CHAPTER 03

Set Theory and Algebra

3.1 Introduction

Definition: The term set is an undefined primitive of mathematical system under our study. According to George canter. "The set is a collection of definite well defined objects of perception or thought".

Objects: Objects constituting a set are called its elements and we express the fact that a is an element of a set S, symbollically as $a \in S$. (Pronounced as a belongs to S).

Since "object" is very general in scope, an element of a set may be letters, numbers or any symbols, or ordered pairs, or even a set itself.

Sets are denoted by capital letters A, B, C etc. and its elements by small letters a, b, c, ... Sets are either be written by enumerating all its elements (listing method) or by a rule (rule method or set builder method) or by statement method.

(a) There are no particular order in a set, since it is only a collection of elements. i.e. A = {1, 2, 3} and B = {2, 3, 1} are both the same set. We say A = B.

(b) Repetition of element is meaningless in a set, since an element is taken only once i.e. A = {1, 2, 2,3} and B = {1, 2, 3} are both the same sets.

3.2 Sets

Finite and Infinite Sets

Sets which have a finite number of elements are called **finite sets** and those having infinite number of elements are called **infinite sets.** If S is a set, then n(S) or $|S|$ denotes the number of elements in S. n(S) is also called as cardinal number of S or cardinality of S.

Examples of finite set:

(*i*) Set of days in a week

(*ii*) Set of dates in a month

(*iii*) Set of chairs in a classroom

Examples of infinite set:

(*i*) Set of natural number

(*ii*) Set of points on a plane

(*iii*) Set of lines passing through one point

Equivalent Sets

Two finite sets are equivalent if their cardinal numbers are same. Notice that two equivalent sets need not be equal.

Example: Let $A = \{1, 2, 3\}$

$B = \{x, y, z\}$

then, A and B are equivalent sets.

Equal Sets

Two sets are equal if they have exactly same elements

Example: If $A = \{1, 2, 3\}$ $B = \{2, 3, 1\}$ then $A = B$.

Empty or Null Sets

A set which does not possesses any element is called empty or null or void set and is denoted by ϕ or { }.

Example: If $A = \{x : x \in N \text{ and } 2 < x < 3\}$ then $A = \phi$.

3.2.1 Subset

A set 'A' is **subset** of B if each element of A is also an element of B. A is called **proper subset** of B if B has at least one element more than that of A and all elements of A are contained in B.

For subset we use $\subseteq$ and for **proper subset** we use $\subset$.

Subset Properties:

1. If a set A has n elements, then total number of subsets of A is 2^n.
   Example: If a set A is $\{1, 2\}$, then subsets of A are { }, $\{1\}$, $\{2\}$ and $\{1, 2\}$
   Here total number of subsets are 2^2 i.e., 4.
2. If $X \in A \Rightarrow X \in B$ (where x is any arbitrary element)
   Then we can say that $A \subseteq B$
   This is the strategy that is used to check or to prove that $A \subseteq B$.
3. $A \subseteq B$ and $B \subseteq A$ then $A = B$
   i.e. $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$
   This is the strategy that is used to prove that some two arbitrary sets are equal.
4. **Power Set:** Let A be a set, then power set of A is P(A) given by $P(A) = \{S : S \subseteq A\}$.
   If A is the set of n elements, then the number of elements in P(A) is 2^n.
   $\Rightarrow n[P(A)] = 2^n$.
   Example: If $S = \{a, b, c\}$, then
   $P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$
   Here S has 3 elements, so P(S) has $2^3 = 8$ elements.
5. If A is the subsect of B, then B is the superset of A Superset is denoted by the symbol "$\supseteq$".
   i.e. $A \subseteq B \Rightarrow B \supseteq A$
6. Every set is a subset of itself and null set is a subset of every set.
   i.e. $A \subseteq A$ (for all A)
   and $\phi \subseteq A$ (for all A)

3.2.2 Universal Set

Universal set U is the superset of all the sets under consideration.

It is a set which contains all the sets in the domain of discussion. For example if we are discussing numbers such as integers, rational nos etc, the real no set is a convenient universal set since it contains all the numbers discussed.

3.2.3 Complement of a Set

Let U be an universal set and A be any element of it, then A^C or A' is the complement of A given by $A^C = \{x : x \notin A \text{ and } x \in U\}$

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

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

Properties of Complements:

1. $(A^C)^C = A$ or $(A')' = A$
   (law of double complementation)
2. $A \cup A^C = U$ or $A \cap A^C = \phi$
   (That is to say that A and A^C together contain everything and A and A^C have nothing in common between themselves).
   ∴ We can write $A^C = U - A$ (where "–" represent difference of two sets as will be discussed later).

3.2.4 Union of Sets

Let A and B be two sets. A set consisting of the elements of both A and B is called union of set A and B and is denoted by $A \cup B$.

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

i.e. $A \cup B$ contains elements belonging to A or B or both A and B. The "or" is being used in inclusive sense. (includes elements belonging to both A & B also).

So, "$\cup$" is the inclusive or.

Example:

Let $A = \{a, b, c, d\}$, $B = \{a, e, f\}$,

$A \cup B = \{a, b, c, d, e, f\}$

3.2.5 Intersection of Sets

Let A and B be two sets, then the set which consists the common elements of A and B is called intersection of A and B and it is denoted by $A \cap B$.

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

Example: It $A = \{a, b, c, d\}$, $B = \{a, e, f\}$, then $A \cap B = \{a\}$. Properties of "$\cup$" & "$\cap$".

1. $A \subseteq A \cup B$ and $B \subseteq A \cup B$
2. $A \cap B \subseteq A$ and $A \cap B\cup \subseteq B$

3.2.6 Disjoint Sets

Two sets A and B are said to be disjoint sets, if there is no common element in A and B. If A and B are disjoint sets, then $A \cap B = \phi$.

Example: Let $A = \{a, b, c\}$, $B = \{x, y, z\}$ then A and B are disjoint sets, because $A \cap B = \phi$.

3.2.7 Difference of Sets

Let A and B be two sets. Then the set of all those elements of A which are not in B is called difference set of A and B and denoted by $A - B = \{x : x \in A, x \notin B\}$

Also $B - A = \{x : x \in B, x \notin A\}$

Example: If $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 5\}$ then $A - B = \{1, 4\}$ and $B - A = \{5\}$.

$A - B$ includes all elements which belong to A only & (not B) and $B - A$ includes all elements which belong to B only (& not A) $A - B$ is also called as relative complement of B in A.

Properties of Set Difference:

1. In general $A - B \neq B - A$
2. $A^C = \cup - A$
3. $A - B = A - (A \cap B)$
   [i.e. $A - B$ can be obtained by removing from A, the elements common to both A & B]
4. $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ = (A only) or (B only) or (both A & B)

3.2.8 Symmetric Difference of Sets

Let A and B be two sets. Then the set of all those elements which are in A but not in B or in B but not in A is called symmetric difference of A & B, denoted by $A \oplus B$.

i.e. $A \oplus B$ contains all elements belonging to either A only or B only but not both.

This is also called as the "XOR" operation. (Exclusive - or).

Example:

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

Then $A \oplus B = \{1, 2, 5, 6\}$

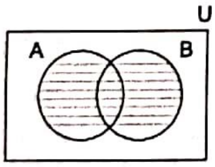
Properties of Symmetric Difference:

1. $A \oplus B = B \oplus A$ (Commutative)
2. $A \oplus B = (A - B) \cup (B - A)$ = A only or B only
3. $A \oplus B = (A \cup B) - (B \cap A)$
4. $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ (Associative)

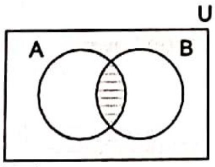
3.2.9 Venn Diagrams

Most of relationship between the sets can be represented by diagrams known as venn diagrams. A universal set U is represented by points in the interior of a rectangle and any of its non empty subsets by points in interior of closed curves (usually circles).

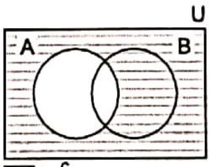
The venn diagrams for common set operations is shown below.



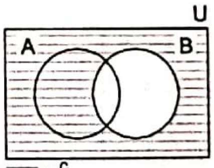
▤ $A \cup B$



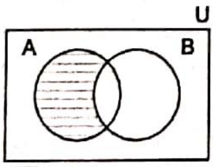
▤ $A \cap B$



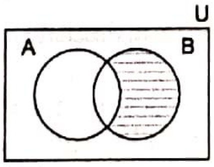
▤ A^c



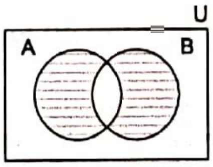
▤ B^c



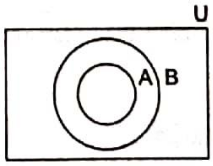
▤ A – B (A only)



▤ B – A (B only)



▤ $A \oplus B$

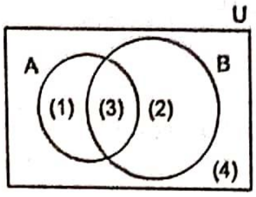


NOTE: Venn diagrams can be effectively used for proving equality of set expressions or for answering question regarding counting of elements of sets.

3.2.10 Fundamental Products

Fundamental products are the disjoint partitions (regions) of a venn diagram with two or more sets.

For example consider a venn diagram with two arbitrtory sets A and B. The four fundamental products are shown below as (1), (2), (3) and (4).

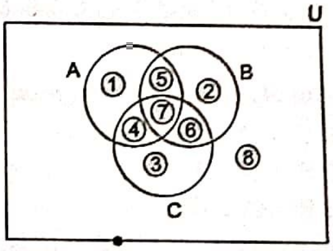


The number of fundamental products is always = 2^n, where n is the number of sets under consideration.

1. $A \cap B^C$	[A only] [A and not B]
2. $A^C \cap B$	[B only] [B and not A]
3. $A \cap B$	[A & B]
4. $A^C \cap B^C$	[neither A nor B]

Similarly for a 3 set venn diagram, there are $2^3 = 8$ fundamental products as shown below:

1. $A \cap B^C \cap C^C$	[A only]
2. $A^C \cap B \cap C^C$	[B only]
3. $A^C \cap B^C \cap C$	[C only]
4. $A \cap B^C \cap C$	[A & C but not B]
5. $A \cap B \cap C^C$	[A & B but not C]
6. $A^C \cap B \cap C$	[B & C but not A]
7. $A \cap B \cap C$	[all three]
8. $A^C \cap B^C \cap C^C$	[none of them]



Fundamental products are useful in counting since they are disjoint in nature and therefore provides no chance for double-counting.

3.2.11 Law of Set Theory

1. $\left.\begin{array}{l} A \cup \phi = A \\ A \cap U = A \end{array}\right\}$ Identity Laws

2. $\left.\begin{array}{l} A \cup \phi = \phi \\ A \cup U = U \end{array}\right\}$ Domination Laws

3. $\left.\begin{array}{l} A \cup A = A \\ A \cap A = A \end{array}\right\}$ Idempotent property

4. $\left.\begin{array}{l} A \cup B = B \cup A \\ A \cap B = B \cap A \end{array}\right\}$ Commutative Property

5. $\left.\begin{array}{l} A \cup (B \cup C) = (A \cup B) \cup C \\ A \cap (B \cap C) = (A \cap B) \cap C \end{array}\right\}$ Associative property

6. $\left.\begin{array}{l} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{array}\right\}$ Distributive property

7. $\left.\begin{array}{l} A \cup A^C = U \\ A \cap A^C = \phi \end{array}\right\}$ Complement laws

8. $(A^C)^C = A$ Law of double complement

9. $\left.\begin{array}{l} (A \cup B)^C = A^C \cap B^C \\ (A \cap B)^C = A^C \cup B^C \end{array}\right\}$ Demorgan's Laws

Set Theory: More results

1. $A - B = A \cap B^C = A\ (A \cap B)$
2. $A - B = B^C - A^C$
3. $A \subseteq B \Leftrightarrow B^C \subseteq A^C$
4. $A \subset B$ and $C \subset D \Rightarrow A \times C \subset B \times D$
5. $n(A \cup B) = n(A) + n(B) - n(A \cap B)$
6. $n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$
7. $n(A^C) = n(U) - n(A)$
8. $n(A - B) = n(A \cap B^C) = n(A) - n(A \cap B)$ 10, 11, 12 and 13 are used in counting problem involving sets.

3.2.12 Cartesian Product of Sets

Let A and B be two sets, then $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$ A × B is called Cartesian product of sets. The elements of A × B are of the form (a, b) called ordered pairs.

If A has m elements and B has n elements then A × B has *mn* elements.

Example: Let $A = \{a, b\}$, $B = \{c, d, e\}$, then $A \times B = \{(a, c), (a, d), (a, e), (b, c), (b, d), (b, e)\}$

$B \times A = \{(c, a), (c, b), (d, a), (d, b), (e, a), (e, b)\}$

Here, A × B has 2 × 3 = 6 elements

B × A also has 3 × 2 = 6 elements

Properties of Cartesian Product:

1. $A \times B \neq B \times A$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
4. $A \times (B - C) = (A \times B) - (A \times C)$
5. $(A \times B) \cap (C \times D) = (A \cap C) \times (C \cap D)$
6. $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$

3.3 Relations

Definition:

Let A and B be two non empty sets, then a relation R from A to B is a subset of A × B.

1. Let $R \subseteq A \times B$. If $(x, y) \in R$ then we say "x is related to y", denote it by $x\,Ry$. In this notes, whenever you see $x\,Ry$, read it as x related to y (by relation R).
2. Let $R \subseteq A \times B$, given by $R = \{(x, y) : x \in A, y \in B\}$, then Domain (R) = $\{x : (x, y) \in R\}$, and Range (R) $= \{y : (x, y) \in R\}$
3. A relation R on set A is a subset of A × A and is called a binary relation on A.

   Example: Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$

   Then a relation R defined on A × B is any subset of A × B. For instance,

   $R = \{(1, a), (2, c), (2, b)\}$

   Now since $(1, a) \in R$, we say 1Ra (1 is related to a by R)

   Domain (R) = $\{1, 2\}$

[The set of all first elements of the ordered pairs of R]

Range (R) = {a, b, c}

[The set of all second elements of the ordered pairs of R]

Note: Since ϕ is also a subset of A × B it is also a relation.

R= ϕ ={ } is called the null relation or void relation.

It is the smallest possible relation on A and B.

Since $A \times B \subseteq A \times B$. A × B itself is a relation. It is the biggest possible relation on A and B, since it contains all possible ordered pair combinations from element of A and B. Similarly, the largest relation from a set A to itself is A × A, which is the universal relation in A.

3.3.1 R-relative Sets

For any element $x \in$ R, we can define a set called R-relative set of x as $R(x) = \{y | xRy\}$ i.e. R relative set of x is all the elements which are related to the element x by relation R.

Example: R = {(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 3)}

R (1) = {1, 2, 3}

R (2) = { 1, 2} and R (3) = {3}

Now for some $B \subseteq A$, we can define also R(B) = $\{y | xRy, \forall x \in B\}$. In example above, If B = {1, 3}, then R(B) = all elements related to 1 or 3 = {1, 2, 3}.

3.3.2 Representation of Relations

Since relations are also sets (of ordered pairs), They can be represented by listing, set builder or statement methods, used for representing sets.

However, relations can be represented by other methods such as matrix method, arrow diagram method, graphical method or digraph method.

Consider a relation R on

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

Set Builder: R = $\{(x, y) | x < y\}$ is a relation expressed in set builder method.

Listing: R = {(1, 2),(1, 3),(1, 4) (2, 3), (2, 4) (3, 4)} is the same relation expressed in listing method.

Matrix: $M_R = \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 1 & 1 & 1 \\ 2 & 0 & 0 & 1 & 1 \\ 3 & 0 & 0 & 0 & 1 \end{array}$ is a matrix representation of the same relation.

If $(x, y) \in$ R, then there will be a 1 in the position corresponding to row representing element x and column representing element y. All other entries in M_R are made zero.

Notice, that the row and column labels are shown for reference only and can be omitted as follows, if order of elements listed in A and B is fixed.

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

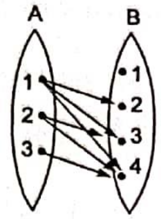
The elements of M_R may therefore be defined as to follows:

q_{ij} = 1 {if there is a relation between element i of A and Element j of B}

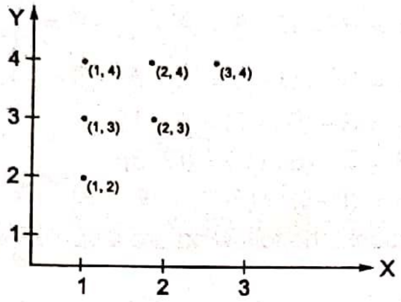
= 0 otherwise

Arrow Diagram

The arrow diagram representation of same relation would be



The graphical representation of R would be as follows:



Digraph

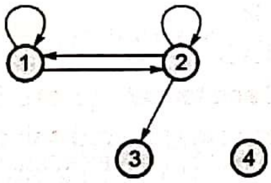
A Digraph (Directed graph) representation is suitable only if the relation is between a set A and itself, i.e. on A × A.

