G, *)$ be a group. A subset H of G is called a subgroup of G if $(H, *)$ is a group.

Note → Let $(G, *)$ be a group with identity element e, then $\{e\}$, and G are the trivial subgroups of G.

Any other subgroup (which is not a trivial subgroup) of G is called proper subgroup of G.

Ex → $G = \{1, -1, i, -i\}$ w.r.t. multiplication is a group, then $H = \{1, -1\}$ is a proper subgroup of G.

Theorem 1 →

Let H be a nonempty subset of a group $(G, *)$. H is a subgroup of G iff $(a * b^{-1}) \in H$ $\forall a, b \in H$

Theorem 2 →

Let H be a non empty finite subset of a group $(G, *)$. H is a subgroup of G iff $(a * b) \in H$ $\forall a, b \in H$.

Theorem 3 → (Lagrange's theorem) →

If H is a subgroup of a finite group $(G, *)$, then $O(H)$ is a divisor of $O(G)$.

The converse of the above theorem need not be true.

Q.17. Let $G = \{0, 1, 2, 3, 4, 5\}$ is a group w.r.t. $\oplus_6$. which of the foll. is/are subgroups of G?

a) $H_1 = \{1, 3\}$.

$\oplus_6$	1	3
1	2	4
3		

$4 \notin H$.

∴ closure property fails. ∴ Not a subgroup

b) $H_2 = \{1, 5\}$.

$\oplus_6$	1	5
1	2	0. $\notin H$.
5		

$\therefore H_2$ is not a subgroup.

c) $H_3 = \{0, 3\}$

$\oplus_6$	0	3
0	0	3
3	3	0

$\} \in H$. $\therefore H_3$ is a subgroup.

d) $H_4 = \{0, 2, 4\}$

$\oplus_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$\} \in H$ $\therefore H_4$ is a subgroup.

e) $H_5 = \{0, 2, 3, 5\}$ $2 \oplus_6 2 = 4 \notin H$ $\therefore H_5$ is not a subgroup.
H_5 is not a subgroup as $O(H_5)$ is not a divisor of $O(G)$.

18. Let $G = \{1, 2, 3, 4, 5, 6\}$ is a group w.r.t $\otimes_7$. which of the foll. are subgroups of G?

a) $H_1 = \{1, 6\}$

$\otimes_7$	1	6
1	1	6
6	6	1

$\} \in H_1$. $\therefore H_1$ is a subgroup.

b) $H_2 = \{1, 2, 4\}$

$\otimes_7$	1	2	4
1	1	2	4
2	2	4	1
4	4	1	2

$\in H_2$ $\therefore H_2$ is a subgroup.

c) $H_3 = \{1, 3, 5\}$. $3 \otimes_7 3 = 2 . \notin H_3$. $\therefore H_3$ is not a subgroup.

d) $H_4 = \{1, 2, 3, 5\} \rightarrow$ A subset with 4 elements cannot a subgroup of G. (lagrange's thm).

19. Let $(G, *)$ be a group of order p where p is a prime no.
No. of proper subgroups in G is ?

→ Let H be a proper subgroup of G with n elements.
By Lagrange's thm, n is a divisor of p. which implies
$\Rightarrow$ $n = 1$ or $n = p$ ($\because$ p is a prime no)
$\downarrow$ $\downarrow$
$\Rightarrow$ $\because \underbrace{H = \{e\} \text{ or } H = G}_{\text{trivial subgroups.}}$

$\therefore$ The only subgroups of G are trivial subgroups. Therefore, no. of proper subgroups in $G = 0$

20. Which of the foll. statements is not true?

a) The union of any two subgroups of a group G is also a subgroup of G. False.
→ We have counte example.
for group $G = \{1, 3, 5, 7\}$ w.r.t. $\otimes_8$.

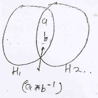
$H_1 = \{1, 3\}$ w.r.t. $\otimes_8$.
$H_2 = \{1, 5\}$ w.r.t. $\otimes_8$. $\Big\}$ subgroups.

$\because H_1 \cup H_2 = \{1, 3, 5\}$ w.r.t. $\otimes_8$. as $3 \otimes_8 5 = 7 \notin H_1 \cup H_2$.

