Set Theory & Algebra

3

Set

A set is an unordered collection of objects.

The objects in a set are called the elements, or members of the set.

- $\mathbb{N}$ be set of natural numbers : {1, 2, 3, ...}
- $\mathbb{Z}$ be set of integers : {..., –2, –1, 0, 1, 2,...}
- $\mathbb{Q}$ be set of rational numbers
- $\mathbb{R}$ be set of real numbers
- $\mathbb{C}$ be set of complex numbers

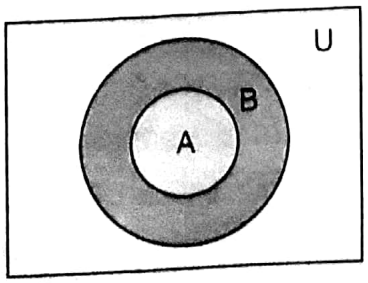
$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Types of Set

1. **Universal set U:** A set which contains all objects under consideration (the universal set varies depending on which objects are of interest)
2. **Equal sets:** Two sets are equal iff they have the same elements i.e., if A and B are sets, then A and B are equal iff $\forall x\ (x \in A \leftrightarrow x \in B)$; denoted by $A = B$.
3. **Equivalent sets:** Two sets A and B are equivalent if they have same number of elements. i.e. $|A| = |B|$.
4. **Empty set or Null set:** A special set that has no elements. Null set can be denoted by ϕ or $\{\}$.

   Example: The set of all positive integers that are greater than their squares is the null set.
5. **Singleton set:** A set with one element is called a singleton set.
6. **Subset:** The set A is said to be a subset of B iff every element of A is also an element of B. $A \subseteq B$ indicates that A is a subset of the set B.

   i.e. $A \subseteq B$ iff $x \in A \Rightarrow x \in B$



Venn Diagram Showing that A is a subset of B

Note:

- For every set S : $\phi \subseteq S$ and $S \subseteq S$

Comparable: If $A \subseteq B$ or $B \subseteq A$ then A and B are comparable.

7. **Proper subset:** A set A is a subset of the set B but also $A \neq B$, we write $A \subset B$ and say that A is a proper subset of B i.e. A is a proper subset of B iff $\forall x\,(x \in A \rightarrow x \in B) \wedge \exists x\,(x \in B \wedge x \notin A)$
8. **Finite set:** A set in which number of elements are finite and hence countable i.e., cardinality of set can be obtained as a number.
9. **Infinite set:** A set is said to be infinite if it is not finite.
   Example: The set of positive integer is infinite.
10. **Power Set:** The power set of a set S is the set of all subsets of the set S. The power set of S is denoted by $\mathcal{P}(S)$.

Note:

- If a set has n-elements, then its power set has 2^n elements.
- *Example:* Power set of the set {0, 1, 2} is
  $\mathcal{P}(\{0, 1, 2\}) = \{\phi, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$

Cartesian Product of Sets

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

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

Note:

- If $|A| = m$ and $|B| = n$ then $|A \times B| = mn$
- In general $A \times B \neq B \times A$ but $A \times B = B \times A$ iff $A = B$ or $A = \phi$ or $B = \phi$.
  However, $|A \times B| = |B \times A|$ always.

Set Operations

1. **Union:** The union of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both.

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Example: The union of the sets {1, 3, 5} and {1, 2, 3} is : {1, 2, 3, 5}

Remember:

- $\text{Max}(|A|, |B|) \le |A \cup B| \le (|A| + |B|)$
- $|A \cup B| = |A| + |B| - |A \cap B|$

2. **Intersection:** The intersection of the sets A and B, denoted by $A \cap B$, is the set containing those elements in both A and B.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

3. **Disjoint:** Two sets are called disjoint if their intersection is the empty set.
4. **Difference:** The difference of A and B, denoted by $A - B$, is the set containing those elements that are in A but not in B.

The difference of A and B is also called the complement of B with respect to A or the relative complement of B in A.

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Inclusion Exclusion Principle

$$n(A_1 \cup A_2 \cup \ldots \cup A_n) = \sum_{1 \le i \le n} n(A_i) - \sum_{1 \le i < j \le n} n(A_i \cap A_j) +$$

$$\sum_{1 \le i < j < k \le n} n(A_i \cap A_j \cap A_k) - \ldots + (-1)^{n-1} n(A_1 \cap A_2 \cap \ldots \cap A_n)$$

Properties of Sets

Let A, B and C are sets, U is universal set and ϕ is an empty set.

