Discrete Mathematics

Study Material

Unit – I: MATHEMATICAL LOGIC

INTRODUCTION

Unit I – Prepositional Logic

INTRODUCTION TO DM

- Mathematical topics that are discussed are logic, set theory, algebraic structures, graph theory. These topics will support many areas of computer science such as automata, artificial intelligence, syntactic analysis, switching theory, programming languages
- Logic is the study and analysis of the nature of valid arguments.
- Set theory, relations, recursive functions are mostly used in programming languages.
- Algebraic structures are used for syntactic analysis, error detecting and correcting codes.
- Graph theory is used in minimal-path problems, fault detection and diagnosis in computers
- The reasoning tool by which valid inferences can be drawn from a set of premises.

✓ A statement cannot be further divided into smaller statements is called Primitive or Primary or Atomic or Simple statements.

✓ A statement cannot be Primitive or Primary or Atomic or Simple, It is called molecular or Compound Statement.

✓ The statements are denoted by the distinct symbols A, B, C, … P, Q, …. And they have one and only one of two possible truth-values.

- ✓ True (T or 1) – Truth of a logical statement
- ✓ False (F or 0) – Falsity of a logical statement

Ex: P : The weather is cloudy.
Q : It is raining today.
R : It is snowing.

Uses of Logic reasoning

- ✓ In Mathematics to prove theorems.
- ✓ In computer science to verify the correctness of programs and to prove theorems.
- ✓ In Natural and Physical Sciences to draw conclusions from experiments.
- ✓ In Social Sciences, and everyday lives to solve a multitude of problems.

1.1. Statements/Propositions and notations:

In symbolic logic we study arguments. The basic building blocks of arguments are declarative sentences called Propositions or Statements.

or

Statement: A declarative sentence which is either true or false but not both.

<u>Example</u>:

✓The Sun rises in the East – Statement - True
✓Smoking is injurious to health. – Statement - True
✓She is an Engineering student – Statement - True
✓The Delhi is capital of the India – Statement - True
✓2+3=5 – Statement - True

MAT-1014 R. Udhayakumar

Module - I Mathematical logic and statement calculus.

Statement (or) Proposition

A proposition (or) statement is a declarative sentence that is either true or false, but not both.

Example:-

(1) Rose is a beautiful flower (T)

(2) $5+5=12$ (F)

Note:- The truth values True and False are denoted by the symbol's **T** and **F** respectively. Some times it is also denoted by **1** and 0, where 1 stands for true and 0 stands for false.

Types of statements

(1) Simple (2) Compound

(1) Simple (or) Atomic (or) Primary (or) primitive statement

The statements which do not contain any of the connectives are called Atomic statements

Ex: (i) 3 is a prime number (T)

(ii) Canada is a country (T)

(2) Compound statement

New statements can be formed from atomic statements through the use of sentential connectives.

The resulting statements are called compound statements.

Ex:- If p is a prime number, then the divisor of 'p' are '1' and 'p' itself.

Truth Table

A table showing all possible truth values of a compound statement is called the truth table.

Logical Connectives

* Negation ($\neg$ or $\sim$) Not
* Conjunction ($\wedge$ and)
* Disjunction ($\vee$ or)
* Conditional (Implication $\rightarrow$) if
* Bi-conditional ($\leftrightarrow$ iff)

* Negation ($\neg$ or $\sim$) Not

If P is a proposition, then not P is also a proposition.

Ex: If P : London is a city.

then $\neg P$ or $\sim P$: London is not a city.

Rule:- If P is true, then $\neg P$ is false and if P is false then $\neg P$ is true.

Truth Table

P	$\neg P$
T	F
F	T

★ Conjunction ($\wedge$ and)

The conjunction of two statements P and Q is also a statement denoted by $P \wedge Q$. We use the connective And for conjunction.

Eg: P : $2+3 = 5$

Q : 5 is a composite number.

So, $P \wedge Q$: $2+3=5$ and 5 is a composite number.

Rule:- $(P \wedge Q)$ is true if both P and Q are true, otherwise false.

Truth Table

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

★ Disjunction ($\vee$ or)

The disjunction of two statements P and Q is also a statement denoted by $P \vee Q$. We use the connective or for disjunction.

Rule:- $(P \vee Q)$ is true, if either P or Q is true and it is false when both P and Q are false.

Truth Table

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

* ## Conditional statement ($\rightarrow$)

"If P, then Q" is called a conditional statement.

Rule:- The statement $P \rightarrow Q$ has a truth value F when Q has the truth value F and P has the truth value T; otherwise it has the truth value T.

Truth Table

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

* ## Bi-conditional ($\leftrightarrow$)

"P if and only if Q" i.e., "P iff Q" is called a bi-conditional statement and is defined as

$$P \leftrightarrow Q : (P \rightarrow Q) \wedge (Q \rightarrow P)$$

Truth Table

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$(P \rightarrow Q) \wedge (Q \rightarrow P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Tautologies

* The proposition is said to be tautology if its truth value is T for any assignment of truth value to its components.

A statement formula which is always true whatever may be the truth values of its components, is called a tautology or a universally valid formula.

Examples

(1) $(P \wedge q) \rightarrow p$

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

(3) $(p \vee q) \longleftrightarrow (q \vee p)$

P	Q	$P \wedge Q$	$P \wedge Q \rightarrow P$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Contradiction

A statement that is always false is called a contraction.

Examples (1) $P \wedge \neg P$ (2) $(P \vee Q) \wedge (\neg P \wedge \neg Q)$

P	$\neg P$	$P \wedge \neg P$
T	F	F
F	T	F

Contingency

A statement formula that is neither tautology nor contradiction is called contingency.

A statement formula that can be either true or false ie, neither a tautology nor a contradiction, is called a contingency.

Example (1) $P \leftrightarrow q$ (2) $(P \vee \neg Q) \rightarrow P \wedge Q$

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$P \leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Logical Equivalence

Two statement formula's are said to be logically equivalent if their truth columns are identical.

Such statements are represented by $P \equiv Q$ (or) $P \Leftrightarrow Q$.

Note:- Equivalence is transitive. Because if $A \Leftrightarrow B$ and $B \Leftrightarrow C$, then $A \Leftrightarrow C$.

Cross elasticity of demand:

Example

1. P.T $(p \to q) \Leftrightarrow (\neg p \vee q)$

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

H.W 2. $S: P \rightleftarrows Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$

P	Q	$P \to Q$	$Q \to P$	$P \rightleftarrows Q$	$(P \to Q) \wedge (Q \to P)$	S
T	T	T	T	T	T	T
T	F	F	T	F	F	T
F	T	T	F	F	F	T
F	F	T	T	T	T	T

A list of equivalent formulae

1. Idempotent laws —

$P \vee P \Leftrightarrow P$ & $P \wedge P \Leftrightarrow P$

2. Associative laws

$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ &

$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$

3. Distributive laws

$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ &

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

4. Commutative laws

$P \vee Q \Leftrightarrow Q \vee P$ &

$P \wedge Q \Leftrightarrow Q \wedge P$

5. Identity laws

$P \vee \mathbf{F} \Leftrightarrow P$, $P \wedge \mathbf{T} \Leftrightarrow P$

6. Dominant laws

$P \vee \mathbf{T} \Leftrightarrow \mathbf{T}$, $P \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$

7. Negation laws

$P \vee \neg P \Leftrightarrow \mathbf{T}$, $P \wedge \neg P \Leftrightarrow \mathbf{F}$

8. Absorption laws

$P \vee (P \wedge Q) \Leftrightarrow P$ &

$P \wedge (P \vee Q) \Leftrightarrow P$

9. De Morgan's Laws

$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$ &

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

Example

1. Without using truth table, show that

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

Solution:-

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

$\Leftrightarrow ((Q \vee P) \wedge (Q \vee \neg Q)) \vee (\neg P \wedge \neg Q)$ Distributive law

$\Leftrightarrow (Q \vee P \wedge T) \vee (\neg P \wedge \neg Q)$ Negation law

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

$\Leftrightarrow (Q \vee P) \vee \neg (P \vee Q)$ De Margon's law

$\Leftrightarrow (P \vee Q) \vee \neg (P \vee Q)$ Commutative law

$\Leftrightarrow T$ tautology.

2. S.T $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$

Soln:-

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

$\Leftrightarrow (\neg P \wedge (\neg Q \wedge R)) \vee [(Q \vee P) \wedge R]$ by distributive laws.

$\Leftrightarrow ((\neg P \wedge \neg Q) \wedge R) \vee ((Q \vee P) \wedge R)$ by associative law

$\Leftrightarrow ((\neg P \wedge \neg Q) \vee (Q \vee P)) \wedge R$ by distributive laws

$\Leftrightarrow (\neg (P \vee Q) \vee (P \vee Q)) \wedge R$ by De Margon's Laws & Commutative laws

$\Leftrightarrow T \wedge R$ Negation laws

$\Leftrightarrow R$ Identity laws

H.W

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

2. $P \rightleftarrows Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$

3. $(P \wedge Q) \to (P \vee Q)$ is a tautology.

Tautology Implications

A statement formula A is said to tautologically imply another statement formula B iff $A \to B$ is a tautology. In symbol, it is denoted by $A \Rightarrow B$.

Note:- $A \Rightarrow B$ means that $A \to B$ is a tautology.

Some Tautology implications

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

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

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

(4) $\neg P \Rightarrow P \to Q$

(5) $Q \Rightarrow P \to Q$

(6) $\neg(P \to Q) \Rightarrow P$

(7) $\neg(P \to Q) \Rightarrow \neg Q$

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

(9) $\neg Q \wedge (P \to Q) \Rightarrow \neg P$

(10) $\neg P \wedge (P \vee Q) \Rightarrow Q$

Note

(1) Connectives $\wedge, \vee$ and $\rightleftarrows$ are symmetric

Since, $P \wedge Q \Leftrightarrow Q \wedge P$

$P \vee Q \Leftrightarrow Q \vee P$

$P \rightleftarrows Q \Leftrightarrow Q \rightleftarrows P$

But $\to$ is need not be symmetric.

i.e., $P \to Q$ is not equivalent to $Q \to P$

i.e; $P \to Q \not\Leftrightarrow Q \to P$.

(2) Converse For any statement formula, $P \to Q$ then the statement formula $Q \to P$ is called its converse.

(3) Inverse For $P \to Q$, $\neg P \to \neg Q$ is called its inverse.

(4) Contrapositive For $P \to Q$, $\neg Q \to \neg P$ is called its Contrapositive.

Discrete Mathematics (DM)- (7F302)

Unit 2 : First order logic

2.1.Predicates

2.2.Quantifiers

2.3.Free and Bound Variables

2.4. Inference theory or Rules of Inference

2.1. Predicate Calculus

The propositional logic is not powerful enough to represent all types of statements that are used in Computer Science and Mathematics, or to express certain types of relationship between propositions such as equivalence.

For example, the statement "X is greater than 1", where X is a variable, is not a proposition because you can not tell whether it is true or false unless you know the value of X.

Thus the propositional logic can not deal with such sentences. However, such statements appear quite often in Mathematics and we want to do inferenceing on those statements.

- **Not all birds fly" is equivalent to "Some birds don't fly".**
- **"Not all integers are even" is equivalent to "Some integers are not even".**
- **"Not all cars are expensive" is equivalent to "Some cars are not expensive".**

Each of those propositions is treated independently of the others in propositional logic.

Example: if **P** represents "**Not all birds fly**" and

Q represents "**Some integers are not even**",

then there is no mechanism in propositional logic to find out that P is equivalent to Q.

- **Thus we need more powerful logic to deal with these and other problems. The predicate logic is one of such logic and it addresses these issues among others.**

2.1. Predicates:

A predicate is a verb phrase template that describes a property of objects, or a relationship among objects represented by the variables.

The logic based upon the analysis of predicates in any statement is called Predicate logic.

Symbolize a predicate by a capital letter and names of individuals or objects in general by small letters.

Example 1: The statement 'x is a student' has two parts.

Part 1: The variable x is the subject of the statement.

Part 2: The predicate ' is a student' refers to a property that the subject of the statement can have.

We can denote the statement ' x is a student' by S(x) where S denotes the predicate and x is a variable.

In general any statement of the type 'p is Q' where Q is the predicate and p is the subject can be denoted by Q(p)

Example 2: Amulya is a Student and This painting is Blue.

$$S(a) \wedge B(p).$$

A predicate requiring m(m>0) names or objects is called an m-place predicate.

Example 3: Amulya is a Student

'is a student' is a 1-place predicate because it is related to one object(Amulya).

Example 4: Naveen is taller than Amul.

The predicate 'is taller than' is a 2-place predicate.

The representation is T(n,a)

When m=0 , then we shall call a statement 0-place predicate because no names are associated with a statement.

A Simple statement function of one variable is defined to be an expression consisting of a predicate symbol and an individual variable.

We can form 'Compound statement functions by combining one or more simple statement functions and the logical connectives.

$M(x) \vee N(x)$, $M(x) \wedge N(x)$, $M(x) \rightarrow N(x)$, $\sim M(x)$ and $M(x) \leftrightarrow N(x)$.

Some restrictions can be introduced by limiting the class of objects under considerations. These limitation means that the variable which are mentioned stand for only those objects which are members of particular set or class. Such a restricted class is called the universe of discourse or the domain of individuals or simply the universe.

Example 5: **consider the statement**

"Given any positive integer, there is greater positive integer"

in this case the universe of discourse is the set of positive integers.

2.2. Quantifiers

The statements involve words that indicate quantity such as 'all', 'some', 'none', or 'one'. These words indicates quantity and they are called Quantifiers.

Sentence	Abbreviated Meaning
Some men are tall.	There is atleast one tall man.
All birds have wings.	
No air balloon is perfectly round.	All air balloons fail to be perfectly round.
There is a real number less than 11.	Atleast one real number is less than 11.

There are two types of quantifiers.

1. **Universal**
2. **Existential**

Universal quantifier: **The quantifier "all" is called as the Universal quantifier, Denoted as $\forall x$.**

The symbol $\forall x$ Represents each of the following phrases have same meaning.

- ✓**For all x**
- ✓**For every x**
- ✓**For each x**
- ✓**Every thing x is such that**
- ✓**Each thing x is such that**

Existential quantifier: **The quantifier "some" is the Existential quantifier. Denoted as $\exists x$.**

The symbol $\exists$ x Represents each of the following phrases have same meaning

- ✓ **For some x**
- ✓**Some x is such that**
- ✓**There exists an x such that**
- ✓**There is an x such that**
- ✓**There is at least one x such that**

Example 1: Some thing is Good

Solution : "There is atleast one x such that x is good"

The Symbolic form: $(\exists x)\, G(x)$

Example 2: Every thing is Good

Solution : "For all x, x is good"

The Symbolic form: $(\forall x)\, G(x)$

Example 3: Nothing is Good

Solution : "For all x, x is not good"

The Symbolic form: $(\forall x)\, {\sim}G(x)$

Example 4: Something is not Good

Solution : "There is atleast one x such that x is good"

The Symbolic form: $(\exists x)\, {\sim}G(x)$

Equivalent Formulas:

- ✓ **"All true" means the same as "None false".**
- ✓ **"All false" means the same as "None true".**
- ✓ **"Not all true" means the same as "Atleast one false".**
- ✓ **"Not all false" means the same as "Atleast one true".**

- ✓ $(\forall x)\ F(x) \Leftrightarrow \sim(\exists x) \sim F(x)$
- ✓ $(\forall x) \sim F(x) \Leftrightarrow \sim(\exists x)\ F(x)$
- ✓ $\sim[\forall x,\ F(x)] \Leftrightarrow (\exists x)\sim F(x)$
- ✓ $\sim[(\forall x)\sim F(x)] \Leftrightarrow (\exists x)\ F(x)$

The symbol ∃!x is read there is a unique x such that ... or There is one and only one x such that ...

Ex: There is one and only one even prime.

$\exists! x$, [x is an even prime]

$\exists! x$, $P(x)$ where $P(x) \equiv x$ is an even prime integer.

To form the negation of a statement involving one quantifier, change the quantifier form universal to existential, or from existential to universal, and negate the statement, which it quantifies.

Statement	Its Negation
$\forall x\ P(x)$	$[\exists x \sim P(x)]$
$\exists x\ P(x)$	$[\forall x \{\sim P(x)\}]$

Example 1: All monkeys have tails

Solution : "For all x, if x is a monkey, then x has tail"

The Symbolic form: $(\forall x)\ [M(x) \rightarrow T(x)]$

Example 2: No monkey has a tail.

Solution : "For all x, if x is a monkey, then x has no tail"

The Symbolic form: $(\forall x)\ [M(x) \rightarrow \sim T(x)]$

Example 3: Some monkeys have tails

Solution : "There is an x such that, x is a monkey and x has tail"

The Symbolic form: $(\exists x)\ [M(x) \wedge T(x)]$

Example 4: Some monkeys have no tails

Solution : "There is an x such that, x is a monkey and x has no tail"

The Symbolic form: $(\exists x)\ [M(x) \wedge \sim T(x)]$

Example 1: All men are good.

Solution : "For all x, if x is a man, then x is Good."

The Symbolic form: $(\forall x)\ [M(x) \rightarrow G(x)]$

Example 2: No men are good.

Solution : "For all x, if x is a man, then x is not Good"

The Symbolic form: $(\forall x)\ [M(x) \rightarrow \sim G(x)]$

Example 3: Some men are good.

Solution : "There is an x such that, x is a man and x is Good."

The Symbolic form: $(\exists x)\ [M(x) \wedge G(x)]$

Example 4: Some men are not good.

Solution : "There is an x such that, x is a man and x is not tail"

The Symbolic form: $(\exists x)\ [M(x) \wedge \sim G(x)]$

Write the following sentences is the closed form or Symbolic form.

1. **Some people who trust others one rewarded.**
2. **If any one is good then john is good.**
3. **He is ambitious or no one is ambitious.**
4. **Some one is teasing**
5. **It is not true that all roads lead to rome.**

Solution : Let

P(x) : x is a Person

T(x) : Trust others

R(x) : is rewarded

G(x) : is good

A(x) : is ambitious

Q(x) : is teasing

S(x) : is a road

L(x) : leads to Rome

1: Some people who trust others one rewarded.

Solution : "There is one x such that, x is a person, x trusts others and x is rewarded."

The Symbolic form: $(\exists x)\ [P(x) \wedge T(x) \wedge R(x)]$

2: If any one is good then john is good.

Solution : "If there is one x such that x is a person and x is good then john is good."

The Symbolic form: $(\exists x)\ [P(x) \wedge G(x)] \rightarrow G(John)$

3: He is ambitious or no one is ambitious.

Solution : He represents a particular person. Let that person be y. so "y is ambitious or for all x, if x is person then x is not ambitious."

The Symbolic form: $A(y) \vee ((\forall x)\ [P(x) \rightarrow \sim A(x)]$

4: Some one is teasing

Solution : "There is one x such that, x is a person and x is teasing"

The Symbolic form: $(\exists x)\ [P(x) \wedge Q(x)]$

5: It is not true that all roads lead to rome.

Solution : The statement can be written as

$$\sim(\forall x)\ [S(x) \to L(x)]$$

Or

$$(\exists x)\ [S(x) \wedge \sim L(x)]$$

Translate each of the following statements into symbols,using quantifiers,variables,and predicate symbols.

1.All birds can fly.

2.Not all birds can fly.

3.All babies are illogical.

4.Some babies are illogical.

5.If x is a man, then x is a giant.

6.Some men are giants.

7.Some men are not giants.

8.All men are giants.

9.No men are giants.

10.There is a student who likes mathematics but not history.

11. x is an odd integer and x is prime.

12. For all integers x, x is odd and x is prime.

13. For each integer x, x is odd and x is prime.

14. There is an integer x such that x is odd and is prime

15. Not every actor is talented who is famous.

16. Some nos. are rational.

17. Some nos. are not rational.

18. Not all nos. are rational.

19. Not every graph is planar.

20. If some students are lazy, then all students are lazy.

21. x is rational implies that x is real.

22. Not all cars have Carburetors.

23. Some people are either religious or pious.

24. No dogs are intelligent.

25. All babies are illogical.

26. Every no. either is negative or has a square root.

27. Some numbers are not real.

28. Every connected and circuit free graph is a tree.

29. Not every graph is connected.

Statement formula in Predicate Calculus

$P(x_1,x_2,\ldots..x_n)$ denotes an n-place predicate formula in which the letter P is an n-place predicate and $x_1,x_2,\ldots..x_n$ are objects or individual variables.

In general $P(x_1,x_2,\ldots..x_n)$ will be called an atomic formula of predicate calculus.

Examples are R, Q(x), A(x,y,z) and A(x,y)

A wff of predicate calculus formula is obtained by using the following rules.

1. **An atomic formula is a wff.**
2. **If A is a formula, then ~A also a wff.**
3. **If A and B are wffs then $A \vee B$, $A \wedge B$, $A \rightarrow B$ and $A \leftrightarrow B$ are also wffs.**
4. **If A is wff x is any variable, then $\forall x\, A(x)$ and $\exists\, x\, A(x)$ are wff.**
5. **Only those formulas obtained by using rules(1) to (4) are wffs.**

Free and Bound Variables

Generally predicate formulas contain a part of the form $(\forall x)P(x)$ or $(\exists x)P(x)$, such a part is called an x-bound part of the formula.

Any variable appearing in an x-bound part of a formula is called a bound variable, otherwise it is called free variable.

The formula $P(x)$ immediately following either $(\forall x)$ or $(\exists x)$ is described as the scope of the quantifier.

Example: $(\forall x)A(x,y)$

Here the scope of $(\forall x)$ is $A(x,y)$

$A(x,y)$ is the scope of the quantifier

x is bounded occurrence.

y is free occurrence.

Valid Formula and Equivalences

Example 1: Show that $(\forall x)P(x) \rightarrow (\exists x)P(x)$ is a tautologically valid statement.

Sol: $(\forall x)P(x)$ is true in particular universe then the universe has atleast one object t in it and P(t) is a true statement for every t in the universe. In particular P(t) must be true. Thus $(\exists x)P(x)$ is true. Therefore $(\forall x)P(x) \rightarrow (\exists x)P(x)$ is a tautologically valid statement

if Why can't we use implication for the existential quantifier?

Example: All Apples are Delicious

Let F be the domain of fruits and

A(x):is an apple D(x):is delicious

$\forall x \in F(A(x) \rightarrow D(x))$ **says "any fruit, if it is an apple, then it is delicious," or simply, "apples are delicious fruit".**

$\forall x \in F(A(x) \land D(x))$ says "any fruit, is an apple *and* is delicious", or simply "all fruit are delicious apples.“

Example: Some Apples are Delicious

$\exists x \in F(A(x) \land D(x))$ says "some fruits, is an apple and is delicious," or simply "there is a delicious apple".

$\exists x \in F(A(x) \rightarrow D(x))$ says "there is some fruit, that if it were an apple then it would be delicious".

Predicate calculus : theory of inference

The Generalization and Specification rules are

Quantified Propositions:

Fundamental rule US: (Universal Specification)

If a statement of a form $\forall x$ P(x) is assumed to be true, then the universal quantifier can be dropped to obtain P(t) is true for an arbitrary object t in the universe. In symbols, he rule is,

$$\frac{(\forall x)\ P(x)}{\therefore\ P(t) \text{ for all } t}$$

Fundamental Rule UG: (Universal Generalisation)

If a statement P(t) is true for all t of the universe, then the universal quantifier may be prefixed to obtain $(\forall x)$ P(x). It is represented as

$$\frac{P(t) \text{ for all } t}{\therefore\ (\forall x)\ P(x)}$$

Fundamental Rule ES: (Existential Specification)

If $(\exists x)\ P(x)$ is assumed to be true, then there is an element t in the universe such that $P(t)$ is true. This may be represented as

$$\frac{(\exists x)\ P(x)}{\therefore\ P(t) \text{ for some } t}$$

Fundamental Rule EG: (Existential Generalization)

If $P(t)$ is true for some element t in the universe then $(\exists x)\ P(x)$ is true. This may be represented as

$$\frac{P(t) \text{ for some } t}{\therefore\ (\exists x)\ P(x)}$$

Example 1: verify the validity of the following argument.

Every living thing is a plant or an animal.

John's gold fish is alive and it is not a plant.

All animals have hearts.

Therefore John's gold fish has a heart.

Let the universe consist of all living things.

P(x) : x is Plant.

A(x) : x is an animal

H(x) : x has a Heart.

G: John's gold fish

Then the inference pattern is

$$
\begin{array}{r}
(\forall x)\,[P(x) \vee A(x)] \\
\sim P(g) \\
(\forall x)\,[A(x) \rightarrow H(x)] \\
\hline
\therefore H(g)
\end{array}
$$

[1]	**(1)**	**$(\forall x)\,[P(x) \vee A(x)]$**	**Rule P**
[2]	**(2)**	**$\sim P(g)$**	**Rule P**
[1]	**(3)**	**$P(g) \vee A(g)$**	**Rule US, from (1)**
[1,2]	**(4)**	**$A(g)$**	**Rule T, from (2) and (3)**
[5]	**(5)**	**$(\forall x)\,[A(x) \rightarrow H(x)]$**	**Rule P**
[5]	**(6)**	**$A(g) \rightarrow H(g)$**	**Rule US**
[1,2,5]	**(7)**	**$H(g)$**	**Rule T, from (4) and (6)**

Thus the conclusion is valid.

Example 2: verify the validity of the following argument.

Lions are dangerous animals.

There are lions.

$\therefore$ There are dangerous animals.

L(x) : x is Lion.

A(x) : x is an animal

Then the inference pattern is

$$(\forall x)\,[L(x) \rightarrow A(x)]$$
$$(\exists x)\,L(x)$$
$$\text{------------------------}$$
$$\therefore\ (\exists x)\,A(x)$$

[1]	(1)	$(\exists x)\,L(x)$	Rule P
[1]	(2)	$L(b)$	Rule ES, FROM (1)
[3]	(3)	$(\forall x)\,[L(x) \rightarrow A(x)]$	Rule P
[3]	(4)	$L(b) \rightarrow A(b)$	Rule EG, from (3)
[1,3]	(5)	$A(b)$	Rule T from (2) and (4)

Thus the conclusion is valid.

Example 3: verify the validity of the following argument.

All men are mortal.

Socrates is a man .

$\therefore$ socrates is a mortal.

H(x) : x is man.

M(x) : x is a mortal.

S: Socrates

Then the inference pattern is

$$(\forall x)\,[H(x) \to M(x)] \wedge H(s) \Rightarrow M(s)$$

[1]	(1)	$(\forall x)\,[H(x) \to M(x)]$	Rule P
[1]	(2)	$H(s) \to M(s)$	Rule US, From (1)
[3]	(3)	$H(s)$	Rule P
[1,3]	(4)	$M(s)$	Rule T, from (2) and (3) I_{11}

Thus the inference is valid.

4: verify the validity of the following argument

All men are fallible.

All kings are men.

∴ All kings are fallible.

Let M(x) : "x is a man"

K(x) : "x is a king"

F(x) : "x is fallible"

The above argument is symbolized as

$$\forall x, [M(x) \rightarrow F(x)]$$

$$\underline{\forall x, [K(x) \rightarrow M(x)]}$$

$$\therefore \forall x, [K(x) \rightarrow F(x)]$$

Proof:

[1]	(1)	$\forall x, [K(x) \rightarrow M(x)]$	Rule P
[1]	(2)	$K(c) \rightarrow M(c)$	Rule US, from (1)
[3]	(3)	$\forall x, [M(x) \rightarrow F(x)]$	Rule P
[3]	(4)	$M(c) \rightarrow F(c)$	Rule US, from (3)
[1,3]	(5)	$K(c) \rightarrow F(c)$	Rule T, from (2) & (4) and chain rule
[1,3]	(6)	$\forall x, [K(x) \rightarrow F(x)]$	Rule UG, from (5)

Thus the inference is valid.

5: Symbolize the following argument and check for its validity

All integers are rational numbers.

Some integers are powers of 3.

$\therefore$ Some rational numbers are powers of 3.

6: Show that from

a. $(\exists x)\,(F(x) \wedge S(x)) \rightarrow (\forall y)\,(M(y) \rightarrow W(y))$

b. $(\exists y)\,(M(y) \wedge \sim W(y))$

The conclusion $(\forall x)\,(F(x) \rightarrow \sim S(x))$ follows.

7: Show that $(\forall x)\,(P(x) \vee Q(x)) \Rightarrow (\forall x)\,P(x) \vee (\exists x)\,Q(x))$

8. Is the following conclusion validity derivable from the premises given?

If $(\forall x)\,(P(x) \rightarrow Q(x))$; $(\exists y)\,P(y)$, then $(\exists z)\,Q(z)$.

9. Using CP or otherwise obtain the following implication.

$(\forall x)\,(P(x) \rightarrow Q(x)), (\forall x)\,(R(x) \rightarrow \sim Q(x)) \Rightarrow (\forall x)\,(R(x) \rightarrow \sim P(x))$

10. Show that $(\exists x)\,(P(x) \wedge Q(x)) \rightarrow ((\exists x)\,P(x) \wedge (\exists x)\,Q(x))$ is logically valid statement.

11. Show that $(\forall x)\,(P(x) \rightarrow Q(x)) \rightarrow ((\forall x)P(x) \rightarrow (\forall x)\,Q(x))$ is logically valid statement.

12. Show that $\sim(P(x) \vee Q(x)) \leftrightarrow (\sim P(x) \wedge \sim Q(x))$ is logically valid statement.

13. Show that $P(x) \rightarrow Q(y)) \leftrightarrow (\sim P(x) \vee Q(y))$ is logically valid statement.

14. Show that $P(x) \wedge Q(y)) \rightarrow (\sim P(x) \rightarrow Q(y))$ is logically valid statement.

15. Show that $R(x) \wedge S(x)) \rightarrow R(x)$ is logically valid statement.

16. Show that $(\forall x)\ (P(x) \vee Q(x)), (\forall x) \sim P(x) \Rightarrow (\forall x)\ Q(x)$ is logically valid statement.

17. Show that $(\forall x)\ (P(x) \rightarrow Q(x)) \wedge (\forall x)(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)(P(x) \rightarrow R(x))$ is logically valid statement.

18. Show that $P \rightarrow ((\exists x)\ Q(x)) \Rightarrow (\exists x)(P(x) \rightarrow Q(x))$ is logically valid statement.

2.2.5. Formulas involving more than one quantifier :

Consider the statement $P(x,y)$: x likes y.

$((\exists x)\ (P(x,y))$: there is an x suchthat, x likes y.

$(\forall x)(P(x,y))$: every one liked y.

$(\exists y)\ (\exists x)\ (P(x,y))$: there is someone whom some one likes.

$(\exists y)\ (\forall x)\ (P(x,y))$: there is someone whom every body likes.

$(\forall y)\ (\exists x)\ (P(x,y))$: Everybody is liked by some one.

$(\forall y)\ (\forall x)\ (P(x,y))$: Everybody is liked by every one.

$(\exists x)\ (\exists y)\ (P(x,y))$: someone likes some body.

$(\exists x)\ (\forall y)\ (P(x,y))$: some one likes every one.

$(\forall x)\ (\exists y)\ (P(x,y))$: Every one likes some one.