$\therefore$ $H_1 \cup H_2$ is not a subgroup of G.

b) The intersection of any two subgroups of group G is also a subgroup of G. True

$\rightarrow$ $a, b \in (H_1 \cap H_2)$



$(a * b^{-1}) \in H_1$, $(a * b^{-1}) \in H_2$

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

$\therefore$ $H_1 \cap H_2$ is also a subgroup of G.

c) The union of two subgroups H1 and H2 of a group $(G, *)$ is also a subgroup of G. true

$\rightarrow$ true when $(H_1 \subseteq H_2)$ or $(H_2 \subseteq H_1)$.

d) Every subgroup of an abelian group is also an abelian group.

$\rightarrow$ $(G, *)$, H is a subgroup. true

$a, b \in H$

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

$\Rightarrow$ $(a*b) = (b*a)$ $\therefore$ H is also abelian.

Cyclic Groups $\rightarrow$

A group $(G, *)$ is said to be cyclic if there exists an element $a \in G$ such that every element of G can be written as a^n for some integer n; then a is called generating element / Generator of group G.

ex $\rightarrow$ 1) $G = \{1, -1\}$ is a cyclic group of order 2 w.r.t. multiplication.

The generator of $G = -1$.

2) $G = \{1, \omega, \omega^2\}$ is a cyclic group w.r.t. multiplication.

$\therefore$ The generator of $G = \omega, \omega^2$ $\leftarrow$ two generators.

1) $G = \{1, -1, i, -i\}$ is a cyclic group w.r.t multiplication
The generators are i and $-i$

Note: If $(G, *)$ is a cyclic group with generator a then

i) a^{-1} is also a generator of G

ii) $\boxed{\text{the order of the generator} = O(G)}$ ← for a cyclic group G.

2) $G = \{0, 1, 2, 3\}$ is cyclic group with resp. to $\oplus_4$.
The generators are 1 and 3

→ 2 cannot be a generator as $O(2) \neq (O(G) = 4)$.

3. $G = \{1, 2, 3, 4\}$ is a cyclic group w.r.t $\otimes_5$. The generators are 2 and 3.

→ $4^2 = 1$ ∴ $O(4) \neq O(G) = 4$.
∴ 4 is not a generator.

P129-1x-

Theorem →
Let $(G, *)$ be a cyclic group of order n with generator a, then
i) the no of generators in $G = \phi(n)$. ← Euler funcn of n

ii) a^m is also a generator of G if $GCD(m, n) = 1$

$a\ a^3 \cdot a^5\ a^7$ S_8 $1, 3, 5, 7$ 8 $1, (2, 3, 5), 8$

$1, 2, 3, 5, 8.$

23. Let $(G, *)$ be a cyclic group of order 8 with generator a.
i) Number of generators in G = ?
ii) Which of the foll. is not a generator of G ?
a) a^2 b) a^3 c) a^5 d) a^7.

→ $S_8 = \{1, 3, 5, 7\}$.

∴ There are 4 generators of G → a, a^3, a^5, a^7.

a^2 is not a generator of G

24. " " of order 84.

→ $S_{84} = \{ ? \}$.

$$\therefore = 84\left\{\frac{(2-1)(3-1)(7-1)}{2 \times 3 \times 7}\right\}$$

$2 \mid 84$, $2 \mid 42$, $3 \mid 21$, 7.

= 24 generators are there.

Q.25. $G = \{1, 2, 3, 4, 5, 6\}$ is a cyclic group w.r.t. $\otimes_7$. How many generators ? what are they ?

→ $o(G) = 6$. ∴ No. of generators of groups $= S_6 = \{1, 5\}$ $= 2$

$3 \to$
$3^2 = 2$ 3×2
$3^3 = 6$ $6 \times 3 = 18$
$3^4 = 4$ $4 \times 3 = 12$
$3^5 = 5$ $3 \times 5 = 15$
$3^6 = 1$

and 5 is an inverse of 3

∴ 5 is also generator

∴ 3 is a generator.

26. Let $G = \{0,1,2,3,4\}$ is a cyclic group w.r.t. $+_5$. How many generators are there and what are they?

→ $S_5 = \{1,2,3,4\}$.

$\phi(5)$.

∴ No. of generators = 4.

∴ (1,2,3,4) are generators.

27. Let $G = \{1,3,5,7\}$ is a group w.r.t. $\times_8$. but not a cyclic group → because there is no generator for G.

28. The composition table of a cyclic group $G = \{a,b,c,d\}$ w.r.t. $*$ is shown below.

*	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

identity element (e) → c

→ We can generate all other elements from a.
So, a is generator and d is inv of a.

∴ d is also a generator.

29. The incomplete composition table of a group $G = \{a,b,c,d\}$ w.r.t. $*$ is shown below.

*	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b.

The last row is

c a d b.

