A Handbook on

Computer Science & IT

Contains well illustrated formulae & key theory concepts

for

GATE

& OTHER COMPETITIVE EXAMS

MADE EASY Publications

MADE EASY Publications

Corporate Office: 44-A/4, Kalu Sarai, New Delhi-110016
Web: www.madeeasypublications.org; Ph: 011-45124660, 8860378007
E-mail: • infomep@madeeasy.in

A Handbook on Computer Science & IT

First Edition: 2014
Reprint : 2015
Reprint: 2016

Published by: MADE EASY Publications, New Delhi-110016

Director's Message

B. Singh (Ex. IES)

During the current age of international competition in Science and Technology, the Indian participation through skilled technical professionals have been challenging to the world. Constant efforts and desire to achieve top positions are still required.

I feel every candidate has ability to succeed but competitive environment and quality guidance is required to achieve high level goals. At MADE EASY, we help you to discover your hidden talent and success quotient to achieve your ultimate goals. In my opinion GATE & PSU's exams are tool to enter in to main stream of Nation serving. The real application of knowledge and talent starts, after you enter in to the working system. Here in MADE EASY you are also trained to become winner in your life and achieve job satisfaction.

MADE EASY alumni have shared their winning stories of success and expressed their gratitude towards quality guidance of MADE EASY. Our students have not only secured All India First Ranks in ESE, GATE and PSU entrance examinations but also secured top positions in their career profiles. Now, I invite you to become alumni of MADE EASY to explore and achieve ultimate goal of your life. I promise to provide you quality guidance with competitive environment which is far advanced and ahead than the reach of other institutions. You will get the guidance, support and inspiration that you need to reach the peak of your career.

I have true desire to serve Society and Nation by way of making easy path of the education for the people of India.

After a long experience of teaching in Computer Science & IT over the period of time MADE EASY team realised that there is a need of good *Handbook* which can provide the crux of Computer Science & IT in a concise form to the student to brush up the formulae and important concepts required for GATE and other competitive examinations. This *handbook* contains all the formulae and important theoretical aspects of Computer Science & IT. It provides much needed revision aid and study guidance before examinations.

B. Singh (Ex. IES)
CMD, MADE EASY Group

A Handbook on

Computer Science & IT

CONTENTS

❍❍❍❍

A Handbook on
Computer Science

1

Engineering Mathematics

CONTENTS

Mathematical Logic

1

INTRODUCTION

- **Proposition:** It is a declarative statement either TRUE or FALSE.
- **Compound Proposition:** It is a proposition formed using the logical operators (Negation ($\neg$), Conjunction ($\wedge$), Disjunction ($\vee$), etc.) with the existing propositions.
- **Logical Operators:**

  (i) Negation of p : $\neg p$ or $\bar{p}$ or $\sim p$

  (ii) Conjunction of p and q : $p \wedge q$

  (iii) Disjunction of p and q : $p \vee q$

  (iv) Implication/Conditional : $p \rightarrow q$ (if p, then q)

  (v) Bi-conditional : $p \leftrightarrow q$

- Precedence order of logical operators from high to low: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

Note:

- Converse of $p \rightarrow q$ is : $q \rightarrow p$
- Inverse of $p \rightarrow q$ is : $\neg p \rightarrow \neg q$
- Contrapositive of $p \rightarrow q$ is : $\neg q \rightarrow \neg p$

Tautology

If compound proposition is always true then it is tautology.

Example: $p \vee \neg p$

Contradiction

If Compound proposition is always false then it is contradiction.

Example: $p \wedge \neg p$

Contingency

Neither tautology nor contradiction.

Example: p

Logical Equivalence

$P \Leftrightarrow Q$ is tautology iff P and Q are logically equivalent.

Functionally Complete

If any formula can be written as an equivalent formula containing only $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$ connectives then such set of operators called as functionally complete.

Example:

$\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \vee, \wedge\}$ are functionally complete.

Consistent

If $H_1 \wedge H_2 \wedge H_3 \wedge \ldots \wedge H_n$ is true then H_1, H_2, ... and H_n are consistent.

Inconsistent

If H_1, H_2, ... and H_n are not consistent then they are inconsistent.

