



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

Department of Mathematics

UNIT I – LOGIC – SMTA1307

LOGIC

Statements - Truth tables - Connectives - Equivalent Propositions - Tautological Implications - Normal forms - Predicate Calculus, Inference theory for Propositional Calculus and Predicate Calculus.

Propositional Logic – Definition

A proposition is a collection of declarative statements that has either a truth value "true" or a truth value "false". A propositional consists of propositional variables and connectives. We denote the propositional variables by capital letters (A, B, etc). The connectives connect the propositional variables.

Some examples of Propositions are given below –

- "Man is Mortal", it returns truth value "TRUE"
- " $12 + 9 = 3 - 2$ ", it returns truth value "FALSE" The following is not a Proposition
- "A is less than 2". It is because unless we give a specific value of A, we cannot say whether the statement is true or false.

Connectives

In propositional logic generally we use five connectives which are – OR (\vee), AND (\wedge), Negation/ NOT (\neg), Implication / if-then (\rightarrow), If and only if (\leftrightarrow).

OR (\vee): The OR operation of two propositions A and B (written as $A \vee B$) is true if at least any of the propositional variable A or B is true.

The truth table is as follows –

A	B	$A \vee B$
True	True	True
True	False	True
False	True	True
False	False	False

False

AND (\wedge) : The AND operation of two propositions A and B (written as $A \wedge B$) is true if both the propositional variable A and B is true.

The truth table is as follows –

A	B	$A \wedge B$
True	True	False
True	False	False
False	True	False
False	False	True

Negation (\neg) :The negation of a proposition A (written as $\neg A$) is false when A is true and is true when A is false.

The truth table is as follows –

A	$\neg A$
True	False
False	True

Implication / if-then (\rightarrow): An implication $A \rightarrow B$ is False if A is true and B is false. The rest of the cases are true.

The truth table is as follows –

A	B	$A \rightarrow B$
True	True	True
True	False	False
False	True	True
False	False	True

If and only if (\leftrightarrow) : $A \leftrightarrow B$ is bi-conditional logical connective which is true when p and q are both false or both are true.

The truth table is as follows –

A	B	$A \leftrightarrow B$
True	True	True
True	False	False
False	True	False
False	False	True

Tautologies

A Tautology is a formula which is always true for every value of its propositional variables.

Example – Prove $[(A \rightarrow B) \wedge A] \rightarrow B$ is a tautology

The truth table is as follows –

A	B	$A \rightarrow B$	$(A \rightarrow B) \wedge A$	$[(A \rightarrow B) \wedge A] \rightarrow B$
True	True	True	True	True
True	False	False	False	True
False	True	True	False	True
False	False	True	False	True

As we can see every value of $[(A \rightarrow B) \wedge A] \rightarrow B$ is “True”, it is a tautology.

Contradictions

A Contradiction is a formula which is always false for every value of its propositional variables.

Example – Prove $(A \vee B) \wedge [(\neg A) \wedge (\neg B)]$ is a contradiction

The truth table is as follows –

A	B	$A \vee B$	$\neg A$	$\neg B$	$(\neg A) \wedge (\neg B)$	$(A \vee B) \wedge [(\neg A) \wedge (\neg B)]$
True	True	True	False	False	False	False
True	False	True	False	True	False	False
False	True	True	True	False	False	False
False	False	False	True	True	True	False

As we can see every value of $(A \vee B) \wedge [(\neg A) \wedge (\neg B)]$ is “False”, it is a contradiction

Contingency

A Contingency is a formula which has both some true and some false values for every value of its propositional variables.

Example – Prove $(A \vee B \vee) \wedge (\neg A)$ a contingency

The truth table is as follows –

A	B	$A \vee B$	$\neg A$	$(A \vee B) \wedge (\neg A)$
True	True	True	False	False
True	False	True	False	False
False	True	True	True	True
False	False	False	True	False

As we can see every value of $(A \vee B) \wedge (\neg A)$ has both “True” and “False”, it is a contingency.

Propositional Equivalences

Two statements X and Y are logically equivalent if any of the following two conditions –

- The truth tables of each statement have the same truth values.
- The bi-conditional statement $X \leftrightarrow Y$ is a tautology.

Example – Prove $\neg(A \vee B)$ and $[(\neg A) \wedge (\neg B)]$ are equivalent

Testing by 1st method (Matching truth table)

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$[(\neg A) \wedge (\neg B)]$
True	True	True	False	False	False	False
True	False	True	False	False	True	False
False	True	True	False	True	False	False
False	False	False	True	True	True	True

Here, we can see the truth values of $\neg(A \vee B)$ and $[(\neg A) \wedge (\neg B)]$ are same, hence the statements are equivalent.

Testing by 2nd method (Bi-conditionality)

A	B	$\neg(A \vee B)$	$[(\neg A) \wedge (\neg B)]$	$[\neg(A \vee B) \leftrightarrow [(\neg A) \wedge (\neg B)]]$
True	True	False	False	True
True	False	False	False	True
False	True	False	False	True
False	False	True	True	True

As $[\neg(A \vee B) \leftrightarrow [(\neg A) \wedge (\neg B)]]$ is a tautology, the statements are equivalent.

EQUIVALENT LAWS

Equivalence	Name of Identity
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity Laws
$p \wedge F \equiv F$ $p \vee T \equiv T$	Domination Laws
$p \wedge p \equiv p$ $p \vee p \equiv p$	Idempotent Laws
$\neg(\neg p) \equiv p$	Double Negation Law
$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$	Commutative Laws
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$	Associative Laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive Laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's Laws
$p \wedge (p \vee q) \equiv p$ $p \vee (p \wedge q) \equiv p$	Absorption Laws
$p \wedge \neg p \equiv F$ $p \vee \neg p \equiv T$	Negation Laws

Logical Equivalences involving Conditional Statements

$p \rightarrow q \equiv \neg p \vee q$
$p \rightarrow q \equiv \neg q \rightarrow \neg p$
$p \vee q \equiv \neg p \rightarrow q$
$p \wedge q \equiv \neg(p \rightarrow \neg q)$
$\neg(p \rightarrow q) \equiv p \wedge \neg q$
$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Logical Equivalences involving Biconditional Statements

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

$$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$$

$$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$$

$$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$$

A conditional statement has two parts – **Hypothesis** and **Conclusion**.

Example of Conditional Statement – “If you do your homework, you will not be punished.” Here, "you do your homework" is the hypothesis and "you will not be punished" is the conclusion.

Inverse, Converse, and Contra-positive

Inverse –An inverse of the conditional statement is the negation of both the hypothesis and the conclusion. If the statement is “If p, then q”, the inverse will be “If not p, then not q”. The inverse of “If you do your homework, you will not be punished” is “If you do not do your homework, you will be punished.”

Converse –The converse of the conditional statement is computed by interchanging the hypothesis and the conclusion. If the statement is “If p, then q”, the inverse will be “If q, then p”. The converse of "If you do your homework, you will not be punished" is "If you will not be punished, you do not do your homework”.

Contra-positive –The contra-positive of the conditional is computed by interchanging the hypothesis and the conclusion of the inverse statement. If the statement is “If p, then q”, the inverse will be “If not q, then not p”. The Contra-positive of "If you do your homework, you will not be punished” is "If you will be punished, you do your homework”.

Example:

Give the converse and the Contra positive of the implication “ If it is raining then I get wet”.

Solution :

P : It is raining Q : I get wet

Converse : $Q \rightarrow P$: If I get wet, then it is raining.

Contrapositive : $\neg Q \rightarrow \neg P$: If I do not get wet, then it is not raining

DUALITY PRINCIPLE

Duality principle set states that for any true statement, the dual statement obtained by interchanging unions into intersections (and vice versa) and interchanging Universal set into Null set (and vice versa) is also true. If dual of any statement is the statement itself, it is said **self-dual** statement.

Examples : i) The dual of $(A \cap B) \cup C$ is $(A \cup B) \cap C$
 ii) The dual of $P \wedge Q \wedge F$ is $P \vee Q \vee T$

Example : 1

Construct a truth table for $(p \rightarrow q) \rightarrow (q \rightarrow p)$

p	q	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \rightarrow (q \rightarrow p)$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Example 2: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent

Solution : The truth tables for these compound proposition is as follows.

1	2	3	4	5	6	7	8
P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	$6 \leftrightarrow 7$
T	T	F	F	T	F	F	T
T	F	F	T	T	F	F	T
F	T	T	F	T	F	F	T
F	F	T	T	F	T	T	T

We can observe that the truth values of $\neg(p \vee q)$ and $\neg p \wedge \neg q$ agree for all possible combinations of the truth values of p and q.

Example 3: Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Solution : The truth tables for these compound proposition as follows.

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

As the truth values of $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Example 4 : Determine whether each of the following form is a tautology or a contradiction or neither :

- i) $(P \wedge Q) \rightarrow (P \vee Q)$
- ii) $(P \vee Q) \wedge (\neg P \wedge \neg Q)$
- iii) $(\neg P \wedge \neg Q) \rightarrow (P \rightarrow Q)$
- iv) $(P \rightarrow Q) \wedge (P \wedge \neg Q)$
- v) $[P \wedge (P \rightarrow \neg Q) \rightarrow Q]$

Solution:

- i) The truth table for $(p \wedge q) \rightarrow (p \vee q)$

P	q	$p \wedge q$	$p \vee q$	$(p \wedge q) \rightarrow (p \vee q)$
T	T	T	T	T
T	F	F	T	T
F	T	F	T	T
F	F	F	F	T

Here all the entries in the last column are 'T'.

$\therefore (p \wedge q) \rightarrow (p \vee q)$ is a tautology.

ii) The truth table for $(p \vee q) \wedge (\neg p \wedge \neg q)$ is

1	2	3	4	5	6	
p	q	$p \vee q$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$3 \wedge 6$
T	T	T	F	F	F	F
T	F	T	F	T	F	F
F	T	T	T	F	F	F
F	F	F	T	T	T	F

The entries in the last column are 'F'. Hence $(p \vee q) \wedge (\neg p \wedge \neg q)$ is a contradiction.

iii) The truth table is as follows.

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$p \rightarrow q$	$(\neg p \wedge \neg q) \rightarrow (p \rightarrow q)$
T	T	F	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	F	T	T
F	F	T	T	T	T	T

Here all entries in last column are 'T'.

$\therefore (\neg p \wedge \neg q) \rightarrow (p \rightarrow q)$ is a tautology.

iv) The truth table is as follows.

p	q	$\neg q$	$p \wedge \neg q$	$p \rightarrow q$	$(p \rightarrow q) \wedge (p \wedge \neg q)$
T	T	F	F	T	F
T	F	T	T	F	F
F	T	F	F	T	F
F	F	T	F	T	F

All the entries in the last column are 'F'. Hence it is contradiction.

v) The truth table for $[p \wedge (p \rightarrow \neg q) \rightarrow q]$

p	q	$\neg q$	$p \rightarrow \neg q$	$p \wedge (p \rightarrow \neg q)$	$[p \wedge (p \rightarrow \neg q) \rightarrow q]$
T	T	F	F	F	T
T	F	T	T	T	F
F	T	F	T	F	T
F	F	T	T	F	T

The last entries are neither all 'T' nor all 'F'.

$\therefore [p \wedge (p \rightarrow \neg q) \rightarrow q]$ is a neither tautology nor contradiction. It is a Contingency.

Example 5: Symbolize the following statement

Let p, q, r be the following statements:

p: I will study discrete mathematics

q: I will watch T.V.

r: I am in a good mood.

Write the following statements in terms of p, q, r and logical connectives.

(1) If I do not study and I watch T.V., then I am in good mood.

(2) If I am in good mood, then I will study or I will watch T.V.

(3) If I am not in good mood, then I will not watch T.V. or I will study.

(4) I will watch T.V. and I will not study if and only if I am in good mood.

Solution:

$$(1) (\neg p \wedge q) \rightarrow r$$

$$(2) r \rightarrow (p \vee q)$$

$$(3) \neg r \rightarrow (\neg q \vee p)$$

$$(4) (q \wedge \neg p) \leftrightarrow r$$



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT –II–DISCRETE MATHEMATICS – SMTA1307

UNIT II - INFERENCE THEORY

Normal Forms, Disjunctive Normal Forms, Conjunctive Normal Forms, Principal Disjunctive Normal Forms, Principal Conjunctive Normal Forms, Rules of Inference, The Predicate Calculus, Predicates, Variables and Quantifiers, Predicate Formula, Free and Bound Variables.