Any group of order ≤ 5 is abelian group and in the composition table of abelian group, the corresp. rows & columns are identical.

11/13

→ For cyclic groups, following properties hold good →

1) Every cyclic group is abelian.

Let $(G, *)$ be a cyclic group and x be the generator.

$\therefore \boxed{a * b} \Rightarrow x^m * x^n = x^{m+n} = x^{n+m} = x^n * x^m$

$= \boxed{b * a.}$

2) Every group of prime order is cyclic. and so, every group of prime order is abelian group.

3) Every subgroup of a cyclic group is also cyclic. but the generator of the subgroup need not be same as that of the cyclic group.

ex → $G = \{1, -1, i, -i\}$; $H = \{1, -1\}$. So, H is subgroup of G.

Generators of $G = i, -i$; Generator of $H = -1$.

4) Let $(G,*)$ be a group of even order, then there exists at least one element $a \in G$ $(a \neq e)$ such that $a^{-1} = a$

ex → 1) $G = \{1, -1\}$, inv. of $1 = 1$, inv. of $-1 = -1$.

2) $G = \{a, b, c, d\}$, inv. of $a = a$ (identity ele.), inv. of $b = c$

So, inv. of $d = d$.

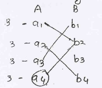
Functions

Function →

A relation 'f' from a set A to a set B is called a function if to each element $a \in A$, we can assign an unique element B.

It is denoted by $f : A \to B$.

ex →



✓ Function

A: Domain of f

B: Codomain of f.

Ran

Range of the function : $\{y \mid y \in B \text{ and } (x,y) \in f\}$

So, range of function f is always a subset of the codomain.

$\therefore$ Ran $f \subseteq B$.

A function $f : A \to A$ is called a function on A.

n^{m} 3 4 $\frac{164}{256}$ $\frac{65535 - 256}{65279}$ 2^8 . 2^{16} 3^3

If no. of elements in A, $|A| = m$ and $|B| = n$, then no. of functions possible from A to B are (n^m)

If no. of elements in A, $|A| = n$, then no. of functions possible on A $= (n^n)$

Q.1. If $A = \{a, b, c, d\}$, then no. of relations on A which are not functions ?

→ No. of functions $= n^n$.
No. of relations $= 2^{(n^2)}$.

∴ No. of relations which are not functions $= (2^{16} - (4^4))$
$= \boxed{65279}$.

Q.2. If there are exactly 81 functions possible from set A to set B, then which of the following statements is not true?

a) $|A| = 4$ $|B| = 3$. true $3^4 = 81$.

b) $|A| = 2$ $|B| = 9$ true $9^2 = 81$

c) $|A| = 1$ $|B| = 81$ true. $(81)^1 = 81$.

d) $|A| = 9$ $|B| = 9$ false $(9)^9 \neq 81$

Q.3. which of the following is a function if domain is set of all real nos.

× a) $f(x) = 1/x$ $f: R \to B$.   ∵ element 0 in R is not mapped to any no in B.
$0 \to ?$

∴ Not a function.

-1 +1 1111 → 1, 3 4.

× b) $g(x) = \sqrt{x}$ It is not a function because the -ve real nos. in the domain are not mapped to any element in codomain.

× c) $h(x) = \pm\sqrt{x^2+1}$ It is not a function because for each real no., we have two images (+/-).

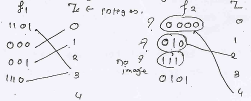
✓d) $\phi(x) = |x|$. It is a function

4. Consider the following relations from set of all bit strings to set of all integers.

$f_1(s)$ = The no. of 1 bits in the bit string s

$f_2(s)$ = The position of a 0 bit in the bit string s.
which of the above relations are functions?

→ f_1 is a function because the no. of 1 bits in a bitstream is a nonnegative integer.



f_2 is not a function because a bit string with 2 or more 0's will have two or more images.

110101 = 11101 → 25

x^2 4. $\sqrt{x}$, $\sqrt{4}$. $\sqrt{81}$ ± 9.

5. which of the foll. relations on set A is a function.

$A = \{a, b, c\}$.

a) $R_1 = \{(a, b), (b, c), (a, c)\}$ → a has 2 images.
∴ Not a function.

b) $R_2 = \{(a, a), (b, a)\}$ → the ele. c has no image.
∴ Not a function.

c) $R_3 = \{(a, c), (b, c), (c, a)\}$ → It is a function.

6. which of the foll. statements is/are true?

S1) There exists an equivalence relation which is also a function.
true.