Example: A = {1, 2, 3, 4,}

Consider a relation on A × A given as follows.

R = {(1,1), (2,2), (1,2), (2,1) (2,3)}

The Digraph for the above relation is shown below.



The lines representing (1, 1) and (2, 2) are called self loops.

NOTE: The representation of a relation in set builder form is complete only when the sets A and B are clearly specified.

For Example R = $\{(x, y) / x \le y\}$ has a different meaning if specified on Z × Z, than when specified on R × R. (Note: the default set for numbers is the set of real nos).

So, if you wish to allow only integer values of x and y the correct representation will be, let R = $\{(x, y) / x \le y\}$ on Z × Z.

Identity Relation

Let A be a non empty set. Then the relation $\{(x, y) : x, y \in$ A and $x = y\}$ is called identity relation.

Example: Let A = {a, b, c, d} then the identity relation I_A = {(a, a), (b, b), (c, c), (d, d)}

Identity relation is also known as diagonal relation, since in matrix representation of I_A, the diagonal elements are all 1 (Identity matrix).

3.3.3 Operations on Relations

Since relations are sets, all set operations can be performed on relations also. i.e. if R and S are two relations, than the following are defined.

$R \cup S$, $R \cap S$, R^C, S^C, $R - S$, $R \cup \oplus S$

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

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

on $A \times A$ where $A = \{1, 2, 3\}$

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

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

$\bar{R} = R^C = U - R = (A \times A) - R = \{1, 3) (2, 1), (2, 2\}, (3, 1) (3, 2) (3, 3)\}$

$\bar{S} = S^C = U - S = (A \times A) - S = \{(1, 1), (1, 3), (2, 1), (2, 2), (3, 1), (3, 2)\}$

$R - S = R - (R \cap S) = \{(1, 1)\}$

$S - R = S - (S \cap R) = \{(3, 3)\}$

$R \oplus S = (R–S) \cup (S–R) = (R \cup S) - (R \cap S) = \{(1, 1), (3, 3)\}$

In addition to the above operations, the following are also defined on R and S. i.e. R^{-1}, S^{-1}, RoS, SoR.

Definition:

$R^{-1} = \{(y, x) / (x, y) \in R\}$

In this example: $R^{-1} = \{(1, 1), (2, 1), (3, 2)\}$

Note that if R relates x to y, then R^{-1} relates y back to x.

$S^{-1} = \{(2, 1), (3, 2), (3, 3)\}$

Using matrics M_{R-1} can be obtaines by taking transpose of M_R i.e. $M_{R-1} = (M_R)^T$

Composition of Relations

$RoS = \{(x, y)/(x, z) \in S \text{ and } (z, y) \in R\}$

RoS is called **composition** of S with R.

Similarly, SoR is composition of R with S.

To find elements of RoS., start with S and for each $(x, z) \in S$ identify elements of the type $(z, y) \in R$ and write $(x, z) \in RoS$. This must be done for each of the ordered pair of S.

Example: In above relation, with $R = \{(1, 1), (1, 2), (2, 3)\}$ and $S = \{(1, 2), (2, 3), (3, 3)\}$

NOTE: Here, $(1, 2) \in S$ and $(2, 3) \in R \Rightarrow (1, 3) \in RoS$

There is no composition for ordered pairs (2, 3) and (3, 3) of S, since no element in R starts with 3. We write

$RoS = \{(1, 3)\}$

$(1, 1) \in R$ & $(1, 2) \in S$. $\therefore (1, 2) \in SoR$

$(1, 2) \in R$ & $(2, 3) \in S$. $\therefore (1, 3) \in SoR$

$(2, 3) \in R$ & $(3, 3) \in S$. $\therefore (2, 3) \in SoR$

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

Note: $RoS \neq SoR$ (Composition is not commutative)

But, $Ro\,(SoT) = (RoS)\,oT$ (Composition is Associative)

Using matrices for R & S, RoS can also be obtained as follows:

$M_{RoS} = M_S \odot M_R$ where $\odot$ is boolean multiplication of matrices.

3.3.4 Types of Relations

1. Reflexive Relation

A relation R on A is called reflexive, if $\forall\, x \in A\ (x, x) \in R$

i.e. $\forall x \in A,\ x\,Rx$

Example: Let S be a set of all straight line. The relation R in S defined by "x is parallel to y", is reflexive because every straight line is parallel to itself.

(a) The matrix of a reflexive relation will contain 1's in all the diagonal position.

Example:

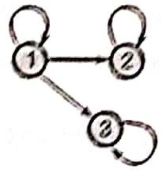
Let, R = {(1, 1), (2, 2), (3, 3), (1, 2), (1, 3)} be defined in A × A where A = {1, 2, 3}

Now,
$$M_R = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Notice that diagonal elements are all 1s.

∴ This is a reflexive relation.

(b) The digraph of a reflexive relation will have self loops on every node. For example for above relation R, the digraph is



(c) R is reflexive iff R^{-1} is reflexive.

(d) Note that when checking for reflexive property, check that every element is related to itself.

(e) To check a set builder relation for reflexivity let $x\ Rx$ for an arbitrary x and see if it is true. Then it is reflexive,

Example: R = {(x, y) | x divides y} Let $x\ Rx \Rightarrow x$ divides x which is true $\forall x$.

∴ R is reflexive.

2. Symmetric Relation:

A relation R in A is called symmetric relation iff $(x, y) \in R \Rightarrow (y, x) \in R$

i.e., $x\ Ry \Rightarrow y\ Rx\ \forall x,\ y \in A$

(a) The matrix of a symmetric relation will be such as that $M_R = M_R^T$ i.e. the matrix will be symmetric matrix.

Since M_R^T represents the inverse relation R^{-1}, ∴ a necessary & sufficient condition for a relation to be symmetric is $R = R^{-1}$

Example: R{(1, 1), (1, 2), (2, 1), (3, 2), (2, 3)} is a symmetric relation

Here,
$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Notice that M_R is a symmetric matrix.

Also, $R^{-1} = R$ & $(M_R)^T = M_R$

(b) The digraph of a symmetric relation will be such that all arrows (which are not self loops) will be bidirectional i.e.

If an arrow goes from (a) to (b), there will be an arrow from (b) to (a). Of course, since self loops are always bidirectional and can be excluded while checking a digraph for symmetric property.

(c) The check a set builder relation for symmetry: Let xRy be true & see if this $\Rightarrow yRx$. If this is so, then R is symmetric.

Example: R $\{(x, y) / x + y = 10\}$

Now, Let xRy be true $\Rightarrow x + y = 10$

$\Rightarrow y + x = 10 \Rightarrow yRx$

$\therefore$ R is symmetric.

(d) Since an implication is true whenever LHS is false, then if xRy itself false, then by default R is symmetric.

$\therefore$ The empty relation is always symmetric.

3. **Anti Symmetric Relation:**

A relation R on A is called **anti symmetric** iff $xRy \Rightarrow y \not{R} x$, unless $x = y$

However the following definition is easier to use in practice. A relation R is antisymmetric iff $(x, y) \in R$ and $(y, x) \in R \Rightarrow x = y$

i.e., xRy and $yRx \Rightarrow x = y \; \forall x, y \in A$.

(a) Antisymmetric property basically means that all relations are one way, (Except for self loops, which are always two-ways).

(b) The matrix of an antisymmetric relation will have a "0" in the mirror image position (using diagonal as mirror) for every "1" in the off diagonal.

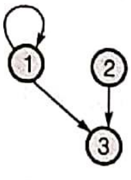
To check for antisymmetry, check the 1s in off diagonal and see if a "0" is there in corresponding mirror image position. Ignore diagonal 1s in this check.

(c) To check a digraph for antisymmetry, ignore self loops and check that for every arrow going form a to b (a, b distinct), there is no arrow from b to a, i.e. All arrows (Except self loops) are unidirectional.

Example: R = {(1, 1), (2, 3), (1, 3)}is antisymmetric

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

The digraph is unidirectional except for self-loops.



(d) To check a set builder relation for antisymmetry, Let xRy and yRx and solve. If the only solution is $x = y$, then R is antisymmetric.

Example: R = $\{(x, y) / x$ divides $y\}$ $x, y \in$ N

Now Let xRy and $yRx \Rightarrow x$ divides y and y divides $x \Rightarrow x = y$.

$\therefore$ R is antisymmetric.

(e) If xRy and yRx cannot be satisfied by any elements i.e. LHS is false, by default the implication becomes true, i.e. R is antisymmetric.

Example: R = {(x, y) / x is father of y}

Now Let xRy and yRx

$\Rightarrow x$ is father of y and y is father of x.

Now, this is not at all possible. Always false.

$\therefore$ by default the implication is true and the relation is antisymmetric.

4. **Transitive Relation:**

A relation R on A is called transitive iff $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$

i.e., xRy and $yRz \Rightarrow xRz \quad \forall x, y, z \in A$

Example: A relation "greater than" defined on the set of natural numbers N is transitive because $x, y, z \in N$ if $x > y$, $y > z$ then $x > z$.

(a) Transition property is difficult to check with a matrix.

(b) Transitive property can be checked on a digraph by scanning each node systematically all possible (x, y), (y, z) arrow and seeing if (x, z) arrow also exists. Self loops can be ignored in this analysis since they always are transitive.

This procedure although tedious, can be used for checking a small digraph for transitivity.

(c) To check a set builder relation for transitivity, Let xRy and yRz and solve these two equations. If there is no solution, or if the solution results in xRz, then relation is transitive.

Example: R = {(x, y) / $x + y$ is even}

Now Let xRy and yRz

$\Rightarrow \quad x + y = 2k_1, \quad \ldots (1)$

and $\quad y + z = 2k_2 \quad \ldots (2)$

Adding (1) and (2) we get

$$x + 2y + z = 2(k_1 + k_2)$$

$$\Rightarrow \quad x + z = 2(k_1 + k_2 - y)$$

$\therefore \Rightarrow x + z$ is also even $\Rightarrow xRz$

$\therefore$ R is transitive

(d) Notice that if xRy and yRz is always false (i.e. no solution to xRy and yRz), then by default R is transitive.

5. **Irreflexive Relation:**

A relation R on A is called **irreflexive** iff $\forall x \in A$, $(x, x) \notin R$.

i.e. $\forall x \in A$, $x \not R x$

Example: Let S be the set of all straight lines, the relation R on S defined by "x is perpendicular to y", is irreflexive, since no line is perpendicular to itself.

(a) Irreflexive property means strictly no self loops in digraphs. Strictly no 1s in the diagonal of the matrix representation. (i.e. all 0's in diagonal of M_R).

(b) In the builder form this can be checked by putting xRx and seeing if this is always false.

Example: R = {(x, y) / x is one inch from y} defined on set of pts in a plane.

Let $xRx \Rightarrow$ pt x is one inch from itself. Which is always false. Hence R is irreflexive.

(c) An irreflexive relation is surely not reflexive, but a not reflexive relation may or may not be irreflexive.

i.e. irreflexive $\Rightarrow$ not reflexive

not reflexive $\not\Rightarrow$ irreflexive

Example: R = {(1, 1), (2, 3), (3, 1)} on

A = {1, 2, 3} is neither reflexive, nor irreflexive.

6. **Asymmetric Relation:**

A relation R on A is an **asymmetric** relation iff $(x, y) \in R \Rightarrow (y, x) \notin R$ $xRy \Rightarrow y \not{R} x$.

This is similar to antisymmetric property in that all relations are unidirectional, except that in antisymmetric the self loops are allowed, but here in asymmetry even self loops are not allowed (i.e. strictly unidirectional).

Example: $R = \{(x, y) | x$ is father of $y\}$

Let $xRy \Rightarrow x$ is father of $y \Rightarrow y$ is not father of x

i.e. $xRy \Rightarrow y \not{R} x$. $\therefore$ R is asymmetric.

Notice that there are no self loops here, i.e. x cannot be father of x.

(a) The matrix of an asymmetric relation must have 0'S in all diagonal positions (no self loops). Also wherever a "1" is in off diagonal, a "0" must be there in corresponding mirror image position.

(b) The digraph of a relation can be easily checked for asymmetry, as follows.
Check that there are no self-loops. Also check that every arrow is unidirectional.

(c) To check a relation in set builder for asymmetry,

Let xRy. This must imply that $y \not{R} x$.

(d) If xRy is always false, then by default the relation is asymmetric i.e.ϕ is an asymmetric relation.

7. **Equivalence Relation:** A relation R on a non empty set A is called equivalence relation iff

(a) R is reflexive i.e $xRx\ \forall x \in A$

(b) R is symmetric i.e $xRy = yRx$

(c) R is transitive i.e xRy and $yRz \Rightarrow xRz \quad \forall x, y, z \in A$

Example: $R = \{(x, y) | x \ || \ y\}$ on straight lines on a plane. Here, ll means "Parallel to".

Let xRx.

$xRx \Rightarrow x||x$ is always true since every line is parallel to itself.

$\therefore$ R is reflexive.

Set $xRy \Rightarrow x|| \ y \Rightarrow \ y||x \Rightarrow yRx$

$\therefore$ R is symmetric

Now, Let xRy and $yRe \Rightarrow x||y$ and $y||z \Rightarrow x||z \Rightarrow xRz$.

$\therefore$ R is transitive.

Now we say that, R is an equivalence relation since it is reflexive, symmetric and transitive.

8. **Partial Order Relation:** A relation R on a non empty set A is called a partial order relation iff.

(a) R is reflexive $\forall x \in A, xRx$

(b) R is antisymmetric xRy and $yRx \Rightarrow x = y$

(c) R is transitive xRy and $yRz \Rightarrow xRz$

Example: $R = \{(A, B) | A \subseteq B\}$ on sets

Now, $\forall A\ A \subseteq A$ is true. $\therefore$ R is reflexive

Let $A \subseteq B$ and $B \subseteq A$

Now, this $\Rightarrow A = B$ $\therefore$ R is antisymmetric

Let $A \subseteq B$ and $B \subseteq C$

Now, this $\Rightarrow A = C$ $\therefore$ R is transitive

We now say that R is a partial order relation, since it is reflexive, antisymmetric and transitive.

Equivalence Relation, Equivalence Classes and Quotient Set

Let R be an equivalence relation on A × A.

Now equivalence class of $x \in$ A can be written as $[x]$.

We define $[x] = \{y | xRy\}$ i.e. for every element of A we can define its equivalence class as the set of all elements related to it.

Example: R = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)} is an equivalence relation on A = {1, 2, 3}

Now,
$$[1] = \{1, 2\}$$
$$[2] = \{2, 1\}$$
$$[3] = \{3\}$$

Notice that [1] = [2] i.e. There are only 2 distinct equivalence classes, Now the set of all equivalence classes is called the quotient set of A induced by R, denoted as A/R

Here A/R = {[1], [2], [3]}= {{1, 2},{3}}

NOTE

- **Theorem:** Every quotient set A/R is also a partition of A.
  Here, the converse is also true.
- **Theorem:** Corresponding to every partition P of A, there exists an unique equivalence relation whose quotient set is exactly P.

To find the equivalence relation corresponding to a given partition, Simply take the union of the cross product of the blocks of the partition with themselves.

Example: Let A ={1, 2, 3, 4}

Find the Equivalence relation corresponding to the partition P_1 = {{1, 2}, {3, 4}}

Now there are two blocks A_1 = {1, 2} & A_2 = {3, 4} in P_1

The equivalence relation R corresponding to partition P_1 is simply,

$$R = A_1 \times A_1 \cup A_2 \times A_2$$
$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$$

Similarly the equivalence relation corresponding to partition P_2 = {{1, 2, 3}, {4}} is

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

Theorem: The relation congruence modulo m is defined as R = {(x, y)} | $x = y \bmod m$} (where m is a fixed integer). This relation partitions the set of integers Z into exactly m distinct equivalence classes.

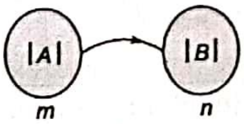
It can be shown that the m distinct equivalence classes are

$$[0] = \{y | y = km, k \in z\}$$
$$[1] = \{y | y = km + 1, k \in z\}$$
$$[m-1] = \{y | y = km + (m-1), k \in z\}$$

These are also called residue classes since 0, 1, 2, ... m−1 are the residues obtained upon dividing any integer by m.

Example - 3.1 Set A has '*m*' elements and Set B has '*n*' elements. What is the total number of relations possible on ARB (from A to B)?

Solution:



The cross product A × B has $m * n$ ordered pairs.

And every relation R is either a subset or proper subset of A × B. This problem reduces to number of subsets of ordered pairs in A × B. There total number of relations are 2^{mn}.