Identity	Name
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative Laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative Laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive Laws
$A \cup \phi = A$ $A \cap U = A$	Identity Laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \phi$	Complement Laws
$A \cup A = A$ $A \cap A = A$	Idempotent Laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption Laws
$(\overline{A}) = A$	Double Complement Law
$A \cup U = U$ $A \cap \phi = \phi$	Domination Laws
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgans Laws

Multiset

A collection of objects in which an element can appear more than once is called a multiset.

Example: $\{a, a, b, b, b, c, c, c, c, c, d\} = \{2 \cdot a, 3 \cdot b, 5 \cdot c, 1 \cdot d\}$

Let $A = \{m_1 \cdot a_1, m_2 \cdot a_2, \ldots\ldots, m_k \cdot a_k\}$ where m_i = multiplicity of a_i

$B = \{n_1 \cdot a_1, n_2 \cdot a_2, \ldots\ldots, n_k \cdot a_k\}$ where n_i = multiplicity of a_i

Then $A \cup B$ = a multiset, in which multiplicity of a_i is max $\{m_i, n_i\}$

$A \cap B$ = a multiset, in which multiplicity of a_i is min $\{m_i, n_i\}$

$A + B$ = a multiset, in which multiplicity of a_i is $(m_i + n_i)$

$A - B$ = a multiset, in which multiplicity of

$$a_i = \begin{cases} m_i - n_i & \text{if} \quad m_i > n_i \\ 0 \quad , & \text{otherwise} \end{cases}$$

Functions

Definition

Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to each element of A.

We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f : A \to B$.

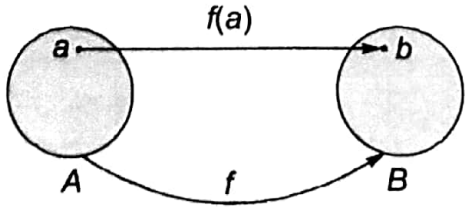
Note:

- Functions are sometimes also called mappings or transformations.

Domain and Codomain

If f is a function from A to B, we say that A is the domain of f and B is the codomain of f.

If $f(a) = b$, we say that "b is the image of a" and "a is the preimage of b".



The function f maps A to B.

- If number of elements $|A| = m$ and $|B| = n$, then number of functions possible from A to $B = n^m$.

- A function $f: A \to A$ is called a function on the set A.
  If $|A| = n$ then number of functions possible on $A = n^n$.

Types of Functions

1. **One-to-one function (Injection):** A function f is said to be one-to-one, or injective, iff $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.
   - If A and B are finite sets then a one-to-one from A to B is possible iff $|A| \le |B|$.
   - If $|A| = m$ and $|B| = n$ then $(m \le n)$ then number of one-to-one function from A to B is $P(n, m) = n(n-1)(n-2)\ldots\ldots (n-(m-1))$.
   - If $|A| = |B| = n$ then number of one-to-one functions from A to B is $P(n, n) = n(n-1)(n-2)\ldots\ldots 1 = n!$

2. **Onto Function (Surjection):** A function f from A to B is called onto, or surjective, iff for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$
   i.e. range(f) = co-domain(f) = B.
   - If A and B are finite sets then an onto function from A to B is possible only when $|B| \le |A|$.
   - If $|A| = |B|$ then every one-to-one function from $A \to B$ is onto and vice-versa.
   - If $|A| = |B| = n$ then number of onto functions possible from A to B $= n!$
   - If $|A| = m$ and $|B| = n\ (n < m)$ then number of onto functions from $A \to B = n^m - {}^nC_1(n-1)^m + {}^nC_2(n-2)^m \ldots + (-1)^{n-1}\,{}^nC_{n-1}(1^m)$.

3. **Bijection:** A function which is one-to-one and onto is called a bijection.
   If A, B are finite sets, then a bijection from A to B is possible only when $|A| = |B|$.
   - If $|A| = |B|$ then number of bijections = number of one-to-one = number of onto possible from A to $B = n!$

4. **Inverse Function:** Let f be a one-to-one correspondence from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$. The inverse function of f is denoted by f^{-1}. Hence, $f^{-1}(b) = a$ when $f(a) = b$. Inverse of function f exists iff f is a bijection.
5. **Identity function:** Identity function on A is denoted by I_A. Inverse of identity function is the function itself. Every identity function is bijection, if $f(a) = a;\ \forall a \in A$.

