Set Theory

* The principle of Inclusion- Exclusion :-

let A and B are subsets of some universal set U then the principle of Inclusion-Exclusion for two sets A and B is

$$|A \cup B| = |A| + |B| - |A \cap B|$$

where $|A| =$ No. of elements in the set A.

$|B| =$ No. of elements in the set B.

$|A \cup B| =$ No. of elements in the set $A \cup B$.

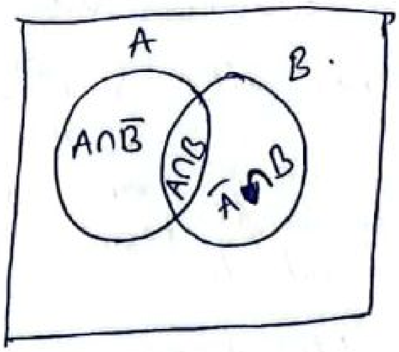
$|A \cap B| =$ No. of elements in the set $A \cap B$.

Note:

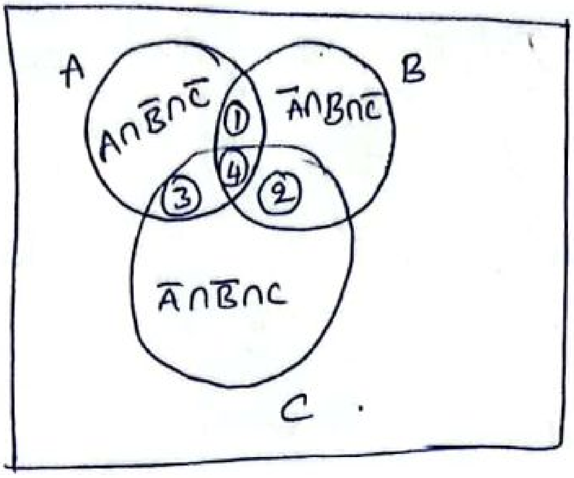
1. The principle of Inclusion- Exclusion for three sets A, B and C is

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

2. Ven diagram for two sets A and B is



3. Ven-diagram for three sets A, B and C is.



① $A\cap B\cap\overline{C}$

② $\overline{A}\cap B\cap C$

③ $A\cap\overline{B}\cap C$

④ $A\cap B\cap C$

4. $|\overline{A}| = N - |A|$, where N is the number of elements in the ceniversal set.

5. $\lfloor x \rfloor$ = The least positive integer.

Problems :-

* A survey among 100 students shows that of the three ice cream flavours vanilla, chocolate, strawberry. 50 students like vanilla, 43 likes chocolate, 28 like strawberry, 13 like ~~and~~ vanilla and chocolate, 11 like chocolate and strawberry, 12 like strawberry and venella, 5 like all of them. Find the following

① Chocolate but not strawberry

② Chocolate and strawberry but not vanilla.

③ Vanilla or chocolate but not strawberry.

Given, $N = 100$.

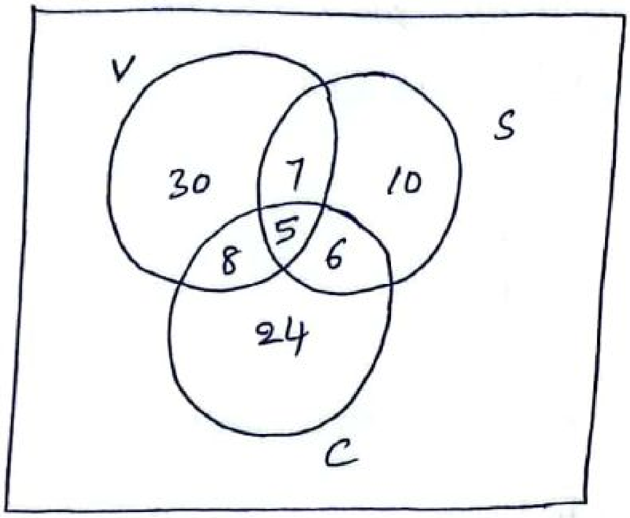
let V: The students like vanilla.

C: the students like chocolate.

S: the students like strawberry.

Given, $|V| = 50$, $|C| = 43$, $|S| = 28$

$|V \cap C| = 13$, $|C \cap S| = 11$, $|S \cap V| = 12$, $|S \cap V \cap C| = 5$.



① From the above ven diagram, the number of Students like chocolate but not strawberry is

$|C \cap \bar{S}| = |C| - |C \cap S \cap \bar{V}| - |C \cap S \cap V|$

$= 43 - 6 - 5.$

$= 32.$

② The number of Students like chocolate and strawberry but not Vanilla is

$|C \cap S \cap \bar{V}| = |C \cap S| - |C \cap S \cap V|$

$= 11 - 5.$

$= 6.$

③ The number of Students like vanilla or chocolate but not strawberry is.

$|(V \cup C) \cap \bar{S}| = |V \cap \bar{C} \cap \bar{S}| + |C \cap \bar{V} \cap \bar{S}| + |V \cap C \cap \bar{S}|$

$= 30 + 8 + 24 = 62$

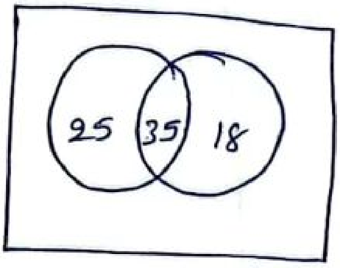
* Out of 80 students in a class, 60 play football, 53 play hockey and 35 both the games. How many students ① do not play of these games ② Play only hockey but not foot ball.

The number of students in a class, $N = 80$

let F : the students play foot ball.

H : the students play hockey.