Example - 3.2 What is the total number of reflexive relations from Set A to itself having 'K' elements in the set.

Solution:

$$\begin{bmatrix} 1 & - & - & - \\ - & 1 & - & - \\ - & - & 1 & - \\ - & - & - & 1 \end{bmatrix}_{K \times K}$$

We can represent relation as matrix of size $K \times K$.

There are 'K' reflexive pairs and hence diagonal elements are fixed as 1.

There are $(K^2 - K)$ non-diagonal pair.

Therefore number of reflexive relations are equal to number of subsets of non-diagonal elements.

$\therefore \quad 2^{K^2 - K}$

Example - 3.3 What is the total number of symmetric, relations from set A to itself that has 'n' elements?

Solution:

Let us consider relation as $n \times n$ matrix. There are 'n' diagonal elements representing reflexive pairs or self loops. Therefore 2^n subsets of reflexive pairs. In symmetric relation, the ordered pairs above the diagonal elements are mirror image of the ordered pairs below the diagonal.

Therefore, $\frac{n^2 - n}{2}$ pairs are to be taken.

$\therefore$ Total $\quad 2^n \times 2^{\frac{n^2 - n}{2}} = 2^{\frac{n^2 + n}{2}}$ symmetric relations

Example - 3.4 What is the total number of antisymmetric relations from Set A to itself which has 'n' elements?

Solution:

Self loops are always allowed. Therefore 2^n subsets of reflexive pairs. In antisymmetric relations symmetric ordered pairs are not allowed.

i.e. If (a, b) exists then (b, a) should not be present.

The image pairs can take {10, 01, 00} but not {11}. Therefore, 3 possibilities for all $\left(\frac{n^2 - n}{2}\right)$ pairs.

$\therefore$ Total antisymmetric relations are $2^n \times 3^{\frac{n^2 - n}{2}}$

Example - 3.5 Let R = {(a, b), (b, c), (c, d)} be a relation on set {a, b, c, d}. Which of the following is transitive closure of R?

(a) {(a, b), (b, c), (c, d), (a, d)}

(b) {(a, b), (b, c), (c, d), (a, c), (b, d), (a, d)}

(c) {(a, b), (b, c), (c, d), (b, a), (c, b), (d, c)}

(d) None of these

Solution: (b)

$$R = \{(a, b), (b, c), (c, d)\}$$

$$\text{Transitive closure of } R = \{(a, b), (b, c), (c, d), (a, c), (b, d), (a, d)\}$$

Missing elements in R:

(*i*) (a, b) and (b, c) ⇒ (a, c) (*ii*) (b, c) and (c, d) ⇒ (b, d)

(*iii*) (a, c) and (c, d) ⇒ (a, d)

3.4 Functions

Definition: A **function or mapping** is a relation between the elements of A and those of B having no ordered pairs with the same first component.

In other words, a function is a unique valued relation. i.e. every element of A is mapped to only one element of B. However, elements of B may be related to more than one element of A.

Note that every function is a relation, but a relation may or may not be a function.

If the first element may be thought of as input and the second element as output, then, in a function, every input has a unique output.

Example: $f = \{(1, 1), (2, 3), (3, 3)\}$ is a function on A × A, where A = {1, 2, 3}

Here; $f(1) = \{1\} = 1$

$f(2) = \{3\} = 3$

$f(3) = \{3\} = 3$

Whereas, $R = \{(1, 1), (2, 3), (2, 4), (3, 3)\}$ is not function, since

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

Here R(2) has 2 values 3 and 4 and hence R is not a function.

There are two ways to write a function, one as a formula and other as a relation.

Example: $f(x) = x^2$ and $f = \{(x, y) \mid y = x^2\}$ are both one and the same function.

If a function is written as $f : A \rightarrow B$, it means that f is a mapping that takes all elements of A and maps each, to a unique element of B. It must be noted here

(a) that there may be some elements of the set B which are not associated to any element of set A.

(b) that each element of set A must be associated with one and only one element of set B.

Then A is the domain of f and B is the Co-domain of "*f*".

If $(x, y) \in f$, it is customary to write $y = f(x)$. *y* is called the image of *x* and *x* is called the preimage of *y*.

y is also called value of *f* at *x*. The set consisting of all images of elements of A is called the range of *f*. It is denoted by *f* (A).

Range of $f = f(A) = \{f(x) \mid x \in A\}$

To check if a given relation is a function $f: A \rightarrow B$ check the following:

(*i*) $\forall x \in A$, is $f(x)$ defined and belongs to B?

(*ii*) $f(x)$ is unique, and single valued.

Example: $S = \{(x, y) \mid y = 3x + 1\}$on R × R is a function, since,

(*i*) $\forall x \in R$, $S(x) = y\, 3x + 1 \in R$

(*ii*) $3x + 1$ has a single value for any real value *x*,

∴ S is a function, We say $S : R \rightarrow R$ or $S_{R \rightarrow R}$.

3.4.1 One-One Mapping

A function $f: A \rightarrow B$ is said to be one-one if different elements of A have different f-images in B i.e $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ or equivalently $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

One-one mapping are also called **injection.**

To check if a function is one to one, Let $f(x_1) = f(x_2)$ and see if this leads to a single solution i.e. $x_1 = x_2$. If so, f is one-to-one. Else, it is many to one. (Assuming, it is a function.)

Example: $S = \{(x, y) \mid y = 3x + 1\}$ on $R \times R$

We already have checked that indeed S is a function.

Now to check 1 – 1, we set $S(x_1) = S(x_2)$

$\Rightarrow y_1 = y_2 \Rightarrow 3x_1 + 1 = 3x_2 + 1 \Rightarrow x_1 = x_2$

$\therefore$ S is one-to-one function.

3.4.2 Many-One Mapping

A function $f: A \rightarrow B$ is said to be many one iff two or more different elements in A have the same f-image in B.

A function which is not one-to-one is many to one.

Example: $T = \{(x, y) \mid y = x^2\}$ on $R \times R$

Not it can easily be checked that T is indeed a function.

Now let $T(x_1) = T(x_2) \Rightarrow y_1 = y_2 \Rightarrow x_1^2 = x_2^2$

Now, $x_1^2 = x_2^2$ has two solutions $x_1 = x_2$ or $x_1 = -x_2$

$\therefore$ We say, $x_1^2 = x_2^2 \nRightarrow x_1 = x_2$

$\therefore \qquad T(x_1) = T(x_2)$

$\therefore \qquad T(x_1) = T(x_2) \nRightarrow x_1 = x_2$

This means T is not one-to-one, i.e., It is many-to-one function.

Let $f: A \rightarrow B$ (here $f: A \rightarrow A$ since A = B)

3.4.3 Into-Mapping

The mapping f is said to be into iff there is at least one element in B which is not the f-image of any element in A.

In this case $f(A) \subset B$.

i.e., range of A is a proper subset of B.

Example: $f = \{(1, 1), (2, 3), (3, 4), (4, 3)\}$

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

Now, $\qquad f(A) = \{1, 3, 4\} \subset \{1, 2, 3, 4\}$

$\therefore$ f is an into function.

3.4.4 Onto Mapping

The mapping f is said to be onto iff every elements in B, is the f image of at least one element in A (i.e. every element of B has atleast one pre-image in A).

In this case $f(A) = B$

i.e., the range of f = Co-domain

Onto Mapping is also called **surjection.**

Example: Let $f: A \to B$ be

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

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

Now, $f(A) = \{1, 2, 3, 4\} = B$

∴ f is an onto function.

We say, f is A onto B.

To check if a given function given in formula or set builder notation is onto or not, see if every element $y \in B$ has a preimage in A.

Example: Check if $f: R \to R$

$$f(x) = 3x + 1 \text{ is onto or not}$$

Let, $f(x) = y = 3x + 1$

Now solve x in terms of y.

i.e.
$$x = \frac{(y-1)}{3}$$

$\forall y \in R$, $\frac{y-1}{3}$ is also real

i.e. $\forall y \in R, x \in R$

∴ Every element y in second set has a primage in the first set. i.e. f is onto function.

NOTE: If a function $f: A \to B$ is both one-one and onto, then it is called a bijection function or a bijection. A bijection is also called a one-one correspondence between A and B.

If two sets A and B are in 1-1 correspondence, then $|A| = |B|$, that is they have exactly same number of elements.

3.4.5 Composition of Function

Definition:

Let $f: A \to B$ and $g: B \to C$

The composition of f and g denoted by gof, read as gof results in a new function from $A \to C$ and is given by (gof). $(x) = g(f(x)) \quad \forall y \in A$

Example: Let A = {1, 2, 3}, B = {a, b} and C = {r, s} and $f: A \to B$ is defined by $f(1) = a$ and $f(2) = a$ and $f(3) = b$ and $g: B \to C$ be defined by $g(a) = s$, $g(b) = r$.

Then gof : $A \to C$ is defined by,

(gof) (1) = $g(f(1)) = g(a) = s$

(gof) (2) = $g(f(2)) = g(a) = s$

(gof) (3) = $g(f(3)) = g(b) = r$

Example:

Let $f: R \to R$ be $f(x) = x + 2$

Let $g: R \to R$ be $g(x) = x^2$

Now (gof) $(x) = g(f(x)) = g(x + 2) = (x + 2)^2$

(fog)$(x) = f(g(x)) = f(x^2) = x^2 + 2$

Note that fog ≠ gof (composition is not commutative)

However, fo(goh) = (fog)oh (composition of functions is associative)

Theorems

(a) If f and g are one-one then gof is one-one

(b) If f and g are onto, then gof is onto

(c) If f and g are bijections, then gof is also a bijection.

Identity Mapping

If A is a non- empty set then $f: A \rightarrow B$ such that $f(x) = x$, $\forall x \in A$ is called identity mapping. It is denoted by I_A.

Inverse Mapping

If f is one-one and onto (bijective), from $f: A \rightarrow B$, then f^{-1} exists and it carries elements of B back to A.

Example: Let $f = \{(1, 2), (2, 3), (3, 1)\}$ is a function on $f: A \rightarrow A$ where $A = \{1, 2, 3\}$

Now $f^{-1} = \{(2, 1), (3, 2), (1, 3)\}$ is the inverse function.

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

To find inverse of set builder functions, the following procedure is given:

Example: Find inverse of $f(x) = 3x + 1$, $f: R \rightarrow R$

$f(x) = y = 3x + 1$

1. Write x in terms of y

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

2. Now, if $f(x) = y, x = f^{-1}(y)$

$$\therefore f^{-1}(y) = x = \frac{y-1}{3}$$

$$\text{i.e. } f^{-1}(y) = \frac{y-1}{3}$$

3. Since y is a dummy variable, we can replace it with x also.

$$\text{i.e. } f^{-1}(x) = \frac{x-1}{3}$$

$$\therefore \text{ if } f(x) = 3x + 1, \text{ then } f^{-1}(x) = \frac{x-1}{3}$$

Here the inverse exists because $f(x) = 3x + 1$ is a bijection from R to R.

Example - 3.6 How many onto functions from a set with six elements to a set with three elements?

Solution:

Let P_1, P_2 and P_3 be the properties that b_1, b_2 and b_3 are not in the range of the function, respectively. Note that a function is ONTO if and only if it has none of properties P_1, P_2 or P_3. Hence by using inclusion-exclusion principle the number of ONTO functions from a set with six elements to a set with three elements are:

$$n(\bar{P}_1 \bar{P}_2 \bar{P}_3) = \text{Total \# of functions possible} - [n(P_1) + n(P_2) + n(P_3)] + [n(P_1P_2) + n(P_1P_3) + n(P_2P_3)] - n(P_1P_2P_3)$$

$n(P_i) \rightarrow$ is the number of functions that do not have b_i in their range.

$n(P_iP_j) \rightarrow$ is the number of functions that do not have b_i and b_j in their range.

$n(P_iP_jP_k) \rightarrow$ is the number of functions that do not have b_i, b_j and b_k in their range.

The total number of functions are 3^6.

$n(P_1) = 2^6$ (since b_1 is not in range every element in domain have two choices (b_2 and b_3).

Similarly,

$$n(P_2) = n(P_3) = n(P_1) = 2^6$$

$\Rightarrow$ $$n(P_1P_2) = n(P_2P_3) = n(P_1P_3) = 1^6 = 1$$

(Every element in the domain will have only one choice)

$\Rightarrow$ $$n(P_1P_2P_3) = 0$$

Because this term is the number of functions that have none of b_1, b_2 and b_3 in their range. Clearly, there are no such functions.

$\therefore$ Number of ONTO functions $= 3^6 - 3 * 2^6 + 3 \times 1^6 = 729 - 192 + 3 = 540$

Note: Let m and n be positive integers with $m \geq n$, then there are

$n^m - {}^nC_1\,(n-1)^m + {}^nC_2\,(n-2)^m - {}^nC_3\,(n-3)^m + \ldots +(-1)^{n-1}\,{}^nC_{n-1}\,1^m$

ONTO functions from a set with m elements to a set with n elements.

Example - 3.7 **How many ways are there to assign five different jobs to four different employees if every employee is assigned to atleast one job?**

Solution:

Consider the assignment of jobs as a function from the set of five jobs to the set of four employees. An assignment where every employee gets atleast one job is same as an onto function from the set of jobs to the set of employees.

Hence number of onto functions are:

$n^m - {}^nC_1(n-1)^m + {}^nC_2(n-2)^m - {}^nC_3(n-3)^m + \ldots + (-1)^{n-1}.\,{}^nC_{n-1}.1^m$

where $n = 4$, $n = 5$

$\therefore$ $$4^5 - {}^4C_1(3)^5 + {}^4C_2\,(2)^5 - {}^4C_3(1)^5 = 1024 - 4 \times 243 + 6 \times 32 - 4 = 240$$

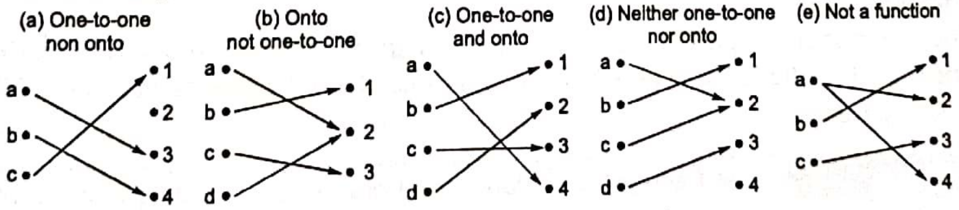
Example - 3.8 **Let f be the function from $\{a, b, c, d\}$ to $\{1, 2, 3, 4\}$ with $f(a) = 4$, $f(b) = 2$, $f(c) = 1$ and $f(d) = 3$. Is f a bijection.**

Solution:

The function f is one-to-one and onto. It is one-to-one because no two values in the domain are assigned the same function value. It is onto because all four elements of the co-domain are images of elements in the domain. Hence f is a bijection.

Figure displays four functions where the first is one-to-one but not onto, the second is onto but not one-to-one, the third is both one-to-one and onto, and the fourth is neither one-to-one nor onto. The fifth correspondence in figure is not a function, because it sends and element to two different elements.

Suppose that f is a function from a set A to itself. If A is finite, then f is one-to-one if and only if it is onto. This is not necessarily the case if A is infinite.



(a) One-to-one non onto (b) Onto not one-to-one (c) One-to-one and onto (d) Neither one-to-one nor onto (e) Not a function

Examples of different types of correspondences

Example - 3.9 **Let f be the function from $\{a, b, c\}$ to $\{1, 2, 3\}$ such that $f(a) = 2$, $f(b) = 3$, and $f(c) = 1$. Is f invertible and if it is what is its inverse?**

Solution:

The function f is invertible because it is a one-to-one correspondence. The inverse function f^{-1} reverse the correspondence given by f, so $f^{-1}(1) = c$, $f^{-1}(2) = a$, and $f^{-1}(3) = b$.

Example-3.10 Let $f : Z \to Z$ be such that $f(x) = x + 1$. Is f invertible, and if it is, what is its inverse?

Solution:
The function f has an inverse because it is a one-to-one correspondence, as we have shown. To reverse the correspondence, suppose that y is the image of x, so that $y = x + 1$. Then $x = y - 1$. This means that $y - 1$ is the unique element of Z that is sent to y by f. Consequently, $f^{-1}(y) = y - 1$.

Example-3.11 Let f be the function from R to R with $f(x) = x^2$. Is f invertible?

Solution:
Because $f(-2) = f(2) = 4$. f is not one-to-one. If an inverse function were defined, it would have to assign two elements to 4. Hence f is not invertible. Sometimes we can restrict the domain or the co-domain of a function, or both, to obtain an invertible function.

Example-3.12 Show that if we restrict the function $f(x) = x^2$ in example previous to a function from the set of all non-negative real numbers to the set of all non-negative real numbers, then f is invertible.