$(\forall x)\ (\forall y)\ (P(x,y))$: Every one likes everybody.

$$(\exists y)\ (\exists x)\ (P(x,y)) \Leftrightarrow (\exists x)\ (\exists y)\ (P(x,y))$$

$$(\forall y)\ (\forall x)\ (P(x,y)) \Leftrightarrow (\forall x)\ (\forall y)\ (P(x,y))$$

Example 1: Symbolize "Every one who likes fun will enjoy each of these plays"

Sol: Let L(x) : 'x likes fun'

P(y) : 'y is play'

E(x,y): x will enjoy y

the statement can be represented as "for each x, if x likes fun and for each y, if y is a play, then x enjoys y". Symbolically $(\forall x)\ (\forall y)\ [L(x) \wedge P(y)] \rightarrow E(x,y)$

2: write the Symbolic form and negate the statement "Everyone who is healthy can do all kinds of work".

3: write the Symbolic form and negate the statement "Some people are not admired by everyone".

4: write the Symbolic form and negate the statement "Everyone should help his neighbors, or his neighbors will not help him".

Example 5: Verify the validity of the following.

If one person is more successful than another, then he has worked harder to deserve success.

Naveen has not worked harder than Amul.

Therefore, Naveen is not more successful then Amul.

Sol: Let S(x,y) : 'x is more successful than y'

W(x,y): 'x has worked harder than y to deserve the success'

n : 'Naveen'

a : 'Amul'

Then the inference pattern is

$$\begin{array}{r} (\forall x)\ (\forall y)\ [S(x,y) \rightarrow W(x,y)] \\ \sim W(n,a) \\ \hline \sim S(n,a) \end{array}$$

[1]	(1)	$\sim W(n,a)$	Rule P
[2]	(2)	$(\forall x)\ (\forall y)\ [S(x,y) \rightarrow W(x,y)]$	Rule P
[2]	(3)	$(\forall y)\ [S(n,y) \rightarrow W(n,y)]$	Rule US, from (2)
[2]	(4)	$S(n,a) \rightarrow W(n,a)$	Rule US, from (3)
[1,2]	(5)	$\sim S(n,a)$	Rule T, from (1) & (4)

Thus the inference is valid.

6: Show that $(\forall x)\ (\forall y)\ [P(x,y)] \rightarrow (\exists\ x)\ (\forall y)\ P(x,y)$ logically valid statement.

7: Show that $(\forall x)\ (\exists\ y)\ [P(x,y)] \rightarrow (\exists\ x)\ (\exists\ y)\ P(x,y)$ logically valid statement.

8: Show that $(\forall x)\ [H(x) \rightarrow A(x)] \rightarrow (\forall x)[(\exists y)(H(y) \wedge N(x,y)) \rightarrow (\exists y)(A(y) \wedge N(x,y))]$ logically valid statement.

9: Show that $\sim P(a,b)$ follows logically from $(\forall x)(\forall y)[P(x,y) \rightarrow W(x,y))$ and $\sim W(a,b)$

Discrete Mathematics (DM)- ()Unit

2 : First order logic

2.1.Predicates

2.2.Quantifiers

2.3.Free and Bound Variables

2.4. Inference theory or Rules of Inference

2.1. Predicate Calculus

The propositional logic is not powerful enough to represent all types of statements that are used in Computer Science and Mathematics, or to express certain types of relationship between propositions such as equivalence.

For example, the statement "X is greater than 1", where X is a variable, is not a proposition because you can not tell whether it is true or false unless you know the value of X.

Thus the propositional logic can not deal with such sentences. However, such statements appear quite often in Mathematics and we want to do inferenceing on those statements.

- **Not all birds fly" is equivalent to "Some birds don't fly".**
- **"Not all integers are even" is equivalent to "Some integers are not even".**
- **"Not all cars are expensive" is equivalent to "Some cars are not expensive".**

Each of those propositions is treated independently of the others in propositional logic.

Example: **if P represents "Not all birds fly" and**

Q represents "Some integers are not even",

then there is no mechanism in propositional logic to find out that P is equivalent to Q.

- **Thus we need more powerful logic to deal with these and other problems. The predicate logic is one of such logic and it addresses these issues among others.**

2.1. Predicates:

A predicate is a verb phrase template that describes a property of objects, or a relationship among objects represented by the variables.

The logic based upon the analysis of predicates in any statement is called Predicate logic.

Symbolize a predicate by a capital letter and names of individuals or objects in general by small letters.

Example 1: The statement '**x is a student**' has two parts.

Part 1: The variable x is the subject of the statement.

Part 2: The predicate ' **is a student**' refers to a property that the subject of the statement can have.

We can denote the statement ' x is a student' by S(x) where **S** denotes the **predicate** and **x** is a **variable**.

In general any statement of the type 'p is Q' where Q is the predicate and p is the subject can be denoted by Q(p)

Example 2: Amulya is a Student and This painting is Blue.

$$S(a) \wedge B(p).$$

A predicate requiring m(m>0) names or objects is called an m-place predicate.

Example 3: Amulya is a Student

'is a student' is a 1-place predicate because it is related to one object(Amulya).

Example 4: Naveen is taller than Amul.

The predicate 'is taller than' is a 2-place predicate.

The representation is T(n,a)

When m=0 , then we shall call a statement 0-place predicate because no names are associated with a statement.

A Simple statement function of one variable is defined to be an expression consisting of a predicate symbol and an individual variable.

We can form 'Compound statement functions by combining one or more simple statement functions and the logical connectives.

$M(x) \vee N(x)$, $M(x) \wedge N(x)$, $M(x) \rightarrow N(x)$, $\sim M(x)$ and $M(x) \leftrightarrow N(x)$.

Some restrictions can be introduced by limiting the class of objects under considerations. These limitation means that the variable which are mentioned stand for only those objects which are members of particular set or class. Such a restricted class is called the universe of discourse or the domain of individuals or simply the universe.

Example 5: consider the statement

"Given any positive integer, there is greater positive integer"

in this case the universe of discourse is the set of positive integers.

2.2. Quantifiers

The statements involve words that indicate quantity such as 'all', 'some', 'none', or 'one'. These words indicates quantity and they are called Quantifiers.

Sentence	Abbreviated Meaning
Some men are tall.	There is atleast one tall man.
All birds have wings.	
No air balloon is perfectly round.	All air balloons fail to be perfectly round.
There is a real number less than 11.	Atleast one real number is less than 11.

There are two types of quantifiers.

1. **Universal**
2. **Existential**

Universal quantifier: **The quantifier "all" is called as the Universal quantifier, Denoted as $\forall x$.**

The symbol $\forall x$ Represents each of the following phrases have same meaning.

- ✓**For all x**
- ✓**For every x**
- ✓**For each x**
- ✓**Every thing x is such that**
- ✓**Each thing x is such that**

Existential quantifier: **The quantifier "some" is the Existential quantifier. Denoted as $\exists x$.**

The symbol $\exists$ x Represents each of the following phrases have same meaning

- ✓ **For some x**
- ✓**Some x is such that**
- ✓**There exists an x such that**
- ✓**There is an x such that**
- ✓**There is at least one x such that**

Example 1: Some thing is Good

Solution : "There is atleast one x such that x is good"

The Symbolic form: $(\exists x)\ G(x)$

Example 2: Every thing is Good

Solution : "For all x, x is good"

The Symbolic form: $(\forall x)\ G(x)$

Example 3: Nothing is Good

Solution : "For all x, x is not good"

The Symbolic form: $(\forall x)\ \sim G(x)$

Example 4: Something is not Good

Solution : "There is atleast one x such that x is good"

The Symbolic form: $(\exists x)\ \sim G(x)$

Equivalent Formulas:

✓"All true" means the same as "None false".

✓"All false" means the same as "None true".

✓"Not all true" means the same as "Atleast one false".

✓"Not all false" means the same as "Atleast one true".

✓ $(\forall x)\, F(x) \Leftrightarrow \sim(\exists x) \sim F(x)$

✓ $(\forall x) \sim F(x) \Leftrightarrow \sim(\exists x)\, F(x)$

✓ $\sim[\forall x, F(x)] \Leftrightarrow (\exists x) \sim F(x)$

✓ $\sim[(\forall x) \sim F(x)] \Leftrightarrow (\exists x)\, F(x)$

The symbol $\exists!x$ is read there is a unique x such that ... or There is one and only one x such that ...

Ex: There is one and only one even prime.

$\exists!x$, [x is an even prime]

$\exists!x$, P(x) where P(x)≡x is an even prime integer.

To form the negation of a statement involving one quantifier, change the quantifier form universal to existential, or from existential to universal, and negate the statement, which it quantifies.

Statement	Its Negation
$\forall x\, P(x)$	$[\exists x \sim P(x)]$
$\exists x\, P(x)$	$[\forall x \{\sim P(x)\}]$

Example 1: All monkeys have tails

Solution : “For all x, if x is a monkey, then x has tail”

The Symbolic form: $(\forall x)\ [M(x) \rightarrow T(x)]$

Example 2: No monkey has a tail.

Solution : “For all x, if x is a monkey, then x has no tail”

The Symbolic form: $(\forall x)\ [M(x) \rightarrow \sim T(x)]$

Example 3: Some monkeys have tails

Solution : “There is an x such that, x is a monkey and x has tail”

The Symbolic form: $(\exists x)\ [M(x) \wedge T(x)]$

Example 4: Some monkeys have no tails

Solution : “There is an x such that, x is a monkey and x has no tail”

The Symbolic form: $(\exists x)\ [M(x) \wedge \sim T(x)]$

Example 1: All men are good.

Solution : "For all x, if x is a man, then x is Good."

The Symbolic form: $(\forall x)\ [M(x) \rightarrow G(x)]$

Example 2: No men are good.

Solution : "For all x, if x is a man, then x is not Good"

The Symbolic form: $(\forall x)\ [M(x) \rightarrow \sim G(x)]$

Example 3: Some men are good.

Solution : "There is an x such that, x is a man and x is Good."

The Symbolic form: $(\exists x)\ [M(x) \wedge G(x)]$

Example 4: Some men are not good.

Solution : "There is an x such that, x is a man and x is not tail"

The Symbolic form: $(\exists x)\ [M(x) \wedge \sim G(x)]$

Write the following sentences is the closed form or Symbolic form.

1. **Some people who trust others one rewarded.**
2. **If any one is good then john is good.**
3. **He is ambitious or no one is ambitious.**
4. **Some one is teasing**
5. **It is not true that all roads lead to rome.**

Solution : Let

P(x) : x is a Person

T(x) : Trust others

R(x) : is rewarded

G(x) : is good

A(x) : is ambitious

Q(x) : is teasing

S(x) : is a road

L(x) : leads to Rome

1: Some people who trust others one rewarded.

Solution : "There is one x such that, x is a person, x trusts others and x is rewarded."

The Symbolic form: $(\exists x)\ [P(x) \wedge T(x) \wedge R(x)]$

2: If any one is good then john is good.

Solution : "If there is one x such that x is a person and x is good then john is good."

The Symbolic form: $(\exists x)\ [P(x) \wedge G(x)] \rightarrow G(John)$

3: He is ambitious or no one is ambitious.

Solution : He represents a particular person. Let that person be y. so "y is ambitious or for all x, if x is person then x is not ambitious."

The Symbolic form: $A(y)\ V\ ((\forall x)\ [P(x) \rightarrow \sim A(x)]$

4: Some one is teasing

Solution : "There is one x such that, x is a person and x is teasing"

The Symbolic form: $(\exists x)\,[P(x) \wedge Q(x)]$

5: It is not true that all roads lead to rome.

Solution : The statement can be written as

$$\sim(\forall x)\,[S(x) \rightarrow L(x)]$$

Or

$$(\exists x)\,[S(x) \wedge \sim L(x)]$$

Translate each of the following statements into symbols,using quantifiers,variables,and predicate symbols.

1.All birds can fly.

2.Not all birds can fly.

3.All babies are illogical.

4.Some babies are illogical.

5.If x is a man, then x is a giant.

6.Some men are giants.

7.Some men are not giants.

8.All men are giants.

9.No men are giants.

10.There is a student who likes mathematics but not history.

11. x is an odd integer and x is prime.

12. For all integers x, x is odd and x is prime.

13. For each integer x, x is x is prime.

14. There is an integer x such that x is odd and is prime

15. Not every actor is talented who is famous.

16. Some nos. are rational.

17. Some nos. are not rational.

18. Not all nos. are rational.

19. Not every graph is planar.

20. If some students are lazy, then all students are lazy.

21. x is rational implies that x is real.

22. Not all cars have Carburetors.

23. Some people are either religious or pious.

24. No dogs are intelligent.

25. All babies are illogical.

26. Every no. either is negative or has a square root.

27. Some numbers are not real.

28. Every connected and circuit free graph is a tree.

29. Not every graph is connected.

Statement formula in Predicate Calculus

$P(x_1,x_2,\ldots..x_n)$ denotes an n-place predicate formula in which the letter P is an n-place predicate and $x_1,x_2,\ldots..x_n$ are objects or individual variables.

In general $P(x_1,x_2,\ldots..x_n)$ will be called an atomic formula of predicate calculus.

Examples are R, Q(x), A(x,y,z) and A(x,y)

A wff of predicate calculus formula is obtained by using the following rules.

1. **An atomic formula is a wff.**
2. **If A is a formula, then ~A also a wff.**
3. **If A and B are wffs then $A \vee B$, $A \wedge B$, $A \rightarrow B$ and $A \leftrightarrow B$ are also wffs.**
4. **If A is wff x is any variable, then $\forall x\, A(x)$ and $\exists\, x\, A(x)$ are wff.**
5. **Only those formulas obtained by using rules(1) to (4) are wffs.**

Free and Bound Variables

Generally predicate formulas contain a part of the form (∀x)P(x) or (∃x)P(x), such a part is called an x-bound part of the formula.

Any variable appearing in an x-bound part of a formula is called a bound variable, otherwise it is called free variable.

The formula P(x) immediately following either (∀x) or (∃x) is described as the scope of the quantifier.

Example: (∀x)A(x,y)

Here the scope of (∀x) is A(x,y)

A(x,y) is the scope of the quantifier

x is bounded occurrence.

y is free occurrence.

Valid Formula and Equivalences

Example 1: Show that (∀x)P(x) →(∃x)P(x) is a tautologically valid statement.

Sol: (∀x)P(x) is true in particular universe then the universe has atleast one object t in it and P(t) is a true statement for every t in the universe. In particular P(t) must be true. Thus (∃x)P(x) is true. Therefore (∀x)P(x)→(∃x)P(x) is a tautologically valid statement

if Why can't we use implication for the existential quantifier?

Example: All Apples are Delicious

Let F be the domain of fruits and

A(x):is an apple D(x):is delicious

∀x∈F(A(x)→D(x)) says "any fruit, if it is an apple, then it is delicious," or simply, "apples are delicious fruit".

$\forall x \in F(A(x) \wedge D(x))$ says "any fruit, is an apple *and* is delicious", or simply "all fruit are delicious apples.“

Example: Some Apples are Delicious

$\exists x \in F(A(x) \wedge D(x))$ says "some fruits, is an apple and is delicious," or simply "there is a delicious apple".

$\exists x \in F(A(x) \rightarrow D(x))$ says "there is some fruit, that if it were an apple then it would be delicious".

Predicate calculus : theory of inference

The Generalization and Specification rules are

Quantified Propositions:

Fundamental rule US: (Universal Specification)

If a statement of a form ∀x P(x) is assumed to be true, then the universal quantifier can be dropped to obtain P(t) is true for an arbitrary object t in the universe. In symbols, he rule is,

$$\frac{(\forall x)\ P(x)}{\therefore P(t) \text{ for all } t}$$

Fundamental Rule UG: (Universal Generalisation)

If a statement P(t) is true for all t of the universe, then the universal quantifier may be prefixed to obtain (∀x) P(x). It is represented as

$$\frac{P(t) \text{ for all } t}{\therefore (\forall x)\ P(x)}$$

Fundamental Rule ES: (Existential Specification)

If $(\exists x)\ P(x)$ is assumed to be true, then there is an element t in the universe such that P(t) is true. This may be represented as

$$\underline{(\exists x)\ P(x)}$$
$$\therefore\ P(t) \text{ for some } t$$

Fundamental Rule EG: (Existential Generalization)

If P(t) is true for some element t in the universe then $(\exists x)\ P(x)$ is true. This may be represented as

$$\underline{P(t) \text{ for some } t}$$
$$\therefore\ (\exists x)\ P(x)$$

Example 1: verify the validity of the following argument.

Every living thing is a plant or an animal.

John's gold fish is alive and it is not a plant.

All animals have hearts.

Therefore John's gold fish has a heart.

Let the universe consist of all living things.

P(x) : x is Plant.

A(x) : x is an animal

H(x) : x has a Heart.

G: John's gold fish

Then the inference pattern is

$$(\forall x)\,[P(x) \vee A(x)]$$
$$\sim P(g)$$
$$(\forall x)\,[A(x) \rightarrow H(x)]$$

$$\therefore H(g)$$

[1]	(1)	$(\forall x)\,[P(x) \vee A(x)]$	Rule P
[2]	(2)	$\sim P(g)$	Rule P
[1]	(3)	$P(g) \vee A(g)$	Rule US, from (1)
[1,2]	(4)	$A(g)$	Rule T, from (2) and (3)
[5]	(5)	$(\forall x)\,[A(x) \rightarrow H(x)]$	Rule P
[5]	(6)	$A(g) \rightarrow H(g)$	Rule US
[1,2,5]	(7)	$H(g)$	Rule T, from (4) and (6)

Thus the conclusion is valid.

Example 2: verify the validity of the following argument.

Lions are dangerous animals.

There are lions.

$\therefore$ There are dangerous animals.

L(x) : x is Lion.

A(x) : x is an animal

Then the inference pattern is

$$
\begin{array}{r}
(\forall x)\,[L(x) \rightarrow A(x)] \\
(\exists x)\,L(x) \\
\hline
\therefore (\exists x)\,A(x)
\end{array}
$$

[1]	(1)	$(\exists x)\,L(x)$	Rule P
[1]	(2)	$L(b)$	Rule ES, FROM (1)
[3]	(3)	$(\forall x)\,[L(x) \rightarrow A(x)]$	Rule P
[3]	(4)	$L(b) \rightarrow A(b)$	Rule EG, from (3)
[1,3]	(5)	$A(b)$	Rule T from (2) and (4)

Thus the conclusion is valid.

Example 3: verify the validity of the following argument.

All men are mortal.

Socrates is a man .

$\therefore$ socrates is a mortal.

H(x) : x is man.

M(x) : x is a mortal.

S: Socrates

Then the inference pattern is

$$(\forall x)\,[H(x) \rightarrow M(x)] \wedge H(s) \Rightarrow M(s)$$

[1]	(1)	$(\forall x)\,[H(x) \rightarrow M(x)]$	Rule P
[1]	(2)	$H(s) \rightarrow M(s)$	Rule US, From (1)
[3]	(3)	$H(s)$	Rule P
[1,3]	(4)	$M(s)$	Rule T, from (2) and (3) I_{11}

Thus the inference is valid.

4: verify the validity of the following argument

All men are fallible.

All kings are men.

∴ All kings are fallible.

Let M(x) : "x is a man"

K(x) : "x is a king"

F(x) : "x is fallible"

The above argument is symbolized as

$$\forall x, [M(x) \rightarrow F(x)]$$

$$\underline{\forall x, [K(x) \rightarrow M(x)]}$$

$$\therefore \forall x, [K(x) \rightarrow F(x)]$$

Proof:

[1]	(1)	$\forall x, [K(x) \rightarrow M(x)]$	Rule P
[1]	(2)	$K(c) \rightarrow M(c)$	Rule US, from (1)
[3]	(3)	$\forall x, [M(x) \rightarrow F(x)]$	Rule P
[3]	(4)	$M(c) \rightarrow F(c)$	Rule US, from (3)
[1,3]	(5)	$K(c) \rightarrow F(c)$	Rule T, from (2) & (4) and chain rule
[1,3]	(6)	$\forall x, [K(x) \rightarrow F(x)]$	Rule UG, from (5)

Thus the inference is valid.

5: Symbolize the following argument and check for its validity

All integers are rational numbers.

Some integers are powers of 3.

$\therefore$ Some rational numbers are powers of 3.

6: Show that from

a. $(\exists x)(F(x) \wedge S(x)) \rightarrow (\forall y)(M(y) \rightarrow W(y))$

b. $(\exists y)(M(y) \wedge \sim W(y))$

The conclusion $(\forall x)(F(x) \rightarrow \sim S(x))$ follows.

7: Show that $(\forall x)(P(x) \vee Q(x)) \Rightarrow (\forall x) P(x) \vee (\exists x) Q(x))$

8. Is the following conclusion validity derivable from the premises given?

If $(\forall x)(P(x) \rightarrow Q(x))$; $(\exists y) P(y)$, then $(\exists z) Q(z)$.

9. Using CP or otherwise obtain the following implication.

$(\forall x)(P(x) \rightarrow Q(x)), (\forall x)(R(x) \rightarrow \sim Q(x)) \Rightarrow (\forall x)(R(x) \rightarrow \sim P(x))$

10. Show that $(\exists x)(P(x) \wedge Q(x)) \rightarrow ((\exists x) P(x) \wedge (\exists x) Q(x))$ is logically valid statement.

11. Show that $(\forall x)(P(x) \rightarrow Q(x)) \rightarrow ((\forall x)P(x) \rightarrow (\forall x) Q(x))$ is logically valid statement.

12. Show that $\sim(P(x) \vee Q(x)) \leftrightarrow (\sim P(x) \wedge \sim Q(x))$ is logically valid statement.

13. Show that $P(x) \rightarrow Q(y)) \leftrightarrow (\sim P(x) \vee Q(y))$ is logically valid statement.

14. Show that $P(x) \wedge Q(y)) \rightarrow (\sim P(x) \rightarrow Q(y))$ is logically valid statement.

15. Show that $R(x) \wedge S(x)) \rightarrow R(x)$ is logically valid statement.

16. Show that $(\forall x)\ (P(x) \vee Q(x)),\ (\forall x) \sim P(x) \Rightarrow (\forall x)\ Q(x)$ is logically valid statement.

17. Show that $(\forall x)\ (P(x) \rightarrow Q(x)) \wedge (\forall x)(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)(P(x) \rightarrow R(x))$ is logically valid statement.

18. Show that $P \rightarrow ((\exists x)\ Q(x)) \Rightarrow (\exists\ x)(P(x) \rightarrow Q(x))$ is logically valid statement.

2.2.5. Formulas involving more than one quantifier :

Consider the statement P(x,y) : x likes y.

(($\exists$x) (P(x,y)) : there is an x suchthat, x likes y.

($\forall$x)(P(x,y)) : every one liked y.

($\exists$y) ($\exists$x) (P(x,y)) : there is someone whom some one likes.

($\exists$y) ($\forall$ x) (P(x,y)) : there is someone whom every body likes.

($\forall$y) ($\exists$x) (P(x,y)) : Everybody is liked by some one.

($\forall$y) ($\forall$x) (P(x,y)) : Everybody is liked by every one.

($\exists$x) ($\exists$y) (P(x,y)) : someone likes some body.

($\exists$x) ($\forall$y) (P(x,y)) : some one likes every one.

($\forall$x) ($\exists$y) (P(x,y)) : Every one likes some one.

($\forall$x) ($\forall$y) (P(x,y)) : Every one likes everybody.

$$(\exists y)\ (\exists x)\ (P(x,y)) \Leftrightarrow (\exists x)\ (\exists y)\ (P(x,y))$$

$$(\forall y)\ (\forall x)\ (P(x,y)) \Leftrightarrow (\forall x)\ (\forall y)\ (P(x,y))$$

Example 1: Symbolize "Every one who likes fun will enjoy each of these plays"

Sol: Let $L(x)$: 'x likes fun'

$P(y)$: 'y is play'

$E(x,y)$: x will enjoy y

the statement can be represented as "for each x, if x likes fun and for each y, if y is a play, then x enjoys y". Symbolically $(\forall x)\ (\forall y)\ [L(x) \wedge P(y)] \rightarrow E(x,y)$

2: write the Symbolic form and negate the statement "Everyone who is healthy can do all kinds of work".

3: write the Symbolic form and negate the statement "Some people are not admired by everyone".

4: write the Symbolic form and negate the statement "Everyone should help his neighbors, or his neighbors will not help him".

Example 5: Verify the validity of the following.

If one person is more successful than another, then he has worked harder to deserve success.

Naveen has not worked harder than Amul.

Therefore, Naveen is not more successful then Amul.

Sol: Let S(x,y) : 'x is more successful than y'

W(x,y): 'x has worked harder than y to deserve the success'

n : 'Naveen'

a : 'Amul'

Then the inference pattern is

$$(\forall x)\,(\forall y)\,[S(x,y) \rightarrow W(x,y)]$$
$$\sim W(n,a)$$
$$\overline{\hspace{10em}}$$
$$\sim S(n,a)$$

[1]	(1)	$\sim W(n,a)$	Rule P
[2]	(2)	$(\forall x)(\forall y)[S(x,y)\rightarrow W(x,y)]$	Rule P
[2]	(3)	$(\forall y)[S(n,y)\rightarrow W(n,y)]$	Rule US, from (2)
[2]	(4)	$S(n,a)\rightarrow W(n,a)$	Rule US, from (3)
[1,2]	(5)	$\sim S(n,a)$	Rule T, from (1) & (4)

Thus the inference is valid.

6: Show that $(\forall x)(\forall y)[P(x,y)]\rightarrow(\exists x)(\forall y)P(x,y)$ logically valid statement.

7: Show that $(\forall x)(\exists y)[P(x,y)]\rightarrow(\exists x)(\exists y)P(x,y)$ logically valid statement.

8: Show that $(\forall x)[H(x)\rightarrow A(x)]\rightarrow(\forall x)[(\exists y)(H(y)\wedge N(x,y))\rightarrow(\exists y)(A(y)\wedge N(x,y))]$ logically valid statement.

9: Show that $\sim P(a,b)$ follows logically from $(\forall x)(\forall y)[P(x,y)\rightarrow W(x,y))$ and $\sim W(a,b)$

Discrete Mathematics (DM)- (8F303)

Unit 3 : First order logic

3.1. Relations

- 3.1.1. Properties of binary relations
- 3.1.2. Equivalence Relations
- 3.1.3. Transitive Closure
- 3.1.4. Compatibility Relations
- 3.1.5. Partial Ordering
- 3.1.6. Hasse Diagrams
- 3.1.7. Lattices & its Properties

3.2: Algebraic Structures

- 3.2.1. Algebraic Systems Definition and examples
- 3.2.2: General Properties
- 3.2.3. Semigroups and Monoids
- 3.2.4. Groups
- 3.2.5. Subgroups
- 3.2.6. Homomorphisms
- 3.2.7. Isomorphisms

A familiar is two dimensional coordinate (x,y)

Let A and B are two sets. The Cartesian product of A and B is defined as

$$AXB = \{(a, b) \,/\, a \in A \text{ and } b \in B\}$$

In generally, the Cartesian product of n sets $A_1,A_2,\ldots.A_n$ is defined as $A_1XA_2XA_3\ldots.XA_n = \{(a_1,a_2,\ldots.a_n) \,/\, a_i \in A_i \; i= 1 \text{ to } n\}$

The expression $(a_1,a_2,\ldots.a_n)$ is called "an ordered n-tuple".

Example: Let A = {0,1,2} and B = {a,b} are two sets. Find A × B and B × A.

A × B = {(0,a), (0,b), (1,a), (1,b), (2,a), (2,b)}

B × A = {(a,0), (b,0), (a,1), (b,1), (a,2), (b,2)}

It is to be noted that A × B ≠ B × A if the sets A and b are different.

If A has m elements and B has n elements then A × B and B × A will have m × n elements.

Relation or Binary Relation:

Binary relations represent relationships between the elements of two sets.

Let A and B be two sets. A binary relation from A to B is subset of $A \times B$. A binary relation R from set A to set B is defined by: $R \subseteq A \times B$

If $(a,b) \in R$, we write aRb (a is related to b by R)

If $(a,b) \notin R$, we write $a \not\mathrel{R} b$ (a is not related to b by R)

A relation is represented by a set of ordered pairs

If A = {a, b} and B = {1, 2, 3}, then a relation R_1 from A to B might be, for example, R_1 = {(a, 2), (a, 3), (b, 2)}.

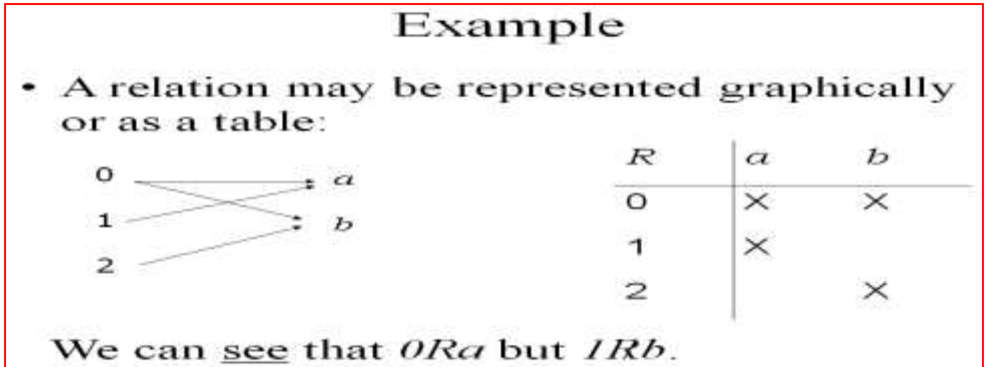
The first element in each ordered pair comes from set A, and the second element in each ordered pair comes from set B

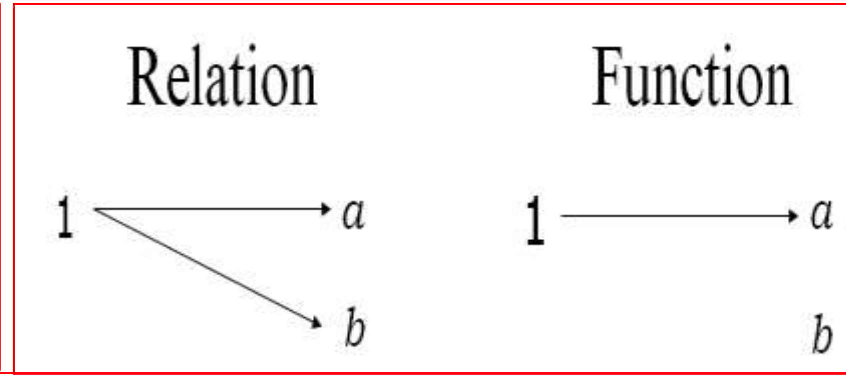
Then R = {(0,a), (0,b), (1,a), (2,b)} is a relation from A to B.

- ✓ **Can we write 0Ra ?**
- ✓ **Can we write 2Rb ?**
- ✓ **Can we write 1Rb ?**

Functions as Relations

A function is a relation that has the restriction that each element of A can be related to exactly one element of B.





Relations on a Set

Relations can also be from a set to itself.

A relation on the set A is a relation from set A to set A, i.e., R $\subseteq$ A $\times$ A

Let A = {1, 2, 3, 4} Which ordered pairs are in the relation R={(a,b) | a divides b}?

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

Which of these relations (on the set of integers) contain each of the pairs (1,1), (1,2), (2,1), (1,-1), and (2,2)?