Equivalences

$$P \vee (P \wedge Q) \equiv P$$
$$P \rightarrow Q \equiv \neg P \vee Q \equiv \neg Q \rightarrow \neg P$$
$$P \wedge (P \vee Q) \equiv P$$
$$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$$
$$P \leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$$
$$P \leftrightarrow Q \equiv \neg P \leftrightarrow \neg Q$$
$$P \rightarrow (Q \rightarrow R) \equiv (P \wedge Q) \rightarrow R$$
$$\neg(P \leftrightarrow Q) \equiv P \leftrightarrow (\sim Q) \equiv (\sim P) \leftrightarrow Q$$
$$(P \rightarrow Q) \wedge (P \rightarrow R) \equiv P \rightarrow (Q \wedge R)$$
$$(P \rightarrow R) \wedge (Q \rightarrow R) \equiv (P \vee Q) \rightarrow R$$
$$(P \rightarrow Q) \vee (P \rightarrow R) \equiv P \rightarrow (Q \vee R)$$
$$(P \rightarrow R) \vee (Q \rightarrow R) \equiv (P \wedge Q) \rightarrow R$$
$$P \vee Q \equiv \neg P \rightarrow Q$$
$$P \wedge Q \equiv \neg(P \rightarrow \neg Q)$$
$$\neg(P \rightarrow Q) \equiv (P \wedge \neg Q)$$

Identity Laws : (i) $P \wedge T = P$, (ii) $P \vee F = P$

Domination Laws : (i) $P \vee T = T$, (ii) $P \wedge F = F$

Idempotent Laws : (i) $P \wedge P = P$, (ii) $P \vee P = P$

Commutative Laws :

(i) $P \vee Q = Q \vee P$

(ii) $P \wedge Q = Q \wedge P$

Associative Laws :

$(i)\quad (P \vee Q) \vee R = P \vee (Q \vee R)$

$(ii)\quad (P \wedge Q) \wedge R = P \wedge (Q \wedge R)$

Distributive Laws :

$(i)\quad P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

$(ii)\quad P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$

Demorgan's Laws :

$(i)\quad \neg(P \wedge Q) = \neg P \vee \neg Q$

$(ii)\quad \neg(P \vee Q) = \neg P \wedge \neg Q$

Absorption Laws :

$(i)\quad P \vee (P \wedge Q) = P$

$(ii)\quad P \wedge (P \vee Q) = P$

Negation Laws :

$(i)\quad P \vee \neg P = T$

$(ii)\quad P \wedge \neg P = F$

Double Negation Laws : $\neg(\neg P) = P$

RULES OF INFERENCE (TAUTOLOGICAL IMPLICATIONS)

Simplification :

$$(P \wedge Q) \Rightarrow P$$
$$(P \wedge Q) \Rightarrow Q$$

Addition :

$$P \Rightarrow (P \vee Q)$$
$$Q \Rightarrow (P \vee Q)$$

Disjunctive Syllogism : $(\sim P, P \vee Q) \Rightarrow Q$

Modus Ponens : $(P, P \rightarrow Q) \Rightarrow Q$

Modus Tollens : $(\sim Q, P \rightarrow Q) \Rightarrow \sim P$

Hypothetical Syllogism : $(P \rightarrow Q, Q \rightarrow R) \Rightarrow (P \rightarrow R)$

Dilemma : $(P \vee Q, P \rightarrow R, Q \rightarrow R) \Rightarrow R$

Constructive Dilemma : $(P \vee Q, P \rightarrow R, Q \rightarrow S) \Rightarrow R \vee S$

Conjunctive Syllogism : $(\sim(P \wedge Q), P) \Rightarrow \sim Q$

Other rules :

$$\sim P \Rightarrow (P \rightarrow Q)$$
$$Q \Rightarrow (P \rightarrow Q)$$
$$\sim(P \rightarrow Q) \Rightarrow P$$
$$\sim(P \rightarrow Q) \Rightarrow \sim Q$$

Principle Conjunctive Normal Form (PCNF)

Product of sums (max term)

PCNF: $[P(x_1) \vee P(x_2)] \wedge [P(x_3) \vee P(x_4)]$

Principle Disjunctive Normal Form (PDNF)

Sums of products (min term)

PDNF: $[P(x_1) \wedge P(x_2)] \vee [P(x_3) \wedge P(x_4)]$

Number of non equivalent propositional functions with n-propositional variables are = 2^{2^n}.