Solution:
The function $f(x) = x^2$ from the set of non-negative real numbers to the set of non-negative real numbers is one-to-one. To see this note that if $f(x) = f(x)$, then $x^2 = y^2$, so $x^2 - y^2 = (x + y)(x - y) = 0$. This means that $x + y = 0$ or $x - y = 0$, so $x = -y$ or $x = y$. Because both x and y are non-negative, we must have $x = y$. So, this function is one-to-one. Furthermore, $f(x) = x^2$ is onto when the codomain is the set of all non-negative real numbers, because each none-negative real number has a square root. That is, if y is a non-negative real number, there exists a non-negative real number x such that $x = \sqrt{y}$, which means that $x^2 = y$. Because the function $f(x) = x^2$ from the set of non-negative real numbers to the set of non-negative real numbers is one-to-one and onto, it invertible. Its inverse is given by the rule $f^{-1}(y) = \sqrt{y}$.

Example-3.13 Let g be the function from the set {a, b, c} to itself such that $g(a) = b$, $g(b) = c$, and $g(c) = a$. Let f be the function from the set {a, b, c} to the set {1, 2, 3} such that $f(a) = 3$, $f(b) = 2$, and $f(c) = 1$. What is the composition of f and g, and what is the composition of g and f?

Solution:
The composition f o g is defined by $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$, and $(f \circ g)(c) = f(g(c)) = f(a) = 3$. Note that g o f is not defined, because the range of f is not a subset of the domain of g.

Example-3.14 Let f and g be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of f and g? What is the composition of g and f?

Solution:

$$(f \circ g)(x) = f(g(x)) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$

and

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) = g(2x + 3)\\ &= 3(2x + 3) + 2 = 6x + 11\end{aligned}$$

3.5 Equal Functions

Two functions f and g on same domain A are equal if $f(x) = g(x)$, $\forall x \in A$.

Symmetric Function

If f and f^{-1} are equal then f is said to be **symmetric function** for example

Let $f = \{(2, 7), (3, 8), (7, 2), (8, 3)\}$ then $f^{-1} = \{(7, 2), (8, 3), (2, 7), (3, 8)\}$

Here $f = f^{-1}$

Hence f is symmetric function.

Binary Operation as a Function

Consider a set 'A' and an operation denoted by '∗' which when placed between two elements a and b produces a unique result denoted by $a * b$ which may or may not belong to A.

If '∗' is **binary operation** on A and $a * b \in A \; \forall \; a, b \in A$, then '∗' is said to be closed and we say 'A' is closed with respect to binary operation '∗'.

Since $a * b$ is unique (single valued) and also if "∗" is closed on A, then we may look at a binary operation as a function from A × A to A.

In such a case instead of $a * b$, we may even write it in functional notation as $*\,(a, b)$.

For example: $a + b = +\,(a, b)$ defined on Z × Z maps pairs of integers to a value which is their sum. i.e. $+\,(1, 2) = 1 + 2 = 3$

$\therefore$ (1, 2) is mapped to 3.

$\therefore$ In this case this is a function $+ : Z \times Z \to Z$

A binary operation may be defined as a formula or as a binary operation table.

Example: $a * b = a + b - ab$ is a binary operation defined by formula method

Say ∗ is defined in Z

Then $2 * 3 = 2 + 3 - 2 \times 3 = -1$

$1 * 2 = 1 + 2 - (1 \times 2) = 1$ and so on.

Example: Let a binary operation be defined as in the following binary operation table.

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

from table we can see that $a * b = a$ & $b * b = c$ & $a * (b * c) = a * c = b$

3.6 Groups

Algebraic Structure: A non empty set S along with one or more binary operations is called an algebraic structure. Suppose ∗ is binary operation on S. Then (S, ∗) is an algebraic structure. (N, +), (Z, +), (Z, −), (R, +, ×) are all examples of algebraic structures.

3.6.1 Semi Group

An algebraic structure (G, ∗) is called a semi group if the binary operation ∗ is closed on G ($a * b \in G \; \forall a, b \in G$) and is associative in G ($(a * b) * c = a * (b * c) \; \forall a, b, c \in G$).

Example: (Z , +) is a semi group since

1. $\forall a, b \in Z$, $a + b \in Z$ (closure)
2. $\forall a, b, c \in Z$, $a + (b + c) = (a + b) + c$

However, (Z, –) is not semigroup since although closure property holds, associative property does not hold for "–", $a-(b-c)^1(a-b)-c$.

3.6.2 Monoid

An algebraic structure (M, ∗) is called a monoid, if.

(*i*) " ∗ " is closed on G

(*ii*) " ∗ " is associative &

(*iii*) $e \in G$ such that $\forall a \in M$, $e * a = a = a * e$

Such an element "*e*" is unique and is called the identity element for the monoid.

NOTE: Every monoid is a semigroup but the converse in not true.

Example: (Z, +) is not only a semigroup, but is also a monoid since

(*i*) and (*ii*) holds and $\forall x \in Z$, $x + 0 = 0 + x = x$

∴ 0 is the identity element for the binary operation "+" on *z*. Notice that (N,+) is also a monoid since $0 \in N$.

However, $(Z^+, +)$ is semigroup, but not a monoid since $0 \notin Z^+$.

NOTE: N = {0, 1, 2, 3, 4....} ← (set of +ve integers)

Set of non - negative integer

→ $Z^+ = \{1, 2, 3, 4....\}$ & $Z^- = \{-1, -2, -3, ...\}$ & $Z = \{0, \pm 1, \pm 2, ...\}$ ← set of integers

3.6.3 Group

An algebraic structure (G, ∗) is called a group, if the binary operation satisfies the following postulates.

1. **Closure property:** $a * b \in G$ $\forall a, b \in G$
2. **Associativity:** $(a * b) * c = a * (b * c)$ $\forall a, b, c \in G$
3. **Existence of identity:** There exists an element $e \in G$ such that $e * a = a = a * e$ $\forall a \in G$. The element *e* is called identity for '∗' in G.'
4. **Existence of inverse:** Each element of G possesses an inverse. In other words for each $a \in G$, there exists an element $b \in G$. Such that $a * b = b * a = e$. The element *b* is called inverse of a and we write $b = a^{-1}$. Thus a^{-1} is an element of G, such that $a * a^{-1} = a^{-1} * a = e$.

Example: (Z, +) is not only a semigroup and a monoid, but it is also a group.

(Z, +) has already has been shown to satisfy (*i*) closure (*ii*) association property and (*iii*) existence of identity. Now we shall show that condition (*iv*) for group, also holds for (Z, +).

$\forall x \in Z$, If inverse exists it must satisfy., $x * x^{-1} = x^{-1} * x = e$

$\Rightarrow$ $x + x^{-1} = x^{-1} + x = 0$ (since 0 is the identity element for +)

$\Rightarrow$ $x^{-1} = -x$ since $-x \in z$ ∴ $\forall x \in Z, x^{-1} \in Z$ exists

Just like identity element, the inverse is also unique for a given element. Notice, however that there is only one identity element for the entire group, whereas there is a unique inverse for each element of G.

In (Z, +), the identity element is 0 for the entire group, while inverse of 1 is –1, inverse of 2 is –2, and so on.

Note however that (Z, ×) is not a group since although it is closed, associative, identity exists (= 1), inverse does not exist for all elements.

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

but $0 \in Z$ and does not have an inverse, since $\frac{1}{0} = \infty \notin Z$

∴ (Z, *x*) is not a group.

3.6.4 Abelian Group or Commutative Group

A group G is said to be **abelian or commutative**, if in addition to the above four postulates, the following postulates are also satisfied.

Commutative: i.e., $a * b = b * a \; \forall a, b \in G$.

Example: (Z, +) is an abelian group, since it has already been shown to be a group, and it has the commutation property also.

i.e. $\forall x, y \in Ƶ \; x + y = y + x$.

Notice that the set of (2 × 2 non singular matrices, *) when "*" is matrix multiplication is a group but not an abelian group, since matrix multiplication is not commutative.

i.e $A * B \neq B * A, \forall A, B \in$ (2 × 2 non singular matrices)

3.6.5 Finite or Infinite Groups

If in a group G, the underlying set G consists of a finite number of elements, then the group is called finite group, otherwise as infinite group.

Order of the Group

The number of elements in a finite group is called the order of a group. An infinite group is said to be of infinite order.

Some General Properties of Groups:

Suppose our group consists of a non-empty set G equipped with a binary operation denoted by *. Then,

1. The identity element in a group is unique.
2. The inverse of each element of a group is unique.
3. If the inverse of a is a^{-1}, then the inverse of a^{-1} is a i.e $(a^{-1})^{-1} = a$.
4. The inverse of the product of two elements of a group G is the product of the inverse taken in reverse order $(ab)^{-1} = b^{-1}a^{-1} \; \forall a, b \in G$.
5. If a, b, c are any elements of G, then $ab = ac \Rightarrow b = c$ (Left Cancellation Law) $ba = ca \Rightarrow b = c$. (Right Cancellation Law).
6. If a, b are any two elements of a group G, then the equation $ax = b$ and $ya = b$ have unique solution in G, given by $x = a^{-1} b$ and $y = ba^{-1}$, respectively.
7. The left inverse of an element is also its right inverse i.e if a^{-1} is left inverse of a (i.e. $a^{-1}a = e$), then $a a^{-1} = e$, which means that a^{-1} is also the right inverse of a.

3.6.6 Cayley Table

The binary operation table for a finite group are called cayley tables.

A cayley table for a group with only 4 elements is presented below:

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

It can be verified that ({e, a, b, c}, *) is indeed a group. It is conventional to put the identity element in the front of both row and column in a cayley table.

Properties of Cayley Tables:

1. The row and column containing e will be a copy of the column headers & row headers respectively. This is because by definition $x * e = e * x = x \quad \forall x \in G$
2. Since $ax = b$ and $ya = b$ have a unique solution, Every element in every row (or column) of the table must be different.

   That it to say that no element can be repeated in any row (or column) i.e. Each row or column is only a permutation of the element of G.

   In the example given each row and column can be seen to be a permutation of *e, a, b, c.*
3. The cayley table tells us if the group is abelian or not. If the cayley table is symmetric about the diagonal (as is the case in the example given), then the group is abelian.
4. In the cayley table, if e appears anywhere in off diagonal, then another e has to appear in its mirror image location (using diagonal as the mirror).

   This is because, an off diagonal e means $a \neq b$ and $a * b = e$, but, this implies that $b * a = e$, Thereby the mirror image location must also have an *e*.

   e appears in the diagonal, then the corresponding element is its own inverse.

Theorem: If every element of a group is its own inverse, then the group is abelian. (The converse is not necessarily true).

In other words, if G is a group and $\forall x \in G$ if $x^2 = e$, then the group is abelian.

Multiplication Modulo p

We shall now define a new type of multiplication known as 'multiplication modulo *p*' and written as $a \times_p b$ where *a* and *b* are any integers and *p* is a fixed positive integer. By definition. We have $a \times_p b = r, o \leq r < p$ where *r* is the least nonnegative remainder when ab is divided by *p*. For Ex.

$$8 \times_5 3 = 4 \text{ (since } 24 = 4(5) + 4)$$

Also, $$4 \times_7 2 = 1 \text{ (since } 4 \times 2 = 8 = 1(7) + 1)$$

Some Properties of Integers:

Let, $Z = \{......-3, -2, -1, 0, 1, 2, 3......\}$ be the set of integers

Division Algorithm

Let $a \in Z$ and $d \in Z^+$. Then we can divide *a* by *b* to get nonnegative remainder *r* which is smaller in size than b. In other words if $a \in Z$ and $d \in Z^+$, then there exist unique integers *q* and *r* such that

$a = dq + r$ where $o \leq r < d$

Example: $a = 23$, $d = 3$, then $23 = 3 \times 7 + 2$.

(*q* is called quotient and *r* is called as reminder).

Divisibility in Set of Integers

Let $a, b \neq 0 \in |$. We say that a is divisible by *b* if $a = bm$ where *m* is some integer. i.e. if **b** divides **a**, then **a** is a multiple of **b**.

Greatest Common Divisor

Let *a* and *b* be any two integers. Then the positive integer *c* is said to be greatest common divisor of *a* and *b* if

(*i*) $c | a$ and $c | b$

(*ii*) Whenever $d | a$ and $d | b$, then $d | c$

The greatest common divisor of integer *a* and *b* will be symbollically denoted by GCD (*a*, *b*).

3.6.7 Some Classic Examples of Group's

1. Let B = {0, 1} & operation + is defined as:

+	0	1
0	0	1
1	1	0

Then (B, +) is an abelian group with 0 as identity and each element is its own inverse. Infact this + as defined in table is nothing but the XOR operation

2. $(Z_m, +_m)$ is an abelian group for every $m \in Z^+$, where Z_m is the set of equivalence classes for the relation congruence modulo m & $+_m$ is the modulo m addition. The operation table for $(Z_5, +_5)$ is

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

Here, [1] = set of all integers which leave a remainder of 1 when divided by 5 = {±6, ±11, ±16, ±...., ± ($5m$ +1)} of course, a simpler form of this is simply ({0, 1, 2, 3, 4}, $+_5$).

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

3. When p is prime, ({1, 2, 3, ... p–1}, $\times_p$) is always on abelian group.
Example: ({1, 2, 3, 4}, $\times_5$)

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Here the inverse of 2 is 3, 3 is 2, 4 is 4 & 1 is 1. A more general version of this is {Z_p–{0}, $\times_p$}, is also an abelian group.

$\times_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

4. **Symmetric group of permutations:**

Let S = {1, 2, 3} Let S_n be the set of all permutations on S. There are 3! = 6 permutations. Each permutations is a one-one, onto map from S to S. The S_n form a group under the operation composition of mappings. This group S_n is called the symmetric group of permutations of order *n*.

Consider S = {1, 2, 3}, Then $S_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}_7$. Where

$$p_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, p_2 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, p_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

$$p_4 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, p_5 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, p_6 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

The compositions 0 are given in table below:

0	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_6	p_5	p_4	p_3
p_3	p_3	p_5	p_1	p_6	p_2	p_4
p_4	p_4	p_6	p_5	p_1	p_3	p_2
p_5	p_5	p_3	p_4	p_2	p_6	p_1
p_6	p_6	p_4	p_2	p_3	p_1	p_5

p_1, is the identity element. S_3 is called the group of symmetric of a triangle.

This group is not abelian.

Power of an Element

Let (G, *) be a group and let $a \in G$, for any position integer *m*, we define, $a^m = a * a * a * ..... * a$ (*m* times) and $a^{-m} = (a^{-1}) * (a^{-1}) * (a^{-1}).... * (a^{-1})$ (*m* times) $a^0 = e$ and if *m* & *n* are position integers, then $a^{m+n} = a^m * a^n$

Example: On (*z*, +) which is a group

$$1^3 = 1 + 1 + 1 = 3$$

$$2^3 = 2 + 2 + 2 = 6$$

$$2^{-3} = 2^{-1} + 2^{-1} + 2^{-1} = (-2) + (-2) + (-2) = -6$$

Order of an Element of a Group

Suppose G is group. By the order of an element $a \in G$, is meant the least positive integer n, if one exists, such that $a^n = e$ (the identity of G).

If there exists no positive integer n such that $a^n = e$, then we say that a is of infinite order. We shall use the symbol O(*a*) to denote the order of *a*.

Example: Consider the group given below

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

The order of the group = $|G| = 4$

The order of element *e* is 1 since $e^1 = e$

The order of element *a* is 4 since $a^4 = a * a * a * a = b * a * a = c * a = e$.

The order of element *b* is 2 since $b^2 = b * b = e$ and the order of element *c* is 4 since $c^4 = c * c * c * c = b * c * c = a * c = e$ in (Z, +), the order of each element other than 0 is ∞ and the order of element 0 is 1.

Some Results Regarding Order of an Element

1. The order of every element of a finite group is finite and is less than or equal to order of group.
2. The order of an element a of a group is the same as that of its inverse a^{-1}.
3. The order of any integral power of an element a, cannot exceed the order of a.
4. If the element a of G is of order m, then $a^n = e$ iff m is a divisor of n.
5. The order of the elements a and $x^{-1}ax$ are the same where a, x are any two elements of a group.
6. Order of ab is same as that of ba where a and b are any elements of a group.
7. If a is an element of order n and p is prime to n, then a^p is also of order n.

3.6.8 Cyclic Group

A group (a, *) is called a cyclic group if there exists an element a ∈ G such that every element of G can be written as a^n for some integer n. That is G = $\{a^n | n \in z\}$. We say that G is generated by a. a is the generator of G, we may then write G – {a} or G (a). Naturally, a cyclic group is abelian.

The order of a cyclic group is same as that of its generator.

1. (Z, +) is a cyclic group generated by 1.
2. (Z_m, t_m) is generated by [1].

