Sets

Date

⇒ Set

A set is a well-defined collection of distinct objects, called elements or members of the set.

Always denoted by "Capital Letters".

For example –

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

we can say

$1 \in A$ $\quad \in \Rightarrow$ belongs to

$2 \in A$

$5 \notin A$ $\quad \notin \Rightarrow$ doesn't belongs to

Elements are denoted by "Lowercase Letters".

⇒ Representation of set

There are three ways to describe a set.

(a) Roster method

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

(b) Description form

$$A = \{\text{Natural numbers less than } 5\}$$

(c) Set-builder form

$$A = \{x : x \text{ is a Natural no. less than } 5\}$$

OR

$$\{x : x \in N \text{ and } x < 5\}$$

N = Natural numbers
Z = Set of all Integers
Z^+ = Set of all +ve Integers
Q = Set of all Rational numbers
R = Set of all Real numbers
C = Set of all Complex numbers

Date

⇒ Types of Sets

(a) Equal Sets

Two sets A and B are said to be equal if all elements of A is present in B and also number of elements is equal.

For example —

$A = \{1, 2, 3\}$ and $B = \{1, 2, 3\}$

$C = \{1, 2, 3\}$ and $D = \{3, 2, 1\}$

Here,

All sets A, B, C, and D all are equal

(b) Empty Set or Null Set or Void Set

A set A is said to be empty if it doesn't contain a single element.

It is denoted by "ϕ"

For example —

$A = \{x : x \in N \text{ and } x < 1\}$

Here $A = \{\}$ or ϕ

(c) Non-Empty Set

A set which contains atleast one element is said to be non-empty set.

(d) Singleton Set

A set which contains exactly one element is said to be singleton set.

(e) Finite Set

A set which contains a finite number of elements is said to be finite.

Date

⑧ Infinite Set
A set which contains infinite number of elements is said to be infinite set.

⑨ Equivalent Set
Two sets A and B are said to be equivalent if both have same number of elements.
For example –

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

Here, A and B are equivalent.

$C = \{1,2,3\}$ and $D = \{2,1,3\}$

Here, C and D are both equal and equivalent.

⇒ Cardinal number
The total number of elements present in a set is known as its cardinal number or its cardinality. Denoted by $n(S)$ or $|S|$.

Thus, Cardinality of a Null Set, ϕ is $= 0$
Caridinality of a Singleton Set is $= 1$
Cardinality of an Infinite Set is $= \infty$

Cardinality of a set is also called the "Order of a Set".

⇒ Subsets
A set A is said to be the subset of B if every element of A is present in B also. It is denoted by $\subseteq$

Thus

$A \subseteq B$

Date

If A is not subset of B then it is denoted as $A \not\subseteq B$.

NOTE: A set is also a subset of itself.

Proper Subset :-
If A is a subset of B, $A \subseteq B$ and $A \neq B$, then A is called the proper subset of B. It is denoted as $A \subset B$.
For example —

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

$C = \{1,2,3\}$

Here, B is a subset of A , $B \subseteq A$
But C is a proper subset of A, $C \subset A$

Superset :-
A set A is said to be the superset of B if all elements of B are also elements of A.
Means if $B \subseteq A$ then B is subset of A and A is Superset of B
It is denoted as

$A \supset B$ (Opposite)

Universal Set :-
A set which contains all the sets given is known as a Universal set.
For example—

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

Then

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

Date

⇒ No. of Subsets

Suppore, A set contains n elements.

$$S = \{1, 2, 3, \ldots, n\}$$

For creating subset we will have to choose elements one-by-one.

Means

1^{st} case $- {}^nC_0$

2^{nd} case $- {}^nC_1$

3^{rd} case $- {}^nC_2$

$\vdots$

n^{th} case $- {}^nC_n$

Total $\Rightarrow {}^nC_0 + {}^nC_1 + {}^nC_2 + \cdots + {}^nC_n$

Now,

we know $(x+y)^n = {}^nC_0 x^n y^0 + {}^nC_1 x^{n-1} y + \ldots + {}^nC_n x^0 y^n$

Putting $x = 1, y = 1$

$$2^n = {}^nC_0 + {}^nC_1 + {}^nC_2 + \cdots + {}^nC_n$$

Thus,

Total no. of subsets = $\boxed{2^n}$

⇒ Power Set

A power set is a set of all subsets of a given set.

For example – If $A = \{1, 2\}$

Then

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

Thus

Cardinality of Power Set $= 2^n$

NOTE: Power set of a Empty Set is Empty itself.

Date

Que How many subset of a set containing first 25 natural no. can be formed, so that the least element is 3 and largest element is 22.

⇒ As given,

Least element should be 3
and Max. " " " 22

So, Available no. of elements = 25 - {1, 2, 3, 22, 23, 24, 25}

= 25 - 7

= 18

Thus, No. of subsets = 2^{18} Ans

Que If A and B are two sets taking from Universal set U which contains n elements. In how many ways, A and B are taken such that $A \cup B = U$.

⇒ We will choose elements from U in three ways :—

	A	U	B	=	U
Case 1 ⇒	✓		×		
	Only in A				
Case 2 ⇒	×		✓		
	Only in B				
Case 3 ⇒	✓		✓		
	In both A and B				

Thus, Total no. of ways = 3^n

Date

⇒ Cartesian Products

Let A and B are two sets. The Cartesian product of A and B, denoted by $A \times B$ is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

Hence,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Que What is the Cartesian Product of $A = \{1, 2\}$ and $B = \{a, b, c\}$?

⇒ Here, Cartesian Product, $A \times B = \{(a, b) \mid a \in A, b \in B\}$

So,

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

NOTE :- (i) $A \times B \neq B \times A$

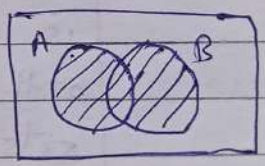
(ii) $n(A \times B) = n(A) \times n(B)$

⇒ Set Operations

(a) Union of Sets

Let A and B are two sets. The union of the sets A and B, denoted by $A \cup B$ is the set that contains all elements that are either in A or in B, or in both.

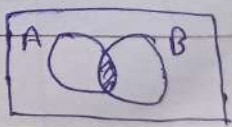
$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$



(b) Intersection of Sets

The intersection of two sets A and B, denoted by $A \cap B$ is the set that contains all elements that are present in both A and B.

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

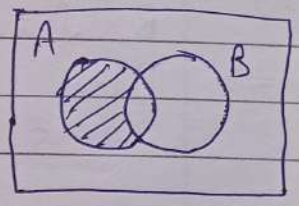


Date

(c) Disjoint Sets:
Two sets are called disjoint if their intersection is a null set or empty set.

(d) Difference of two Sets
The difference of two sets A and B, denoted by A-B is the set of elements that are only in A not in B.

$$A - B = \{x : x \in A \text{ and } x \notin B\}$$

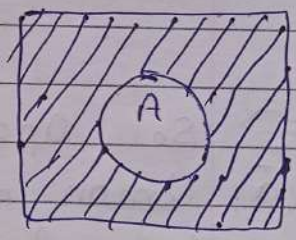


Also $A - B = A - A \cap B$

(e) Complement of a Set
The complement of a set A, denoted by $\bar{A}$ or A^c, is the difference of Universal set U and set A.

$$\bar{A} = A^c = U - A$$

Means $\bar{A} = \{x : x \in U \text{ and } x \notin A\}$



(f) Symmetric Difference of two Sets
It is denoted by $A \ominus B$ and it is the set of all elements that is either present in A or in B not in both sets.

$$A \ominus B = \{x : x \in A, x \in B \text{ and } x \notin A \cap B\}$$

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

$n(\overline{A \cup B}) = m$
Then $n(A \cup B) = n(U) - m$

$n(\bar{A}) = m$
$n(A) = n(U) - m$

Date

⇒ Set Identities

ⓐ Identity Law ⇒ $A \cap U = A$
$A \cup \emptyset = A$

ⓑ Domination Law ⇒ $A \cup U = U$
$A \cap \emptyset = \emptyset$

ⓒ Idempotent Law ⇒ $A \cup A = A$
$A \cap A = A$

ⓓ Commutative Law ⇒ $A \cup B = B \cup A$
$A \cap B = B \cap A$

ⓔ Associative Law ⇒ $A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$

ⓕ Distributive Law ⇒ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

ⓖ Involuntary Law ⇒ $\overline{(\bar{A})}$ or $(A^c)^c = A$

ⓗ De Morgan's Law ⇒ $\overline{A \cup B} = \bar{A} \cap \bar{B}$
$\overline{A \cap B} = \bar{A} \cup \bar{B}$

⇒ Countable and Uncountable sets

A set A is said to be countably infinite if it has the same cardinality as the set of natural numbers, denoted by N and its elements have a one-to-one mapping with these natural numbers.
It is also called "Denumerable Set".

If a set is either finite or Denumerable then it is known as countable.
otherwise it is uncountable.

So, for infinite sets, we will try to create a one-to-one (onto) function b/w given set and N.

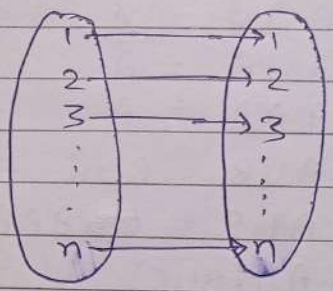
Date

For example -

$N = \{1, 2, 3, \ldots\}$ Set of Natural No.

We can define a function

$N \to N$



One-One
Onto
(Bijective)

Thus, N is countable

Que Prove that set of integers, Z is countable.

⇒ As given,

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

Let's try to define a function from $N \to Z$

$$\text{Let } f(n) = \begin{cases} \frac{n}{2}, & \text{when } n \text{ is even} \\ -\left(\frac{n+1}{2}\right), & \text{when } n \text{ is odd} \end{cases}$$

Then, If $n = 0$, $f(n) = 0$

If $n = 1$, $f(n) = -1$

If $n = 2$, $f(n) = 1$

If $n = 3$, $f(n) = -2$

If $n = 4$, $f(n) = 2$

Clearly, $f(n) : N \to Z$ is a one-one function.

Hence, Set Z is countable.