$|F| = 60, \quad |H| = 53, \quad |F \cap H| = 35.$



① The no. of students do not play hockey and foot ball is $|\overline{F} \cap \overline{H}|$

$$|\overline{F} \cap \overline{H}| = N - |F \cap \overline{H}| - |\overline{F} \cap H| - |F \cap H|$$
$$= 8 - 25 - 18 - 35.$$
$$= 2$$

(or)

$$|\overline{F} \cap \overline{H}| = |\overline{F \cup H}| = N - |F \cup H|$$
$$= N - \left[|F| + |H| - |F \cap H| \right]$$
$$= 80 - [60 + 53 - 35]$$
$$= 2.$$

② The number of students play hockey but not foot ball is $|\overline{F} \cap H| = |H| - |F \cap H|$
$$= 55 - 35.$$
$$= 18.$$

* Consider a set of integers from 1 to 250. Find how many of these numbers are divisible by 3 or 5 or 7. Also indicate how many are divisible by 3 or 7 but not by 5 and divisible by 3 or 5.

let us consider a set $S = \{1, 2, 3, \cdots 250\}$.

Here, $N = 250$.

let A_1: The no|| which are divisible by 3.

A_2: The no|| which are divisible by 5.

A_3: The no|| which are divisible by 7.

$$|A_1| = \left\lfloor \frac{250}{3} \right\rfloor = 83.$$

$$|A_2| = \left\lfloor \frac{250}{5} \right\rfloor = 50$$

$$|A_3| = \left\lfloor \frac{250}{7} \right\rfloor = 35.$$

$|A_1 \cap A_2|$ = The no|| which are divisible by 3 and 5.

$$|A_1 \cap A_2| = \left\lfloor \frac{250}{LCM(3,5)} \right\rfloor = 16$$

$|A_1 \cap A_3|$ = The no|| which are divisible by 3 and 7.

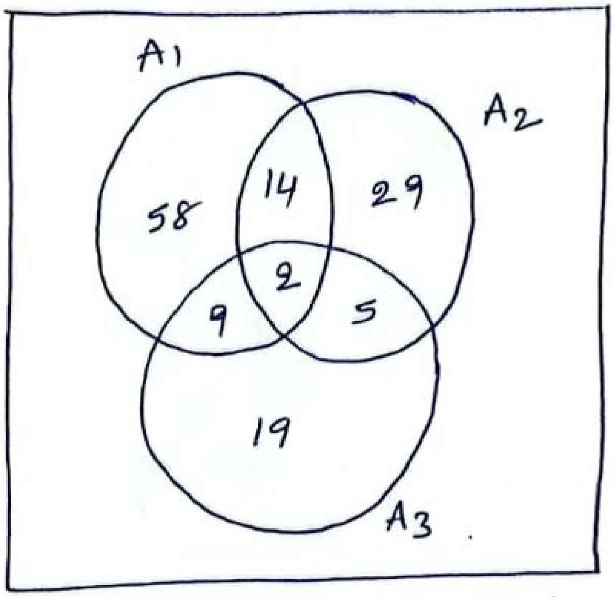
$$|A_1 \cap A_3| = \left\lfloor \frac{250}{LCM(3,7)} \right\rfloor = 11.$$

$|A_2 \cap A_3|$ = The no|| which are divisible by 5 and 7.

$$|A_2 \cap A_3| = \left\lfloor \frac{250}{LCM(5,7)} \right\rfloor = 7.$$

$|A_1 \cap A_2 \cap A_3|$ = The no. which are divisible by 3, 5 and 7.

$$|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{250}{LCM(3,5,7)} \right\rfloor = 2$$



From the above ven-diagram, the number of integers which are divisible by 3 or 5 or 7. is

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

$$= 83 + 50 + 35 - 16 - 11 - 7 + 2$$

$$= 136.$$

The number of integers which are divisible by 3 or 7 but not by 5 is $|(A_1 \cup A_3) \cap \overline{A_2}|$

$$|(A_1 \cup A_3) \cap \overline{A_2}| = |A_1 \cap \overline{A_2} \cap \overline{A_3}| + |\overline{A_1} \cap \overline{A_2} \cap A_3| + |A_1 \cap \overline{A_2} \cap A_3|.$$

$$= 58 + 19 + 9.$$

The number of integers which are divisible by 3 or 5 is $|A_1 \cup A_3|$

$$|A_1 \cup A_3| = |A_1| + |A_3| - |A_1 \cap A_3| = 83 + 35 - 11 = 107.$$

* Find how many integers between 1 and 60 that are divisible by 2 not by 3 and not by 5. Also determine the number of integers divisible by 5 not by 2 not by 3.

let $S = \{1, 2, \cdots 60\}$ then $N = n(S) = 60$

let $|A_1|$ = The number of integers which are divisible by 2

$$|A_1| = \left\lfloor \frac{60}{2} \right\rfloor = 30.$$

let $|A_2|$ = The number of integers which are divisible by 3.

$$|A_2| = \left\lfloor \frac{60}{3} \right\rfloor = 20.$$

let $|A_3|$ = The number of integers which are divisible by 5.

$$|A_3| = \left\lfloor \frac{60}{5} \right\rfloor = 12$$

$|A_1 \cap A_2|$ = The number of integers which are divisible by 2 and 3.

