27/12/21

UNIT-3

ABSTRACT ALGEBRA

Set: A collection of well defined objects.

subset: A set A is said to be a subset of B if each and every element of A is an element of B.

$A \subseteq B$ $B \supseteq A$

eg: $A = \{a, e, i, o, u\}$.

$B = \{a, b, c, d, e, i, g, o, u, s, t\}$

$A \subseteq B$.

[B is a super set of A].

Empty set:

A set that has no element is known as empty set. [ϕ or $\{\}$]

Universal set:

set of all elements under consideration. It is denoted by $\mathbb{E}$ or U.

Cardinality:

The cardinality of a set A is denoted by $O(A)$ or $n(A)$ or $|A|$ and it is defined as the no. of elements of A.

Note:

1. Empty set is a set of cardinality zero.
2. A set A is said to be a singleton set if $|A| = 1$.
3. Let A be a set. Then A has two trivial subsets - they are $\{\}$ and A itself. [Every set is a subset of itself and empty set is a subset of every set].

Power set:

The power set of A is denoted by $P(A)$ or $\mathcal{P}(A)$ and it is defined as the set of all subsets of A.

Eg: If $A = \{1, 2\} \rightarrow |A| = 2$.

$P(A) = \{\phi, \{1\}, \{2\}, \{1, 2\}\} \rightarrow |P(A)| = 4$

If $A = \{1, 2, 3\} \rightarrow |A| = 3$

$P(A) = \{\phi, \{1\}, \{2\}, \{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

$|P(A)| = 8$.

Note:

$|P(A)| = 2^{|A|}$.

If $A = \{\{1\}, \{2\}\}$.

$P(A) = \{\phi, \{\{1\}\}, \{\{2\}\}, \{\{1\}, \{2\}\}\}$

If $A = \phi$

$P(A) = \{\}$ $P(A) = \{\phi\}$ or $\{\{\}\}$.

$(A = \{1, 2, 3, 4, 5\})$

How many 2-element subsets of A are there? 3,2

Union:-

Let A and B be any two sets then the union of A and B is defences $A \cup B = \{x \in E / x \in A \text{ or } x \in B\}$.

Intersection:-

Let A and B be any two sets then the intersection of A and B is defined as $A \cap B = \{x \in E / x \in A \text{ and } x \in B\}$.

Disjoint sets:-

Two sets A and B are said to be disjoint if $A \cap B = \phi$.

$A = \{1, 2, 3, 4, 5, \ldots, 25\}$

$B = \{1, 3, 5, 7, 9, \ldots, 35\}$.

$A \cup B = \{1, 2, 3, \ldots, 25, 27, 29, 31, 33, 35\}$.

$A \cap B = \{1, 3, 5, 7, 9, \ldots, 25\}$.

Relative complement:-

Let A and B be any two sets. Then the relative complement of B w.r.t A is defined as

$A - B = \{x \in E / x \in A \text{ and } x \notin B\}$.

Eg: $A = \{1, 2, 3, \ldots, 10\}$.

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

$A - B = \{2, 4, 6, 8, 10\}$.

$B - A = \phi$.

A-B → elements

$A = \{1, 2, 3, 4, 5\}$; $B = \{3, 4, 6, 7, 8\}$.

$A - B = \{1, 2, 5\}$ — Δ element B cancel.

$B - A = \{6, 7, 8\}$.

symmetric difference:-

The symmetric difference of A and B is defined as $A \Delta B = (A - B) \cup (B - A)$

Eg: $A = \{1, 2, 3\}$; $B = \{3, 4, 5, - - -, 10\}$.

$A \Delta B = \{1, 2\} \cup \{4, 5, - - -, 10\}$

$= \{1, 2, 4, 5, - - -, 10\}$.

complement:

The complement of A is denoted by $\bar{A}$ or A' or A^c and it is defined as

$\bar{A} = \{x \in E \mid x \notin A\}$.

Eg: $E = \{1, 2, 3, - - -, 25\}$

$A = \{1, 2, - - -, 15\}$.

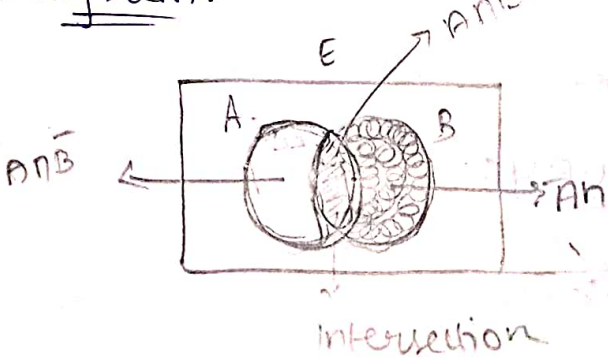
$\bar{A} = \{16, 17, - - -, 25\}$

Note:

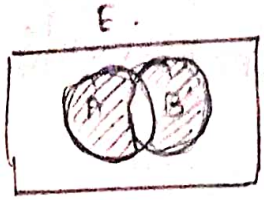
$A \Delta B = (A - B) \cup (B - A)$

$= (A \cap \bar{B}) \cup (\bar{A} \cap B)$

Venn diagram:



$A \Delta B = (A - B) \cup (B - A)$.



$\bar{A} \cap B \rightarrow B - A$

$\bar{B} \cap \bar{A} \rightarrow A - B$.

cartesian product:

The cartesian product of A and B is defined as $A \times B = \{(a,b) / a \in A \text{ and } b \in B\}$.

Eg:

$A = \{1, 2, 3\}$, $B = \{a, b\}$.

$A \times B = \{(1,a)(2,a)(3,a)(1,b)(2,b)(3,b)\}$

$B \times A = \{(a,1)(a,2)(a,3)(b,1)(b,2)(b,3)\}$.

Is $A \times B = B \times A$?

No $A \times B \neq B \times A$.

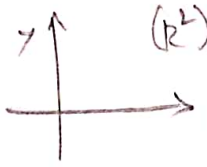
Note:

① $|A \times B| = |B \times A| = |A|\,|B|$

② $A = B \iff A \subseteq B$ and $B \subseteq A$

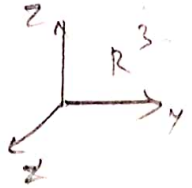
③ $A \times B = B \times A$ if $A = B$.

④ $A_1 \times A_2 \times A_3 = \{(a_1, a_2, a_3) / a_1 \in A_1, a_2 \in A_2, a_3 \in A_3\}$

⑤ 

(R^2) It is R2, shld nt b called as Rsquare i.e, (R^2).

$R^2 = R \times R$



$R^3 = R \times R \times R$.

LAWS OF SET THEORY:-

1. Idopotent laws:-

$A \cup A = A$

$A \cap A = A$.

2. Associative law:-

$A \cup (B \cup C) = (A \cup B) \cup C$

$A \cap (B \cap C) = (A \cap B) \cap C$.

3. Commutative law:-

$A \cup B = B \cup A$

$A \cap B = B \cap A$

4. Distributive law:

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

5- Absorption law:-

$A \cup (A \cap B) = A$

$A \cap (A \cup B) = A$

6. Identity law:-

$A \cup \phi = A$

$A \cap E = A$

7- Domination:-

$A \cup E = E$

$A \cap \phi = \phi$

8. Involution

$(A')' = A$

9. De-morgan's law;-

$(A \cup B)' = A' \cap B'$

$(A \cap B)' = A' \cup B'$.

28/12/21

10 State and prove De-morgan's laws for set theory.

Soln:

(i) $(A \cup B)' = A' \cap B'$. / $\overline{A \cup B} = \bar{A} \cap \bar{B}$

(ii) $(A \cap B)' = A' \cup B'$ / $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

IHS = RHS

LHS ⊆ RHS

RHS ⊇ LHS

(i) Let $x \in \overline{A \cup B}$

Then $x \notin A \cup B$.

$\Rightarrow x \notin A$ and $x \notin B$.

$\Rightarrow x \notin A \Rightarrow x \in \bar{A}$

$\Rightarrow x \notin B \Rightarrow x \in \bar{B}$.

$\Rightarrow x \in \bar{A} \cap x \in \bar{B}$.

$\because x$ is arbitrary

$$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B} \longrightarrow (1).$$

On the other hand, let $x \in \bar{A} \cap \bar{B}$

Then $x \in \bar{A}$ and $x \in \bar{B}$.

$\Rightarrow x \notin A$ and $x \notin B$.

$\Rightarrow x \notin A \cup B$.

$\Rightarrow x \in \overline{A \cup B}$.

$\because x$ is arbitrary.

$$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B} \longrightarrow (2).$$

From (1) & (2), we conclude that

$$\overline{A \cup B} = \bar{A} \cap \bar{B}.$$

(ii) Let $x \in \overline{A \cap B}$.

Then $x \notin A \cap B$.

$\Rightarrow x \notin A$ or $x \notin B$.

$\Rightarrow x \in \bar{A}$ or $x \in \bar{B}$.

$\Rightarrow x \in \bar{A} \cup \bar{B}$.

$\because x$ is arbitrary.

$$\overline{A \cap B} = \bar{A} \cup \bar{B} \longrightarrow (3)$$

On the other hand, Let $x \in \bar{A} \cup \bar{B}$.

Then $x \notin \bar{A}$ or $x \in \bar{B}$

$\Rightarrow x \notin \bar{A}$ or $x \notin \bar{B}$.

$\Rightarrow x \notin A \cap B$.

$\Rightarrow x \in \overline{A \cap B}$.

$\because x$ is arbitrary.

$\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$ — ②.

From ① & ② we conclude that 2 ->

$$\overline{A \cap B} = \bar{A} \cup \bar{B}.$$

. If A, B and C are sets, then prove the following

(ii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Let $x \in A \cup (B \cap C)$

Then $x \in A$ or $x \in B \cap C$.

$\Rightarrow x \in A$ or ($x \in B$ and $x \in C$)

$\Rightarrow (x \in A$ or $x \in B)$ and $(x \in A$ or $x \in C)$.

$\Rightarrow x \in A \cup B$ and $x \in A \cup C$

$\Rightarrow x \in (A \cup B) \cap (A \cup C)$

$\because x$ is arbitrary.

$\therefore A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ — ①

On the other hand, let $x \in (A \cup B) \cap (A \cup C)$

Then $x \in A \cup B$ and $x \in A \cup C$.

$\Rightarrow (x \in A$ or $x \in B)$ and $(x \in A$ or $x \in C)$

$\Rightarrow x \in A$ or ($x \in B$ and $x \in C$).

$\Rightarrow x \in A$ or $x \in (B \cap C)$

$\Rightarrow x \in A \cup (B \cap C)$.

$\because x$ is arbitrary

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C), \text{ — } ②$$

From ① , ② we conclude that.

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

(ii) $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$ } H/W. sums.

(iii) $A \times (B \cup C) = (A \times B) \cup (A \times C)$ }

(iv) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Let $(x, y) \in (A \times (B \cap C))$

then $x \in A$ and $y \in (B \cap C)$

$\Rightarrow x \in A$ and $(y \in B$ and $y \in C)$

$\Rightarrow (x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$

$\Rightarrow (x, y) \in (A \times B)$ and $(x, y) \in A \times C$

$\Rightarrow (x, y) \in (A \times B) \cap (A \times C)$

$\Rightarrow \because (x, y)$ is arbitrary

$A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$ — ①.