Date

⇒ Inclusion - Exclusion Principle

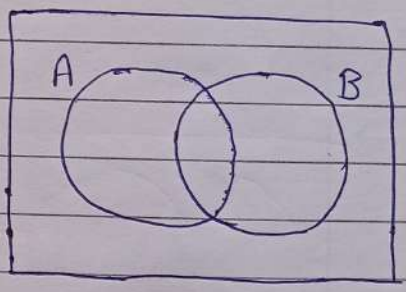
$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

Also

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

Que Among 50 students in a class, 26 got A grade in Exam 1 and 21 got A grade in Exam 2. If 17 students didn't get A in any exam either. How many students got A grade in both exams.

⇒ Let, Set A denotes those students who got A grade in Exam 1
and Set B denotes those students who got A grade in Exam 2



Then $n(A) = 26$

$n(B) = 21$

Total students, $n(U) = 50$

As given

$$n(\overline{A \cup B}) = 17$$

$$\Rightarrow n(A \cup B) = n(U) - 17 = 50 - 17 = 33$$

Now,

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

$$\Rightarrow n(A \cap B) = n(A) + n(B) - n(A \cup B)$$
$$= 26 + 21 - 33$$
$$= 47 - 33$$
$$= 14 \quad \text{Ans}$$

Date

Que In a class of 80 students, 50 students know English and 55 students French, and 46 know German. 37 students know both English and French, 28 know both French and German and 25 know both English and German and 7 know none.

(i) How many of them know all three language?
(ii) How many of them know exactly two "
(iii) " " " " " only one "

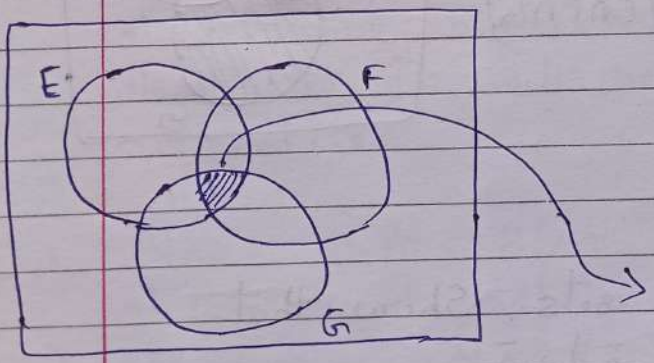
⇒ Let, Set E denotes English
Set F denotes French
and Set G denotes German

Then

$n(E) = 50$ $\quad n(E \cap F) = 37$
$n(F) = 55$ $\quad n(E \cap G) = 25$
$n(G) = 46$ $\quad n(F \cap G) = 28$

Also,
Total students, $n(U) = 80$

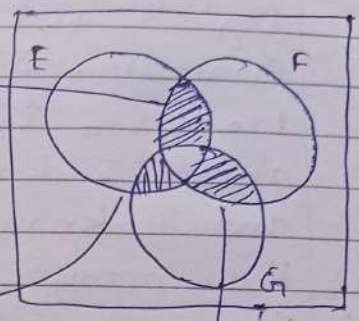
(i) No. of students who know all three languages
, $n(E \cap F \cap G) =$
$n(E \cup F \cup G) - n(E) - n(F) - n(G) + n(E \cap F) + n(F \cap G) + n(E \cap G)$



$= (80 - 7) - 50 - 55 - 46 + 37 + 28 + 25$
$= 73 - 151 + 90$
$= 163 - 151$
$= 12$ Ans (All three)

Date

(ii) For exactly two language, we need Here



$\Rightarrow$ $n(E \cap F) - n(E \cap F \cap G)$

$= 37 - 12$

$= 25$

$\Rightarrow$ $n(E \cap G) - n(E \cap F \cap G)$

$= 25 - 12$

$= 13$

$\Rightarrow$ $n(F \cap G) - n(E \cap F \cap G)$

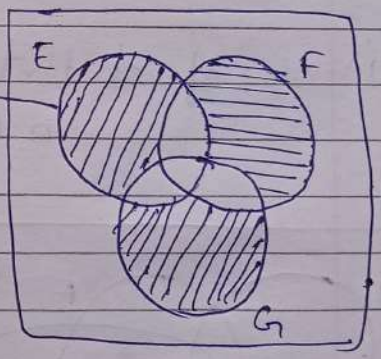
$= 28 - 12$

$= 16$

$\text{Total} = 25 + 13 + 16$

$= 54$ Ans

(iii) for exactly one language, we need Here



$\Rightarrow$ $n(E \cup F \cup G) - 25 - 13 - 16 - n(E \cap F \cap G)$

$\Rightarrow (80 - 7) - 54 - 12$

$\Rightarrow 73 - 66$

$\Rightarrow 7$ Ans

Que Let A, B, and C be sets. Show that

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

$\Rightarrow$ Using De-Morgan's law,

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

Date

Also, $\overline{(B \cap C)} = (\bar{B} \cup \bar{C})$

Thus,

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

$= (\bar{B} \cup \bar{C}) \cap \bar{A}$ (commutative law for intersection)

$= (\bar{C} \cup \bar{B}) \cap \bar{A}$ (commutative law for Unions)

Proved

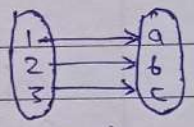
⇒ Power set theorem (Cantor's theorem)

For any set S, there is no surjection from S to P(S) i.e. Power set.

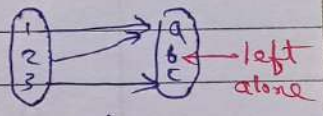
One - One ⇒ Injective

Onto ⇒ Surjective

One - One and Onto ⇒ Bijective



Onto



Into

Means, $f: S \to P(S)$ is not "Surjective"

Power set will contain all possible subsets of S including S itself also. So on mapping atleast one element of P(S) will get left alone. So, it will become "into" i.e. not surjective.

Que Prove that P(N) is Uncountable where N is set of natural numbers.

⇒ We know $N \to N$ is defined as "Surjective"

So, N is countable.

But using Cantor's theorem

$N \to P(S)$ is not Surjective

Thus, P(S) is not countable.

Date

⇒ Cantor's Diagonal Argument

Suppose you are said to prove $[0,1]$ is uncountable.

Then we will use this approach

Let $N \to R$ be a mapping such that

$$R = r_i \qquad (i = 1, 2, 3 \ldots n)$$

Then

Let $1 \to r_1 = 0.a_{11}\, a_{12}\, a_{13} \ldots$

$2 \to r_2 = 0.a_{21}\, a_{22}\, a_{23} \ldots$

$3 \to r_3 = 0.a_{31}\, a_{32}\, a_{33} \ldots$

$n \to r_n = 0.a_{n1}\, a_{n2}\, a_{n3} \ldots a_{nn}$

Clearly, here is a mapping

But there exist $r = 0.b_1 b_2 b_3 \ldots$

such that $b_i \neq a_{ii}$ i.e the diagonal elements.

Here, r is not present in this mapping.

This leads to contradiction

So this interval is "Uncountable".

⇒ Relation

Any subset of $A \times B$ is said to be a relation from set A to set B.

$$n(A \times B) = n(A) \times n(B)$$

If $n(A) = m$, $n(B) = n$

Then No. of Relation $= \boxed{2^{m \times n}}$

Now, ϕ (Null set) is also a subset of $A \times B$. This is known as "void relation".

Date

NOTE ⇒ Total no. of subset of a Set $= 2^n$
But if said, subset contains exactly k elements then
No. of subsets $= {}^nC_k$

Then No. of Relations from A, $n(A) = n$ will be ⇒ $2^{{}^nC_k}$

⇒ Types of Relations
(i) One - One (ii) Many - One (iii) One - Many
(iv) Many - Many

⇒ Relation on a Set A itself $(A \times A)$
$R : A \to A$ Then $n(A \times A) = n^2$
So, $n(R) = 2^{n^2}$

Types :-

(a) Identity Relation
A relation R on set A is said to be identity relation if $R = \{(a,a) \ \forall \text{ (for all) } a \in A\}$
i.e.
Each element of A must have to be related to itself (only).
If $A = \{1,2,3\}$ then only $R = \{(1,1), (2,2), (3,3)\}$ is Identity relation.

$\{(1,1), (2,2)\}$ or $\{(1,1)\}$

Not

Thus,
If $n(A) = n$
Then, No. of Identity relation = 1 i.e. Unique
And It will contain exactly 'n' elements.

Date

(b) Reflexive Relation

A relation R on set A is said to be reflexive if

$\forall$ (for all) $a \in A$, $(a,a) \in R$

i.e. must contain one identity part

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

Then ~~$R_1 = \{(1,1)\}$~~ ~~$R_2 = \{(1,1),(2,2)\}$~~

~~$R_3 = \{(1,1),(2,2),(3,3)\}$~~

~~$R_4 = \{(1,1),(2,2),(3,3),(1,2)\}$~~

~~$R_5 = A \times A$~~

~~$R_6 = \phi$~~

If $n(A) = n$ then,

No. of Reflexive Relations = $\boxed{2^{n^2-n}}$

Proof :-

We know, $A \times A =$

$$\begin{cases} (1,1), (1,2), \dots (1,n) \\ (2,1), (2,2), \dots (2,n) \\ (3,1), (3,2) \dots (3,n) \\ \vdots \\ (n,1), (n,2) \dots (n,n) \end{cases}$$

Identity part

The identity part must has to be present.

Here, $n(A \times A) = n^2$

No. of elements left after excluding diagonal elements $= (n^2 - n)$

Thus,

Total Reflexive relation $= 2^{n^2-n}$

Date

(c) Symmetric Relation

A relation R is said to be symmetric if $(a,b) \in R$ then $(b,a) \in R$ also.

But the condition is if (a,b) is present then only (b,a) must also be present

If (a,b) is not present then no Problem.

If $A = \{1,2,3\}$ then

$R_1 = \{(1,1)\}$ $R_2 = \{(1,1), (2,2)\}$

$R_3 = \{(1,1), (2,2), (3,3)\}$

$R_4 = \{(1,2), (2,2)\}$

$R_5 = \{(1,2), (2,1), (2,2)\}$

$R_6 = \phi$

$R_7 = A \times A$

(d) Anti- Symmetric Relation

A relation R on set A is said to be anti- symmetric if

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

Again if (a,b) and (b,a) are not present then no problem.