6. **Constant function:** A function $f: A \to B$ is said to be constant function if $f(x) = c; \forall x \in A$ i.e., all the elements of domain are mapped to only one element of codomain. Therefore the range of constant function contains only one element.

Function Composition

Let f and g are two functions defined on set A:

$(f \circ g) : A \to A$ defined by $(f \circ g)x = f(g(x))$

$(g \circ f) : A \to A$ defined by $(g \circ f)x = g(f(x))$

Note:

- In general $(f \circ g)x \neq (g \circ f)x$
- Let $f: A \to B$ and $g: B \to C$ then $(g \circ f) : A \to C$
  but $(f \circ g)$ may not be defined
  $(f \circ g)$ is defined if range of $g(x)$ is a subset of A.
- If $f: A \to A$ is a bijection then
  $f \circ f^{-1} = f^{-1} \circ f = I$ where I is identity function on A.
- If $f: A \to B$ is a bijection then $f \circ f^{-1} = I_B$, $f^{-1} \circ f = I_A$, $f^{-1} : B \to A$
- If $f: A \to B$ and $g: B \to C$ are injective (one-one) then $g \circ f: A \to C$ is also injective.
- If $f: A \to B$ and $g: B \to C$ are surjective (onto) then $g \circ f: A \to C$ is also surjective.
- If $f: A \to B$ and $g: B \to C$ are functions, and $g \circ f: A \to C$ is injective then f is also injective.
- If $f: A \to B$ and $g: B \to C$ are functions, and $g \circ f: A \to C$ is surjective then g is also surjective (onto)

Relation

Definition

Let A and B be two sets. Then a binary relation from A to B is a subset of $A \times B$.

Relations on a Set

A relation on the set A is a relation from $A \times A$ i.e., a relation on a set A is a subset of $A \times A$.

- If $|A| = m$ and $|B| = n$ then number of relations possible on $A = 2^{mn}$.
- If $|A| = n$ and $|B| = n$ then number of relations possible on $A = 2^{(n^2)}$.

Types of Relation

1. **Inverse Relation:** Let R be a relation from a set A to B. The inverse of R, denoted by R^{-1} is the relation from B to A which consists of those ordered pairs, which when reversed belongs to R i.e.,
   $R^{-1} = \{(b, a) | (a, b) \in R\}$
2. **Complementary Relation:** If R is a relation from A to B then
   $R^c = \bar{R} = \{(a, b) | (a, b) \notin R\} = (A \times B) - R$.
3. **Diagonal Relation:** A relation R on a set A is called diagonal relation or identity relation if $R = \{(a, a) | a \in A\} = \Delta_A$.
4. **Reflexive Relation:** A relation R on a set A is said to be reflexive if aRa $\forall a \in A$ i.e. $(a, a) \in R$, $\forall a \in A$.
   - If $|A| = n$ then number of reflexive relations possible on $A = 2^{n(n-1)}$.
   - A diagonal relation on a set A is reflexive and any superset of diagonal relation is also reflexive.
   - Smallest reflexive relation on $A = \Delta_A$ (diagonal relation)
   - Largest reflexive relation on $A = A \times A$.
5. **Irreflexive Relation:** A relation R on a set A is said to be irreflexive, if $a\not{R}a$ i.e., $(a, a) \notin R$, $\forall a \in A$.
   - If $|A| = n$ then number of irreflexive relations possible on $A = 2^{n(n-1)}$.
   - Smallest irreflexive relation on $A = \phi$
   - Largest irreflexive relation on $A = (A \times A) - \Delta_A$.
6. **Symmetric Relation:** A relation R on a set A, is said to be symmetric if aRb then bRa, $\forall a,b \in A$.
   - If $|A| = n$ then number of symmetric relations possible on
     $A = 2^n \times 2^{\frac{n^2-n}{2}} = 2^{n(n+1)/2}$.
   - Number of symmetric relations possible with only diagonal pairs $= 2^n$.
   - Number of symmetric relations possible with only non-diagonal pairs $= 2^{(n^2-n)/2}$.
   - Smallest symmetric relation on $A = \phi$
   - Largest symmetric relation on $A = A \times A$.
7. **Antisymmetric Relation:** A relation R on a set A is said to be antisymmetric, if aRb and bRa then $a = b$, $\forall a,b \in A$.