On the other hand, let $(x, y) \in (A \times B) \cap (A \times C)$

then $(x, y) \in (A \times B)$ and $(x, y) \in (A \times C)$

$\Rightarrow (x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$

$\Rightarrow x \in A$ and $(y \in B$ and $y \in C)$

$\Rightarrow x \in A$ and $y \in (B \cap C)$

$\Rightarrow (x, y) \in A \times (B \cap C)$.

$\because (x, y)$ is arbitrary.

$(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$ — ②.

From ① & ② we conclude that

$A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Relations:

Relations:

Any subset of $A \times B$ is a relation from A to B

Note:

(1) $R = \{\}$ is a void relation.

(2) $R = A \times B$ is an universal relation

(3) If $|A| = n$ and $|B| = m$ then the no. of relations that can be defined from A to B is 2^{mn}.

Any subset of $A \times A \times A \times \cdots \times n$ times is called as n-ary relation on A.

when $n = 2 \rightarrow$ **Binary relation.**

Properties:

Let R be a relation on A. then R is said to be

(i) Reflexive. (ii)

If $(a, a) \in R$ (or) aRa, $\forall a \in A$.

(ii) symmetric:

If $(a, b) \in R$ then $(b, a) \in R$, $\forall a, b \in A$.

(or)

If aRb then bRa, $\forall a, b \in A$

(iii) Transitive:

If $(a, b) \in R$ and $(b, c) \in R$ then

$(a, c) \in R$, $\forall a, b, c \in R$.

(or)

If (i) aRb and bRc then aRc,

for all $\in \forall a, b, c \in A$.

(iv) Anti-symmetric:

If $(a,b) \in R$ and $(b,a) \in R$ then $a=b$ $\forall$ $a,b \in A$

(or)

If aRb and $bRa \Rightarrow a=b$, $\forall$ $a,b \in A$

(v) Assymetric:-

If $(a,b) \in R \Rightarrow (b,a) \notin R$

(or)

if $aRb \Rightarrow b \not R a$, $\forall$ $a,b \in A$.

(vi) Irreflexive:-

If $(a,a) \notin R$, $\forall$ $a \in A$.

(or)

If $a \not R a$, $\forall$ $a \in A$.

Equivalence relation:-

Let R be a relation on A. Then R is said to be an equivalance relation if R is reflexive, symmetric and transitive.

Equivalence class:-

Let R be a equivalance relation on A. and Then the equivalance class of $a \in A$ is defined as

$$[a]_R = \{x \in A / a \xrightarrow{\text{such that}} R x\}$$

Partial order relation:-

A relation R on the set A is said to be a partial order relation if R is reflexive, anti-symmetric and transitive.

Poset:-

A non-empty set X together with a partial order

relation is known as partially ordered set or poset.

Relation matrix:

Let R be a relation from A to B. Then the relation matrix of R is denoted by M_R and it is defined as

$$M_R = [m_{ij}]_{m \times n}.$$

where $m_{ij} = \begin{cases} 1, & \text{if } a_i R b_j, \ 1 \le i \le m, \\ 0, & \text{otherwise.} \end{cases} \quad 1 \le j \le n.$

Relation graph:

Let R be a relation on A. Then the relation graph of R is a digraph whose vertices or nodes are the elements of A such that there is a directed edge or arc from a_i to a_j iff $a_i R a_j$ $\forall$ $a_i, a_j \in A$.

31/12/21.

1. ST the relation $R = \{(a,b) / a \equiv b \pmod n\}$ (such that, concurrent) on the set of integers is an equivalence relation.

Soln:

Equivalence relation:

The relation is said to be symmetric, transitive, reflexive.

Let $R = \{(a,b) / a \equiv b \pmod n\}$ be a relation on Z.

Then TPT R is an equivalence relation.

The meaning for $a \equiv b \pmod n$ is $a-b$ is divisible by n

Let $a \in Z$

$\because a - a = 0$ and $n | 0$.

$\Rightarrow a \equiv a \pmod{n}$.

$\Rightarrow aRa, \forall a \in Z$.

$\therefore$ R is reflexive — ①

If $(a,b) \in R$

then $a \equiv b \pmod{n}$.

$\Rightarrow$ TPT $b \equiv a \pmod{n}$. i.e., $n \mid a-b$.

$\Rightarrow$ ~~$n = k(a-b)$~~, for some integer k.

$\Rightarrow$ ~~$n = -k(b-a)$~~ (or) $a-b = kn$

$= (b-a) = -kn$

$\Rightarrow$ ~~$n = k_1(b-a)$~~, where $k_1 = -k$.

$b-a = -k$

$\Rightarrow n \mid b-a$

$\Rightarrow b \equiv a \pmod{n}$.

$\Rightarrow (b,a) \in R$

$\therefore$ R is symmetric.

$n \mid b-a$

$b \equiv a \pmod{n}$

$n \mid a-b$

$a \equiv b \pmod{n}$

If $(a,b) \in R$ and $(b,c) \in R$

then ~~$(a,c) \in R$~~. $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$.

$\Rightarrow n \mid a-b$ and $n \mid b-c$

$\Rightarrow n = k(a-b)$ and $n = m(b-c)$

where m and k are integers.

$\Rightarrow a-b = kn$ and $b-c = mn$,

where m and k are integers

Now $a-c = a-b+b-c$.

$a-c = kn+mn$

$a-c = (k+m)n$

$a-c = k_1 n$ where $k_1 = k+m$

$\Rightarrow n \mid a-c$

$\Rightarrow a \equiv c \pmod{n}$ $\therefore$ R is transitive.

$\because a,b \in R$, $b,c \in R$ then $a,c \in R$ transitive

Thus R is an equivalence relation

2. Let $R = \{(a,b) / a \equiv b \pmod 4\}$ be an equivalence relation on $A = \{1,2,3,\ldots,10\}$. Then find the equivalence class of all the elements of A.

Soln:

Let $A = \{1,2,3,4,5,6,7,8,9,10\}$

and $R = \{(a,b) / a \equiv b \pmod 4\}$.

Now; $[a]_R = \{x \in A / aRx\}$

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

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

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

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

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

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

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

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

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

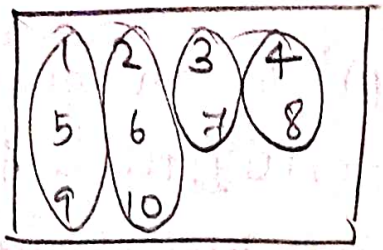
$[10] = \{2,6,10\}$.

Note: 1. Any two equivalence classes are either identical or disjoint.

2. $\bigcup_{a \in A} [A] = A$

3. $a \in [b] \iff [a] = [b]$.

A.



Equivalence relation decomposes the set into mutually disjoint subsets.

Partition:

Let $A_1, A_2, A_3, \ldots, A_k$ be subsets of A. then $\{A_1, A_2, A_3, \ldots, A_k\}$ is said to form a partition if $\bigcup_{i=1}^{k} A_i = A$ and $A_i \cap A_j = \phi$ if $i \neq j$.

$A = \{1, 2, 3, \ldots, 10\}$

$A_1 = \{1, 2, 3\}$; $A_2 = \{2, 4, 6, 8, 10\}$

$A_3 = \{1, 3, 5, 7, 9\}$; $A_4 = \{4, 5, 6, 7, 8\}$

$A_5 = \{9\}$; $A_6 = \{10\}$; $A_7 = \{9, 10\}$.

$A_1 \cup A_4 \cup A_7 = A$

$A_1 \cap A_4 = \phi = A_1 \cap A_7 \subseteq A_4 \cap A_7$

$A_1 \cup A_2 \cup A_3 = A$.

$A_1 \cap A_2 = \phi$; $A_2 \cap A_2 \neq \phi$

$A_1 \cap A_4 = \phi$

$A_1 \cap A_4 \neq 4$

3. Let $R = \{(A, B) / A \subseteq B\}$ be a relation on the power set of S (ie) $P(S)$. Then ST R is a partial order relation.

Soln:-

Let $R = \{(A, B) / A \subseteq B\}$ be a relation on the power

set of S, P(S).

Then TPT · R is a partial order relation

For $A \in P(S)$,

$A \subseteq A$.

$\Rightarrow (A, A) \in R$

$\therefore R$ is reflexive.

If $(A, B) \in R$ and $(B, A) \in R$, for $A, B \in P(S)$

Then $A \subseteq B$ and $B \subseteq A$

$\Rightarrow A = B$.

$\therefore R$ is anti-symmetric.

$A \subseteq B$ B will values all some A is included

If $(A, B) \in R$ and $(B, C) \in R$

Then $A \subseteq B$ and $B \subseteq C$

$\Rightarrow A \subseteq C$

$\Rightarrow (A, C) \in R$

$\therefore R$ is transitive.

Thus R is a partial order relation

---

4. Check whether the relation $R = \{(a, b) / a-b$ is an integer$\}$ on the set of integers is an equivalence relation or not. (H/W).

03/01/22.

1. Let $R = \{(a, b) / a/b\}$ be a relation on the set of integers then PT R is a partial order relation.

Partial order relation:

The relation is said to be reflexive, anti-symmetric, transitive.

Let $R=\{(a,b) : a|b\}$ be a relation on the set of integers.

Then TPT R is a partial order relation.

$\because a|a, \forall a \in z$

$\Rightarrow (a,a) \in R, \forall a \in z.$

$\therefore$ R is reflexive — ①.

If $(a,b) \in R$ and $(b,a) \in R$, for $a,b \in z$

Then $a|b$ or $b|a$.

$\Rightarrow a=b.$

$\therefore$ R is anti-symmetric — ②

If $(a,b) \in R$ and $(b,c) \in R$, for $a,b,c \in z$

Then $a|b$ and $b|c$.

$\Rightarrow b=na$ and $c=mb$.

Now $c = mb.$

$= m(na)$

$= (mn)a.$

$a|c$

$\therefore$ R is transitive — ③.

From ① & ② & ③ we conclude that R is a partial order relation.

---

2. If $A=\{1,2,3,4,5,\ldots,25\}$ and $R=\{(a,b) / a<b\}$ is a relation on A. Then find R.

Soln:

$A=\{1,2,3,\ldots,25\}$

$a<b$

$R=\{(a,b) / a<b\}.$

$R=\{(1,2)(1,3),(1,4)\ldots(1,25),(2,3)(2,4)\ldots (2,25),(3,4)(3,5)\ldots(3,25),(24,25)\}.$

Let $R = \{(1,1)(1,2)(1,4)(2,1)(2,2)(3,1)(3,2)(3,3)(4,1)(4,2)(4,3)(5,3)(5,4)(5,5)\}$ be a relation on $A = \{1,2,3,4,5\}$. Then find

(i) M_R (the relation matrix)

(ii) the relation graph.