PREDICATE LOGIC

Quantifiers

- Universal ($\forall$) : "for all" or "for every"
- Existential ($\exists$) : "there exist"

Predicates

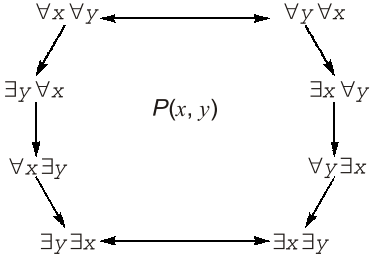
- $P(x)$: Propositional statement with one variable.
- $Q(x, y)$: Propositional statement with two variables.

Note: .....

- $\neg\exists x\, P(x) = \forall x\, \neg P(x)$
- $\neg\forall x\, P(x) = \exists x\, \neg P(x)$

.....

Logical Equivalences



- $\forall x\, P(x) \wedge \exists x\, Q(x) \equiv \forall x \exists y [P(x) \wedge Q(y)]$

- $\forall x\, P(x) \vee \exists x\, Q(x) \equiv \forall x \exists y [P(x) \vee Q(y)]$
- $\exists x [P(x) \rightarrow Q(x)] \equiv \forall x\ P(x) \rightarrow \exists x\ Q(x)]$
- $\exists x [P(x) \rightarrow Q(x)] \equiv \exists x\, P(x) \rightarrow \forall x\ Q(x)$
- $\exists x [P(x) \vee Q(x)] \equiv \exists x\, P(x) \vee \exists x\ Q(x)$
- $\forall x\ [P(x) \wedge Q(x)] \equiv \forall x\ P(x) \wedge \forall x\ Q(x)$

■■■

PROBABILITY

2

MEAN, MEDIAN AND MODE

- $$\text{Mean } (\bar{X}) = \frac{\sum_{i=1}^{n} x_i}{n} = \frac{\sum_{i=1}^{n} f_i x_i}{\sum f_i} = A + \frac{\sum f_i d_i}{\sum f_i} = A + h \cdot \frac{\sum f_i u_i}{\sum f_i}$$

where A = mid value of class at maximum frequency

$$u_i = \frac{x_i - A}{h}$$

$$d_i = x_i - A$$

- $$\text{Median} = \frac{\frac{n}{2} + \left(\frac{n}{2} + 1\right)}{2};\ n \text{ is even}$$

$$= \frac{n+1}{2};\ n \text{ is odd}$$

$$= L + \frac{h}{C_f}\left(\frac{N}{2} - C_P\right)$$

where L = lower limit of median class

$N = \Sigma f_i$

C_f = Cumulative ($N/2$) frequency of median class

C_P = Cumulative frequency of preceding median class

Mode : Value of 'x' corresponding to maximum frequency.

$$L + \frac{f_m - f_1}{(f_m - f_1) + (f_m - f_2)} \times h$$

where L = Lower limit of modal class

f_m = maximum frequency of modal class

f_1 = preceding frequency of modal class

f_2 = Following frequency of modal class

Note:

- Mode = 3 Median – 2 Mean [for Asymmetric distribution]
- Mean = Mode = Median [for Symmetric distribution]