Note that in example 1, order of G = order of 1 = ∞ and in example 2, order of G = $|Z_m|$ = order of [1] = m.

Properties of Cyclic Group:

1. Every cyclic group is an abelian group.
2. If a is generator of a cyclic group G, then a^{-1} is also a generator of G.
3. A cyclic group G with generator a of finite order n, is isomorphic to multiplicative group of n, n^{th} roots of unity.
4. A cyclic group G with a generator of finite order n is isomorphic to the additive group of residue classes modulo n.
5. If a finite group of order n contains element of order n, the group must be cyclic.
6. Every group of prime order is cyclic.
7. Every subgroup of a cyclic group is cyclic.

Method for Finding the number of generators of a cyclic group of order n: The number of generators of a cyclic group of order n is same as the number of numbers from 1 to n, which are relatively prime to n.

Method for finding the number of numbers from 1 to n, which are relatively prime to n: The number of numbers from 1 to n, which are relatively prime to n i.e., gcd $(m, n) = 1$, is given by the Euler Totient function $\phi(n)$. If n is broken down into its prime factors as $n = p_1^{n_1} \cdot p_2^{n_2} \ldots$ where p_1, p_2 etc. are distinct prime numbers, then

$\phi(n) = \phi(p_1^{n_1})\,\phi(p_2^{n_2})\ldots$ then by using the property

$$\phi(p^k) = p^k - p^{k-1}$$

we can find each of $\phi(p_1^{n_1}), \phi(p_2^{n_2})\ldots$ etc.

For *example*, let us find the number of generators of a cyclic group of order 80:

The number of generators of a cyclic group of order 80 = The number of numbers from 1 to n, which are relatively prime to 80.

Since $80 = 2^4 \times 5^1$.

The number of numbers from 1 to n, which are relatively prime to 80 = $\phi(80) = \phi(2^4) \times \phi(5^1)$

Now $\phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$.

Similarly, $\phi(5^1) = 5^1 - 5^0 = 5 - 1 = 4$.

So, $\phi(80) = 8 \times 4 = 32$.

So, the number of generators of a cyclic group of order 80 is exactly 32.

3.6.9 Subgroup

Let (G, $*$) be a group. A non empty subset H of G is called a subgroup of G if the following conditions are satisfied.

1. $a \in H, b \in H \Rightarrow a * b \in H$ (closure)
2. The identity $e \in H$ also (existence of identity)
3. $a \in H \Rightarrow a^{-1} \in H$ (existence of inverse)

In other words, (H,$*$) is a subgroup of (G,$*$), if $H \subseteq G$ and (H, $*$) is itself a group (since associative law holds in H also.)

Example: (E, +) where E is the set of even integers is a subgroup. In fact, $(kz, +)$ when $k \in z^+$, is a subgroup of $(z, +)$.

Properties of Subgroup:

1. For any group (G, $*$), ($\{e\}$, $*$) and (G, $*$) are called trivial subgroups. Other subgroups (if any) of (G, $*$) are called proper subgroups.
2. The identity of a sub group is same as that of the group (as seen in definition).
3. The inverse of any element of a subgroup is same as the inverse of that element when regarded as part of the group.
4. The order of any element of a subgroup is same as the order of that element when regarded as member of the group.

Important Results

1. A necessary and sufficient condition for a non-empty subset H of a group to be a subgroup is that $a \in H, b \in H, \Rightarrow ab^{-1} \in H$ where b^{-1} is the inverse of b in G.
2. A necessary and sufficient condition for a non empty finite subset H of a group G, to be a subgroup is that H must be closed with respect to multiplication i.e $a \in H, b \in H \Rightarrow ab \in H$.
3. If H, K are two subgroups of a group G, then HK is a subgroup of G iff HK = KH.
4. If H, K are subgroups of an abelian group G, then HK is subgroup of G.
5. If H_1, H_2 are two subgroups of a group G, then $H_1 \cap H_2$ is also a subgroup of G.
6. Arbitrary intersection of subgroups i.e the intersection of any family of subgroups of a group is a subgroup.
7. The union of two subgroups is not necessarily a subgroup.

Cayley's Theorem

Every finite group G is isomorphic to a permutation group.

Cosets

Let (G, $*$) be a group and (H, $*$) be a sub group of G for any $a \in G$, the set

$aH = \{a * h \mid h \in H\}$ is called the left coset of H, determined by a.

$Ha = \{h * a \mid h \in H\}$ is called the right coset of H, determined by a.

Example: Consider the group ({0, 1, 2, 3}, $+_4$), whose table is given below:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Now consider H = {0, 2}

H since H $\subseteq$ G,

$a \in$ H, $b \in$ H, $a * b \in$ H, (it is closed), identity $e = 0 \in$ H,

$0^{-1} = 0 \in$ H and $2^{-1} = 2 \in$ H

$\therefore$ H is clearly a subgroup of G.

Now the left coset determined by 0 is {0, 2}

Now the left coset determined by 1 is {1, 3}

Now the left coset determined by 2 is {0, 2}

Now the left coset determined by 3 is {1, 3}

$\therefore$ There are only two distinct left cosets of H in G.

Note: If $a \in$ H, aH = H

Similarly the right coset determined by 0 is {0, 2}

Similarly the right coset determined by 1 is {1, 3}

Similarly the right coset determined by 2 is {0, 2}

Similarly the right coset determined by 3 is {1, 3}

Since in this subgroup the set of left cosets & right cosets of H in G are same, H is a normal subgroup of G.

Notice that although H = {0, 2} is a subgroup of G, T = {1, 3} is not a subgroup of H (closure property does not hold).

3.6.10 Normal Subgroup

A subgroup H of a group G is said to be a **normal subgroup** of G iff aH = Ha $\forall a \in$ G (Where aH and Ha are the left and right cosets of H in G).

Alternatively, if for every $x \in$ G, and for every $h \in$ H, $x h x^{-1} \in$ H, then H is a normal subgroup of G.

A group having no proper normal subgroups is called a simple group.

Some important results on normal subgroups:

1. A subgroup H of a group G is normal iff x Hx^{-1} = H $\forall x \in$ G.
2. A subgroup H of a group G is a normal subgroup of G iff each left coset of H in G is a right coset of H in G i.e aH = Ha $\forall a \in$ G.
3. The intersection of any two normal subgroups of a group is a normal subgroup.
4. The intersection of any collection of normal subgroups is itself a normal subgroup.

Lagrange's Theorem

The order of each subgroup of a finite group is a divisor of the order of the group.

NOTE: Converse of Lagrange's theorem is not true.

Corrollary: Order of the product of two subgroups of a group G.

Let H and K be finite subgroups of a group G.

$$O(HK) = \frac{O(H)\circ O(K)}{O(H\cap K)}$$

Example for lagranges theorem:

We have seen that in the group ({0, 1, 2, 3} $+_4$)

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

H = {0, 2} is a sub group.

The order of this group is $|G| = 4$

The order of this subgroup is $|H| = 2$

Clearly $|H|$ divides $|G|$, which verifies the lagranges theorem.

In fact from lagranges theorem, we can conclude that in this case a subgroup of order 3 is not possible since 3 does not divide 4.

3.7 Lattice

Posets: A non empty set P, together with a binary relation R is said to form a partially ordered set or a poset if following conditions are satisfied

1. **Reflexivity:** aRa for all $a \in P$
2. **Anti symmetry:** If $a\,Rb$ and $b\,Ra$ then $a = b (\forall a, b \in P)$
3. **Transitivity:** If $a\,Rc$, $b\,Rc$ then $a\,Rc$ $(\forall a, b, c \in P)$

In other words, a non empty set P, together with a partial order relation is called as a poset (or partially ordered set.)

For convenience, we generally use the symbol ≤ in place of R. We read ≤ as "less than or equal to" (although it may have nothing to do with the usual "less than or equal to" that we are so familiar with).

If $a \leq b$ or $b \leq a$ in a poset, we say that a and b are comparable. Two elements of a poset may or may not be comparable. If $a \leq b$ and $a \neq b$, we will write $a < b$ (and read as "a is less than b").

Example: (S, ⊆) is a poset where S is the set of all sets. So if (P(A), ⊆) where P(A) is the power set of a given set A. The set (Z, ≤) is also a poset where "≤" is the usual numerical ≤.

The set (Z^+, divides) denoted also as (Z^+, |) is also a poset where "|" symbol means aRb iff $a|b$ (a divides b).

3.7.1 TOSET

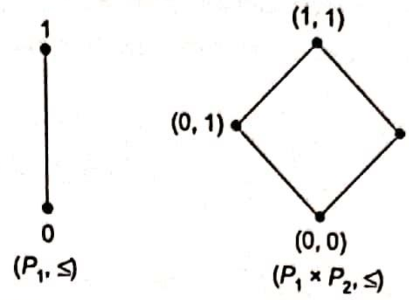
A poset (P, ≤) in which every pair of element $a, b \in P$ are comparable (i.e. either $a \leq b$ or $b \leq a$) is called a toset (totally ordered set) or a chain. Example (Z, ≤) is a toset.

Product Partial Order

If $(P_1, \leq_1)$ and $(P_2, \leq_2)$ are two partial order. Then we define a new partial order called product partial order which is $(P_1 \times P_2, \leq)$ in this way.

$(a_1, b_1) \leq (a_2, b_2)$ iff $a_1 \leq_1 a_2$ and $b_1 \leq_2 b_2$ where $(a_1, b_1), (a_2, b_2) \in P_1 \times P_2$

Example:



$(P_1, \leq)$ $(P_1 \times P_2, \leq)$

Here, $P_1\{0, 1\} = P_2(P_1 \times P_2, \leq)$

If the posets P_1 and P_2 are lattices, then $(P_1 \times P_2, \leq)$ is called the product lattice.

3.7.2 Hasse Diagram

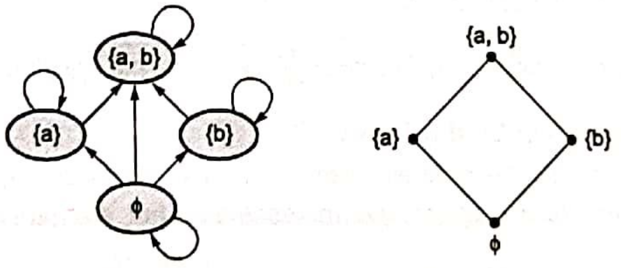
The digraph of a poset may be very complicated. To simplify this diagram while retaining the essential features of the poset, a diagram called Hasse diagram is drawn. The Hasse diagram contains all information regarding poset; but is much more simplified and easier to interpret and use than a digraph. The procedure for constructing a Hasse diagram of a poset is as follows:

1. Draw the digraph of the poset, so that all arrows are pointing upwards.
2. Reduce the circle of the nodes to points with labels adjacent to the points.
3. Remove all self loops (since it is understood that a partial order relation is always reflexive)
4. Remove all arrows which can be inferred by transitive property (i.e. *aRb*, *bRc* and *aRc*, then remove arrow corresponding to aRc.)
5. Remove all the arrow heads (since it is understood that the arrows are pointing upwards)

The result of the above 5 steps is a Hasse diagram of the poset.

NOTE: The Hasse diagram of a Toset (or a chain) will have no branches. (i.e. it will be a line of nodes in a chain).

Example: The digraph and the corresponding hasse diagram for the Poset (P(A),⊆), where A = {*a*, *b*} is shown next page:



Digraph Hasse Diagram

3.7.3 Supremum and Infimum of Poset

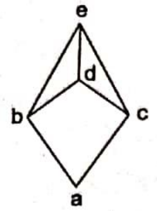
Let S be a non empty subset of a poset P. An element $a \in$ P is called an upper bound of S if $x \leq a \, \forall x \in$ S. Further if a is an upper bound of S such that $a \leq b$ for all upper bounds b of s, then a is called least upper bound (ℓ. u. b) or supremum of S. We write sup S for supremum S.

It is important to note that there can be more than one upper bound of a set. But sup, if it exists, will be unique. Again comparing with the definition of greatest element we notice whereas the greatest element belonged to the set itself, an upper bound or sup can lie outside the set.

An element $a \in$ P will be called a lower bound of S if $a \leq x$, $\forall x \in$ S and a will be called greatest lower bound ($g . \ell . b$) or infimum S or Inf S, if $b \leq a$ for all lower bounds b of S.

In the hasse diagram example above, if we take say S = {{a}, {b}}, then LUB(S) =Sup (S) = {a, b} GLB(S) = Inf (S) = ϕ

In the hasse diagram given below:



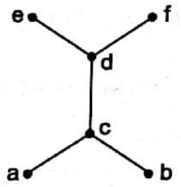
Let, S = {*b*, *c*, *d*}, Now UB (S) = upper bounds of S = {*d*, *e*}
LUB (S) = Sup (S) = *d*
GLB (S) = Inf (S) = *a*

NOTE: Although, there may be many upper and lower bounds for a given subset S of a poset, there can be only one LUB and one GLB of S. i.e. LUB (or Sup (S)) and GLB (or Inf (S)) of S in unique.

3.7.4 Maximal and Minimal Elements of Poset

An element $a \in$ P is called maximal if there exist no element x such that $a \leq x$. (i.e. no element is above a in hasse diagram) An element $a \in$ P is called minimal if there exist no element x such that $x \leq a$. (i.e. no element is below **a** in the hasse diagram).

Example: In the hasse diagram below:



e and *f* are maximal elements of the poset.
a and *b* are the minimal elements of the poset.

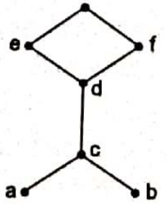
NOTE: There can be more than one maximal or minimal elements in a poset.

3.7.5 Greatest and Least Elements of a Poset

An element $a \in$ P is called the greatest element if $\forall x \in$ P, $x \leq a$. (Usually the greatest element s sometimes devoted by I in the hasse diagram) (i.e. In hasse diagram, element *a* is above all elements of the poset).

An element $a \in$ P is called the least element if. $\forall x \in$ P, $a \leq x$ (i.e. in hasse diagram, element *a* is below every element of the poset). Usually the least element is sometimes denoted by 0 in the Hasse diagram.

Example:



In the hasse diagram shown above, *g* is the greatest element. But there is no least element in this poset. Notice, however, that there are two minimal elements in this poset, none of which is the least element (since they are not comparable).

NOTE: There can be only one greatest element and only one least element, if they exist for any poset. A chain is a set of all comparable elements and an antichain is a set of all incomparable elements in a poset.

Theorem

If the longest chain in a partial order is of length n, then the partial order can be written as a partition of n antichains.

Dual of the Above Theorem

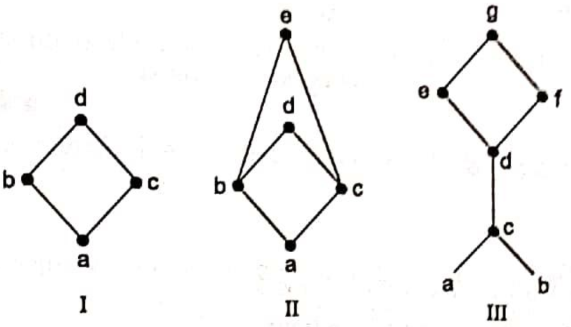
If the longest antichain has size *t*, then the set can be partitioned into *t*-chains.

Lattices

A poset (L, ≤) is said to form a lattice if for every pair of elements *a*, *b* ∈ L, Sup{*a*, *b*} and Inf {*a*, *b*} exist in L.

In that case, we write

Sup{*a*, *b*} = $a \vee b$ (read '*a* join *b*') = LUB (*a*, *b*)
Inf{*a*, *b*} = $a \wedge b$ (read '*a* meet *b*') = GLB (*a*, *b*)



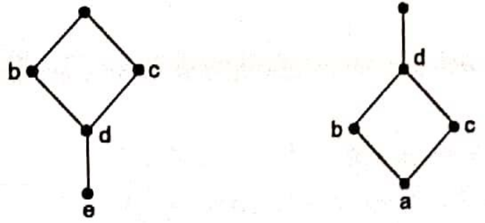
(*i*) is a lattice, while II and III are not lattices.

(*ii*) is not a lattice, since $b \vee c$ does not exist (There are two upper bounds to {*b*, *c*}, which are *d* and *e*. But *d* and *e* are not comparable, hence no LUB.

(*iii*) is not an lattice since, GLB (*a*, *b*) does not exist.

Dual Lattice

For a lattice (P, ≤), the dual is (P, ≥). The duals are shown in figure below. The diagram of (P, ≥) is obtained from that of (P, ≤) by simply turning it upside down.



$a \leq b \leq d \leq e$ $\quad$ $e \geq d \geq b \geq a$

$a \leq c \leq d \leq e$ $\quad$ $e \geq d \geq c \geq a$

Example: Let A be a non empty set then the poset (P(A), $\subseteq$) of all subset of A is a lattice. Here for A, B $\in$ P(A) $A \wedge B = A \cap B$ and $A \vee B = A \cup B$.