But if present then $(a = b)$.

If $A = \{1,2,3\}$ then

$R_1 = \{(1,1)\}$ $R_2 = \{(1,1), (2,2)\}$

$R_3 = \{(1,1), (2,2), (3,3)\}$

$R_4 = \{(1,2), (2,1)\}$

$R_5 = \phi$

$R_6 = A \times A$

Date

(e) Transitive Relation

A relation R on a set A is said to be transitive if $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$

If $A = \{1,2,3\}$ then

$R_1 = \{(1,1)\}$

$R_3 = \{(1,2)\}$

$R_5 = \phi$

$R_6 = A \times A$

$R_2 = \{(1,1), (2,2)\}$

$R_4 = \{(1,2), (2,1)\}$

↳ Because

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

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

But no $(a,c) = (1,1)$

(f) Universal Relation or Full Relation

A relation R on a set A is said to be universal if in that relation every element of set A are related to each other.

It is given by, $R = A \times A$

(g) Equivalence Relation

A relation R is said to be equivalence on set A if it is simultaneously

- (i) Reflexive $(a = a)$
- (ii) Symmetric $(a = b), (b = a)$
- (iii) Transitive $(a = b), (b = c)$ then $(a = c)$

Que Consider the relation

$R = \{(x,y) \mid |x-y| = \text{Even Integer}, x,y \in I\}$

Then prove this relation is equivalence.

Date

⇒ If Relation R is Equivalence then, it must be

(a) Reflexive

Means $(a,a) \in R$

So, If $(a,a) \in R$ then $|a-a| = 0$

This is even Integer

So, it is Reflexive

(b) Symmetric

Means if $(a,b) \in R$ then $(b,a) \in R$

So, If $|a-b|$ = Even Integer

then $|b-a| = |-(a-b)|$

$= |a-b|$ = Even Integer

So, it is Symmetric too

(c) Transitive

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

So, If $|a-b|$ = Even Integer

and $|b-c|$ = Even Integer

Then, clearly a, b, c are same either odd or even

So, $|a-c|$ = Even Integer

because Even - Even = Even

Odd - Odd = Odd

So, it is Transitive too.

Thus, Relation R is "Equivalence".

(f) Partial Order Relation

A relation R on set A is said to be partial order if it is simultaneously

(i) Reflexive (ii) Anti-Symmetric (iii) Transit

Date

⇒ **Pigeon - Hole Principle**

If there are 'm' pigeons and 'n' holes where $m > n$, then atleast one hole contains more than one pigeon

Proof :-

If each hole contains atmost one pigeon then maximum no. of pigeons accomodated will be n.
Thus $(m-n) > 0$ pigeons will not get hole which is contradiction. So, atleast one hole contains more than one pigeon.

Que If there are n pairs of socks then what is the minimum no. socks which are required to be selected randomly to assume that atleast one pair of socks in selected.

⇒ Here, if there are n pairs of socks then we must select atleast $(n+1)$ socks so that one pair of sock is selected.
Because, exactly n socks will be of same type. So, $(n+1)^{th}$ sock will definitely pair with any existing one.

⇒ **Prime Number**

A number P greater 1 is called prime if it is only divisible by 1 or itself. Means it has exactly two divisors.
For example :- 2, 3, 5, 11 etc.

Date

⇒ **Composite Number**

A number which is not Prime is known as composite.

Over the set of integer other then 0 and ±1, If any number is only divisible by ±1 and ±P then it is "Prime".

⇒ **Co-prime**

Two integer p and q are said to be "prime to each other" or "relatively prime" or "co-prime" if they do not have any common prime factor.

Means their GCD = 1 i.e. $\boxed{HCF = 1}$

⇒ **Fundamental theorem of Arithmetic**

According to this,

Every natural number can be uniquely expressed as product of its prime factors

$$N = a^p b^q c^r \ldots$$

Then

$$\text{No. of Divisors} = (p+1)(q+1)(r+1)\ldots$$

$$\text{Sum of Divisors} = \left(\frac{a^{p+1}-1}{a-1}\right)\left(\frac{b^{q+1}-1}{b-1}\right)\left(\frac{c^{r+1}-1}{c-1}\right)\ldots$$

⇒ **GCD**

Let a and b are two integers $(a, b \neq 0)$ then d is called the common divisor of a and b if d divides both a and b.

NOTE: d cannot be greater than $|a|$ or $|b|$.

Express both integers as prime factor then common prime factors will give HCF or GCD.

Date

Euclidean Algorithm :-

This is the "long division method". It is used specially when numbers a, b are sufficiently large so that finding prime factors of large number gets difficult.

For example :- GCD (540 and 168)

$$168)\,540\,(3 \quad \Rightarrow \quad 540 = 168\times 3 + 36$$
$$504$$
$$36)\,168\,(4 \quad \Rightarrow \quad 168 = 36\times 4 + 24$$
$$144$$
$$24)\,36\,(1 \quad \Rightarrow \quad 36 = 24\times 1 + 12$$
$$24$$
$$12)\,24\,(2 \quad \Rightarrow \quad 24 = 12\times 2$$
$$24$$
$$xx$$

Each GCD can be expressed, $d = ax + by$ where x, y are integers

From Here →

$$36 = 24\times 1 + 12$$
$$\Rightarrow 12 = 36 - 24\times 1$$
$$\Rightarrow 12 = (540 - 168\times 3) - (168 - 36\times 4)$$
$$\Rightarrow 12 = 540 - 168\times 3 - 168 + 36\times 4$$
$$\Rightarrow 12 = 540 - 4\times 168 + (540 - 168\times 3)4$$
$$\Rightarrow 12 = 540 - 4\times 168 + 4\times 540 - 12\times 168$$
$$\Rightarrow 12 = 5\times 540 - 16\times 168$$ Ans

Thus, $12 = 540x + 168y$

So, $x = 5$, $y = -16$

Date

Que Find the no. of solution of eq^n $15x+27y=5$

⇒ This is of form, $d = ax + by$
when d is the GCD (a,b)

Now, $a = 15$, $b = 27$

So, Using Euclidean Algorithm

$15)27(1$
$\frac{15}{12})15(1$
$\frac{12}{3})12(4$
$\frac{12}{xx}$

Here, any integer solution exists only if 5 is divisible by 3.
But 5 is not divisible by 3.

So, this eq^n has no integer solution because GCD of 15 and 27 does not divide 5.
Hence, No. of integer solutions $= 0$.

Thus, If GCD $(a,b) = k$
and $ax + by = m$
Then, Equation has a solution if and only if k divides m.

⇒ Congruence modulo

If n is a +ve integer greater than 1 then two integers a and b are said to be congruence modulo n if both of them gives same non-negative remainder when divided by n.

It is written as $a \equiv b \pmod n$

Now, if $a = q_1 n + r$
and $b = q_2 n + r$ such that q_1 and q_2 are quotients and r is Remainder

Then $a - b = (q_1 - q_2)n$

$\Rightarrow \frac{a-b}{n} = q_1 - q_2$ [Means n divides $(a-b)$]

Date

(i) $-7 \equiv 11 \pmod 3$ ✓

(ii) $13 \equiv 5 \pmod 4$ ✓

(iii) $729 \equiv 13 \pmod{11}$ ✗

$729 - 13 = 716$ and 716 is not divisible by 11

Que Prove that $a \equiv b \pmod n$ is Equivalence Relation.

⇒ Any relation is Equivalence if

(i) Reflexive

Means $a \in A$, $(a, a) \in R$

So, $a \equiv a \pmod n$

Clearly, Remainders will be same

So, It is Reflexive.

(ii) Symmetric

Means if $(a, b) \in R$

then $(b, a) \in R$ also

Now,

If $a \equiv b \pmod n$

Then $a = q_1 n + r$

$b = q_2 n + r$

Thus, $b \equiv a \pmod n$ will also satisfy (Same Remainder)

(iii) Transitive

Means if $(a, b) \in R$ and $(b, c) \in R$

then $(a, c) \in R$ also

So,

$a \equiv b \pmod n$ $\quad a = q_1 n + r_1$

$b = q_2 n + r_1$

Date

And $b \equiv c \pmod n$ $\quad b = q_2 n + r_2$, $c = q_3 n + r_3$

Clearly $b = q_2 n + r_2 = q_2 n + r_1$

So, $r_1 = r_2 = r_3$ (Same Remainder)

Thus,

$a \equiv c \pmod n$

So, $a \equiv b \pmod n$ is Equivalence Relation.

⇒ Residue class (or Congruence or Equivalence class)
It is the set of all integers that leave the same remainder when divided by a given positive integer n, known as modulus.

For example :- when divided by 5
Remainders could be ⇒ 0, 1, 2, 3, 4
Thus, Residue class :-
[0], [1], [2], [3] and [4]

$a[0] = 0$
$a[1] = 1$
$\vdots$
$a[n] = n$

So, $a[0] = \{\ldots -10, -5, 0, 5, 10 \ldots\}$
$a[1] = \{\ldots -9, -4, 1, 6, 11 \ldots\}$
$a[2] = \{\ldots -8, -3, 2, 7, 12 \ldots\}$
$a[3] = \{\ldots -7, -2, 3, 8, 13 \ldots\}$
$a[4] = \{\ldots -6, -1, 4, 9, 14 \ldots\}$

⇒ Arithmetic of Residue classes :-

(i) $[a] + [b] = [a+b]$ ⇒ $[2] + [3] = [5] = [0]$
(ii) $[a] \cdot [b] = [a.b]$ ⇒ $[2] \cdot [3] = [6] = [1]$

we will use this to find $[x]$ to $[x^2]$ to 3^e etc.