Normal Forms

We can convert any proposition in two normal forms –

1. Conjunctive normal form
2. Disjunctive normal form

Elementary Product: A product of the variables and their negations in a formula is called an elementary product. If P and Q are any two atomic variables, then P , $\neg P \wedge Q$, $\neg Q \wedge P \wedge \neg P$ are some examples of elementary products.

Elementary Sum: A sum of the variables and their negations in a formula is called an elementary sum. If P and Q are any two atomic variables, then P , $p \vee q$, $\neg Q \vee \neg p$ are some examples of elementary sums.

Conjunctive Normal Form

A compound statement is in conjunctive normal form if it is obtained by operating AND among variables (negation of variables included) connected with ORs.

Examples

- $(P \cup Q) \cap (Q \cup R)$
- $(\neg P \cup Q \cup S \cup \neg T)$

Disjunctive Normal Form

A compound statement is in disjunctive normal form if it is obtained by operating OR among variables (negation of variables included) connected with ANDs.

Examples

- $(P \cap Q) \cup (Q \cap R)$
- $(\neg P \cap Q \cap S \cap \neg T)$

Predicate Logic deals with predicates, which are propositions containing variables.

Functionally Complete set

A set of logical operators is called functionally complete if every compound proposition is logically equivalent to a compound proposition involving only this set of logical operators. \wedge , \vee , and \neg form a functionally complete set of operators.

Minterms: For two variables p and q there are 4 possible formulas which consist of conjunctions of p , q or its negation given by $p \wedge q$, $p \wedge \neg q$, $\neg p \wedge q$ and $\neg p \wedge \neg q$

Maxterms: For two variables p and q there are 4 possible formulas which consist of disjunctions of p , q or its negation given by $p \vee q$, $p \vee \neg q$, $\neg p \vee q$ and $\neg p \vee \neg q$

Principal Disjunctive Normal Form: For a given formula an equivalent formula consisting of disjunctions of minterms only is known as principal disjunctive normal form (PDNF)

Principal Conjunctive Normal Form: For a given formula an equivalent formula consisting of conjunctions of maxterms only is known as principal conjunctive normal form (PCNF)

Predicate Logic – Definition

A predicate is an expression of one or more variables defined on some specific domain. A predicate with variables can be made a proposition by either assigning a value to the variable or by quantifying the variable.

The following are some examples of predicates –

- Let $E(x, y)$ denote " $x = y$ "
- Let $X(a, b, c)$ denote " $a + b + c = 0$ "
- Let $M(x, y)$ denote " x is married to y "

Well Formed Formula

Well Formed Formula (Wff) is a predicate holding any of the following –

- All propositional constants and propositional variables are wffs
- If x is a variable and Y is a wff, $\forall x Y$ and $\exists x Y$ are also wff
- Truth value and false values are wffs
- Each atomic formula is a wff
- All connectives connecting wffs are wffs

Quantifiers

The variable of predicates is quantified by quantifiers. There are two types of quantifier in predicate logic – Universal Quantifier and Existential Quantifier.

Universal Quantifier

Universal quantifier states that the statements within its scope are true for every value of the specific variable. It is denoted by the symbol \forall .

$\forall x P(x)$ is read as for every value of x , $P(x)$ is true.

Example – "Man is mortal" can be transformed into the propositional form $\forall x P(x)$ where $P(x)$ is the predicate which denotes x is mortal and the universe of discourse is all men.

Existential Quantifier

Existential quantifier states that the statements within its scope are true for some values of the specific variable. It is denoted by the symbol \exists .

$\exists x P(x)$ is read as for some values of x , $P(x)$ is true.

Example – "Some people are dishonest" can be transformed into the propositional form $\exists x P(x)$ where $P(x)$ is the predicate which denotes x is dishonest and the universe of discourse is some people.

Nested Quantifiers

If we use a quantifier that appears within the scope of another quantifier, it is called nested quantifier.

Example

- $\forall a \exists b P(a, b)$ where $P(a, b)$ denotes $a + b = 0$
- $\forall a \forall b \forall c P(a, b, c)$ where $P(a, b, c)$ denotes $a + (b + c) = (a + b) + c$

Note – $\forall a \exists b P(x, y) \neq \exists a \forall b P(x, y)$

To deduce new statements from the statements whose truth that we already know, Rules of Inference are used.

What are Rules of Inference for?

Mathematical logic is often used for logical proofs. Proofs are valid arguments that determine the truth values of mathematical statements.

An argument is a sequence of statements. The last statement is the conclusion and all its preceding statements are called premises (or hypothesis). The symbol “ \therefore ”, (read therefore) is placed before the conclusion. A valid argument is one where the conclusion follows from the truth values of the premises.

Rules of Inference provide the templates or guidelines for constructing valid arguments from the statements that we already have.

Addition

If P is a premise, we can use Addition rule to derive $P \vee Q$.

$\begin{array}{l} P \\ Q \\ \hline \end{array}$

Example

Let P be the proposition, “He studies very hard” is true

Therefore – “Either he studies very hard Or he is very bad student.” Here Q is the proposition “he is a very bad student”.

Conjunction

If P and Q are two premises, we can use Conjunction rule to derive $P \wedge Q$.

$$\begin{array}{c} P \\ Q \\ \hline \end{array}$$

Example

Let P – “He studies very hard”

Let Q – “He is the best boy in the class”

Therefore – “He studies very hard and he is the best boy in the class”

Simplification

If $P \wedge Q$ is a premise, we can use Simplification rule to derive P.

$$\begin{array}{c} P \wedge Q \\ \hline \therefore P \end{array}$$

Example

“He studies very hard and he is the best boy in the class”

Therefore – “He studies very hard”

Modus Ponens

If P and $P \rightarrow Q$ are two premises, we can use Modus Ponens to derive Q.

$$\begin{array}{c} P \rightarrow Q \\ \hline P \end{array}$$

Example

“If you have a password, then you can log on to face book”
“You have a password”

Therefore – “You can log on to face book”

Modus Tollens

If $P \rightarrow Q$ and $\neg Q$ are two premises, we can use Modus Tollens to derive $\neg P$.

	$P \rightarrow Q$
	$\neg Q$

	$\neg P$

Example

"If you have a password, then you can log on to face

book" "You cannot log on to face book"

Therefore – "You do not have a password"

Disjunctive Syllogism

If $\neg P$ and $P \vee Q$ are two premises, we can use Disjunctive Syllogism to derive Q .

	$\neg P$
	$P \vee Q$

	Q

Example

"The ice cream is not vanilla flavored"

"The ice cream is either vanilla flavored or chocolate flavored"

Therefore – "The ice cream is chocolate flavored"

Hypothetical Syllogism

If $P \rightarrow Q$ and $Q \rightarrow R$ are two premises, we can use Hypothetical Syllogism to derive $P \rightarrow R$

P	$\rightarrow Q$
Q	$\rightarrow R$

	$P \rightarrow R$

Example

"If it rains, I shall not go to school"

"If I don't go to school, I won't need to do homework"

Therefore – "If it rains, I won't need to do homework"

Constructive Dilemma

If $(P \rightarrow Q) \wedge (R \rightarrow S)$ and $P \vee R$ are two premises, we can use constructive dilemma to derive $Q \vee S$.

$$(P \rightarrow Q) \wedge (R \rightarrow S)$$

$$P \vee R$$

$$\therefore Q \vee S$$

Example

"If it rains, I will take a leave"

"If it is hot outside, I will go for a shower"

"Either it will rain or it is hot outside"

Therefore – "I will take a leave or I will go for a shower"

Destructive Dilemma

If $(P \rightarrow Q) \wedge (R \rightarrow S)$ and $\neg Q \vee \neg S$ are two premises, we can use destructive dilemma to derive $\neg P \vee \neg R$.

$$(P \rightarrow Q) \vee (R \rightarrow S)$$

$$\neg Q \vee \neg S$$

Example “If it rains, I will take a leave”

“If it is hot outside, I will go for a

shower”

“Either I will not take a leave or I will not go for a shower”

Therefore – “It rains or it is hot outside”

Solved Problems

Write the truth table for the formula $(p \wedge q) \vee (\neg p \wedge \neg q)$

Ans:

P	q	$\neg p$	$\neg q$	$p \wedge q$	$\neg p \wedge \neg q$	$(p \wedge q) \vee (\neg p \wedge \neg q)$
T	T	F	F	T	F	T
T	F	F	T	F	F	F
F	T	T	F	F	F	F
F	F	T	T	F	T	T

Check whether $((p \rightarrow q) \rightarrow r) \vee \neg p$ is a tautology.

Ans:

$$\begin{aligned} ((p \rightarrow q) \rightarrow r) \vee \neg p &\Leftrightarrow ((\neg p \vee q) \rightarrow r) \vee \neg p \Leftrightarrow (\neg(\neg p \vee q) \vee r) \vee \neg p \Leftrightarrow (p \wedge \neg q) \vee (r \vee \neg p) \\ &\Leftrightarrow (r \vee \neg p \vee p) \wedge (r \vee \neg p \vee \neg q) \Leftrightarrow T \wedge (r \vee \neg p \vee \neg q) \Leftrightarrow (r \vee \neg p \vee \neg q) \end{aligned}$$

The given statement is not a tautology

What is meant by Tautology? Without using truth table, show that

$((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ is a tautology.

Solution: A Statement formula which is true always irrespective of the truth values of the individual variables is called a tautology.

$$\text{Consider } \neg(\neg P \wedge (\neg Q \vee \neg R)) \Rightarrow \neg(\neg P \wedge \neg(Q \wedge R)) \Rightarrow P \vee (Q \wedge R) \Rightarrow (P \vee Q) \wedge (P \vee R) \quad (1)$$

$$\text{Consider } (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R) \Rightarrow \neg(P \vee Q) \vee \neg(P \vee R) \Rightarrow \neg((P \vee Q) \wedge (P \vee R)) \quad (2)$$

Using (1) and (2)

$$((P \vee Q) \wedge (P \vee R) \wedge (P \vee R)) \vee \neg((P \vee Q) \wedge (P \vee R))$$

$$\Rightarrow [(P \vee Q) \wedge (P \vee R)] \vee \neg[(P \vee Q) \wedge (P \vee R)] \Rightarrow T$$

Prove the following equivalences by proving the equivalences of the dual

$$\neg((\neg P \wedge Q) \vee (\neg P \wedge \neg Q)) \vee (P \wedge Q) \equiv P$$

Solution: It's dual is

$$\neg((\neg P \vee Q) \wedge (\neg P \vee \neg Q)) \wedge (P \vee Q) \equiv P$$

Consider,

$\neg((\neg P \vee Q) \wedge (\neg P \vee \neg Q)) \wedge (P \vee Q) \equiv P$	Reasons
$\Rightarrow ((P \wedge \neg Q) \vee (P \wedge Q)) \wedge (P \vee Q)$	(Demorgan's law)
$\Rightarrow ((Q \wedge P) \vee (\neg Q \wedge P)) \wedge (P \vee Q)$	(Commutative law)
$\Rightarrow ((Q \vee \neg Q) \wedge P) \wedge (P \vee Q)$	(Distributive law)
$\Rightarrow (T \wedge P) \wedge (P \vee Q)$	$(P \vee \neg P \Rightarrow T)$
$\Rightarrow P \wedge (P \vee Q)$	$(P \wedge T = P)$
$\Rightarrow P$	(Absorption law)

Obtain DNF of $Q \vee (P \wedge R) \wedge \neg((P \vee R) \wedge Q)$.