$R_1 = \{(a,b) \mid a \leq b\}$

$R_2 = \{(a,b) \mid a > b\}$

$R_3 = \{(a,b) \mid a = b, a = -b\}$

$R_4 = \{(a,b) \mid a = b\}$

$R_5 = \{(a,b) \mid a = b + 1\}$

$R_6 = \{(a,b) \mid a + b \leq 3\}$

The pair (1,1) is in R_1, R_3, R_4 and R_6

The pair (1,2) is in R_1 and R_6

The pair (2,1) is in R_2 , R_5 and R_6

The pair (1,-1) is in R_2 , R_3 and R_6

The pair (2,2) is in R_1 , R_3 and R_4

How many relations are there on a set with n elements? 2^{n^2}

If A has n elements, how many elements are there in $A \times A$? n^2

How many relations are there on set $S = \{a, b, c\}$?

There are 3 elements in set S, so $S \times S$ has $3^2 = 9$ elements.

Therefore, there are $2^9 = 512$ different relations on the set $S = \{a, b, c\}$.

What is the total number of relations for a set that are containing elements?

$$|\mathcal{P}(S \times S)| = 2^{|S|^2}$$

A relation on a set, S, is a subset of $S \times S$.

The total number of such relations is the cardinality of the power set, $\mathcal{P}(S \times S)$, the set of all subsets of ordered pairs from S.

This grows exponentially with the size of the set. For example, a set $S = \{a, b, c\}$, containing only three elements, already has $2^9 = 512$ possible relations. Add a fourth element and you have $2^{16} = 65\,536$ relations...

3.1.1. Properties of Relations

Let R be a relation on set A is said to be

(i) Reflexive: if xRx or $(x,x) \in R$ for every $x \in A$.

Determine the properties of the following relations on {1, 2, 3, 4} Which of these is reflexive?

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

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

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$R_6 = \{(3,4)\}$

The relations R_3 and R_5 are reflexive because they contain all pairs of the form (a,a); the other don't [they are all missing (3,3)].

(ii) Irreflexive: **A relation R on a set A is called irreflexive if and only if <x, x>∉R for every element a of A.**

if $x \not{R} x$ or $(x,x) \notin R$ for every $x \in A$.

Determine the properties of the following relations on {1, 2, 3, 4}.

Which of these are Irreflexive?

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

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

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$R_6 = \{(3,4)\}$

The relations R_4 and R_6 are irreflexive. The other don’t [they are all has (1,1)].

(iii) Symmetric: if $xRy \Rightarrow yRx$ for all $x,y \in A$

A relation is symmetric iff "x is related to y" implies that "y is related to x".

Which of these are symmetric?

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

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

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$R_6 = \{(3,4)\}$

The relations R_2 and R_3 are symmetric because in each case (y,x) belongs to the relation whenever (x,y) does.

The other relations are not symmetric.

(iv) Antisymmetric:

A relation R on a set A is called antisymmetric if and only if for any a, and b in A, whenever <a, b>$\in$R, and <b, a>$\in$R, a=b must hold. Equivalently, R is antisymmetric if and only if whenever <a, b>$\in$R , and a$\neq$ b , <b, a>$\notin$R . Thus in an antisymmetric relation no pair of elements are related to each other.

if whenever xRy and yRx, then x=y.

or

If $x \neq y$ and xRy $\Rightarrow y \not R x$ or $(y,x) \notin R$, for all $x,y \in A$.

Note: Symmetric and antisymmetric are NOT exactly opposites.

Which of these is antisymmetric?

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

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

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$R_6 = \{(3,4)\}$

The relations R_4, R_5 and R_6 are antisymmetric because there is no pair of elements a and b with $a \neq b$ such that both (a,b) and (b,a) belong to the relation. The other relations are not antisymmetric.

(v). Assymetric: if $xRy \Rightarrow y \not R x$ or $(y,x) \notin R$.

A relation R is symmetric iff, if x is related by R to y, then y is related by R to x.

For example, being a cousin of is a symmetric relation:

if John is a cousin of Bill, then it is a logical consequence that Bill is a cousin of John.

A relation R is asymmetric iff, if x is related by R to y, then y is not related by R to x.

For example, being the father of is an asymmetric relation:

if John is the father of Bill, then it is a logical consequence that Bill is not the father of John.

A relation R is non-symmetric iff it is neither symmetric nor asymmetric.

For example, loves is a non-symmetric relation:

if John loves Mary, then there is no logical consequence concerning Mary loving John.

Which of these is Assymetric?

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

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

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

$R_4 = \{(2,1), (3,1), \underline{(3,2)}, (4,1), \underline{(4,2)}, \underline{(4,3)}\}$

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$R_6 = \{(3,4)\}$

The relations R_4, R_5 and R_6 are Assymetric.

The other relations aren't Assymetric.

(vi). Transitive: if xRy and yRz $\Rightarrow$ xRz for all x, y, z $\in$ A.

Which of these is transitive?

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

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

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

$R_4 = \{ (2,1), (3,1), \underline{(3,2)}, (4,1), \underline{(4,2)} , \underline{(4,3)}\}$

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$R_6 = \{(3,4)\}$

The relations R_4, R_5 are transitive because if (x,y) and (y,z) belong to the relation, then (x,z) does also.

The other relations aren't transitive.

If A = {1,2,3,4} then the following relations holds which properties?

$R_1 = \{(1,2), (2,4)\}$

$R_2 = \{(1,1), (2,2),(3,3),(4,4),(1,3), (3,2)\}$

$R_3 = \{(1,1), (1,3), (3,1), (3,4), (4,3)\}$

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

$R_5 = \{(1,1), (2,2), (3,3), (4,4), (1,3), (3,1), (3,4), (4,3)\}$

$R_6 = \{(1,1),(2,2),(2,3),(3,2),(3,3)\}$

$R_7 = \{(1,1),(2,2),(3,3),(4,4),(1,3)\}$

R_1 not reflexive, not symmetric not transitive

R_2 reflexive, but neither symmetric nor transitive

R_3 Symmetric but neither reflexive nor transitive

R_4 transitive neither reflexive nor symmetric

R_5 reflexive symmetric bot not transitive

R_6 symmetric, transitive but not reflexive

R_7 reflexive, transitive but not symmetric

Representing Relations

There are two methods

Relation Matrix:

If $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ are finite set containing m and n elements respectively and R is a relation from A to B, then we can represent relation R by an m X n matrix, called Relation Matrix, denoted by

$$M_R = \{ M_{ij} \} \text{ where}$$

$$M_{ij} = 1 \quad \text{if } (a_i, b_j) \in R$$

$$= 0 \quad \text{if } (a_i, b_j) \notin R$$

The zero-one matrix representing the relation R has a 1 as its (i, j) entry when a_i is related to b_j and a 0 in this position if a_i is not related to b_j.

Example: Let $A=\{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4\}$ The relation R from A to B is given by $R=\{(a_1, b_1), (a_1, b_4), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_3)\}$ Find the relation matrix for R.

Example: Let $A=\{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$ The relation R from A to B is given by $R=\{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_3), (a_2, b_4), (a_3, b_1), (a_3, b_3), (a_3, b_5)\}$ Find the relation matrix for R.

Example: Let A={a, b, c} and B = {d,e} The relation R from A to B is given by R={(a, d), (b, e), (c, d)} Find the relation matrix for R.

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

Note that A is represented by the rows and B by the columns in the matrix.

Cell$_{ij}$ in the matrix contains a 1 iff a_i is related to b_j.

Relation Matrices and Properties

Let R be a binary relation on a set A and let M be the zero-one matrix for R.

R is reflexive if all t he elements on the main diagonal of M_R is 1(M_{ii} = 1 for all i)

R is symmetric iff if $M_{j\,i}$= 1 whenever $M_{i\,j}$ = 1 for all $i \neq j$ M is a symmetric matrix, i.e., $M = M^T$

R is antisymmetric if $M_{i\,j}$= 1 with $i \neq j$ then M_{ji} = 0

Suppose that the relation R on a set is represented by the matrix M_R.

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

Is R reflexive, symmetric, and / or antisymmetric?

Example

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

Is *R* reflexive?
Is *R* symmetric?
Is *R* antisymmetric?

- **All the diagonal elements = 1, so *R* is reflexive.**
- **The lower left triangle of the matrix = the upper right triangle, so *R* is symmetric.**
- **To be antisymmetric, it must be the case that no more than one element in a symmetric position on either side of the diagonal = 1. But $M_{23} = M_{32} = 1$. So *R* is not antisymmetric.**

Using Digraphs

A relation can be represented pictorially by drawing digraph as follows.

1. **A small circle is drawn for each element of A and marked with the corresponding element. These circles are called vertices.**
2. **An arrow is drawn from the vertex a_i to the vertex a_j iff a_i R a_j. This is called an edge (directed)**

An element of the form (a,a) is a relation corresponds to a directed edge from a to a. such edge is called a loop. This pictorial representation of R is called a directed graph or digraph of R.

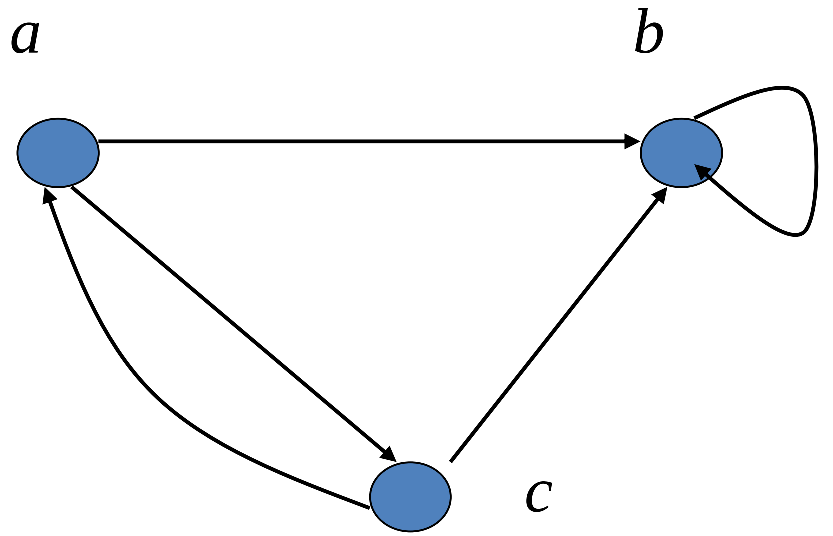
A directed graph (or digraph) consists of a set V of vertices (or nodes) together with a set E of <u>ordered pairs</u> of elements of V called edges (or arcs).

The vertex a is called the initial vertex of the edge (a, b).

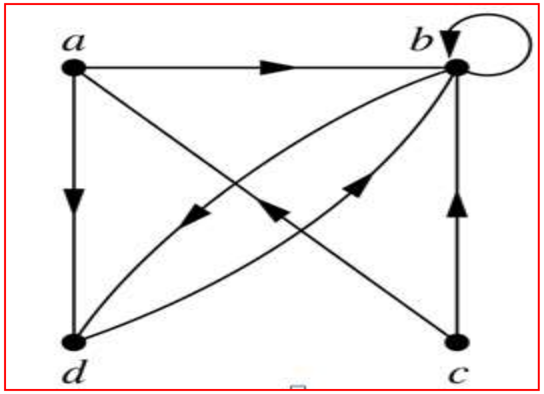
The vertex b is called the terminal vertex of the edge (a, b).

Let R be a relation on set A={a, b, c} and R={(a, b), (a, c), (b, b), (c, a), (c, b)}.

Draw the digraph that represents R

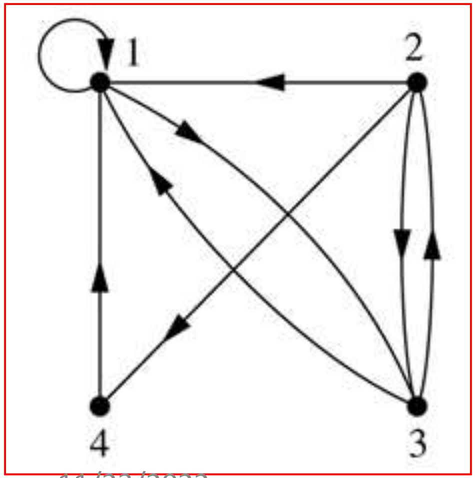


Let R be a relation on set V = {a, b, c} and R={(a, b), (a, d), (b, b),(b, d), (c, a), (c, b), (d, b)}.Draw the digraph that represents R



Note that edge (*b*, *b*) is represented using an arc from vertex *b* back to itself. This kind of an edge is called a *loop*.

What are the ordered pairs in the relation *R* represented by the directed graph to the below?

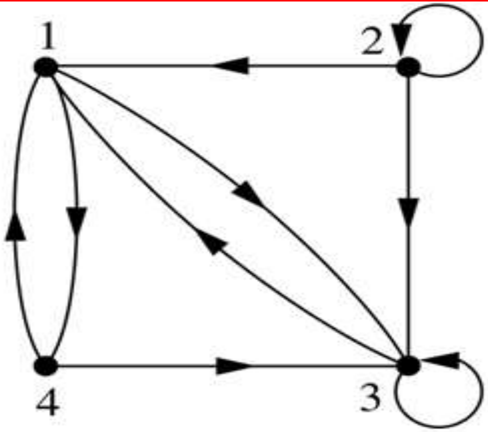


This digraph represents the relation

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

on the set {1, 2, 3, 4}.

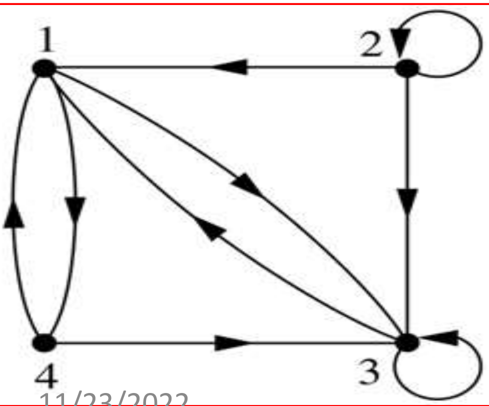
What are the ordered pairs in the relation *R* represented by the directed graph to the below?



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

According to the digraph representing *R*:

- **is (4,3) an ordered pair in *R*?**
- **is (3,4) an ordered pair in *R*?**
- **is (3,3) an ordered pair in *R*?**



(4,3) is an ordered pair in *R*

(3,4) is <u>not</u> an ordered pair in *R* – no arrowhead pointing from 3 to 4

(3,3) is an ordered pair in *R* – loop back to itself

Relation Digraphs and Properties

A relation digraph can be used to determine whether the relation has various properties

A relation is Reflexive iff there is a loop at every vertex in directed graph. So that every order pair of the form (x, x) occurs in the relation.

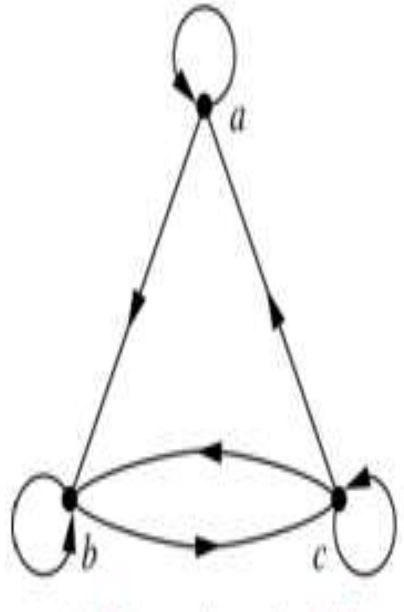
A relation is Symmetric iff for every edge between two distinct vertices in its digraph there is an edge in the opposite direction. So that (y, x) in the relation whenever (x, y) in the relation.

A relation is Antisymmetric iff there are never two edges in opposite direction between two distinct vertices.

A relation is Transitive iff whenever there is an edge from a vertex x to vertex y and an edge from vertex y to vertex z, there is an edge from x to z.

According to the digraph representing *R*:

- **is *R* Reflexive?**
- **is *R* Symmetric?**
- **is *R* Antisymmetric?**
- **is *R* Transitive?**

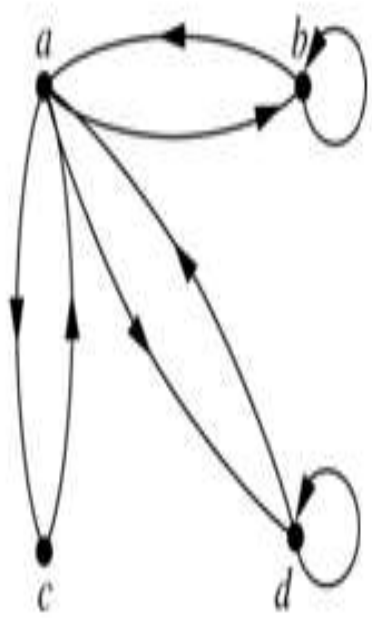


(a) Directed graph of *R*

- **R is Reflexive – there is a loop at every vertex**
- **R is not Symmetric – there is an edge from *a* to *b* but not from *b* to *a***
- **R is not Antisymmetric – there are edges in both directions connecting *b* and *c***
- **R is not Transitive – there is an edge from *a* to *b* and an edge from *b* to *c*, but not from *a* to *c***

According to the digraph representing *S*:

- is *S* Reflexive?
- is *S* Symmetric?
- is *S* Antisymmetric?
- is *S* Transitive?



(b) Directed graph of *S*

- S is not Reflexive – there aren't loops at every vertex
- S is Symmetric – for every edge from one distinct vertex to another, there is a matching edge in the opposite direction
- S is not Antisymmetric – there are edges in both directions connecting *a* and *b*
- S is not transitive – there is an edge from *c* to *a* and an edge from *a* to *b*, but not from *c* to *b*

Partitions (partition of a set A divides A into non-overlapping subsets)

Let A be a non empty set and $A_1, A_2, A_3, \ldots, A_n$ are the sub sets of A. A set denoted by π is called a Partition Set of A if

i). If $A_i \cap A_j = \phi$. $i \neq j$

ii). $\cup A_i = A$. i = 1 to n.

Example 1: Let A = {a, b, c, d, e, f, g, h, i, j}

Let the subsets are

$A_1 = \{ a, b, c, d, e\}$

$A_2 = \{ f, g, h\}$

$A_3 = \{ i, j\}$

$A_4 = \{ a, b, c, d\}$

$A_5 = \{ c\}$

Now $\pi_1 = \{A_1, A_2, A_3\}$ is a partition because

$A_1 \cap A_2 = \phi$ $A_1 \cap A_3 = \phi$ $A_2 \cap A_3 = \phi$ also $A_1 \cup A_2 \cup A_3 = A$.

But $\pi_2 = \{A_1, A_4, A_5\}$ is not a partition because $A_1 \cap A_4 \neq \phi$.

$\pi_3 = \{A_2, A_4, A_5\}$ is not a partition because $A_4 \cap A_5 \neq \phi$ and $A_2 \cup A_4 \cup A_5 \neq A$.

Example 2: $S = \{a, b, c, d, e, f\}$ and $S_1 = \{a, d, e\}$, $S_2 = \{b\}$, $S_3 = \{c, f\}$, the $P = \{S_1, S_2, S_3\}$. Is P is a partition of set S?.

Yes, it is Partition. Because $S_1 \cap S_2 = \phi$, $S_1 \cap S_3 = \phi$, $S_2 \cap S_3 = \phi$ also $S_1 \cup S_2 \cup S_3 = S$.

Example 3: If $S = \{1, 2, 3, 4, 5, 6\}$, then $A_1 = \{1, 3, 4\}$, $A_2 = \{2, 5\}$, $A_3 = \{6\}$ the $P = \{A_1, A_2, A_3\}$. Is P is a partition of set S?.

Yes, it is Partition. Because $A_1 \cap A_2 = \phi$, $A_1 \cap A_3 = \phi$, $A_2 \cap A_3 = \phi$ also $A_1 \cup A_2 \cup A_3 = S$.

Example 4: If $S = \{1, 2, 3, 4, 5, 6\}$, then $A_1 = \{1, 3, 4, 5\}$, $A_2 = \{2, 5\}$, $A_3 = \{6\}$ the $P = \{A_1, A_2, A_3\}$. Is P is a partition of set S?.

No, it is not Partition. Because $A_1 \cap A_2 = \{5\} \neq \phi$.

Example 5: If $S = \{1, 2, 3, 4, 5, 6\}$, then $A_1 = \{1, 3\}$, $A_2 = \{2, 5\}$, $A_3 = \{6\}$. The $P = \{A_1, A_2, A_3\}$. Is P is a partition of set S?.

No, it is not Partition. Because $A_1 \cap A_2 = \phi$, $A_1 \cap A_3 = \phi$, $A_2 \cap A_3 = \phi$ but $A_1 \cup A_2 \cup A_3 \neq S$.

Example 6: If $S = \{1, 2, 3, 4, 5, 6\}$, then $A_1 = \{1, 3, 4\}$, $A_2 = \{2, 5\}$, $A_3 = \{6, 7\}$. The $P = \{A_1, A_2, A_3\}$. Is P is a partition of set S?.

No, it is not Partition. Because $A_1 \cap A_2 = \phi$, $A_1 \cap A_3 = \phi$, $A_2 \cap A_3 = \phi$ but $A_1 \cup A_2 \cup A_3 \neq S$. that is 7 not in S.

3.1.2. Equivalence Relations

A relation R on set X is called an Equivalence Relation if it is: Reflexive, Symmetric, and Transitive

Two elements a and b that are related by an equivalence relation are said to be equivalent. We use the notation a~b to denote that a and b are equivalent elements with respect to a particular equivalence relation.

Definition: **Let n be a positive integer. For integers a and b we say that a is congruent to b modulo n, and write $a \equiv b \pmod{n}$, provided $a - b$ is divisible by n.**

Example 1: Let X = {1, 2, 3, 4, 5, 6, 7} and R = {(x, y) / x – y is divisible by 3} in X. Show that R is an equivalence relation?

Sol :

XXX={(1,1)(1,2)(1,3)(1,4)(1,5)(1,6)(1,7),(2,1)(2,2),(2,3)(2,4)(2,5)(2,6)(2,7)(3,1)(3,2)(3,3)(3,4)(3,5)(3,6)(3,7)(4,1)(4,2)(4,3)(4,4)(4,5)(4,6)(4,7)(5,1)(5,2)(5,3)(5,4)(5,5)(5,6)(5,7)(6,1)(6,2)(6,3)(6,4)(6,5)(6,6)(6,7)(7,1)(7,2)(7,3)(7,4)(7,5)(7,6)(7,7)}

R={ (1,1)(1,4)(1,7)(2,2)(2,5)(3,3)(3,6)(4,1)(4,4)(4,7)(5,2)(5,5)(6,3)(6,6)(7,1)(7,3)(7,7)}

For any a ∈ X, a – a is divisible by 3. {(1,1)(2,2)(3,3)(4,4)(5,5)(6,6)(7,7)}

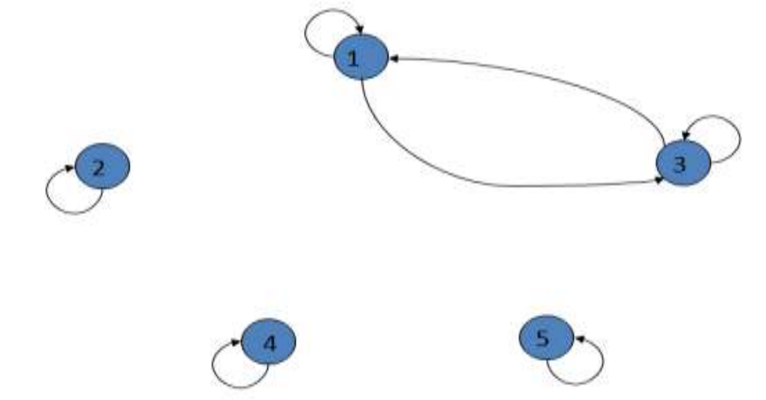
Hence aRa. There fore R is Reflexive.

For any a,b ∈ X, if a – b is divisible by 3, then b – a is also divisible by 3. that is aRb ⇔ bRa. There fore R is Symmetric.

For any a,b,c ∈ X, if aRb and bRc then both a – b and b – c are divisible by 3. So that a–c=(a–b)+(b–c) is also divisible by 3. Hence aRc. There fore R is Transitive.

Therefore R is an Equivalence Relation

Example 2: Let R be a relation on set A, where A = {1, 2, 3, 4, 5} and R = {(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1)} Is R an equivalence relation?



Sol : Yes

We can solve this by drawing a relation digraph:

Reflexive – there must be a loop at every vertex.

Symmetric - for every edge between two distinct points there must be an edge in the opposite direction.

Transitive - if there is an edge from x to y and an edge from y to z, there must be an edge from x to z.

Example 3: Congruence modulo m. Let R = {(a, b) | a ≡ b (mod m)} be a relation on the set of integers and m be a positive integer > 1. Is R an equivalence relation?

Example – Show that the relation $R = \{(a, b) \mid a \equiv b(mod\ m)\}$ is an equivalence relation.
$a \equiv b(mod\ m)$ is the congruence modulo m function. It is true if and only if m divides $a - b$.

Solution – To show that the relation is an equivalence relation we must prove that the relation is reflexive, symmetric and transitive.

1. **Reflexive –** For any element a, $a - a = 0$ is divisible by m.
   $\therefore a \equiv a(mod\ m)$. So, congruence modulo m is reflexive.
2. **Symmetric –** For any two elements a and b, if $(a, b) \in R$ or $a \equiv b(mod\ m)$ i.e. $a - b$ is divisible by m, then $b - a$ is also divisible by m.
   $\therefore b \equiv a(mod\ m)$. So Congruence Modulo m is symmetric.
3. **Transitive –** For any three elements a, b, and c if $(a, b), (b, c) \in R$ then-
   $(a - b) mod\ m = 0$
   $(b - c) mod\ m = 0$
   Adding both equations,
   $$\Rightarrow (a - b) mod\ m + (b - c) mod\ m = 0$$
   $$\Rightarrow (a - b + b - c) mod\ m = 0$$
   $$\Rightarrow (a - c) mod\ m = 0$$
   $\therefore a \equiv c(mod\ m)$. So, R is transitive.

Since the relation R is reflexive, symmetric, and transitive, we conclude that R is an equivalence relation.

Example 4: R is the relation on the set of strings of English letters such that aRb iff l(a) = l(b), where l(x) is the length of the string x. Is R an equivalence relation?

Since l(a) = l(a), then aRa for any string a.

So R is Reflexive.

Suppose aRb, so that l(a) = l(b). Then it is also true that l(b) = l(a), which means that bRa.

Consequently, R is Symmetric.

Suppose aRb and bRc. Then l(a) = l(b) and l(b) = l(c). Therefore, l(a) = l(c) and so aRc.

Therefore, R is Transitive.

Therefore, R is an Equivalence Relation.

Equivalence Class

Let R be a equivalence relation on set A.

The set of all elements that are related to an element a of A is called the equivalence class of a.

The equivalence class of a with respect to R is: $[a]_R = \{s \mid (a,s) \in R\}$

When only one relation is under consideration, we will just write [a].

If $b \in [a]_R$, then b is called a representative of this equivalence class.

Let R be the relation on the set of integers such that aRb iff a = b or a = -b.

We can show that this is an equivalence relation.

The equivalence class of element a is [a] = {a, -a}

Examples: $[7] = \{7, -7\}$ $[-5] = \{5, -5\}$ $[0] = \{0\}$

Important Note : All the equivalence classes of a Relation R on set A are either equal or **disjoint** and their union gives the set A.

$$\bigcup[a]_R = A$$

The equivalence classes are also called **partitions** since they are disjoint and their union gives the set on which the relation is defined

- **Example :** What are the equivalence classes of the relation Congruence Modulo m?
- **Solution :** Let a and b be two numbers such that $a \equiv b\ (mod\ m)$. This means that the remainder obtained by dividing a and b with m is the same. Possible values for the remainder- $0, 1, 2, ..., m-1$

  Therefore, there are m equivalence classes –

  $$[0]_m, [1]_m, ..., [m-1]_m$$
  $$[0]_m = \{..., -2m, -m, 0, m, 2m, ..., \}$$
  $$[1]_m = \{..., -2m+1, -m+1, 1, m+1, 2m+1, ..., \}$$

  .

  .

  $$[m-1]_m = \{..., -2m-1, -m-1, m-1, 2m-1, ..., \}$$

Consider the equivalence relation R on set A. What are the equivalence classes? $A = \{1, 2, 3, 4, 5\}$

$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1)\}$$

Just look at the aRb relationships. Which elements are related to which?

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

$[3] = \{3, 1\}$ $[4] = \{4\}$

$[5] = \{5\}$

A useful theorem about classes

Let R be an equivalence relation on a set A. These statements for a and b of A are equivalent: aRb

$[a] = [b]$

$[a] \cap [b] \neq \varnothing$

More importantly: Equivalence classes are EITHER equal or disjoint

Constructing an Equivalence Relation from a Partition

Given set S = {1, 2, 3, 4, 5, 6} and a partition of S, A_1 = {1, 2, 3}, A_2 = {4, 5}, A_3 = {6} then we can find the ordered pairs that make up the equivalence relation R produced by that partition.

The subsets in the partition of S, A_1 = {1, 2, 3}, A_2 = {4, 5}, A_3 = {6} are the equivalence classes of R. This means that the pair (a,b) $\in$ R iff a and b are in the same subset of the partition. Let's find the ordered pairs that are in R:

$A_1 = \{1, 2, 3\} \rightarrow (1,1), (1,2), (1,3), (2,1),(2,2), (2,3), (3,1), (3,2), (3,3)$

$A_2 = \{4, 5\} \rightarrow (4,4), (4,5), (5,4), (5,5)$

$A_3 = \{6\} \rightarrow (6,6)$

So R is just the set consisting of all these ordered pairs:

R = {(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4), (4,5), (5,4), (5,5), (6,6)}

Combining Relations operations on Relation:

Two relations from A to B can be combined in any way that two sets can be combined. Specifically, we can find the union, intersection, exclusive-or, and difference of the two relations.

Relations from A to B are subsets of $A \times B$.

For example, if A = {1, 2,3} and B= {a, b, c, d}, then R={(1, a), (2, b), (3, c)} and S = {(1,a), (1, b), (1, c), (1, d)} then

i. Intersection: $R \cap S=\{(a,b) \in AXB/(a,b) \in R$ and $(a,b) \in S\}$ is the intersection of the relation R and S. that is, $a(R \cap S)b \Leftrightarrow aRb \cap aSb$

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

ii. Union: $R \cup S=\{(a,b) \in AXB/(a,b) \in R$ or $(a,b) \in S\}$ is the union of the relation R and S. that is, $a(R \cup S)b \Leftrightarrow aRb \cup aSb$

$$R \cup S= \{(1,a), (1, b),(1, c), (1, d), (2, b), (3, c)\}$$

iii. Difference: R-S={(a,b)∈AXB/(a,b)∈R and (a,b)∉S} is the difference of the relation R and S. that is, a(R-S)b ⇔ aRb∪a not in Sb

R-S= {(2, b), (3, c)}

S-R= {(1, b), (1, c), (1,d)}

iv. Compliment: R^c={(a,b)∈AXB/(a,b)∉R is the compliment of the relation R. that is, a(R^c)b ⇔ a not related Rb

R^c= { (1,b), (1, c), (1, d), (2,a),(2, c), (2, d), (3, a), (3, b), (3, d)}

S^c = { (2,a), (2, b), (2, c), (2,d),(3, a), (3, b), (3, c), (3, d)}

Composition of Relations

If R_1 is a relation from A to B and R_2 is a relation from B to C, then the composition of R_1 with R_2 (denoted $R_1 \circ R_2$) is the relation from A to C.