Date

⇒ Properties

(i) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$

Then $a \pm c = b \pm d \pmod n$

and $ac = bd \pmod n$

Let $a = q_1 n + r_1$ $\quad$ $c = q_3 n + r_2$

$b = q_2 n + r_1$ $\quad$ $d = q_4 n + r_2$

Then

$a \pm c = n(q_1 \pm q_3) + (r_1 \pm r_2)$ → Same Remainder

$b \pm d = n(q_2 + q_4) + (r_1 \pm r_2)$

Clearly, Both remainders are Same

So, $a \pm c = b \pm d \pmod n$

And $ac = (q_1 n + r_1)(q_3 n + r_2)$

$= n^2 q_1 q_3 + q_1 r_2 n + q_3 r_1 n + r_1 r_2$

$= n(n q_1 q_2 + q_1 r_2 + q_3 r_1) + r_1 r_2$ → Same Remainder

$bd = (q_2 n + r_1)(q_4 n + r_2)$

$= n^2 q_2 q_4 + n q_2 r_2 + n q_4 r_1 + r_1 r_2$

$= n(n q_2 q_4 + q_2 r_2 + q_4 r_1) + r_1 r_2$ → Same Remainder

Clearly, Both remainders are Same

So, $ac = bd \pmod n$

(ii) If $a \equiv b \pmod n$ then $a^k \equiv b^k \pmod n$

⇒ Last Digits of a Number

We know,

The last digit of number is the remainder we get when divided by 10.

Date

Similarly, the last two digit, when divided by 100.

the last three digit, when divided by 1000.

Thus, when divided by 10^k, we get last k digits of a number.

Que Find the last two digits of $(24107)^{71235}$.

⇒ Here,

$$24107 = 07 \pmod{100}$$

So, $(24107)^k = (07)^k \pmod{100}$

So, $(24107)^{71235} = (07)^{71235} \pmod{100}$

Now,

$$07 = 07 \pmod{100}$$
$$(07)^2 = 49 \pmod{100}$$
$$(07)^3 = 343 = 43 \pmod{100}$$
$$(07)^4 = 2401 = 01 \pmod{100}$$

Repeat ↓
$$(07)^5 = 16807 = 07 \pmod{100}$$
$$(07)^6 = 117649 = 49 \pmod{100}$$

Clearly value is repeating after power 4.

So, $(07)^{4m+r} = (07)^{71235}$

Now,

$$\frac{71235}{4} = 17808 \times 4 + 3$$

So, 3 is remainder

Now,

$$(07)^3 = 43 \pmod{100}$$

So, Last two digits of $(24107)^{71235}$ is 43.

Date

⇒ **Linear Congruent Equation**

If a and b are congruence modulo n means, $a \equiv b \pmod{n}$

Then the linear congruent equation is given by

$$ax \equiv b \pmod{n}$$

Means

$$\frac{ax-b}{n} = q \text{ (Integer)} \quad (q \text{ is quotient})$$

Let $q = y$.

Then $ax - b = ny$

$\Rightarrow ax - ny = b$

Now, this is of form $ax - by = c$ where $GCD(a,b) = c$

So, This equation has a solution if and only if $GCD(a,n)$ divides b.

For example:-

$3x \equiv 11 \pmod{12}$

Then

$3x - 12y = 11$

Here $GCD(3,12) = 3$

But 3 didn't divides 11

So, No Solution.

Que Find if the equation given below has solution

$3x \equiv 15 \pmod{7}$

⇒ Here, $3x \equiv 15 \pmod{7}$

So, $3x - 7y = 15$

Now, $GCD(3,7) = 1$

And 1 divides 15. So, This equation has a solution.

Date

Que Check if given eq^n has solution or not
$x^2 \equiv 1 \pmod 3$

⇒ As given,
$x^2 \equiv 1 \pmod 3$
Then $x^2 - 3y = 1$

We will use another approach,
for $n = 3$
Residue classes :-

x	$x^2 = x \cdot x$
[0]	[0]
[1]	[1]
[2]	[4] = [1]

we need Remainder equal to 1.
So, $x = [1]$
$[2]$

Que Check if given eq^n has solution or not
$x^2 \equiv 2 \pmod 3$

⇒ Using above table
its clear remainder is never (2).
So, No solution.

Que Check if given eq^n has solution or not
$x^2 + 3x + 1 \equiv 0 \pmod 5$

⇒ Here, $n = 5$
Residue classes :-

x	x^2	$3x$	x^2+3x	x^2+3x+1
[0]	[0]	[0]	[0]	[1]
[1]	[1]	[3]	[4]	[0]
[2]	[4]	[1]	[0]	[1]
[3]	[4]	[4]	[3]	[4]
[4]	[1]	[2]	[3]	[4]

We need Remainder equal to 0.
So, $x = [1]$

Date

Que Given the modulus $m>0$ show that $[a]=[a+m]$ and $[a]=[a-m]$ for all a.

$\Rightarrow$ As given,

Let, p is an integer belonging to Residue class $[a]$

Then

$$p = qm + a$$ (q is quotient, a is remainder)

Now,

$$p+m = qm+a+m$$
$$p+m = (qm+m)+a$$
$$p+m = m(q+1)+a$$

Clearly, remainder is same.

So, $p+m \in [a]$

So, $[a] = [a+m]$

Now,

$$p-m = qm+a-m$$
$$p-m = m(q-1)+a$$

Clearly, Remainder is Same.

So, $(p-m) \in [a]$

Thus, $[a] = [a-m]$

Binary Operation

Date

⇒ **Binary Operation or Binary Composition**

A binary operation is a function on a non-empty set G

$f: G \times G \to G \quad \forall (a,b) \in G$

$f(a,b) = c$ such that $c \in G$

It is denoted by symbol $*$ or $\circ$ which can be any operation add (+), subtract (−) multiply (×) etc.

If $n(G) = n$ then $n(G \times G) = n^2$

Then, No. of Functions from $G \times G \to G$

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

⇒ **Algebric Structure**

An algebric structure is a set G together with one or more binary operations.

It is denoted as

$(G, *)$

For example :-

(i) $(N, +)$ ⟶ Yes

For all $(a,b) \in N$

also $a+b \in N$

(ii) $(N, -)$ ⟶ No

For all $(a,b) \in N$ $(5,6) \in N$

$a-b \notin N$ $5-6 = -1 \notin N$

(iii) $(R, *)$ → Yes

(iv) $(R, \div)$ ⟶ No

For all $(a,b) \in R$ $(5,0) \in N$

$a/b \notin R$ $5/0 = \infty \notin R$

(v) $(Z, -)$ ⟶ Yes

Date

Properties :-

(a) Closure Property
A set G with a binary operation * is said to satisfy the closure property if
$$\forall\ (a,b) \in G$$
$$a * b \in G \quad \text{also.}$$

(b) Associative Property
A non-empty set G with a binary operation * is said to satisfy the associative property iff $\forall\ (a,b,c) \in G$
$$(a*b)*c = a*(b*c)$$

Note :- Addition and multiplication are associative over any number system.

Subtraction is not associative over any number system.
Division is also not associative.

Even if a set follow closure property then it can be said an algebric structure.

⇒ **Semigroup**
An algebric structure is called semigroup if it follow associative property.
This means, a non-empty set G with a binary operation * is said to be semigroup if it follows both
(i) Closure property and
(ii) Associative property

Date

$(Z, -) \longrightarrow$ No $(Z, +) \longrightarrow$ Yes
$(R, +) \longrightarrow$ Yes $(R, -) \longrightarrow$ No
$(Q, +) \longrightarrow$ Yes $(Q, -) \longrightarrow$ No

⇒ Existence of Identity

A non-empty set G with binary operation * consists of an element, $e \in G$ such that

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

Then, e is called the "Identity element". And set G is said to have Identity.

$(N, \times)$ ⇒ Here, $e = 1$ Because $5 \times 1 = 1 \times 5 = 5$ (Yes)
$(N, +)$ ⇒ Here, $e = 0$ But $0 \notin N$ So, (No)
$(R, \times)$ ⇒ Here, $e = 1$ and $1 \in R$ So, (Yes)
$(Q, +)$ ⇒ Here, $e = 0$ and $0 \in Q$ So, (Yes)
$(Q, \times)$ ⇒ Here, $e = 1$ and $1 \in Q$ So, (Yes)

Monoid :-

If identity element exist in a "semigroup" then it is called "monoid".

Means, a set G must follow

(i) Closure Property ⇒ $\forall \ (a, b) \in G, \ a * b \in G$

(ii) Associative " ⇒ $\forall \ (a, b, c) \in G$

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

(iii) Identity " ⇒ $e \in G$ such that

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

For example :-

$(N, \times) \longrightarrow$ Yes

$(N, +) \longrightarrow$ No, because $e = 0$ and $0 \notin N$

So, it is a semigroup but not monoid

$(R, +) \longrightarrow$ Yes

$(R, \times) \longrightarrow$ Yes $(R, -) \longrightarrow$ No, because it is not associative

Date

For a Matrix, $M_{n\times n}$

$(M_{n\times n}, \times)$ = Here, $e = I$ (Identity Matrix)
$(M_{n\times n}, +)$ = Here, $e = 0$ (Null Matrix)

⇒ Existence of Inverse

In a non-empty set G with binary operation * we can say there exist inverse of an element $a \in G$ if there exist an element $b \in G$ such that

$a * b = b * a = e$ where e is the Identity element

So,

For the existence of Inverse, first the identity element must exist.

Means, a non-empty set G must follow :-

(i) Closure Property } → Semigroup
(ii) Associative " }
(iii) Identity " } → Monoid
(iv) Inverse Property ⇒ $(a, b) \in G$ such that $a * b = b * a = e$

For example :-

$(Z, +)$ → (Yes) Here, $e = 0$

Now, $\forall\ a \in Z$ there exist $(\exists)\ (-a) \in Z$ such that $a + (-a) = (-a) + a = 0$

$(R-0, \times)$ → (Yes) there $e = 1$

Now $\forall\ a \in R-0$ $\exists\ \frac{1}{a} \in R-0$ such that $a \times \frac{1}{a} = \frac{1}{a} \times a = 1$

$(N, \times)$ → (No) Because $e = 1$

Now, $\forall\ a \in N$ there must exist $\frac{1}{a} \in N$

But $\frac{1}{a} \notin N$ So, (No)

Date

Group :-

If in a Monoid, there exist inverse of each element the we say that monoid as "Group".