$$|A_1 \cap A_2| = \left\lfloor \frac{60}{Lcm(2,3)} \right\rfloor = 10.$$

$|A_2 \cap A_3|$ = The number of integers which are divisible by 3 and 5

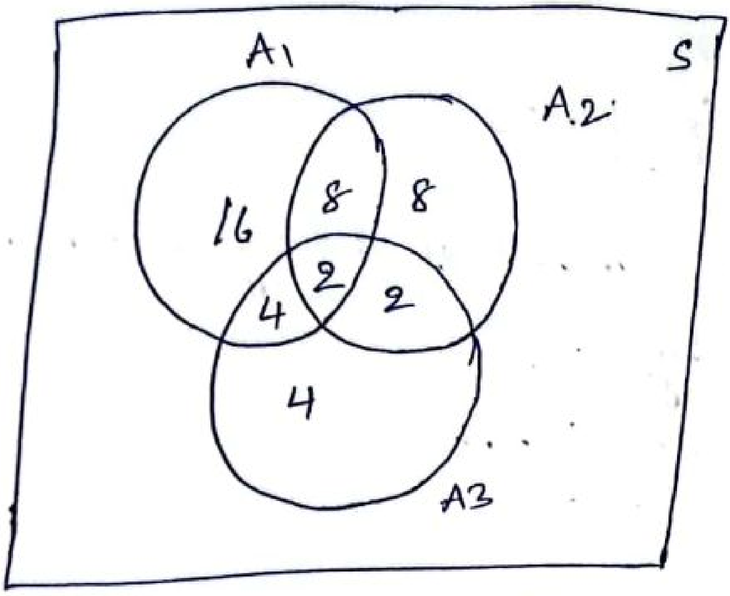
$$|A_2 \cap A_3| = \left\lfloor \frac{60}{Lcm(3,5)} \right\rfloor = \left\lfloor \frac{60}{15} \right\rfloor = 4$$

$|A_1 \cap A_3|$ = The number of integers which are divisible by 2 and 5.

$$|A_1 \cap A_3| = \left\lfloor \frac{60}{\text{Lcm}(2,5)} \right\rfloor = 6$$

Similarlly.

$$|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{60}{\text{Lcm}(2,3,5)} \right\rfloor = \frac{60}{30} = 2.$$



From the above ven diagram.

The number of integers which are divisible by 2 not by 3 and not by 5 is

$$|A_1 \cap \overline{A_2} \cap \overline{A_3}| = |A_1| - |A_1 \cap A_2 \cap \overline{A_3}| - |A_1 \cap \overline{A_2} \cap A_3| - |A_1 \cap A_2 \cap A_3|$$

$$= 30 - 8 - 4 - 2 = 16.$$

The number of integers which are divisible by 5 not by 2, not by 3 is

$$|\overline{A_1} \cap \overline{A_2} \cap A_3| = |A_3| - |\overline{A_1} \cap A_2 \cap A_3| - |A_1 \cap \overline{A_2} \cap A_3| - |A_1 \cap A_2 \cap A_3|$$

$$= 12 - 4 - 2 - 2 = 4.$$

* Pigeon hole principle and its application :—

Statement : If m pigeons are assigned to n pigeon holes and $m>n$ then two or more pigeon occupies the same pigeon hole.

(or)

In other words, m pegeons occupies n pigeon holes and if $m>n$ then atleast one pigeon hole must contains two or more pigeons in it.

The extended pigeon hole principle :—

If m pigeons are assigned to n pigeon holes then one of the pigeon hole must contain $\left[\frac{m-1}{n}\right]+1$ pigeons.

Note:

To apply the principle, we must decide which objects will play the role of pigeon and which objects will play the role of pigeon hole.

* Show that if 8 people are in a room, at least two of them have birthdays that occur on the same day of the week.

let $m=8$ and $n=7$.

(ie) ~~the~~ Treat the 8 people as the pigeons and 7 days of the week as the pigeon holes.

Here $8>7$.

(ie) $m>n$

Then by using the pigeon hole principle, we can say that atleast two people have birthday on the same day of the week.

* Applying pigeon hole principle show that of any 14 integers are selected from the set $S=\{1,2,3,\cdots 25\}$ there are atleast two whose sum is 26. Also write a statement that generalizes this result.

Given $S=\{1,2,3,\cdots 25\}$

let the integer sets having the sum 26 as

$S_1=\{1,25\}$, $S_2=\{2,24\}$, $S_3=\{3,23\}$ $S_4=\{4,22\}$

$S_5=\{5,21\}$, $S_6=\{6,20\}$, $S_7=\{7,19\}$, $S_8=\{8,18\}$

$S_9=\{9,17\}$, $S_{10}=\{10,16\}$, $S_{11}=\{11,15\}$, $S_{12}=\{12,14\}$

$S_{13}=\{13,13\}$.

Treat 14 integers as the pigeons and $s_1, s_2, \dots s_{13}$ are the pigeons holes then

$m = 14, \quad n = 13.$

$$\left\lfloor \frac{m-1}{n} \right\rfloor + 1 = \left\lfloor \frac{14-1}{13} \right\rfloor + 1 = 2.$$

Here $m > n$ (ie $14 > 13$)

then by using pigeon hole principle,

at least one integer set must be repeated twice.

If $S = \{1, 2, 3, \dots 2n+1\}$, for a positive integer n. Then any subset of size $n+2$ from the set S must contain at least one two element subset whose sum is $2n+2$.

* Find the minimum number of students in a class to be sure that 4 out of them are born on the same month.

Here we have to find the number of pigeons m and using the extended principle of 4 students were born on the same month.

The no of months in a year $= 12$.

$$\left\lfloor \frac{m-1}{n} \right\rfloor + 1 = 4$$

$$\left\lfloor \frac{m-1}{12} \right\rfloor + 1 = 4$$

$$\frac{m-1}{12} = 3.$$

$$m-1 = 36$$

$$m = 37.$$

Functions:-

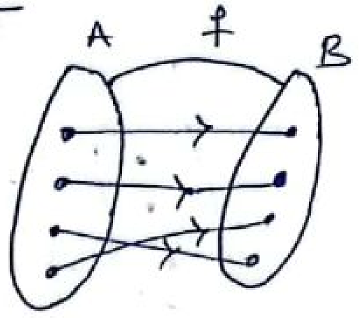
Let A and B be two non-empty sets, a function f from A to B is a set of ordered pairs $f \subseteq A \times B$ with the property that for each element x in A. there is a unique element y in B such that $(x, y) \in f$. The statement f is a function from A to B is usually represented symbolically by $f: A \rightarrow B$.