If (a, b) is a member of R_1 and (b, c) is a member of R_2, then (a, c) is a member of $R_1 \circ R_2$, where $a \in A$, $b \in B$, $c \in C$.

Example 1: Let A={1,2,3}, B = {a,b,c,d} C={x,y,z} R: from A to B: {(1,a), (1, d),(2, c), (3, a), (3, d)}and S: from B to C: {(a, x), (b, x),(c, y), (c, z), (d, y)}find SoR.

SoR = ∅

RoS = {(1, x), (1, y), (2, y), (3, x), (3, y)}

Example2: Let A={a,b,c}, B={w,x,y,z}, C={A,B,C,D}, the relations R_1={(a,z),(b,w)}, R_2={(w,B),(w,D),(x,A)}. Find R1o R2.

R1o R2 = { (b, B),(b, D)}

Example 3: Find S∘R from the relations R={(1,1), (1,4), (2,3), (3,1), (3,4)} and S= {(1,0),(2,0), (3,1), (3,2), (4,1)}

iv. Given a relation R from X to Y, a relation R from Y to X is called "Converse of R". where the ordered pairs of R(bar) are obtained by inter changing the members ineach of the ordered pairs of R.

This means for $x \in X$ and $y \in Y$, thet $xRy \Leftrightarrow y$ R(bar) x

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

R(bar) = (1, 1), (4, 1), (3, 2), (1, 3), (4, 3)}

Let A = {1, 2, 3} and B= {1, 2, 3, 4}, and suppose we have the relations R_1 = {(1,1), (2,2), (3,3)} , and R_2 = {(1,1), (1,2), (1,3), (1,4)}. Then compute the operations on them.

$R_1 \cup R_2$ = {(1,1), (1,2), (1,3), (1,4), (2,2), (3,3)}

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

$R_1 - R_2$ = {(2,2), (3,3)}

$R_2 - R_1$ = {(1,2), (1,3), (1,4)}

The Powers of a Relation

The powers of a relation R are recursively defined from the definition of a composite of two relations.

Let R be a relation on the set A. The powers R^n, for n = 1, 2, 3, … are defined recursively by:

$$R^1 = R$$

$$R^2 = R \circ R$$

$$R^3 = R^2 \circ R = (R \circ R) \circ R)$$

$$R^{n+1} = R^n \circ R$$

Let R = {(1,1), (2,1), (3,2), (4,3)} Find the powers R^n , where n = 1, 2, 3, 4, 5.

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

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

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

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

$R^5 = R^4 \circ R = \{(1,1), (2,1), (3,1), (4,1)\}$

3.1.3. Transitive Closure

Important Note : A relation R on set A is transitive if and only if $R^n \subset R$ for $n = 1, 2, 3, \ldots$.

Closure of Relations :

Consider a relation R on set A. R may or may not have a property P, such as reflexivity, symmetry, or transitivity.

If there is a relation S with property P containing R such that S is the subset of every relation with property P containing R, then S is called the closure of R with respect to P.

We can obtain closures of relations with respect to property P in the following ways –

1. **Reflexive Closure –** $\Delta = \{(a, a) \mid a \in A\}$ is the diagonal relation on set A. The reflexive closure of relation R on set A is $R \cup \Delta$.
2. **Symmetric Closure –** Let R be a relation on set A, and let R^{-1} be the inverse of R. The symmetric closure of relation R on set A is $R \cup R^{-1}$.
3. **Transitive Closure –** Let R be a relation on set A. The **connectivity relation** is defined as – $R^* = \bigcup_{n=1}^{\infty} R^n$. The transitive closure of R is R^*.

Example – Let R be a relation on set $\{1, 2, 3, 4\}$ with $R = \{(1,1), (1,4), (2,3), (3,1), (3,4)\}$. Find the reflexive, symmetric, and transitive closure of R.

Solution –

For the given set, $\Delta = \{(1,1), (2,2), (3,3), (4,4)\}$. So the reflexive closure of R is

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

For the symmetric closure we need the inverse of R, which is

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

The symmetric closure of R is-

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

For the transitive closure, we need to find R^*.

$\therefore$ we need to find $R^1, R^2, \ldots,$ until $R^n = R^{n-1}$. We stop when this condition is achieved since finding higher powers of R would be the same.

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

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

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

Since, $R^2 = R^3$ we stop the process.

Transitive closure, $R^* = R^1 \cup R^2$ -

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

3.1.4. Compatibility Relation

A relation R in set X is said to be a compatibility relation if it is reflexive and symmetric. Clearly all equivalence relations are compatibility relations.

Example: Let X = {ball, bed, dog, let, egg} and the relation R be given by

R = {(x, y) / x, y ϵ X ∧ x R y if x and y contain some common letter} then R is compatibility relation, and x, y are called compatible. If xRy.

The compatibility relation is some times denoted by ≈.

Note that ball ≈bed, bed ≈egg. But ball ≠ egg is not transitive.

Maximal Compatibility Relation

Let X be a set and R is a compatibility relation on X. A is a subset of X is called a maximal compatibility block if any element of A is compatible to every other element of A and no element of X –A is compatible to all the elements of A.

3.1.5. Partial Ordering

A relation R on a set P is called a partial order relation or partial ordering on P, if R is

(1). Reflexive

(2). Antisymmetric

(3). Transitive.

POSet

We denote the Partial ordering by the symbol "$\leq$". If $\leq$ is a partial ordering on P, then the ordered pair (P, $\leq$) is called Partially Ordered Set or POSet.

If X is a partial ordering on P, then it is easy to see the converse of X, namely, $\bar{x}$ is also partial ordering on P. if X is denoted by $\leq$, then $\bar{x}$ is denoted by $\geq$.

This means that if (P, $\geq$) is a POset and (P, $\geq$) also POset .

Note: (P, $\geq$) is called the dual of (P, $\geq$).

- **Example –** Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set A.
- **Solution –** Since every set $S \subseteq S$, $\subseteq$ is reflexive. If $S \subseteq R$ and $R \subseteq S$ then $R = S$, which means $\subseteq$ is anti-symmetric. It is transitive as $R \subseteq S$ and $S \subseteq T$ implies $R \subseteq T$.

  Hence, $\subseteq$ is a partial ordering on $P(S)$, and $(P(S), \subseteq)$ is a poset.

Important Note : The symbol $\preceq$ is used to denote the relation in any poset. The notation $a \prec b$ is used to denote $a \preceq b$ but $a \neq b$.

Example 2: Let R be a relation on set $A = \{1, 2, 3, 4\}$ and $R = \{(1,1), (1,2), (1,3), (1,4), (2,2),(2,3), (2,4), (3,3), (3,4), (4,4)\}$. Is R a partial order?

Sol: Given that A = { 1,2,3,4} and

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

To be a partial order, R must be Reflexive, Antisymmetric, and Transitive.

R is Reflexive : Because R includes (1,1), (2,2), (3,3) and (4,4).

R is Antisymmetric: Because for every pair (a,b) in R, (b,a) is not in R (unless a= b).

R is Transitive: Because for every pair (a,b) in R, if (b,c) is in R then (a,c) is also in R.

So, the set A = {1, 2, 3, 4} and relation R = {(1,1), (1,2), (1,3), (1,4), (2,2),(2,3), (2,4), (3,3), (3,4), (4,4)}

R is a partial order, and (A, R) is a poset.

Example 3: Show that " greater than or equal to $(\geq)$" relation is a partial ordering on the set of integers.

Sol: To be a partial order, R must be Reflexive, Anti-symmetric, and Transitive.

Reflexive: Since $a \geq a$ for every integer a.

Therefore, "$\geq$" is reflexive

Anti-symmetric: If $a \geq b$ and $b \geq a$, then $a = b$.

Hence "$\geq$" is anti-symmetric.

Transitive : finally, $a \geq b$ and $b \geq c$ implies $a \geq c$.

Hence "$\geq$" is transitive.

Therefore "$\geq$" is a partial ordering on the set of integers and $(Z, \geq)$ is a poset.

Example 4: Show that " less than or equal to $(\leq)$" relation is a partial ordering on the set of integers.

Comparable / Incomparable

In a poset the notation a ≼ b denotes (a, b) ∈ R

The "less than or equal to" (≤)is just an example of partial ordering

The elements a and b of a poset (S, ≼) are called comparable if either a≼b or b≼a.

The elements a and b of a poset (S, ≼) are called incomparable if neither a≼b nor b≼a.

- **Example –** In the poset $(Z^+, |)$ (where Z^+ is the set of all positive integers and | is the divides relation) are the integers 3 and 9 comparable? Are 7 and 10 comparable?
- **Solution –** 3 and 9 are comparable since $3|9$ i.e. 3 divides 9. But 7 and 10 are not comparable since $7 \nmid 10$ and $10 \nmid 7$.

Total Order

Let (P, ≤) be a POSet. If for every x, y ∈ P we have either x≤y or y≤x then "≤" is called a Simple Ordering or Linear Ordering on P and (P, ≤) is called a Totally Ordered or Simply Ordered Set or a Chain.

We said "Partial ordering" because pairs of elements may be incomparable.

If every two elements of a poset (S, $\preccurlyeq$) are comparable, then S is called a totally ordered or linearly ordered set and $\preccurlyeq$ is called a total order or linear order.

Example 1: The poset (Z, ≤) is totally ordered. Why?

Every two elements of Z are comparable; that is, a ≤ b or b ≤ a for all integers.

Example 2: The poset (Z^+, |) is not totally ordered. Why?

It contains elements that are incomarable; for example $5 \nmid 7$.

3.1.6. Hasse Diagram

A partial order, being a relation, can be represented by a di-graph. But most of the edges do not need to be shown since it would be redundant.

For instance, we know that every partial order is reflexive, so it is redundant to show the self-loops on every element of the set on which the partial order is defined.

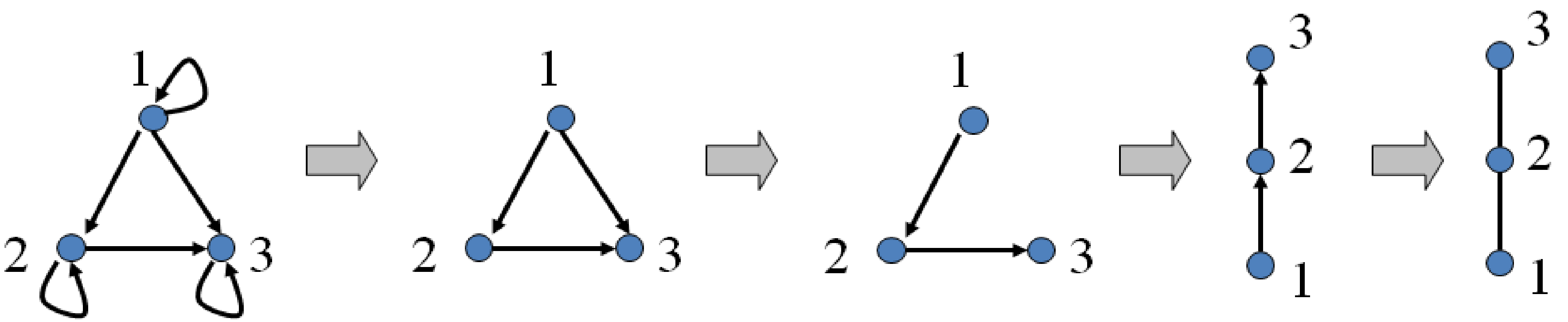
Every partial order is transitive, so all edges denoting transitivity can be removed.

The directions on the edges can be ignored if all edges are presumed to have only one possible direction, conventionally upwards.

In general, a partial order on a finite set can be represented using the following procedure –

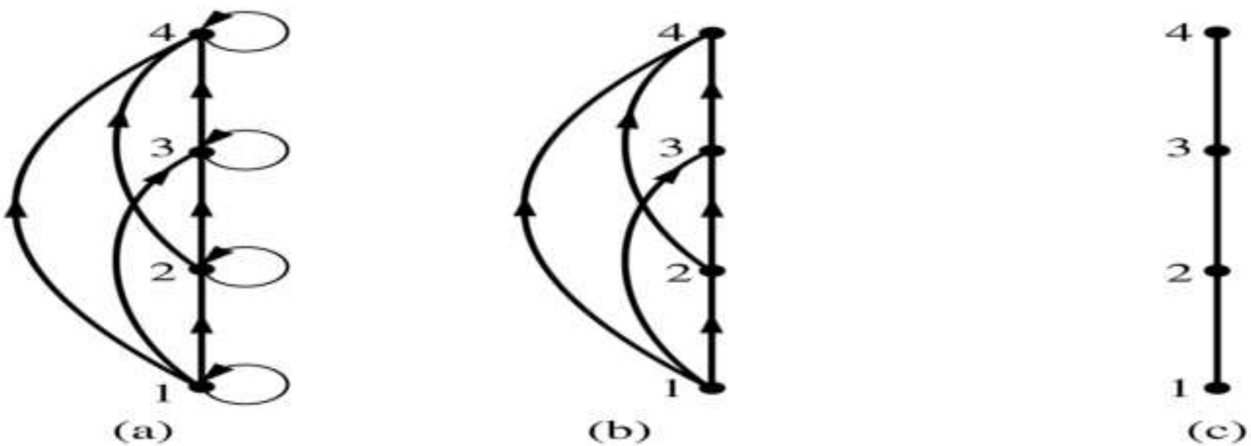
1. Remove all self-loops from all the vertices. This removes all edges showing reflexivity.
2. Remove all edges which are present due to transitivity i.e. if (a, b) and (b, c) are in the partial order, then remove the edge (a, c). Furthermore if (c, d) is in the partial order, then remove the edge (a, d).
3. Arrange all edges such that the initial vertex is below the terminal vertex.
4. Remove all arrows on the directed edges, since all edges point upwards.

Example 1: Construct the Hasse diagram for ({1, 2, 3}, ≤)



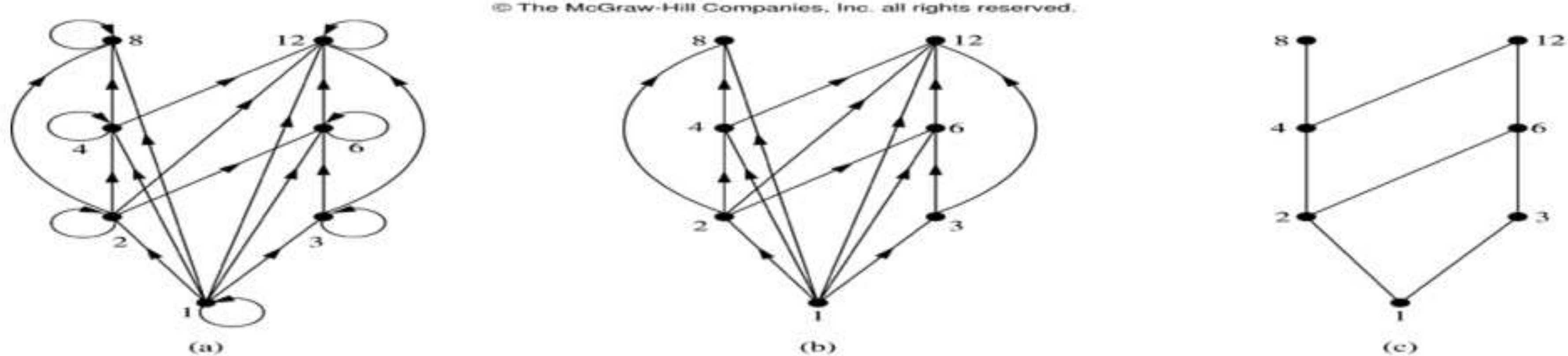
Example 2: Construct the Hasse diagram for ({1, 2, 3,4}, ≤) "less than or equal

Steps in the construction of the Hasse diagram for ({1, 2, 3, 4}, ≤)



Example 3: Construct the Hasse diagram for ({1, 2, 3, 4, 6, 8, 12}, /)

Steps in the construction of the Hasse diagram for ({1, 2, 3, 4, 6, 8, 12}, |)



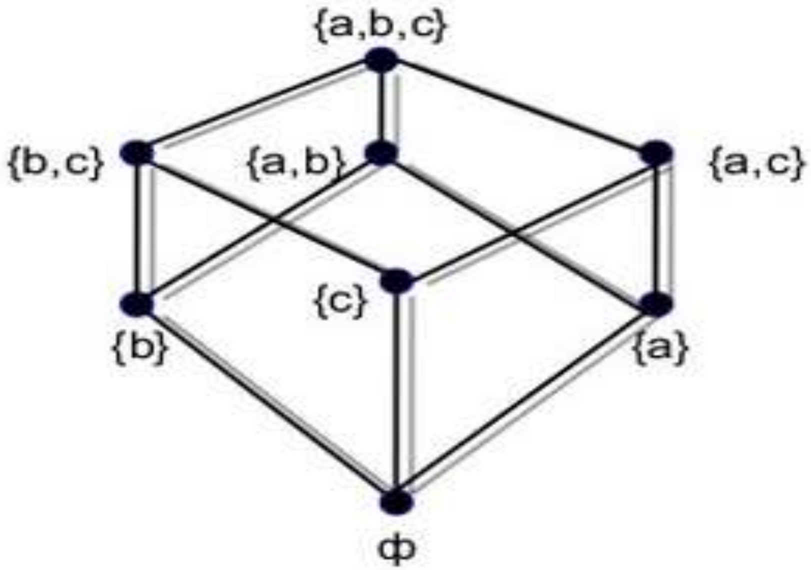
4. Construct the Hasse diagram for A={2, 3, 6, 12, 24, 36} and the relation ≤ be such that x ≤ y if x divides y.

5. Construct the Hasse diagrams for (P(a), ⊆). Let A be a given finite set and P(A) its power set. Let ⊆ be the inclusion relation on the elements of P(A).

(a) A={a}　　　(b) A = {a, b}　　　(c) A = {a, b, c}

Example

Let S={a,b,c} and A=P(S). Draw the Hasse diagram of the poset A with the partial order '⊆'



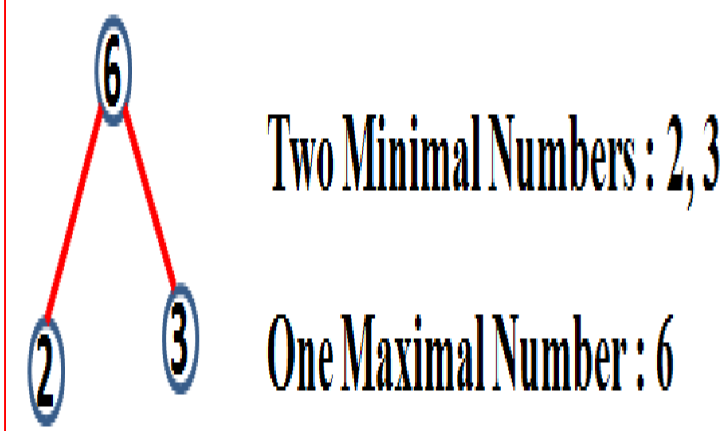
Example 2: Let S_n be the set of all divisors of n.

(a) n= 6 (b). n = 24 ©. n= 8 Draw the Hasse diagrams

Note: For a given POSet, the Hasse diagram is not unique.

Let (P, ≼) be a poset. An element y∈P is called a is minimal number of P relation to a partial ordering ≼ if for no x∈P is x < y. (bottom of the Hasse diagram)

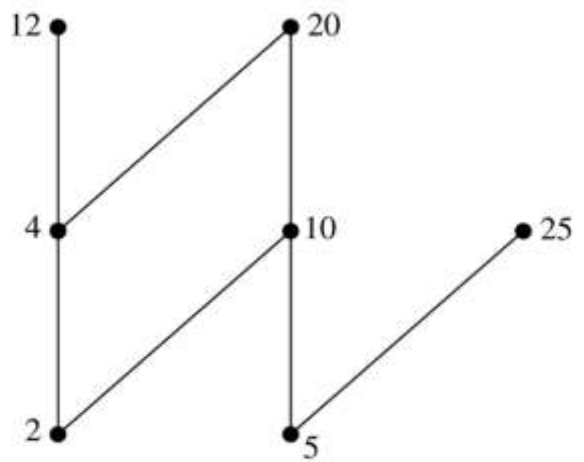
Let (P, ≼) be a poset. An element y∈P is called a is maximal number of P relation to a partial ordering ≼ if for no x∈P is y<x. (top of the Hasse diagram)



Note: (1). A minimal number need not be unique. All those members which appears at the lowest level of Hasse diagram of a POSet are minimal numbers.

(2). Distinct minimal numbers are incomparable and distinct maximal numbers are incomparable.

Which elements of the poset ({, 2, 4, 5, 10, 12, 20, 25}, |) are maximal? Which are minimal?



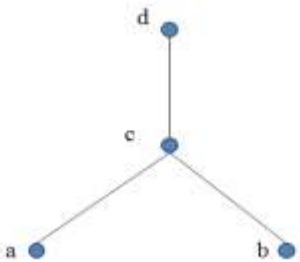
The Hasse diagram for this poset shows that the maximal elements are: 12, 20, 25

The minimal elements are: 2, 5

Let (S, ≼) be a POSet. a is the Greatest Element of (S, ≼) if b≼a for all b∈S. It must be unique.

Let (S, ≼) be a POSet. a is the Least Element of (S, ≼) if a≼b for all b∈S. It must be unique

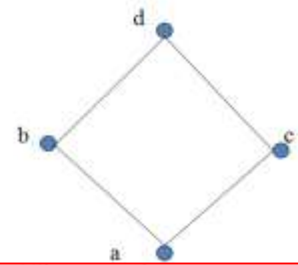
- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?



The poset represented by this Hasse diagram does not have a *least element*, because the least element must be unique.

It does have a *greatest element*, *d*.

- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?



The poset represented by this Hasse diagram has a *greatest element*, *d*.

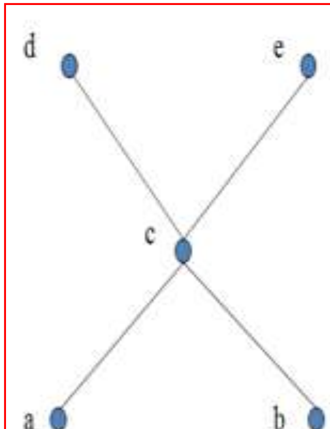
It also has a *least element*, *a*.

- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?

The poset represented by this Hasse diagram does not have a *greatest element*, because the greatest element must be unique.

It does have a *least element*, *a*.

- Does the poset represented by this Hasse diagram have a *greatest element*? If so, what is it? Does it have a *least element*? If so, what is it?

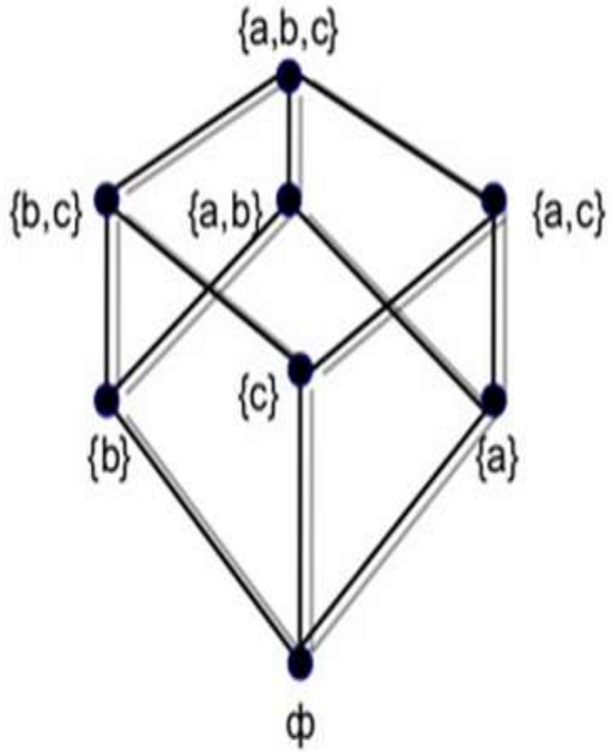


The poset represented by this Hasse diagram has neither a *greatest element* nor a *least element*, because they must be unique.

Let (P, ≼) be a POSet and A be a subset of P. Any element u∈P is upper bound for A. If for all a∈A, such that a≼u. then u is called **Upper Bound** of A.

Let (P, ≼) be a POSet and A be a subset of P. Any element l∈P is lower bound for A. If for all a∈A, such that l≼a. then l is called **Lower Bound** of A.

Example 1: Let us consider (P(A), ⊆) we choose a subset B of P(A) is {{b, c}, {b}, {c}} then A is upper bound of B and Ø is lower bound of B.



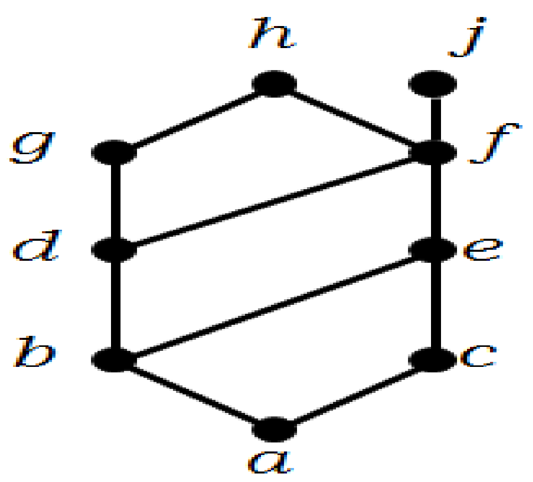
Example 2: Let us consider (P(A), ⊆) we choose a subset B of P(A) is {{a, c}, {c}} then A is upper bound of B and Ø is lower bound of B.

Note: Upper and lower bounds of a subset are not necessarily unique.

Let (P, ≼) be a POSet and A⊆P. Any element u∈P is a **Least Upper Bound(LUB) or Supremum** for A. If u is an upper bound for A and u≼y. y is any upper bound for *A*. **It must be unique.**

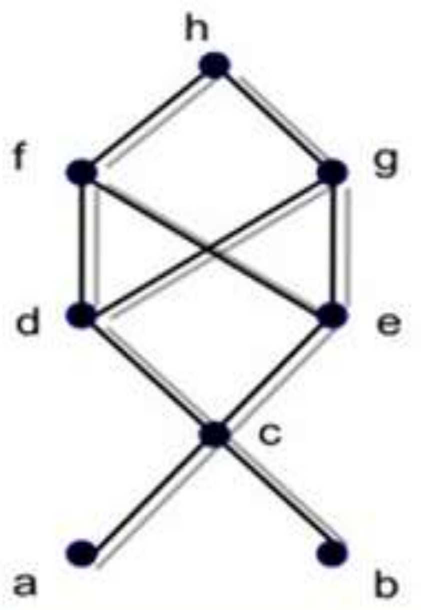
Let (P, ≼) be a POSet and A⊆P. Any element l∈P is a **Greatest Lower Bound(GLB) or Minimum** for A. If l is an lower bound for A and y≼l. y is any Lower bound for *A*. **It must be unique.**

Example: From the below Hasse diagram, Find the Maximal, Minimal, Greatest element, Least element, UB, LUB, LB and GLB of {a,b,c}.



Maximal	: h, j
Minimal	: a
Greatest element	: None
Least element	: a
Upper bound of {a,b,c}	: e, f, j, h
Least upper bound of {a,b,c}	: e
Lower bound of {a,b,c}	: a
Greatest lower bound of {a,b,c}	: a

Example: From the below Hasse diagram, Find the UB, LUB, LB and GLB of B1= {a,b}, B2 = {c, d, e}.



(a) Since B1 has no lower bounds, it has no greatest lower bounds; However,

LUB(B1)=c

(b)Since the lower bounds of B2 are c, a and b, we find that GLB(B2)=c

The upper bounds of B2 are f, g and h. Since f and g are not comparable, we conclude that B2 has no least upper bound.

- Unit element

  The greatest element of a poset, if it exists, is denoted by I and is often called the unit element.

- Zero element

  The least element of a poset, if it exists, is denoted by 0 and is often called the zero element.

3.1.7. Lattice:

A lattice is a POSet (L, ≼) in which every pair of elements a, b∈L has a LUB and GLB.

The GLB of a sub set {a, b}⊆L will be denoted by a*b and LUB denoted by a⊕b.

That is , GLB{a,b} = a*b (product of a, b) or a∧b (meet of a and b)

LUB{a,b}=a⊕b (Sum of a, b) or a∨b (Join of a and b)

From the definitions of lattice that both * and ⊕ are binary operations on L because of the uniqueness of the LUB and GLB of any subsets of POSet.

it is obvious that, a totally ordered set is trivially a lattice, but not all partially ordered sets are lattices can be concluded from Hasse diagrams of POSets.

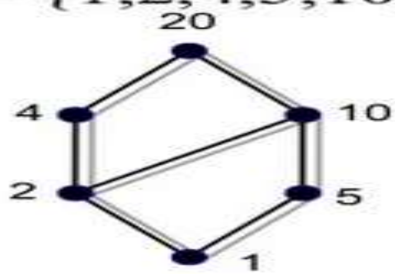
Example 1: **Let I^+ be the set of all positive integers and D denote the relation of " Division", in I^+ such that for any a,b ∈ I^+ aDb ⇔ a divides b then (I^+, D) is a lattice in which a ⊕ b = LCM of a and b, a*b = GCD of a and b.**

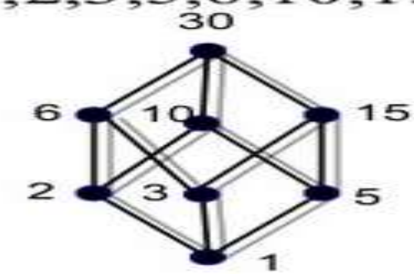
Lattices

- Example

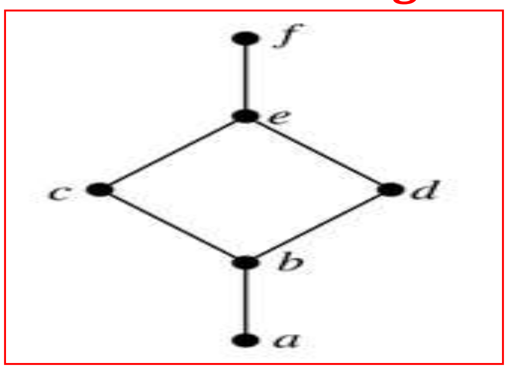
  Let n be a positive integer and D_n be the set of all positive divisors of n. Then D_n is a lattice under the relation of divisibility. For instance,

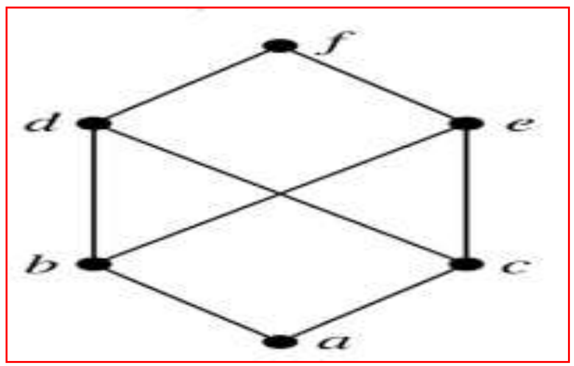
  $D_{20} = \{1,2,4,5,10,20\}$ $D_{30} = \{1,2,3,5,6,10,15,20\}$

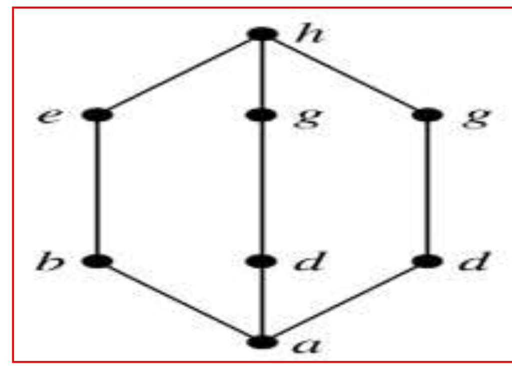




Are the following three POSets lattices?