- Smallest antisymmetric relation is ϕ.
- Largest antisymmetric relation on A is not unique. Number of elements in largest antisymmetric relation includes all diagonal pairs and half of non-diagonal pairs.
  i.e., $n + (n^2 - n)/2$ elements $= (n^2 + n)/2$ elements.
- Any subset of antisymmetric relation is also antisymmetric relation.
- If $A = \{1, 2, \ldots, n\}$ then number of antisymmetric relations possible on $A = 2^n \times 3^{n(n-1)/2}$.
  With n diagonal pairs, 2^n choices.
  With $\frac{n(n-1)}{2}$ non-diagonal pairs. $3^{n(n-1)/2}$ choices.
- A relation R is antisymmetric iff $R \cap R^{-1} \subseteq \Delta_A$.

8. **Asymmetric Relation:** A relation R on a set A is called asymmetric, if $(b, a) \notin R$, whenever $(a, b) \in R$, $\forall a, b \in A$.
   - Relation R is asymmetric iff it is both antisymmetric and irreflexive.
   - If $A = \{1, 2, \ldots, n\}$ then number of asymmetric relations $= 3^{n(n-1)/2}$.

Note:
- Number of reflexive and symmetric relations with n-elements $= 2^{n(n-1)/2}$.
- Number of neither reflexive nor irreflexive relations $= 2^{n^2} - 2.2^{n(n-1)}$.
- ϕ is not reflexive [empty relation]

9. **Partial Ordering Relation:** A relation R on a set A is partial ordered if R is reflexive, antisymmetric and transitive.
   Poset: A set A with a partial ordered relation R defined on A is called a poset. Poset is partially ordered set.
   Totally ordered set: A poset $[A; R]$ is totally ordered set, if every pair of elements in A are comparable i.e., either aRb or bRa $\forall a, b \in A$.

Note:
- **A relation R on a set A is:**
  (*i*) Symmetric $\Leftrightarrow R = R^{-1}$
  (*ii*) Antisymmetric $\Leftrightarrow (R \cap R^{-1}) \subseteq \Delta_A$
  (*iii*) Reflexive $\Leftrightarrow R^{-1}$ is also reflexive
  (*iv*) Reflexive $\Leftrightarrow R^C$ or $\bar{R}$ is irreflexive

- If R and S are antisymmetric, then $(R \cap S)$ is also antisymmetric for any relation S on A.
- If R is antisymmetric then every subset of R is also antisymmetric.
- If R is relation on a set A then $R \cup R^{-1}$ is always symmetric and $R \cup \Delta$ is always reflexive.
- **If R and S on set A are any two:**
  - (i) Reflexive relations then $(R \cup S)$ and $(R \cap S)$ are also reflexive.
  - (ii) Symmetric relations then $(R \cup S)$ and $(R \cap S)$ are also symmetric
  - (iii) Antisymmetric relations the $(R \cap S)$ is always antisymmetric
  - (iv) Transitive relations then $(R \cap S)$ is always transitive.
  - (v) Equivalence relations then $(R \cap S)$ is always equivalence relation.

Closures of Relations

1. **Transitive Closure :** Transitive closure of $R = R^*$ = smallest transitive relation on set A which contains R.

   Example: Let $A = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 3)\}$.

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

2. **Reflexive Closure :** Reflexive closure of $R = R^+$ = smallest reflexive relation on set A which contains $R = (R \cup \Delta_A)$.

   Example: Let $A = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 3)\}$.

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

3. **Symmetric Closure :** Symmetric closure of $R = R^\#$ = smallest symmetric relation on set A which contains $R = (R \cup R^{-1})$

   Example: Let $A = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 3)\}$.

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

Partition of a Set

Let A be a set with 'n' elements dividing the set A into subsets $\{A_1, A_2, \ldots, A_n\}$ is called partition of A, if

- (i) every subset is a non-empty set and
- (ii) $\forall_{i,j}\ A_i \cap A_j = \phi$; $(i \neq j)$ and
- (iii) $(A_1 \cup A_2 \cup A_3 \cup \ldots \ldots \cup A_n) = A$.

Example: Let $A = \{1, 2, 3\}$. Then there are 5 partitions possible on A.