Example: The poset {2, 3, 4, 6} under divisibility is not a lattice as $4 \vee 6 =$ LCM (4, 6) does not exist.

NOTE: A poset (L, $\leq$) is a lattice iff every non empty finite subset of L has sup and Inf.

Some Lattice Results

If L is any lattice, then for any $a, b, c \in L$, the following results hold

1. $a \wedge b \leq a,\ b \leq a \vee b$
2. $a \leq b \Leftrightarrow a \wedge b = a$ (Consistency)

   $\Leftrightarrow a \vee b = b$
3. $a \wedge a = a,\ a \vee a = a$ (Idempotency)
4. $a \wedge b = b \wedge a,\ a \vee b = b \vee a$ (Commutativity)
5. $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ (Associativity)

   $a \vee (b \vee c) = (a \vee b) \vee c$
6. **Domination Laws:**

   If $0, I \in L$, then

   $0 \wedge a = 0,\ 0 \vee a = a$

   $I \wedge a = a,\ I \vee a = I$
7. $a \wedge (a \vee b) = a$ (Absorption Laws)

   $a \vee (a \wedge b) = a$
8. $a \leq b,\ c \leq d \Rightarrow a \wedge c \leq b \wedge d$

   $a \vee c \leq b \vee d$

   In particular

   $a \leq b \Rightarrow a \wedge x \leq b \wedge x$ and $a \vee x \leq b \vee x\ \forall x \in L$
9. In any lattice the distributive inequalities hold.

   $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$

   $a \wedge (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$
10. In any lattice L, the modular inequality holds.

    $a \wedge (b \vee c) \geq b \vee a \wedge c$

    holds for all $a, b, c \in L$, $a \geq b$.
11. In any lattice L

    $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$

Another Definition of a Lattice

A non empty set L together with two binary operations $\wedge$ and $\vee$ is said to form a lattice if $\forall\ a, b, c \in L$, the following conditions hold.

(i) Idempotency: $a \wedge a = a,\ a \vee a = a$

(ii) Commutativity: $a \wedge b = b \wedge a,\ a \vee b = b \wedge a$

(iii) Associativity: $a \wedge (b \wedge c) = (a \wedge b) \wedge c,\ a \vee (b \vee c) = (a \vee b) \vee c$

(iv) Absorption: $a \wedge (a \vee b) = a,\ a \vee (a \wedge b) = a$

NOTE

- Dual of lattice is a lattice.
- Product of two lattice is a lattice.
- A finite lattice surely has least and greatest elements i.e. a finite lattice is always bounded.
- Every chain is a lattice.
- The set (D_n, I) is always a lattice, where D_n is the set of divisors of integer n. Here LUB (a, b) = LCM (a, b) and GLB (a, b) = GCD (a, b).
- The set (Z^+, I) is also a lattice.
- The set (P (A), $\subseteq$) is a lattice, (In fact, it is also a Boolean Algebra). Here for any two sets A and B.
  LUB (A, B)=$A \cup B$ and GLB(A, B) = $A \cap B$.

3.8 Types of Lattices

Bounded Lattice: A Lattice (L, ≤) is called bounded, if the lattice has a greatest and least element, usually denoted by I and O respectively. (or sometimes 1 and 0).

3.8.1 Bounded Lattice Properties

1. $\forall a \in L$ $\qquad$ $0 \leq a \leq 1$,
2. $0 \wedge a = 0$, $\qquad$ $0 \vee a = a$
3. $I \wedge a = a$, $\qquad$ $I \vee a = I$

Example: (P (A), $\subseteq$) is bounded where A = {a, b} with I = {a, b} & 0 = ϕ while (Z, ≤) is an unbounded lattice.

3.8.2 Complemented Lattice

The complement a of any element in a lattice (L, ≤) is an element which satisfies both the properties give below:

$a \wedge a' = 0$ & $a \wedge a' = I$

Obviously, complement is defined only for a bounded lattice. If in a lattice (L, ≤), if at least one complement exists for every element $a \in$ L, then such a lattice is called a complemented lattice.

3.8.3 Distributive Lattice

A Lattice (L, ≤) is called distributive, if it satisfies both the distributive laws.

i.e. $\forall a, b, c \in L$

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

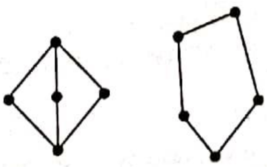
$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

Checking if a given hasse diagram corresponds to a distributive lattice or not, is tedious.

However the following result is useful for checking if a lattice is non distributive or not.

Theorem

A lattice is non-distributive iff it contains a sublattice, isomorphic to one of the non distributive lattices given below.



Another result that is useful for establishing if a lattice is distributive or not is the following.

Theorem

In a distributive bounded lattice, if a complement exists, then it is unique.

Another way to understand this is that if in a lattice, there is more than one compliment for some element of the lattice, then such a lattice cannot be distributive. This theorem cannot be used to prove that the lattice is distributive. It can only be used to show that a lattice is non-distributive.

NOTE: A bounded, complemented and distributive lattice is also called a Boolean Algebra.

3.8.4 Semi Lattices

1. A poset (P, ≤) is called a meet semi lattice if for all a, $b \in$ P, Inf $\{a, b\}$ exists.
2. A non empty set P together with a binary composition $\wedge$ is called a meet semi lattice if a, b, $c \in$ P.
   (*i*) $a \wedge a = a$
   (*ii*) $a \wedge b = b \wedge a$
   (*iii*) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$

3.8.5 Complete Lattices

A lattice L is called a complete lattice if every non empty subset of L has its Sup and Inf in L.

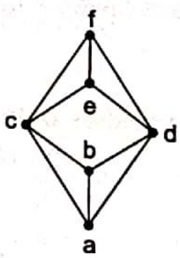
Results

1. Dual of a complete lattice is complete.
2. If (P, ≤) is a poset with greatest element I such that every non empty subset S of P has Inf, then P is a complete lattice.
3. If (P, ≤) is a poset with least element 0 such that every non empty subset S of P has Sup then, P is a complete lattice.

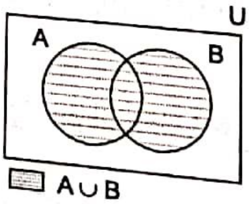
3.8.6 Sub-lattices

A non empty subset s of a lattice L is called a **sublattice** if, a, $b \in$ S $\Rightarrow a \wedge b$, $a \vee b \in$ S (it is understood that $\wedge$ and $\vee$ are taken in L).

Example: Consider the lattice given below:



Now the lattice given below is a sublattice of the lattice given above.



A sublattice S of a lattice L is called a **"convex sublattice"** if for all a, $b \in$ S $[a \wedge b, a \vee b] \subseteq$ S.

Results Regarding Sub-lattices

1. ϕ is a subset of every lattice (as it vacuously satisfies definition).
2. Every lattice is a sublattice of itself.

3. If L is any lattice and a $\in$ L be any element then {a} is a sublattice of L.
4. Every non empty subset of a chain is a sublattice (called a subchain)
5. The union of two sublattice may not be a sublattice.
6. A lattice is a chain iff every non-empty subset of it is a sublattice.

3.9 Boolean Algebra

Definition: A Lattice is called a **boolean algebra** if it is bounded, complemented and distributive.

A non empty set alongwith two binary operations "$\vee$" and "$\wedge$" (i.e. Sup and Inf), is called a Boolean Algebra if it is satisfies the following 6 axioms.

We may substitute + 4 for $\vee$ and . for $\wedge$ in a Boolean Algebra.

Axioms

1. **Closure:** $\forall a, b \in S$, $a + b \in S$ $a.b \in S$
2. **Commutativity:** $\forall a, b \in S$, $a + b = b + a$ $a.b = b.a$
3. **Associativity:** $\forall a, b, c \in S$, $a + (b + c) = (a + b) + c$ $a.(b.c) = (a.b).c$
4. **Distributivity:** $\forall a, b, c \in S$, $a + (b.c) = (a + b).(a + c)$ $a.(b + c) = (a.b) + (a.c)$
5. **Existence of Identity:** $\forall a \in S$, $\exists e$ (unique) such that $a + e = e + a = a$
6. **Existence of Compliment:** $\forall a \in S$, $\exists e' \in$ such that $a + a' = a' + a = 1$ and $a.a' = a'.a = 0$

Other Derived Laws of Boolean Algebra

1. $\left.\begin{array}{r} a+a=a \\ a.a=a \end{array}\right]$ idempotent laws

2. $(a')' = a$ - double complement law

3. $\left.\begin{array}{r} a+a.b=a \\ a.(a+b)=a \end{array}\right]$ absorption laws

4. $\left.\begin{array}{l} (a+b)'=a'.b' \\ (a.b)'=a'+b' \end{array}\right]$ Demorgan's Laws

5. $\left.\begin{array}{l} a+0=a,\ a.0=0 \\ a+1=1,\ a.1=a \end{array}\right]$ Domination Laws

Operator Precedence in Boolean Expressions

1. Expressions are scanned from left to right.
2. Expressions are evaluated with following precedence, ( ), complement, ., +

   Examples: A + B. C will be Evaluated as A + (B. C)

   In $\overline{(A+B)}$, (A+B) is evaluated first and then complemented.

Simplification of Boolean Expressions

Boolean algebraic expressions may be simplified by using axioms and derived laws of Boolean Algebra.

Example:

$$\begin{aligned} (a + ab)'\,(a + b) &= (a)'\,(a + b) && \text{\{Absorption law\}} \\ &= a'\,a + a'\,b && \text{(Distributive law)} \\ &= 0 + a'\,b && \text{(Complement law)} \\ &= a'\,b && \text{(Domination law)} \end{aligned}$$

Summary

- Sets which have a finite number of elements are called **finite sets** and those having infinite number of elements are called **infinite sets.**
- Most of relationship between the sets can be represented by diagrams known as venn diagrams.
- Venn diagrams can be effectively used for proving equality of set expressions or for answering question regarding counting of elements of sets.
- **Properties of Cartesian Product:**

  1. $A \times B \neq B \times A$
  2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
  3. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
  4. $A \times (B - C) = (A \times B) - (A \times C)$
  5. $(A \times B) \cap (C \times D) = (A \cap C) \times (C \cap D)$
  6. $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$

- The representation of a relation in set builder form is complete only when the sets A and B are clearly specified.
- A relation R on A is called **reflexive,** if $\forall x \in A\ (x, x) \in R$ i.e. $\forall x \in A, xRx$
- A relation R in A is called symmetric relation iff $(x, y) \in R \Rightarrow (y, x) \in R$ i.e., $xRy \Rightarrow yRx\ \forall x, y \in A$
- A relation R on A is called **anti symmetric** iff $xRy \Rightarrow y\not{R}x$, unless $x = y$
- A relation R on A is called transitive iff $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$ i.e., xRy and $yRz \Rightarrow xRz \quad \forall x, y, z \in A$
- A relation R on A is called **irreflexive** iff $\forall x \in A, (x, x) \notin R$. i.e. $\forall x \in A,\ x\not{R}x$
- A relation R on A is an **asymmetric** relation iff $(x, y) \in R \Rightarrow (y, x) \notin R \quad xRy \Rightarrow y\not{R}x$.
- A relation R on a non empty set A is called equivalence relation iff
  (a) R is reflexive i.e $xRx\ \forall x \in A$
  (b) R is symmetric i.e $xRy = yRx$
  (c) R is transitive i.e xRy and $yRz \Rightarrow xRz \quad \forall x, y, z \in A$
- A relation R on a non empty set A is called a partial order relation iff.
  (a) R is reflexive $\forall x \in A, xRx$
  (b) R is antisymmetric xRy and $yRx \Rightarrow x = y$
  (c) R is transitive xRy and $yRz \Rightarrow xRz$
- Every quotient set A/R is also a partition of A. Here, the converse is also true.
- Corresponding to every partition P of A, there exists an unique equivalence relation whose quotient set is exactly P.
- A **function or mapping** is a relation between the elements of A and those of B having no ordered pairs with the same first component.
- If in a group G, the underlying set G consists of a finite number of elements, then the group is called finite group, otherwise as infinite group.
- **Properties of Cyclic Group:**

  1. Every cyclic group is an abelian group.
  2. If a is generator of a cyclic group G, then a^{-1} is also a generator of G.
  3. A cyclic group G with generator a of finite order n, is isomorphic to multiplicative group of n, n^{th} roots of unity.

4. A cyclic group G with a generator of finite order n is isomorphic to the additive group of residue classes modulo n.
5. If a finite group of order n contains element of order n, the group must be cyclic.
6. Every group of prime order is cyclic.
7. Every subgroup of a cyclic group is cyclic.

- Every finite group G is isomorphic to a permutation group.
- A subgroup H of a group G is said to be a **normal subgroup** of G iff $aH = Ha\ \forall a \in G$ (Where aH and Ha are the left and right cosets of H in G).
- A poset $(P, \leq)$ in which every pair of element $a, b \in P$ are comparable (i.e. either $a \leq b$ or $b \leq a$) is called a toset (totally ordered set) or a chain. Example $(Z, \leq)$ is a toset.
- Although, there may be many upper & lower bounds for a given subset S of a poset, there can be only one LUB and one GLB of S. i.e. LUB (or Sup (S)) & GLB (or Inf (S)) of S in unique.

Student's Assignment

Q.1 An equivalence relation is a relation which is
(a) Reflexive and symmetric
(b) Symmetric and Transitive
(c) Reflexive, Symmetric and transitive
(d) None of the above

Q.2 A function $f: N \rightarrow N$ defined by $f(n) = 2n + 3$ is
(a) Surjective
(b) Injective
(c) Both
(d) Non injective

Q.3 Let L be the set of lines in the Euclidean plane. Let R be the relation on L defined by "is parallel to". Then which of the following is true?
(a) R is an equivalence relation
(b) R is POSET
(c) R is reflexive symmetric
(d) None of the above

Q.4 If a lattice is distributive, then
(a) $a * (b \cdot c) = (a \cdot b) * (b \cdot c)$
(b) $a \cdot (b * c) = (a \cdot b) * (a \cdot c)$
(c) $a * (b * c) = (a * b) \cdot (a * c)$
(d) None of these

Q.5 Let A and B be sets with cardinalities 2 and 4 respectively. The number of one-one mapping from A to B is
(a) 4^2
(b) ${}^4P_2$
(c) 4!
(d) 1

Q.6 Match **List-I** with **List-II** and select the correct answer using the codes given below the lists:

List-I	List-II
A. Identity	1. Monoids
B. Associativity	2. Abelian groups
C. Commutative	3. Semi groups
D. Left inverse	4. Groups

Codes:

	A	B	C	D
(a)	1	3	2	4
(b)	1	2	3	4
(c)	4	3	1	2
(d)	2	3	4	1

Q.7 Given set S = {1, 5, 7, 11}. Then S is a group w.r.t.
(a) multiplication modulo 12
(b) addition modulo 6
(c) summation modulo 8
(d) S is not a group

Q.8 Let P and Q be any two equivalence relations on a non-empty set S, then choose the correct one
(a) $P \cup Q, P \cap Q$, are both equivalence relations
(b) $P \cup Q$ is an equivalence relation
(c) $P \cap Q$ is an equivalence relation
(d) Neither $P \cup Q$ nor $P \cap Q$ is an equivalence relation

Q.9 Consider the following binary relation

$s = \{(x, y) \mid y = x + 1$ and
$x, y \in \{0, 1, 2, ...\}\}$

The symmetric closure of S is

(a) $\{(x, y) \mid x = y + 1$ and $x, y \in \{0, 1, 2, ...\}\}$
(b) $\{(x, y) \mid y = x + 1$ and $x, y \in \{0, 1, 2, ...\}\}$
(c) $\{(x, y) \mid y = x \pm 1$ and $x, y \in \{0, 1, 2, ...\}\}$
(d) None of the above

Q.10 Which of the following statements is not true?

(a) If z is the set of integers and $\leq$ is the usual ordering on z, then $[z; \leq]$ is partially ordered and totally ordered.
(b) If z is the set of integers and $\leq$ is the usual ordering on z, then $[z; \leq]$ is partially ordered but not totally ordered
(c) U be an arbitrary set and A = P (U) be the collection of all subsets of U. Then $[P(U); \subseteq]$ is a poset.
(d) If U contains more than one element then it is not totally ordered.

Q.11 Consider the following relation:

$\{(a, a), (a, b), (a, c)\} \subseteq \{a, b, c\} \times \{a, b, c\}$

Which of the following statement is true about the above relation

(a) It is not a function
(b) It is a function which is not one-to-one or onto
(c) It is a function which is one-to-one but not onto
(d) It is a function which is both one-to-one and onto

Q.12 N denotes the set of natural numbers, $\{0, 1, 2, ...3)$. Z denotes the integers, $\{..., -2, -1, 0, 1, 2, ...\}$ which of the following statements are true?