Yes

No; elements b and c have no least upper bound.

Yes

Properties of Lattices

1. Idempotent Properties

a*a=a

a ⊕ a=a

2. Absorption Properties

a* (a ⊕ b)=a

a ⊕(a*b)=a

3. Commutative Properties

a*b = b*a

a ⊕ b = b ⊕ a

4. Associative Properties

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

a ⊕(b ⊕ c)=(a ⊕ b) ⊕ c

Properties of Lattices

Idempotent Properties

- $a \vee a = a$
- $a \wedge a = a$

Absorption Properties

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

Commutative Properties

- $a \vee b = b \vee a$
- $a \wedge b = b \wedge a$

Associative Properties

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

Dual of a Lattice

The dual of a lattice is obtained by interchanging the '$*$' and '$\oplus$' operations.

Example The dual of $[a * (b \oplus c)]$ is $[a \oplus (b * c)]$

Dual of a Lattice

Let R be a partial order on a set A, and let R^{-1} be the inverse relation of R. Then R^{-1} is also a partial order.

The poset (A, R^{-1}) is galled the **dual** of the poset (A, R).

whenever $(A, \leq)$ is a poset, we use "$\geq$" for the partial order $\leq^{-1}$

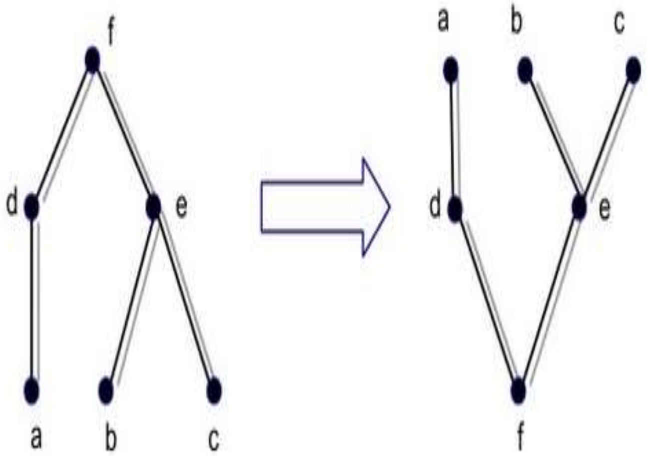
- **Dual of a lattice**: Let $(L, \leq)$ be a lattice, then the $(L, \geq)$ is called dual lattice of $(L, \leq)$.
- **Note**: Dual of dual lattice is original lattice.
- **Note**: In $(L, \leq)$, if $a \vee b = c$; $a \wedge b = d$, then in dual lattice $(L, \geq)$, $a \vee b = d$; $a \wedge b = c$
- **Principle of duality:** If P is a valid statement in a lattice, then the statement obtained by interchanging meet and join everywhere and replacing $\leq$ by $\geq$ is also a valid statement.

- Example

Fig. a shows the Hasse diagram of a poset $(A, \leq)$, where

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

Fig. b shows the Hasse diagram of the dual poset $(A, \geq)$



Bounded Lattices

- Bounded

  A lattice L is said to be bounded if it has a greatest element 1 and a least element 0

For instance:

Example: The lattice P(S) of all subsets of a set S, with the relation containment is bounded. The greatest element is S and the least element is empty set.

Example : The lattice Z^+ under the partial order of divisibility is not bounded, since it has a least element 1, but no greatest element.

- If L is a bounded lattice, then for all a in A

$$0 \leq a \leq 1$$

$$a \vee 0 = a, \qquad a \vee 1 = 1$$

$$a \wedge 0 = 0, \qquad a \wedge 1 = a$$

Note: 1(0) and a are comparable, for all a in A.

Distributive Lattices

- Distributive

  A lattice (L, ≤) is called distributive if for any elements a, b and c in L we have the following distributive properties:

  1. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
  2. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

  If L is not distributive, we say that L is nondistributive.

Note: the distributive property holds when

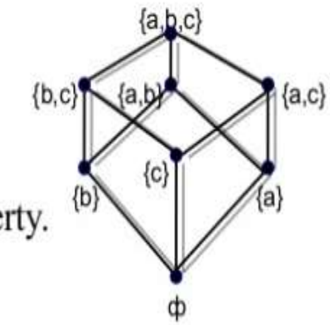
a. any two of the elements a, b and c are equal or

b. when any one of the elements is 0 or I.

Distributive Lattices

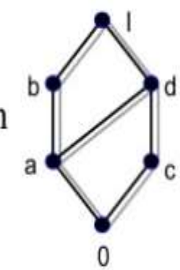
- Example

  For a set S, the lattice P(S) is distributive, since join and meet each satisfy the distributive property.



- Example

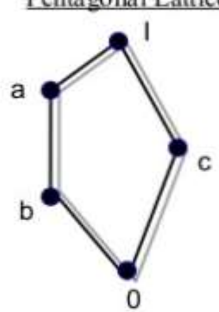
  The lattice whose Hasse diagram shown in adjacent diagram is distributive.

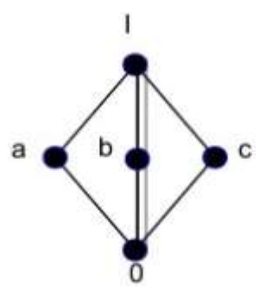


- Example

  Show that the lattices as follows are non-distributive.

Pentagonal Lattice





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

$(a \wedge b) \vee (a \wedge c) = b \vee 0 = b$

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

$(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0$

Modular Lattices

A lattice $(L, \leq)$ is called **Modular** if for any elements a, b and c in L if $b \leq a$ then

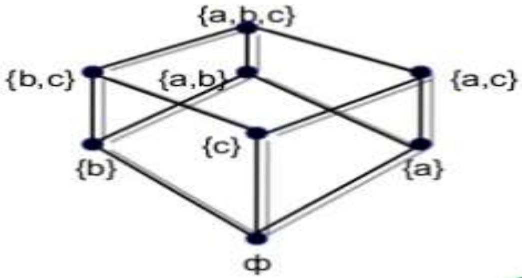
$$b \vee (a \wedge c) = a \wedge (b \vee c)$$

- Example

For a set S, the lattice

P(S) is modular, (if $B \subseteq A$)

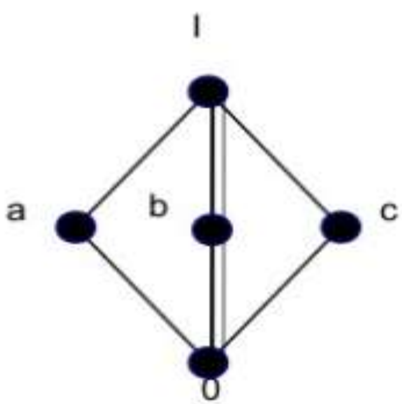
$B \cup (A \cap C) = A \cap (B \cup C)$



- Example

Every chain is a modular lattice

- Example: Given Hasse diagram of a lattice which is modular



$0 \leq a$ i.e. taking b=0;

$b \vee (a \wedge c) = 0 \vee 0 = 0$

$a \wedge (b \vee c) = a \wedge c = 0$

Complemented Lattice

- Complement of an element:

  Let L be bounded lattice with greatest element 1 and least element 0, and let a in L. An element b in L is called a complement of a if

  $$a \vee b = 1 \text{ and } a \wedge b = 0$$

  Note: $0' = 1$ and $1' = 0$

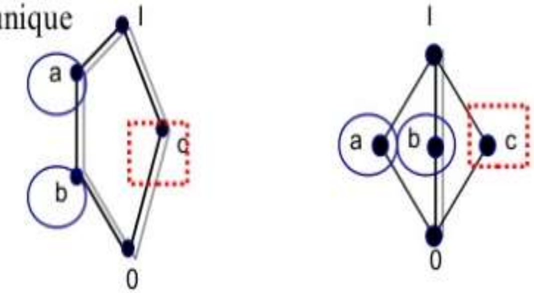
- Complemented Lattice:

  A lattice L is said to be complemented if it is bounded and every element in it has a complement.

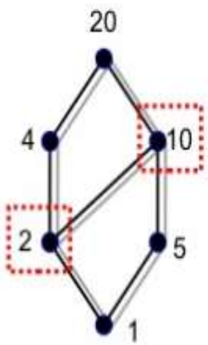
- Example

  The lattice L=P(S) is such that every element has a complement, since if A in L, then its set complement $\bar{A}$ has the properties $A \vee \bar{A} = S$ and $A \wedge \bar{A} = \phi$. That is, the set complement is also the complement in L.

- Example : complemented lattices where complement of element is not unique



- Example: D_{20} is not complemented lattice



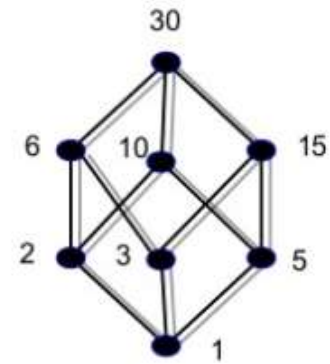
D_{20}

Element	Its Complement
1	20
2	10
4	5
5	4
10	2
20	1

$2 \wedge 10 \neq 0 \ (2 \wedge 10 = 2)$

- D_{30} is complemented lattice

Element	Its Complement
1	30
2	15
3	10
5	6
6	5
10	3
15	2
30	1



D_{30}

3.2.1. Algebraic systems

A Set together with one or more n-ary operations is called an Algebraic System or simply an Algebra.

An n-ary operation on a set X which is a mapping from X^n -> X.

If n=1 such operation is called Unary Operation.

If n=2, it is called Binary Operation.

Since the operations and relations on the set S define a structure on the elements of S, an algebraic system is called Algebraic Structure.

N = {1,2,3,4,…..∝} = Set of all natural numbers.

Z = { 0, ± 1, ± 2, ± 3, ± 4 , ….. ∝} = Set of all integers.

Q = Set of all rational numbers.

R = Set of all real numbers.

■**Binary Operation:** Let A be a non empty set. The * is said to be a binary operation (closed operation) on a non empty set A, if $a*b \in A\ \forall a,b \in A$ (Closure property).

Ex: The set N is closed with respect to addition and multiplication but not w.r.t subtraction and division.

■**Algebraic System:** A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.

Ex: (N, +), (Z, +, –), (R, +, . , –) are algebraic systems.

3.2.2. General Properties

■ **Closure:** Let * be a binary operation on a set A. The operation * is said to be Closure in A, if $a*b \in A\ \forall a, b \in A$

■ **Associative:** Let * be a binary operation on a set A. The operation * is said to be associative in A if $(a*b)*c = a*(b*c),\ \forall a, b, c \in A$

■ **Identity:** Let a be an element in A. An element e is said to be identity of A if $a*e = e*a = a,\ \forall a \in A$.

Note: For an algebraic system (A, *), the identity element, if exists, is unique.

- **Inverse:** Let (A, *) be an algebraic system with identity 'e'. Let a be an element in A. An element b is said to be inverse of A if $a*b= b*a=e, \forall a,b \in A$.
- **Commutative:** Let * be a binary operation on a set A. The operation * is said to be commutative in A, if $a*b=b*a, \forall a,b \in A$
- **Idempotent:** Let (A, *) be an algebraic system. Let a be an element in A.

$$a*a=a, \forall a \in A.$$

- **Distributive:** Let (A, *) be an algebraic system. Let a,b,c are element in A.

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

$$a+(b*c)= (a+b)*(a+c), \forall a,b,c \in A.$$

- **Cancellation:** Let (A, *) be an algebraic system. Let a,b,c are element in A and $a \neq 0$.

$$a * b = a*c$$

$$\Leftrightarrow b= c \ \forall a,b,c \in A.$$

■Let (S,*) and (H,o) be two algebraic systems then a mapping f: S→H from (S,*) to (H,o) satisfying the property that

$$f(a*b) = f(a) \text{ o } f(b) \text{ for any } a,b \in S$$

is called **Homomorphism** or simply **Morphism**.

■Let f be a homomorphism from (S,*) to (H,o).

If mapping f: S→H from (S,*) to (H,o) is onto then f is called **Epimorphism**.

If f: S→H is one-to-one then f is called **Monomorphism**.

If f: S→H is both one-to-one and onto then f is called **Isomorphism.**

If f: S→H is an isomorphic mapping then (S,*) to (H,o) are called as **Isomorphic.**

■Let (S, *) and (H, o) be two algebraic systems such that H⊆S then a homomorphism f from (S,*) and (H, o) is called **Endomorphism.**

An isomorphism from (S,*) to (H,o) is called an **Automorphism** if H = S.

■Let (S, *) be an algebraic system and A⊆S, if A is closed under the operation * then (A,*) is called **sub Algebra** of (S,*)

3.2.3. Semi Group

An algebraic system (A, *) is said to be a semi group if

1. * is closed on A. that is, $a * b \in A \ \forall a, b \in A$

2. * is an associative, $\forall$a, b, c in A. that is, $(a * b) * c = a *(b * c)$

Ex. (N, +), (N, .) are Semi Groups and (N, –) is not a Semi Group.

Sub semigroup

Let (S, *) be a Semi Group and let T be a subset of S. If T is closed under operation * , then (T, *) is called a sub Semi Group of (S, *).

Ex: (N, .) is Semi Group and T is set of multiples of positive integer m then (T,.) is a sub Semi Group.

Abelian Semi Group: **Let (S, *) be any set of algebraic system where S is non empty set and * be a binary relation on S. if the * is commutative in S then (S,*) is called Abelian or Commutative Semi Group for any a,b$\in$S, a*b =b*a.**

Monoid

An algebraic system (A, *) is said to be a Monoid if the following properties are satisfied.

1) *** is a closed in A. That is, $a * b \in A\ \forall a, b \in A$.**
2) *** is an associative $\forall$a, b, c in A. that is, $(a * b) * c = a*(b*c)$.**
3) **There is an identity in A. if $a * e = e * a = a, \forall a \in A$.**

Sub Monoid

Let (S, *) be a Monoid with identity e, and let T be a non- empty subset of S. If T is closed under the operation * and $e \in T$, then (T, *) is called a Sub Monoid of (S, *).

Abelian Monoid

Let (S,*) is a Semi Group satisfying the identity property with respect to * and also if it is commutative, then it is known as Abelian or Commutative Monoid.

Example 1: Show that the set 'N' is a monoid with respect to multiplication.

Solution: Given that N = {1,2,3,4,……} and the binary operation .

1. **Closure property** : We know that product of two natural numbers is again a natural number. i.e., $a.b \in N \ \forall \ a,b \in N$.

$\therefore$ Multiplication is a closed operation.

2. **Associativity** : Multiplication of natural numbers is associative.

i.e., $(a.b).c = a.(b.c) \ \forall a,b,c \in N$

3. **Identity** : We have, $1 \in N$ such that

$a.1 = 1.a = a, \ \forall \ a \in N.$

$\therefore$ Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

Example 2: Show that the set ‘N’ is not a monoid with respect to addition.

Solution: Given that $N = \{1,2,3,4,\ldots\ldots\}$ and the binary operation +.

1. **Closure property :** We know that addition of two natural numbers is again a natural number. i.e., $a+b \in N \ \forall \ a,b \in N$.

   $\therefore$ Addition is a closed operation.

2. **Associativity :** Addition of natural numbers is associative.

   i.e., $(a+b)+c = a+(b+c) \ \forall a,b,c \in N$

3. **Identity :** We have, $0 \notin N$ such that

   $a+0 = 0+a = a, \ \forall \ a \in N$.

   $\therefore$ Identity element does not exists.

Hence, N is a not a monoid with respect to addition.

$$\mathbb{N} = \{1, 2, 3, 4, 5, 6 \ldots\}$$

Example 3: Let (Z, *) be an algebraic structure, where Z is the set of integers and the operation * is defined by n * m = maximum of (n, m). S.T. (Z, *) is a semi group. Is (Z, *) a monoid ?. Justify your answer.

Solution: Given that (Z, *) be an algebraic structure, where Z is the set of integers and the operation * is defined by n * m = maximum of (n, m). Let a , b and c are any three integers.

1. Closure: Now, a * b=maximum of (a, b)$\in$Z, $\forall$a,b$\in$Z

2. Associativity: (a * b) * c = maximum of {a,b,c} = a * (b * c)

$\therefore$ (Z, *) is a semi group.

3. Identity: There is no integer x such that

a * x = maximum of (a, x) = a, $\forall$a$\in$Z

$\therefore$Identity element does not exist. Hence, (Z, *) is not a monoid.

$\therefore$The given algebraic structure does not have an identity element since it is defined on the set of Integers and there is no minimum element in the set of integers.

$\therefore$Since it does not have an identity element, it is not a Monoid and consequently not a Group or Abelian Group.

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

Semi group Homomorphism

Let (S,*) and (T, o) be two semi groups. A mapping $f:S \rightarrow T$ satisfying the properties that $f(s_1 * s_2) = f(s_1) \circ f(s_2)$ is called a semigroup homomorphism, where $S_1, S_2 \in S$

1.If f is one to-one then it is called Monomorphism.

2.If f is onto then it is called epimorphism.

3.If f is both one-to-one and onto then it is called Isomorphism.

4.An isomorphism defined from a semigroup to itself is called automorphism.

Monoid Homomorphism

Let (S,*) and (T, o) be two monoids with identity elements e_S and e_T respectively. A mapping $f:S \rightarrow T$ is called monoid homomorphism if it satisfies the following properties,

1. $f(s_1 * s_2) = f(s_1) \circ f(s_2)$ and

2. $f(e_S) = e_T$

3.2.4. Group

An algebraic system (G, *) is said to be a group if the following properties are holds.

1) *** is a Closed: $\forall a, b \in G, a * b \in G$.**
2) *** is an Associative: that is, $\forall a,b,c \in G$. $(a * b) * c = a *(b * c)$.**
3) **Identity: $\forall a \in G$ there exists an element $e \in G$ then, $a*e = e * a = a$.**
4) **Inverse: $\forall a\in G$ there exists an element $a^{-1} \in G$ then, $a* a^{-1} = a^{-1} * a = e$.**

Abelian group (Commutative group): A group (G, *) is said to be abelian (or commutative) if * is commutative in S. that is $a * b = b * a$ $\forall a, b\in G$.

Order of a Group: the order of a group (S,*) is denoted by |S|, is the number of elements of S when S is finite.

Finite group: If the order of a group G is finite, then G is called a finite group.

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z} \right\}$$

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$$

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$$

Both rational numbers and irrational numbers are real numbers.

Example 1: Show that set of all non zero real numbers is a group with respect to multiplication.

Solution: Given that, R^*= set of all non zero real numbers and Multiplication is Binary Operation. Let a, b, c are any three elements $\in R^*$.

1. Closure: We know that, product of two nonzero real numbers is again a nonzero real number . i.e., $a . b \in R^* \ \forall a,b \in R^*$.

2.Associativity: We know that multiplication of real numbers is associative. i.e., $(a.b).c = a.(b.c) \ \forall a,b,c \in R^*$.

3. Identity: We have $1 \in R^*$ and $a.1 = 1.a, \ \forall a \in R^*$.

$\therefore$ Identity element exists, and '1' is the identity element.

4. Inverse: To each $a \in R^*$, we have $1/a \in R^*$ such that $a.(1/a) = 1$

i.e., Each element in R^* has an inverse.

5.Commutativity: We know that multiplication of real numbers is commutative. i.e., $a.b=b.a \ \forall a,b \in R^*$.

Hence, $(R^*, .)$ is an abelian group.

Example 2: Show that the set of all integers is a group with addition.

Solution: Given that Z=set of all integers and Multiplication is Binary Operation. Let a, b, c are any three elements of Z.

1. Closure: We know that, Sum of two integers is again an integer.

i.e., $a+b \in Z, \forall a,b \in Z$

2. Associativity: We know that addition of integers is associative.

i.e., $(a+b)+c = a+(b+c), \forall a,b,c \in Z$.

3. Identity: We have $0 \in Z$ and $a+0=a, \forall a \in Z$.

$\therefore$ Identity element exists, and '0' is the identity element.

4. Inverse: To each $a \in Z$, we have $-a \in Z$ such that $a+(-a)=0$

Each element in Z has an inverse.

5. Commutative: We know that addition of integers is commutative.

i.e., $a+b = b+a, \forall a,b \in Z$.

Hence, (Z, +) is an abelian group.

Example 3: Show that set of all real numbers 'R' is not a group with respect to multiplication

Solution: Given that R=set of all real numbers and Multiplication is Binary Operation. Let a, b, c are any three elements of Z.

1. Closure: We know that, Sum of two integers is again an integer.

i.e., $a.b \in R, \forall a,b \in R$

2. Associativity: We know that addition of integers is associative.

i.e., $(a.b).c = a.(b.c), \forall a,b,c \in R$.

3. Identity: We have $1 \in R$ and $a.1=a, \forall a \in Z$.

$\therefore$ Identity element exists, and '1' is the identity element.

4. Inverse: To each $a \in R$, we have $1/a \in Z$ such that $a.(1/a)=1$

But The multiplicative inverse of 0 does not exist.

Hence. R is not a group

Example 4: Show that the set of all strings 'S' is a monoid under the operation 'concatenation of strings'. Is S a group w.r.t the above operation? Justify your answer.

Solution: Let us denote the operation 'concatenation of strings' by + .

Let s_1, s_2, s_3 are three arbitrary strings in S.

1. Closure property: Concatenation of two strings is again a string.

i.e., $s_1+s_2 \in S$

2. Associativity: Concatenation of strings is associative.

$$(s_1+ s_2) + s_3 = s_1+ (s_2 + s_3)$$

3. Identity: We have null string , $\lambda \in S$ such that $s_1 + \lambda = S$.

$\therefore$ S is a monoid.

Note: S is not a group, because the inverse of a non empty string does not exist under concatenation of strings.

Example 5: Let S be a finite set, let F(S) be the collection of all functions $f:S \rightarrow S$ under the operation of composition of functions, then Show That F(S) is a monoid. Is S a group w.r.t the above operation? Justify your answer.

Solution: Let f_1, f_2, f_3 are three arbitrary functions on S.

1. Closure: Composition of two functions on S is again a function on S.

i.e., $f_1 o\, f_2 \in F(S)$

2. Associativity: Composition of functions is associative.

i.e., $(f_1\, o\, f_2)\, o\, f_3 = f_1\, o\, (f_2\, o\, f_3),\ \forall f_1, f_2, f_3 \in F(S)$

3. Identity: We have identity function $I : S \rightarrow S$ such that $f_1\, o\, I = f_1$.

$\therefore$ F(S) is a monoid.

Note: F(S) is not a group, because the inverse of a non bijective function on S does not exist.

Example 6: Show That the set of all positive rational numbers forms an abelian group under the composition * defined by a * b = (ab)/2 .

Solution: Let given A = set of all positive rational numbers and the composition * defined by $a * b = (ab)/2$.

Let a,b,c are any three elements of A.

1. Closure: We know that, Product of two positive rational numbers is again a rational number. i.e., $a * b \in A \ \forall \ a,b \in A$.

2. Associativity: $(a*b)*c = (ab/2) * c = (abc) / 4$

$a*(b*c) = a * (bc/2) = (abc) / 4$

Therefore $(a*b)*c = a*(b*c) = (abc) / 4$ and associative law holds.

3. Identity: Let e be the identity element. We have $a*e = (ae)/2$ …(1)

By the definition of * again, $a*e = a$ …..(2), Since e is the identity.

From (1)and (2), $(ae)/2 = a \Rightarrow e = 2$ and $2 \in A$.

$\therefore$ Identity element exists, and '2' is the identity element in A.

4. Inverse: Let $a \in A$

let us suppose b is inverse of a.

Now, $a * b = (ab)/2$ ….(1) (By definition of inverse.)

Again, $a * b = e = 2$ …..(2) (By definition of inverse)

From (1) and (2), it follows that

$(ab)/2 = 2$

$\Rightarrow b = (4/a) \in A$

$\therefore$ (A ,*) is a group.

5. Commutativity: $a * b = (ab/2) = (ba/2) = b * a$

Hence, (A,*) is an abelian group.

Example 7: If M is set of all non singular matrices of order 'n x n'. S.T M is a group w.r.t. matrix multiplication. Is (M, *) an abelian group?. Justify your answer.

Solution: Let $A,B,C \in M$.

1.Closure: Product of two non singular matrices is again a non singular matrix, because $|AB| = |A|.|B| \neq 0$ (Since, A and B are nonsingular) i.e., $AB \in M \ \forall A,B \in M$.

2. Associativity: Matrix multiplication is associative.

i.e., $(AB)C = A(BC) \ \forall A,B,C \in M$.

3. Identity: We have $I_n \in M$ and $A.I_n = A, \ \forall A \in M$.

$\therefore$ Identity element exists, and 'I_n' is the identity element.

4. Inverse: To each $A \in M$, we have $A^{-1} \in M$ such that

$A.A^{-1} = I_n$ i.e., Each element in M has an inverse.

$\therefore$ M is a group w.r.t. matrix multiplication.

5. Abelian: We know that, matrix multiplication is not commutative.

Hence, M is not an abelian group.

Example 8: consider (Z,*) where * is a binary operation defined by a*b=a+b-ab. Show that (Z, *) is a monoid. Is (Z, *) a group?. Justify your answer.

Solution: Given that (Z,*) where * is a binary operation defined by a*b=a+b-ab.

1. Closure: $a*b=a+b-ab \in \mathbb{Z}, \forall a, b \in \mathbb{Z}$.

$\therefore$ closure property holds

2. Associativity:

$$
\begin{aligned}
(a*b)*c &= (a+b-ab)*c \\
&= (a+b-ab)+c-(a+b-ab)c \\
&= a+b+c-ab-ac-bc+abc \\
a*(b*c) &= a*(b+c-bc) \\
&= a+(b+c-bc)-a(b+c-bc) \\
&= a+b+c-bc-ab-ac+abc
\end{aligned}
$$

$\therefore$ $(a*b)*c = a*(b*c) = a+b+c-bc-ab-ac+abc \ \forall a, b, c \in \mathbb{Z}$

$\therefore$ Therefore associative law holds.

3. identity: $0 \in \mathbb{Z}$ is the identity element as $a*0 = a+0-a.0 = 0+a-0.a = 0*a = a$

Therefore identity property holds and 0 as the identity element.

Therefore (Z,*) is Monoid.

4. inverse: for $3 \in \mathbb{Z}$, there is no $x \in \mathbb{Z}$ such that

$$3 + x - 3x = 0 \Rightarrow 3 + x = 3x \Rightarrow x = 3/2 \notin Z.$$

Inverse does not exists, so (Z,*) is not a Group.

Example 9: Let R be the set of all real numbers and * is a binary operation defined by a*b=a+b+ab. Show that (R,*) is a monoid. Is (R,*) a group?. Justify your answer.

Solution: Given that (R,*) where * is a binary operation defined by a*b=a+b+ab.

1. Closure: $a*b=a+b+ab \in R, \forall a, b \in R$. $\therefore$ closure property holds

2. Associativity:

$$(a*b)*c = (a+b+ab)*c$$
$$= (a+b+ab)+c+(a+b+ab)c$$
$$= a+b+c+ab+ac+bc+abc$$
$$a*(b*c) = a*(b+c+bc)$$
$$= a+(b+c+bc)+a(b+c+bc)$$
$$= a+b+c+bc+ab+ac+abc$$

$\therefore$ $(a*b)*c = a*(b*c) = a+b+c+bc+ab+ac+abc \ \forall a, b, c \in R$

$\therefore$ Therefore associative law holds.

3. identity: $0 \in R$ is the identity element as $a*0 = a+0+a.0 = 0+a+0.a = 0*a = a$

Therefore identity property holds and 0 as the identity element.

Therefore (R,*) is Monoid.

4. inverse: for $a \in R$, there is $x \in R$ such that

$$a + x + 3a = 0 \Rightarrow a + x = -ax \Rightarrow x = -a/a+1 \in R.$$

Inverse exists, so (R,*) is a Group.

Theorem

In a Group (G, *) the following properties hold good

1. Identity element is unique.

2. Inverse of an element is unique.

3. Cancellation laws hold good

$a * b = a * c \Rightarrow b = c$ **(left cancellation law)**

$a * c = b * c \Rightarrow a = b$ **(Right cancellation law)**

4. $(a * b)^{-1} = b^{-1} * a^{-1}$

In a group, the identity element is its own inverse.

Theorem 1: In a group (G, *) , Prove that the identity element is unique.

Proof : Let e_1 and e_2 are two identity elements in G.

Now, $e_1 * e_2 = e_1$ …(1) (since e_2 is the identity)

Again, $e_1 * e_2 = e_2$ …(2) (since e_1 is the identity)

From (1) and (2), we have $e_1 = e_2$

$\therefore$ Identity element in a group is unique.

Theorem 2: In a group (G,*), Prove that the inverse of any element is unique.

Proof : Let a ,b, c $\in$ G and e is the identity in G.

Let us suppose, Both b and c are inverse elements of a.

Now, $a * b = e$ …(1) (Since, b is inverse of a)

Again, $a * c = e$ …(2) (Since, c is also inverse of a)

From (1) and (2), we have

$a * b = a * c$

$\Rightarrow$ $b = c$ (By left cancellation law)

In a group, the inverse of any element is unique.

Theorem 3: In a group (G,*), Prove that $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a,b \in G$.

Proof : Consider, $(a * b) * (b^{-1} * a^{-1})$

$= (a * (b * b^{-1}) * a^{-1})$ (By associative property).

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

$= (a * a^{-1})$ (Since, e is identity)

$= e$ (By inverse property)

Similarly, we can show that $(b^{-1} * a^{-1}) * (a * b) = e$

Hence, $(a * b)^{-1} = b^{-1} * a^{-1}$.

If (G,*) is a group and $a \in G$ such that $a*a=a$, Show That $a = e$, where e is identity element in G.

- **Proof**: Given that, $a * a = a$
- $\Rightarrow a * a = a * e$ (Since, e is identity in G)
- $\Rightarrow a = e$ (By left cancellation law)
- Hence, the result follows.

If every element of a group is its own inverse, then show that the group must be abelian .

Proof: Let (G, *) be a group.

Let a and b are any two elements of G.

Consider the identity,

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

$\Rightarrow (a*b)=b*a$ **(Since each element of G is its own inverse)**

Hence, G is abelian.

Note: $a^2 = a * a$

$a^3 = a * a * a$ **etc.**

Example: In a group $(G, *)$, if $(a * b)^2 = a^2 * b^2$ $\forall a,b \in G$. Show that G is abelian group.

Proof: Given that $(a * b)^2 = a^2 * b^2$

$\Rightarrow (a * b) * (a * b) = (a * a) * (b * b)$

$\Rightarrow a * (b * a) * b = a * (a * b) * b$ **(By associative law)**

$\Rightarrow (b * a) * b = (a * b) * b$ **(By left cancellation law)**

$\Rightarrow (b * a) = (a * b)$ **(By right cancellation law)**

Hence, G is abelian group.

Example: Show that G = {1, -1} is an abelian group under multiplication.

Solution: The composition table of G

$\cdot$	1	-1
1	1	-1
-1	-1	1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.