Means $\forall\, a \in G$ there must exist $b \in G$ such that $a * b = b * a = e$ (Identity element)

So, a non-empty set G must follow :-

(i) Closure property } → Semigroup
(ii) Associative property } → Monoid
(iii) Identity property } → Group
(iv) Inverse property

$\forall\, a \in G$ there must exist $b \in G$ such that $a * b = b * a = e$

$(\mathbb{Q}, +) \rightarrow$ Yes
$(\mathbb{R}, +) \rightarrow$ Yes
$(\mathbb{Z}, +) \rightarrow$ Yes
$(\mathbb{Z}, \times) \rightarrow$ No

$(\mathbb{R} - \mathbb{Q}, +) \rightarrow$ No Because, $(2+\sqrt{3}) + (2-\sqrt{3}) \Rightarrow 2$

↳ Only Irrational

But $2 \notin \mathbb{R} - \mathbb{Q}$

Closure Property ✗

$(\mathbb{Q}, \times) \rightarrow$ No Because, $0 \rightarrow \frac{1}{0} \notin \mathbb{Q}$

Abelian Group :-

If in a Group, there holds the commutative property i.e

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

then it is known as abelian group.

⇒ Matrix :—

Date

Matrix ⇒ Inverse of a matrix exist only if it square matrix and its Determinant is Zero.

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

Also, If A and B are two non-singular matrix i.e. determinent not equal to zero, then

$A \times B$, A, B all belongs to G

(a) Let S be a set of all matrix of real numbers of order 2.

Then

$(S, \times)$ ⇒ Closure Property → Yes

$\forall A, B \in S$, $A \times B \in S$

Associative → Yes

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

Identity →

$e = I$ and $I \in S$

So, (Yes)

Inverse ⇒

$A \times B = B \times A = e$ $\quad (B = A^{-1})$

No, Because Determinant of A may be Zero.

So, A^{-1} does not exist

Thus, $(S, \times)$ is not Group.

But, $(S, +)$ will be a Group.

Date

(b) If S is a set of all matrix of real number of order 2 such that their Determinat is not zero

$$S = \{A_i \text{ such that } |A_i| \neq 0\}$$

Then $(S, \times)$ will be a Group

Now, $A \times B \neq B \times A$

So, it is not Abelian Group.

(c) If S is a set of all matrix of integers of order 2 such that their Determinant is not zero

(i) Then $(S, \times)$ will not be a Group

Because

Inverse of $A \in S$ may not belong to S.

If $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$

Then $A^{-1} = \frac{1}{3}\begin{bmatrix} 2 & -1 \\ -1 & 2 \end{bmatrix}$ clearly it is not Integer value

So, $A^{-1} \notin S$

(ii) Then $(S, +)$ will also not be a Group

Because

$A + B \notin S \quad \forall \ (A, B) \in S$

Date

If $A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Then $A+B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ Here, $|A+B| = 0$

Thus $A+B \notin S$

(Closure Property)

Even if S is set of matrix of real no. still (S, +) will not hold Closure property.

⇒ Modulo class :-

Let Z_n be a modulo class

Then $Z_n = \{0, 1, 2, \cdots, (n-1)\}$

Then

$(Z_n, +) \Rightarrow$ (i) Closure

Let (n=3)

$Z_3 = \{0, 1, 2\}$

$0+1 = 1 \in Z_3$

$0+2 = 2 \in Z_3$

$1+2 = 3 = 0 \in Z_3$

So, (Yes)

(ii) Associative

$1+2 = 2+1 = 3 = 0 \in Z_3$

So, (Yes)

(iii) Identity

For addition, $e = 0$

And $e \in Z_3$

Also, $\forall\ a \in Z_3$

$a+e = e+a = a$

So, (Yes)

Date

(iv) Inverse

$\forall\, a \in Z_3 \quad \exists\, b \in Z_3$

such that $a+b = b+a = e$

For example

If $a = 1$

Then $b = 2$ so that $a+b = 1+2$

$= 3$

$= 0$

So, $(a+b) \in Z_3$

So, Yes

Hence, $(Z_n, +)$ is a Group.

⇒ If $(Z, *)$ such that $a * b = a+b+1$ then ($Z \rightarrow$ Integer)

(i) Closure

$a, b \in Z$ then $a+b+1 \in Z$ also

So, Yes

(ii) Associative

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

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

$a+b+c+2 = a+b+c+2$

So, Yes

(iii) Identity

$a*e = e*a = a$

$\Rightarrow e+a+1 = a$

$\Rightarrow e = -1$ and $e \in Z$

So, Yes

(iv) Inverse

$a*b = b*a = e$

$\Rightarrow b+a+1 = -1$

$\Rightarrow b = -a-2$ and $(-a-2) \in Z$

Date

Hence, $(Z, *)$ is a Group.

Now, $a * b = b * a$

$a + b + 1 = b + a + 1$ So, it is also Ambelian Group

Que Check if $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \right.$ such that $a \in R$ and $a \neq 0$ is a Group, for $(S, \times)$.

⇒ The given set of matrix is not a normal matrix.

So, here, Identity, $e \neq I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

also $I \notin S$

(i) Closure Property

Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$

Then $A \times B = \begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix}$ (Row of A × Column of B)

	b,0	0,0
a,0	ab+0	0+0
0,0	0+0	0+0

If $a \neq 0$ and $b \neq 0$

Then $ab \neq 0$ also,

$ab \in R$ also

Thus, Closure property satisfied

(ii) Associative

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

It will also satisfied

(iii) Identity

Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ Then $A \times E = A$

Now let $E = \begin{bmatrix} e & 0 \\ 0 & 0 \end{bmatrix}$ So, $A \times E = \begin{bmatrix} ae & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$

Date

Thus $ae = a$

$e = 1$

So, $E = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ Clearly $E \in S$ and $e \neq 0$

So, Identity Property also satisfied

(iv) Inverse

Let $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} b & 0 \\ 0 & 0 \end{bmatrix}$

If B is inverse of A

Then

$A \times B = E$

$\begin{bmatrix} ab & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ So, $ab = 1$

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

Clearly, $b = \frac{1}{a} \in R$

So, Inverse also exists

$B = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{bmatrix}$ Thus, $(S, \times)$ is a Group

Also,

$A \times B = B \times A$

So, It is an Ambelian Group as well.

Que Check if $S = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \right.$ such that $a \in R$ and $a \neq 0$ is a Group for $(S, \times)$

$\Rightarrow$ We will use same approach as above ↑

Identity, $E = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}$ Inverse, $I = \begin{bmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{bmatrix}$

Date

⇒ **Subgroup of a Group**

Let $(G, *)$ is a group and H is a subset of G (H is non-empty) then H is a sub-group iff. H is itself a Group wrt. same Binary operation.

For example :- $(R, +)$ is a Group and $Z \subseteq R$ and $(Z, +)$ is also a Group

So, $(Z, +)$ is a sub-group of $(R, +)$

Trivial Subgroup :-

For any Group, $(G, *)$

$H_1 = \{e\}$

$H_2 = G$ are two Trivial Subgroups $\forall$ G (always)

Que If $Z_4 = \{0, 1, 2, 3\}$ and $(Z_4, +)$ is the Group check if (Z_4 is modulo class)

$H_1 = \{0\}$

$H_2 = \{0, 1, 2, 3\}$

$H_3 = \{0, 1, 2\}$

$H_4 = \{0, 1\}$

$H_5 = \{0, 2\}$ are its sub-group ?

⇒ H_1 and H_2 are Trivial sub-groups, so no need to check.

For $H_3 = \{0, 1, 2\}$

$1 + 2 = 3$ But under 4 modulo $3 \notin H_3$ Closure Property Failed

So, (No)

For $H_4 = \{0, 1\}$

$0 + 1 = 1 \in H_4$

$1 + 1 = 2 \notin H_4$ Closure Property Failed

Date

For $H_5 = \{0, 2\}$

$0 + 0 = 0 \in H_5$

$0 + 2 = 2 \in H_5$

$2 + 2 = 4$ under 4 modulo

$2 + 2 = 4 = 0 \in H_5$

Closure ✓

Associative → Yes

Identity → $e = 0 \in H_5$ Yes

Inverse →

$2 \rightarrow (-2) \rightarrow$ Under 4 modulo

$-2 = 2 \in H_5$ So, Yes

Thus, $H_5 = \{0, 2\}$ is a sub-group.

⇒ Subgroups of Modulo class

If given $G = (Z_4, +)$, $Z_4 = \{0, 1, 2, 3\}$

Then Multiples of 4 = 1, 2, 4

So, there are three subgroups

For 1 ⇒ $H_1 = \{0, 1, 2, 3\}$ ← Multiples of 1

For 2 ⇒ $H_2 = \{0, 2\}$ ← Multiples of 2

For 4 ⇒ $H_3 = \{0\}$ ← Multiples of 4

Similarly, if $G = (Z_{50}, +)$, $Z_{50} = \{0, 1, 2, \ldots 49\}$

Then, Multiples of 50 = 1, 2, 5, 10, 25, 50

So, there are six subgroups

For 1 ⇒ $H_1 = \{0, 1, 2, 3, \ldots 49\}$

For 2 ⇒ $H_2 = \{0, 2, 4, 6, 8, \ldots 48\}$

For 5 ⇒ $H_3 = \{0, 5, 10, 15, \ldots 45\}$

For 10 ⇒ $H_4 = \{0, 10, 20, 30, \ldots 40\}$

For 25 ⇒ $H_5 = \{0, 25\}$

For 50 ⇒ $H_6 = \{0\}$

Date

Case $\Rightarrow$ $(\mathbb{Q}, \times)$ is not Group
Because inverse of 0 is $\frac{1}{0}$
and $\frac{1}{0} \notin \mathbb{Q}$

But, $(\mathbb{Q}^*, \times)$ is Group where $\mathbb{Q}^* = \{\mathbb{Q} - 0\}$

Also, For $\oplus$, $a^{-1} = -a$
For $\otimes$, $a^{-1} = \frac{1}{a}$

$\Rightarrow$ Theorem :-

1. If G is a group and H is a subset of G then H is a subgroup of G iff.
$ab^{-1} \in H \quad \forall \; a, b \in H$

Proof :-

Case 1 : Let H is a subgroup of G
and $a \in H$, $b \in H$
Then, $b^{-1} \in H$
Then $a * b^{-1} \in H$ also
(closure property)
Thus, $ab^{-1} \in H$

Case 2 : Let $ab^{-1} \in H \quad \forall \; a, b \in H$
Now, we need to show H is a Group.