$P_1 = \{\{1, 2, 3\}\}$, $P_2 = \{\{1\}, \{2, 3\}\}$, $P_3 = \{\{2\}, \{1, 3\}\}$, $P_4 = \{\{3\}, \{1, 2\}\}$, and $P_5 = \{\{1\}, \{2\}, \{3\}\}$

Groups

Closure

Binary operator $*$ is said to be closed on a non-empty set A, if $a * b \in A$ for all $a, b \in A$

Number of binary operations on set 'G' = $|G|^{|G|\times|G|}$

Associativity

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

Identity

$\exists e \in G \forall a \in G$ $(a*e = e*a = a)$ where 'e' is identity

Note:

- If there exist an identity element in G then it must be unique.

Inverse

$\forall a \in G \exists b \in G$ $(a * b = b * a = e)$.

This also means $a^{-1} = b$ and $b^{-1} = a$

Commutative

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

Groupoid

An algebraic system $(G, *)$ is groupoid if it is closed operation on G.

Semigroup

An algebraic system which is groupoid and associative.

Monoid

An algebraic system $(G, *)$ which is semigroup and there is an identity in G.

Group

An algebraic system $(G, *)$ which is monoid and every element in G has inverse.

Abelian Group

An algebraic system $(G, *)$ which is a group and it is also commutative i.e., $a * b = b * a$; $\forall a, b \in G$.

Order of an Element of a Group

1. Let G be a group and let $g \in G$ be an element of G. Then the order of g is the smallest positive number k, such that $ak = e$.
2. Let G be a finite group and let $g \in G$. Then the order of g divides the order of G.
3. Any group of even order contains an element of order two.

Cyclic Group

- Let $G = \langle a \rangle$ be a cyclic group $G = \{a^i \mid i \in \mathbb{Z}\}$.
- Let G be a group. We say that G is cyclic if it is generated by one element.
- Let G be a cyclic group, generated by a. Then
  1. G is abelian
  2. If G is infinite, the elements of G are precisely
     $\ldots a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots$
  3. If G is finite, of order n, then the elements of G are precisely
     $e, a, a^2, \ldots, an^{-2}, an^{-1}$ and $an = e$.
  4. Let G be a group of prime order. Then G is cyclic.
  5. A finite group is cyclic iff there exists an element $g \in G$ whose order is same as the order of the group. Also such an element g will be the generator of that cyclic group.
  6. Let G be a finite cyclic group of order n, say $G = \langle g \rangle$. For every positive integer $d \mid n$ there is exactly one subgroup of G of order d. These are all the subgroups of G.
  7. Let G be a cyclic group. Every subgroup of G is cyclic.

Subgroup

- H is a subgroup of G iff
  (*i*) H is subset of G ($H \subseteq G$)
  (*ii*) Closure: $ab \in H$ for $a, b \in H$.
  (*iii*) Identity: The identity element of G is contained in H.
  (*iv*) Inverse: For all $a \in H$ we have $a^{-1} \in H$.
- Let G be a group and let H_i, $i \in I$ be a collection of subgroups of G. Then the intersection

$$H = \bigcap_{i \in I} H_i \text{, is a subgroup of } G.$$

- **Lagrange's theorem:** If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Coset

- **Left Coset:** Let G be a group H is subgroup of G. A right H-coset in G is a set of the form $aH := \{ah \mid h \in H\}$.
- **Right Coset:** Let G be a group H is subgroup of G. A right H-coset in G is a set of the form $Ha := \{ha \mid h \in H\}$.
- The number of distinct right cosets (equivalently left cosets) of G is called the index of H in G and is denoted $[G : H]$.
- A left coset of a subgroup $H < G$ is is a subset of G of the form $gH = (gh : h \in H)$.
- Two left cosets are either equal or disjoint; $gH = g'H \Leftrightarrow g^{-1}g' \in H$
- A right coset of H in H is a subset of the form $Hg = (hg : h \in H)$. Two right cosets are either equal or disjoint; we have $Hg = Hg' \Leftrightarrow g^{-1}g' \in H$.
- A coset is a left or right coset. Any element of a coset is called a representative of that coset.
- If H is finite, all cosets have cardinality $|H|$.
- There are equal number of left and right cosets in group G.