2. Associativity: The elements of G are real numbers, and we know that multiplication of real numbers is associative.

3. Identity : Here, 1 is the identity element and $1 \in G$.

4. Inverse: From the composition table, we see that the inverse elements of 1 and -1 are 1 and -1 respectively.

Hence, G is a group w.r.t multiplication.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.

Hence, G is an abelian group w.r.t. multiplication.

Example: Show that $G = \{1, \omega, \omega^2\}$ is an abelian group under multiplication. Where $1, \omega, \omega^2$ are cube roots of unity.

Solution: The composition table of G is

$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.

2. Associativity: The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.

3. Identity : Here, 1 is the identity element and $1 \in G$.

4. Inverse: From the composition table, we see that the inverse elements of $1\ \omega, \omega^2$ are $1, \omega^2, \omega$ respectively.

Hence, G is a group w.r.t multiplication.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative.

Hence, G is an abelian group w.r.t. multiplication.

Example: Show that G = {1, –1, i, –i } is an abelian group under multiplication.

Solution: The composition table of G is

.	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

1. **Closure property:** Since all the entries of the composition table are the elements of the given set, the set G is closed under multiplication.

2. **Associativity:** The elements of G are complex numbers, and we know that multiplication of complex numbers is associative.

3. **Identity :** Here, 1 is the identity element and $1 \in G$.

4. **Inverse:** From the composition table, we see that the inverse elements of

   1 -1, i, -i are 1, -1, -i, i respectively.

5. **Commutativity:** The corresponding rows and columns of the table are identical. Therefore the binary operation . is commutative. Hence, (G, .) is an abelian group.

Modulo systems

Addition modulo m($+_m$)

let m is a positive integer. For any two positive integers a and b

$a +_m b = a + b$ if $a + b < m$

$a +_m b = r$ if $a+b \geq m$ where r is the remainder obtained by dividing (a+b) with m.

Multiplication modulo p(X_p)

let p is a positive integer. For any two positive integers a and b

$a X_p b = a\,b$ if $a\,b < p$

$a X_p b = r$ if $ab \geq p$ where r is the remainder obtained by dividing (ab) with p.

Ex. $3X_5 4=2$, $5X_5 4=0$, $2X_5 2=4$

Example: The set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

Solution: The composition table of G is

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

2. Associativity: The binary operation $+_6$ is associative in G.

for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and $2 +_6 (3 +_6 4) = 2 +_6 1 = 3$

3. Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 0 is the identity element.

4. Inverse: From the composition table, we see that the inverse elements of 0, 1, 2, 3, 4. 5 are 0, 5, 4, 3, 2, 1 respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $+_6$ is commutative.

Hence, $(G, +_6)$ is an abelian group.

The set G = {1,2,3,4,5,6} is a group with respect to multiplication modulo 7.

Solution: The composition table of G is

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $\times_7$.

2. Associativity: The binary operation $\times_7$ is associative in G.

for ex. $(2 \times_7 3) \times_7 4 = 6 \times_7 4 = 3$ and $2 \times_7 (3 \times_7 4) = 2 \times_7 5 = 3$

3. Identity : Here, The first row of the table coincides with the top row. The element heading that row , i.e., 1 is the identity element.

4. Inverse: From the composition table, we see that the inverse elements of 1, 2, 3, 4. 5 ,6 are 1, 4, 5, 2, 5, 6 respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $\times_7$ is commutative.

Hence, $(G, \times_7)$ is an abelian group.

More on finite groups

In a group with 2 elements, each element is its own inverse

In a group of even order there will be at least one element (other than identity element) which is its own inverse

The set G = {0,1,2,3,4,…..m-1} is a group with respect to addition modulo m.

The set G = {1,2,3,4,….p-1} is a group with respect to multiplication modulo p, where p is a prime number.

Order of an element of a group:

Let (G, *) be a group. Let 'a' be an element of G. The smallest integer n such that $a^n = e$ is called order of 'a'. If no such number exists then the order is infinite.

3.2.5. Sub groups

A non empty sub set H of a group (G, *) is a sub group of G, if (H, *) is group.

Note: For any group {G, *}, {e, * } and (G, *) are trivial sub groups.

Example 1: G = {1, -1, i, -i } is a group w.r.t multiplication.

H_1 = { 1, -1 } is a subgroup of G .

H_2 = { 1 } is a trivial subgroup of G.

Example 2:(Z , +) and (Q , +) are sub groups of the group (R +).

Theorem: A non empty sub set H of a group (G, *) is a sub group of G iff

i) $a * b \in H \quad \forall a, b \in H$

ii) $a^{-1} \in H \quad \forall a \in H$

Proof:

Suppose H is a subgroup of G, then H must be closed with respect to composition * in G, i.e. $a \in H, b \in H \Rightarrow a*b \in H$

Let $a \in H$ and a^{-1} be the inverse of a in G. Then the inverse of a in H is also a^{-1}.

As H itself is a group, each element of H will possess inverse in it,

i.e. $a \in H \Rightarrow a^{-1} \in H$.

Thus the condition is necessary.

Now let us examine the sufficiency of the condition.

(i) Closure Axiom: $a \in H, b \in H \Rightarrow a*b \in H$. Hence the closure axiom is satisfied with respect to the operation *.

(ii) Associative Axiom: Since the elements of H are also the elements of G, the composition is associative in H also.

(iii) Existence of Identity: The identity of the subgroup is the same as the identity of the group because $a \in H$, $a^{-1} \in H \Rightarrow a * a^{-1} \in H \Rightarrow e \in H$. The identity e is an element of H.

(iv) Existence of Inverse: Since $a \in H \Rightarrow a^{-1} \in H$, $\forall a \in H$. Therefore each element of H possesses an inverse.

The H itself is a group for the composition * in G.

Hence H is a subgroup.

Theorem: A necessary and sufficient condition for a non empty subset H of a group (G, *) to be a sub group is that $a \in H$, $b \in H \Rightarrow a * b^{-1} \in H$.

Proof:

Case 1: Let (G, *) be a group and H is a subgroup of G

Let $a, b \in H \Rightarrow b^{-1} \in H$ (since H is is a group)

$\Rightarrow a * b^{-1} \in H$. (By closure property in H)

Case 2: Let H be a non empty set of a group (G, *).

Let $a * b^{-1} \in H \quad \forall a, b \in H$

Now, $a * a^{-1} \in H$ (Taking $b = a$)

$\Rightarrow e \in H$ i.e., identity exists in H.

Now, $e \in H$, $a \in H \Rightarrow e * a^{-1} \in H$

$\Rightarrow a^{-1} \in H$

$\therefore$ Each element of H has inverse in H.

Further, $a \in H$, $b \in H \Rightarrow a \in H$, $b^{-1} \in H$

$\Rightarrow a * (b^{-1})^{-1} \in H$.

$\Rightarrow a * b \in H$.

$\therefore$ H is closed w.r.t $*$.

Finally, Let $a,b,c \in H$

$\Rightarrow a,b,c \in G$ (since $H \subseteq G$)

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

$\therefore$ $*$ is associative in H

Hence, H is a subgroup of G.

Example: Show that the intersection of two sub groups of a group G is again a sub group of G.

Proof:

Let (G, *) be a group.

Let H_1 and H_2 are two sub groups of G.

Let $a , b \in H_1 \cap H_2$.

Now, $a , b \in H_1 \Rightarrow a * b^{-1} \in H_1$ (Since, H_1 is a subgroup of G)

again, $a , b \in H_2 \Rightarrow a * b^{-1} \in H_2$ (Since, H_2 is a subgroup of G)

$\therefore\ a * b^{-1} \in H_1 \cap H_2$.

Hence, $H_1 \cap H_2$ is a subgroup of G .

Example: Show that the union of two sub groups of a group G need not be a sub group of G.

Proof:

Let G be an additive group of integers.

Let $H_1 = \{ 0, \pm 2, \pm 4, \pm 6, \pm 8, \ldots\}$

and $H_2 = \{ 0, \pm 3, \pm 6, \pm 9, \pm 12, \ldots\}$

Here, H_1 **and** H_2 **are groups w.r.t addition.**

Further, H_1 **and** H_2 **are subsets of G.**

$\therefore$ H_1 **and** H_2 **are sub groups of G.**

$H_1 \cup H_2 = \{ 0, \pm 2, \pm 3, \pm 4, \pm 6, \ldots\}$

Here, $H_1 \cup H_2$ **is not closed w.r.t addition.**

For ex. $2, 3 \in G$

But, $2 + 3 = 5$ **and** 5 **does not belongs to** $H_1 \cup H_2$ **.**

Hence, $H_1 \cup H_2$ **is not a sub group of G.**

3.2.6. Homomorphism and Isomorphism

Homomorphism :

Consider the groups $(G, *)$ and $(G^1, \oplus)$. A function $f:G \to G^1$ is called a homomorphism if $f(a*b)=f(a)\oplus f(b)$

Isomorphism:

If a homomorphism $f : G \to G^1$ is a bijection then f is called isomorphism between G and G^1 .Then we write $G \equiv G^1$.

Example: Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f : R \to R^+$ defined by $f(x) = 2^x$ for all $x \in R$ is an isomorphism.

Solution: First, let us show that f is a homomorphism.

Let $a, b \in R$.

Now, $f(a+b) = 2^{a+b} = 2^a \; 2^b = f(a).f(b)$

$\therefore$ f is an homomorphism.

Next, let us prove that f is a Bijection.

For any $a , b \in R$, Let, $f(a) = f(b)$

$$\Rightarrow 2^a = 2^b$$

$$\Rightarrow a = b \quad \therefore f \text{ is one.to-one.}$$

Next, take any $c \in R^+$.

Then $\log_2 c \in R$ and $f(\log_2 c) = 2^{\log 2\, c} = c$.

$\Rightarrow$ Every element in R^+ has a pre image in R. i.e., f is onto.

$\therefore$ f is a bijection.

Hence, f is an isomorphism.

Example: Let R be a group of all real numbers under addition and R^+ be a group of all positive real numbers under multiplication. Show that the mapping $f : R^+ \to R$ defined by $f(x) = \log_{10} x$ for all $x \in R$ is an isomorphism.

Solution: First, let us show that f is a homomorphism.

Let $a, b \in R^+$.

Now, $f(a.b) = \log_{10}(a.b)$

$$= \log_{10} a + \log_{10} b$$

$$= f(a) + f(b)$$

$\therefore$ f is an homomorphism.

Next, let us prove that f is a Bijection

For any $a, b \in R^+$, Let, $f(a) = f(b)$

$$\Rightarrow \log_{10} a = \log_{10} b$$

$$\Rightarrow a = b$$

$\therefore$ f is one.to-one.

Next, take any $c \in R$.

Then $10^c \in R$ and $f(10^c) = \log_{10} 10^c = c$.

$\Rightarrow$ Every element in R has a pre image in R^+.

i.e., f is onto.

$\therefore$ f is a bijection.

Hence, f is an isomorphism.

Theorem: Consider the groups $(G_1, *)$ and $(G_2, \oplus)$ with identity elements e_1 and e_2 respectively. If $f : G_1 \to G_2$ is a group homomorphism, then prove that

a) $f(e_1) = e_2$

b) $f(a^{-1}) = [f(a)]^{-1}$

c) If H_1 is a sub group of G_1 and $H_2 = f(H_1)$, then H_2 is a sub group of G_2.

d) If f is an isomorphism from G_1 onto G_2, then f^{-1} is an isomorphism from G_2 onto G_1.

a) $f(e_1) = e_2$

Proof: we have in G_2, $e_2 \oplus f(e_1) = f(e_1)$ (since, e_2 is identity in G_2)

$= f(e_1 * e_1)$ (since, e_1 is identity in G_1)

$= f(e_1) \oplus f(e_1)$ (since f is a homomorphism)

$e_2 = f(e_1)$ (By right cancellation law)

b) $f(a^{-1}) = [f(a)]^{-1}$

Proof: For any $a \in G_1$, we have

$$f(a) \oplus f(a^{-1}) = f(a * a^{-1}) = f(e_1) = e_2$$

and $f(a^{-1}) \oplus f(a) = f(a^{-1} * a) = f(e_1) = e_2$

$\therefore$ $f(a^{-1})$ is the inverse of $f(a)$ in G_2

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

c) If H_1 is a sub group of G_1 and $H_2 = f(H_1)$, then H_2 is a sub group of G_2.

Proof: $H_2 = f(H_1)$ is the image of H_1 under f; this is a subset of G_2.

Let $x, y \in H_2$. Then $x = f(a)$, $y = f(b)$ for some $a,b \in H_1$

Since, H_1 is a subgroup of G_1, we have $a * b^{-1} \in H_1$.

Consequently, $x \oplus y^{-1} = f(a) \oplus [f(b)]^{-1}$

$$= f(a) \oplus f(b^{-1})$$

$$= f(a * b^{-1}) \in f(H_1) = H_2$$

Hence, H_2 is a subgroup of G_2.

d) If f is an isomorphism from G_1 onto G_2, then f^{-1} is an isomorphism from G_2 onto G_1.

Proof: Since $f : G_1 \rightarrow G_2$ is an isomorphism, f is a bijection.

$\therefore$ $f^{-1} : G_2 \rightarrow G_1$ exists and is a bijection.

Let $x, y \in G_2$. Then $x \oplus y \in G_2$ and there exists $a, b \in G_1$ such that $x = f(a)$ and $y = f(b)$.

$$\therefore f^{-1}(x \oplus y) = f^{-1}(f(a) \oplus f(b))$$
$$= f^{-1}(f(a * b))$$
$$= a * b$$
$$= f^{-1}(x) * f^{-1}(y)$$

This shows that $f^{-1} : G_2 \rightarrow G_1$ is an homomorphism as well.

$\therefore$ f^{-1} is an isomorphism.

Example: Prove that every sub group of an abelian group is abelian.

Solution: Let $(G, *)$ be a group and H is a sub group of G.

Let $a, b \in H \Rightarrow a, b \in G$ (Since H is a subgroup of G)

$\Rightarrow a * b = b * a$ (Since G is an abelian group)

Hence, H is also abelian.

UNIT - I

Q. What is Discrete Mathematics?

Ans: Discrete mathematics is the part of mathematics devoted to the study of discrete objects.

Discrete means "distinct or unconnected elements".

Discrete object is something that is countable.

Examples: ① The Integers or natural numbers.

② The rational numbers ③ Finite sets

④ Functions from $\{1, 2, ---, n\} \rightarrow \{0, 1\}$

⑤ People, chairs, tables, balls, ...

Q. Why study Discrete Mathematics?

→ ① It develops your mathematical thinking.

② Improves your problem solving ability.

③ Foundation for many courses in Computer Science/Eng.

- Data structures, algorithms (Graph, Computability).
- Artificial Intelligence (logic, graph, Automata)
- Databases (Relations, logic)
- Computer N/W's (Graphs).
- Compiler design, formal languages, automata theory, Computer security, and operating systems.

④ Foundation for a new discipline: Formal method for CS/Eng.

- proving correctness of programs.
- proving properties of S/W systems: Deadlock-free.
- Verifying protocols: ISDN protocol, security protocol.
- Finding bugs in μp's. (used by Intel, IBM, Motorola)
- Verifying configurations of N/W systems - Firewalls.

The phrase propositional logic is composed of two words:

→ The area of logic that deals with propositions.

→ also called propositional calculus.

proposition   Logic

Q. What is logic?

→ • Logic is the study of correct reasoning.
It helps us to understand and reason about different mathematical " stmts.
statements. The Rules of logic gives precise meaning to mathematical statements.

• With rules of logic, we would be able to think about mathematical statements and finally we would be able to prove or disprove those mathematical statements precisely.

Use of logic: ① In Mathematics
↳ to prove theorems.

② In CS: to prove that programs do what they are supposed to do.

Logic focuses on the relationship among statements.

For example: ① My watch is digital
All digital devices run on batteries.

Therefore, My watch runs on batteries.

Note that Logic is not concerned with the truth of the first two statements. But if they were true, then the inference is true.

② For every positive integer n, the sum of positive integers not exceeding n is $\frac{n(n+1)}{2}$.

purpose of logic is to construct valid arguments (or proofs). Once we prove a mathematical statement is TRUE then we call it as a Theorem. and this is the basis of whole mathematics.

purpose of logic is to distinguish b/w valid and Invalid mathematical arguments.

Course
Major goal of this Subject: how to understand & how to construct correct mathematical arguments.

Scanned by CamScanner

Q. What is proposition? $\to$ Statement

→ A proposition is a declarative sentence that is either true or false, but not both. The basic building blocks of logic.

For example, "My name is Ramu" is a declarative statement. but "What is your name?" is not a declarative statement.

Examples :- ① Delhi is the Capital of India.

② $1+1=2$

③ 5 is a prime number.

④ $2+2=3$

propositions 1, 2, 3 are true, where as 4 is false.

Sentences which are not propositions:

(1) $x+y=z$

(2) How beautiful are you?

③ Read this Carefully.

④ What a beautiful Morning!

⑤ Do your homework.

⑥ $x+2=3$

⑦ what time is it?

propositional (statement) Variable :-

A Variable that represents a proposition. Denoted by p, q, r, s.

The truth or falsity of a proposition is called its truth_value.

These two values 'true' and 'false' are denoted by the symbols T and F respectively. Sometimes these are also denoted by the symbols 1 and 0 respectively.

Truth value : True or False.

Compound proposition : (~~Conted~~ Connectives)

A Compound proposition are formed by combining more than one propositions Using logical operators. (or)

A proposition constructed by combining propositions Using logical operators.

logical operators.
↳ operators used to combine propositions.

Compound proposition is also named as Connectives.

Example : ① Rama is a boy and Sita is a girl.

Rama is a boy ↑ proposition 1

and ↓ Joining two propositions with logical Connective

Sita is a girl ↑ proposition 2

Q. Why do we need Compound propositions?

Example ③: p : Einstein is a genius.
Q : It is not the case that Einstein is a genius.
Modifying the statement using negation.

There are Five basic connectives namely negation, Conjunction, disjunction, Conditional and biconditional, exclusive-or.

① Negation :- Let p be a proposition. The negation of p, denoted by ¬p, is the statement "It is not the case that p". The proposition ¬p is read as "not p". [also named as ~]

Example ①: p : Einstein is a genius.
¬p : It is not the case that Einstein is a genius.
(or)
It is false that Einstein is a genius.
(or)
Einstein is not a genius.

Example 2: Q. Find the negation the propotition "Hyderabad is a city" and express this in Simple English.
A: The negation is "It is not the case that Hyderabad is a city.
(or)
Hyderabad is not a city.

Truth table:

p	¬p
T	F
F	T

Truth table: a table displaying the truth values of propositions.

Types of Connectives (or) compound propositions :-
1) Negation (not)
2) Conjunction (and)
3) Disjunction (or)
   ⓐ Exclusive-or (⊕)
④ Conditional (if . . then)
⑤ Biconditional (if and only if)

② Conjunction :-

Let p and q be propositions. The conjunction of p and q, denoted by $p \wedge q$, is the proposition of p and q.

The conjunction $p \wedge q$ is true when both p and q are true and is false otherwise.

Truth Table:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Note: The word "but" sometimes is used instead of "and" in conjunction.

Example: ① The sun is shining, but it is raining. is another way of saying "The sun is shining and it is raining".

② p: Jack went up the hill

q: Jill went up the hill.

$p \wedge q$: Jack and Jill went up the hill.

③ Disjunction :- Let p and q be propositions. The Disjunction of p and q, denoted by $p \vee q$, is the proposition "p or q".

The disjunction $p \vee q$ is false when both p and q are false and is true otherwise. Disjunction is also known as inclusive-or.

Truth Table :-

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

A disjunction is true when atleast one of the two propositions is true.

Types: Inclusive-or and Exclusive-or

Examples: ① I shall goto Market or Cinema.

② There is something wrong with the bulb or wiring.

③ It is raining or it is cold.

Scanned by CamScanner

(6) Exclusive-or :-

Let p and q be propositions. The exclusive-or of p and q, denoted by $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise.

Truth Table :-

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

(7) Conditional or If.. then Statement :- (Implication)

Let p and q be propositions. The conditional statement $p \rightarrow q$ is the proposition "if p, then q".

The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise.

In the conditional statement $p \rightarrow q$, p is called the hypothesis (or antecedent or premise) and q is called conclusion (or consequence).

The Truth table for the conditional statement $p \rightarrow q$:-

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

The statement $p \rightarrow q$ is called a conditional statement because $p \rightarrow q$ asserts that q is true on the condition that p holds. The conditional statement is also called an implication.

The proposition $p \to q$ may be expressed as:

(1) "if p, then q"
(2) "if p, q"
(3) "p is sufficient for q"
(4) "q if p"
(5) "q when p"
(6) "a necessary condition for p is q"
(7) "q unless $\neg p$"
(8) "p implies q"
(9) "p only if q"
(10) "a sufficient condition for q is p"
(11) "q whenever p"
(12) "q is necessary for p"
(13) "q follows from p"

Example: ① If triangle ABC is equivalent, then it is isoscales.

② p: it is hot
q: $2+3=5$
$p \to q$: If it is hot, then $2+3=5$.

③ If you get 100% on the final exam, then you will get an A grade.

④ If it is sunny tomorrow, you may go swimming.

Q. Write the following statements in symbolic form:

ⓐ If either Jerry takes Calculus or Ken takes sociology, then Larry will take English.

ⓑ The crop will be destroyed if there is a flood.

Ans: ⓐ We denote the statement as
J: Jerry takes Calculus
K: Ken takes sociology
L: Larry takes English

These stmts can be symbolized as $(J \vee K) \to L$

ⓑ C: The crop will be destroyed
F: There is a Flood.
The statement can be symbolized as: $F \to C$

There are three related conditional statements.

<u>Implication</u> $p \rightarrow q$ if p, then q p is sufficient for q q is necessary for p	<u>Converse</u> $q \rightarrow p$ If q, then p q is sufficient for p p is necessary for q.
Inverse/opposite $(\neg p) \rightarrow (\neg q)$ if not p, then not q (equivalent to the Converse)	Contrapositive $(\neg q) \rightarrow (\neg p)$ If not q, then not p (equivalent to the implication)

<u>Equivalent Statement</u> :- When two compound statements always have the same truth value is called <u>equivalent</u> statement.

ⓐ Implication and its contrapositive are equivalent.

ⓑ Converse and the inverse are also equivalent.

ⓒ Neither converse nor inverse is not equivalent to Implication.

<u>Q ①</u>: State (What are) the contrapositive, converse and inverse of the conditional statement.

" ~~If the home team wins, then it is raining~~"

" If <u>it is raining</u>, then <u>the home team wins</u>".

① <u>Contrapositive</u> : $\neg p$ $\neg q$ $(\neg q) \rightarrow (\neg p)$

"If the home team does not win, then it is not raining".

② <u>Converse</u> : $q \rightarrow p$

"If the home team wins, then it is raining".

③ <u>Inverse</u> :- $\neg p \rightarrow (\neg q)$

" If it is not raining, then the home team does not win".

Q2. If triangle ABC is a right angle, then $|AB|^2 + |BC|^2 = |AC|^2$.

Scanned by CamScanner

(5) Biconditional statement :-

Let p and q be propositions. The biconditional statement $p \leftrightarrow q$ (or) $p \rightleftarrows q$, read as "p if and only if q" or "p iff q". The statement $p \leftrightarrow q$ is true whenever both p and q have the same truth values and is false otherwise. It is also called bi-implication.

$p \leftrightarrow q$ is equivalent to $(p \to q) \wedge (q \to p)$.

Truth table :-

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

The proposition $p \leftrightarrow q$ may be expressed as:

a) "p if and only if q"

b) "p iff q"

c) "if p then q, and conversely"

d) "p is necessary and sufficient for q"

Example :- let p : You can take the flight and

q : You buy a ticket then $p \leftrightarrow q$ is the statement

" You can take the flight if and only if you buy a ticket".

Scanned by CamScanner

Well-formed formula (wff):-

A statement formula is not a statement; However, a statement can be obtained from it by replacing the variables by statements.

A Statement formula is an expression which is a string consisting of variables, parentheses, and connective symbols. Not every ~~symbol~~ string of these symbols is a formula. We shall now give a recursive definition of a statement formula, often called a well-formed formula.

A well-formed formula can be generated by the following rules:

1. A statement variable standing alone is a wff.
2. If P is a wff, then $\neg P$ is a wff.
3. If P and Q are wff's, then $(P \wedge Q)$, $(P \vee Q)$, $(P \rightarrow Q)$, $(P \leftrightarrow Q)$ are wff's.
4. A string of symbols containing the statement variables, connectives, and parenthesis is a wff, iff it can be obtained by finitely many applications of the rules 1, 2, and 3.

The following are wff's:-

$((\neg P) \vee Q)$, $\neg(P \wedge Q)$, $\neg(P \vee Q)$, $(P \rightarrow (P \vee Q))$, $((P \wedge Q) \vee R)$
$(P \rightarrow (Q \rightarrow R))$, $((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightleftarrows (P \rightarrow R)$.

The following are not wff's:

1. $\neg P \wedge Q$. obviously P and Q are wff's. A wff would be either $(\neg P \wedge Q)$ or $\neg(P \wedge Q)$
2. $(P \rightarrow Q) \rightarrow (\wedge Q)$. This is not a wff.
3. $(P \rightarrow Q$. parenthesis is missing.

Precedence of logical operators:-

Examples:-

$\neg p \wedge q$ is the conjunction of $\neg p$ and q,
i.e $(\neg p) \wedge q$.

$p \wedge q \vee r$ means $(p \wedge q) \vee r$

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

operator	precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Construction of Truth Table:-

Q. Construct the truth table of the compound proposition
$(p \vee \neg q) \rightarrow (p \wedge q)$

Sol: Truth table of $(p \vee \neg q) \rightarrow (p \wedge q)$

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

Rows: Need a row for every possible combination of values for the atomic propositions.

Columns: Need a column for the compound proposition (usually at far right)
- Need a column for the truth value of each expression that occurs in the compound proposition as it is built up.
- This includes the atomic propositions.

Q. How many rows are there in a truth table with n propositional variables?

Ans: With n propositional variables, we can construct 2^n distinct.

Scanned by CamScanner

Applications of propositional logic :-

① Translating English sentences to propositional Logic.

② System specifications.

③ Boolean searches.

④ Logic puzzles.

⑤ Logic ~~circuits~~ and Bit operations.

① Translating English sentences :-

There are many reasons to translate English sentences into expressions involving propositional variables and logical Connectives. In perticular, English is often ambiguous. Translating sentences into compound statements removes ambiguity.

steps: ① Identify atomic propositions and represent using propositional variables.

② Determine appropriate logical connectives.

Example ①: Translate the following English sentences into a logical expression.

ⓐ you can access the Internet from campus only if you are a computer science major or you are not a freshman.

Ans: a : you can access the Internet from Campus

c : you are a computer science major

f : you are a freshman.

only if is one way conditional statement.

Then the sentence can be translated to

$$a \rightarrow (c \vee \neg f)$$

ⓑ you cannot ride the rollercoaster if you are under 4 feet tall unless you are older than 16 years old.

p : you can ride the roller coaster

q : you are older than 16 years

r : you are under 4 feet tall

Then the sentence can be represented as

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

② **System Specifications:-**

Translating sentences in natual language (such as English) into logical expressions is an essential part of specifying both hardware and software systems.
System and software engineers take requirements in natural language and produce precise and unambiguous specifications that can be used as the basis for system development.

Example: (i) Express the specification " The automated reply cannot be sent when the file system is full" Using logical connectives.

Sol: Let p: The automated reply can be sent
q: The file system is full.
Specification can be represented by $q \to \neg p$.

Consistent System Specifications:- A list of propositions is consistent if it is possible to assign truth values to the proposition variables so that each proposition is true.

Example: Determine whether these system specifications are consistent.
" The diagnostic message is stored in the buffer or it is retransmitted."
" The dignostic message is not stored in the buffer"
" If the diagnostic message is stored in the buffer, then it is retransmitted".

So: First, we express them using logical expressions.
Let p: The diagnostic message is stored in the buffer
q: The diagnostic message is retransmitted.
The specifications can be written as $p \vee q$, $\neg p$ and $p \to q$.
Because we want $p \vee q$ to be true but p must be false and q must be true.
Because $p \to q$ is true when p is false and q is true.
So, we conclude that ~~thes~~ these specifications are consistent.
because they are all true when p is false and q is true.

Sol

③ Boolean Searches :-

Logical connectives are used extensively in searches of large collections of information, such as indexes of web pages. Because these searches employ techniques from propositional logic, In Boolean Searches, the connective AND is used to match records that contain both of two search terms, the connective OR is used to match one or both of two search terms, and the connective NOT (sometimes written as AND NOT) is used to exclude a perticular search term.

Example: Web page Searching. Most Web Search engines support Boolean Searching techniques, usually can help find web pages about perticular subjects.
For instance, Using Boolean searching to find web pages about

① Universities in New Mexico.
↓
we can look for pages matching NEW AND MEXICO AND UNIVERSITIES.

② To find pages that deal with Univerties in New Mexico or Arizona.
we can search for pages matching, (NEW AND MEXICO OR ARIZONA) AND UNIVERSITIES.

③ Universities in Mexico (and not New Mexico)
↳ (MEXICO AND UNIVERSITIES) NOT NEW. (or)
MEXICO UNIVERSITIES — NEW.
↳ NOT replaced by — (minus).

④ Logic puzzles :-

puzzles that can be solved Using logical reasoning are known as logic puzzles. Solving logic puzzles is an excellent way to practice working with the rules of logic. Computer programs designed to carry out logical reasoning often use well-known logic puzzles to illustrate their capabilities.

Example: Raymond Smullyan, An island has two kinds of inhabitants, knights, who ~~says~~ always tell the truth, and knaves, who always lie.
You go to the island and meet A and B.

- A says " B is a knight"
- B says " The two of us are of opposite types".

Example: What are the types of A and B?

Sol: Let p and q be the statements that A is a knight and B is a Knight, respectively. So, then $\neg p$ represents the proposition that A is a knave and $\neg q$ that B is a Knave.

- If A is a knight, then p is true. Since knight tells the truth, q must also be true. Then $(p \wedge \neg q) \vee (\neg p \wedge q)$ would have to be true, but it is not. So, A is not a knight and therefore $\neg p$ must be true.
- If A is a knave, then B must not be a knight since knaves always lie. So, then both $\neg p$ and $\neg q$ hold since both are knaves.

⑤ logic and Bit operations:-

Computers represent information using bits. A bit is a symbol with two possible values, namely, 0 (zero) and 1 (one). bit represents a binary digit. i.e. zeros and ones are the digits used in binary representation of numbers.

A bit can be used to represent a ~~truth~~ truth value, because there are two truth values, namely true and false.

True (T) — 1

false (F) — 0

A variable is called a Boolean variable if its value is either true or false. Boolean variable can be represented using a bit.

Computer bit operations correspond to the logical connectives. Replace true by a one and false by a zero in the truth tables for the operators $\wedge, \vee, \oplus$, as is for the operators $\vee, \wedge$, and $\oplus$, as is done in various programming languages. for the bit operators OR, AND, and XOR

Truth table for the bit operators OR, AND, and XOR

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

A bit string is a sequence of zero or more bits. The length of a string is the number of bits in the string.

Example: 1010100011 is a bit string of length nine.