Soln:

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

$R = \{(1,1)(1,2)(1,4)(2,1)(2,2)(3,1)(3,2)(3,3)(4,1)(4,2)(4,3)(5,3)(5,4)(5,5)\}$

(i)

$M_R = [m_{ij}]_{m \times n}$

$M_{ij} = \begin{cases} 1, & \text{if } a_i \text{ is related to } a_j \\ 0, & \text{otherwise.} \end{cases}$

$$M = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \end{array}.$$

Note: [If we are finding reflexive in the matrix then the diagonal elements shld be '1'. In this (4,4) is '0', so the diagonal elements are not same. i.e. no '1' in the place of (4,4) so, it is not reflexive.]

{Reflexive - Every element is related to itself
Irreflexive - No element is related to itself}

Is it symmetric? → a transpose = a.

(neither reflexive nor irreflexive)

⇒ To check whether R is transitive or not we have compute M^2.

i^{th} row × i^{th} column

1st row × 1st column, 1st row × 2nd col, 1st row × 3rd col ... 5th row × 5th column

[If $M^2 = M$ then it is transitive].

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

Boolean addition & multiplication

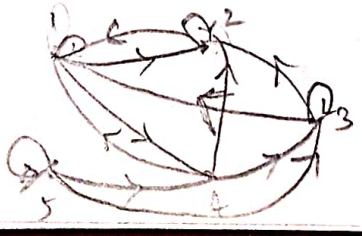
$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \neq M.$$

$M^2 \neq M$.

It is neither reflexive nor irreflexive, it is not symmetric and it is not transitive

(11) The relation graph.

Vertices are used to denote the elements of the set, order & shape is immaterial.



04/01/22.

1. Find the relation matrix and discuss its properties for the following relations on the set $A = \{1,2,3,4\}$.

(i) $R = \{(1,1)(1,2)(1,3)(2,1)(2,2)(3,1)(3,3)\}$

(ii) $R = \{(1,1)(1,2)(2,2)(3,1)(3,2)(3,3)(3,4)(4,1)(4,2)(4,4)\}$.

(iii) $R = \{(1,2)(1,3)(2,3)(2,4)(3,4)(4,1)\}$.

(iv) $R = \{(1,1)(2,2)(3,3)(4,4)\}$

(v) $R = \{(1,1)(1,2)(1,3)(2,3)(2,4)(3,3)(3,4)(4,1)(4,4)\}$

(vi) $R = \{(1,2)(2,3)(2,4)(3,2)(3,4)(4,2)(4,3)\}$

(vii) $R = \{(1,1)(1,2)(2,1)(2,2)(3,3)(3,4)(4,3)(4,4)\}$.

Soln.

(i) $R = \{(1,1)(1,2)(1,3)(2,1)(2,2)(3,1)(3,3)\}$.

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Not reflexive $\rightarrow (4,4) \notin R$.

Not irreflexive $\rightarrow (1,1)(2,2)(3,3) \in R$

symmetric $\rightarrow M_R = M^T_R$

Transitive $\rightarrow M_R^2 = M_R \cdot M_R$.

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

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

$\neq M_R$.

$\therefore$ R is not transitive.

Not symmetric, not anti-symmetric.

(ii) $M_R =$

	1	2	3	4
1	1	1	0	0
2	0	1	0	0
3	1	1	1	1
4	1	1	0	1

Reflexive, ~~symmetric~~, Transitive, ~~Asymmetric~~, Anti-symmetric, ~~Irref~~ reflexive.

$M_R^2 = M_R M_R$

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

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

$= M_R$.

(iii) $M_R =$

	1	2	3	4
1	1	0	0	0
2	0	1	0	0
3	0	0	1	0
4	0	0	0	1

Reflexive, symmetric, transitive, assymmetric, Anti-symmetric, Irreflexive

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

$$M_R^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

(iv)
$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Reflexive, transitive, symmetric, Irreflexive, assymmetric, Anti-symmetric.

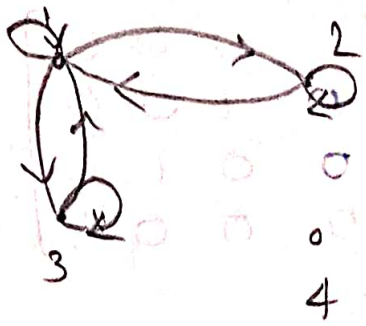
$$M_R^2 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

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

$\neq M_R$.

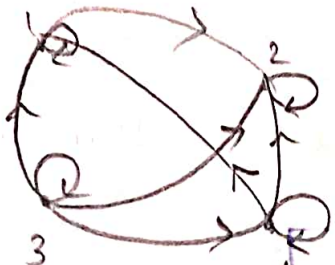
2. Draw relation graph for the above and discuss its properties.

(i)

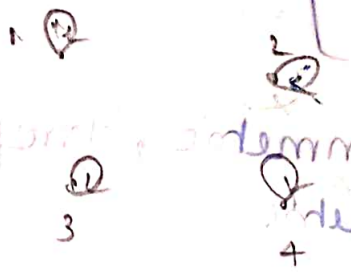


symmetric.

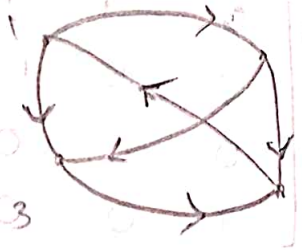
(ii)



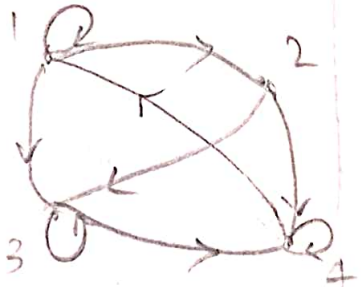
(iii)



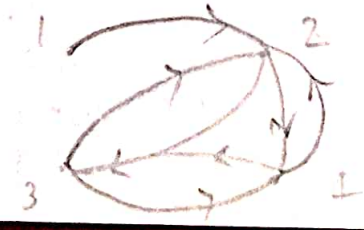
(iv)



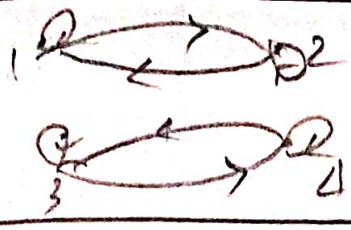
(v)

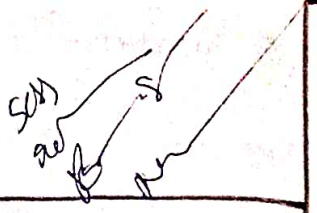


(vi)



(iii)





08/01/22. Revision.

Problems on generating functions:-

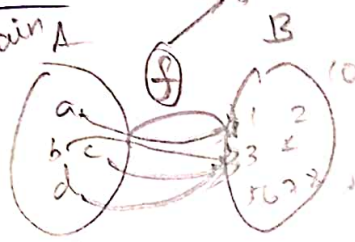
1. Solve $a_n + 3a_{n-1} - 4a_{n-2} = 0$, gn. that $a_0 = 3$, $a_1 = -2$.

2. Solve $a_{n+2} - 6a_{n+1} + 9a_n = 3^n$, $n \geq 0$, gn. that $a_0 = 2$ and $a_1 = 9$.

20/01/22.

Functions :-

① domain A — function f — codomain B



Not onto fnc.

f is a relation from A to B.

a → 1, b → 3, c → 3, d → 3.

Is it a function?

Yes

Is it a function?

No

Bcz the element a is associated with two elements in set B:

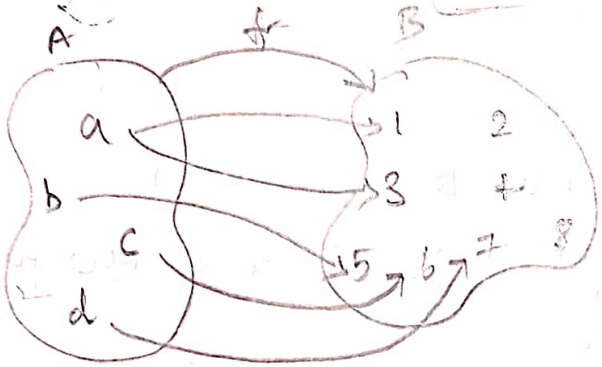
a → 1
a → 3

Is it a fnc?

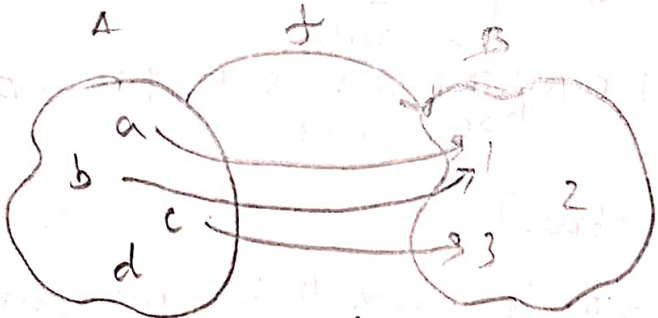
No

d → ___ .

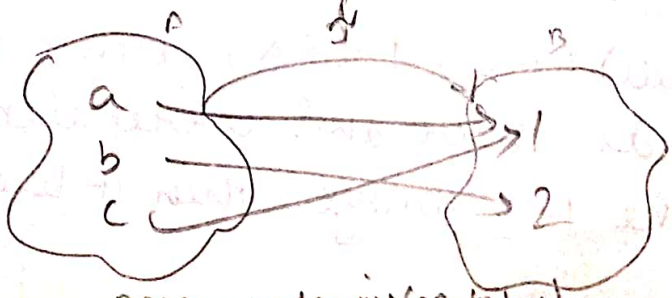
② Not onto fnc.



③



④



Is it a fnc?

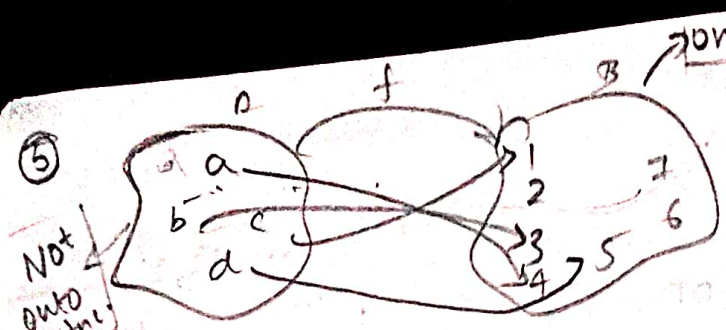
yes.

codomain = {1,2}

Range = {1,2}

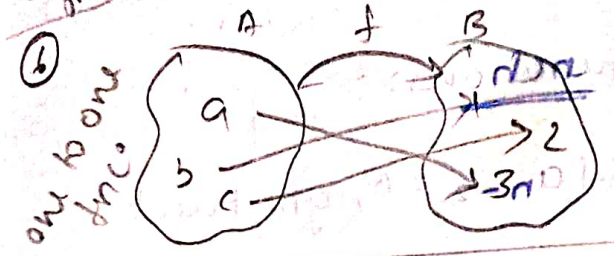
Range = codomain (onto fnc)

Every element in set A is related to one and only one element in B.



one to one fnc?
Is it a fnc?
Yes
codomain = B
Range = {1, 3, 4, 5} ≠ B.
It is not onto fnc.

⑤ Not onto fnc.



⑥ one to one fnc.

Is it a fnc? Yes
Onto fnc.