Solution:

$$\begin{aligned}
 & Q \vee (P \wedge R) \wedge \neg((P \vee R) \wedge Q) \\
 & \Leftrightarrow (Q \vee (P \wedge R)) \wedge (\neg((P \vee R) \wedge Q)) \quad (\text{Demorgan law}) \\
 & \Leftrightarrow (Q \vee (P \wedge R)) \wedge ((\neg P \wedge \neg R) \vee \neg Q) \quad (\text{Demorgan law}) \\
 & \Leftrightarrow (Q \wedge (\neg P \wedge \neg R)) \vee (Q \wedge \neg Q) \vee ((P \wedge R) \wedge \neg P \wedge \neg R) \vee ((P \wedge R) \wedge \neg Q) \\
 & \quad \quad \quad (\text{Extended distributed law}) \\
 & \Leftrightarrow (\neg P \wedge Q \wedge \neg R) \vee F \vee (F \wedge R \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \quad (\text{Negation law}) \\
 & \Leftrightarrow (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \quad (\text{Negation law})
 \end{aligned}$$

Obtain the conjunctive normal form of $P \square Q$

$$P \square Q \quad \square \quad (P \square Q) \square (Q \square P)$$

$$\square(\square P \square Q) \square (\square Q \square P)$$

Obtain Pcnf and Pdnf of the formula $(\neg P \vee \neg Q) \rightarrow (P \leftrightarrow \neg Q)$

Solution:

Let $S = (\neg P \vee \neg Q) \rightarrow (P \leftrightarrow \neg Q)$

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$P \leftrightarrow \neg Q$	S	Minterm	Maxterm
T	T	F	F	F	F	T	$P \wedge Q$	
T	F	F	T	T	T	T	$P \wedge \neg Q$	
F	T	T	F	T	T	T	$\neg P \wedge Q$	
F	F	T	T	T	F	F		$P \vee Q$

PCNF: $P \vee Q$ and PDNF: $(P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$

Obtain the PDNF and PCNF of $P \vee (\neg P \rightarrow (Q \vee (\neg Q \rightarrow R)))$.

Solution:

$$P \vee (\neg P \rightarrow (Q \vee (\neg Q \rightarrow R)))$$

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

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

$$S = (P \vee Q \vee R)$$

$$\neg S = (\neg P \vee \neg Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee \neg Q \vee \neg R)$$

$$\wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee \neg R) \wedge (P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R)$$

$$\neg \neg S = \neg((\neg P \vee \neg Q \vee R) \wedge (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee \neg Q \vee \neg R)$$

$$\wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee \neg R) \wedge (P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R))$$

$$= (P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge \neg R) \vee (P \wedge Q \wedge R)$$

$$\vee (\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R)$$

Show that $R \rightarrow S$ can be derived from the premises $P \rightarrow (Q \rightarrow S)$, $\neg R \vee P$ & Q

Solution:

R	Assumed premises
$\neg R \vee P$	Rule P
$R \rightarrow P$	Rule T
P	Rule T
$P \rightarrow (Q \rightarrow S)$	Rule P
$Q \rightarrow S$	Rule P
Q	Rule P
S	Rule T
$R \rightarrow S$	Rule CP

Show that the following statements constitute a valid argument.

If there was rain, then traveling was difficult. If they had umbrella, then traveling was not difficult

They had umbrella. Therefore there was no rain.

Solution:

Let P : There was rain Q : Traveling was difficult R : They had umbrella

Then, the given statements are symbolized as

(1) $P \rightarrow Q$ (2) $R \rightarrow \sim Q$ (3) R

Conclusion : $\sim P$

1) R	Rule P
2) $R \rightarrow \sim Q$	Rule P
3) $\sim Q$	Rule T,1,2
4) $P \rightarrow Q$	Rule P
5) $\sim P$	Rule T,3,4

Therefore, it is a valid conclusion.

Symbolize the following statements:

- (a) All men are mortal
- (b) All the world loves a lover
- (c) X is the father of mother of Y
- (d) No cats has a tail
- (e) Some people who trust others are rewarded

Solution:

(a) Let $M(x)$: x is a man $H(x)$: x is Mortal
 $(\forall x) (M(x) \supset H(x))$

(b) Let $P(x)$: x is a person $L(x)$: x is a lover $R(x,y)$: x loves y
 $(\forall x) (P(x) \supset (\forall y) (P(y) \supset L(y) \supset R(x,y)))$

(c) Let $P(x)$: x is a person $F(x,y)$: x is the father of y
 $M(x,y)$: x is the mother of y
 $(\forall z) (P(z) \supset F(x,z) \supset M(z,y))$

(d) Let $C(x)$: x is a cat $T(x)$: x has a tail

$(\forall x) (C(x) \supset \neg T(x))$

(e) Let $P(x)$: x is a person $T(x)$: x trust others $R(x)$: x is rewarded
 $(\forall x) (P(x) \supset T(x) \supset R(x))$

Show that the following premises are inconsistent.

- (1) If Nirmala misses many classes through illness then he fails high school.
- (2) If Nirmala fails high school, then he is uneducated.
- (3) If Nirmala reads a lot of books then he is not uneducated.
- (4) Nirmala misses many classes through illness and reads a lot of books.

Solution:

E : Nirmala misses many classes

S: Nirmala fails high school

A: Nirmala reads lot of books

H: Nirmala is uneducated

Statement:

$$(1) E \rightarrow S$$

$$(2) S \rightarrow H$$

$$(3) A \rightarrow \sim H$$

$$(4) E \wedge A$$

Premises are : $E \rightarrow S$, $S \rightarrow H$, $A \rightarrow \sim H$, $E \wedge A$

1) $E \rightarrow S$	Rule P
2) $S \rightarrow H$	Rule P
3) $E \rightarrow H$	Rule T, 1,2
4) $A \rightarrow \sim H$	Rule P
5) $H \rightarrow \sim A$	Rule T,4
6) $E \rightarrow \sim A$	Rule T,3,5
7) $\sim E \vee \sim A$	Rule T,6
8) $\sim(E \wedge A)$	Rule T,7
9) $E \wedge A$	Rule P
10) $(E \wedge A) \wedge \sim(E \wedge A)$	Rule T,8,9

Which is nothing but false

Therefore given set of premises are inconsistent

Let p, q, r be the following statements:

p: I will study discrete mathematics

q: I will watch T.V.

r: I am in a good mood.

Write the following statements in terms of p, q, r and logical connectives.

(1) If I do not study and I watch T.V., then I am in good mood.

(2) If I am in good mood, then I will study or I will watch T.V.

(3) If I am not in good mood, then I will not watch T.V. or I will study.

(4) I will watch T.V. and I will not study if and only if I am in good mood.

Solution:

$$(1) (\neg p \wedge q) \rightarrow r$$

$$(2) r \rightarrow (p \vee q)$$

$$(3) \neg r \rightarrow (\neg q \vee p)$$

$$(4) (q \wedge \neg p) \leftrightarrow r$$

Use the indirect method to prove that the conclusion $\exists zQ(z)$ follows from the premises

$\forall x(P(x) \rightarrow Q(x))$ and $\exists yP(y)$

Solution:

1	$\neg \exists zQ(z)$	P(assumed)
2	$\forall z\neg Q(z)$	T, (1)
3	$\exists yP(y)$	P
4	$P(a)$	ES, (3)
5	$\neg Q(a)$	US, (2)
6	$P(a) \wedge \neg Q(a)$	T, (4),(5)
7	$\neg(P(a) \rightarrow Q(a))$	T, (6)
8	$\forall x(P(x) \rightarrow Q(x))$	P
9	$P(a) \rightarrow Q(a)$	US, (8)
10	$P(a) \rightarrow Q(a) \wedge \neg(P(a) \rightarrow Q(a))$	T,(7),(9) contradiction

Show that $(\exists x) (P(x) \wedge Q(x)) \Rightarrow (\exists x) P(x) \wedge (\exists x) Q(x)$

Solution:

1) $(\exists x) (P(x) \wedge Q(x))$	Rule P
2) $P(a) \wedge Q(a)$	ES, 1
3) $P(a)$	Rule T, 2
4) $Q(a)$	Rule T, 2
5) $(\exists x) P(x)$	EG, 3
6) $(\exists x) Q(x)$	EG, 4
7) $(\exists x) P(x) \wedge (\exists x) Q(x)$	Rule T, 5, 6



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES

DEPARTMENT OF MATHEMATICS

UNIT –III–DISCRETE MATHEMATICS – SMTA1307

UNIT-III-SEMIGROUPS AND MONOIDS

Semigroups, Monoids, Homomorphism of Semigroups and Monoids, Subsemigroups and Submonoid.

Semigroup: Let S be a non- empty set with a binary operation $*$ defined on it. The algebraic system $(S, *)$ is called a semigroup if $*$ is associative.

$$(i.e) a * (b * c) = (a * b) * c \quad \forall a, b, c \in S$$

Examples:

1. $(2\mathbb{Z}, +)$ and $(2\mathbb{Z}, \cdot)$ are semigroups.
2. If S is the set of all $n \times n$ matrices with real entries, then $(S, +)$ and (S, \cdot) are semigroups, where $+$ is matrix addition and \cdot is matrix multiplication.
3. $(\mathbb{Z}, -)$ is not a semigroup because $' - '$ is not associative, since $2 - (3 - 4) \neq (2 - 3) - 4$

Monoid: A semigroup $(M, *)$ with identity element e is called a monoid. Sometimes a monoid is denoted as $(M, *, e)$ indicating the fact that e is the identity element.

Examples:

1. (\mathbb{N}, \times) is a monoid with identity element 1 . But $(\mathbb{N}, +)$ is not a monoid, since identity for $+$ is 0 , which is not in \mathbb{N} .
2. The set of non-negative integers $S = \mathbb{N} \cup \{0\}$ is the monoid under $+$ and \times . (i.e) $(S, +)$ and (S, \times) are monoids with identity 0 and 1 .
3. Let S be the non-empty set and let S^S denote the set of all mappings from S to S . Let \circ denote the composition of functions operation.

If $f, g \in S^S$, then f and g are functions from $S \rightarrow S$. Their composite $(f \circ g)(x) = f(g(x)) \forall x \in S$. Then $f \circ g$ is a function from $S \rightarrow S$ and $f \circ g \in S^S$. We know composition function is associative.

The identity function $I : S \rightarrow S$ defined by $I(x) = x \quad \forall x \in S$ is the identity element of S^S . For $(I \circ f)(x) = I(f(x)) = f(x) \forall x \in S$ and $(f \circ I)(x) = f(I(x)) = f(x) \forall x \in S$

$\therefore I \circ f = f \circ I = f \quad \forall f \in S^S \therefore (S^S, \circ)$ is a monoid with identity I .

Sub semigroups: Let $(S, *)$ be a semigroup and let $T \subseteq S$ be a non-empty subset. If T is closed under $*$, then $(T, *)$ is called a sub semigroup.

Submonoid: Let $(M, *)$ be monoid and e be the identity. If T be a non-empty subset of M and if T is closed under $*$ with $e \in T$, then $(T, *)$ is called a submonoid of $(M, *)$.

Examples:

1. (N, \times) is a semigroup. Let $T = 3N$ then $T \subset S$, if $x, y \in T$ then $x = 3r, y = 3s$ for some positive integers r and s . Now $x \times y = 3r \times 3s = 3(3rs) \in 3N = T$. $\therefore T$ is closed under \times .
Hence (T, \times) is a sub semigroup of (N, \times) . More generally, if $S = mN$, where m is a fixed positive integer, then (S, \times) is a sub semigroup.
2. For the semigroup $(N, +)$, $(2N, +)$ is a sub semigroup.
3. $(Z, +)$ is monoid with identity 0. If $T =$ the set of all non-negative integers $= \{0, 1, 2, 3, \dots\}$, then $(T, +)$ is a submonoid with identity 0.

Cyclic Monoid: A monoid $(M, *)$ having identity is said to be cyclic if there exists an element $a \in M$ such that every element $x \in M$ can be written as $a^n = e$ for some $n \in N$. Then 'a' is called a generator of M . Any cyclic monoid is commutative.

Problems:

1. For any commutative monoid $(M, *)$, prove that the set of all idempotent elements of M forms a submonoid.

Solution: Given $(M, *)$ be a commutative monoid.

Let e be its identity element.

Let S be the set of all idempotent elements of M . (i.e) $S = \{x \in M / x * x = x\}$

Since $e * e = e$, e is an idempotent element of M .

$\therefore e \in S$ and hence S is non-empty.

Let $a, b \in S$ be any two elements. They are idempotent elements.

$\therefore a * a = a$ and $b * b = b$.

We have to prove $a * b$ is idempotent.

Now $(a * b) * (a * b) = a * (b * a) * b$ [Since $*$ is associative

$$= a * (a * b) * b \text{ [Since } * \text{ is commutative}$$

$$= (a * a) * (b * b) \text{ [Since } * \text{ is associative}$$

$$= a * b$$

Hence $a * b$ is idempotent and so S is closed under $*$ and $e \in S$.