Example: Find the bitwise OR, bitwise AND, bitwise XOR of the bit strings: 01 1011 0110 and 11 0001 1101.

bitwise OR

```
  01 1011 0110
  11 0001 1101
  ------------
  11 1011 1111
```

bitwise AND

```
  01 1011 0110
  11 0001 1101
  ------------
  01 0001 0100
```

bitwise XOR

```
  01 1011 0110
  11 0001 1101
  ------------
  10 1010 1011
```

Scanned by CamScanner

Propositional Equivalences:-

① **Tautology**:- A compound proposition that is always true is called "Tautology".

Example: $p \vee \neg p$

p	$\neg p$	$p \vee \neg p$
T	F	T
F	T	T

② **Contradiction**:- A compound proposition that is always false is called a "contradiction".

Example: $p \wedge \neg p$

p	$\neg p$	$p \wedge \neg p$
T	F	F
F	T	F

③ **Contingency**:- A compound proposition that is neither a tautology nor a contradiction is called a contingency.

Example: $p \rightarrow q$, $p \leftrightarrow q$.

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

Logical Equivalences:-

Compound propositions that have the same truth values in all possible cases are called "logically equivalent".

The compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology.

The notation $p \equiv q$ denotes that p and q are logically equivalent. The symbol $\Leftrightarrow$ is sometimes used instead of $\equiv$ to denote logical equivalence.

Logical equivalences:-

Table 1

Equivalence	Name
① $p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
② $p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
③ $p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
④ $\neg(\neg p) \equiv p$	Double negation law
⑤ $p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
⑥ $(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
⑦ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
⑧ $\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
⑨ $p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
⑩ $p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation laws

Table 2: Logical equivalences involving conditional statements.

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

Table 3: Logical equivalences involving biconditionals

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

Q. Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent

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

$$\therefore \neg(p \vee q) \underset{\leftrightarrow}{\overset{}{\equiv}} \neg p \wedge \neg q$$

Rules of Inference :- proofs in mathematics are valid arguments that establish the truth of mathematical statements.

Argument :- An argument in propositional logic is a sequence of propositions. (or) A sequence of statements that end with a conclusion. All but the final proposition in the argument are called premises and the final proposition is called the conclusion.

An argument is valid if the truth of all its premises implies that the conclusion is true.

Valid argument :- A valid argument is a sequence of propositions $P_1, P_2, ---, P_n$ called premises, together with a proposition C called the conclusion, such that the implication $P_1 \wedge P_2 \wedge \ldots \wedge P_n \Rightarrow C$ is a tautology.

An argument is valid if, whenever each of its premises $P_1, P_2, -- P_n$ is true, its conclusion C is also true.

Each inference can be written as an implication, as

(Conjunction of premises) $\longrightarrow$ Conclusion

The conclusion is a valid one, if the implication is a tautology.

$$\left.\begin{array}{l} P_1 \\ P_2 \\ \vdots \\ P_n \end{array}\right\} \text{sequence of premises}$$

$$\frac{\qquad\qquad}{\therefore C} \rightarrow \text{Conclusion}$$

An argument form in propositional logic is a sequence of compound propositions involving propositional variables. An argument form is valid if no matter which perticular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Rules of inference provide the justification of the steps used in a proof.

[inference - is an idea or conclusion that is drawn from evidence and reasoning.]

Scanned by CamScanner

Table 1. Rules of Inference for propositional logic

	Rule of Inference	Tautology	Name
1	p, $p \to q$, $\therefore q$	$[p \wedge (p \to q)] \to q$	Modus ponens (or) Law of detachment
2	$\neg q$, $p \to q$, $\therefore \neg p$	$[\neg q \wedge (p \to q)] \to \neg p$	Modus tollens (or) Law of contraposition
3	$p \to q$, $q \to r$, $\therefore p \to r$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$	Hypothetical Syllogism (or) Transitive rule
4	$p \vee q$, $\neg p$, $\therefore q$	$[(p \vee q) \wedge q] \to q$	Disjunctive Syllogism
5	p, $\therefore p \vee q$	$p \to (p \vee q)$	Addition
6	$p \wedge q$, $\therefore p$	$(p \wedge q) \to p$	Simplification
7	p, q, $\therefore p \wedge q$	$[(p) \wedge (q)] \to (p \wedge q)$	Conjunction
8	$p \vee q$, $\neg p \vee r$, $\therefore q \vee r$	$[(p \vee q) \wedge (\neg p \vee r)] \to (q \vee r)$	Resolution

Rules of inference :-

Establish the validity of some relatively simple argument forms, called rules of inference. These rules of inference can be used as building blocks to construct more complicated valid argument forms.

Example:

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array}$$

Using this notation, the hypotheses are written in a column, followed by a horizontal bar, followed by line that begins with the therefore ($\therefore$) symbol and ends with a conclusion.

Q. Check the validity of the following argument.

(a) It is below freezing now.
Therefore, it is either below freezing or raining now.

→ Let p be the proposition "It is below freezing" and q be the proposition "It is raining now". Then this argument is of the form.

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$ This is the addition rule.

(b) It is below freezing and raining now.

→ let p : below freezing
q : It is raining now. Then this argument is of the form,

$$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$$ This argument uses the Simplification rule.

(c) If John has a B in calculus, he will graduate
John has a B in Calculus.
Therefore, he will graduate.

→ let p : John has a B in Calculus
q : He will graduate
Then this argument is of the form $\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$ Modus ponens

(d) If Harry is dentist, then Harry drills teeth.
Harry does not drill teeth.
Therefore, Harry is not a dentist.

Let p: Harry is dentist
q: Harry drills teeth
then this argument is of the form

$$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

Modus tollens

(e) Either elephants are black or monkeys are green
Elephants are grey.
Therefore, monkeys are green.

Let p: Elephants are black
q: Monkeys are green
then this argument is of the form

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Disjunctive syllogism

(f) If Mary is a senior, then Mary wears a pin
If Mary wears a pin, then Mary will graduate.
Therefore, If Mary is a senior, then Mary will graduate.

Let p: Mary is a senior
q: Mary wears a pin
r: Mary will graduate
Then this argument is of the form

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

Hypothetical syllogism

Q. Check the validity of the following argument.
If Ram has completed B.E Computer science or M.B.A, then he is assured of a good Job.
If Ram is assured of a good Job, he is happy.
Ram is not happy.
Therefore, Ram is not completed M.B.A.

+ Let p: Ram has completed B.E computer science
q: Ram has completed M.B.A.
r: Ram is assured of a good Job.
s: Ram is happy.

The given premises are: 1. $(p \vee q) \to r$
2. $r \to s$
3. $\neg s$

1.	$(p \vee q) \to r$	premise 1
2.	$r \to s$	premise 2
3.	$(p \vee q) \to s$	Hythothetical Syllogism Using (1) & (2)
4.	$\neg s$	premise 3
5.	$\neg(p \vee q)$	Modus tollens Using (3) & (4)
6.	$\neg p \wedge \neg q$	Using De Morgans Law
7.	$\neg q$	Simplification Using (6).

Therefore, the conclusion is $\neg q$.

Fallacies:- Several common fallacies arise in incorrect arguments. These fallacies resemble rules of inference but are based on contingencies rather than tautologies.

Example: The proposition $[(p \to q) \wedge q] \to p$ is not a tautology. because it is false when p is false and q is true.

Scanned by CamScanner

Predicates and Quantifiers :-

Predicate Logic :- deals with predicates, which are propositions containing variables. It is an extension of propositional logic. It adds the concept of predicates and quantifiers to better capture the meaning of statements that cannot be adequately expressed by propositional logic.

(meaning satisfactory or acceptable extent.)

Example: "Every person who is 18 years or older, is eligible to vote".
The above statement cannot be adequately expressed using only propositional logic. Therefore we need a more powerful type of logic.

Q. What is a predicate?

Consider the statement, "x is greater than 3" has two parts.
The first part, the variable x, is the subject of the statement.
The second part, "is greater than 3", is the predicate.
It refers to the property that the subject of the statement can have.

The statement "x is greater than 3" can be denoted by $P(x)$ where P denotes the predicate "is greater than" and x is the variable.

The predicate P can be considered as a function. It tells the truth value of the statement $P(x)$ at x. Once a value has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth or false value.

In general, a statement involving n variables $x_1, x_2, \ldots, x_n$ can be denoted by $P(x_1, x_2, \ldots, x_n)$. Here P is also referred to as n-place predicate or n-ary predicate.

Example ①: Let $P(x)$ denote the statement "$x > 10$". What are the truth values of $P(11)$ and $P(5)$?

Sol: $P(11)$ is equivalent to the statement $11 > 10$, which is True.
$P(5)$ is equivalent to the statement $5 > 10$, which is False.

Example ②:- Let $R(x,y)$ denote the statement "$x = y+1$". What is the truth of the propositions $R(1,3)$ and $R(2,1)$?

Sol: $R(1,3)$ is the statement $1 = 3+1$, which is False.

$R(2,1)$ is the statement $2 = 1+1$, which is True.

We shall symbolize/represent a predicate by capital letters and subject by small letter.

① "Florida is a State" can be represented as $S(f)$.

② "Joe is a mathematician" represented as $M(j)$.

n-place predicate:

Examples: ① Ram is a student – $S(r)$ – 1-place predicate

② Jack is taller than Jill – $T(j_1, j_2)$ – 2-place predicate.

③ Sushan sits between Jack and Jill – $S(s_1, j_1, j_2)$ – 3 place predicate.

Predicate: 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.

Examples: ① $R(x)$: x is a rational number

② $G(y)$: $y > 5$

③ $S(x,y)$: $x + y = 5$

④ $L(x)$: x is a lawyer.

⑤ $C(y)$: y is a computer programmer

Quantifiers:-

When the variables in a propositional function are assigned values, the resulting statement becomes a proposition with a certain truth value. However, there is another important way, called quantification, to create a proposition from a proposition function.

Quantification expresses the extent to which a predicate is true over a range of elements. In English, all, some, many, none, and few are used in quantifications.

There are two types of quantifiers. They are:

① Universal quantifier: Which tells us that a predicate is true for every element under consideration.

② Existential quantifier:- Which tells us that there is one or more element under consideration for which the predicate is true.

① Universal quantifier:-

Many mathematical statements assert that a property is true for all values of a variable in a perticular domain, called the domain of discourse (or the universe of discourse) or domain.

Def: The universal quantification of $P(x)$ is the statement "$p(x)$ is true for all values of x in the domain".

The notation $\forall x\, P(x)$ denotes the universal quantification of $P(x)$.
Here $\forall$ is called the universal quantifier.

We read $\forall x\, P(x)$ as "For all x $P(x)$" or
"For every x $P(x)$" or "For each x $P(x)$".

$\forall x$ quantifies a conditional statement.
An element for which $P(x)$ is false is called a counterexample of $\forall x\, P(x)$.

$\forall x$ may be expressed as: All, for each, given any, for any, for arbitrary.

Note: It is best to avoid using 'for any'. It is ambiguous as to whether "any" means every or some.

Examples: ① All roses are red.
This can be understood as ~~for~~ every x.
If x is rose then x is red.

$R(x)$: x is rose

$P(x)$: x is red

The statement as $[R(x) \rightarrow P(x)]$ before use $\forall x$

$\therefore \quad \forall x \, [R(x) \rightarrow P(x)]$.

② Every apple is red

For every x, if x is apple then x is red.

$A(x)$: x is apple

$R(x)$: x is red.

$\forall x \, [A(x) \rightarrow R(x)]$.

③ Any integer is positive or negative

For any x if x is an integer then x is either positive or negative.

$I(x)$: x is an integer

$P(x)$: x is positive or negative.

$\forall x \, [I(x) \rightarrow P(x)]$.

The symbols (x) or $(\forall x)$ are called universal quantifiers.

(2) Existential quantifier :-

Many mathematical statements assert that there is an element with a certain property.

A proposition that is true if and only if $P(x)$ is true for at least one value of x in the domain.

Definition: The existential quantification of $P(x)$ is the proposition "There exists an element x in the domain such that $P(x)$".

We use the notation $\exists x \, P(x)$ for the existential quantification.

Here $\exists$ is called existential quantifier.

Without specifying the domain, the stmt $\exists x \, P(x)$ has no meaning.

$\exists x \, P(x)$ is read as ① There exists an x such that $P(x)$

② There is an x such that $P(x)$

③ There is atleast one x such that $P(x)$

④ for some x $P(x)$.

$\exists x$ quantifies a conjunction

Existential quantification may be expressed as:
There exists, for some, for at least one, or there is.

Examples: ① There exists a man

~~f~~: There exists an x such that x is a man.

$M(x)$: x is a man

$\exists x \; M(x)$

② Some men are clever.

There exists an x such that x is a man and x is clever.

$M_1(x)$: x is a man

$M_2(x)$: x is a clever.

$\exists x \, [M_1(x) \wedge M_2(x)]$.

Sentence	meaning	
① $\forall x \; P(x)$	All true	1
② $\exists x \; P(x)$	At least one true	5
③ $\neg [\exists x \; P(x)]$	None true	7
④ $\forall x [\neg P(x)]$	All False	3
⑤ $\exists x [\neg P(x)]$	Atleast one False	6
⑥ $\neg [\exists x [\neg P(x)]]$	None False	8
⑦ $\neg [\forall x \; P(x)]$	Not all true	2
⑧ $\neg [\forall x [\neg P(x)]]$	Not all False.	4

From the above table, we can conclude that

"All true" means "None False"

"All False" means "None True".

"Not all true" means "At least one False"

"Not all False" means "At least one True".

The above eight expressions can be grouped as: (Equivalent)

"All true" $\{\forall x\, P(x)\} \equiv \{\neg\{\exists x\, \{\neg P(x)\}\}\}$ = "None False"

"All False" $\{\forall x\, \{\neg P(x)\}\} \equiv \{\neg\{\exists x\, P(x)\}\}$ = "None True".

"Not all true" $\{\neg\, \{\forall x\, P(x)\}\} \equiv \{\exists x\, [\neg P(x)]\}$ = "At least one False".

"Not all False" $\{\neg\{\forall x \{\neg P(x)\}\}\} \equiv \{\exists x\, P(x)\}$ = "At least one True".

Quantifiers:

Statement	When true?	When False
① $\forall x\, P(x)$	$P(x)$ is true for every x	There is an x for which $P(x)$ is false.
② $\exists x\, P(x)$	There is an x for which $P(x)$ is true	$P(x)$ is false for every x.

Negating Quantified Expressions:-

	Statement	Negation
① All true	$\forall x\, P(x)$	$\exists x\, [\neg P(x)]$ At least one False
② At least one False	$\exists x\, [\neg P(x)]$	$\forall x\, P(x)$ All true
③ All False	$\forall x\, [\neg P(x)]$	$\exists x\, P(x)$ At least one true
④ At least one true	$\exists x\, P(x)$	$\forall x\, [\neg P(x)]$ All False.

predicate calculus:-

The area of logic that deals with predicates and quantifiers is called the predicate calculus.

Q. Write the following statements in Symbolic form:

ⓐ Some thing is good

ⓑ Every thing is good

ⓒ Nothing is good

ⓓ something is not good.

Let $G(x)$ be a good.

ⓐ $\exists x(G(x))$

ⓑ $\forall x(G(x))$

ⓒ $\forall x(\neg(G(x)))$

ⓓ $\exists x(\neg(G(x)))$.

Q. Write each of the following in symbolic form:

ⓐ All men are good $\quad \forall x[M(x) \rightarrow G(x)]$

ⓑ NO men are good $\quad \forall x(M(x) \rightarrow \neg G(x)) \equiv \neg \exists x [M(x) \wedge G(x)]$

ⓒ Some men are good $\quad \exists x[M(x) \wedge G(x)]$

ⓓ Some men are not good $\quad \exists x[M(x) \wedge \neg G(x)]$.

$M(x)$: x is a man

$G(x)$: x is good.

---

predicate logic uses the following new features:

Variables: x, y, z

predicates: $P(x), Q(x)$

Quantifier — Universal — $\forall x\ P(x)$
— Existential — $\exists x\ Q(x)$

propositional functions are a generalization of propositions.

- They contain variables and a predicate e.g. $P(x)$.

- Variables can be replaced by elements from their domain

Ex: Let $P(x)$: $x > 0$ domain be the integers.

$P(-3)$ is false

$P(0)$ is false

$P(3)$ is True.

Q. Translate each of the following Statements into symbols, Using quantifiers, Variables, and predicate Symbols.

ⓐ All birds Can fly

Let $B(x)$: x is a bird

$F(x)$: x Can fly

Then the stmt Can be written as $\forall x\,[B(x) \rightarrow F(x)]$

where universe of discourse is the set of all birds.

ⓑ Some babies are illogical.

Let $B(x)$: x is a baby

$I(x)$: x is illogical

The given stmt can be symbolized as $\exists x\,[B(x) \wedge I(x)]$

The universe of discourse is the set of all babies.

(f) All babies are illogical.

$\forall x\,[B(x) \rightarrow I(x)]$

(i) some men are not gaints

$\exists x\,[M(x) \wedge (\neg G(x))]$

ⓒ Some men are gaints

Let $M(x)$: x is a man

$G(x)$: x is a gaint

Stmt can be written as $\exists x\,[M(x) \wedge G(x)]$

where Universe of discourse is the set of Men in the World.

(g) All men are gaints

$\forall x\,[M(x) \rightarrow G(x)]$

(h) No men are gaints

$\forall x\,[(M(x)) \rightarrow \neg G(x)]$

ⓓ There is a student who likes mathematics but not history.

Let $S(x)$: x is a Student

$M(x)$: x likes mathematics

$H(x)$: x likes history

The stmt Can be written as $\exists x\,[S(x) \wedge M(x) \wedge H(x)]$

where universe of discourse is the set of all students at your college.

ⓔ Not all birds Can fly.

$\neg(\forall x)\,[B(x) \rightarrow F(x)]$ or $\exists x\,[B(x) \wedge (\neg F(x))]$

(J) If x is a man, then x is gaint.

Let $M(x)$: x is a man

$G(x)$: x is gaint

Symbolized as $M(x) \rightarrow G(x)$.

(K) x is an odd integer and x is prime.

$I(x)$: x is an odd integer

$P(x)$: x is prime

The Stmt can be symbolized as $I(x) \wedge P(x)$.

(l) For all integers x, x is odd and x is prime.

Let $I(x)$: x is odd

$P(x)$: x is prime

The Stmt can be written as $\forall x\, [I(x) \wedge P(x)]$

(m) There is an integer x such that x is odd and x is prime.

$\exists x\, [I(x) \wedge P(x)]$

(n) Not every actor is talented who is famous.

Let $A(x)$: x is an actor

$T(x)$: x is talented

$F(x)$: x is famous

$\exists x\, [A(x) \wedge F(x) \wedge (\neg T(x))]$

At least one actor who is famous is not talented.

(o) x is rational implies that x is real.

Let $R_1(x)$: x is rational

$R_2(x)$: x is real

$R_1(x) \rightarrow R_2(x)$.

(p) Not every graph is planar

Let $G(x)$: x is a graph

$P(x)$: x is planar

The Stmt can be written as $\neg[\forall x\, (G(x) \rightarrow P(x))]$

(q) Some numbers are rational.

Let $N(x)$: x is a number

$R(x)$: x is rational

The stmt can be written as $\exists x [N(x) \wedge R(x)]$

(r) Some numbers are not rational

$\exists x [N(x) \wedge (\neg R(x))]$

(s) Not all numbers are rational.

$\neg [\forall x [N(x) \rightarrow R(x)]]$

(t) If some students are lazy, then all students are lazy.

$S(x)$: x is a student

$L(x)$: x is lazy.

some students are lazy

$[\exists x [S(x) \wedge L(x)]]$

All students are lazy

$\forall x [S(x) \rightarrow L(x)]$

$\therefore$ The final stmt can be written as

$(\exists x [S(x) \wedge L(x)]) \rightarrow (\forall x [S(x) \rightarrow L(x)])$.

---

(1) Examples:

$p(x)$ — x is free

$p(5)$ — x is bound to 5

$\forall x\, p(x)$ — x is bound by quantifier

Other quantifiers:-

① Uniqueness quantifier:-

Definition: "There exists a unique x such that $P(x)$ is true".
denoted by $\exists!$ or $\exists_1$. $\exists! x\, P(x)$ or $\exists_1 x\, P(x)$.
Other phrases for uniqueness quantification include "There is exactly one" and "There is one and only one".

Precedence of Quantifiers:-

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus.
For example, $\forall x\, P(x) \vee Q(x)$ is the disjunction of $\forall x\, P(x)$ and $Q(x)$.
$\equiv (\forall x\, P(x)) \vee Q(x)$.

Binding Variables:-

When a quantifier is used on the variable x, we say that this occurance of the variable is bound. Example: $P(5)$ - x is bound to 5

An occurance of a variable that is not bound by a quantifier (or) set equal to a perticular value is said to be free. Ex: $P(x)$ - x is fee

① All the variables that occur in a propositional function must be bound or set equal to a perticular value to turn it onto a proposition. This can be done using a combination of universal quantifiers, existential quantifiers and value assignments.
Ex: $\forall x\, P(x)$ x is bound by quantifier.

Example: $\exists x\,(x+y=1)$, the variable x is bound by the existential quantifier $\exists x$, but the variable y is free because it is not bound by a quantifier and no value is assigned to this variable. $\therefore$ $\exists x\,(x+y=1)$, x is bound, but y is free.

The part of a logical expression to which a quantifier is applied is called the scope of this quantifier.
A variable is free if it is outside the scope of all quantifiers.

$\exists x\,(P(x) \wedge Q(x)) \vee \forall x\, R(x)$, all variables are bound. The scope of the first quantifier, $\exists x$, is the expression $P(x) \wedge Q(x)$. because $\exists x$ is applied only to $P(x) \wedge Q(x)$. and not to the rest of the stmt.

i.e the existential quantifier binds the variable x in $P(x) \wedge Q(x)$.
and the universal quantifier $\forall x$ binds the variable x in $R(x)$.
observe that ~~we can~~ using two different variables x and y, as
$\exists x (P(x) \wedge Q(x)) \vee \forall y R(y)$. because the scopes of the two quantifiers
donot overlap.

Logical equivalences involving quantifiers:-

Definition:- stmts involving predicates and quantifiers are logically equivalent if and only if they have the same truth value nomatter which predicates are substituted into these stmts and which domain of discourse is used for the variables in these propositional functions.

$S \equiv T$, indicates that S and T involving predicates and quantifiers are logically equivalent.

Example: $\underbrace{\forall x (P(x) \wedge Q(x))}_{\text{true}} \equiv \underbrace{\forall x P(x) \wedge \forall x Q(x)}_{\text{true}}$.

true — Also — true

Translating from English into logical expression:-

Q. Express the stmt " Every student in this class has studied calculus" Using predicates and quantifiers.

A We rewrite the Smt as:
"For every student in this ~~cal~~ class, that student has studied calculus".

Next, we introduce a variable x, so the above stmt becomes
For every student x in this class, x has studied calculus.

Let $C(x)$: x has studied calculus.
if the domain for x consists of the students in the class,
so, we can translate the stmt as $\forall x \, C(x)$.

Q. For every person x, if x is a student, then x has visited Mexico or x has visited Canada.

Let $M(x)$: x has visited Mexico
$C(x)$: x has visited Canada
$S(x)$: x is a student

$$\forall x [S(x) \rightarrow [M(x) \vee C(x)]]$$

Scanned by CamScanner

Using quantifiers in system specifications:-

Q. Use predicates and quantifiers to express the system specifications

① "Every mail message larger than one megabyte will be compressed".

② "If a user is active, at least one network link will be available".

A.

① Let $S(m, y)$ be Mail message m is larger than y megabytes.
Where the variable x has the domain of all mail messages and the variable y is a positive real number.
$C(m)$ denote Mail message m will be compressed.
So, the stmt can be written as $\forall m[S(m,1) \rightarrow C(m)]$

② Let $A(u)$: User u is active
Where u has the domain of all users.
$S(n, x)$: Network link n is in state x
Where n has the domain of all network links and
x has the domain of all possible states for a network link.
Then the specification ~~as~~ "If a user is active, at least one network link will be available".
Can be represented as $\exists u\, A(u) \longrightarrow \exists n\, S(n, \text{available})$.

problem solving:-

Q①:-
All Lions are fierce. } premises
Some Lions ~~are~~ do not drink coffee.
Some fierce creatures do not drink coffee.

Conclusion:

A. Let $P(x)$: x is a Lion
$Q(x)$: x is fierce
$R(x)$: x drinks coffee
Assuming that the domain ~~of~~ consists of all creatures.
We express the above stmts as

$$\forall x\,[P(x) \rightarrow Q(x)]$$

$$\exists x\,[P(x) \wedge \neg R(x)]$$

$$\exists x\,[Q(x) \wedge \neg R(x)]$$

Scanned by CamScanner

~~Nested Quantifiers~~:-

Rules of Inference for Quantified statements:-

Rule of Inference	Name
① $\dfrac{\forall x\, P(x)}{\therefore P(c)}$	Universal instantiation
② $\dfrac{P(c) \text{ for any arbitrary } c}{\therefore \forall x\, P(x)}$	Universal generalization
③ $\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
④ $\dfrac{P(c) \text{ for some element } c}{\therefore \exists x\, P(x)}$	Existential ~~instantiation~~ generalization

---

① Universal instantiation/Specification:-

The rule of inference used to conclude that $P(c)$ is true, where c is a perticular member of the domain, given the premise $\forall x\, P(x)$.

$$\frac{\forall x\, P(x)}{\therefore P(c)}$$

Example ①:- Universe is the set of humans.

let $M(x)$: x is mortal, then if $\forall x\, M(x)$ is true.

i.e All men are mortal, they as per this rule we can conclude that " Socrates is mortal".

② All women are wise

so Lisa is wise. where Lisa is a member of the domain of all women.

② Universal generalization:-

$\forall x\, P(x)$ is true, given the premise that $P(c)$ is true for all elements c in the domain.

This rule holds - provided we know $P(c)$ is true for each element in the Universe.

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x\, P(x)}$$

③ Existential instantiation:-

There is an element c in the domain for which $P(c)$ is true if we know that $\exists x\, P(x)$ is true.

We cannot select an arbitrary value of c.

$$\frac{\exists x\, P(x)}{\therefore P(c) \text{ for some element } c}$$

④ Existential generalization:-

$\exists x\, P(x)$ is true when a perticular element c with $P(c)$ true is known.

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x\, P(x).}$$

problems:-

① Consider the argument

All men are fallible

All kings are men

Therefore, all kings are fallible.

Let $M(x)$: x is a man

$K(x)$: x is a king

$F(x)$: x is fallible

Then the above argement is symbolized as

1. $\forall x\,[M(x) \rightarrow F(x)]$
2. $\forall x\,[K(x) \rightarrow M(x)]$
3. $\therefore \forall x\,[K(x) \rightarrow F(x)]$

A formal proof is as follows:

	Assertion	Reason
1.	$\forall x\,[M(x) \rightarrow F(x)]$	premise 1
2.	$M(c) \rightarrow F(c)$	Step 1 and Universal Specification) instantiation
3.	$\forall x\,[K(x) \rightarrow M(x)]$	premise 2
4.	$K(c) \rightarrow M(c)$	Step 3 and Universal instantiation
5.	$K(c) \rightarrow F(c)$	steps 2 & 4 & ~~Simplification~~ (HS) transitive rule.
6.	$\forall x\,[K(x) \rightarrow F(x)]$	Step 5 and hypothetical syllogism.

(2) Lions are dangerous animals
There are Lions.
Therefore, there are dangerous animals.

$L(x)$: x is a Lion
$D(x)$: x is dangerous

1 $\forall x\,[L(x) \rightarrow D(x)]$
2 $\exists x\, L(x)$

3 $\therefore \exists x\, D(x)$.

Formal proof:-

	Assertion	Reasons
1.	$\exists x\, L(x)$	premise 2
2.	$L(a)$	Step 1 & Existential instantiation
3.	$\forall x\,[L(x) \rightarrow D(x)]$	~~Step 2 and universal instantiation~~ premise 1
4.	$L(a) \rightarrow D(a)$	step 3 & universal instantiation
5.	$D(a)$	step 2 & 4 & Hypothetical syllogism
6.	$\exists x\, D(x)$	step 5 & Existential generalization.

Nested quantifiers:-

Two quantifiers are nested if one is within the scope of the other.

Example: ① $\forall x\ \underbrace{\exists y \boxed{(x+y=0)}}_{Q(x)}$ — $P(x,y)$

Everything within the scope of a quantifier. in the propositional function.

$\forall x\ Q(x)$
$\hookrightarrow \exists y\ P(x,y)$

$P(x,y)$ is $(x+y=0)$

Nested quantifiers commonly occur in mathematics and computer science.

② $\forall x \forall y\ (x+y=y+x)$ — x and y are variables in the domain of all real numbers.

& For all real numbers x and y, $x+y=y+x$

similarly, $\forall x \forall y \forall z\ (x+(y+z)=(x+y)+z) \Rightarrow$ Associative law for addition of real numbers.

③ $\forall x \forall y\ ((x>0)\wedge(y<0)\rightarrow(xy<0))$ consists of all real numbers.

Where the domain for both variables

& For every real numbers x and y, if x is positive and y is negative then xy is negative.

The product of a positive real number and a negative real number is always a negative real number.

④

Note: In working with quantifications of more than one variables, it is sometimes helpful to think in terms of nested loops.

The order of quantifiers:-

Many mathematical statements involve multiple quantifications of propositional functions involving more than one variable.

Example ①: Let $P(x,y)$: $x+y=y+x$. What are the truth values of the quantifications $\forall x \forall y\, P(x,y)$ and $\forall y \forall x\, P(x,y)$. Where the domain for all variables consists of all real numbers?

Ans. $\forall x \forall y\, P(x,y)$ denotes the proposition

"For all real numbers x, for all real numbers y, $x+y=y+x$".

because $P(x,y)$ is true for all real numbers x and y, the proposition $\forall x \forall y\, P(x,y)$ is true.

$\boxed{\text{Theorem 1}}$ The stmt says " The order of nested universal quantifiers in a stmt without other quantifiers can be changed without changing the meaning of the quantified stmt.

Theorem 2: The order of nested existential quantifiers in a stmt without other quantifiers can be changed without changing the meaning of the quantified stmt.]

Table: Quantification of two variables

Stmt	When True?	When False?
① $\forall x \forall y\, P(x,y)$ $\forall y \forall x\, P(x,y)$	$P(x,y)$ is true for every pair x, y.	There is a pair x, y for which $P(x,y)$ is false.
② $\forall x \exists y\, P(x,y)$	For every x there is a y for which $P(x,y)$ is true.	There is an x such that $P(x,y)$ is false for every y.
③ $\exists x \forall y\, P(x,y)$	There is an x for which $P(x,y)$ is true for every y	For every x there is a y for which $P(x,y)$ is false.
④ $\exists x \exists y\, P(x,y)$ $\exists y \exists x\, P(x,y)$	There is a pair x, y for which $P(x,y)$ is true.	$P(x,y)$ is false for every pair x, y.

Ex: Let $Q(x,y,z)$: $x+y=z$. What are the truth values of the stmts $\forall x \forall y \exists z\, Q(x,y,z)$ and $\exists z \forall x \forall y\, Q(x,y,z)$, where domain of all variables consists of all real numbers?

Ans Let x & y are assigned variables. $\forall x \forall y \exists z\, Q(x,y,z)$ means

" For all real numbers x and for all real numbers y, there is a real number z such that $x+y=z$".