Definition of a function:

Let A and B be any two sets. Then a fn f from A to B is defined as for every element $a \in A$, $\exists$ (there exists) an unique element $b \in B$ such that $f(a) = b$.

Note:

Let $f: A \xrightarrow{\text{from}} B$ (to) be a function

(i) A – domain

(ii) B – (to) domain

(iii) If $f(a) = b$ for $a \in A$, $b \in B$.

Then the image of 'a' is 'b' and the pre-image of 'b' is 'a'.

(iii) The set of all images is called as range

(iv) Range $(f) = \{ b \in B \mid \exists\ (\rightarrow \text{for all})\ a \in A \text{ s.t } (\rightarrow \text{such that})\ f(a) = b \}$.

Onto function: (surjective)

A function $f: A \to B$ is said to be an onto function if $\forall$ (for all) $b \in B$, $\exists\ a \in A$, such that $f(a) = b$. In other words, each and every element of B has atleast one pre-image. Then it becomes a onto fnc.

(Range (f) = codomain)

∀ - forall
∃ - there exist
s.t - such that

one-to-one function:-(Injective).

A function $f: A \xrightarrow{\text{from}} B$ is said to be an one-to-one function if for every $b \in B$ ∃ almost one $a \in A$ s.t $f(a) = b$.

one to one fnc. means one I/P & one O/P.

almost - over!

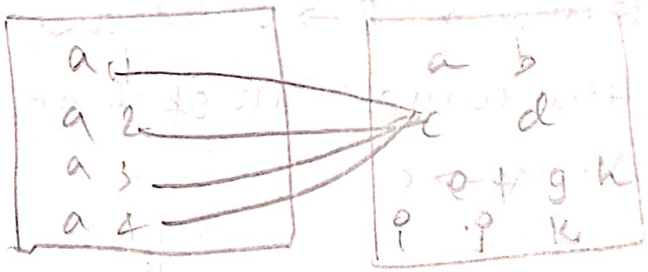
[Different elements having different images].

1-1 correspondence:- (Bijective).

A function $f: A \to B$ is said to be an 1-1 correspondence if f is both 1-1 and onto.

constant function:-

A function $f: A \to B$ (f from A to B) is said to be a constant function if ∀ $a \in A$ ∃ (/∈B/ s.t an element $c \in B$ s.t $f(a) = c$.



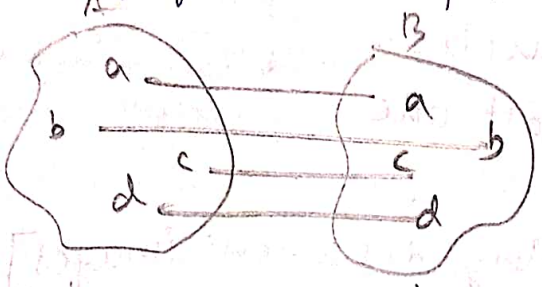
$f: R \to R$ (R - set of all real no's).

s.t - $f(x) = 3$.

y=3

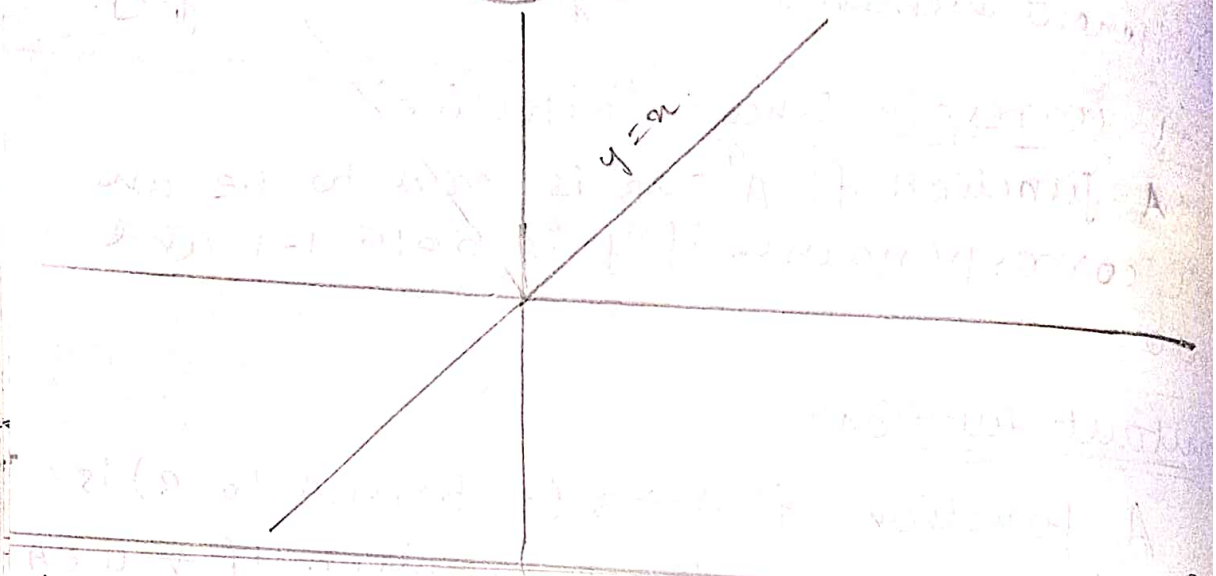
Identity function:-

A function $f: A \to A$ is said to be an identity function if $f(a) = a$, $\forall\ a \in A$.



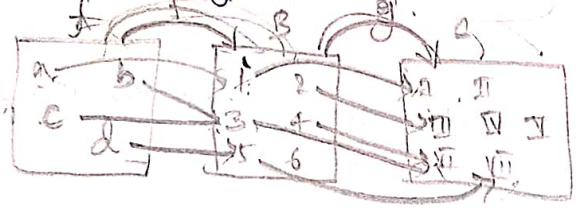
$f: R \to R$

$f(x) = x$.

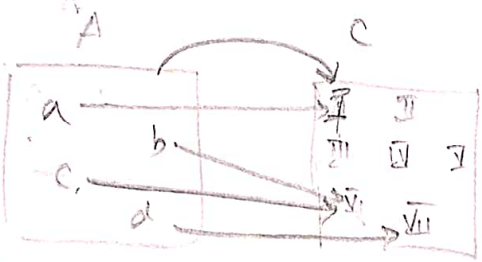


Composition of a function:-

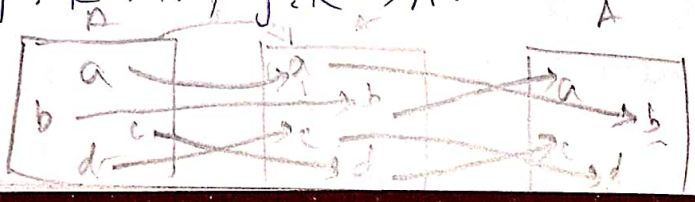
Let $f: A \to B$ and $g: B \to C$ be any two functions. Then the composition of f and g is a function $(g \circ f): A \to C$.

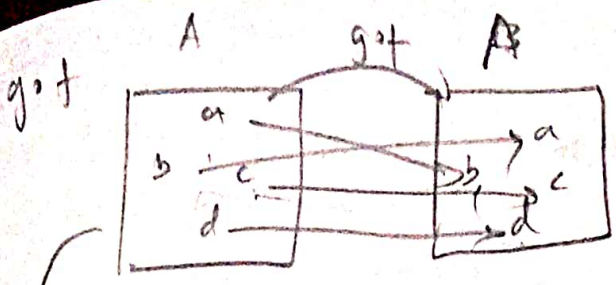


$g \circ f$



(2) $f: R \to R$; $g: R \to A$.

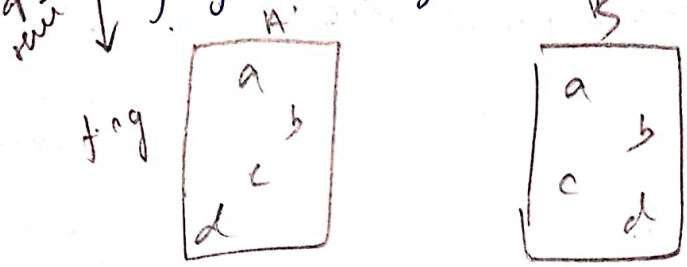




$f \circ g(a) = f(g(a)) = f(b) = b$

$f \circ g(b) = f(g(b)) = f(a) = a.$

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



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

Is $g \circ f = f \circ g$?

---

1. If $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ s.t

$f(x) = x + 5$, $g(x) = x^2 - 3$.

$$(g \circ f)(x) = g(f(x)) = g(x+5)$$
$$= (x+5)^2 - 3$$
$$= x^2 + 10x + 25 - 3$$
$$= x^2 + 10x + 22.$$

$$f \circ g = f(g(x)) = f(x^2 - 3)$$
$$= x^2 - 3 + 5$$
$$= x^2 + 2.$$

$f \circ g \neq g \circ f.$

- **Inverse function:**

Let $f : A \to B$ be any function. Then f is said to be invertible if $\exists$ a func. $f^{-1} : B \to A$ s.t

$f \circ f^{-1} = I_B$ and $f^{-1} \circ f = I_A$.

21/01/22

when $f: A \to B$ is onto

$|A| \geq |B|$

$f: A \to B$ is 1-1

$|A| \leq |B|$.

$f: A \to B$ is 1-1 correspondence

$|A| = |B|$.

$f: A \to B \quad f^{-1}: B \to A$

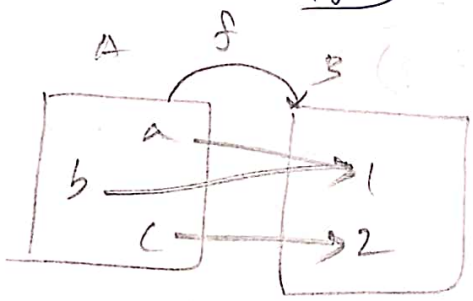
$f \circ f^{-1} = I_B \quad f^{-1} \circ f = I_A$

$$\boxed{f \circ f^{-1} = f^{-1} \circ f = I}$$

Theorem :1 :-

Let $f: A \to B$ be a function. Then f^{-1} exists if and only if f is ~~both~~ bijective.

$f: A \to B \quad \boxed{f^{-1}}$

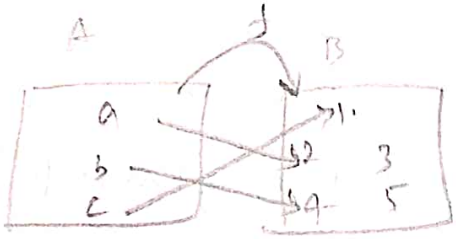


$$\boxed{f(a) = b \quad f^{-1}(b) = a}$$

$f(a) = 1, f(b) = 1, f(c) = 2$

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

$f^{-1}(2) = c$



$f(a) = 2, f(b) = 1, f(c) = 1$

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

$f^{-1}(2) = a$

$f^{-1}(4) = b \quad f^{-1}(5) = ?$

$f^{-1}(3) = ?$

Problems:

1. Let $f: R \to R$ and $g: R \to R$ be defined as $f(x) = x+2$ and $g(x) = x^2 - 4$, then find fog, gof, fof, gog, fofog, fofof, gogog.