Types of functions:-

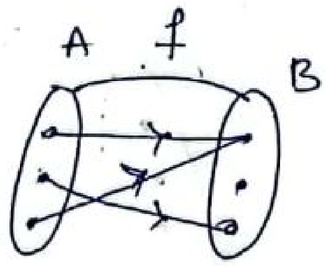
① one-one function:-

A function from A to B. is one-one or into or Ijective function for all $x_1, x_2 \in A$ such that $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Example:-



f is one-one

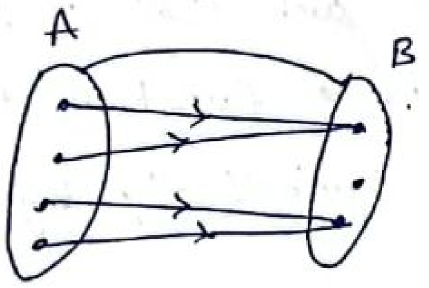


f is not one one.

② Many to one function:-

A function f from A to B is said to be many to one function iff two or more elements of A have the same ~~but~~ image in B.

<u>Example:</u> $f(x)=x^2$ is many-one function.

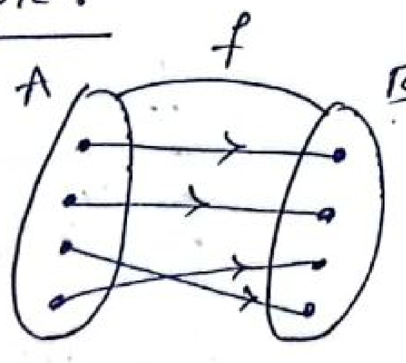


many to one function.

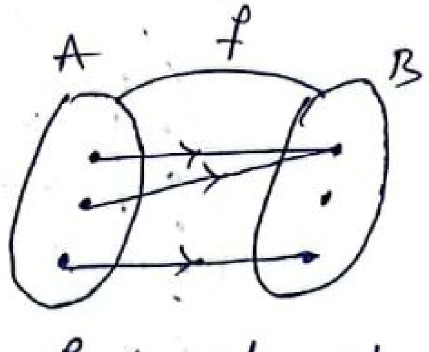
③ Onto function:-

A function $f: A \to B$ is onto function if every element of B has a pre image in A (i.e) Codomain of B = Range of f.

<u>Example:</u>



f is onto

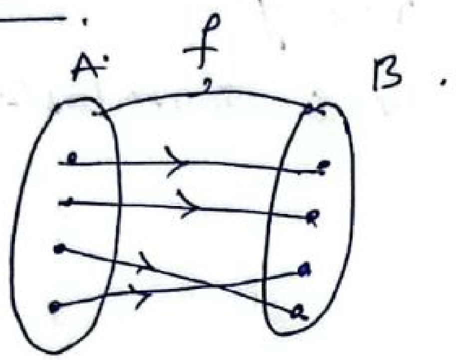


f is not onto.

(4) Bijective function :-

A function $f : A \to B$ is said to be bijective if it is both one-one and onto.

Example:



f is bijective.

(5) Identity function :-

A mapping $I_x : x \to x$ is called an identity function if and only if $I_x = \{(x, x) / x \in X\}$

thus $f : A \to A$ is said to be identity function if and only if $f(x) = x \;\; \forall \; x \in X$.

* Composition of functions :-

It is given by, let $f : A \to B$ and $g : B \to C$. The composition of f and g is denoted by gof is a new function from $A \to C$

$(gof)(x) = g[f(x)], \; \forall \; x \in A$

$$\begin{tikzcd} a \arrow[r, "f"] \arrow[rr, bend right, "gof"'] & f(a) \arrow[r, "g"] & g(f(a)) \end{tikzcd}$$

* ## Inverse functions: —

If $f: X \to Y$ is bijective then $f^{-1}: Y \to X$ is a function and f^{-1} is called the inverse of f.

Thus $f(x) = y \iff x = f^{-1}y$.

A function $f: X \to Y$ is invertable iff it is bijective.

* let $f: R \to R$ such that $f(x) = 2x+1$, $g: R \to R$ such that $g(x) = \frac{x}{3}$ then verify that $(gof)^{-1} = f^{-1} o g^{-1}$

Given f and g are bijective function $\forall x \in R$ then they are invertable.

Given $f(x) = 2x+1$, $g(x) = \frac{x}{3}$

Now, $(gof)(x) = g[f(x)]$

$$= g[2x+1]$$

$$= \frac{2x+1}{3}.$$

let $y = (gof)(x)$

$$y = \frac{2x+1}{3}.$$

$$2x = 3y - 1$$

$$x = \frac{3y-1}{2}.$$

$$(gof)^{-1}(x) = \frac{3x-1}{2}.$$

Now, let $y = f(x)$

$$y = 2x+1$$

$$x = \frac{y-1}{2}.$$

$$f^{-1}(x) = \frac{x-1}{2}$$

let $y = g(x)$

$$y = \frac{x}{3}$$

$$x = 3y$$

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

$$(f^{-1} o g^{-1})(x) = f^{-1}[g^{-1}(x)]$$

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

$$= \frac{3x-1}{2}$$

$$= (gof)^{-1}(x).$$

Hence, $(gof)^{-1} = f^{-1} o g^{-1}$.

* Verify $f(x) = 2x+1$, $g(x) = x$ $\forall x \in R$ are bijective from $R \to R$.

Given $f(x) = 2x+1$.

<u>One-one:-</u> let $x_1, x_2 \in R$.