(i) If $ab^{-1} \in H$ then $a(b^{-1})^{-1} \in H$ also
$\Rightarrow ab \in H$
(closure) ✓

(ii) Just because $a, b \in H$ and $H \subseteq G$
And G is a group
So, It must follow Associative property ✓

Date

(iii) If $a = b$

Then $ab^{-1} = aa^{-1} \in H$

(Inverse Property)

And a^{-1} also Exists

(Identity Property)

2. Intersection of two subgroups of a group is a subgroup also.

Proof:-

Let H, K are subgroups of G

Now,

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

Means $a \in H$ and $a \in K$

$b \in H$ and $b \in K$

Thus, $ab^{-1} \in H$ and $ab^{-1} \in K$

Because H and K are subgroups

Thus, $ab^{-1} \in H \cap K$

Thus, $H \cap K$ is also a subgroup.

3. Union of two subgroups of a group may or may not be a subgroup.

Only if, one subgroup is subset of other then their union will also a subgroup.

Let $G = (Z, +)$

Then $H = 2Z = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots\}$

$K = 3Z = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \ldots\}$

Then,

$H \cap K = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \ldots\}$

Date

⇒ Permutation Group or Symmetric Group
The set of all one-one onto function $f: S \to S$ where $S = \{1, 2, 3, \ldots n\}$ form a group wrt composition is called permutation group.

It is denoted by S_n.

(a) If $S = \{1\}$ then all one-one onto functions are ⇒ $f_1(1) = 1$ (only one)

So, $S_1 = \{f_1\}$

(b) If $S = \{1, 2\}$ then

$f_1(1) = 1$	$f_2(1) = 2$
$f_1(2) = 2$	$f_2(2) = 1$

So, $S_2 = \{f_1, f_2\}$

Here, f_1 and f_2 can be represented as

$f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ (1 gives 1, 2 gives 2)

$f_1 = I$

$f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ (1 gives 2, 2 gives 1)

$f_2 = (1, 2)$

(c) If $S = \{1, 2, 3\}$ then

$f_1(1) = 1$
$f_1(2) = 2$
$f_1(3) = 3$

$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$ (order = 1)

↳ Image

Date

$f_2(1)=2$
$f_2(2)=3$
$f_2(3)=1$
$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$
order = 3

$f_3(1)=3$
$f_3(3)=2$
$f_3(2)=1$
$\Rightarrow \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = (1,3,2)$
order = 3

$f_4(1)=1$
$f_4(2)=3$
$f_4(3)=2$
$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2,3)$
Order = 2

$f_5(1)=3$
$f_5(2)=2$
$f_5(3)=1$
$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1,3)$
order = 2

$f_6(1)=2$
$f_6(2)=1$
$f_6(3)=3$
$\Rightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1,2)$
order = 2

Thus, $S_3 = \{ I, f_1, f_2, f_3, f_4, f_5, f_6 \}$

Rule $\Rightarrow$ If $n(S) = n$
Then $n(S_n) = n!$

Here, S_1 and S_2 are only Abelian Groups, while rest all $S_3, S_4 \ldots$ are only Group.

Date

Que Prove $(S_3, \cdot)$ is not a Abelian Group

⇒ We already know,

$$S_3 = \{ I, (1,2,3), (1,3,2), (1,3), (2,3), (1,2) \}$$

(i) Let $a = (1,2,3)$

$b = (1,3,2)$

Then $a \cdot b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 3 & 2 \end{pmatrix} = I$

$I \in S_3$

If $a = (1,2)$

$b = (1,3,2)$

Then $a \cdot b = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} = (1,3)$

$(1,3) \in S_3$

Thus, $\forall\ a, b \in S_3$

$a \cdot b \in S_3$ also **Closure**

(ii) Let $a = (1,2,3)$

$b = (1,3,2)$

$c = (1,2)$

Now, $a \cdot (b \cdot c) = (1,2,3)\left[(1,3,2) \cdot (1,2)\right] = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

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

$(a \cdot b) \cdot c = \left[\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}\right](1,2)$

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

Thus, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ So, **Associative**

(iii) $\forall\ a \in S_3\ \ \exists\ I \in S_3$

such that $a \cdot I = I \cdot a = a$ So, **Identity**

$a = (1,2)$ then $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1,2)$

Date

(iv) what about Inverse,

Let $a = (1,2,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $1 \to 2 \to 3 \to 1$

Then

there exists $b = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $1 \leftarrow 2 \leftarrow 3 \leftarrow 1$ (Reverse)

Then $a.b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ or $\begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}$

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

Thus, Inverse exists and $I \in S_3$

So, Identity ✓ Inverse ✓

Thus, S_3 is a Group.

(v) Commutative $\Rightarrow$

Let $a = (1,2,3)$ and $b = (1,3,2)$

Then

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

$b.a = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ Same

Let's take another example

$a = (1,2)$ and $b = (1,3)$

Then,

$a.b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = (1,3,2)$

$b.a = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3)$

Clearly $(1,3,2) \neq (1,2,3)$

So, It is not Abelian Group.

Date

⇒ **Ring**

Let R be a non-empty set then $(R, +, \cdot)$ is said to be a Ring wrt the two binary compositions if

(a) $(R, +)$ is a Abelian Group or Commutative Group

(b) $(R, \cdot)$ is a Semi-group

(c) Left and Right distributive law is satisfied

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

(ii) $(a+b) \cdot c = a \cdot c + b \cdot c \quad \forall\ a, b, c \in R$

For example :- $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$

⇒ **Commutative Ring**

If $(R, +, \cdot)$ is a ring and $(R, \cdot)$ satisfies commutative property i.e.

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

then $(R, +, \cdot)$ is a commutative ring.

Que If $M_2(R) = \{ [a_{ij}]_{2\times 2} \ ; \ a_{ij} \in R \}$ then show $(M_2(R), +, \cdot)$ is a Ring or not ?

⇒ As given,

(a) Let's check if $(M_2(R), +)$ is a Abelian Group

(i) $\forall\ a, b \in M_2(R)$

$a + b \in M_2(R)$, Yes (Sum of Real number is also Real)

Closure

(ii) $\forall\ a, b, c \in M_2(R)$

$a + (b+c) = (a+b) + c$, Yes

Associative

Date

(iii) $\forall a \in M_2(R)$ $\exists \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M_2(R)$

such that $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$

Identity ✓

(iv) $\forall a \in M_2(R)$ there exist $-a \in M_2(R)$

If $a = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then $b = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in M_2(R)$

such $a+b = 0$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Inverse

(v) $\forall a, b \in M_2(R)$, $a+b = b+c$ Yes

If $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

Then

$$A+B = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}$$

$$B+A = \begin{bmatrix} a_2+a_1 & b_2+b_1 \\ c_2+c_1 & d_2+d_1 \end{bmatrix}$$

Thus, $A+B = B+A$ **Commutative**

Hence, $(M_2(R), +)$ is a Abelian Group

Date

(b) Now, check if $(M_2(R), \cdot)$ is a Semigroup or not

(i) $\forall\ a, b \in M_2(R)$

$a \cdot b \in M_2(R)$ (Product of two Real Number is Real also)

Yes, Closure

(ii) $\forall\ a, b, c \in M_2(R)$

$a(b \cdot c) = (a \cdot b) \cdot c$ Yes, Associative

So, $(M_2(R), \cdot)$ is a Semigroup

(c) Left and Right Distributive law

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$, $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$, $C = \begin{bmatrix} a_3 & b_3 \\ c_3 & d_3 \end{bmatrix}$

Then, $A \cdot (B+C) = A \cdot \begin{bmatrix} a_2+a_3 & b_2+b_3 \\ c_2+c_3 & d_2+d_3 \end{bmatrix}$

$$= \begin{bmatrix} a_1(a_2+a_3)+b_1(c_2+c_3) & a_1(b_2+b_3)+b_1(d_2+d_3) \\ c_1(a_2+a_3)+d_1(c_2+c_3) & c_1(b_2+b_3)+d_1(d_2+d_3) \end{bmatrix}$$

Now, $AB = \begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & b_1b_2+d_1d_2 \end{bmatrix}$

$AC = \begin{bmatrix} a_1a_3+b_1c_3 & a_1b_3+b_1d_3 \\ c_1a_3+d_1c_3 & b_1b_3+d_1d_3 \end{bmatrix}$

So, $AB+AC = A \cdot (B+C)$

Similarly $(A+B) \cdot C = AC+BC$

Thus, $(M_2(R), +, \cdot)$ is a Ring

Date

But, $(M_2(R), \cdot)$ is not Commutative Ring because

$$AB \neq BA$$

$\Rightarrow$ Ring with Unity

A ring $(R, +, \cdot)$ is called Ring with unity if it satisfied Identity property for $(R, \cdot)$ means,

there exist $e \in R$ such that

$$a \cdot e = e \cdot a = a \quad \forall a \in R$$

Also, R must contain atleast 2 element.

Also, If R is commutative Ring then R is said to be commutative Ring with Unity.

$(R, +, \cdot)$, $(Z, +, \cdot)$, $(Q, +, \cdot)$ all are Ring with unity.

$(Z_n, +, \cdot)$ $\rightarrow$ It is an Abelian Group wrt $(Z_n, +)$
It is a semi-group wrt $(Z_n, \cdot)$

Also, It satisfies Left and Right Dist.

Thus, $(Z_n, +, \cdot)$ is a Ring.

Also,

$\forall a \in Z_n$ there exist $1 \in Z_n$ such that (except Z_1)

$$a \cdot 1 = 1 \cdot a = a$$

↳ Only one element

So, $(Z_n, +, \cdot)$ is a Ring with Unity.

Also,

$(Z_n, +, \cdot)$ is Commutative wrt $(Z_n, \cdot)$

So, $(Z_n, +, \cdot)$ is a Commutative Ring with Unity.

$a^2 \Rightarrow a * a$

Date

⇒ Boolean Ring

A ring $(R, +, \cdot)$ is called Boolean Ring if

$$a^2 = a \quad \forall \; a \in R$$

It is valid only for two value 0 and 1
That's why it is called "Boolean".