Soln: $f: R \to R$ and $g: R \to R$ be defined as

$f(x) = x+2$ & $g(x) = x^2 - 4$

(i) $(fog)(x) = f(g(x)) = f(x^2-4)$

$= x^2 - 4 + 2 = x^2 - 2$ //

(ii) $(gof)(x) = g(f(x)) = g(x+2)$.

$= (x+2)^2 - 4$

$= x^2 + 4x + 4 - 4$.

$= x^2 + 4x$ //

(iii) $(fof)(x) = f(f(x)) = f(x^2+x)$

$= x + 4$ //

(iv) $(gog)(x) = g(g(x)) = g(x^2-4)$

$= (x^2-4)^2 - 4$

$= x^4 - 8x^2 + 16 - 4$

$= x^4 - 8x^2 + 12$ //.

(v) $(fofog)(x) = f(f(g(x)))$

$= f(f(x^2-4))$

$= f(x^2 - 4 + 2) = f(x^2 - 2)$

$= x^2 - 2 + 2$

$= x^2$ //

(vii) $g^3(x) = (gogog)(x) = g(g(g(x))) = g(g(x^2-4))$

$= g(x^2-4)^2 - 4$.

$= g(x^4 - 8x^2 + 16 - 4)$

$= g(x^4 - 8x^2 + 12) = (x^4 - 8x^2 + 12)^2 - 4$.

(vi) $f^3 = f \circ f \circ f$

$f^3(x) = f(f(f(x))) = f(f(x+2))$

$= f(x+4) = x+6.$

(vii) $g^3 = g \circ g \circ g$.

$g^3(x) = g(g(g(x))) = g(g(x^2-4))$.

$= g(x^2-4)^2 - 4$

$= g(x^4 - 8x^2 + 16 - 4)$

$= g(x^4 - 8x^2 + 12) \Rightarrow (x^4 - 8x^2 + 12)^2 - 4.$

$=$

---

2. If $f: R \to R$ and $g: R \to R$ are any two fncs then prove that (gof) (f composition g) is

(i) one-to-one if both f and g are one-to-one

(ii) onto if both f and g are onto.

Soln:

Given that $f: R \to R$ and $g: R \to R$ are two fnc.

(i) If both f and g are one-to-one then to prove that (gof) is one-to-one.

Suppose $(gof)(x) = (gof)(y)$ for some $x, y \in R$.

then $g(f(x)) = g(f(y))$

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

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

$\because$ g is one-to-one

$\Rightarrow a = b.$

$\Rightarrow f(x) = f(y)$

$\Rightarrow x = y$, $\because f$ is 1-1

(ii) If f and g are onto, then TPT $g \circ f$ is onto.

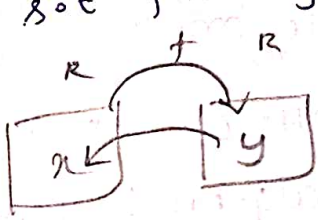
Let $y \in R$

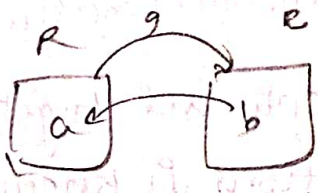
Rough

y is in co-domain

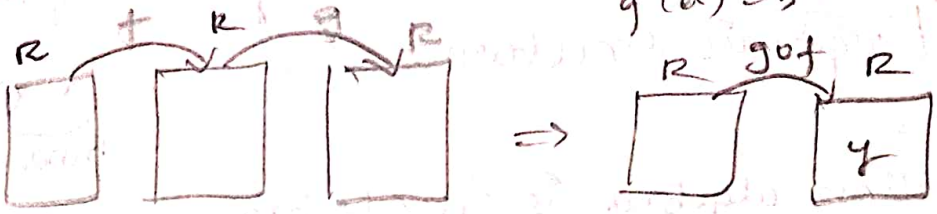
$\because f$ is onto, so $\exists\ x \in R$.

s.t $f(x) = y$.





$g(a) = b$.



$x \in R$

$f(x) = y$

$g(f(x))$

$= g(y) \in R$

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

$f: A \to B \quad g: B \to C$.

$(g \circ f): A \to C$

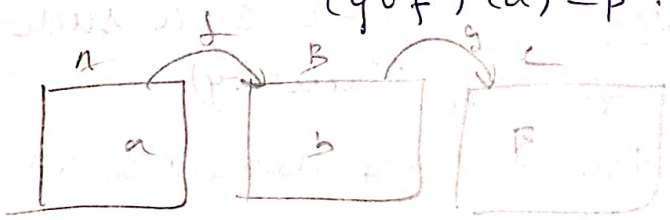
$(gof)(a) = \beta$

$\forall\ \beta \in C\ \exists\ b \in B$ s.t $g(b) = \beta$

$a \in A \quad f(a) = b$

$g(f(a)) = \beta$

$(gof)(a) = \beta$.



$(g \circ f)(a) = g(f(a)) = g(b) = \beta$.

22/01/22.

Groups:-

n-ary operation:

An n-ary operation on a set A is a

function from A^n to A (i.e.) $A \times A \times A \times \ldots \times n$ times to A.

Note:-

n=1 → unary operation

n=2 → binary " "

n=3 → ternary " "

Algebric system (or) structure (or) Algebra:-

A non-empty set together with one or more n-ary operations is known as algebra / algebraic system / algebraic structure.

Note:-

$(\wedge, \vee)$ ① binary unary

Boolean algebra is an algebraic system with two binary operation and one unary operation.

Group:-

A non-empty set G together with a binary operation $* : G \times G \to G$ is called a group if the following conditions are satisfied.

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

(ii) For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$ (Associative)

(iii) There exist (∃) an unique (one) element $e \in G$ such that $a * e = e * a = a$, $\forall a \in G$. (identity)

(where e is called the identity element of G)

(iv) For any element $a \in G$, ∃ an element $a' \in G$ s.t $a * a' = a' * a = e$. (a' is called inverse of a) (inverse).

Examples:-

✓ 1. $(\mathbb{Z}, +)$ → set of all integers, → usual addition. (0 is the identity element)

✗2. $(\mathbb{Z}, \times)$ usual multiplication.

✓3. $(R, +)$

✗4. $(R, \times)$ If it is $(R - \{0\}, \times)$ ✓

✓5. $(C, +)$

✓6. $(C - \{0\}, \times)$ $\quad i = \sqrt{-1}$

7. $a = \{1, -1, i, -i\}$ w.r.t usual multiplication

(i) 1 plays the role of identity elements.

Cayley (or) operation 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

$i^{-1} = 1.$

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

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

$i^{-1} = -i.$

$i \cdot i = -1$

$i \cdot -i = +1.$

8. Klein four group:

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

e is a identity element(i),

*	e	a	b	c
e	[e]	a	b	c
a	a	[e]	c	b
b	b	c	[e]	a
c	c	b	a	[e]

$a * a = e$

$b * b = e$

$c * c = e$

$a^{-1} = a$

$(a, b) \to c$

$(b, c) \to a$

$(c, a) \to b$

Row and column should b same that it is closure property

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

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

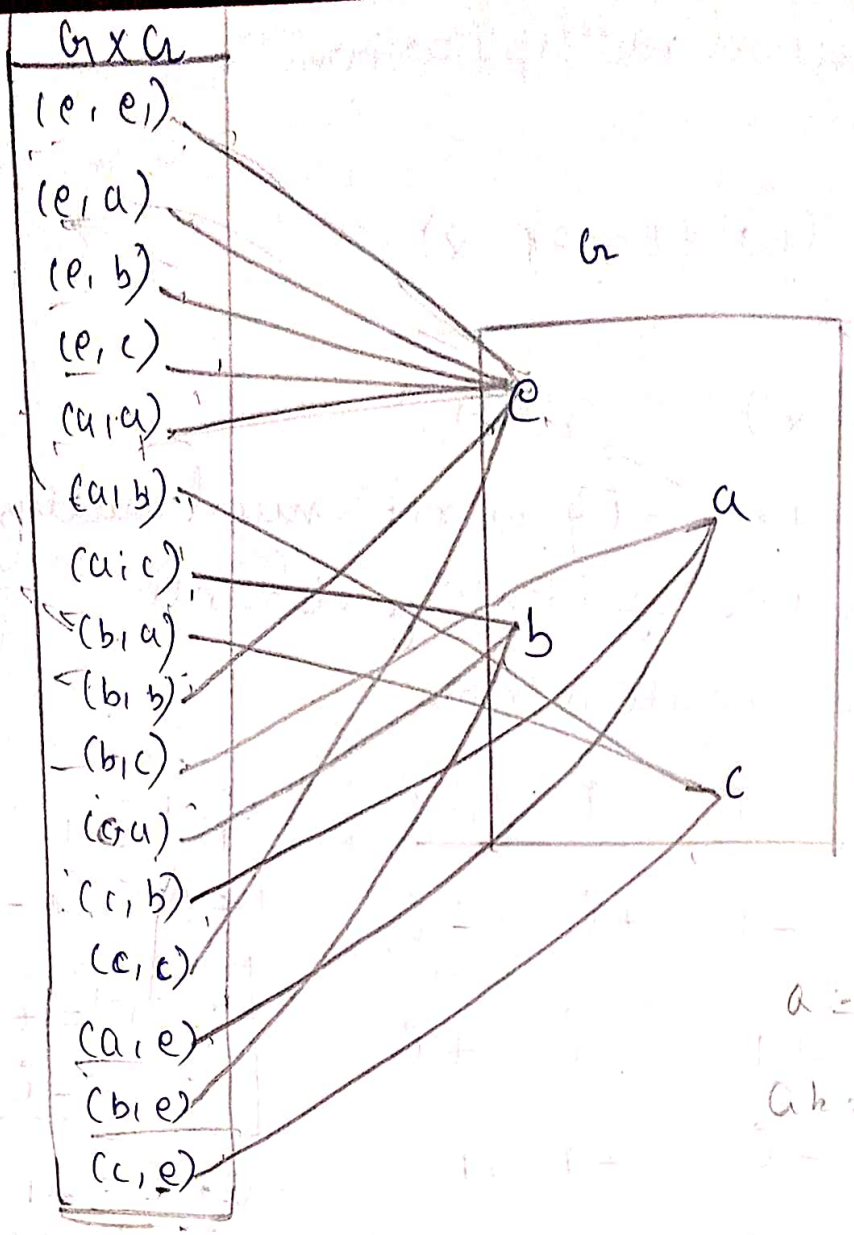
$(b * a) * c = c * c = e$

$e^{-1} = e$

$a^{-1} = a$

$b^{-1} = b$

$c^{-1} = c$



$(\mathbb{Z}, +)$

$(\mathbb{Z}_n, +_n)$

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

$ab = \frac{1}{ab}$

---

9. $G = \left\{ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \Big/ a_{ii} \in R \right\}$

$(G, +)$ → usual addition

G is a grp w.r.t usual addition.

matrix.