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

$$2x_1+1=2x_2+1$$

$$2x_1=2x_2$$

$$x_1=x_2.$$

f is one-one.

onto :- let $y=f(x)$

$$y=2x+1$$

$$x=\frac{y-1}{2}\in R$$

$\forall\ y\in R \Rightarrow x\in R.$

f is onto.

$\therefore$ f is bijective.

Also given $g(x)=x$.

one-one ; let $x_1, x_2 \in R$.

$$g(x_1)=g(x_2)$$

$$x_1=x_2$$

g is one-one.

onto :
let $y=g(x)$

$$y=x$$

$$x=y\in R.$$

$\forall\ y\in R \Rightarrow x\in R.$

g is onto.

$\therefore$ g is bijective.

CamScanner

* let $f: A \to B$, $g: B \to C$ and $h: C \to D$

then $ho(gof) = (hog)of$.

let $f: A \to B$, $g: B \to C$, $h: C \to D$.

By Composition of functions

$gof: A \to C$, $hog: B \to D$.

$ho[gof]: A \to D$, $[hog]of: A \to D$.

So. domain $ho(gof)$ = domain $(hog)of$.

let $x \in A$, $y \in B$, $z \in C$ such that

$f(x) = y$, $g(y) = z$.

Then $[ho(gof)](x) = h[g[f(x)]]$

$= h[g(y)]$

$= h(z)$

$[(hog)of](x) = h[g[f(x)]]$

$= h[g(y)]$

$= h[z]$

Hence, $ho(gof) = (hog)of$.

* Recursive functions:-

A function $f(x)$ is to specify the value of $f(x)$ for some particular values of x and then to indicate how the remaining values of $f(x)$ can be got with the aid of these specified values, we say that the function is defined recursively, which is also referred to as a recursive function.

Example:- let $f(x) = n!$

The explicit method of decribing this function as $f(0)=1$ and $f(n) = 1 \cdot 2 \cdot 3 \cdots n$ for $n \in z^+$

The recursive method of describing this function as $f(0)=1$, $f(n) = n f(n-1)$ for $n \in z^+$.

In this method of description of f, the value of $f(n)$ for $n=0$ is first specified and then a formula for obtaining the remaining values of $f(n)$ with the aid of this specified value is indicated.

CamScanner

* A function $f(n) = a^n$ is defined recursively by $a_0 = 4$ and $a_n = a_{n-1} + n$ for $n \geq 1$. Find $f(n)$ in explicit form.

Given $a_0 = 4$ and $a_n = a_{n-1} + n$ for $n \geq 1$

using the given recursive formula repeatedly, we find that

$$
\begin{aligned}
a_n &= a_{n-1} + n \\
&= [a_{n-2} + (n-1)] + n \\
&= [a_{n-3} + (n-2)] + (n-1) + n. \\
&= [a_{n-4} + (n-3)] + (n-2) + (n-1) + n. \\
&\quad \cdots\cdots\cdots \\
&= (a_1 + 2) + 3 + \dots + n. \\
&= (a_0 + 1) + 2 + 3 + \dots + n \\
&= 4 + 1 + 2 + 3 + \dots + n.
\end{aligned}
$$

$$a_n = 4 + \frac{n(n+1)}{2}.$$

This is the explicit formula for $f(n) = a_n$.

Relation (or) Binary relation :-

let A and B are two non-empty sets.

A binary relation or simply a relation from A to B is a subset of $A \times B$.

Given $x \in A$ and $y \in B$, we write xRy if $(x,y) \in R$

and $x \not R y$ if $(x,y) \notin R$

If R is a relation from A to A, then R is said to be relation on A.

Properties of relations :—

Reflexive : $(a,a) \in R$ (i.e) aRa for all $a \in A$.

Symmetry : $(a,b) \in R \Rightarrow (b,a) \in R$ for all $a, b \in A$.

Anti symmetry : $(a,b) \in R$, $(b,a) \in R \Rightarrow a = b$ for all $a, b \in A$

Transitivity :- $(a,b) \in R$ & $(b,c) \in R \Rightarrow (a,c) \in R$ for all $a, b, c \in A$.

Partially ordered set :—

A relation R on a set S, is called a partial order or partial ordering ~~or Poset~~ if it is reflexive, anti symmetric, and transitive.

(i.e) ① aRa for all $a \in S$ (reflexive)

② aRb and $bRa \Rightarrow a = b$ (anti symmetric)

③ aRb and $bRc \Rightarrow aRc$ (transitivity)

A set together with a partial order R is called a partially ordered set or a poset. It is denoted by (S, R).

Upper bound and lower bound :-

let $(A, \leq)$ be a poset and B is a subset of A. An element $u \in A$ is called an upper bound of B if u succeeds every element of B (i.e) $x \leq u$ for all $x \in B$.

An element $l \in A$ is called a lower bound of B if l preceeds every element of B (i.e) $l \leq x$ for all $x \in B$.

* If $B \subseteq A$ and $a \in A$ then 'a' is called the least upper bound of B if

① a is upper bound of B

② $a \leq a'$ for every upper bound a' of B

It is also called supremum of B.

and is denoted by $\sup B$. (or) lub B.

* If $B \subseteq A$ and $b \in B$ then b is called the greatest lower bound of B or infimum of B, then
① b is the lower bound of B.
② $b' \leq b$ for every lower bound b' of B
It is denoted by glb of B (or) inf B.

* Lattices and its properties:—

A poset $(P, \preceq)$ is called a lattice if every 2-element subset of P has both a least upper bound and greatest lower bound (i.e) if lub (x,y) and glb (x,y) exists for every x and y in P. In this case, we denote

$x \vee y =$ lub $\{x,y\}$ [read as join of x and y or x join y]

$x \wedge y =$ glb $\{x,y\}$ [read as meet of x and y or x meet y]

In a poset $(P, \preceq)$, the relation is usually denoted by $\preceq$. (read as less than or equal) and $a \preceq b$ is read as a preceeds b
$b \succeq a$ is read as b succeeds a.