So $(S, *)$ is a submonoid of $(M, *)$.

2. Show that every finite semigroup has an idempotent element.

Solution: Let $(S, *)$ be a finite semigroup.

Let $a \in S$, then by closure a, a^2, a^3, a^4, \dots are all elements of S .

Since S is finite, these elements are not all different. So we have repetitions.

Let $a^m = a^r$, where $r > m$. Let $r = m + n$.

$$\therefore a^m = a^r = a^{m+n}$$

$$\text{Then } a^m * a^n = a^{m+n} * a^n \Rightarrow a^{m+n} = a^{m+2n}$$

$$\text{And } a^{m+n} * a^n = a^{m+2n} * a^n \Rightarrow a^{m+2n} = a^{m+3n} \text{ and so on.}$$

$$\therefore a^m = a^{m+n} = a^{m+2n} = a^{m+3n} = \dots = a^{m+mn}$$

$$\text{Since } a^m = a^{m+mn}$$

$$\text{We have } a^{nm} = a^{nm+mn} \text{ [Replacing m by nm]}$$

$$= a^{nm} * a^{mn}$$

This proves that a^{nm} is an idempotent element of S.

\therefore Every finite semigroup has an idempotent element.

3. Show that the set of all invertible elements of a monoid form a group under the same operation as that of the monoid.

Solution: Let $(M, *)$ be a monoid having the identity e .

Let G be the set of all invertible elements of M .

Since $e^{-1} = e$, we have $e \in G$. So G is non- empty. Further inverse is unique.

Let $a, b \in G$, then a and b have inverse. Let a^{-1}, b^{-1} be their inverses.

We have to prove that $a * b \in G$.

So we have to prove that it is invertible.

$$\text{Now consider } (a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$$

$$= a * (e) * a^{-1}$$

$$= a * a^{-1}$$

$$= e$$

$$\text{And } (b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$$

$$= b^{-1} * (e) * b$$

$$= b^{-1} * b = e$$

$\therefore b^{-1} * a^{-1}$ is the inverse of $a * b$.

(i.e) $a * b$ is invertible.

Hence $a * b \in G$. So G is closed under $*$.

Associativity: Since G is a subset of M , associativity is inherited in G .

Identity: $e \in G$ is the identity. Since $a * e = e * a = a$, $\forall a \in G$.

Inverse: Let $a \in G$ be any element. So ' a ' is invertible.

$$\therefore a * a^{-1} = a^{-1} * a = e \Rightarrow (a^{-1})^{-1} * a^{-1} = a^{-1} * (a^{-1})^{-1} = e \text{ [Since } (a^{-1})^{-1} = a$$

Since a^{-1} is invertible and so $a^{-1} \in G$.

Hence inverse exists for every $a \in S$. So $(G, *)$ is a group.

4. If \mathbf{Z}_6 is the set of equivalence classes generated by the equivalence relation “Congruence modulo 6”, prove that (\mathbf{Z}_6, \times_6) is a monoid where the operation \times_6 on \mathbf{Z}_6 is defined as $[j] \times_6 [k] = [(j \times k) \bmod 6]$ for any $[j], [k] \in \mathbf{Z}_6$.

Solution: We know $\mathbf{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. We shall form the composition table.

\times_6	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

$\therefore \mathbf{Z}_6$ is closed under \times_6 .

Associativity: Since $[a] \times_6 [b] \times_6 [c] = [a] \times_6 [bc]$

$$= [a(bc) \bmod 6]$$

\times_6 depends on associativity of usual multiplication. $\therefore \times_6$ is associative.

Identity: From the table we find, $[1] \times_6 [a] = [a]$ for all $[a] \in \mathbf{Z}_6$.

$\therefore [1]$ is the identity element. Hence (\mathbf{Z}_6, \times_6) is a monoid.

Homomorphism: Homomorphism is a structure preserving map between two algebraic systems of same type. Homomorphisms of semigroups and monoids are useful in the economical design of sequential machines and in formal languages.

Homomorphism of semigroups: Let $(S, *)$ and (T, \cdot) be two semigroups. A mapping $f : S \rightarrow T$ is called homomorphism if $f(a * b) = f(a) \cdot f(b) \quad \forall a, b \in S$.

The homomorphism of semigroups f is called a monomorphism if f is one-one.

f is called epimorphism if f is onto.

f is called an isomorphism if f is one-one and onto.

If f is an isomorphism of S onto T , we say S is isomorphic to T as semigroups.

Example: Consider the semigroups $(\mathbf{N}, +)$ and $(\mathbf{Z}_m, +_m)$. Define $f : \mathbf{N} \rightarrow \mathbf{Z}_m$ by $f(a) = [a]$ then $f(a + b) = [a + b] = [a] +_m [b] = f(a) +_m f(b)$.

$\therefore f$ is a semigroup homomorphism.

Monoid Homomorphism: Let $(M, *)$ be a monoid with identity e and (T, \cdot) be a monoid with identity e' . A mapping $f : M \rightarrow T$ is called a homomorphism of monoids if

$$f(a * b) = f(a) \cdot f(b) \quad \forall a, b \in M \text{ and } f(e) = e'.$$

The homomorphism of monoids f is called

- (i) a monomorphism if f is one-one
- (ii) an epimorphism if f is onto
- (iii) an isomorphism if f is one-one and onto.

Theorem 1: Let $(S, *)$ be a semigroup and (T, \cdot) be an algebraic system. If $f : S \rightarrow T$ is an onto homomorphism, then (T, \cdot) is also a semigroup.

Proof: Given $(S, *)$ is a semigroup and $f : S \rightarrow T$ is an onto homomorphism.

$$(i.e) f(a * b) = f(a) \cdot f(b)$$

To prove (T, \cdot) is a semigroup, we have to prove (\cdot) is associative.

Let $x, y, z \in T$ be any three elements. Since f is onto, we can find pre images $a, b, c \in S$ such that $f(a) = x, f(b) = y, f(c) = z$

$$\text{Now } f[a * (b * c)] = f(a) \cdot f(b * c) = f(a) \cdot (f(b) \cdot f(c)) = x \cdot (y \cdot z) \text{ and } f[(a * b) * c] = f(a * b) \cdot f(c) = (f(a) \cdot f(b)) \cdot f(c) = (x \cdot y) \cdot z$$

$$\text{Since } a * (b * c) = (a * b) * c, f[a * (b * c)] = f[(a * b) * c].$$

$$\therefore x \cdot (y \cdot z) = (x \cdot y) \cdot z, \forall x, y, z \in T.$$

Hence (T, \cdot) is a semigroup.

Theorem 2: Let $(S, *)$ and (T, \cdot) be semigroups and $g : S \rightarrow T$ be a homomorphism. If $a \in S$ is an idempotent element. Prove that $g(a)$ is an idempotent element of T .

Proof: Given $g : S \rightarrow T$ is a homomorphism of semigroups and $a \in S$ is an idempotent element.

$$\therefore a * a = a \Rightarrow g(a * a) = g(a) \Rightarrow g(a) \cdot g(a) = g(a) \text{ [Since } g \text{ is a homomorphism]}$$

$$\therefore g(a) \text{ is an idempotent element of } T.$$

Theorem 3: If $(M, *)$ is a monoid having identity e and g is an epimorphism from $(M, *)$ to an algebraic system (T, \cdot) , then (T, \cdot) is a monoid.

Proof: Given $(M, *)$ is a monoid with identity e .

$$\therefore (M, *) \text{ is a semigroup and } g : M \rightarrow T \text{ is an epimorphism.}$$

(i.e) an onto homomorphism.

$\therefore (T, \cdot)$ is also a semigroup. [By theorem 1

We have to only prove (T, \cdot) has identity.

Let $a \in M$ be any element and $e \in M$ is the identity.

$$\therefore a * e = a = e * a$$

Now $a * e = a \Rightarrow g(a * e) = g(a) \Rightarrow g(a).g(e) = g(a)$ and
 $e * a = a \Rightarrow g(e * a) = g(a) \Rightarrow g(e).g(a) = g(a)$

$g(a).g(e) = g(e).g(a) = g(a) \Rightarrow g(e)$ is the identity of (T, \cdot) and hence (T, \cdot) is a monoid.

Theorem 4: Let $(S, *)$, (T, \cdot) and (V, \oplus) be semigroups and $g : S \rightarrow T, h : T \rightarrow V$ be semigroup homomorphism such that their composite $h \circ g : S \rightarrow V$ is defined. Prove that $h \circ g$ is a semigroup homomorphism of $(S, *)$ to (V, \oplus) .

Proof: Given $g : S \rightarrow T, h : T \rightarrow V$ are semigroup homomorphisms.

We have to prove $h \circ g : S \rightarrow V$ is a homomorphism.

Let $a, b \in S$ be any two elements.

$$\begin{aligned} \therefore (h \circ g)(a * b) &= h(g(a * b)) = h(g(a).g(b)) = h(g(a)) \oplus h(g(b)) \\ &= (h.g)(a) \oplus (h.g)(b) \end{aligned}$$

$\therefore h \circ g$ is a homomorphism of semigroups.

Theorem 5: The set of all semigroup endomorphisms of a semigroup is a semigroup under the operation of composition.

Proof: Let G be the set of all endomorphisms of the semigroup $(S, *)$.

An endomorphism is a homomorphism of $S \rightarrow S$ and so G is the set of all homomorphisms from S to S .

We have to prove (G, \circ) is a semigroup where \circ is composition of functions.

Let $g_1, g_2 \in G$ be any two elements. (i.e) g_1, g_2 are endomorphisms of S .

$$\begin{aligned} \therefore (g_1 \circ g_2)(a * b) &= g_1(g_2(a * b)) = g_1(g_2(a) * g_2(b)) = g_1(g_2(a)) * g_1(g_2(b)) \\ &= (g_1 \circ g_2)(a) * (g_1 \circ g_2)(b) \end{aligned}$$

$\therefore (g_1 \circ g_2)$ is a homomorphism of $S \rightarrow S$ and hence an endomorphism.

$\therefore (g_1 \circ g_2) \in G$. Hence G is closed under the operation (\circ) .

Next we shall prove that (\circ) is associative.

Let $g_1, g_2, g_3 \in G$ be any three endomorphisms of s .

To prove $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$

Now for $a \in S$, we have,

$$(g_1 \circ (g_2 \circ g_3))(a) = g_1(a) * (g_2 \circ g_3)(a) = g_1(a) * [g_2(a) * g_3(a)] \text{ and}$$

$$((g_1 \circ g_2) \circ g_3)(a) = (g_1 \circ g_2)(a) * g_3(a) = g_1(a) * [g_2(a) * g_3(a)]$$

Since $g_1(a)$, $g_2(a)$, $g_3(a)$ are elements of S and $*$ is associative, we have

$$g_1(a) * [g_2(a) * g_3(a)] = g_1(a) * [g_2(a) * g_3(a)]$$

$$\therefore (g_1 \circ (g_2 \circ g_3))(a) = ((g_1 \circ g_2) \circ g_3)(a), \text{ for any } a \in S.$$

$\Rightarrow g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$. Hence (\circ) is associative and so (G, \circ) is a semigroup.

Theorem 6: Let $(S, *)$ be a semigroup and S^S be the set of all functions from S to S . Then (S^S, \cdot) is a semigroup under composition of functions. Prove that there is a homomorphism $g : S \rightarrow S^S$.

Proof: For each $a \in S$, we shall identify a function $f_a : S \rightarrow S$, defined by

$$f_a(x) = a * x \quad \forall x \in S$$

$$\therefore f_a \in S^S$$

Define $g : S \rightarrow S^S$ by $g(a) = f_a \quad \forall a \in S$

Let $a, b \in S$ be any two elements, then $a * b \in S$

$$\therefore g(a * b) = f_{a * b}$$

But for any $x \in S$, $f_{a * b}(x) = (a * b) * x = a * (b * x) = f_a(b * x) = f_a(f_b(x)) = (f_a \cdot f_b)(x)$

$$\therefore f_{a * b} = f_a \cdot f_b$$

Hence $g(a * b) = f_{a * b} = f_a \cdot f_b = g(a) \cdot g(b)$

$$\therefore g \text{ is a homomorphism of } (S, *) \text{ into } (S^S, \cdot).$$

Theorem 7: Show that monoid homomorphism preserves the property of invertibility.