0 matrix means all the elements are zero. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

---

10. $G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\} / a, b, c, d \in R \text{ and } ad - bc \neq 0$

G is a group w.r.t usual matrix multiplication

(identity) $\Rightarrow e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

the inverse of $\begin{pmatrix} a & -b \\ c & d \end{pmatrix}$ is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$ad - bc$ $\quad \begin{pmatrix} +d & -b \\ -c & +a \end{pmatrix}$ $\quad \begin{pmatrix} 1 & -0 \\ -0 & 1 \end{pmatrix}$

10. $Z_n = \{0, 1, 2, 3, \ldots, n-1\}$

$(Z_n, +_n)$

Z_n addition modulo n.

$(Z_6, +_6)$ $\quad Z_6 = \{0, 1, 2, 3, 4, 5\}$.

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

Addition modulo

$10 - 6 = 4$

$Z_6 - \{0\}$

X_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

24/01/22.

Recall:-

$(G, *)$ — closure, Associative, identity, inverse.

Note:

1. $(\mathbb{Z}, +)$

$2^4 = 2+2+2+2 = 8$

$2^{10} = 20$

$3^3 = 3+3+3 = 9$.

2. $(\mathbb{Z}_6, +_6)$

$3^3 = (3 +_6 3) +_6 3$

$= 0 +_6 3$

$= 3$

$2^3 = (2 +_6 2) +_6 2$

$= 4 +_6 2 = 0$.

In general $a \in G$, $a^n = a * a * a * n$ times. ($n \in \mathbb{Z}$ → integer.)

Abelian group: (A group that satisfies commutative property)

A group $(G, *)$ is said to be an abelian group if $a * b = b * a$, $\forall a, b \in G$

Eg: $(\mathbb{Z}, +)$ is an abelian group. (→ usual addition.)

$(R, +)$ $(R - \{0\}, \times)$ $C - \{0\}$

$(C, +)$ $(C^*, \times)$

$(\mathbb{Z}_n, +_n)$

$(G = \{1, -1, +i, -i\}, \times)$.

Klein group:

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(Matrix × is not commutative)

$a * b = b * a$

It is a abelian group

cyclic group:-

A group $(G, *)$ is said to be a cyclic group if $\exists$ an element $a \in G$ s.t $x = a^n \; \forall x \in G$, $n \in Z$

Note: a is a cyclic group then it is denoted as

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

* a is called generator of G.

Eg: $G = \{1, -1, i, -i\}$

$i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$ ✓

$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1$ ✓

$(-1)^1 = -1$, $(-1)^2 = 1$, $(-1)^3 = -1$ ✗.

Note:-
Let a be a cyclic group and $a \in G$ be its generator then a^{-1} is also a generator.

Proof:-

Then for all $x \in G$, we have

$x = a^n$, for some $n \in Z$.

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

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

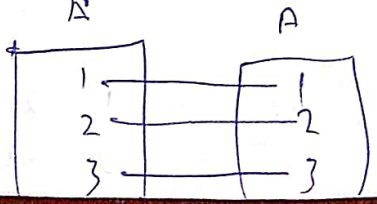
$x = (a^{-1})^m$ where $m = -n$

$\therefore a^{-1}$ is also a generator

Permutation group:-

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

Eg:-



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

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

Symmetric groups:

Let A be a finite set containing n elements. Then the set of all permutation of A is a group under the operation composition of functions. This group is called Symmetric group of degree n! and it is denoted by S_n.

$\langle S_3, \circ \rangle$ binary, identity element e

$S_3 = \{ e, P_1, P_2, P_3, P_4, P_5 \}$

$e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $P_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $P_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ $P_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$P_4 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $P_5 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

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

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

$P_1 \circ P_2 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = P_3$

$P_1 \circ P_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_2$

$P_1 \cdot P_4 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_5$

$P_1 \cdot P_5 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = P_4$

$P_2 \cdot P_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = P_4$

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

$P_2 \cdot P_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_5$

$P_2 \cdot P_4 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = P_1$

$P_2 \cdot P_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = P_3$

$P_3 \cdot P_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_5$

$P_3 \cdot P_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = P_1$

$P_3 \cdot P_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = P_4$

$P_3 \cdot P_4 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e$

$P_3 \cdot P_5 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_2$

$P_4 \cdot P_1 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = P_2$

$P_4 \cdot P_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = P_5$

$P_4 \cdot P_3 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e$

$P_4 \cdot P_4 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = P_3$

$P_4 \cdot P_5 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = P_1$

$P_5 \cdot P_1 = P_3$

$P_5 \cdot P_2 = P_4$

$P_5 \cdot P_3 = P_1$

$P_5 \cdot P_4 = P_2$

$P_5 \cdot P_5 = e$

HW:-

Construct the operation table for the symmetric group of degree n and find the inverse of all the elements. check whether it is an abelian group (or) not.

---

order of a group:-

Let $(G, *)$ be a group. Then the order of the group G is denoted by $O(G)$ (or) $n(G)$ (or) $|G|$ and it is defined as the no. of elements of G.

Note:

1. If G is klein group then
   $|G| = 4$
2. $(G = \{1, -1, i, -i\}, \times)$
   $|G| = 4$
3. $|S_3| = 6$.
4. $|S_n| = \lfloor n$.

order of an element:

Let $(G, *)$ be a group and $a \in G$. Then order of a is denoted by $o(a)$ and it is defined as the least (+)ve integer m such that $a^m = e$.

Eg: $(G = \{1, -1, i, -i\}, \times)$.

$O(1) = 1$, $O(-1) = 2$, $O(-i) = 4$.
$O(e) = 1$, $O(i) = 4$,

$O(-i) = 4$
$O(e) = 1$
$O(-1) = 2$
$O(1) = 1$
$O(i) = 4$

Theorem:1 (properties of group).

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

(i) the identity element is unique

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

(iii) for any $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$ and $(a^{-1})^{-1} = a$.

(iv) the left cancellation law :- $a * b = a * c \Rightarrow b = c$ and the right cancellation law :- $b * a = c * a \Rightarrow b = c$

(v) For $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solution in G.

(vi) then the identity element is only idempotent element.

Proof:

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

(i) TPT :- the identity element is unique.

Suppose that e and e' are identity elements of G.

Then treating 'e' as identity element and e' as some other element, so we have $e' * e = e * e' = e'$ — ①

Treating e' as identity element and e as some other element. Then we have

$e * e' = e' * e = e$ — ②

Now, $e = e' * e$ (By ②)

$= e'$ (By ①)

$\Rightarrow e = e'$

$e * e = e$

$e * a = e$

$e * e' =$

∴ the identity element of a group is unique

(ii) Let $a \in G$

Suppose that $b, c \in G$ are inverse of a.

Then $a * b = b * a = e$ — ③.

$a * c = c * a = e$ — (4)

Now, $b = b * e$ ... (6)

$= b * (a * c)$ ... (By (4))

$= (b * a) * c$

$= e * c$ (By (3))

$= c$.

i.e. $b = c$.

∴ the inverse of a is unique.

(iii) For $a, b \in G$.

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

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

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

$= a * a^{-1}$

$= e$

∴ $(a * b) * (b^{-1} * a^{-1}) = e$ — (5)

Also; $(b^{-1} * a^{-1}) * (a * b)$

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

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

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

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

$= e$.

∴ $(b^{-1} * a^{-1}) * (a * b) = e$ — (6).

From (5) and (6) we have;

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

Now, for $a \in G$, $\exists\ a^{-1} \in G$ s.t

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

∴ $(a^{-1})^{-1} = a$.

(LHS)$^{-1}$ = RHS

$x^{-1} = y$

$x * y = y * x$

$= e$

(iv) For $a, b, c \in G$.

If $a * b = a * c$

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

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

$\Rightarrow e * b = e * c$

$\Rightarrow b = c$.

ii) If $a * b = a * c$ then $b = c$.

similarly; if $b * a = c * a$

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

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

$\Rightarrow b * e = c * e$

$\Rightarrow b = c$

$ab = ac$
$a^{-1}ab = a^{-1}bc$
$(a^{-1}a)b =$
$(a^{-1}a)c$
$eb = ec$
$b = c$

(v) For $a, b, x, y \in G$

If $ax = b$.

then $a^{-1}(ax) = a^{-1}b$

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

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

$x = a^{-1}b \in G$

suppose x_1 and x_2 are solutions to the eqn, $ax = b$.

then $ax_1 = b$ and $ax_2 = b$

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x_1 = x_2$ (By 2 <<].

similarly, if $ya = b$

then, $(ya)a^{-1} = ba^{-1}$

$\Rightarrow y(aa^{-1}) = ba^{-1}$

$\Rightarrow ye = ba^{-1}$.

$\Rightarrow y = ba^{-1}$.

If y_1 and y_2 are solutions to $ya=b$ then

$y_1 a = b$ and $y_2 a = b$

$\Rightarrow y_1 a = y_2 a$

$\Rightarrow y_1 = y_2$ (RY RCL).

∴ the eqns, $ax=b$ and $ya=b$ have unique solutions in G.

(vi) Suppose that $a \neq e \in G$ is an idempotent element of G.

Then $a * a = a$.

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

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

$\Rightarrow e * a = e$

$\Rightarrow a = e$.

∴ the identity element is the only idempotent element of G.

25/01/22

Subgroup:

A non-empty subset H of a group $(G, *)$ is said to be a subgroup if H itself is a group w.r.t the binary operation $*$.

Examples:

1. $(Z, +)$ $H = \{2k / k \text{ is an integer}\}$

$H \subseteq (Z, +)$ $\quad a = a$

2. $(Z, +) \subseteq (R, +)$

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

$H = \{1, -1\}$

×	1	−1
1	1	−1
−1	−1	1

Theorem: 2:-

Let H be a subgroup of G. then

(i) the identity element of H is the same as that of G.

(ii) for each $a \in H$, the inverse of a in H is the same as the inverse of a in G.

Proof: Let H be a subgroup of G.

(i) suppose that e and e' are the identity element of G and H respectively.

Then $\forall a \in H$, $a * e' = e' * a = a$ — ①

$\because a \in G$, $a * e = e * a = a$ — ②

$\Rightarrow a * e' = a$ (By ①)

$= a * e$. (By ②)

(i.e.) $a * e' = a * e$.

$\therefore e' = e$ (By LCL).

(ii) suppose a is the inverse of a in G and a'' is the inverse of a in H.

Then $a * a' = e$.

and $a * a'' = e$

$\Rightarrow a * a' = a * a''$

$\Rightarrow a' = a''$ (By LCL)

Theorem: 3:-

A subset H of a group G is a subgroup of G if

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

(ii) The identity e of G is in H.

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

Proof:

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

Suppose that H is a subgroup of G

Then by the defn. of subgroup, H itself is a group w.r.t the binary operation $*$.

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

(ii) $e \in H$, where e is the identity element of G.

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

conversely suppose that.

(i) H is closed under the binary operation $*$ that is defined in G.

(ii) $e \in H$, where e is the identity element of G.

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

$\Rightarrow$ H itself is a group w.r.t the binary operation $*$.

$\therefore$ H is a subgroup of G.

Hence the theorem.

$a, b, c \in H$

$a, b, c \in G$

$a * (b * c) =$

$1 \in H$

$(a * b) * c$

$\in H$.

---

(2) Theorem: 1:

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

Proof:

Let H be a non-empty subset of a group $(G, *)$

Suppose that H is a subgroup of G.