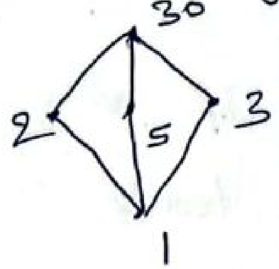
* If $A = \{1,2,3,5,30\}$ and R is the divisibility relation, Prove that (A, R) is a Lattice but not a distributive Lattices.

Given $A = \{1,2,3,5,30\}$

Relation R is divisibility relation.

we have to show that (A, R) is a lattice but not a distributive Lattice.

Hasse diagram



Least upper bound table:-

∨	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

By observing the LUB table, for every pair of elements on set A, LUB is exist.

Greatest lower bound table:-

∧	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30

By observing the GLB table, for every pair of elements on set A, GLB exist.

For every pair of elements in set A, both LUB and GLB exists.

Hence we can say that $\langle A, R \rangle$ is a lattice.

A lattice is distributive lattice iff it satisfies the conditions.

① $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

② $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

verify ① $a=2,\ b=3,\ c=5 \quad \forall\ a, b, c \in A$

$$2 \vee (3 \wedge 5) = (2 \vee 3) \wedge (2 \vee 5)$$

$$2 \vee 1 = 30 \wedge 30$$

$$2 \neq 30 \text{ (not satisfied.}$$

$\langle A, R \rangle$ is not a distributive lattice.

Properties of lattices:-

let (L, R) be a lattice.

① Idempotent property :- ① $a \vee a = a$ ② $a \wedge a = a$

② Commutative property :- ① $a \vee b = b \vee a$
② $a \wedge b = b \wedge a$

③ Associative property :- ① $a \vee (b \vee c) = (a \vee b) \vee c$
② $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

④ Absorption property :- ① $a \vee (a \wedge b) = a$
$a \wedge (a \vee b) = a$.

Algebraic structures

* Algebraic systems - Examples and General properties:-

Binary and n-ary operation:-

let X be a set and f be a mapping $f: X \times X \to X$ then f is said to be a binary operation on X.

In general, a mapping $f: X^n \to X$ is called an n-ary operation and n is called the order of the operation.

for $n=1$, $f: X \to X$ is called a unimary operation.

for $n=2$, $f: X \times X \to X$ is called a binary operation.

The binary operations are generally denoted by the symbols $*$, $+$, $\times$, $-$, $\div$, $\otimes$, $\oplus$, Δ etc.

Algebraic systems:-

A system consisting of a set and one or more n-ary operations on the set will be called an algebraic systems or simply an algebra or algebraic structure.

we shall denote an algebraic system by $(S, f_1, f_2, \ldots)$ where s is a non-empty set and $f_1, f_2, \ldots$ are operations on S.

Examples:-

① Since $+, \times$ are binary operations on Z, the system $(Z, +, \times)$ is an algebraic structure.

② Let S be a non-empty set, then the cartesian product $S \times S$ is the set of all ordered pairs of elements of S. A function from $S \times S$ to S is called a binary operation on S.

General properties:-

Let G be a set and $(G, *, \Delta)$ is an algebraic system then the properties of these binary operations $*, \Delta$ is given by.

① closure law:- For any $a, b \in G$, $a * b \in G$ then G is said to be closure

② Associative:- For any a, b and $c \in G$ then $a * (b * c) = (a * b) * c$

③ Identity:- For $a \in G$, $e \in G$.

If $a * e = e * a = a$ then 'e' is called an identity element in G.

Note: ① '0' is additive identity element (ie) $a + 0 = 0 + a = a$.

Note: (2) '1' is the multiplicative identity 3

(ie) $a \times 1 = 1 \times a = a$.

(4) Inverse: For any $a, b \in G$, If $a * b = e$ then b is called an inverse element of a.

(5) Commutative property:— For any $a, b \in G$ then $a * b = b * a$.

(6) Distributive:— For any $a, b, c \in G$ then

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

(7) Cancellation laws:— For any $a, b, c \in G$. and $a \neq 0$ then $a * b = a * c \Rightarrow b = c$ (left cancellation)

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

* Semi groups and monoids:—

Semi group:-

let S be a non-empty set $\circ$ be a binary operation on S. The algebraic system $(S, \circ)$ is called a semi group if the following conditions satisfied.

(1) operation $\circ$ is closed (ie) $a \circ b \in S$ for all $a, b \in S$.

(2) Operation $\circ$ is associative (ie) $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in S$

In otherwords (S, o) is a semi group

if ① for any $a, b \in S$, $a o b \in S$

② for any $a, b, c \in S$, $(a o b) o c = a o (b o c)$

Example: The set Z of all integers is closed under addition and associative under addition.

So $(Z, +)$ is a semi group.

Monoid: A semi group (M, o) with an identity element with respect to the operation o is called a monoid.

In otherwards, an algebraic system (M, o) is called a monoid if ① for any $x, y, z \in M$, $x o y \in M$

② for any $x, y, z \in M$, $(x o y) o z = x o (y o z)$.

③ there exist an element $e \in M$ such that for any $x \in M$, $e o x = x o e = x$.

Examples:

① let $(N, \times)$ is a monoid with identity 1.

② If E denotes the set of positive even number then $(E, +)$, $(E, \times)$ are semigroups but not monoids.

③ let s be a non empty set and $P(S)$ be its power set, the algebra $(P(S), \cup)$ and $(P(S), \cap)$ are monoids with the identities ϕ and s respectively.

Note: A monoid has a unique identity element e.

Groups:-

A group $(G, *)$ is an algebraic system in which the binary operation $*$ on G satisfies following conditions.

① for all $x, y \in G$.

$x * y \in G$ (Closure)

② for all $x, y, z \in G$.