AXIOMS OF PROBABILITY

Let A and B be two events. Then

1. $P(\bar{A}) = 1 - P(A)$
2. $P(\phi) = 0$; ϕ is the empty set
3. $P(A - B) = P(A) - P(A \cap B)$
4. $P(A \cap \bar{B}) = P(A - B)$
5. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$
6. $P(A \cup B) = P(A) + P(B)$; mutually exclusive events.
7. $P(A \cap B) = \phi$; mutually exclusive events.
8. $P(A \cap B) = P(A) \cdot P(B)$; independent events.
9. $P(S) = 1$; S is sample space.
10. $P(A_1 \cap A_2 \cap \ldots \cap A_n) \geq \sum_{i=1}^{n} P(A_i) - (n-1)$
11. $P(A_1 \cup A_2 \cup \ldots \cup A_n) \leq \sum_{i=1}^{n} P(A_i)$
12. $P(A \mid B) = \dfrac{P(A \cap B)}{P(B)}$
13. $P(A \mid B) = P(A)$; independent events.
14. $P(E_1 \cap E_2 \cap \ldots \cap E_n) = P(E_1) \cdot P(E_2) \ldots P(E_n)$; mutually independent events.
15. $P(E_2 \mid X) = \dfrac{P(X \mid E_2) \cdot P(E_2)}{P(X \mid E_1) \cdot P(E_1) + P(X \mid E_2) \cdot P(E_2) + P(X \mid E_3) \cdot P(E_3)}$
16. $P(E_i \mid X) = \dfrac{P(X \mid E_i) \cdot P(E_i)}{\sum_{j=1}^{n} P(X \mid E_j) \cdot P(E_j)}$

RANDOM VARIABLE (STOCHASTIC VARIABLE)

Random variable assigns a real number to each possible outcome.

Let X be a discrete random variable, then

1. $F(x) = P(X \le x)$ is called distribution function $\sum_{i=0}^{n} P(i)$ of X.
2. Mean or Expectation of $X = \mu = E(X) = \sum_{i=1}^{n} x_i\, P(x_i)$
3. Variance of $X = \sigma^2 = E(X^2) - [E(X)]^2 = \sum_{i=1}^{n} (x_i - \mu)^2 P(x_i)$
4. Standard deviation of $X = \sigma = \sqrt{\text{Variance}}$
5. $\sum_{i=1}^{n} P(x_i) = 1$

Types of Random Variables

1. **Discrete Random Variable:** "Finite set of values" or "Countably infinite".
2. **Continous Random Variable (Non-discrete):** "Infinite number of uncountable values".

Discrete Distributions

1. **Binomial Distribution:** The probability that the even will happen exactly r times in n trials i.e. r successes and $n - r$ failures will occur.

   $P(X = r) = P(r) = \Sigma\, {}^{n}C_r\, p^r q^{n-r}$

   Mean $= E(x) = np$

   Variance $(\sigma^2) = V(x) = npq$

   $S.D\,(\sigma) = \sqrt{npq}$

   Where $r = 0, 1, \ldots, n$

   $q = 1 - p$

   n = fixed number of trials

   p = probability of success

2. **Poisson Distribution:**

$$P(X = x) = \sum \frac{e^{-\lambda} \cdot \lambda^x}{x!};\ x = 0, 1, 2, \ldots, \infty$$

Where X = Discrete random variable

λ = Parameter of distribution (positive constant)

- Mean (μ) = Variable (σ^2) = λ
- $S.D = \sqrt{\lambda}$

Poisson distribution is a limiting case of binomial distribution as $n \to \infty$ and $P \to 0$.

CONTINUOUS DISTRIBUTION

Let X be continous random variable. Then

(i) **Density functions:**

- $P(X \le a) = \int_{-\infty}^{a} f(x) \cdot dx$
- $P(a \le X \le b) = \int_{a}^{b} f(x) \cdot dx$

(ii) **Mean** = $E(x) = \int_{-\infty}^{\infty} \dot{x} \cdot f(x) \cdot dx$

(iii) **Variance of X** = $V(X) = \int_{-\infty}^{\infty} [x - E(x)]^2 \cdot f(x)\, dx$

(iv) $\int_{-\infty}^{\infty} f(x)\, dx = 1$

1. Uniform Distribution (Rectangular Distribution)

(i) **Density function:**

$$f(x) = \frac{1}{b-a}; \quad a \le x \le b$$

$$= 0 \text{ ; otherwise}$$

(ii) **Cumulative function:**

$$f(x) = P(X \le x) = \int_{-\infty}^{x} f(x) \cdot dx$$

$$P(X \le x) = \int_{-\infty}^{x} f(x)\cdot dx = \begin{cases} 0 & ; \quad \text{if } x \le a \\ \dfrac{x-a}{b-a} & ; \quad \text{if } a \le x \le b \\ 1 & ; \quad \text{if } x > b \end{cases}$$