Proof: Let $(M, *)$ and (M', \cdot) be two monoids with identity e and e' respectively.

Let $g : M \rightarrow M'$ be a homomorphism.

Let $a \in M$ be an element with inverse a^{-1} .

We have to prove $g(a^{-1}) = [g(a)]^{-1}$. Since a^{-1} is the inverse of a , we have

$$a * a^{-1} = a^{-1} * a = e.$$

Now $a * a^{-1} = e \Rightarrow g(a * a^{-1}) = g(e) = e' \Rightarrow g(a) \cdot g(a^{-1}) = e'$

Similarly, $a^{-1} * a = e \Rightarrow g(a^{-1} * a) = g(e) = e' \Rightarrow g(a^{-1})g(a) = e'$

Hence $g(a^{-1})$ is the inverse of $g(a)$

(i.e) $g(a^{-1}) = [g(a)]^{-1}$.



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES
DEPARTMENT OF MATHEMATICS

UNIT – IV–DISCRETE MATHEMATICS – SMT1304

UNIT – IV- LATTICES

Lattices as Partially Ordered Set, Properties of Lattices, Lattices as Algebraic Systems, Sublattices, Direct Product and Homomorphism.

Definition: The relation f defined on a nonempty set X is called an anti-symmetric relation if and only if, $\forall x, y \in X$, the property $(x, y) \in f$ and $(y, x) \in f$ implies that $x = y$.

It is possible to interpret an anti-symmetric relation using the arrow diagrams of relations.

In this context, a relation is called anti-symmetric if, whenever there is an arrow going from one element to an element different from it, there does not exist an arrow going back from the second element to the first.

Example: Let $R_1 = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x \text{ divides } y\}$ and $R_2 = \{(x, y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \mid x \text{ divides } y\}$.
(a) Show that R_1 is an anti-symmetric relation on the set of positive integers. (b) Show that R_2 is not an anti-symmetric relation on the set of integers by giving a counter example.

There are two relations which play a prominent role in mathematics. One of them is the equivalence relation, which we have already seen is a relation which is reflexive, symmetric and transitive.

We now introduce the other relation called a partial order.

Definition: A relation f on a nonempty set X is called a partial order if f is reflexive, transitive and anti-symmetric. Here (X, f) is a partially ordered set and is colloquially referred to as a poset.

The relation less than or equal to on the set of real numbers and the relation subset on the set of sets are two fundamental partial orders. These can be thought of as models for the general partial order. It is common practice to use the symbol \leq to denote a partial order.

Further, if (X, \leq) is a poset and $x \leq y$, then we read this as x is less than or equal to y .

Definition: Let (X, \leq) be a poset. If there exist elements x and y in X , such that either $(x, y) \in \leq$ or $(y, x) \in \leq$ holds, then x and y are said to be comparable. In neither (x, y) nor (y, x) belongs to \leq , then x and y are said to be incomparable.

Example1: Let $X = \{1, 2, 3, 4, 5\}$.

(a) The identity relation Id on X is reflexive, transitive and anti-symmetric and is therefore a partial order. However, no two elements of X are comparable.

(b) The relation $\text{Id} \cup \{(1, 2)\}$ is also a partial order on X . Here 1 and 2 are comparable.

(c) The relation $= \text{Id} \cup \{(1, 2), (2, 1)\}$ is both reflexive and transitive, but not anti-symmetric. Observe that $(1, 2), (2, 1) \in =$ and $1 \neq 2$.

(d) The relation $\text{Id} \cup \{(1, 2), (3, 4)\}$ is a partial order on X . Here, 1 and 2 are comparable and so are 3 and 4.

Example: Let $X = \mathbb{N}$. The relation $= \{(a, b) : a \text{ divides } b\}$ is a partial order on X .

Example: Let X be a nonempty collection of sets. Here, $= \{(A, B) : A, B \in X, A \subseteq B\}$ is a partial order on X . 4. On \mathbb{R} the set $= \{(a, b) : a \leq b\}$ is a partial order. It is called the usual partial order on \mathbb{R} .

Definition: Let (X, \leq) be a poset. 1. If any two elements in the poset (X, \leq) are comparable, then \leq is called a linear order and (X, \leq) is called a linearly ordered set.

Often a linear order is also referred to as a total order or a complete order.

A subset, C of X , is called a chain if and only if it induces a linear order on C . If C is a finite set, then the length of C is equal to the number of elements of C . If C is not a finite set, then the length of C is said to be infinite.

A subset, A of X , is called an antichain if and only if no two elements of A are comparable. The length of an antichain is defined in precisely the same manner as that of the chain.

The maximum of the lengths of the chains of X is called the height of X and the maximum of the lengths of the antichains of X is called the width of X .

Let X be a nonempty set and let f be a relation on X . Then, recall from Definition, that f is reflexive if $(x, x) \in f$ for all $x \in X$; f is transitive if $(x, y) \in f$ and $(y, z) \in f$ imply $(x, z) \in f$ for all $x, y, z \in X$; and f is anti-symmetric if $(x, y) \in f$ and $x \neq y$ implies $(y, x) \notin f$, i.e., for all distinct elements x, y of X both (x, y) and (y, x) cannot be in f . Relations which are simultaneously reflexive, transitive and anti-symmetric play an important role in mathematics; and we give a name to such relations.

Definition: Let X be a nonempty set. A relation f on X is called a partial order if f is reflexive, transitive and anti-symmetric. Let f be a partial order on X and let $a, b \in X$. Then, a and b are said to be comparable (with respect to the partial order f) if either $(a, b) \in f$ or $(b, a) \in f$. When a partial order satisfies some other desirable properties, they are given different names. We fix some of these in the following definition.

Definition: Let X be a nonempty set.

1. The pair (X, f) is called a partially ordered set (in short, poset) if f is a partial order on X .
2. A partial order f on X is called a linear order if either $(x, y) \in f$ or $(y, x) \in f$ for all $x, y \in X$, i.e., when any two elements of X are comparable. A linear order is also called a total order, or a complete order.
3. The poset (X, f) is said to be a linearly ordered set if f is a linear order on X .
4. A linearly ordered subset of a poset is called a chain in the poset. The maximum size of a chain in a poset is called the height of a poset.
5. Let (X, f) be a poset and let $A \subseteq X$. A is called an anti-chain in the poset if no two elements of A are comparable.

The maximum size of an anti-chain in a poset is called the width of the poset. You may imagine the elements of a linearly ordered set as points on a line. The height of a poset is the maximum of the cardinalities of all chains in the poset. The width of a poset is the maximum of the cardinalities of all anti-chains in the poset.

Examples:

1. The poset in Example 1 has height 1 (size of the chain $\{1\}$) and width 5 (size of the anti-chain $\{1, 2, 3, 4, 5\}$).

2. The poset in Example 1 has height 2 (respective chain is $\{1, 2\}$) and width 4 (respective anti-chains are $\{2, 3, 4, 5\}$ and $\{1, 3, 4, 5\}$).
3. The poset in Example 1 has height 2 (respective chains are $\{1, 2\}$ and $\{3, 4\}$) and width 3 (a respective anti-chain is $\{1, 3, 5\}$).
4. The usual order (usual \leq) in N is a linear/complete/total order. The same holds for the usual order in Z , Q and R .
5. If (X, f) is a finite linearly ordered set then the singleton subsets of X are the only anti-chains.

In this case, the height of X is the number of elements in X and the width of X is 1.

6. The set N with the partial order f defined by “ $(a, b) \in f$ if a divides b ” is not linearly ordered. However, the set $\{1, 2, 4, 8, 16\}$ is a chain. This is just a linearly ordered subset of the poset.

There are larger chains, for example, $\{2^k : k = 0, 1, 2, \dots\}$. The set of all primes is an anti-chain here. The poset (N, f) has infinite height and infinite width.

7. The poset $(P(\{1, 2, 3, 4, 5\}), \subseteq)$ is not linearly ordered. However, $\{\emptyset, \{1, 2\}, \{1, 2, 3, 4, 5\}\}$ is a chain in it. Also, $\{\emptyset, \{2\}, \{2, 3\}, \{2, 3, 4\}, \{2, 3, 4, 5\}, \{1, 2, 3, 4, 5\}\}$ is a chain. The height of this poset is 6.

That is, if f is a partial order on a nonempty set X we write $x \leq y$ to mean that $(x, y) \in f$. Accordingly, the poset (X, f) is written as (X, \leq) . Also, instead of writing ‘ (X, f) is a poset’ we will often write ‘ X is a poset with the partial order f ’. Following custom, by $x \geq y$ we mean $y \leq x$; by $x < y$ we mean that $x \leq y$ and $x \neq y$; by $x > y$ we mean $y < x$. Also, we read $x \leq y$ as x is less than or equal to y ; $x < y$ as x is less than y ; $x \geq y$ as x is greater than or equal to y ; and $x > y$ as x is larger than y .

Definition: Let (Σ, \leq) be a finite linearly ordered set (like the English alphabet with $a < b < c < \dots < z$) and let Σ^* be the collection of all words formed using the elements of Σ . For $a = a_1 a_2 \dots a_n$, $b = b_1 b_2 \dots b_m \in \Sigma^*$ for $m, n \in N$, define $a \leq b$ if (a) $a_1 < b_1$, or (b) $a_i = b_i$ for $i = 1, \dots, k$ for some $k < \min\{m, n\}$ and $a_{k+1} < b_{k+1}$, or (c) $a_i = b_i$ for $i = 1, 2, \dots, n = \min\{m, n\}$. Then (Σ^*, \leq) is a linearly ordered set. This ordering is called the lexicographic or dictionary ordering. Sometimes Σ is called the alphabet and the linearly ordered set Σ^* is called the dictionary.

A directed graph representation of the poset (A, \leq) with $A = \{1, 2, 3, 9, 18\}$ Given a set, X , we can order the subsets of X by the subset relation: $A \subseteq B$, where A, B are any subsets of X .

For example, if $X = \{a, b, c\}$, we have $\{a\} \subseteq \{a, b\}$.

However, note that neither $\{a\}$ is a subset of $\{b, c\}$ nor $\{b, c\}$ is a subset of $\{a\}$.

We say that $\{a\}$ and $\{b, c\}$ are incomparable.

Definition:

A binary relation, \leq , on a set, X , is a partial order (or partial ordering) iff it is reflexive, transitive and antisymmetric,

that is: (1) (Reflexivity): $a \leq a$, for all $a \in X$;

(2) (Transitivity): If $a \leq b$ and $b \leq c$, then $a \leq c$, for all $a, b, c \in X$.

(3) (Antisymmetry): If $a \leq b$ and $b \leq a$, then $a = b$, for all $a, b \in X$.

A partial order is a total order (ordering) (or linear order (ordering)) iff for all $a, b \in X$, either $a \leq b$ or $b \leq a$. When neither $a \leq b$ nor $b \leq a$, we say that a and b are incomparable.

A subset, $C \subseteq X$, is a chain iff \leq induces a total order on C (so, for all $a, b \in C$, either $a \leq b$ or $b \leq a$).

The strict order (ordering), $<$ is the strict order associated with a partial order, \leq , then $<$ is transitive and antireflexive, which means that (4) $a \nless a$, for all $a \in X$.

Conversely, let $<$ be a relation on X and assume that $<$ is transitive and anti-reflexive.

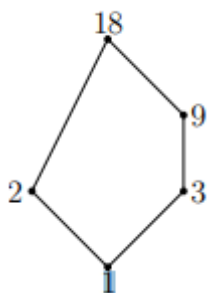
If confusion may arise, for example when we are dealing with several posets, we denote the partial order on X by \leq_X .

The trick is to draw a picture consisting of nodes and oriented edges, where the nodes are all the elements of X and where we draw an oriented edge from a to b iff a is an immediate predecessor of b . Such a diagram is called a Hasse diagram for (X, \leq) .

The Hasse diagram of a finite poset (X, \leq) is a picture drawn in the following way:

1. Each element of X is represented by a point and is labeled with the element.
2. If $a \leq b$ then the point labeled a must appear at a lower height than the point labeled b and further the two points are joined by a line.
3. If $a \leq b$ and $b \leq c$ then the line between a and c is removed.

Example: Hasse diagram for the poset (A, \leq) with $A = \{1, 2, 3, 9, 18\}$ and \leq as the 'divides' relation is given below.