Group Theory Classification

Groupoid	Semigroup	Monoid	Group	Abelian
Closure	closure + Associative	closure + Associative + Identity	closure + Associative + Identity + Inverse	Group + Commutative
Example:	*Example:*	*Example:*	*Example:*	*Example:*
$(N, +, *)$ $(Z, +, -, *)$ $(R, +, -)$ $(R - \{0\}, *, /)$	$(N, +, *)$ $(Z, +, *)$ $(R, +)$ $(R - \{0\}, *)$ [– and ÷ are always not associative]	$(N, *)$ $(Z, +, \times)$ $(\{0, 1\}, \times)$ $(\{a, b\}^*, +)$	Non-singular matrices closed under '*' (multiplication)	$(\{0, 1, 2, 3\}, +_4)$ $(Z, +)$ $(R, +)$ $(R - \{0\}, *)$ $(Q, +)$ $(Q - \{0\}, *)$ $(\{1, -1, i, -i\}, *)$ $(\{1, \omega, \omega^2\}, *)$ $(\{1, -1\}, *)$

Note:

- $O(G) \leq 5$ is always "Abelian group".
- Order of a group is equal to the number of elements in the group
- Every group of prime order is a cyclic group and every cyclic group is an Abelian group.

- $(\{0, 1, 2, \ldots, m-1\}, +_m)$ Addition modulo is Abelian group.
- If G is a finite group, and $g \in G$, then $g^{|G|} = e$, and $|g|$ always divides $|G|$ (where $|g|$ means order of element g).
- $(\{1, 2, 3, \ldots, q-1\}, \times_q)$ Multiplication modulo is Abelian group.
- If $O(G) = 2n$, then there exist atleast one element other than identity element which is "Self Invertible".
- Set of all non-singular matrices is a group under matrix multiplication, but not abelian.
- The set {0, 1, 2 . . . m – 1} with $\oplus_m$ is always a group, where $\oplus_m$ is also called addition modulo m define as follows:

  $$a \oplus_m b = r\left(\frac{a+b}{m}\right);$$

  Identity of this group is $e = 0$
- The set {1, 2 . . . p – 1} with $\otimes_p$ is always a group, where $\otimes_p$ is also called multiplication modulo p defined as follows:

  $$a \otimes_p b = r\left(\frac{a \times b}{p}\right);$$

  Identity of this group is $e = 1$
- Order of an element $O(a) = n$ and $O(a) = O(a^{-1})$ where $a \in G$ and $a^n = e$.

Lattice Theory

- **First (Least) Element:** Let A be an ordered set, the element 'a' in 'A' is first element of A if for every element 'x' in A, $a \leq x$.
- **Last (Greatest) Element:** Let A be an ordered set. The element 'b' in 'A' is last element of A if for every element 'x' in A, $x \leq b$.

  Example:

  1. Let N be the set of natural numbers, then first element of $N = 1$ and there is no last element.
  2. Let 'A' be any set and let $\mathcal{P}(A)$ be the power set of A. Then first element of $\mathcal{P}(A) = \phi$ and last element of $\mathcal{P}(A) = A$
- **Minimal Element:** Elements which do not have predecessors.
- **Maximal Element:** Elements which do not have successors.

Note:

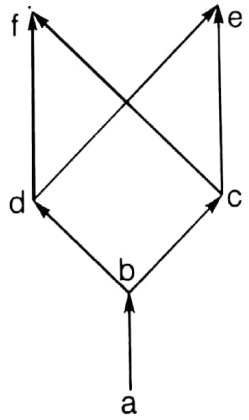
- Many minimals and maximals may exist.

- **Least Element:** 'a' is a least element of poset P; if $a \le x$; $\forall x \in P$.
- **Greatest Element:** 'b' is a greatest element of P; if $x \le b$; $\forall x \in P$.
- **Lower Bound:** Let $A \subseteq P$. Element a is a lower bound of A, if $a \in P$ and $a \le x, \forall x \in A$.
- **Upper Bound:** Let $A \subseteq P$. Element b is an upper bound of A, if $b \in P$ and $x \le b, \forall x \in A$.
- **Greatest Lower Bound [Infimum]:** 'y' is infimum of A, if y is a lower bound of 'A' and if 'z' is any other lower bound of A then $z \le y, \forall z \in P$.
- **Least Upper Bound [Supremum]:** 'x' is supremum of A, if x is an upper bound of 'A' and if 'z' is any other upper bound, then $x \le z, \forall z \in P$.

Note:

- If only one minimal exist then it is always "least"
- If only one maximal exist then it is always "greatest"
- Immediate successors of lower bound are called "atoms"

Example: Consider the following hasse diagram for a poset P.
Given P = {a, b, c, d, e, f}. Let S = {b, c, d} and $S \subseteq P$.