Then for $a, b \in H \Rightarrow a * b \in H$

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

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

(i) If H is a subgroup then $a * b^{-1} \in H$, $\forall a, b \in H$.

converse, if $a * b^{-1} \in H$, $\forall a, b \in H$.

Then TPT H is a subgroup of G.

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

(ii) $e \in H$, where e is the identity element of G.

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

Let $a, b \in H$

Then $a * b^{-1} \in H$ (By assumption)

Put $b = a$

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

$\Rightarrow e \in H$

Now, $e \in H$ and $a \in H$.

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

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

$\therefore \forall a \in H \Rightarrow a^{-1} \in H$

Since $a, b^{-1} \in H$.

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

$\Rightarrow a * b \in H$.

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

if H is a subgroup of G. thus; a non empty subset of a group G is a subgroup of G iff $\forall a, b \in H$

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

Theorem: 5

Let H be a non-empty finite subset of G. If H is closed under the operation in G then H is a subgroup of G.

Proof:

Let H be a non-empty finite subset of a group $(G, *)$

If H is closed under the operation $*$.

Then let $a \in H$.

$\Rightarrow a^2 = a * a \in H$,

$a^3 = a^2 * a \in H$

$\vdots$

$a^n \in H$.

$\because$ H is finite, the elements $a, a^2, a^3, \ldots,$ cannot all be distinct.

$\Rightarrow$ ∃ integers $r < s$ such that

$a^r = a^s$

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

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

$(\because)\ a \in H \Rightarrow a^{s-r} = e$ for some integers $r < s$

Put $s - r = n$

Then $a \in H \Rightarrow a^n = e$

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

$\Rightarrow a^{-1} = a^{n-1} \in H$.

$\therefore$ H is a subgroup of G.

a
$a^2 = a * a \in H$
$a^3 \in H \quad a \in H$.
$a^2 * a \in H$
$a^3 \in H$
$a^4 \in H$
$a^5 \in H$
$a^n \in H$
⋮

$a\ a^2\ a^3\ a^4\ a^5$
$\ldots a^{10}\ a^{11}\ a^{12}$
$a^r * a^{-r} = e$

21/04/22

Cosets:

The cayley's table of (S_3, o) is

o	e	P_1	P_2	P_3	P_4	P_5
e	e	P_1	P_2	P_3	P_4	P_5
P_1	P_1	e	P_3	P_2	P_5	P_4
P_2	P_2	P_4	e	P_5	P_1	P_3
P_3	P_3	P_5	P_1	P_4	e	P_2
P_4	P_4	P_2	P_5	e	P_3	P_1
P_5	P_5	P_3	P_4	P_1	P_2	e.

coding theory

Cosets:-

Let H be a subgroup of a group $(G, *)$ let $a \in G$ then the set

(i) $aH = \{a * h / h \in H\}$ is called as the left coset of H defined by a in G.

(ii) $Ha = \{h * a / h \in H\}$ is called as the right coset of H defined by a in G

Eg: $G = \{1, -1, i, -i\}$

$H = \{1, -1\}$

Left cosets

$a = 1$; $aH = \{$

Right cosets.

1. Left coset

$a=1$; $aH=\{1\times 1, 1\times -1\}$

$=\{1,-1\}=H$

$a=-1$; $aH=\{-1\times 1, -1\times -1\}$

$=\{-1,+1\}=H$

$a=i$; $aH=\{1\times i, i\times -1\}$

$=\{i,-i\}$

$a=-i$; $aH=\{1\times -i, -i\times -i\}$

$=\{-i,i\}$

Right coset

$a=1$; $Ha=\{1\times 1, -1\times 1\}$

$=\{1,-1\}$

$a=-1$; $Ha=\{1\times -1, -1\times -1\}$

$=\{-1,1\}$

$a=i$; $Ha=\{1\times i, -1\times i\}$

$=\{i,-i\}$

$a=-i$; $Ha=\{1\times -i, -i\times -i\}$

$=\{-i,i\}$

2. $(S_3, 0)$ $G=S_3$ $H=\{e, P_5\}$.

$e^{-1}=e$

$P_5^{-1}=P_5$

Left cosets:-

$a=e$; $aH=\{e\cdot e, e\cdot P_5\}=\{e, P_5\}=H$.

$a=P_1$; $aH=\{P_1\cdot e, P_1\cdot P_5\}=\{P_1, P_4\}$

$a=P_2$; $aH=\{P_2\cdot e, P_2\cdot P_5\}=\{P_2, P_3\}$ $\rightarrow P_3\in P_2H$

$a=P_3$; $aH=\{P_3\cdot e, P_3\cdot P_5\}=\{P_3, P_2\}$ $P_2H=P_3H$

$a=P_4$; $aH=\{P_4\cdot e, P_4\cdot P_5\}=\{P_4, P_1\}$ $P_2\in P_3H$

$a=P_5$; $aH=\{P_5\cdot e, P_5\cdot P_5\}=\{P_5, e\}=H$. $P_2=P_3*P_5$

$H=\{e, P_5\}$.

Right cosets:-

$a=e$; $Ha=\{e\cdot e, P_5\cdot e\}=\{e, P_5\}$

$a=P_1$; $Ha=\{e\cdot P_1, P_5\cdot P_1\}=\{P_1, P_3\}$

$a=P_2$; $Ha=\{e\cdot P_2, P_5\cdot P_2\}=\{P_2, P_4\}$

$a=P_3$; $Ha=\{e\cdot P_3, P_5\cdot P_3\}=\{P_3, P_1\}$

$a=P_4$; $Ha=\{e\cdot P_4, P_5\cdot P_4\}=\{P_4, P_2\}$

$a=P_5$; $Ha=\{e\cdot P_5, P_5\cdot P_5\}=\{P_5, e\}$

1. $a \in H \iff aH = H$.

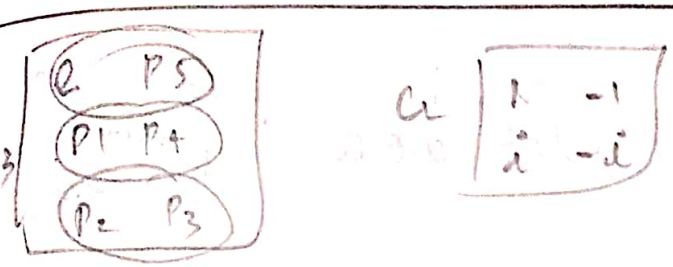
2. $\bigcup_{a \in G} aH = G$.

3. $a \in bH \iff b \in aH$.

   $a \in bH \iff aH = bH$.

4. Any two left cosets are either identical or disjoint.

5. $|aH| = |H|$.



Note:

* No. of distinct left cosets = No. of distinct right cosets.
* The no. of distinct left cosets of right cosets of H in G is denoted by $[G : H]$ and it is called as index of H in G.

Lagrange's theorem:

Let $(G, *)$ be a finite group and H be a subgroup of G. Then $o(H) / o(G)$.

Proof:

Let $(G, *)$ be a finite group and H be a subgroup of G.

$H = G$
$H = \{e\}$.

If $H = \{e\}$ then there is nothing TP.

If $H \neq \{e\}$ then let $o(G) = n$ and $o(H) = m$.

$x \in A \cup B \quad A = B$
$a_1H, a_2H, a_3H, \ldots a_{10}H$.
$x \in a_1H \cup a_2H \cup a_3H \cup \ldots \cup a_{10}H$

Claim 1: $\bigcup_{a \in G} aH = G$

$a_1H \cup a_2H \cup a_3H \cdots a_{10}H$
$x \in a_1H \cup a_2H \cup a_3H \cup \cdots \cup a_{10}H$

Let $x \in \bigcup_{a \in G} aH$

Then $x \in aH$, for some aH.

$\Rightarrow x = a * h$ for some $h \in H$ (By defn. of Lt cosets)

$\Rightarrow x \in G$.

$\because x$ is arbitrary

$\therefore \bigcup_{a \in G} aH \subseteq G$ — ① (subset)

On the other hand, let $a \in G$.

$a * h \in aH$
$a * e$

Then $a = a * e \in aH$

$\Rightarrow a \in aH$

$\Rightarrow a \in \bigcup_{a \in G} aH$

$\because A$ is arbitrary

$G \subseteq \bigcup_{a \in G} aH$ — ② (subset)

From ① & ② we have

$G = \bigcup_{a \in G} aH$

Hence the claim 1.

Claim: 2:-

$aH = bH$ (or) $aH \cap bH = \phi$ -s(empty)

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

Then $\exists\ x \in G$ s.t $x \in aH \cap bH$.

$\Rightarrow x \in aH$ and $x \in bH$.

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

$\Rightarrow x = a * h_i$ and $x = b * h_j$, for some $h_i, h_j \in H$

$\Rightarrow x * h_i^{-1} = a * h_j * h_i^{-1}$ and $x * h_j^{-1} = b * h_j * h_j^{-1}$

$\Rightarrow x * h_i^{-1} = a * e$ and $x * h_j^{-1} = b * e$.

$\Rightarrow x * h_i^{-1} = a$ and $x * h_j^{-1} = b$.

$\Rightarrow a \in xH$ and $b \in xH$.

(or)

$\Rightarrow x \in aH$ and $x \in bH$.

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

$\Rightarrow aH = bH$.

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

Hence the claim 2.

Claim 3:

$|aH| = |H|$.

Define $f : H \to aH$ as

$$f(h) = a * h, \forall h \in H \quad - (3)$$

TPT, f is bijective $\to$ (one to one) (onto).

(i.e.,) f is both one to one and onto

Suppose $f(h_i) = f(h_j)$ for some $h_i, h_j \in H$.

$\Rightarrow a * h_i = a * h_j$ [By (3)]

$\Rightarrow a^{-1} * (a * h_i) = a^{-1} * (a * h_j)$.

$\Rightarrow (a^{-1} * a) * h_i = (a^{-1} * a) * h_j$ (By associativity)

$\Rightarrow e * h_i = e * h_j$.

$\Rightarrow h_i = h_j$.

$\therefore f$ is 1-1. — (4)

Now, for $a * h \in aH$, $\exists\ h \in H$ s.t.

$f(h) = a * h$

$\therefore f$ is onto — (5)

From (4) & (5), we infer that

f is bijective.

$\therefore |aH| = |H|$. — (6)

Hence the claim 3.

Let r be the no. of distinct left cosets of H in G. Then by claim 1 we have

$$G = \bigcup_{a \in G} aH$$

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH.$$

$n(A \cup B) = n(A) + n(B) - n(A \cap B)$

$\Rightarrow$ Order of G = $O(a_1H) + O(a_2H) + \cdots +$ $O(a_rH)$.

$O(a) \nearrow$

$\Rightarrow n = O(H) + O(H) + \cdots + r$ times

$\Rightarrow n = m + m + \cdots + r$ times $[\because O(H) = m]$ {$\because$ By claim 3 & $O(G) = n$}

$\because O(H) \Rightarrow n = rm.$

$\Rightarrow m/n.$

$\because O(H)/O(a)$

Hence the theorem //

Converse of Lagrange's theorem is not true because the subset $H = \{i, -i\}$ is a group $G = \{1, -1, i, -i\}$ w.r.t usual multiplication is not a subgroup even though $O(H)/O(a)$.