(*iii*) **Mean (μ)** = $(a + b)/2 = E(X)$

(*iv*) **Variance (σ^2)** = $(b - a)^2/12$

2. Exponential Distribution

(*i*) Density function:

$$f(x) = \lambda \cdot e^{-\lambda x} \quad ; x > 0$$
$$= 0 \quad ; \text{ Otherwise}$$

(*i*) **Mean (μ)** = $\dfrac{1}{\lambda} = S.D(\sigma)$

(*i*) **Variance (σ^2)** = $\dfrac{1}{\lambda^2}$

3. Normal Distribution

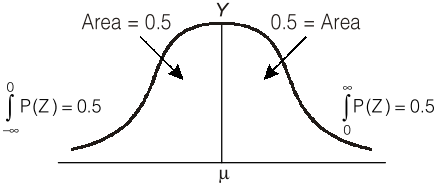
(*i*) **Density function** $f(x) = \dfrac{1}{\sigma\sqrt{2\pi}} \cdot e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}$; $-\infty \le x \le \infty$, $\sigma > 0$, $-\infty < \mu < \infty$

(*ii*) Normal distribution is symmetrical

(*iii*) Mean = μ; Variance = σ^2

(*iv*) $f(x) \ge 0$ for all x

(*v*) $\int_{-\infty}^{\infty} f(x)\cdot dx = 1$ and variate $(Z) = \dfrac{x-\mu}{\sigma} = \dfrac{x - nP}{\sqrt{nPq}}$



(*vi*) $P(Z) = \dfrac{1}{\sqrt{2\pi}} e^{-\frac{Z^2}{2}}$; $-\infty \le Z \le \infty$ and $Z = \dfrac{x-\mu}{\sigma}$

Z = Standard normal variate

■■■

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.

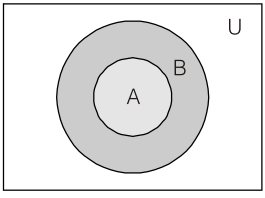
- $\mathbb{N}$ be set of natural numbers : {1, 2, 3, ...}
- $\mathbb{Z}$ be set of integers : {..., –2, –1, 0, 1, 2,...}
- $\mathbb{Q}$ be set of rational numbers
- $\mathbb{R}$ be set of real numbers
- $\mathbb{C}$ be set of complex numbers

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

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. **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.
4. **Singleton set:** A set with one element is called a singleton set.
5. **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.



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.

6. **Proper subset:** A set A is a subset of the set B but that $A \neq B$, we write $A \subset B$ and say that A is a proper subset of B i.e. A is a proper subset of B if $\forall x\,(x \in A \rightarrow x \in B) \wedge \exists x\,(x \in B \wedge x \notin A)$
7. **Finite set:** A set in which number of elements are countable i.e., cardinality of set can be obtained.
8. **Infinite set:** A set is said to be infinite if it is not finite.
   Example: The set of positive integer is infinite.
9. **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 if $|A \times B| = |B \times A|$ then $A = B$ or $A = \phi$ or $B = \phi$.

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:

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

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.

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

Principle of Extension

Two sets A and B are equal iff they have same members (elements).

Principle of Abstraction

Given set 'U' and property 'P' there is set 'A' such that the elements of set 'A' are exactly those members of U which have property P.

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
$A \cup \phi = A$ $A \cap U = A$	Identity Laws
$A \cup U = U$ $A \cap \phi = \phi$	Domination Laws
$A \cup A = A$ $A \cap A = A$	Idempotent Laws
$(\overline{A}) = A$	Complementation Law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	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
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	De Morgans Laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption Laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \phi$	Complement Laws

MULTISET

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

Example: $\{a, a, b, b, b, c, c, c, c, c, d\} = \{2\cdot a, 3\cdot b, 4\cdot c, 1\cdot d\}$

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 $f : A \to B$.

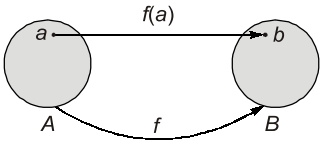
Note:

- 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 $P(n, m) = n(n-1)(n-2)..... (n-(m-1))$.
   - If $|A| = |B| = n$ then number of one-to-one functions from A to B is $P(n, n) = n(n-1)(n-2).... 1 = n!$

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 $f(a) = b$.
   - 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 $A \to B = n^m - {}^nC_1(n-1)^m + {}^nC_2(n-2)^m ... + (-1)^{n-1}\,{}^nC_{n-1}(1^m)$.