$x * (y * z) = (x * y) * z$ (Associative)

③ There exist an element $e \in G$ such that for any $x \in G$, $x * e = e * x = x$ (Identity)

④ For every $x \in G$, there exists an element denoted by $x^{-1} \in G$ such that

$x^{-1} * x = x * x^{-1} = e$ (Inverse)

Abelian group:- A group $(G, *)$ in which the operation $*$ is commutative is called an abelian group.

Examples:

① The set z of integers, $(z,+)$ is an abelian group.

Here z is closed, associative under addition

Also '0' is the identity element.

$-a$ is the additive inverse of a.

② The set of rational numbers excluding zero is an abelian group under multiplication.

Problems:-

* Prove that the set z of all integers with the binary operation $*$ defined as $a*b = a+b+1 \ \forall \ a,b \in z$ is an abelian group.

Given $*$ is a binary operation on z defined by $a*b = a+b+1 \ \forall \ a,b \in z$.

Closure: for any $a,b \in z$.

$$a*b = a+b+1 \in z.$$

$*$ is closued.

Associative: for any a,b and $c \in z$.

$$a*(b*c) = a*(b+c+1)$$
$$= a+b+c+1+1$$
$$= a+b+c+2$$

$$(a*b)*c = (a+b+1)*c$$
$$= a+b+1+c+1$$
$$= a+b+c+2$$
$$\therefore (a*b)*c = a*(b*c)$$

Hence $*$ is associative.

Identity: let e is the identity element in z

$\forall\ a \in z$, $a*e = a$
$$a+e+1 = a$$
$$e+1 = 0$$
$$e = -1 \in z.$$

$e=-1$ is the identity element for $(z, *)$

Inverse: let the integer 'a' have its inverse b, then $\forall\ a \in z$.
$$a*b = e$$
$$a+b+1 = -1.$$
$$a+b = -2$$
$$b = -2-a \in z.$$

The inverse element of a is $-2-a$.

Commutative: For any $a, b \in z$ then
$$a*b = a+b+1$$
$$= b+a+1$$
$$= b*a.$$
$$a*b = b*a.$$

$(z, *)$ is commutative.

Thus the operation satisfies closure, Associative identity, inverse and commutative.

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

* Show that the binary operation $*$ defined on $(R, *)$ where $x*y = x^y$ is not associative.

Given $x*y = x^y$.

we have to show that $(R, *)$ is not associative.

$$(x*y)*z = x^y * z.$$
$$= (x^y)^z.$$
$$= x^{yz},$$

$$x*(y*z) = x*(y^z)$$
$$= x^{y^z}.$$

$$x*(y*z) \neq (x*y)*z.$$

Hence $(R, *)$ is not associative.

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

let Q^+ denotes the set of all positive rational number, we have to show that $(Q^+, *)$ is an abelian group under

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

<u>Closure:</u> for any $a * b \in Q^+$.

$$a * b = \frac{ab}{2} \in Q^+.$$

$(Q^+, *)$ is closued.

<u>Associative:</u> For any $a, b, c \in Q^+$.

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

$$= \frac{\frac{ab}{2} \cdot c}{2}$$

$$= \frac{abc}{4}.$$

$$a * (b * c) = a * \frac{bc}{2}$$

$$= \frac{a \cdot \frac{bc}{2}}{2}$$

$$= \frac{abc}{4}.$$

$(Q^+, *)$ is associative.

<u>Identity:</u> let e be the identity element in Q^+ such that $a * e = a$.

$$\frac{ae}{2} = a$$

$$e = 2 \in Q^+.$$

$e = 2$ is the identity element in Q^+.

<u>Inverse:</u> let $a \in Q^+$, b is inverse of a.

then $a * b = e$.

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

$$ab = 4$$

$$b = \frac{4}{a} \in Q^+ .$$

The inverse of a is $\frac{4}{a}$

Commutative : For any $a, b \in Q^+$.

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

$$= \frac{ba}{2}$$

$(Q^+, *)$ is commutative.

Thus, $(Q^+, *)$ satisfies closure, associative identity, inverse and commutative properties.

Hence, $(Q^+, *)$ is an abelian group

* Show that the set $\{1, 2, 3, 4, 5\}$ is not a group under addition and multiplication modulo 6.

let $G = \{1, 2, 3, 4, 5\}$.

(1) The operation addition modulo 6 is denoted by $+_6$. we can operate $+_6$ on the elements in G and prepare composition table as

I

In this system $(G, +_6)$.

$2 +_6 5 = 1 \Rightarrow 2+5 = 7 = 1 \times 6 + 1 \Rightarrow$ remainder $= 1$

$1 +_6 4 = 5 \Rightarrow 1+4 = 5 = 0 \times 6 + 5 \Rightarrow$ remainder $= 5$.

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

Since all the entries in the composition table do not belongs to G in particular $0 \notin G$.

Hence G is not closed with respect to $+_6$. $(G, +_6)$ is not a group.

(2) The operation multiplication modulo 6 is denoted by $\times_6$. The composition table for $\times_6$ is given below.

$2 \times_6 5 = 10 = 1 \times 6 + 4 \Rightarrow$ remainder $= 4$

$5 \times_6 5 = 25 = 4 \times 6 + 1 \Rightarrow$ remainder $= 1$

$\times_6$	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

Since all the entries in the composition table do not belong to G. In particular $0 \notin R$. Hence G is not closed w.r.to $\times_6$. $(G, \times_6)$ is not a group.

* Show that the set of all roots of the equation $x^4 = 1$ forms a group under multiplication.

Given, $x^4 = 1$

$x^4 - 1 = 0$

$(x^2+1)(x^2-1) = 0$

$x^2 = 1, \quad x^2 = -1$

$x = \pm 1 \quad x = \pm i$

The roots of $x^4 = 1$ are $1, -1, i, -i$

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

The composition table is given by

×	1	−1	i	−i
1	1	−1	i	−i
−1	−1	1	−i	i
i	i	−i	−1	1
−i	−i	i	1	−1

Since all the entries in the above table are the elements of G.