Then

Lower bound of S = b, a

Upper bound of S = e, f

Infimum = b

No supremum element exist.

Minimal = a

Maximal = e, f

Least = a

No greatest element exist.

Lattice

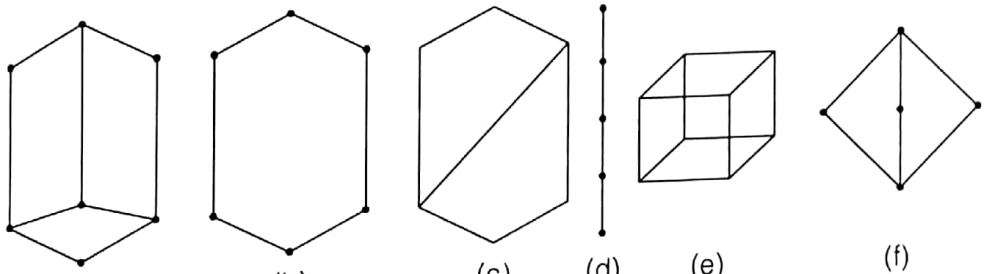
- Let (P, ≤) is a poset, in which for every two elements there exist infimum or greatest lower bound or meet (∧) and supremum or least upper bound or Join (∨) then such poset is called a "lattice".

OR

- Let 'L' be a non-empty set closed under two binary operations called meet ($\wedge$) and join ($\vee$), then 'L' is a "lattice" if for any element a, b and c of 'L' the following axioms hold.

1. **Commutative Laws:**
   (*i*) $a \wedge b = b \wedge a$
   (*ii*) $a \vee b = b \vee a$
2. **Associative Laws:**
   (*i*) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$
   (*ii*) $(a \vee b) \vee c = a \vee (b \vee c)$
3. **Absorption Laws:**
   (*i*) $a \wedge (a \vee b) = a$
   (*ii*) $a \vee (a \wedge b) = a$

- Following hasse diagrams are "lattices".



Note:

- Every chain is a lattice (i.e., linearly ordered set is a lattice).
- Let 'L' be a lattice, then $a \wedge b = a$ iff $a \vee b = b$.
- $x \wedge y$ = infimum (x, y) and $x \vee y$ = supremum (x, y).
- In lattice every 2-element subset has infimum and supremum.

Types of Lattices

Bounded Lattice

If there exist least element (0) and greatest element (1) for a lattice, such lattice is called "Bounded Lattice" i.e., if $0 \in L$ and $1 \in L$ then $0 \leq x \leq 1$, $\forall x \in L$.

- $(L, \leq, \wedge, \vee)$ and $(P(S), \subseteq, \cap, \cup)$ are bounded lattices.
- $(N, \leq, \text{Min}, \text{Max})$ and $(N, /, \text{gcd}, l\text{cm})$ are not bounded.
- Every finite lattice is "Bounded Lattice".

Complemented Lattice

In a bounded lattice, if there exist atleast one complement for every element then such a bounded lattice is "complemented lattice".

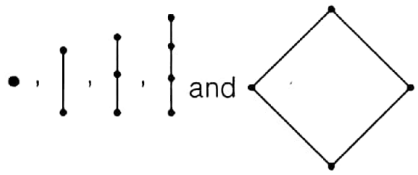
- If $x \vee y = 1$ and $x \wedge y = 0$, then x and y are complements to each other.
- Every element of complemented lattice can contain one or more complements.

Distributive Lattice

A distributive lattice 'L' satisfies:

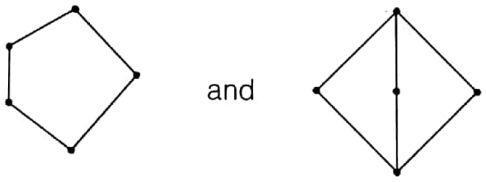
$$\left.\begin{array}{ll}(i) & a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \\ (ii) & a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)\end{array}\right\} \forall\, a, b, c \in L$$

- If a distributive lattice is complemented, then every element has a unique complement.
- A lattice with less than 5-elements is always 'distributive'.