(*i*) For all $p \in Z$, $p > 5 \rightarrow$ There exists $x \in N$, $x^2 \equiv 1(\text{mod} p)$
(*ii*) If m is any natural number satisfying $m \equiv 1(\text{mod}2)$, then the equation $2048 \times \equiv 1(\text{mod}m)$ is guaranteed to have a solution for x.

(a) Only (*i*) is true
(b) Only (*ii*) is true
(c) Both (*i*) and (*ii*) are true
(d) Both (*i*) and (*ii*) are false

Q.13 If $|A| = k$ and $|B| = m$, how many relation are between A and B? If in addition $|C| = n$ how many relations are there between there in $A \times B \times C$?

(a) $k + m$ and $k + m + n$
(b) $k \times m$ and $k \times m \times n$
(c) 2^{k+m} and 2^{k+m+n}
(d) 2^{km} and 2^{kmn}

Q.14 (G, $*$) is an abelian group. Then

(a) $X = X^{-1}$, for any X belonging to G
(b) $X = X^2$, for any X belonging to G
(c) $(X * Y)^2 = X^2 * Y^2$, for any X, Y belonging to G
(d) G is of finite order

Q.15 Enumerate each of the following sets

(*i*) $\phi \times \{3, 5, 9\}$
(*ii*) 2^{ϕ}
(*iii*) $2^{\{3, 5, 9\}}$

(a) $\phi, \{\phi\}, \{\phi, \{3\}, \{5\}, \{9\}, \{3,5\}, \{5,9\}, \{3,9\}, \{3,5,9\}\}$
(b) $\{\phi\}, \phi, \{\phi, \{3\}, \{5\}, \{9\}, \{3,5\}, \{5,9\}, \{3,9\}, \{3,5,9\}\}$
(c) $\{\phi\}, \phi, \{\phi, \{3\}, \{5\}, \{9\}, \{5,9\}, \{3,9\}, \{3,5,9\}\}$
(d) None of these

Q.16 Let $R \subseteq A \times A$ and $S \subseteq A \times A$ be a binary relations as defined below:

Let A be the set of positive integers. And
$R = \{(a, b) \mid b$ is divisible by $a\}$.
Let $A \equiv N \times N$ and $S = \{((a, b), (c, d)) \mid a \leq c$ or $b \leq d\}$.

Which of the following statements are true?

(a) R is partial order but not total order and S is partial order but not a total order
(b) R is both partial order and total order and S is neither partial order nor a total order
(c) R is partial order but not total order and S is neither partial order nor a total order
(d) R is neither partial order nor a total order and S is neither partial order nor a total order

Q.17 N denotes the set of natural numbers, $\{0, 1, 2, ...\}$. Z denotes the integers, $\{....., -2, -1, 0, 1, 2, ...?$

which of the following statements are true?

(*i*) $\forall w \in z, \exists x \in z, \forall y \in z, \exists z \in z$, such that $w + x = y + z$
(*ii*) $\exists x \in N, \forall p \in z, p > 5 \rightarrow x^2 \equiv 1(\text{mod } p)$

(a) Only (*i*) is true
(b) Only (*ii*) is true
(c) Both (*i*) and (*ii*) are true
(d) Both (*i*) and (*ii*) are false

Q.18 Let $R \subset A \times A$ and $S \subset B \times B$ be binary relations as defined below:

Let $A = N$ and $R = \{(a, b) \mid b = a \text{ or } b = a + 1\}$

Let B be the set of English words. and let $(a, b) \in S$ when a is not longer than b.

(a) R is partial order but not total order and S is partial order but not a total order.
(b) R is both partial order and total order and S is neither partial order nor a total order.
(c) R is partial order but not total order and S is neither partial order nor a total order.
(d) R is neither partial order nor a total order and S is neither partial order nor a total order.

Q.19 Which of the following statements are true?

(*i*) Let $\Sigma_1 = \{a, b\}$ and $\Sigma_2 = \{0, 1, 2\}$ be disjoint alphabets.
Let $\Sigma_1{}^*$ be the set of (finite-length) strings over S_1 and let $\Sigma_2{}^*$ be the set of (finite-length) strings over S_2.
We can show that card $(\Sigma_1{}^*) =$ card $(\Sigma_2{}^*)$

(*ii*) Let $S = \{2^i \mid i \in N\}$ be the set of integers that are powers of two. We can show that S. is uncountable.

(a) Only (*i*) is true
(b) Only (ii) is true
(c) Both (*i*) and (*ii*) are true
(d) Both (*i*) and (*ii*) are false

Q.20 Each of the following defines a relation on the set N of positive integers. Determine which of the following relations are reflexive.

(a) $R : x$ is greater than y
(b) $S : x + y = 10$
(c) $T : x + 4y = 10$
(d) None of the above

Q.21 Which of the following are symmetric

(a) $R : x$ is greater than y
(b) $S : x + y = 10$
(c) $T : x + 4y = 10$
(d) None of the above

Q.22 Let P(X) be the collection of all subsets of a set X with atleast three elements. Each of the following defines a relation on P(X):

$R : A \subseteq B$
$S :$ A is disjoint from B
$T : A \cup B = X$

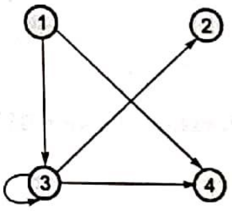
Determine which of the following relation is antisymmetric.

(a) $R : A \subseteq B$
(b) $S :$ A is disjoint from B
(c) $T : A \cup B = X$
(d) None of the above

Q.23 Determine which of the following relation is transitive

(a) $R : A \subseteq B$
(b) $S :$ A is disjoint from B
(c) $T : A \cup B = X$
(d) None of the above

Q.24 Find the transitive closure R* of the relation R on $A = \{1, 2, 3, 4\}$ defined by the directed graph



(a) $R^* = \{(1,2), (2,3), (1,3), (1,4), (3,2) (3,3), (3,4)\}$
(b) $R^* = \{(1,2), (1,3), (1,4), (3,2), (3,3), (3,4)\}$
(c) $R^* = \{(1,1), (2,2), (3,3), (4,4)\}$
(d) None of the above

Q.25 Let $S = \{1, 2, 3, 4, 5, 6\}$. Determine which of the following is a partition of S:

(a) $P_1 = [\{1,2,3\}, \{1,4,5,6\}]$
(b) $P_2 = [\{1,2\}, \{3,5,6\}]$
(c) $P_3 = [\{1,3,5\}, \{2,4\}, \{6\}]$
(d) $P_4 = [\{1,3,5\}, \{2,4,6,7\}]$

Q.26 Let $X = \{1, 2, ..., 8, 9\}$

Determine whether each of the following is a partition of X

(*i*) $[\{1,3,6\}, \{2,8\}, \{5,7,9\}]$
(*ii*) $[\{1,5,7\}, \{2,4,8,9\}, \{3,5,6\}]$
(*iii*) $[\{2,4,5,8\}, \{1,9\}, \{3,6,7\}]$
(*iv*) $[\{1,2,7\}, \{3,5\}, \{4,6,8,9\}, \{3,5\}]$

(a) (*i*) and (*ii*)
(b) (*ii*) and (*iii*)
(c) (*iii*) and (*iv*)
(d) (*iv*) and (*i*)

Q.27 Let A be set of integers and let ~ be the relation on A × A defined by

$$(a, b) \sim (c, d) \text{ iff } a + d = b + c$$

This relation satisfies

(a) Reflexive, symmetric
(b) Symmetric, transitive
(c) Reflexive, symmetric and transitive
(d) None of above

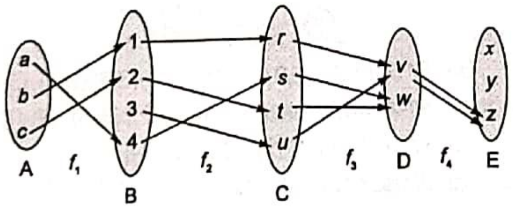
Q.28 The relation R = {(1,1), (1,2), (2,1), (2,2), (3,3)} is an equivalence relation of the set S = {1, 2, 3}. Find the quotient S/R

(a) {[2]}
(b) {[1], [2]}
(c) {[1]}
(d) {[1], [3]}

Q.29 Determine which of the following is a partition of the set R of real numbers.

(a) $[\{x : x > 4\}, \{x : x < 5\}]$
(b) $[\{x : x > 0\}, \{0\}, \{x : x < 0\}]$
(c) $[\{x : x^2 > 11\}, \{x : x^2 < 11\}]$
(d) None of the above

Common Data Questions (30 and 31):



Functions $f_1 : A \rightarrow B$, $f_2 : B \rightarrow C$, $f_3 : C \rightarrow D$ and $f_4 : D \rightarrow E$,

Q.30 Which of the functions are one-to-one

(a) f_1 and f_2
(b) f_2 and f_3
(c) f_3 and f_4
(d) f_4 and f_1

Q.31 Which of the following functions are onto functions

(a) f_1 and f_2
(b) f_2 and f_3
(c) f_3 and f_4
(d) f_4 and f_1

Q.32 Which of the following functions are invertible

(a) f_1
(b) f_2
(c) f_3
(d) f_4

Q.33 Let R be a binary relation on the set of all positive integers such that

R = {(*a*, *b*) | *a* − *b* is an odd positive integer}

Thus R is

(a) anti-symmetric relation
(b) reflexive and symmetric relation
(c) equivalence relation
(d) partial ordering relation

Q.34 A ∪ B = A ∩ B if and only if

(a) A is empty set
(b) B is empty set
(c) A and B are non-empty sets
(d) A = B

Q.35 Let A and B be sets with cardinalities *m* and *n*. The number of one-one mappings from A to B, when $m < n$ is

(a) m^n
(b) ${}^nP_m$
(c) ${}^mC_n$
(d) ${}^nC_m$

Q.36 Which additional properties are true if a partial order "≤" must become a linear order

(*i*) for any *a* and *b* is S, atleast one of $a \leq b$ (or) $b \leq a$ is true.

(*ii*) for all *a*, *b* and *c* in S, if $a \leq b$ and $b \leq c$, then $a \leq c$.

(*iii*) for any *a* and *b* in S, exactly one of $a \leq b$, (or) $b \leq a$ is true.

(a) Only (*i*)
(b) Both (*ii*) and (*iii*)
(c) Only (*iii*)
(d) All of the above

Q.37 Suppose A = { }, B = {1, 2, 3}. What does the set B × A contain?

(a) { }
(b) {1, 2, 3}
(c) {(1), (2), (3)}
(d) None of these

Q.38 Consider a binary relation R shown in the following matrix on set

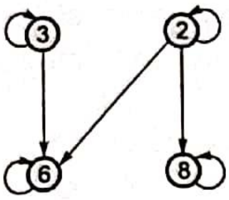
S = {1, 2, 3, 4}.

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

The relation R is

(a) Equivalence relation
(b) Irreflexive and antisymmetric
(c) Irreflexive, symmetric and transitive
(d) Transitive but neither reflexive nor irreflexive

Q.39 Following figure shows relation on set S = {2, 3, 6, 8}.



The relation is
(a) Equivalence relation
(b) Poset (partial order relation)
(c) Symmetric and reflexive relation
(d) None of the above

Common Data Questions (40 and 41):

Let X = {1, 2, 3, 4} if
$R = \{<x, y> | x \in X; y \in X; |x-y| > 0; |x-y| \%2 = 0\}$
$S = \{<x, y> | x \in X; y \in X; |x-y| > 0; |x-y| \%3 = 0\}$

Q.40 Find $|R \cup S|$ and $|R \cap S|$
(a) $|R \cup S| = 6$, $|R \cap S| = 0$
(b) $|R \cup S| = 3$, $|R \cap S| = 6$
(c) $|R \cup S| = 2$, $|R \cap S| = 2$
(d) $|R \cup S| = 5$, $|R \cap S| = 3$

Q.41 If X = {1, 2, 3 ....}, what is R ∩ S?

(a) $R = \begin{Bmatrix} <x,y> | x \in X; y \in X; (x-y) > 0; \\ (x-y)\%2 = 0 \text{ or } (x-y)\%3 = 0 \end{Bmatrix}$

(b) $R = \{<x, y> | x \in X; y \in X; (x-y) > 0; (x-y)\% 6 = 0\}$
(c) $R = \{<x, y> | x \in X; y \in X; (x-y) > 0; (x-y)\% 5 = 0\}$
(d) None of the above

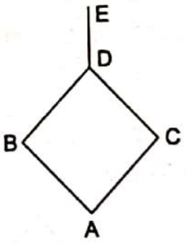
Q.42 An empty relation f is
(a) symmetric but reflexive
(b) equivalence relation
(c) partial order
(d) None of the above

Q.43 Let A be the set of non-zero integers and let # be the relation on A × A defined as (a, b) # (c, d) iff ad = bc. The relation A is
(a) Equivalence relation
(b) Poset
(c) Antisymmetric
(d) Reflexive and symmetric but not transitive

Q.44 Which of the following statements is true about B = {D, {A}}
(a) A ∈ B
(b) {A} ∈ B
(c) {A} ⊆ B
(d) {D, A} ∈ pow (B)

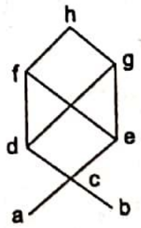
Q.45 $R : A \to B$.
A_1 is subset of A and A_2 is also a subset of A. Which of the following statements is not correct?
(a) $R(A_1 \cup A_2) \subseteq R(A_1) \cup R(A_2)$
(b) $R(A_1 \cap A_2) \subseteq R(A_1) \cap R(A_2)$
(c) $R(A_1) \cup R(A_2) \subseteq R(A_1 \cup A_2)$
(d) $R(A_1) \cap R(A_2) \subseteq R(A_1 \cap A_2)$

Q.46 Consider the following figure which of the following is true?



(a) There exists a Euler path but not Euler circuit
(b) There exists a Euler circuit
(c) Euler path is not possible
(d) None of the above

Q.47 Consider the poset A = {a, b, c, d, e, f, g, h}. The Hasse diagram is given below.



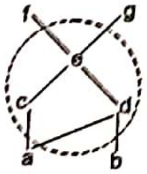
Find the lower and upper bound for B = {a, b} respectively.

(a) {a, b} and {c}
(b) {a, b} and {f}
(c) {} and {c, d, e, f, g, h}
(d) {} and {c}

Q.48 With respect to previous question, the lower and upper bound for B_1 = {*c, d, e*} respectively are
(a) {*a, b*} and {*h*} (b) {*c*} and {*h*}
(c) {*c, a, b*} and {*h*} (d) {*c, a, b*} and {*f, g, h*}

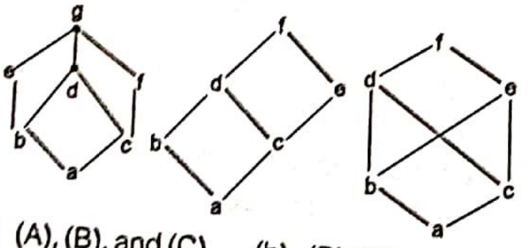
Q.49 What is the cardinality of a multiset having letters "MI SSI SSI PPI"?
(a) 4 (b) 11
(c) 3 (d) 6

Q.50 Let V = {a, b, c, d, e, f, g} be a partially ordered set as shown in figure and let X = {c, d, e}. Find the upper and lower bounds of *x*.



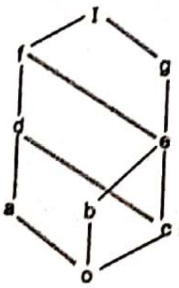
(a) Upper bounds-e,f, and g, lower bound-a
(b) Upper bounds-d, e, and f, lower bound b
(c) Upper bounds-c, d, and e, lower bound-a
(d) None of the above

Q.51 Identify which of the partially ordered sets shown in the figure are lattices



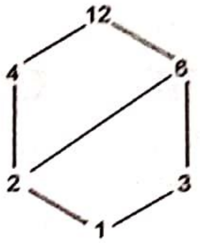
(a) (A), (B), and (C) (b) (B), (C)
(c) (C), (A) (d) (A), (B)

Q.52 Find the join- irreducible elements of the lattice *k* shown in figure.



(a) a, b, c, d (b) b, c, d, g
(c) a, b, c, g (d) b, c, g, e

Q.53 Consider the lattice D_{12} = {1, 2, 3, 4, 6, 12}, the divisors of 12 ordered by divisibility as shown in figure. Find
1. Lower bound and upper bound of D_{12}
2. The complements of 4 and 6
3. Is D_{12} a complemented lattice?