Associative: $\forall\ a, b, c \in G$ then

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

Identity: For any $a \in G$, $1 \in G$:

$$a \times 1 = 1 \times a = a$$

1 is the identity element.

Inverse: The inverse of 1, −1, i, −i are 1, −1, −i, i respectively and all the elements belongs to G.

Hence G is a group under multiplication.

* On the set Q of all rational number, the operation * is defined by $a * b = a + b - ab$. Show that this operation and Q formes a commutative monoid.

let Q be the set of all rational numbers.

Given $a * b = a + b - ab$.

Closure: let $a, b \in Q$.

$a * b = a + b - ab \in Q$.

$(Q, *)$ is closed.

Associative: $\forall$ $a, b, c \in Q$ then

$$a * (b * c) = a * (b + c - ab)$$
$$= a + (b + c - abc) - a(b + c - abc)$$
$$= a + b + c - bc - ab - ac + abc$$
$$= (a + b - ab) + c - c(a + b - ab)$$
$$= (a * b) + c - c(a * b)$$
$$= (a * b) * c.$$

Identity: let $e \in Q$, $\forall$ $a \in Q$ then

$$a * e = a$$
$$a + e - ae = a$$
$$e(1 - a) = 0$$
$$e = 0$$

$e = 0 \in Q$ is an identity element.

Commutative: $\forall$ $a, b \in Q$ then

$$a * b = a + b - ab$$
$$= b + a - ba.$$
$$= b * a$$

Hence $(Q, *)$ is commutative.

Thus, $(Q, *)$ forms a commutative monoid.

CamScanner

* Sub groups:

let $(G, *)$ be a group and $S \subseteq G$ be such that it satisfies the following conditions.

1. $e \in S$, where e is the element of $(G, *)$
2. any $a \in S$, $a^{-1} \in S$
3. $a, b \in S$, $a * b \in S$ then $(S, *)$ is called subgroup of $(G, *)$.

Note:

1. $(S, *)$ itself is a group with the same identity element as that of $(G, *)$.
2. All other subgroup of $(G, *)$ are called proper subgroups except $(\{e\}, *)$ and $(G, *)$ and these are called trivial subgroups of $(G, *)$.

Theorem: Prove that the necessary and sufficient condition for a non-empty subset H of a group $(G, *)$ to be a group is $a \in H$, $b \in H \Rightarrow a * b^{-1} \in H$ where b^{-1} is the inverse of b in G.

Proof: let H be a subgroup and

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

Since H is a sugroup and $b \in H \Rightarrow b^{-1}$ must exist in H.

Now $a \in H$, $b^{-1} \in H \Rightarrow a * b^{-1} \in H$ by closure property.

Thus the condition is necessary.

Next, to prove that this condition is also sufficient.

First we assume that $a \in H$, $b \in H \Rightarrow a * b^{-1} \in H$.

we have to prove that H is a Sub group of G.

By given condition, we have $a \in H$, $a^{-1} \in H$

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

where e is the identity element

Again we have $e \in H$, $a \in H \Rightarrow e * a^{-1} \in H$

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

where a^{-1} is the inverse of a.

Now, if $b \in H$ then $b^{-1} \in H$.

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

$\Rightarrow a * b \in H$ (Closure property)

Now $H \subset G$ and the associative law holds ~~good~~ good for G as G is a group.

Hence it is true for the element of ~~H~~ H

$\therefore$ H is a subgroup of G.

* Homomorphism :-

let g be a homomorphism from $(X, *)$ to (Y, o). If $g : X \to Y$ is said to be homomorphism of two algebraic systems $(X, *)$ to (Y, o) then $x_1, x_2 \in X$.

$$g(x_1 * x_2) = g(x_1) \circ g(x_2)$$

Here, (Y, o) is called a homomorphic image of (X, o) although $g(X) \subseteq Y$.

Monomorphism :-

let g be a homomorphism from $(X, *)$ to (Y, o). If g is one-one then g is called Monomorphism.

Epimorphism :-

let g be a homomorphism from $(X, *)$ to (Y, o). If $g : X \to Y$ is onto, then g is called an epimorphism.

* Isomorphism :-

let G be a homomorphism from $(X, *)$ to (Y, o). If $g : X \Rightarrow Y$ is one-one and onto then g is called an isomorphism.
In this case $(X, *)(Y, o)$ are said to be isomorphic.

Endomorphism and automorphism:-

let $(X, *)$ and (Y, o) be two algebraic structures such that $Y \subseteq X$. A homomorphism g from $(X, *)$ to (Y, o) in such a case is called an endomorphism

If $Y = X$ then an isomorphism from $(X, *)$ to (Y, o) is called an automorphism.

* let $S = \{a, b, c\}$ and let $*$ denote a binary operation on S given by following table. Also let $P = \{1, 2, 3\}$ and $\oplus$ be a binary operation on P given by following table show that $(S, *)$ and $(P, \oplus)$ are isomorphic.

$*$	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

$\oplus$	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

Consider a mapping $g : S \to P$ given by $g(a) = 3$, $g(b) = 1$, $g(c) = 2$.

The binary operation tables are given by 19.

$*$	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

$\oplus$	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

Now for $a, b \in S$.

$g(a*b) = g(b)$ from table
$= 1$

Also $g(a) \oplus g(b) = 3 \oplus 1$
$= 1$
$= g(a*b)$

$g(a*b) = g(a) \oplus g(b)$

Hence g is homomorphism.

Also g is one-one and there is no element with out pre image

g is onto

$\therefore$ g is homomorphism, one-one and onto

Hence g is isomorphism.