Definition:

Let (X, \leq) be a poset and let $A \subseteq X$.

1. We say that an element $x \in X$ is an upper bound of A if for each $z \in A$, $z \leq x$; or equivalently, when each element of A is less than or equal to x . An element $y \in X$ is called a lower bound of A if for each $z \in A$, $y \leq z$; or equivalently, when y is less than or equal to each element of A .
2. An element $x \in A$ is called the maximum of A , if x is an upper bound of A . Thus, maximum of A is an upper bound of A which is contained in A . Such an element is unique provided it exists. In this case, we denote $x = \max\{z : z \in A\}$. Similarly, minimum of A is an element $y \in A$ which is a lower bound of A . If minimum of A exists, then it is unique; and we write $y = \min\{z : z \in A\}$.

3. An element $x \in X$ is called the least upper bound (lub) of A in X if x is an upper bound of A and for each upper bound y of A , we have $x \leq y$; i.e., when x is the minimum (least) element of the set of all upper bounds of A . Similarly, the greatest lower bound (glb) of A is a lower bound of A which is greater than or equal to all upper bounds of A ; it is the maximum (largest) of the set of all lower bounds of A .

4. An element $x \in A$ is a maximal element of A if $x \leq z$ for some $z \in A$ implies $x = z$; or equivalently, when no element in A is larger than x . An element $y \in A$ is called a minimal element of A if $z \leq y$ for some $z \in A$ implies $y = z$; or equivalently, when no element in A is less than y . **Example:** Consider the two posets $X = \{a, b, c\}$ and $Y = \{a, b, c, d\}$ described by the following Hasse diagrams:



Let $A = X$. Then,

- (a) the maximal elements of A are b and c ,
- (b) the only minimal element of A is a ,
- (c) a is the lower bound of A in X ,
- (d) A has no upper bound in X ,
- (e) A has no maximum element,
- (f) a is the minimum element of A ,
- (g) no element of X is the lub of A , and
- (h) a is the glb of A in X .

Example:

The following table illustrates the definitions by taking different subsets A of X , and also considering the same A as a subset of Y .

	$A = \{b, c\} \subseteq X$	$A = \{a, c\} \subseteq X$	$A = \{b, c\} \subseteq Y$
Maximal element(s) of A	b, c	c	b, c
Minimal element(s) of A	b, c	a	b, c
Lower bound(s) of A in X	a	a	a
Lower bound(s) of A in Y	a	a	a
Upper bound(s) of A in X	does not exist	c	d
Upper bound(s) of A in Y	does not exist	c	d
Maximum element of A	does not exist	c	does not exist
Minimum element of A	does not exist	a	does not exist
lub of A in X	does not exist	c	d
lub of A in Y	does not exist	c	d
glb of A in X	a	a	a
glb of A in Y	a	a	a

Definition: A linear order \leq on a nonempty set X is said to be a well order if each nonempty subset of X has minimum. We call (X, \leq) a well ordered set to mean that \leq is a well order on X .

Often we use the phrase ‘ X is a well ordered set with the ordering as \leq ’ to mean ‘ (X, \leq) is a well ordered set’.

Lattice: A poset (L, \leq) is called a lattice if each pair $x, y \in L$ has an lub and also a glb. A lub of x, y is also written as $x \vee y$ (read as ‘ x or y ’ / ‘join of x and y ’) and a glb of x, y as $x \wedge y$ (read as ‘ x and y ’ / ‘meet of x and y ’). A lattice is a poset in which any two elements have a meet and a join.

A complete lattice is a poset in which any subset has a greatest lower bound and a least upper bound.

It is easy to show that any finite lattice is a complete lattice and that a finite poset is a lattice iff it has a least element and a greatest element.

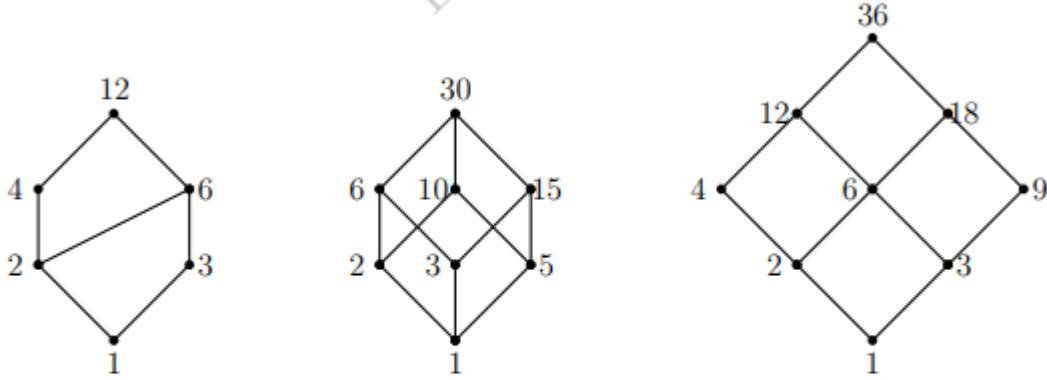
The poset \mathbb{N}^+ under the divisibility ordering is a lattice!

A lattice is called a distributive lattice if for all pairs of elements x, y the following conditions, called distributive laws, are satisfied: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.

Indeed, it turns out that the meet operation corresponds to greatest common divisor and the join operation corresponds to least common multiple.

However, it is not a complete lattice. The power set of any set, X , is a complete lattice under the subset ordering.

Fix a positive integer n and let $D(n)$ denote the set of all divisors of n . For elements $x, y \in D(n)$, define $x \leq y$ if x divides y . Then $(D(n), \leq)$ is a distributive lattice, where $\vee = \text{lcm}$ and $\wedge = \text{gcd}$. For $n = 12, 30$ and 36 , the corresponding lattices are shown below.



To check the first distributive law, let $a, b, c \in D(n)$, p a prime, and let $k \in \mathbb{N}$. Further, let $p^k \mid \text{lcm}\{a, \text{gcd}\{b, c\}\}$. Then, either $p^k \mid a$ or $p^k \mid b, c$. In that case, $p^k \mid \text{lcm}\{a, b\}$ and $p^k \mid \text{lcm}\{a, c\}$. So, $p^k \mid \text{gcd}\{\text{lcm}\{a, b\}, \text{lcm}\{a, c\}\}$.

Now, let us assume that $p^k \nmid \text{gcd}\{\text{lcm}\{a, b\}, \text{lcm}\{a, c\}\}$. Then, $p^k \mid \text{lcm}\{a, b\}$ and $p^k \mid \text{lcm}\{a, c\}$. Then, either $p^k \mid a$ or ($p^k \mid b$ and $p^k \mid c$). So, $p^k \mid \text{lcm}\{a, \text{gcd}\{b, c\}\}$.

Thus, any power of a prime divides $a \vee (b \wedge c)$ if and only if it divides $(a \vee b) \wedge (a \vee c)$. Therefore, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Similarly, the second distributive law can be verified.

Proposition: If X is a lattice, then the following identities hold for all $a, b, c \in X$:

$$\text{L1 } a \vee b = b \vee a, a \wedge b = b \wedge a$$

$$\text{L2 } (a \vee b) \vee c = a \vee (b \vee c), (a \wedge b) \wedge c = a \wedge (b \wedge c)$$

$$\text{L3 } a \vee a = a, a \wedge a = a$$

$$\text{L4 } (a \vee b) \wedge a = a, (a \wedge b) \vee a = a.$$

Properties (L1) correspond to commutativity,

properties (L2) to associativity,

properties (L3) to idempotence and

properties (L4) to absorption.

Furthermore, for all $a, b \in X$, we have $a \leq b$ iff $a \vee b = b$ iff $a \wedge b = a$, called consistency.

Properties (L1)-(L4) are algebraic properties.

Properties: In a lattice (L, \leq) , the following are true:

$$1. [\text{Idempotence}] : a \vee a = a, a \wedge a = a$$

$$2. [\text{Commutativity}] : a \vee b = b \vee a, a \wedge b = b \wedge a$$

$$3. [\text{Associativity}] : a \vee (b \vee c) = (a \vee b) \vee c, a \wedge (b \wedge c) = (a \wedge b) \wedge c$$

4. $a \leq b \Leftrightarrow a \vee b = b$. Similarly, $a \leq b \Leftrightarrow a \wedge b = a$
5. [Absorption] : $a \vee (a \wedge b) = a = a \wedge (a \vee b)$
6. [Isotonicity] : $b \leq c \Rightarrow a \vee b \leq a \vee c$, $b \leq c \Rightarrow a \wedge b \leq a \wedge c$
7. $a \leq b, c \leq d \Rightarrow a \vee c \leq b \vee d$, $a \leq b, c \leq d \Rightarrow a \wedge c \leq b \wedge d$
8. [Distributive Inequality] : $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$
9. [Modularity] : $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$

Proof. We prove only the first parts of all assertions; the second parts can be proved similarly.

(1) $a \vee a$ is an upper bound of $\{a, a\}$.

Hence $a \vee a \geq a$. On the other hand, a is an upper bound of $\{a, a\}$.

So, $a \vee a$ being the least of all upper bounds of $\{a, a\}$, is less than or equal to a .

Hence $a \vee a = a$.

(2) $a \leq b \vee a, b \leq b \vee a$.

So, $b \vee a$ is an upper bound of a, b .

Since $a \vee b$ is the least of all upper bounds of a, b , we have $a \vee b \leq b \vee a$.

Exchanging a and b , we get $b \vee a \leq a \vee b$.

Hence $a \vee b = b \vee a$.

(3) Let $d = a \vee (b \vee c)$.

Then, $d \geq a, d \geq b \vee c$ so that $d \geq a, d \geq b$ and $d \geq c$. So, $d \geq a \vee b$ and $d \geq c$.

That is, $d \geq (a \vee b) \vee c$. Similarly, $e = (a \vee b) \vee c$ implies $e \geq a \vee (b \vee c)$.

Thus, the first part of the result follows.

(4) Let $a \leq b$. As b is an upper bound of $\{a, b\}$, and $a \vee b$ is the least of all upper bounds of $\{a, b\}$, we have $a \vee b \leq b$.

Also, $a \vee b$ is an upper bound of $\{a, b\}$ and hence $a \vee b \geq b$.

So, we get $a \vee b = b$.

Conversely, let $a \vee b = b$.

As $a \vee b$ is an upper bound of $\{a, b\}$, we have $a \leq a \vee b = b$.

Therefore, $a \leq b \Leftrightarrow a \vee b = b$.

(5) By definition $a \wedge b \leq a$. So, $a \vee (a \wedge b) \leq a \vee a = a$ using (1).

Also, by definition $a \vee (a \wedge b) \geq a$.

Hence, $a \vee (a \wedge b) = a$.

(6) Let $b \leq c$. Note that $a \vee c \geq a$ and $a \vee c \geq c \geq b$.

So, $a \vee c$ is an upper bound of $\{a, b\}$.

Thus, $a \vee c \geq \text{lub}\{a, b\} = a \vee b$.

(7) Using (6), we have $a \vee c \leq b \vee c \leq b \vee d$.

Again, using (6), we get $a \wedge c \leq b \wedge c \leq b \wedge d$.

(8) Note that $a \leq a \vee b$ and $a \leq a \vee c$.

Thus, $a = a \wedge a \leq (a \vee b) \wedge (a \vee c)$.

As $b \leq a \vee b$ and $c \leq a \vee c$, by (7), we get $b \wedge c \leq (a \vee b) \wedge (a \vee c)$.

So, by definition $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$.

(9) Let $a \leq c$. Then, $a \vee c = c$ and hence by (8), we have $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$. Conversely, let $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

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

Theorem:

The direct product of two distributive lattices is a distributive lattice. Proof. Let $(a_1, b_1), (a_2, b_2), (a_3, b_3)$ be elements in the direct product of two distributive lattices. Then $[(a_1, b_1) \vee (a_2, b_2)] \wedge (a_3, b_3) = (a_1 \vee a_2, b_1 \vee b_2) \wedge (a_3, b_3) = (a_1 \vee a_2) \wedge a_3, (b_1 \vee b_2) \wedge b_3 = (a_1 \wedge a_3) \vee (a_2 \wedge a_3), (b_1 \wedge b_3) \vee (b_2 \wedge b_3) = (a_1 \wedge a_3), (b_1 \wedge b_3) \vee (a_2 \wedge a_3), (b_2 \wedge b_3) = (a_1, b_1) \wedge (a_3, b_3) \vee (a_2, b_2) \wedge (a_3, b_3)$.