A → A
1 — 1
2 — 2
3 — 3

Diagonal relation on A. AA
∴ the statement is true

equival. relatn as well as a func^n.

S2) The functions $f(x) = x$, $g(x) = \sqrt{x^2}$ are identical.
→ two functions are identical if they have same domain and codomain. false

Range of $f(x)$ = set of all real nos. i.e. $-\infty$ to $+\infty$
whereas, range of $g(x)$ is only 0 to ∞. (+ve)

∴ these two functions are not identical.

S3) $f(x) = \log_e(x^2)$ and $g(x) = 2 \cdot \log_e(x)$ are identical, false
→ Domain of $f(x) = R - \{0\}$, Domain of $g(x) = (0, \infty)$
∴ not identical

$-(-x)$ $x+x$ $x<0$ $-\infty,0]$ $(-1$ $(0$ $-\infty.$ $(+2$

✓64) The domain of $f(x) = \frac{1}{\sqrt{|x|-x}}$ is $(-\infty, 0)$

→ $|x| = \begin{cases} x, & x \geq 0 \\ -x, & x < 0. \end{cases}$ ∴ the statement is <u>true</u>

case 1: when $x \geq 0$. $|x| - x = x - x = 0$.

∴ $f(x) = \frac{1}{0}$ } ∴ f is not defined ∵ $x \geq 0$.

case 2: when $x < 0$, $|x| - x = -x - x = -2x > 0$ (∵ $x < 0$)

Q.7*

<u>One-to-one Function</u> → (injection)

A function f from a set A to set B is said to be one-to-one if no two elements in A are mapped to some element in B.

<u>ote</u> →1) A function $f: A \to B$ is one-to-one if $f(a) = f(b)$, then <u>$a = b$</u>. $a, b \in A$

<u>ex</u> $f: A \to B$

$a_1 \to b_2$, $a_2 \to b_1$

$a_3 - b_3$ ✓

$b_4 - b_4$

b_5

If A and B are finite sets, then a one-to-one funcn $f: A \to B$ is possible iff $\boxed{|A| \leq |B|}$

$(m \leq n)$

2) If no. of elements in $|A| = m$ and $|B| = n$, then no. of one-to-one functions possible from A to B is $({}^nP_m)$

$a=b$ a,b 6 $|a|:$ $6\times5\times4$ $5P_4$ 6 5! $a_1 - b_1$ $a_2 - b_2$ b_3 $6P_4$ 6! $6\times5\times\ldots$

3) If $|A|=|B|=n$, then no. of one-to-one functions possible from A to B is $\underline{^nP_n = n!}$

If there are exactly 120 one-to-one functions possible from A to B, then which of the foll. is not true?

✓ a) $|A|=5$ and $|B|=5$ true $5P_5 = 5! = 120$

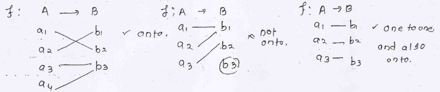
✓ b) $|A|=4$ and $|B|=5$ true $5P_4 = 5\times4\times3\times2\times1 = 120$.

✓ c) $|A|=3$ and $|B|=6$ true. $6P_3 = 6\times5\times4 = 120$.

d) $|A|=5$ and $|B|=4$ false. $|A| > |B|$

Onto function (Surjection) →

A function $f: A\to B$ is said to be onto if each element of B is mapped by at least one element of A. i.e. range of the function = B.



* If A and B are finite sets, then an onto function from A to B is possible iff. $|B| \le |A|$

* If $|B|=|A|$, then every onto funcn from A to B is also one to one and viceversa.

* If $|B|=|A|=n$, then no. of onto functions possible from A to B, $= (n!)$

$(m>n)$

* If $|A| = m$, and $|B| = n$, then no. of onto functions possible from A to B, is

$$= \boxed{n^m - {}^nC_1 \cdot (n-1)^m + {}^nC_2 \cdot (n-2)^m - {}^nC_3 (n-3)^m + \cdots + (-1)^{(n-1)} \, {}^nC_{n-1} \, (1)^m}$$

Q.8. If no. of elements in A, $|A| = 6$, and $|B| = 3$, then no. of onto functions possible from A to B are ?

→ $m = 6, \quad n = 3.$

$$= 3^6 - {}^3C_1 (2)^6 + {}^3C_2 (1)^m - {}^3C_3 (0)^m$$

$$= 729 - (3 \times 64) + (3 \times 1)$$

$$= \boxed{540}$$

Q9. If $|A| = n$, $|B| = 2$, $(n>2)$, then no. of onto functions possible from A to B is ?