(a) 1. low bound is 2 and upper bound is 12
2. complement of 4 is 3, 6 has no complement
3. NO
(b) 1. L. B. is 1 and U. B. is 12
2. complement of 4 is 3, 6 has no complement
3. NO
(c) 1. L. B. is 1 and U. B. is 12
2. complement 4 is 3. complement of 6 is 3
3. YES
(d) 1. L. B. is 1 and U. B. is 12
2. 4 has no complement, complement of 6 is 3
3. YES

Q.54 Which of the following statements are true?
(*i*) If *x* is positive and irrational, then $\sqrt{x}$ is also irrational.
(*ii*) Let {0, 1}* denote the set of all binary strings $y.z$ denotes the concatenation of two strings *y* and *z*.
Every string X ∈ {0, 1}* can be written in the from $x = y.z$ where the number of 0' *s* in *y* is the same as the number of 1's in *z*. (Empty strings are allowed).
(a) Only (*i*) is true
(b) Only (*ii*) is true
(c) Both (*i*) and (*ii*) are true
(d) Both (*i*) and (*ii*) are true

Q.55 Set A has 4 elements and Set B has 2 elements. What is the total number of relations from B to A?

Q.56 Set S has '9' elements. Suppose you where asked to find the number of Irreflexive relations possible from set S to itself, what would be your answer.

Q.57 Set S has '6' elements, what is the total number of reflexive relations possible from set S to itself?

Q.58 What is the total number of asymmetric relations from Set A to itself which has '*n*' elements?

Answer Key:

1. (c)	**2.** (b)	**3.** (a)	**4.** (b)	**5.** (b)
6. (a)	**7.** (a)	**8.** (c)	**9.** (c)	**10.** (b)
11. (a)	**12.** (c)	**13.** (d)	**14.** (c)	**15.** (a)
16. (c)	**17.** (c)	**18.** (d)	**19.** (a)	**20.** (d)
21. (b)	**22.** (a)	**23.** (a)	**24.** (b)	**25.** (c)
26. (c)	**27.** (c)	**28.** (d)	**29.** (b)	**30.** (a)
31. (b)	**32.** (b)	**33.** (a)	**34.** (d)	**35.** (b)
36. (a)	**37.** (a)	**38.** (d)	**39.** (b)	**40.** (a)
41. (b)	**42.** (d)	**43.** (a)	**44.** (b)	**45.** (d)
46. (a)	**47.** (c)	**48.** (d)	**49.** (b)	**50.** (a)
51. (d)	**52.** (c)	**53.** (b)	**54.** (c)	**55.** 256
56. 2^{72}	**57.** 2^{30}	**58.** $3^{\frac{n^2-n}{2}}$		

Student's Assignments Explanations

1. (c)
A relation R on a set A is called an equivalence relation if it is reflexive, symmetric, and transitive.

2. (b)

$$f(n) = 2n + 3$$

Now, $f(x_1) = f(x_2)$

$\Rightarrow \quad 2x_1 + 3 = 2x_2 + 3$

$\Rightarrow \quad x_1 = x_2$

$\therefore$ $f(n)$ is one-to-one, i.e. injective.

To check for onto, write the function as

$$y = 2x + 3$$

$$\Rightarrow \quad x = \frac{y-3}{2}$$

Here, $y = 4 \in \text{N}$ but $x = \frac{4-3}{2} = \frac{1}{2} \notin \text{N}$

$\therefore$ f is not onto, i.e. not surjective

7. (a)
The composition table (Cayley table) of S w.r.t. multiplication module 12 is

X_{12}	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

8. (c)
PUQ may not be transitive.

9. (c)
Let us take some samples which satisfy the given binary relation. They are {(0,1), (1, 2), (2, 3), ...}
The symmetric closure of this is
{(0,1), (1, 0), (1,2), (2,1), (2,3), (3,2), ...}
The above samples satisfy the equation
$\{(x, y) \mid y = x \pm 1$ and $x, y \in \{0, 1, 2, —\}\}$
completely

11. (a)
It is not a function, since (a, b) and (a, c) are in the relation.

12. (c)
Consider A. Since, $I^2 \equiv 1 \text{ mod } (p)$ always,
$\therefore$ $\exists x \in \text{N}$ such that $x^2 \equiv 1 \text{ mod } (p)$, A is true.
Consider B. Since $\text{m} \equiv 1 \text{ (mod 2)}$, this means m is a odd number.
This means 2048 and m are relatively prime.
The equation, $ax \equiv b \text{ (mod } m)$ has a solution whenever a ad m are relatively prime.
$\therefore$ The equation $2048x \equiv 1(\text{mod } m)$ is guaranted to have a solution for x, since 2048 and m are relatively prime.
So B is also true.

13. (d)

The number of binary relations between A and B is the number of subsets of A × B.

Similarly, the number of 3-ary relations between A and B and C is the number of subsets of $A \times B \times C$.

The answers are therefore $2^{k \times m}$ and $2^{k \times m \times n}$

14. (c)

$$\begin{aligned}(x * y)^2 = (x * y)*(x * y) &= (x * (y * x) * y)\\ &= (x * (x * y) * y)\\ \text{(since (G, *) is abelian)} &= ((x * x) * (y * y))\\ &= (x^2 * y^2)\\ &= x^2 * y^2\end{aligned}$$

16. (c)

R : {(a, b) | b is divisible by A} on A × A

S : {((a, b), (c, d)) | $a \leq c$ or $b \leq d$ on A × A where

A = z^+

R is reflexive, antisymmetric and transitive and hence is a partial order.

R is not a total order, as can be seen by a counter example such as 3 ∈ A, 5 ∈ A. Here, 3 does not divide 5 ad 5 does not divide 3.

i.e. 3 R 5 and 5/3.

∴ 3 and 5 are not comparable.

R is therefore not a total order.

Consider the relation S.

S is neither a partial order nor total order since S is not antisymmetric and it is not transitive.

S is not antisymmetric since (1, 2) S(4, 1) and (4, 1) S(1, 2) but (1, 2) ≠ (4, 1)

S is not transitive since (4, 8) S (8, 4) and (8, 4) S(3, 6) but (4, 8) S (3, 6).

18. (d)

R is neither partial order nor a total order, because R is not transitive. This can be seen from the following counter example

$$\begin{aligned} &(1, 2) \in R\\ &(2, 3) \in R\\ \text{but}\quad &(1, 3) \notin R\end{aligned}$$

S is neither partial order nor a total order, because *s* is not antisymmetric, this can be seen from the two distinct english words fox and cat. Both (fox, cat) ∈ S and (cat, fox) ∈ S, since both words have the same length, but fox ≠ cat.

19. (d)

Consider statement (*i*)

Since we cannot set up a one-to-one correspondence from $\Sigma*$ to Σ_2*, we cannot show that $|\Sigma_1^*| = |\Sigma_2^*|$. Therefore, (*i*) is false.

Consider (*ii*).

Since $f(i) = 2^i$ is a one-to-one correspondence from the set N to the set S, and since N is countable so is S.

∴ Statement (*ii*) is also false.

20. (d)

None of these are reflexive, since (1, 1) does not belong R, S or T.

21. (b)

R is not symmetric since $x > y \nRightarrow y > x$

S is symmetric since $x + y = 10 \Rightarrow y + x = 10$

T is not symmetric since $x + 4y = 10 \nRightarrow y + 4x = 10$

22. (a)

Since $A \subseteq B$ and $B \supseteq A \Rightarrow A = B$

∴ R is antisymmetric.

Since

A is disjoint from B and B is disjoint from A

$\nRightarrow$ A = B

∴ S is not antisymmetric

Since $A \cup B = X$ and $B \cup A = X \nRightarrow A = B$

∴ T is not antisymmetric.

23. (a)

Since $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$

∴ R is transitive.

Consider the velation S : A is disjoint from B let A = {1, 2, 3} B = {a, b} C = {2, 3, 5}

Here $A \cap B = \phi$, $B \cap C = \phi$ but $A \cap C \neq \phi$

∴ A is disjoint from B and B disjoint from C

$\nRightarrow$ A disjoint from C

S is therefore, not transitive.

Consider the velation T : $A \cup B = X$

Let A = {1, 2, 3}, B = {4}, C = {1, 2, 3} and X = {1, 2, 3, 4}

clearly, $A \cap B = X$ and $B \cap C = X$ but $A \cap C \neq X$

∴ T is not transitive.

24. (b)

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

$(1, 3) \in R$ and $(3, 2) \in R \Rightarrow (1, 2) \in R*$

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

All the elements are now transitive in R*.

25. (c)

P_1 is not partition since $1 \in S$ elong to two cells.

P_2 is not partition since $4 \in S$ does not belong to any cell.

P_3 is a partition of S.

P_4 is not partition sice $\{2, 4, 6, 7\}$ is not a subset of S.

26. (c)

Part (c) because each element of X belongs to exactly one cell. In other words the cells are disjoint and their union is X.

27. (c)

$(a, b) \sim (c, d)$ iff $a + d = b + c$

Reflexive Property

Since $a + b = b + a$, $(a, b) \sim (a, b)$

$\therefore \sim$ is reflexive.

Symmetry Property

Let $(a, b) \sim (c, d)$

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

$\Rightarrow (c, d) \sim (a, b)$

$\therefore (a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$

$\sim$ is symmetric.

Transitive property

Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$

$\Rightarrow a + d = b + c$ and $c + f = d + e$

Adding then two equation we get

$a + d + c + f = b + c + d + e$

$\Rightarrow a + f = b + e \Rightarrow (a, b) \sim (e, f)$

$\therefore (a, b) \sim (c, d)\ \&\ (c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f)$

$\sim$ is transitive.

28. (d)

Under the relation R, $[1] = \{1, 2\}$, $[2] = \{1,2\}$ and $[3] = \{3\}$. Noting that $[1] = [2]$. We have SIR = $\{[1], [3]\}$

29. (b)

(a) No, since the two cells are not disjoint e.g. 4.5 belongs to both cells.

(b) Yes, since the three cells are mutually disjoint and their union is R.

(c) No, since $\sqrt{11}$ in R does not belong to either cell.

30. (a)

The function f_1 is one-to-one since no element of B is the image of more than one element of A. Similarly f_2 is one-to-one. However, neither f_3 nor f_4 is one-to-one since $f_3(r) = f_3(u) = v$ and $f_4(v) = f_4(w) = z$.

31. (b)

The functions f_2 and f_3 are both onto function since every element of C is the image under f_2 of some element of B and every element of D is the image under f_3 of some element of C. i.e. $f_2(B) = C$ and $f_3(C) = D$. On the other hand, f_1 is not onto, since $3 \in S$ is not the image under f_1 of any element of A, and f_4 is not onto since $x \in S$ is not the image under f_4 of any element of D.

32. (b)

The function f_1 is one-to-one but not onto, f_3 is onto but not one-to-one and f_4 is neither one-to-one nor onto. However f_2 is both one-to-one and onto, i.e., f_2 is bijective function between A and B. Hence f_2 is invertible anf f_2^{-1} is a function from C to B.

33. (a)

R is equivalence relation if it is reflexive symmetric and transitive.

R is partial ordering relation if it is reflexive, antisymmetric and transitive.

as a-b odd positive integer, b-a is not odd positive hence antisymmetric a-b is odd positive, b-c is odd positive but (a-c) is even positive, hence not transitive.

$\therefore$ R is antisymmetric.

34. (d)

(*i*) If A is empty set then $A \cup B = B$ and $A \cap B = \phi$.

$\therefore A \cup B \neq A \cap B$

(*ii*) Same for if B is empty set.

(*iii*) Consider $A = \{1\}$ $B = \{2\}$ $A \cup B = \{1, 2\}$ and

$A \cap B = \phi$

$\therefore A \cup B \neq A \cap B$

(*iv*) is correct since if $A = B$,

$A \cup B = A \cup A = A$

and $A \cap B = A \cap A = A$

$\therefore A \cup B = A \cap B$

and conversely if $A \cup B = A \cap B$

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

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

$\therefore A = B$

$\therefore A \cup B = A \cap B$ iff $A = B$

35. (b)

The first element of A can be mapped in n different ways. The second element of A can be mapped only in $(n - 1)$ ways since function is one-to-one. and so on.

$\therefore$ Total number of one-to-one mappings from A to B is $n(n - 1)(n - 2) \ldots (n - m + 1) = np_m$.

37. (a)

Suppose $A = \{a, b\}$ and $B = \{1,2\}$, the set $B \times A$ will contain $\{(1, a), (1, b), (2, 1), (2, b)\}$.

However if either of set in relation, for instance, A or B in $B \times A$ is { }, the relation is also an empty set i.e. { }. Thus, $B \times A = \{\} = \phi$

38. (d)

One could see from the matrix for R that

- All entires in the diagonal are not 1, hence the matrix is not reflexive.
- All entires in the diagonal are not 0, hence the relation is also not irreflexive.
- The relation A is transitive since
  $(2, 3), (3, 1) \Rightarrow (2, 1)$
  $(3, 2), (2, 3) \Rightarrow (3, 3)$
  $(2, 3), (3, 2) \Rightarrow (2, 2)$
  $(3, 2), (2, 4) \Rightarrow (3, 4)$

$\therefore$ The answer is that the relation is transitive but neither reflexive nor irreflexive.

39. (b)

The relation is {<2, 2>, <3, 3>, <6, 6>, <8, 8>, <2, 8>, <2, 6>, <3, 6>}

We could see that

- The relation is reflexive as <2, 2>, <3, 3>, <6, 6>, and <8, 8> are present.
- The relation is not symmetric, since <2, 6> $\in$ R but <6, 2> $\notin$ R.
- The relation is antisymmetric, That means, the pair (x, y), (y, x) is present if and only if $x = y$. (i.e. all arrows are unidirectional except self loops).
- The relation is transitive.
  The relation is reflexive, antisymmetric and transitive that means, its is a partially ordered set or poset.

40. (a)

R = {<1, 3>, <3, 1>, <2, 4>, <4, 2>}

S = {<1, 4>, <4, 1>}

$R \cup S$ {<1, 3>, <3, 1>, <2, 4>, <4, 2>, <1, 4>, <4, 1>}

$R \cap S = \{\}$, $|R \cup S| = 6$, $|R \cup S| = 0$

42. (d)

f is not reflexive

f is symmetric, antisymmetric and transitive

43. (a)

Given (a, b) # (c, d) iff ad = bc

1. Since ab = ba, (a, b) # (a,b)
   $\therefore$ Relation # is reflexive
2. Let (a, b) # (c, d) $\Rightarrow$ ad = bc $\Rightarrow$ cb = da
   $\Rightarrow$ (c, d) # (a, b)
   $\therefore$ Relation # is symmetric
3. Let (a, b) # (c, d) & (c, d) # (e, f)
   $\Rightarrow$ ad = bc and cf = de
   $\Rightarrow$ adcf = bcde $\Rightarrow$ af = be (cancelling cd from both sides)
   Now since af = be $\Rightarrow$ (a, b) # (e, f)
   $\therefore$ We have how shown that
   (a, b) # (c, d) and (c, d) # (e, f) $\Rightarrow$ (a, b) # (e, f)
   $\therefore$ The relation # is transitive.
   $\therefore$ # is an equivalence relation.

45. (d)

1. Since $R(A_1 \cup A_2) = R(A_1) \cup R(A_2)$, statement (a) and (c) are correct

2. $R(A_1 \cap A_2) \subseteq R(A_1) \cap R(A_2)$ is true. So, statement (b) is correct.
Only statement (d) is false.

46. (a)
Since there are exactly 2 vertices (E and D) in this graph with odd degree, this graph has an euler path but not an euler circuit.

49. (b)
The multi-set

$$S = \{M * 1, I * 4, S * 4, P * 2\}$$
$$|S| = 11$$

50. (a)
The elements e, f and g succeed every element of x; hence e, f and g are the upper bounds of x. The element a precedes every elements of x; hence it is the lower bound of x. Note that b is not a lower bound since b does not precede c; b and c are not comparable.

51. (d)
An ordered set S is a lattice if and only if sup (x, y) and inf (x, y) exist for each pair (x, y) in S. Posets (A) and (B) of given figures are lattices. Poset (C) is not a lattice since (b, c) has three upper bounds d, e and f and no one of them precedes the other two (d, e being incomparable) hence sup (b, c) does not exist.

52. (c)
The join-irreducible elements of the lattice are those with a unique predecessor. Therefore join-irreducible elements are a, b, c and g.

53. (b)
1. Lower bound is 1 and upper bound is 12.
2. The complement of 4 is 3 since
   g.c.d (4, 3) = 1 (which is the least element) and *l*.c.m. (4, 3) = 12 (which is the greatest element).
   6 has no complement since there is no element x satisfying both gcd $(6, x) = 1$ and lcm$(6, x) = 12$.
3. D_{12} is not a complemented lattice, since 6 has no complement.
   (In a complementes lattice, every element must have at least one complement).

56. Solution:
2^{72} Irreflexive relations [**Hint:** Diagonal elements are fixed as 0].

57. Solution:
2^{30} reflexive relations [**Hint:** Diagonal elements are fixed as 1].

•■•■•■•