$i \times -i = -i^2 = -(-1) = 1$

28/01/22

Theorem 7: The order of any element of a finite group G divides the order of G.

Proof:

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

$\{a\}$ which has $o(a)$ elements.

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

$(-1)^{2m} = e$

$o(-1) = 2$

$i^4 = 1 = e$

$i^8 = 1$ $(-1)^2 = 1$

$i^{12} = 1$ $(-1)^3 = -1$

Now consider the cyclic subgroup by a, i.e. $\langle a \rangle$ which has $o(a)$ elements.

(ie;) $o(H) = o(a)$

Now, by Lagrange's theorem.

$o(H) \mid o(G)$

$\therefore o(a) \mid o(G)$.

Theorem:-8

Every group of prime order is cyclic.

Proof:-

Let G be a group of prime order

(ie;) Let $o(G) = p$, where p is a prime number.

Then TPT G is cyclic.

Let $a \neq e \in G$.

Then $o(a) \mid o(G) = p$

(ie;) $o(a) \mid p$

$\Rightarrow o(a) = 1$ (or) $o(a) = p$.

$\Rightarrow a = e$ (or) $G = \langle a \rangle$.

$\because a \neq e$

$\Rightarrow a = \langle a \rangle$

$\therefore G$ is cyclic.

Thus, every group of prime order is cyclic.

Theorem: 9

Let G be a group of order n and let

$a \in G$. Then $a^n = e$.

Proof:

Let G be a group of order n

(ie;) $O(G) = n$

Let $a \in G$ and let $O(a) = m$

$\therefore O(a) \mid O(G)$

$\Rightarrow m/n$

$\Rightarrow n = mq$, where $q \in Z$.

$\Rightarrow a^n = a^{mq}$.

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

$\Rightarrow e^q$

$\Rightarrow e$

$\therefore a^n = e$

Euler's theorem: 10:-

If n is any integer and $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is the no. of positive integers less than n and relatively prime to n.

Proof:

Let $G = \{m \mid m < n \text{ and } (m, n) = 1\}$ multiplication modulo n

Then G is a group under the operation $\times_n$

$\Rightarrow O(G)$

Now, let $(a, n) = 1$

Let $a = qn + r$, $0 \le r < n$

$a - r = qn$ $\quad a \equiv r \pmod{n}$

$\therefore (a, n) = 1$.

$(n, r) = 1$

29/11/22

Theorem:-11 Fermat's Theorem:-

Let p be a prime number and a be any integer relatively prime to p. Then $a^{p-1} \equiv 1 \pmod{p}$

Proof:

Prove Euler's Theorem.

$a^{\phi(n)} \equiv 1 \pmod{n}$

Let $n = p$, where p is a prime no.

Then $a^{\phi(p)} \equiv 1 \pmod{p}$

$\phi(n) \rightarrow$ no: of +ve integers less than n and relatively prime to n.

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

$$a^{p-1} \equiv 1 \pmod{p}$$

$\phi(5) = 4$
$\{1, 2, 3, 4\}$
$\phi(6) = 5$
$\phi(7) = 6.$
$\phi(11) = 10$
$\phi(13) = 12$

Problems:-

1. PT every cyclic group is abelian is the converse true? Justify.

Soln:

Let $(G, *)$ be a cyclic group. Then $\exists$ an element $a \in G$ s.t. $x = a^m, \forall x \in G,$ where m is some integer.

TPT G is abelian

Let $x, y \in G.$

Then $x = a^m$ and $y = a^r$ for some integers m and r.

Now, $x * y = a^m * a^r$

$= a^{m+r}$

$= a^{r+m}$

$= a^r * a^m$

$= y * x$.

(ie) $x * y = y * x$

∴ $(G, *)$ is abelian.

Thus, every cyclic group is abelian.

But the converse is not true because the group $(\mathbb{R}, +)$ is an abelian group but not cyclic.

---

2. PT the intersection of any two subgroups of a group is also a subgroup.

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

Then TPT $H \cap K$ is also a subgroup.

Now, $H \cap K \neq \phi$ because $e \in H \cap K$.

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

Then $a, b \in H$ and $a, b \in K$.

$\Rightarrow a * b^{-1} \in H$ and $a * b^{-1} \in K$, since H and K are subgroups.

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

∴ $H \cap K$ is a subgroup

Thus, the intersection of any two subgroups is again a subgroup.

---

3. PT the union of any two subgroups of a group need not be a subgroup.

Soln:- Let us consider the subgroups

$H = \{2m / m \text{ is an integer}\}$ and

$K = \{3m / m \text{ is an integer}\}$ of the grp $(\mathbb{Z}, +)$

∵ $H \cup K$ is not closed under the operator '+'

∴ $H \cup K$ is not a subgroup.

Thus the union of any two subgroups need not be a subgroup.

Rough column:-

$H = \{\ldots, -8, -4, -6, -2, 0, 2, 4, 8, 10 \ldots\}$

$K = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, 15 \ldots\}$

$H \cup K = \{\ldots, -9, -8, -6, -4, -3, -2, 0, 2, 3, 6, 8, 9, 12, 14, 18 \ldots\}$

$2 + 3 = 5 \notin H \cup K$.

---

4. If H and K are subgroups of a group $(G, *)$ then prove that $H \cup K$ is a subgroup of G iff either $H \subseteq K$ or $K \subseteq H$.

(or)

Pr the union of two subgroups of a grp is a subgroup iff one is contained in the other

Soln: Let H and K be subgroup of a group $(G, *)$

Let us assume that $H \subseteq K$

Then $H \cup K = K$

$\because$ K is a subgroup.

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

Thus if $H \subseteq K$ or $K \subseteq H$ then $H \cup K$ is a subgrp.

Conversly, let us assume that $H \cup K$ is a subgrp.

Then TPT either $H \subseteq K$ or $K \subseteq H$.

Suppose neither H is contained in K nor K is contained in H.

Then $\exists$ elements a, b such that $a \in H$ & $a \notin K$ — ①

and $b \in K$ and $b \notin H$ — ②

Now clearly $a, b \in H \cup K$.

$\Rightarrow a * b \in H \cup K$, $\because H \cup K$ is a subgroup.

$\Rightarrow a * b \in H$ or $a * b \in K$.

Case (i):- If $a * b \in H$.

then $a^{-1} * (a * b) \in H$ [$\because a \in H$, so $a^{-1} \in H$]

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

$\Rightarrow e * b \in H$.

$\Rightarrow b \in H$.

which is a contradiction to (2)

Case(ii): If $a * b \in K$.

Then $(a*b) * b^{-1} \in K$ [$\because b \in K$, so $b^{-1} \in K$].

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

$\Rightarrow a * e \in K$

$\Rightarrow a \in K$.

which is contradiction to (2), (1).

$\Rightarrow$ our assumption that neither H is contained in K nor K is contained in H is wrong.

i.e Either $H \subseteq K$ or $K \subseteq H$.

Thus, $H \cup K$ is a subgroup iff $H \subseteq K$ or $K \subseteq H$

29/01/22

5. ST in an abelian group $(a*b)^2 = a^2 * b^2$.

Soln

Let $(G, *)$ be an abelian group.

For $a, b \in G$.

$a^2 = a * a$

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

$= a * (b * a) * b$ (By associative)

$= a * (a * b) * b$ ($\because$ G is abelian)

$= (a * a) * (b * b)$ (By associative)

$= a^2 * b^2$

i.e $(a*b)^2 = a^2 * b^2$ //

---

6. Let $(G, *)$ be a group s.t $a^2 = e \ \forall \ a \in G$ Then PT $(G, *)$ is abelian.

Soln:-

Let $(G, *)$ be a group st $a^2 = e \; \forall \; a \in G$.
then TPT $(G, *)$ is an abelian group.

Abelian group: A group that satisfies commutative property is known as abelian group

For $a, b \in G$.

$\boxed{(a*b)^2 = e.}$ (⊗ key step.

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

$\Rightarrow a*(b*a)*b = e$ (By associative)

$\Rightarrow$ @ operator both sides 'a'

ie; $a*(a*(b*a)*b) = a*e.$

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

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

$\Rightarrow e * ((b*a)*b) = a \quad [\because a^2 = e].$

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

operator both sides by b

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

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

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

$\Rightarrow (b*a)*e = a*b. \quad (\because b^2 = e)$

$\Rightarrow b*a = a*b.$

ii G is abelian.

Note:- the above problem can be stated as "P.T a group G is abelian if each and every element of a has its inverse $[(ii)\; a^{-1} = a \; \forall \; a \in G]$

7. If in a group $b^{-1} * a^{-1} * b * a = e$, $\forall a, b \in G$. Then s.t G is abelian group.

Soln:

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

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

then TPT G is abelian.

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

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

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

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

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

$\Rightarrow b * a = a * b$, $\forall a, b \in G$

i.e $(G, *)$ is a abelian group.

commutative $a * b = b * a$

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

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

Rings: Define ring and write examples

A non-empty set R together with two binary operations denoted by "+" and "·" and called addition and multiplication which satisfy the following axioms is called a rings.

(i) The algebric structure $(R, +)$ is an abelian group. (closure, associative, inverse, identity, commutative)

(ii) The operation " · " is an associative binary operation on R

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ $\forall a, b, c \in R$. (ie); '·' is distributed over '+' but '+' is not distributed over '·'

Eg: 1. $(Z, +, \cdot)$ [set of all integers w.r.t usual + and ·]

2. $(Q, +, \cdot)$

3. $(R, +, \cdot)$ → ~~addition~~ rational no's
   ↳ real no's

4. $(C, +, \cdot)$ · complex no's

5. $R = \{a + ib \mid a, b \in Z\}$ R is a ring wrt usual addition and multiplication this is called as Ring of Gaussian integers

6. Let M be the set of all $n \times n$ matrices. then M is a ring w.r.t matrix addition and matrix multiplication.

7. $(Z_n, +_n, \times_n)$

$2 \cdot (3+5) = 16$
$2 \cdot 3 + 2 \cdot 5 = 16$
$2 + (3 \cdot 5) = 17$
$(2+3) \cdot (7+5) = 35$

Define: commutative ring:

A ring R is said to be a commutative ring if $a \cdot b = b \cdot a, \forall a, b \in R$

Eg: $(Z, +, \cdot)$; $(R, +, \cdot)$; $(C, +, \cdot)$; $(Q, +, \cdot)$

Define ring with identity:

Let R be a ring then R is said to be a ring with identity if there exists an element $1 \in R$ s.t $a \cdot 1 = 1 \cdot a = a \ \forall a \in R$.

Eg: $(Z, +, \cdot)$; $(R, +, \cdot)$; $(Q, +, \cdot)$; $(C, +, \cdot)$;
$(M, +, \times)$ → identity matrix.

This continuation is in back side

Defn:- Let R be a ring with identity then an element $a \in R$ is said to be an unit in R if it has as multiplicative inverse in R.

Eg: $(Z, +, \cdot)$ unit elements of this are $+1, -1$.
have multiplicative inverse another
Multiplicative inverse of $+1 \to -1$ & for $-1 \to +1$