For example :-

$(Z_2, +, \cdot)$ is a Boolean Ring

$Z_2 = \{0, 1\}$

$0 \cdot 0 = 0$
$1 \cdot 1 = 1$. and $(Z_n, +, \cdot)$ is a Ring already.

Also
Cartesian Products $\Rightarrow Z_2 \times Z_2 = \{(0,0), (0,1), (1,0), (1,1)\}$

↓

$Z_2 \times Z_2 \times Z_2$ etc.

Cartesian Product of two Ring is also Ring.

Now,

$(0,0) \cdot (0,0) = (0,0)$
$(0,1) \cdot (0,1) = (0,1)$ so on.... !!

Thus,

$Z_2 \times Z_2$ is a Boolean Ring.

⇒ Gaussian Integer

A Gaussian integer is a complex number whose real and imaginary parts are both integers.

$$Z[i] = \{(a + ib) \;/\; a, b \in Z\}$$

Real part $= a$
Img. part $= ib$

Date

For example :- $(3+4i)$, $(-2+i)$, $3i$ etc..

Que Check if $Z[i]$ is a Ring wrt $(+,\cdot)$?

⇒ As given

For $(Z[i], +) = a+bi$, $a,b \in Z$

(i) Sum of two integer is also integer

So, closure ✓

(ii) $(a+b)+c = a+(b+c)$ $\forall$ $a,b,c \in Z$

So, Associative ✓

(iii) $Z[i] = 0+0i$ $(a=b=0)$

such that $Z[i] + (0+0i) = Z[i]$

So, Identity ✓

(iv) $\forall$ $(a+bi) \in Z[i]$ there exists $(-a-bi) \in Z[i]$ such that

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

If $(a,b) \in Z$ then $(-a,-b) \in Z$ also

So, Inverse ✓

(v) $(a+bi)+(c+di) = (c+di)(a+bi)$

$= (a+b)+(c+d)i$

So, Commutative ✓

Date

Thus, $(Z[i], +)$ is an Abelian Group.

For $(Z[i], \cdot)$,

(i) Product of two integer is also Integer
$(a+bi) \in Z[i]$ and $(c+di) \in Z[i]$
Then
$(a+bi)(c+di) \in Z[i]$ closure ✓

(iii) $[(a_1+b_1i)\cdot(a_2+b_2i)]\cdot(a_3+b_3i)$
$= (a_1+b_1i)\cdot[(a_2+b_2i)\cdot(a_3+b_3i)]$

So, Associative ✓

Thus, $(Z[i], \cdot)$ is a semi-group.

Also, Left and Right distributive law
$a\cdot(b+c) = a\cdot b + a\cdot c$
$(a+b)\cdot c = a\cdot c + b\cdot c$ are satisfied

So, $(Z[i], +, \cdot)$ is a Ring.

Now, $a\cdot b = b\cdot a \quad \forall \; a, b \in Z[i]$
So, $(Z[i], +, \cdot)$ is a commutative Ring also.

$\Rightarrow Z_n[i] = \{(a+bi) \mid a, b \in Z_n\}$

Z_n is Modulo class

In $n>1$, then $(Z_n[i], +, \cdot)$ is also Ring.

Date

⇒ Zero Divisor of a Ring

Let $(R, +, \cdot)$ is a commutative ring and a non-zero element $a \in R$ is zero divisor if there exists

$b \in R$ and $b \neq 0$

such that $a \cdot b = 0$

For example :- $(Z_{10}, +, \cdot)$ is a Commutative Ring.

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

If $a = 2$ then there exists $b = 5$ such that $a \cdot b = 2 \times 5 = 10$

Under mod 10 $\Rightarrow$ $10 = 0$

Thus, $a \cdot b = 0$

⇒ Integral Domain

Let $(R, +, \cdot)$ is a commutative ring with unity, then it is called integral domain if $\longrightarrow$

$a \neq 0 \quad \forall \; a \in R$

$b \neq 0 \quad \forall \; b \in R$ such that

$a \cdot b \neq 0$

OR

If $a \cdot b = 0$ then either $a = 0$ or $b = 0$

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

For example :-

$(Z, +, \cdot) \rightarrow$ Yes

$(Q, +, \cdot) \rightarrow$ Yes

$(R, +, \cdot) \rightarrow$ Yes

$(Z_{10}, +, \cdot) \rightarrow$ No $(2 \times 5 = 10 = 0)$

$(Z_3, +, \cdot) \rightarrow$ Yes

$(Z_4, +, \cdot) \rightarrow$ No $(2 \times 2 = 4 = 0)$

Date

Rule ⇒ $(Z_p, +, \cdot)$ is an Integral domain if p is prime

Z_3, Z_5, Z_7 etc.

Also,

$(Z_p[i], +, \cdot)$ is an Integral domain if p is prime and 4 divides $(p-3)$

For example :- $(Z_{13}[i], +, \cdot)$

Here,

13 is prime but $13-3 = 10$

4 doesn't divide 10

So, $(Z_{13}[i], +, \cdot)$ is not integral domain.

$A = (a+bi)$ and $B = (a-bi)$

$A = (2+3i)$ and $B = 2-3i = 2+10i$

Then $A \cdot B = 2^2 - (3i)^2 = 4+9 = 13 = 0$ (Under mod 13)

So, It is not an Integral domain

⇒ **Subring**

Let $(R, +, \cdot)$ is a ring and S is a subset of R $(S \subseteq R)$ then S is called subring of R if

(a) S itself is a Ring wrt $(+, \cdot)$

(b) $\forall\ a, b \in S$, $a \cdot b \in S$ also.

Date

For example :- $(\mathbb{Q}, +, \cdot)$ is a Ring
$(\mathbb{Z}, +, \cdot)$ is also a Ring
and $\mathbb{Z} \subseteq \mathbb{Q}$
$\forall\ a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$
Product of two integer is also Integer.
Thus,
$\mathbb{Z}$ is a sub-ring of $(\mathbb{Q}, +, \cdot)$

⇒ Ideal
Let S be a non-empty subset of $(R, +, \cdot)$ then $(S, +, \cdot)$ is said to be ideal of $(R, +, \cdot)$ if
(a) $\forall\ a, b \in S$, $a - b \in S$
(b) $\forall\ a \in S$ and $r \in R$ then
$a \cdot r$ or $r \cdot a \in S$.

Left ideal ⇒ If $r \cdot a \in S$
Right ideal ⇒ If $a \cdot r \in S$

If $(R, +, \cdot)$ is a Commutative Ring then
Left ideal = Right ideal

For example :-
(a) If $R = \mathbb{Q}$ and $S = \mathbb{Z}$ $(\mathbb{Z} \subseteq \mathbb{Q})$
Then
$\forall\ a, b \in \mathbb{Z}$, $a - b \in \mathbb{Z}$ (Integer − Integer = Integer)
But,
$\forall\ a \in \mathbb{Z}$ and $r \in \mathbb{Q}$
$a \cdot r$ or $r \cdot a \notin \mathbb{Z}$
· Suppose $a = 5$ and $r = \frac{1}{7}$
Then $a \cdot r = \frac{5}{7} \notin \mathbb{Z}$
So, $\mathbb{Z}$ is not an Ideal of $\mathbb{Q}$.

Date

(b) If $R = R$ (Real No.) and $S = Q$ $(Q \subseteq R)$

Then

$\forall\ a, b \in Q$, $a - b \in Q$ (Rational − Rational = Rational)

But

$\forall\ a \in Q$ and $r \in R$

$a \cdot r$ or $r \cdot a \notin Q$

Suppose, $a = \frac{1}{2}$ and $r = \sqrt{3}$

Then $a \cdot r = \frac{\sqrt{3}}{2} \notin Q$.

Q is not Ideal of R

(c) If $R = Z$ and $S = mZ = \{0, \pm m, \pm 2m, \ldots\}$ $(S \subseteq Z)$

Then

$\forall\ a, b \in S$, $a - b \in S$ (Under mod m)

Also,

$\forall\ a \in S$ and $r \in Z$

$a \cdot r$ or $r \cdot a \in S$ (Under mod m)

Thus,

mZ is an Ideal of Z.

Theorem

Proof that Every Ideal is a subring of R but converse is not true.

⟹ Let S is an Ideal of R $(S \subseteq R)$

Then

(a) $\forall\ a, b \in S$, $a - b \in S$

(b) $\forall\ a \in S$, $r \in R$, $a \cdot r$ or $r \cdot a \in S$

Means,

$\forall\ a \in S$ and $b \in S \Rightarrow b \in R$ also $(S \subseteq R)$

So, $a \cdot b$ or $b \cdot a \in S$

Thus,

S is a subring of R.

Date

Case ⟹ If $R = Z$ and $S = Z_m \{0, 1, 2, \ldots m-1\}$

Then

Z_m is not ideal of Z

Because Z_m and Z are two different structures.

For example :—

$2 \in Z$ but In Z_2, $2 = 0$

So, it behaves differently

Hence,

Z_m is neither ideal of Z nor subring of Z.

Theorem If S is an ideal of R and $1 \in S$ then $R = S$.

Proof ⟹ First of all, if two sets are equal $(A = B)$

then $A \subseteq B$ and $B \subseteq A$

Now,

If S is an ideal of R then $S \subseteq R$

Also,

$1 \in S$ Then $\forall\ r \in R$

$1 \cdot r$ or $r \cdot 1 \in S \Rightarrow r \in S$

$\forall\ r \in R$ and $r \in S$ as well implies that $R = S$

Proved

⟹ Field :—

Let $(F, +, \cdot)$ be a commutative ring with unity then it is called a field if each non-zero element of F has its multiplicative inverse.

Date

OR Let $(F, +, \cdot)$ be an Integral Domain then $(F, +, \cdot)$ is called field if each non-zero element has multiplicative inverse.