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 $f \circ f^{-1} = I_B$, $f \circ f^{-1} = I_A$, $f^{-1} : B \to A$
- 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., $R^{-1} = \{(b, a) \mid (a, b) \in R\}$
2. **Complementary Relation:** If R is a relation from A to B then $R^C = \{(a, b) \mid (a, b) \notin R\} = (A \times B) - R$.
3. **Diagonal Relation:** A relation R on a set A is called diagonal relation if $R = \{(a, a) \mid a \in A\} = \Delta_A$.
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 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 diagonal pairs $= 2^n$.
   - Number of symmetric relations possible with 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.
- Any subset of antisymmetric relation is also antisymmetric relation.
- If $A = \{1, 2, ..., n\}$ 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.
- If $R \cap R^{-1} \subseteq \Delta_A$.

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 $A = \{1, 2, ..., n\}$ 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 $\overline{R}$ is irreflexive

(*v*) Antisymmetric, then $(R \cap S)$ is also antisymmetric for any relation S on A.

- If $(R \cap S) \subseteq R$ and every subset of R is also antisymmetric.
- If R is relation on a set A then $R \cup R^{-1}$ is always symmetric.
- **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 every subset is a non-empty set and (*i*) $\forall_{i,j}\ A \cap A_j = \phi$; $(i \neq j)$ (ii) $(A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n) = A$.

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 Operation] (*)

Binary operator $*$ is said to be a binary operation 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

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

Identity

$a * e = e * a = a; \quad \forall a \in G$ where 'e' is identity

Note:

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

Inverse

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

Commutative

$a * b = b * a; \ \forall a,b \in G$

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., $a * b = b * a; \ \forall a,b \in G$.

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 and let $g \in G$ be an element of G. Then the order of g is the smallest positive number k, such that $ak = e$.
  5. Let G be a finite group and let $g \in G$. Then the order of g divides the order of G.
  6. Let G be a group of prime order. Then G is cyclic.
- Any group of even order contains an element of order two.
- Let G be a cyclic group. Every subgroup of G is cyclic.
- 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.

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

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

- 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 riht 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 order of group is prime, is cyclic group and every cyclic group is 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 $|g|$ divides $|G|$.
- $(\{1, 2, 3, \ldots, q-1\}, \times_q)$ 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.
- $a \oplus_m b = r\left(\frac{a+b}{m}\right)$; Identity $e = 0$
- $a \otimes_p b = r\left(\frac{a \times b}{p}\right)$; Identity $e = 1$
- Order of an element $O(a) = n$ and $O(a) = O(a^{-1})$ where $a \in G$ and $a^n = e$.

Example:

$$\{1, -1, i, -i\} \Rightarrow e = 1$$
$$(-1)^2 = 1 = e \Rightarrow O(-1) = 2 \text{ and}$$
$$(i)^4 = 1 = e \Rightarrow O(i) = 4$$

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, $a \le x$.
- **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, $x \le b$.

  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.

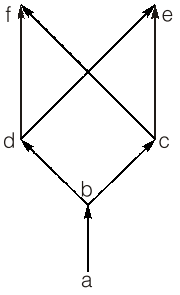
- **Least Element:** 'a' is a least element of poset P; if $a \le x$; $\forall x \in P$.
- **Greatest Element:** 'b' is a greatest element of P; if $x \le b$; $\forall x \in P$.
- **Lower Bound:** Let $A \subseteq$ P. Element a is a lower bound of A, if $a \in$ P and $a \le x$, $\forall x \in A$.

- **Upper Bound:** Let $A \subseteq P$. Element b is an upper bound of A, if $b \in P$ and $x \leq b, \forall x \in A$.
- **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 $z \leq y, \forall z \in P$.
- **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 $x \leq z, \forall z \in P$.

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".