→ $2^n - {}^2C_1 (1)^n$

$$= \boxed{2^n - 2}$$

Q10. In how many ways we can assign 5 employess to 4 projects so that every employee is assigned to only one project and every project is assigned by to at least one employee.?

→

e_1	P_1
e_2	P_2
e_3	P_3
e_4	P_4
e_5	

403

$\frac{243}{4}\ \ \frac{4!}{1!\,3!}\ \ \frac{729}{3}\ \ \frac{1024}{192}\ \ \frac{1216}{976\atop 240}$

$m = 5 \qquad n = 4.$

Reqd. no of ways

$= 4^5 - {}^4C_1\,(3)^5 + {}^4C_2\,(2)^5 - {}^4C_3\,(1)^m + 0.$

$= 1024 - (243 \times 4) + 6\,(32) - 4\,(1)$

$= 1024 - 972 + 192 - 4 = \boxed{240}$

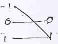
11. Consider the foll. functions on set of all integers.
$f(x) = x^2$, $g(x) = x^3$ and $h(x) = \lceil \frac{x}{2} \rceil$

which of the foll. true ?

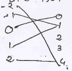
S1) f is one-to-one · false
S2) f is on-to. false
S3) g is one-one true
S4) g is on-to false.
S5) h is one-one false
S6) h is onto. ~~false~~ true.

→ S1) $f : Z \to Z$

S6, it is not one-one ex:-
$f(-1) = f(+1) = 1$



S2) $f : Z \to Z$. it is not on-to function ex. the negative integers in codomain are not mapped by any integer of the domain.



S3) Let $g(a) = g(b)$. $\because a, b \in Z$.
$a^3 = b^3$.
$\therefore a = b$.

So, g is one-one funcn.

54) g is not on-to because elements like 2, 3 in codomain are not mapped by any int. in domain.
i.e. $g(x) = x^3 = 2$ ← is not possible.

55) h is not one-one ex. $h(1) = h(2) = 1$

56) h is on-to because every integer in the codomain is mapped by at least one integer in the domain.

Bijection → (1-1 correspondence)
A function $f: A \to B$ is called a bijection if f is one-one as well as on-to.

If A and B are finite sets then a bijection from A to B is possible iff.
$|A| = |B|$

If $|A| = |B| = n$, then no. of bijections possible from A to B = $n!$

Q-12 Let $A = R - \{3\}$ and $B = R - \{1\}$. A function $f: A \to B$ is defined by $f(x) = \dfrac{x-2}{x-3}$.

Which of the foll. statements is true?

a) f is one-one but not onto
b) f is onto but one-one.
c) f is a bijection.
d) f is neither one-one nor on-to.

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

$\Rightarrow \quad \frac{a-2}{a-3} = \frac{b-2}{b-3} \Rightarrow (a-2)(b-3) = (b-2)\cdot(a-3)$

$\Rightarrow \quad \boxed{a=b} \quad \therefore f$ is one-one.

Let $f(x) = \frac{x-2}{x-3} = y. \Rightarrow x-2 = (x-3)\cdot y.$

$\Rightarrow \quad x - xy = 2 - 3y. \quad \Rightarrow x(1-y) = 2-3y.$

$\Rightarrow \quad x = \frac{2-3y}{1-y}.$ For each y, there exists x such that $f(x) = y$.

$\therefore f$ is on-to.

Inverse of a function $\to$

Let $f: A \to B$. If the inverse relation $f^{-1}: B \to A$ is a function then it is called inverse of f and is denoted by $f^{-1}: B \to A$.

Theorem $\to$

Inverse of $f: A \to B$ exists iff f is a bijection.

Q.13. which of the foll. functions have inverse defined on their ranges?

a) $f(x) = x^2, \quad x \in R$ It is not one-one $\therefore$ not bijection $\therefore$ Inverse does not exist.

b) $f(x) = x^3, \quad x \in R$ Here f is bijection. $\therefore$ Inv is defined.

$f^{-1}(x) = x^{1/3}.$

2. 2^{x}. $1/2$ 2^{1} $2^{0.5}$ $2^{1/3}$ 2^{3}. 3 $2^{0.1}$ $-\pi/2$ to $\pi/2$.

c) $g(x) = \sin x$, $x \in (0, \pi)$

→ g is not one-one in the interval $(0, \pi)$

ex. $g(\pi/4) = g(3\pi/4) = \frac{1}{\sqrt{2}}$

∴ Inv. of $g(x)$ does not exist.

d) $h(x) = 2^{x}$, $x \in R$.