$(R, +, \cdot) \rightarrow$ Yes
$(Z, +, \cdot) \rightarrow$ No (Inverse is absent)
$(Q, +, \cdot) \rightarrow$ Yes
$(C, +, \cdot) \rightarrow$ Yes

$(Z_p, +, \cdot) \rightarrow$ (a) If p is Prime no $\rightarrow$ Yes
(b) otherwise $\rightarrow$ No

Theorem Every Finite Integral Domain is a Field

For example:-
$Z_3 = \{0, 1, 2\}$ It is an Integral Domain

and $1 \rightarrow 1$ $(1 \times 1 = 1)$
$2 \rightarrow 2$ $(2 \times 2 = 4 = 1)$ under mod 3

So, Yes

$(R, +, \cdot) \rightarrow$ Yes
↳ Finite set

Theorem If $(F, +, \cdot)$ is a field then $(F, +, \cdot)$ has only and exactly two ideals -
$I_1 = \{0\}$ and $I_2 = (F, +, \cdot)$ Itself

Proof ⇒ Case 1 :- $I_1 = \{0\}$ is an ideal of $(F, +, \cdot)$

Case 2 :- Suppose, $I_2 \neq \{0\}$ is also an ideal of $(F, +, \cdot)$

Date

Then,

(i) $\forall\ a, b \in I_2$, $a-b \in I_2$

(ii) $\forall\ a \in I_2 \neq 0$, $a^{-1} \in I_2$ also

Then

$a \cdot a^{-1} \in I_2$

$1 \in I_2$

$(F, +, \cdot)$ is a field and $I_2 \subseteq F$

and,

we already know, if S is an Ideal of R and $1 \in S$ then $(S = R)$

Thus,

$I_2 = F$

Hence, $(F, +, \cdot)$ has exactly two ideals $\{0\}$ and $(F, +, \cdot)$ Itself

Now, Finite Every Integral Domain is a Field, So, Every Integral Domain also has exactly two ideal - $\{0\}$ and itself

⟹ Subfield

Let $(F, +, \cdot)$ be a field and $0 \neq S \subseteq F$ then S is called subfield of F if

(a) $\forall\ a \in S$, $b \in S$, $a-b \in S$

(b) $\forall\ a \in S$, $b \in S$ and $b \neq 0$

$\Rightarrow a b^{-1} \in S$

For example :—

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

$(\mathbb{R}, +, \cdot)$ " " " $(\mathbb{C}, +, \cdot)$

While

$(Z_3, +, \cdot)$ is not subfield of $(Z_7, +, \cdot)$

Z_3 and Z_7 are two different structures.

Date

⇒ Ring Homomorphism

Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be two Rings then, A mapping $f: R \to S$ is called ring homomorphism if:

ⓐ $f(x+y) = f(x) + f(y)$ $\quad \forall\ x, y \in R$

ⓑ $f(xy) = f(x) \cdot f(y)$ $\quad \forall\ x, y \in R$

For example:-

(i) $f: Z \to Z_n$ and $f(x) = x \bmod n$

Then,

ⓐ $f(x+y) = (x+y) \bmod n$
$= x \bmod n + y \bmod n$
$= f(x) + f(y)$

ⓑ $f(xy) = xy \bmod n$
$= (x \bmod n) \cdot (y \bmod n)$
$= f(x) \cdot f(y)$

Thus, $f: Z \to Z_n$ is Ring Homomorphus.

(ii) $f: Z_2 \to Z_2$ and $f(x) = x^2 - x$

Then

ⓐ $f(x+y) = (x+y)^2 - (x+y)$
$= x^2 + y^2 + 2xy - x - y$
$= (x^2 - x) + (y^2 - y^2) + 2xy$ → 0 under mod 2
$= f(x) + f(y)$

ⓑ $f(xy) = (xy)^2 - xy$
$= x^2y^2 - xy \neq f(x) \cdot f(y) = (x^2 - x)(y^2 - y)$
$= x^2y^2 - x^2y - xy^2 + xy$

But

$x, y \in \{0, 1\}$

And for any combination of x and y

$x^2y^2 - xy = x^2y^2 - x^2y - xy^2 + xy$

Date

So, $f(xy) = f(x) \cdot f(y)$

Thus,

$f: Z_2 \to Z_2$ is Ring Homomorphus.

⇒ **Ring Isomorphism**

Let $(R, +, \cdot)$ and $(S, +, \cdot)$ be two rings then a mapping $f: R \to S$ is isomorphus if

ⓐ f is itself Homomorphus

ⓑ f is one-one and onto

⇒ **Kernel of Ring Homomorphism**

Let a mapping $f: R \to S$ is a Ring Homomorphism then Kernel of f is equal to

$$\text{Kernel of } f = \{ x \in R \mid f(x) = 0 \}$$

For example :—

(i) $f: Z_4 \to Z_{10}$ and $f(x) = 5x$ (under mod 10)

Here,

ⓐ $f(x+y) = 5(x+y) = 5x + 5y = f(x) + f(y)$

ⓑ $f(xy) = 5xy$

$= 5x \cdot 5y = f(x) \cdot f(y)$

$= 25xy = 5xy$ (Under mod 10)

Thus,

∴ It is Ring Homomorphism

Now,

$R = Z_4 = \{0, 1, 2, 3\}$

Cleary,

Kernel of $f = \{0, 2\}$

$f(x) = 0 \times 5 = 0$

$= 2 \times 5 = 10 = 0$

Date

(iii) $f: Z_5 \to Z_{10}$ and $f(x) = 5x$

Then

(a) $f(x+y) = (x+y)5 = 5x + 5y = f(x) + f(y)$ Wrong

If $x = 1$ and $y = 4$

Then $x + y = 5 = 0$ (Under mod 5)

Also, $f(0) = 0$

But $f(1+4) = f(1) + f(4) = 5 + 20 = 25$ (Under mod 10) $= 5$

Thus,

$f(0) \neq f(1+4)$ So, it is not Ring Homomorphus

Note ⇒ Always check Ring Homomorphus at $f(x+y)$ where $x+y = n$

$(f: Z_n \to Z_m)$

⇒ Group Homomorphism

Let $(G_1, \cdot)$ and $(G_2, *)$ be two groups then a mapping $f: G_1 \to G_2$ is called group homomorphism if —

(a) $f(x \cdot y) = f(x) * f(y)$

And if it is one-one and onto then it is "Group Isomorphism".

For example:—

$f: Z \to Z$ and $f(x) = x$ $(Z+)$

Then

$f(x+y) = x + y = f(x) + f(y)$

Thus, It is Group Homomorphus.

Propositional Logic

Date

⟹ **Proposition and Compound Proposition**

A proposition (or statement) is a declarative statement which is true or false but not both.

For example :-

(i) $2+2=4$ → True
(ii) $2+2=5$ → False
(iii) Ice floats in water → True
(iv) where are you going → Neither True nor False
(v) $x+1=2$ → Neither True nor False
(vi) $x+y=2$ → " " " "

- We use letters to denote propositional variables (or sentential variables) — p, q, r, s etc.
- If a proposition is "True", it is denoted by T
  If a proposition is "False", it is denoted by F
- Propositions that cannot be expressed in terms of simpler propositions are called "atomic propositions".
- Propositions that are composed of two or more sub-statements and logical connectives and can be expressed in terms of atomic propositions are known as "compound propositions".

For example :-

It is raining (and) it is cold.
P_1 — logic connective — P_2

Date

The area of logic that deals with propositions, is called the "propositional logic or propositional calculus".

⇒ Basic Logical Operators

(a) Conjunction (AND)

Any two propositions can be combined by the word "and" to form a compound proposition called conjunction.

Denoted by (∧)

$P \wedge Q$ = P and Q

Only if both p as well as q are True then $(p \wedge q)$ is also True.

(b) Disjuction (OR) (Inclusive)

Denoted by (∨) $p \vee q$ = P or q

Only if both p as well as q are False then $(p \vee q)$ is also False

(c) Negation (NOT)

Denoted by $(\neg p)$ or $(\bar{p})$ or $(!p)$ or (p') read as "not p"

Let p be a proposition then $\neg p$ is the statement — "It is not the case that p".

Que Find the negation of the proposition "Michael's PC runs Linux"

⇒ Negation :- "It is not the case that Michael's PC runs Linux"

OR "Michael's PC doesn't run Linux".

Date

The connective "or" in a disjunction is used in two ways :-

(i) Inclusive OR $(P \vee q)$

(ii) Exclusive OR (Ex-OR) (XOR) $\Rightarrow P \oplus q$

Exclusive OR :-

Let p and q be two propositions then the exclusive or of p and q $(P \oplus q)$ is true when exactly one of p and q is true, otherwise it is false.

P	q	$P \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Que Let p and q be the propositions that state "A student can have a salad with dinner" and "A student can have a soup with dinner" respectively.
What is $P \oplus q$?

$\Rightarrow$ As given

$P \oplus q$ will be true only if exactly one of them is true means A student can not have both salad and soup.

So, $P \oplus q$ is the statement

"A student can have soup or salad, but not both, with dinner".

Date

⇒ Conditional statements

Let p and q be two propositions then the conditional statement $(p \to q)$ is the proposition "if p then q"

$(p \to q)$ is false when p is true but q is false otherwise true

In the conditional statement,
p is called the "hypothesis or antecedent or premise"
q is called the "conclusion or consequence."

The statement $p \to q$ is called conditional because $p \to q$ asserts that q is true on the condition that p holds.
A conditional statement is also known as "implication".

Truth Table :-

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

(i) if p, then q → p implies q
(ii) if p, q → p only if q
(iii) q if p → q whenever p

⇒ Biconditional statement

Let p and q be two propositions then the biconditional state $p \leftrightarrow q$ is the proposition "p if and only if q".
The biconditional statement $p \leftrightarrow q$ is true when both p and q are same otherwise false.

Date

Truth Table :-

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Common ways to express $p \leftrightarrow q$:-

(i) p is necessary and sufficient for q
(ii) if p then q, and conversely
(iii) p iff q
(iv) p exactly when q

Que Let p be the statement "Maria learns DM" and q be the statement "Maria will find a good job". Express the statement $p \rightarrow q$ as a statement in English.

$\Rightarrow$ Here, $p \rightarrow q$ represents the statement "If Maria learns DM, then she will find a good job".

There are many other ways as well "Maria will find a good job when she learns DM."

We can form some new conditional statements starting with a conditional statement $p \rightarrow q$.

(a) **Converse**

If $p \rightarrow q$ is a conditional statement then $q \rightarrow p$ is known as its converse.

(b) **Contrapositive**

If $p \rightarrow q$ is a conditional statement then $\neg q \rightarrow \neg p$ is known as it contrapositive.