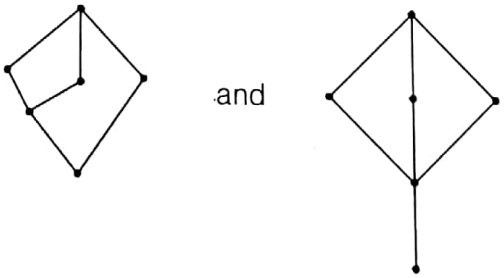
are distributive lattices

- A lattice 'L' is non-distributive iff it contains a sublattice isomorphic to the following lattices:



[Non-distributive Lattices]

- The following lattices are non-distributive lattices since they contain a sublattice isomorphic to one of the above lattice



Modular Lattice

A modular lattice 'L' satisfies: $a \vee (b \wedge c) = (a \vee b) \wedge c$; $\forall a, b, c \in L$ and $a \leq c$.

Note:

- Every distributive lattice is modular

Sublattice

A lattice 'L' is called "sublattice", if has the same meet ($\wedge$) and same join ($\vee$) as the parent lattice.

Example: $(D_{12}, /, gcd, lcm)$ is sublattice of $(N, /, gcd, lcm)$, where '$/$' represents the 'divides' relation.

Dual Poset

If $(P, \leq)$ is poset then $(P, \geq)$ is also a poset, such posets are called "dual posets".

Dual Lattice

If $(L, \leq, \wedge, \vee)$ is a lattice, $(L, \geq, \vee, \wedge)$ is also a lattice, such lattices are called "Dual Lattices".

Complete Lattice

A lattice 'L' is said to be complete if every subset of 'L' has infimum and supremum in L.

Lexicographical Order (Dictionary Order)

Let A_1 and A_2 be partial ordered sets, the lexicographical ordering ($\leq$) on $A_1 \times A_2$ is defined as:

$(a_1, a_2) < (b_1, b_2)$; either "if $a_1 < b_1$" or "both $a_1 = b_1$ and $a_2 \leq b_2$".

Well-ordered Set

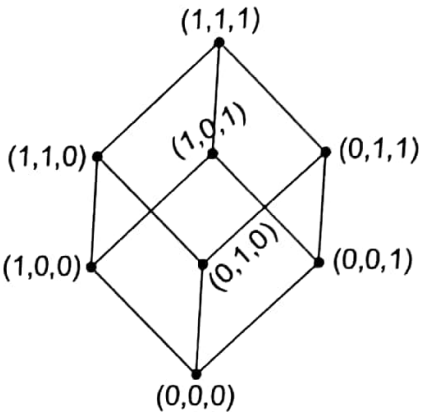
An ordered set 'A' is well-ordered if it is a chain (linearly ordered) and if it is a discrete set and every subset of 'A' contains "first element" (least element).

- Every "Finite Linearly Ordered Set" is well-ordered.
- Every well-ordered set must be linearly ordered (chain).

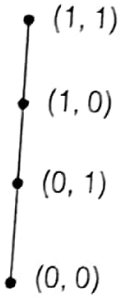
Boolean Algebra $(B, \leq, \wedge, \vee)$

- If a lattice is complemented and distributive, it is boolean algebra.

  Example: $(\mathcal{P}(S), \subseteq, \cap, \cup)$



Boolean algebra
(complemented & distributive)



Not boolean algebra
(not complemented)

- Boolean algebra satisfies: "Lattice [Poset, meet, join], Bounded [lower, upper], distributed and complemented lattices".
- Let B be a finite boolean algebra having n-atoms. Then B has 2^n elements and "every non-zero element of B is the sum of unique set of atoms".

  Example: B is boolean algebra with less than 100 elements, then B can have 2^1, 2^2, 2^3, 2^4, 2^5 or 2^6 elements.

- Let a, b, c be any elements in a boolean algebra 'B' $(B, +, *, ', 0, 1)$

1. **Commutative Laws:**

$$a + b = b + a$$
$$a * b = b * a$$

2. **Associative Laws:**

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

3. **Distributive Laws:**

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

4. **Identity Laws:**

$$a + 0 = a$$
$$a * 1 = a$$

5. **Complement Laws:**

$$a + a' = 1$$
$$a * a' = 0$$

6. **Idempotent Laws:**

$$a + a = a$$
$$a * a = a$$

7. Absorption Laws:

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

8. Involution Law or Double Complement Law:

$$[(a')' = a]$$

$$0' = 1 \quad 1' = 0 \quad \Rightarrow \quad (0')' = 0$$

9. DeMorgan's Law

$$(a + b)' = a' * b'$$
$$(a * b)' = a' + b'$$

10. Domination Law:

$$a + 1 = 1$$
$$a * 0 = 0$$

■■■