This verifies one of the distributive laws. Similarly, the other one can be verified.

Definition: Let (L_1, \leq_1) and (L_2, \leq_2) be lattices. A function $f : L_1 \rightarrow L_2$ satisfying $f(a \vee_1 b) = f(a) \vee_2 f(b)$ and $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$ is called a lattice homomorphism.

Further, if f is a bijection, then it is called a lattice isomorphism.

Definition:

Let (L, \leq) be a lattice. It is called a bounded lattice if there exist elements $\alpha, \beta \in L$ such that for each $x \in L$, we have $x \leq \alpha$ and $\beta \leq x$. Such an element α is called the largest element of L , and is denoted by 1. The element $\beta \in L$ satisfying $\beta \leq x$ for all $x \in L$ is called the smallest element of L , and is denoted by 0.

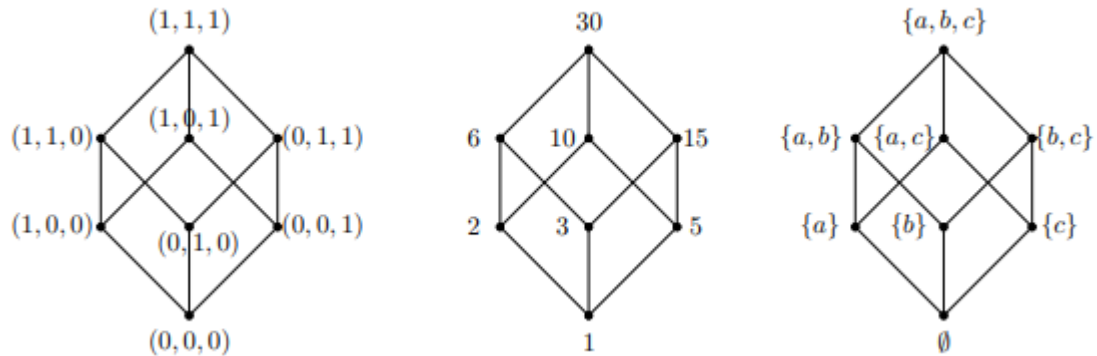
Notice that if a lattice is bounded, then 1 is the lub of the lattice and 0 is the glb of the lattice.

Definition: A lattice (L, \leq) is said to be complete if each nonempty subset of L has lub and glb in L . For $A \subseteq L$, we write lub of A as $\vee A$, and glb of A , as $\wedge A$. It follows that each complete lattice is a bounded lattice.

Examples:

1. The set $[0, 5]$ with the usual order is a lattice which is both bounded and complete. So, is the set $[0, 1) \cup [2, 3]$.
2. The set $(0, 5]$ with the usual order is a lattice which is neither bounded nor complete.

3. The set $[0, 1] \cup (2, 3]$ with the usual order is a lattice which is bounded but not complete.
4. Every finite lattice is complete, and hence, bounded.
5. The set \mathbb{R} with the usual order is a lattice. It is not a complete lattice. Observe that the completeness property of \mathbb{R} , i.e., “for every bounded nonempty subset a glb and an lub exist” is different from the completeness in the lattice sense.



Definition: Let (L, \leq) be a bounded lattice. We say that (L, \leq) is a complemented lattice if for each $x \in L$, there exists $y \in L$ such that $x \vee y = 1$ and $x \wedge y = 0$. Such an element y corresponding to the element x is called a complement of x , and is denoted by $\neg x$.

Theorem: Let (L, \leq) be a lattice and let $a, b, c \in L$. The following table lists the properties that hold (make sense) in the specified type of lattices.

Properties	Lattice type
\vee, \wedge are idempotent	Any lattice
\vee, \wedge are commutative	Any lattice
\vee, \wedge are associative	Any lattice
$a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$	Any lattice
[Absorption] $a \wedge (a \vee b) = a = a \vee (a \wedge b)$	Any lattice
[Isotonicity] $b \leq c \Rightarrow \{a \vee b \leq a \vee c, a \wedge b \leq a \wedge c\}$	Any lattice
[Distributive inequalities] $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$ $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$	Any lattice
[Modular inequality] $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$	Any lattice
0 is unique; 1 is unique	Bounded lattice
If a is a complement of b , then b is also a complement of a	Bounded lattice
$\neg 0$ is unique and it is 1 ; $\neg 1$ is unique and it is 0	Bounded lattice
An element a has a unique complement	Distributive complemented lattice
[Cancellation] $\{a \vee c = b \vee c, a \vee \neg c = b \vee \neg c\} \Rightarrow a = b$ $\{a \wedge c = b \wedge c, a \wedge \neg c = b \wedge \neg c\} \Rightarrow a = b$	Distributive complemented lattice
[De-Morgan] $\neg(a \vee b) = \neg a \wedge \neg b$ $\neg(a \wedge b) = \neg a \vee \neg b$	Distributive complemented lattice
$a \vee \neg b = 1 \Leftrightarrow a \vee b = a$ $a \wedge \neg b = 0 \Leftrightarrow a \wedge b = a$	Distributive complemented lattice

Proof. We will only prove the properties that appear in the last three rows; others are left as exercises.

Cancellation property: $b = b \vee 0 = b \vee (c \wedge \neg c) = (b \vee c) \wedge (b \vee \neg c) = (a \vee c) \wedge (a \vee \neg c) = a \vee (c \wedge \neg c) = a \vee 0 = a$. $b = b \wedge 1 = b \wedge (c \vee \neg c) = (b \wedge c) \vee (b \wedge \neg c) = (a \wedge c) \vee (a \wedge \neg c) = a \wedge (c \vee \neg c) = a \wedge 1 = a$.

De-Morgan's property: $(a \vee b) \vee (\neg a \wedge \neg b) = (a \vee b \vee \neg a) \wedge (a \vee b \vee \neg b) = 1 \wedge 1 = 1$. $(a \vee b) \wedge (\neg a \wedge \neg b) = (a \wedge \neg a \wedge \neg b) \vee (b \wedge \neg a \wedge \neg b) = 0 \vee 0 = 0$.

$(a \wedge b) \vee (\neg a \vee \neg b) = (a \vee \neg a \vee \neg b) \wedge (b \vee \neg a \vee \neg b) = 1 \wedge 1 = 1$.

$(a \wedge b) \wedge (\neg a \vee \neg b) = (a \wedge b \wedge \neg a) \vee (a \wedge b \wedge \neg b) = 0 \wedge 0 = 0$.

Using Definition, on the first two equalities, we get $\neg(a \vee b) = \neg a \wedge \neg b$; and using it again on the last two equalities, we obtain $\neg(a \wedge b) = (\neg a \vee \neg b)$.

To prove the next assertion, note that if $a \vee \neg b = 1$, then $a = a \vee (b \wedge \neg b) = (a \vee b) \wedge (a \vee \neg b) = (a \vee b) \wedge 1 = a \vee b$.

Conversely, if $a = a \vee b$, then $a \vee \neg b = (a \vee b) \vee \neg b = 1$.

Similarly, the second part is proved.



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF SCIENCE AND HUMANITIES
DEPARTMENT OF MATHEMATICS

UNIT –V–DISCRETE MATHEMATICS – SMTA1307

UNIT – V – BOOLEAN ALGEBRA

Boolean Algebra, Basic properties, Sub algebra, Direct Product, and Homomorphism, Boolean Functions.

Definition:

A **Boolean algebra** is a nonempty set S which is closed under the binary operations \vee (called join), \wedge (called meet), and the unary operation \neg (called inverse or complement) satisfying the following properties for all $x, y, z \in S$:

1. [Commutativity] : $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$.
2. [Distributivity] : $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ and $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.
3. [Identity elements] : There exist elements $0, 1 \in S$ such that $x \vee 0 = x$ and $x \wedge 1 = x$.
4. [Inverse] : $x \vee \neg x = 1$ and $x \wedge \neg x = 0$.

When required, we write the Boolean algebra S as (S, \vee, \wedge, \neg) showing the operations explicitly. Notice that the fourth property in the definition above uses the two special elements 0 and 1 , whose existence has been asserted in the third property.

This is meaningful when these two elements are uniquely determined by the third property.

Theorem:

Let S be a Boolean algebra. Then the following statements are true:

1. Elements 0 and 1 are unique.
2. Corresponding to each $s \in S$, $\neg s$ is the unique element in S that satisfies the property: $s \vee \neg s = 1$ and $s \wedge \neg s = 0$.
3. For each $s \in S$, $\neg \neg s = s$.

Proof. (1) Let $0_1, 0_2 \in S$ be such that for each $x \in S$, $x \vee 0_1 = x$ and $x \vee 0_2 = x$.

Then, in particular, $0_2 \vee 0_1 = 0_2$ and $0_1 \vee 0_2 = 0_1$.

By Commutativity, $0_2 \vee 0_1 = 0_1 \vee 0_2$.

So, $0_2 = 0_1$. That is, 0 is the unique element satisfying the property that for each $x \in S$, $0 \vee x = x$.

A similar argument shows that 1 is the unique element that satisfies the property that for each $x \in S$, $x \wedge 1 = x$.

(2) Let $s \in S$. By definition, $\neg s$ satisfies the required properties.

For the converse, suppose $t, r \in S$ are such that $s \vee t = 1$, $s \wedge t = 0$, $s \vee r = 1$ and $s \wedge r = 0$.

Then $t = t \wedge 1 = t \wedge (s \vee r) = (t \wedge s) \vee (t \wedge r) = 0 \vee (t \wedge r) = (s \wedge r) \vee (t \wedge r) = (s \vee t) \wedge r = 1 \wedge r = r$. (3)
It directly follows from the definition of inverse, due to commutativity.

Examples:

1. Let S be a nonempty set. Then $P(S)$ is a Boolean algebra with $\vee = \cup$, $\wedge = \cap$, $\neg A = A^c$, $0 = \emptyset$ and $1 = S$. This is called the power set Boolean algebra. So, we have Boolean algebras of finite size as well as of uncountable size.
2. Take $D(30) = \{n \in \mathbb{N} : n \mid 30\}$ with $a \vee b = \text{lcm}(a, b)$, $a \wedge b = \text{gcd}(a, b)$ and $\neg a = 30/a$. It is a Boolean algebra with $0 = 1$ and $1 = 30$.
3. Let $B = \{T, F\}$, where \vee , \wedge and \neg are the usual connectives. It is a Boolean algebra with $0 = F$ and $1 = T$.
4. Let B be the set of all truth functions involving the variables p_1, \dots, p_n , with usual operations \vee , \wedge and \neg . Then B is a Boolean algebra with $0 = \perp$ and $1 = \top$. This is called the free Boolean algebra on the generators p_1, \dots, p_n .
5. The set of all formulas (of finite length) involving variables p_1, p_2, \dots is a Boolean algebra with usual operations. This is also called the free Boolean algebra on the generators p_1, p_2, \dots . Here also $0 = \perp$ and $1 = \top$. So, we have a Boolean algebra of denumerable size.

Remark: The rules of Boolean algebra treat $(\vee, 0)$ and $(\wedge, 1)$ equally. Notice that the second parts in the defining conditions of Definition 8.3.1 can be obtained from the corresponding first parts by replacing \vee with \wedge , \wedge with \vee , 0 with 1 , and 1 with 0 simultaneously. Thus, any statement that one can derive from these assumptions has a dual version which is derivable from the same assumptions. This is called the principle of duality.

Theorem: [Laws]

Let S be a Boolean algebra. Then the following laws hold for all $s, t \in S$:

1. [Constants] : $\neg 0 = 1$, $\neg 1 = 0$, $s \vee 1 = 1$, $s \wedge 1 = s$, $s \vee 0 = s$, $s \wedge 0 = 0$.
2. [Idempotence] : $s \vee s = s$, $s \wedge s = s$.
3. [Absorption] : $s \vee (s \wedge t) = s$, $s \wedge (s \vee t) = s$.
4. [Cancellation] : $s \vee t = r \vee t$, $s \vee \neg t = r \vee \neg t \Rightarrow s = r$.
5. [Cancellation] : $s \wedge t = r \wedge t$, $s \wedge \neg t = r \wedge \neg t \Rightarrow s = r$.
6. [Associativity] : $(s \vee t) \vee r = s \vee (t \vee r)$, $(s \wedge t) \wedge r = s \wedge (t \wedge r)$.