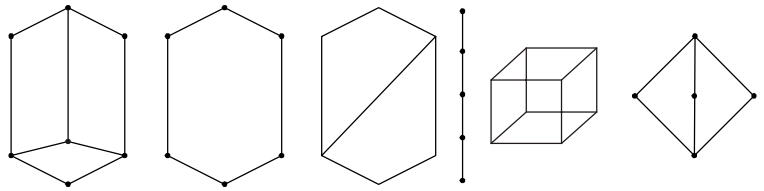
OR

- Let 'L' be a non-empty set closed under two binary operations called meet (∧) and join (∨), 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 lower bound (l) and upper bound (u) for a lattice, such lattice is called "Bounded Lattice" i.e., if $l \in L$ and $u \in L$ then $l \leq x \leq u$, $\forall x \in L$.

- (L, $\leq$, $\wedge$, $\vee$) and (P(S), $\subseteq$, $\cap$, $\cup$) are bounded lattices.
- (N, $\leq$, Min, Max) and (N, /, gcd, lcm) 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".

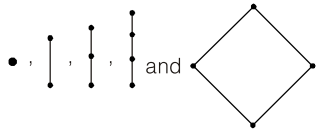
- If $x \vee y$ = upper bound and $x \wedge y$ = lower bound, then x and y are complements to each other.
- Every element of complemented lattice can contain one or more complements.

Distributive Lattice

A distributive lattice 'L' satisfies :

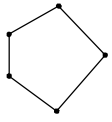
$$\left.\begin{array}{ll}(i) & a \wedge (b \wedge c) = (a \wedge b) \vee (a \wedge c) \\ (ii) & a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)\end{array}\right\} \forall\, a, b, c \in L$$

- A distributive lattice is a bounded lattice where every element has unique complement.
- A lattice with less than 5-elements is always 'distributive'.

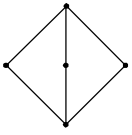


are distributive lattices

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

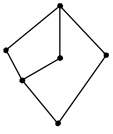


and

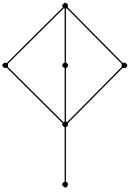


[Non-distributive Lattice]

- The following lattices are non-distributive.



and



are non-distributive lattices
(Isomorphic to 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 under same meet ($\wedge$) and same join ($\vee$)

Example: (D_{12}, /, *gcd*, *lcm*) is sublattice

Dual Order

(P, ≤) is poset then (P, ≥) is also a poset, such poset is called "dual order".

Dual Lattice

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

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 (≤) on $A_1 \times A_2$ is defined as:

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

OR

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

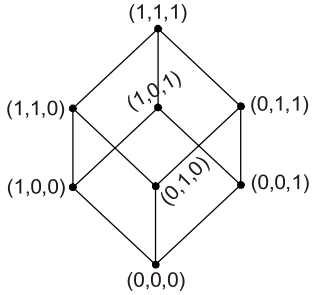
Well-ordered Set

An ordered set 'A' is well-ordered if every subset of 'A' contains "first element" (least element).

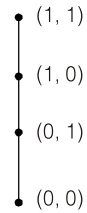
- "Finite Linearly Ordered Set" is well-ordered.
- Every well-ordered set must be linearly ordered (chain).

Boolean Algebra (B, ≤, ∧, ∨)

- If a lattice is complemented and distributive, it is boolean algebra.
  Example: $(\mathcal{P}(S), \subseteq, \cap, \cup)$
- Let 'B' be a boolean algebra. Then 'B' is a partially ordered set, where $a \leq b$ is defined by $a \vee b = b$.



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. Distributive Laws:
$$a + (b * c) = (a + b) * (a + c)$$
$$a * (b + c) = (a * b) + (a * c)$$
3. Identity Laws:
$$a + 0 = a$$
$$a * 1 = a$$
4. Complement Laws:
$$a + a' = 1$$
$$a * a' = 0$$
5. idempotent Laws:
$$a + a = a$$
$$a * a = a$$
6. Boundedness Laws:
$$a + 1 = 1$$
$$a * 0 = 0$$
7. Absorption Laws:
$$a + (a * b) = a$$
$$a * (a + b) = a$$
8. Associative Laws:
$$(a + b) + c = a + (b + c)$$
$$(a * b) * c = a * (b * c)$$
9. Involution Law [(a′)′ = a]:
$$\left.\begin{array}{l} 0' = 1 \\ 1' = 0 \end{array}\right\} \Rightarrow \quad (0')' = 0$$

■■■