Proof. We give the proof of the first part of each item and that of its dual is left for the reader.

$$(1) 1 = 0 \vee (\neg 0) = \neg 0.$$

$$s \vee 1 = (s \vee 1) \wedge 1 = (s \vee 1) \wedge (s \vee \neg s) = s \vee (1 \wedge \neg s) = s \vee \neg s = 1.$$

$$s \vee 0 = s \vee (s \wedge \neg s) = (s \vee s) \wedge (s \vee \neg s) = s \wedge 1 = s.$$

$$(2) s = s \vee 0 = s \vee (s \wedge \neg s) = (s \vee s) \wedge (s \vee \neg s) = (s \vee s) \wedge 1 = (s \vee s).$$

$$(3) s \vee (s \wedge t) = (s \wedge 1) \vee (s \wedge t) = s \wedge (1 \vee t) = s \wedge 1 = s.$$

$$(4) \text{ Suppose that } s \vee t = r \vee t \text{ and } s \vee \neg t = r \vee \neg t. \text{ Then } s = s \vee 0 = s \vee (t \wedge \neg t) = (s \vee t) \wedge (s \vee \neg t) = (r \vee t) \wedge (r \vee \neg t) = r \vee (t \wedge \neg t) = r \vee 0 = r.$$

(5) This is the dual of (4) and left as an exercise.

(6) Using distributivity and absorption, we have $s \vee (t \vee r) \wedge \neg s = (s \wedge \neg s) \vee (t \vee r) \wedge \neg s = 0 \vee (t \vee r) \wedge \neg s = (t \vee r) \wedge \neg s = (t \wedge \neg s) \vee (r \wedge \neg s)$.

$(s \vee t) \vee r \wedge \neg s = (s \vee t) \wedge \neg s \vee (r \wedge \neg s) = (s \wedge \neg s) \vee (t \wedge \neg s) \vee (r \wedge \neg s) = (0 \vee (t \wedge \neg s) \vee (r \wedge \neg s)) = (t \wedge \neg s) \vee (r \wedge \neg s)$.

Hence, $s \vee (t \vee r) \wedge \neg s = (s \vee t) \vee r \wedge \neg s$.

Also, $(s \vee t) \vee r \wedge s = (s \vee t) \wedge s \vee (r \wedge s) = s \vee (r \wedge s) = s = s \vee (t \vee r) \wedge s$.

Now, apply Cancellation law to obtain the required result.

Isomorphisms between two similar algebraic structures help us in understanding an unfamiliar entity through a familiar one. Boolean algebras are no exceptions.

Definition: Let $(B_1, \vee_1, \wedge_1, \neg_1)$ and $(B_2, \vee_2, \wedge_2, \neg_2)$ be two Boolean algebras.

A function $f : B_1 \rightarrow B_2$ is a Boolean homomorphism if it preserves 0, 1, \vee , \wedge , and \neg . In such a case, $f(0_1) = 0_2$, $f(1_1) = 1_2$, $f(a \vee_1 b) = f(a) \vee_2 f(b)$, $f(a \wedge_1 b) = f(a) \wedge_2 f(b)$, $f(\neg_1 a) = \neg_2 f(a)$.

A Boolean isomorphism is a Boolean homomorphism which is a bijection.

Unless we expect an ambiguity in reading and interpreting the symbols, we will not write the subscripts with the operations explicitly as is done in Definition.

Examples: Recall the notation $[n] = \{1, 2, \dots, n\}$. The function $f : P([4]) \rightarrow P([3])$ defined by $f(S) = S \setminus \{4\}$ is a Boolean homomorphism.

We check two of the properties and leave others as exercises. $f(A \vee B) = f(A \cup B) = (A \cup B) \setminus \{4\} = (A \setminus \{4\}) \cup (B \setminus \{4\}) = f(A) \vee f(B)$. $f(1) = f([4]) = [4] \setminus \{4\} = [3] = 1$.

Theorem: Let (B, \vee, \wedge, \neg) be a Boolean algebra. Define the relation \leq on B by $a \leq b$ if and only if $a \wedge b = a$ for all $a, b \in B$. Then (B, \leq) is a distributive complemented lattice in which $\text{lub}\{a, b\} = a \vee b$ and $\text{glb}\{a, b\} = a \wedge b$ for all $a, b \in B$.

Proof: We first verify that (B, \leq) is a partial order.

Reflexive: $s \leq s$ if and only if $s \wedge s = s$, which is true.

Antisymmetry: Let $s \leq t$ and $t \leq s$. Then we have $s = s \wedge t = t$.

Transitive: Let $s \leq t$ and $t \leq r$. Then $s \wedge t = s$ and $t \wedge r = t$.

Using associativity, $s \wedge r = (s \wedge t) \wedge r = s \wedge (t \wedge r) = s \wedge t = s$;

consequently, $s \leq r$. Now, we show that $a \vee b = \text{lub}\{a, b\}$.

Since B is a Boolean algebra, using absorption, we get $(a \vee b) \wedge a = a$ and hence $a \leq a \vee b$. Similarly, $b \leq a \vee b$.

So, $a \vee b$ is an upper bound for $\{a, b\}$. Now, let x be any upper bound for $\{a, b\}$.

Then, by distributive property, $(a \vee b) \wedge x = (a \wedge x) \vee (b \wedge x) = a \vee b$.

So, $a \vee b \leq x$. Thus, $a \vee b$ is the lub of $\{a, b\}$.

Analogous arguments show that $a \wedge b = \text{glb}\{a, b\}$.

Since for all $a, b \in B$, $a \vee b$ and $a \wedge b$ are in B , we see that $\text{lub}\{a, b\}$ and $\text{glb}\{a, b\}$ exist.

Thus (B, \leq) is a lattice.

Further, if $a \in B$, then $\neg a \in B$. This provides the complement of a in the lattice (B, \leq) .

Further, both the distributive properties are already satisfied in B .

Hence (B, \leq) is a distributive complemented lattice.

Definition: Let (B, \vee, \wedge, \neg) be a Boolean algebra. The relation \leq on B given by $a \leq b$ if and only if $a \wedge b = a$ for all $a, b \in B$ is called the induced partial order.

A minimal element of B with respect to the partial order \leq , which is different from 0 is called an atom in B .

Examples:

1. In the power set Boolean algebra, singleton sets are the only atoms.
2. In Example atoms of $D(30)$ are 2, 3 and 5.
3. The $\{F, T\}$ Boolean algebra has only one atom, namely T .

Proposition: Each finite Boolean algebra has at least one atom.

Proof:

Let B be a finite Boolean algebra.

Assume that no element of B is an atom.

Now, $0 < 1$ and 1 is not an atom.

Then there exists $b_1 \in B$ such that $0 < b_1 < 1$.

Since b_1 is not an atom, there exists $b_2 \in B$ such that $0 < b_2 < b_1 < 1$.

By induction it follows that we have a sequence of elements (b_i) such that $0 < \dots < b_i < b_{i-1} < \dots < b_1 < 1$.

As B is finite, there exist $k > j$ such that $b_k = b_j$.

We then have $b_k < b_{k-1} < \dots < b_j = b_k$.

This is impossible. Hence B has at least one atom.

Proposition: Let p and q be atoms in a Boolean algebra B . If $p \neq q$, then $p \wedge q = 0$.

Proof:

Suppose that $p \wedge q \neq 0$.

We know that $p \wedge q \leq p$.

If $p \wedge q \neq p$, then $p \wedge q < p$.

But this is not possible since p is an atom.

So, $p \wedge q = p$. Similarly, $q \wedge p = q$.

By commutativity, $p = p \wedge q = q \wedge p = q$.

Theorem: [Representation] Let B be a finite Boolean algebra. Then there exists a set X such that B is isomorphic to $P(X)$.

Proof: Let X be the set of all atoms of B .

By Proposition, $X \neq \emptyset$.

Define $f : B \rightarrow P(X)$ by $f(b) = \{x \in X : x \text{ is an atom and } x \leq b\}$ for $b \in B$.

We show that f is the required Boolean isomorphism.

Injection: Suppose $b_1 \neq b_2$.

Then, either $b_1 < b_2$ or $b_2 < b_1$.

Without loss of generality, let $b_1 < b_2$.

Note that $b_1 = b_1 \wedge (b_2 \vee \neg b_2) = (b_1 \wedge b_2) \vee (b_1 \wedge \neg b_2)$.

Also, the assumption $b_1 < b_2$ implies $b_1 \wedge b_2 \neq b_1$ and hence $b_1 \wedge \neg b_2 \neq 0$.

So, there exists an atom $x \leq (b_1 \wedge \neg b_2)$ and hence $x = x \wedge b_1 \wedge \neg b_2$.

Then $x \wedge b_1 = (x \wedge b_1 \wedge \neg b_2) \wedge b_1 = x \wedge b_1 \wedge \neg b_2 = x$.

Thus, $x \in f(b_1)$.

Similarly, $x \leq \neg b_2$. As $x \neq 0$,

we cannot have $x \leq b_2$ (for, $x \leq \neg b_2$ and $x \leq b_2$ imply $x \leq b_2 \wedge \neg b_2 = 0$).

Thus there is an atom in $f(b_1)$ which is not in $f(b_2)$.

Therefore, $f(b_1) \neq f(b_2)$.

Surjection: Let $A = \{x_1, \dots, x_k\} \subseteq X$.

Write $a = x_1 \vee \dots \vee x_k$ (if $A = \emptyset$, take $a = 0$).

Clearly, $A \subseteq f(a)$. We show that $A = f(a)$. So, let $y \in f(a)$.

Then y is an atom in B and $y = y \wedge a = y \wedge (x_1 \vee \dots \vee x_k) = (y \wedge x_1) \vee \dots \vee (y \wedge x_k)$.

Since $y \neq 0$, by Proposition, $y \wedge x_i \neq 0$ for some $i \in \{1, 2, \dots, k\}$.

As x_i and y are atoms, we have $y \wedge x_i = x_i$ and hence $y \in A$.

That is, $f(a) \subseteq A$ so that $f(a) = A$.

Thus, f is a surjection. Preserving $0, 1$: Clearly $f(0) = \emptyset$ and $f(1) = X$. Preserving \vee, \wedge : By definition, $x \in f(b_1 \wedge b_2) \Leftrightarrow x \leq b_1 \wedge b_2 \Leftrightarrow x \leq b_1 \text{ and } x \leq b_2 \Leftrightarrow x \in f(b_1) \text{ and } x \in f(b_2) \Leftrightarrow x \in f(b_1) \cap f(b_2)$.

For the other one, let $x \in f(b_1 \vee b_2)$. Then, $x = x \wedge (b_1 \vee b_2) = (x \wedge b_1) \vee (x \wedge b_2)$.

So, $x \wedge b_1 \neq 0$ or $x \wedge b_2 \neq 0$.

Without loss of generality, suppose $x \wedge b_1 \neq 0$.

As x is an atom, $x \leq b_1$ and hence $x \in f(b_1) \subseteq f(b_1) \cup f(b_2)$.

Conversely, let $x \in f(b_1) \cup f(b_2)$. Without loss of generality, let $x \in f(b_1)$.

Thus, $x \leq b_1$ and hence $x \leq b_1 \vee b_2$ which in turn implies that $x \in f(b_1 \vee b_2)$.

Therefore, $x \in f(b_1 \vee b_2) \Leftrightarrow x \in f(b_1) \cup f(b_2)$.

Preserving \neg : Let $x \in B$. Then $f(x) \cup f(\neg x) = f(x \vee \neg x) = f(1) = X$ and $f(x) \cap f(\neg x) = f(x \wedge \neg x) = f(0) = \emptyset$.

Thus $f(\neg x) = f(x)^c$.

As immediate consequences of the representation theorem, we obtain the following results.

Corollary: Let B be a finite Boolean algebra.

1. If B has exactly k atoms then B is isomorphic to $P(\{1, 2, \dots, k\})$. Hence, B has exactly 2^k elements.
2. Fix $b \in B$. If p_1, \dots, p_n are the only atoms less than or equal to b , then $b = p_1 \vee \dots \vee p_n$.