Translating Mathematical stmts into stmts involving Nested quantifiers:-

Q① Translate the stmt " The sum of two positive integers is always positive" into a logical expression.

A " For every two integers, if these integers are both positive, then the sum of these integers is positive".

We introduce the variables x and y. So we can state the stmt as " For all positive integers x and y, $x+y$ is positive".

$\Rightarrow \forall x \forall y\, ((x>0) \wedge (y>0) \rightarrow (x+y>0))$

domain: x and y are variables consists of all integers.

Then the stmt: The sum of two positive integers is always positive". becomes " For every two positive integers, the sum of these integers is positive".

We can express this as $\forall x \forall y\, (x+y>0)$, where the domain for both variables consists of all positive integers.

② " Every real number except zero has a multiplicative inverse" (A multiplicative inverse of a real number x is a real number y such that $xy=1$).

A " For every real number x except zero, x has a multiplicative inverse".

We can rewrite this as " For every real number x, if $x \neq 0$, then there exists a real number y such that $xy=1$".

This can be rewritten as $\forall x\, (x \neq 0) \rightarrow \exists y\, (xy=1)$.

③ " If a person is female and is a parent, then this person is someone's mother" with a domain consisting of all people.

A " For every person x, if person x is female and person x is a parent, then there exists a person y such that person x is the mother of person y"

Let $F(x)$: x is female

$P(x)$: x is a parent

$M(x,y)$: x is the mother of y

The stmt can be written as $\forall x((F(x) \wedge P(x)) \rightarrow \exists y\, M(x,y))$

The final stmt is $\forall x \exists y \left[(F(x) \wedge P(x)) \rightarrow M(x,y)\right]$

Negating Nested Quantifiers:-

Statements involving nested quantifiers can be negated by successively applying the rules for negating statements involving a single quantifier.

Example ①: Express the negation of the stmt $\forall x \exists y (xy = 1)$.

Apply De. Morgan's Laws for quantifiers.

$\neg(\forall x \exists y (xy=1)) = \exists x \forall y (xy \neq 1)$

Quantifiers as conjunctions and Disjunctions:-

$\forall x P(x) = P(1) \wedge P(2) \wedge P(3)$

$\exists x P(x) = P(1) \vee P(2) \vee P(3)$.

If U consists of the integers 1, 2 and 3.

Counter example:-

An element for which $P(x)$ is false is called a Counterexample of $\forall x P(x)$.

Example ②: Let $Q(x): x < 2$. What is the truth value of the quantification $\forall x Q(x)$, where the domain consists of all real numbers?

$Q(x)$ is not true for every real number x, because, for instance, $Q(3)$ is false. i.e $x = 3$ is a counterexample for the stmt $\forall x Q(x)$. Thus $\forall x Q(x)$ is false.

Q. Translate the following stmt into English.

$\forall x (C(x) \vee \exists y (C(y) \wedge F(x,y)))$

Where $C(x)$: x has a Computer

$F(x,y)$: x and y are friends

Domain of x and y: all Students.

For every student x in your school, x has a computer or there is a student y such that y has a computer and x and y are friends.

In other words, Every Student has a Computer or has a friend that has a Computer.

Q. Translating the following statements into logical expression.

ⓐ Everyone has exactly one best friend.

$B(x,y)$: y is the best friend of x.

→ For every person x, person x has exactly one best friend.

Introducing the universal quantifier, then the statement as

$\forall x$ (person x has exactly one best friend)

Where the domain consists of all people.

We rewrite the statement as

For all x, there is y who is the best friend of x and for every person z, if person z is not person y, then z is not the best friend of x.

$\forall x \exists y (B(x,y) \wedge \forall z [(z \neq y) \rightarrow \neg B(x,z)])$

Domain of x, y, and z: all people.

ⓑ There is a woman who has taken a flight on every airline in the world.

→ Let $T(w,f)$: w has taken flight

$A(f,a)$: flight is on airline

$\exists w \forall a \exists f (T(w,f) \wedge A(f,a))$

Domain of w: all people

Domain of f: all flights

Domain of a: all airlines.

[In other way, $\exists w \forall a \exists f \, R(w,f,a)$ where $R(w,f,a)$ is "w has taken f on a"]

Introduction to proofs:-

① A theorem is a statement that can be shown to be true. → Can also be referred to as facts or results.

A proof is a valid argument that establishes the truth of a mathematical statement. A proof can use the hypothesis of the theorem.

A theorem is true with a proof (valid argument) using:

- Definitions
- previously proven theorems or other theorems.
- Rules of Inference
- Axioms — A stmt that is assumed to be true.

Applications:- ① Verifying that computer programs are correct

② Establishing that operating systems are secure.

③ Making inferences in artificial Intelligence.

④ Showing that system specifications are consistent.

- A Lemma is a 'helping theorem' or a result which is needed to prove a theorem.
- A corollary is a result which follows directly from a theorem.
- Less important theorems are sometimes called propositions.
- A Conjucture is a statement that is being proposed to be true. Once a proof of a conjucture is found, it becomes a theorem. It may turn out to be false. so they are not theorems.

Understanding how Theorems are stated. / Forms of Theorems

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers.
- often the universal quantifier (needed for a precise stmt of a theorem) is omitted by standard mathematical convention.

Example: If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$. means that

For all positive real numbers x and y,

if $x > y$, then $x^2 > y^2$.

Methods of proving theorems:-

① Direct proof :-

In a direct proof, we show that conditional statement $p \to q$ is true. We assume that p is true and show that q must also be true, so that the combination p is true and q false never occcers.

In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, finally to show that q must also be be true.

→ Sequence of steps leading from the hypothesis to the conclusion. [Direct proof lead from hypothesis of a theorem to the conclusion].

Definition ①: The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k+1$. (Every integer is either even or odd and no integer is both even and odd).

Example ①: Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd".

Sol: Assume n is an odd integer

Then $n = 2k+1$ for some integer k

We can square both sides of the equation $n = 2k+1$

$$n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$$
$$= 2m+1$$

where $m = 2k^2+2k$

Hence n^2 is odd.

∴ We have proved that if n is an odd integer, then n^2 is odd.

Scanned by CamScanner

Example ②: Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.

Sol: Let r and s are two integers,

then $m = r^2$ and $n = s^2$

now $nm = s^2 r^2$

$= (sr)^2$

$= (t)^2$ where $t = sr$

Hence proved.

$\therefore$ if m and n are both perfect squares, then nm is also a perfect square.

② proof by Contraposition:-

proof by contraposition is a type of indirect proof.

We know that $p \rightarrow q \equiv \neg q \rightarrow \neg p$.

This means that the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive $\neg q \rightarrow \neg p$ is true.

In a proof by contraposition of $p \rightarrow q$, we assume that $\neg q$ is true (or we take $\neg q$ as a hypothesis) and using axioms, definitions, and previously proven theorems, together with rules of inference, and we show that $\neg p$ is true.

Example ①:- prove that if n is an integer and $\underbrace{3n+2 \text{ is odd}}_{p}$, then $\underbrace{n \text{ is odd}}_{q}$. $(\neg q)$

Sol: Assume that n is even (negation). So, n can be expressed as $2k$ for some integer k (definition of even)

$n = 2k$

$\therefore \quad 3n+2 = 3(2k)+2$

$= 6k+2$

$= 2(3k+1)$

So, $3n+2$ is even $(\neg p)$

Hence proved.

Example ⑧ :- prove that if $n = ab$, where a and b are positive integers, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$.

Sol: $n = ab$ then $a \le \sqrt{n}$ or $b \le \sqrt{n}$

Now assume that the above stmt is false

$\neg (a \le \sqrt{n}$ or $b \le \sqrt{n})$
$\vee$

$a > \sqrt{n}$ and $b > \sqrt{n}$

$ab > \sqrt{n} \cdot \sqrt{n}$

$ab > n$

ab is not equal to n i.e $ab \neq n$

which contradicts the statement $n = ab$.

③ proof by Contradiction :- (AKA reductio ad absurdum)

It is another type of indirect proof. $p \to q$

[To prove P, assume $\neg P$ and derive a contradiction such as $P \wedge \neg P$. Since we have shown that $\neg P \to F$ is true, it follows that the contrapositive $T \to p$ as holds.]

Assume p and $\neg q$ are true. showing that q must also be true. This implies that q and $\neg q$ are both true. This is a contradiction. (or) Assume P and $\neg q$ is true. Showing that $\neg P$ must also be true. This implies that P & $\neg P$ are both true. This is a contradiction.

Example ①: prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Definition 2: The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called irrational.

let p be the proposition "$\sqrt{2}$ is irrational".

$\neg P$: $\sqrt{2}$ is rational, and thus $2 = \frac{a}{b}$ where a & b have no common factors. Thus $2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2$ and thus a^2 is even.

a^2 is even and so a is even.

let $a = 2c$ for some Integer c

$2b^2 = 4c^2$ and $b^2 = 2c^2$, and b^2 is even, b must also even.

This is contradiction. our assumption must be false.

Example ②: If $3n+2$ is odd, then n is odd. Give proof by Contradiction.

Let p: $3n+2$ is odd & q: n is odd

To construct a proof by contradiction, Assume p & $\neg q$ are true.

i.e $3n+2$ is odd and n is even.

If n is even, there is an integer k such that $n=2k$.

This implies that $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1) =$ even $= \neg p$

because an integer is even iff it is not odd. Because p & $\neg p$ are true, we have a contradiction.

④ Vacuous and Trivial proofs:-

Vacous proof:- If we know p is false then $p \rightarrow q$ is true as well. [or $p \rightarrow q$ is true when p is false]

Example: ① ~~If it is raining then~~ If I am both rich and poor ~~then~~ then $2+2=5$.

② let $P(n)$: $\forall n$ If $n>1$, then $n^2>n$, where the domain is all integers. sol: Vacuously, $P(0)$ is true since $\underset{F}{0>1} \rightarrow \underset{F}{0>0}$ is true

Trivial proof:- If we know q is true, then $p \rightarrow q$ is true as well. [or $p \rightarrow q$ is true when q is true]

Example ①: If it is raining, then $1=1$.

② let $P(n)$: If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$ where the domain is all integers.

sol: Trivially, $P(0)$ is true since: $a^0 \geq b^0$ regardless to the hypothesis

⑤ Counterexample:-

A statement of the form $\forall x\, P(x)$ to be false.

Ex ① Show that the stmt "Every positive integer is the sum of the squares of two integers" is false.

sol: 3 cannot be written as the sum of the squares of two integers. This statement is ~~false~~ True.

Ex ②: Let $Q(x)$ be the stmt '$x<2$'. $\forall x\, Q(x)$ is false.

sol: $Q(x)$ is not true for every real number x, for instance, $Q(3)$ is false. i.e $x=3$ is a counterexample for the stmt $\forall x\, Q(x)$.

Therefore, $\forall x\, Q(x)$ is false.

⑥ proofs of Equivalence:-

To prove a theorem that is a biconditional statement, i.e a stmt of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. The validity is based on the tautology.

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$$

Example ①: prove the theorem "If n is a positive integer, then n is odd if and only if n^2 is odd".

Sol: let p: n is odd and q: n^2 is odd

To prove this theorem, we need to show that $p \to q$ and $q \to p$ are true.

prove $p \to q$ is true: Assume n is an odd integer

Then $n = 2k+1$ for some integer k

square on both sides

$$n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1 = 2m+1$$

where $m = 2k^2+2k$

$n^2 = $ odd

$\therefore$ $p \to q$ is true.

prove $q \to p$ is true:-

~~proof by contradiction example①~~

~~Assume n^2 is odd~~

~~Then $n = 2k+1$ for some integer k, n is odd.~~

$\cancel{[n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k+1)]}$

~~$q \to p$ is also true~~

$\therefore$ ~~$p \to q$ is true and $q \to p$ is true~~.

Hence $p \leftrightarrow q$ is true.

The propositions $p_1, p_2, p_3, \ldots, p_n$ are equivalent. This can be written as $p_1 \leftrightarrow p_2 \leftrightarrow p_3 \ldots \leftrightarrow p_n$, which states that all n propositions have same truth values, and consequently, that for all i and j with $1 \le i \le n$ & $1 \le j \le n$, p_i and p_j are equivalent. one way to prove these mutually equivalent is to use the tautology.

$$[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n] \leftrightarrow [(p_1 \to p_2) \land (p_2 \to p_3) \land \ldots \land (p_n \to p_1)].$$

if the conditional stmts $p_1 \to p_2, p_2 \to p_3, \ldots p_n \to p_n$ can be shown to be true, then the propositions $p_1, p_2, \ldots p_n$ are all equivalent.

Example in Next page. ①

⑦ Mistakes in proofs:- There are many common errors made in constructing mathematical proofs.

Example ①: What is wrong with this proof that $1=2$?

proof: We use these steps, where a and b are two equal positive integers.

	Step	Reason
1.	$a=b$	Given
2.	$a^2 = ab$	multiply both sides of (1) by a
3.	$a^2-b^2 = ab-b^2$	subtract b^2 from both sides of (2)
4.	$(a-b)(a+b) = b(a-b)$	Factor both sides of (3)
5.	$a+b=b$	Devide both sides of (4) by $a-b$
6.	$2b=b$	Replace a by b in (5) because $a=b$ and simplify
7.	$2=1$	Devide both sides of (6) by b

Sol: Every step is valid except for one, step 5.
There is an error in step 5.
$a-b=0$ by the premise and division by 0 is undefined.

Example ②: What is wrong with this proof?

Theorem:- If n^2 is positive, then n is positive.

proof: Suppose that n^2 is positive. Because the conditional stmt "If n is positive, then n^2 is positive" is true.
We can conclude that n is positive.

Sol: A counter example is supplied by $n=-1$ for which $n^2=1$ is positive, but n is negative.

① ~~Logical~~ proofs of equivalence:-

Example ②: show that these stmts about the integer n are equivalent:

P_1 : n is even

P_2 : $n-1$ is odd

P_3 : n^2 is even.

Sol: We use a direct proof to show that $P_1 \rightarrow P_2$.

Suppose that n is even.

Then $n = 2k$ for some integer k

Consequently, $n-1 = 2k-1 = 2(k-1)+1$

$= 2m+1$ where $m = k-1$

$n-1 = \text{odd}$

We also use a direct proof to show that $P_2 \rightarrow P_3$:

Suppose $n-1$ is odd, then $n-1 = 2k+1$ for some integer k

Hence $n = 2k+2$

Square on both sides

$n^2 = (2k+2)^2 = 4k^2+8k+4 = 2(2k^2+4k+2)$

$= \text{even}$

To prove $P_3 \rightarrow P_1$, we use a proof by contraposition.

We prove ~~Assume~~ that if n is not even, then n^2 is not even. Means that "if n is odd, then n^2 is odd. [Example problem in proof by contraposition].

This completes the proof.

$P_3 \rightarrow P_1 \equiv$ If n^2 is even, then n is even

$P + \neg P$

n is odd

$n = 2k+1$

$n^2 = (2k+1)^2 = 2m+1 = \text{odd}$. $m \rightarrow 2k^2+2k$

$\neg P$.

Hence proved.

Proof methods and Strategy:-

1. Proof by cases.
2. Exhaustive proof.
3. Existence proofs
   - (a) Constructive
   - (b) Nonconstructive.
4. Uniqueness proofs.
5. proof strategies
   - (a) Forward Reasoning
   - (b) Backward Reasoning
   - (c) Looking (Searching) for Counterexamples
   - (d) Adapting Existing proofs
6. The Role of open problems
7. Validity problem for propositional and predicate Logic.

1. proof by cases:-

Def:- A proof by cases must cover all possible cases that arise in a theorem.

- To prove a conditional statement of the form:

$$(P_1 \vee P_2 \vee \ldots \vee P_n) \to q$$

$$\equiv \neg(P_1 \vee P_2 \vee \ldots \vee P_n) \vee q$$

$$\equiv (\neg P_1 \wedge \neg P_2 \wedge \ldots \wedge \neg P_n) \vee q$$

$$\equiv (\neg P_1 \vee q) \wedge (\neg P_2 \vee q) \wedge \ldots \wedge (\neg P_n \vee q)$$

$$\equiv (P_1 \to q) \wedge (P_2 \to q) \wedge \ldots \wedge (P_n \to q).$$

- Use the tautology

$$[(P_1 \vee P_2 \vee \ldots \vee P_n) \to q] \leftrightarrow [(P_1 \to q) \wedge (P_2 \to q) \wedge \ldots \wedge (P_n \to q)]$$

can be used as a rule of inference.

- Each of the implications $P_i \to q$ is a case. where $i = 1, 2, \ldots n$.

- prove a theorem by considering different cases seperately.

Example ①:- prove that if n is an integer, then $n^2 \geq n$.

Solution: ~~Proof~~: Consider 3 possible cases, when $n=0$, when $n \geq 1$, (positive) and when $n \leq -1$. (negative).

Case (i): If $n=0$, then $0^2=0$, we see that $0^2 \geq 0$. Thus, $n^2 \geq n$ is true in this case.

Case (ii): when $n \geq 1$, we multiply both sides by n, then $n \cdot n \geq n \cdot 1$. This implies that $n^2 \geq n$ for $n \geq 1$.

Case (iii): when $n \leq -1$. However, $n^2 \geq 0$, It follows that $n^2 \geq n$.

Because the inequality $n^2 \geq n$ holds in all three cases, we conclude that if n is an integer, then $n^2 \geq n$.

Example ②:- prove that $|xy| = |x||y|$, where x and y are real numbers.

[Definition: The absolute value of a, $|a|$, equals a when $a \geq 0$ and equals $-a$ when $a < 0$].

Sol: Break the theorem into some cases:

① x and y both nonnegative

② x nonnegative and y is negative

③ x negative and y is nonnegative

④ x and y both negative.

check possible cases:

Case 1: We see that $P_1 \to q$ because $xy \geq 0$ when $x \geq 0$ and $y \geq 0$,
So that $|xy| = xy = |x||y|$.

Case 2: To see that $P_2 \to q$, because $x \geq 0$ & $y < 0$, then $xy \leq 0$,
So that $|xy| = -xy = x(-y) = |x||y|$.

Case 3: To see that $P_3 \to q$, because $x < 0$ & $y \geq 0$, then $xy \leq 0$,
So that $|xy| = -xy = (-x)y = |x||y|$

Case 4: To see that $P_4 \to q$, because $x < 0$ & $y < 0$, then $xy \geq 0$.
So that $|xy| = xy = (-x)(-y) = |x||y|$.

Because it is true for all four cases, so $|xy| = |x||y|$, where x and y are real numbers.

Leveraging proof by cases:- When it is not possible to consider all cases of a proof at the same time, a proof by cases should be considered. When should you use such a proof? We look for a proof by cases when there is no obvious way to begin a proof, but when extra information in each case helps move the proof forward.

Without Loss of Generality (WLOG):-

How to shorten the proof by cases.

- If the same argument is used in different cases.
  - proved the cases together, without loss of generality (WLOG).
- Incorrect use of this principle can lead to errors.

Common errors with Exhaustive proof and proof by Cases:-

A Common error of reasoning is to draw incorrect Conclusions from examples. No matter how many seperate examples are considered, a theorem is not proved by considering examples unless every posible case is covered.

The problem of proving a theorem is analogous to showing that a computer program always produces the desired output. No matter how many input values are tested, unless all input values are tested, we cannot conclude that the program always produces the correct output.

Example 1: What is wrong with this 'proof'?

Theorem: If x is a real number, then x^2 is a positive real number.

Proof: Let P_1 be "x is positive",
P_2 be "x is negative", and
q be "x^2 is positive".

To show that $P_1 \to q$ is true, when x is positive, x^2 is positive.
Because, the product of two positive numbers is positive $= x \cdot x = +ve$.

To show that $P_2 \to q$ is true, when x is negative, x^2 is positive.
Because, the product of two negative numbers is positive $\} = (-x)(-x) = +ve$

This completes the proof.

Solution: We have missed the case when $x=0$, $x^2=0$ is not positive. So this theorem is false.

If P is "x is a real number", then we can prove results where P is the hypothesis with three cases, P_1, P_2 and P_3, where P_1 is "x is positive", P_2 is "x is negative", and P_3 is "$x=0$" because of the equivalence $P \to P_1 \vee P_2 \vee P_3$.

② Exhaustive proof :-

Some theorems can be proved by examining a relatively small number of examples. Such proofs are called Exhaustive proofs, because these proofs proceed by exhausting all possibilities.

It is a special type of proof by cases where each case involves checking a single example.

Example ①: prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Sol: We verify the inequivality $(n+1)^3 \geq 3^n$ when $n = 1, 2, 3, \& 4$.

For $n=1$, we have $(n+1)^3 = 2^3 = 8$ and $3^1 = 3$, so $8 \geq 3$ true.

for $n=2$, $(n+1)^3 = 3^3 = 27$ and $3^2 = 9$, so $27 \geq 9$ true.

For $n=3$, $(n+1)^3 = 4^3 = 64$ and $3^3 = 27$, so $64 \geq 27$ true.

For $n=4$, $(n+1)^3 = 5^3 = 125$ and $3^4 = 81$, so $125 \geq 81$ true.

In each of these four cases, we see that $(n+1)^3 \geq 3^n$.

$\therefore$ The method of exhaustion to prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

③ Existence proof :-

A proof of a proposition of the form $\exists x\, P(x)$ is called an Existence proof. where P is a predicate.

[objects of a perticular type exist.].

There are two types of Existence proof.

ⓐ Constructive Existence proof :-

Sometimes an existence proof of $\exists x\, P(x)$ can be given by finding an element a such that $P(a)$ is true. (or)

Sometimes an existence proof of $\exists x\, P(x)$ can be given by finding an element a, called a witness, such that $P(a)$ is true.

Example ①: prove that there is a positive integer that can be written as the sum of ~~squares~~ cubes of positive integers in two different ways.

Solution:- $1729 = 10^3 + 9^3 = 12^3 + 1^3$

[(or) $50 = 5^2 + 5^2 = 7^2 + 1^2$

(or) $65 = 8^2 + 1^2 = 4^2 + 7^2$] Sum of squares of positive integers in two different ways.

⑥ Non-Constructive existence proof :-

We do not find an element a such that $P(a)$ is true, but rather prove that $\exists x\, P(x)$ is true in Some other way. One common method of giving this method is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction.

Example①:- prove that there exist irrational numbers x and y such that x^y is rational.

Sol: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x & y with x^y rational, namely $x=\sqrt{2}$ and $y=\sqrt{2}$. on the otherhand, if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$

So that $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = (\sqrt{2})^2 = 2$ rational.

This proof is an example of a nonconstructive existence proof. Because we have not found irrational numbers x and y such that x^y is rational. Rather, we have shown that either the pair $x=\sqrt{2}$ and $y=\sqrt{2}$. or the pair $x=\sqrt{2}^{\sqrt{2}}$, $y=\sqrt{2}$ have the desired property, but we donot know which of these two pairs works.

④ Uniqueness proof :-

Some theorems assert that the existence of a Unique element with a perticular property. (or) Some theorems assert that there is exactly one element with this property.

To prove a stmt of this type we need to show that an element with this property exists and that no other element has this property. The two parts of a Uniqueness proof are:

Existence: we show that an element x with the desired property exists.

Uniqueness: We show that if $y \neq x$, then y does not have the desired property.

Equivalently, we can show that if x & y both have the desired property, then $x=y$.

Remark: showing that there is a unique element x such that $P(x)$ is the same as proving the stmt

$$\exists x (P(x) \wedge \forall y (y \neq x \rightarrow \neg P(y))).$$

Example ①: show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar+b=0$.

Sol:

method 1: The real number $r = \frac{-b}{a}$ is a solution of $ar+b=0$ because $a(\frac{-b}{a})+b=0$.

Consequently, a real number r exists for which $ar+b=0$.

This is the existence part of the proof.

method 2: Suppose s is a real number such that $as+b=0$. Then $ar+b = as+b$ where $r = \frac{-b}{a}$.

subtracting b from both sides, so $ar=as$.

Deviding both sides by a, but $a \neq 0$.

We see that $r=s$.

This means that if $s \neq r$, then $as+b \neq 0$

This establishes the uniqueness part of the proof.

---

proof Strategies:-

Finding proofs can be a challenging business. (Task)

When you take a statement to prove, you should first replace the terms by their definitions and then carefully analyze what the hypotheses and conclusion. After doing so, you can attempt to prove the result by using one of the Methods of proof.

Generally, if the stmt is a conditional stmt, you should first try with a direct proof, if this fails, you can try with an indirect proof.

If neither of these approaches works, you might try a proof by Contradiction.

Scanned by CamScanner

① Forward Reasoning :-

In a direct proof of a conditional stmt,

1) Start with the premises.
2) Using these premises, together with axioms and known theorems, you can construct a proof using a sequence of steps that leads to the conclusion.

This type of reasoning called forward reasoning.
It is the most common type of reasoning used to prove relatively simple results.

Similarly, with Indirect proof of reasoning, you can
(1) start with negation of the conclusion
(2) Using sequence of steps and
(3) finally, obtain the negation of the premises.

Forward reasoning is difficult to construct to prove more complicated results, because the reasoning is needed to reach the desired conclusion may be far from obvious. In such cases it may be helpful to use backward reasoning.

Backward Reasoning :-

For proving a stmt q, we try to find a stmt p such that p is true and we can prove $p \to q$.

$x=4, y=6$

Example ①: prove that $\frac{x+y}{2} \geq \sqrt{xy}$ for positive distinct real numbers x and y.

Arithmetic mean

Geometric mean.

Sol:

$$\frac{(x+y)}{2} \geq \sqrt{xy}$$

$$\left(\frac{x+y}{2}\right)^2 \geq xy \quad \text{(square on both sides)}$$

$$\frac{(x+y)^2}{4} \geq xy$$

$$(x+y)^2 \geq 4xy$$

$$(x+y)^2 - 4xy \geq 0$$

$$(x-y)^2 \geq 0$$

Because $(x-y)^2 \geq 0$ when $x \neq y$.

This gives the backwerk reasoning.

Scanned by CamScanner

Adapting Existing proofs:-

Existing proofs can be adapted to prove a new result.
Existing proofs provide clues for new proof.

Example ①: we proved that $\sqrt{2}$ is irrational. We can adapt the proof to show that $\sqrt{3}$ is irrational?

Looking (searching) for Counterexample:-

Use of counterexample to show that certain statements are false.

A stmt of the form $\forall x\, P(x)$ is false, we need only find a counterexample, i.e an example x for which $P(x)$ is false.

Example: ① Every positive integer is the sum of the squares of two integers is false. (3 is not possible)

② "Every positive integer is the sum of the squares of three integers" is false.

Sol: successive +ve integers as a sum of three squares.

we find that $1 = 0^2+0^2+1^2$

$$2^2 = 0^2+1^2+1^2$$
$$3 = 1^2+1^2+1^2$$
$$4 = 0^2+0^2+2^2$$
$$5 = 0^2+1^2+2^2$$
$$6 = 1^2+1^2+2^2$$
$$7 = ?$$

It follows that 7 is a counterexample.

The Role of open problems:- Many advances in Mathematics have been made by people trying to solve famous unsolved problems.

Fermat's Last Theorem:-

The equation $x^n + y^n = z^n$ has no solutions in integers x, y, z with $xyz \neq 0$ whenever n is an integer with $n > 2$.

Validity problem for propositional and predicate Logic:-

A formula (well formed formula (wff)) of the propositional logic is an assertion involving propositional variables by using the connectives $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$ in a proper manner.

Example: $P \wedge q$ is a wff of the propositional logic.

When we assign perticular propositions to p and q, we are giving an interpretation for the formula.

Example: p: I have exam tomorrow and
q: I am going to study

$P \wedge q$: I have exam tomorrow and I am going to study.

Tautology:- A wff of the propositional logic is a tautology if the wff always takes the value true whatever interpretation is given to it. Example: $P \vee \neg P$.

Contradition:- A wff which is always false for all interpretations is called a contradiction.
Example: $P \wedge \neg P$

Contingency:- A wff which is neither a tautology nor a contradiction is called a contingency. Example: $P \rightarrow q$.

The validity problem for the propositional logic is that given a wff of propositional logic, does there exist an interpretation which will make the wff take the value true.
Considering the propositional variables, as Boolean variables, this is called Boolean satisfiability problem.
A problem is decidable that an algorithm to find out if the given wff is a tautology or contingency.
The simplest way ~~to~~ is to draw the truth table for the wff and if for all assignments it takes the value true, it is a Tautology, otherwise it is contingency.

In the first order logic, a predicate has n ~~assignments~~ arguments.
If P is a n-place predicate constant and values $c_1, c_2, \ldots c_n$ are assigned to each of the individual variables, the result is a proposition.

Suppose the domain is U. If the value of $P(c_1, c_2, \ldots, c_n)$ is true for every choice of arguments $c_1, c_2, \ldots, c_n$ selected from U, then P is said to be valid in the domain U. If the values $P(c_1, c_2, \ldots, c_n)$ is true for some (but not for all) choices of arguments selected from U, then P is said to be satisfiable in the domain U, and the values $c_1, c_2, \ldots, c_n$ which make $P(c_1, c_2, \ldots, c_n)$ true are said to satisfy P.
If P is not satisfiable in the domain U, then we say P is unsatisfiable in U.

An expression involving predicate variables and quantifiers and connectives included in the proper manner is called a formula (wff) of the first order logic.
Example: $\forall x P(x) \vee \forall x Q(x)$ is a wff.
When we assign perticular predicates to P and Q it is called an interpretation.
A wff involving predicate variables is valid if it is true for every domain no matter how the predicate variables are interpreted.
A wff is said to be satisfiable if there exist a domain and some interpretation of the predicate variables which makes it true.
If a wff is not true for any domain or interpretation it is unsatisfiable.
Example: $\forall x P(x) \rightarrow \exists x P(x)$ is true for all domains and interpretation and hence a valid wff.
$\exists x P(x) \rightarrow \exists x Q(x)$ may be true for some interpretation but may not be true for some other interpretation.

Let $P(x)$: x is a third semester B.Tech student
$Q(x)$: x has taken a course on Discrete Mathematics.
If Discrete Mathematics is a compulsory course for third semester students, $\exists x P(x) \rightarrow \exists x Q(x)$ will be true.

Suppose $Q(x)$ denotes x is female student

$\exists x\, P(x) \rightarrow \exists x\, Q(x)$ may not be true, if the class has no female candidates.

If a wff is not true for any domain or interpretation, it is said to be unsatisfiable. $\forall x (P(x) \wedge \neg P(x)$ is unsatisfiable.

Given a wff of first order logic, find if it is valid or not. This is called the validity problem of the first order logic.

A

Unit - 6

Fundamentals of Graphs

R. Udhayakumar

Graph

A graph $G = \langle V, E, \Phi \rangle$ consists of a non-empty set V called set of vertices (or nodes or points) of the graph; E is said to be the set of edges of the graph and Φ is mapping from the set E to a set of ordered or unordered pairs of ~~other~~ elements of V. (ie, $\Phi : E \rightarrow V \times V$)

Assume that, the both sets V and E of a graph are finite.

Notation:- $G(V, E, \Phi)$ (or) $G(V, E)$ (or) simply G.
↳ Vertex set ↳ Edge set

Remarks * If an edge $e \in E$ is associated with an ordered pair (u, v) or an unordered pair (u, v) where $u, v \in V$, then e is said to connect or join the nodes u and v.

* The edge e is said to be incident on each of the nodes u & v.

Adjacent Vertices Any pair of nodes which are connected by an edge in a graph is called adjcent nodes.

Directed graph (Digraph)

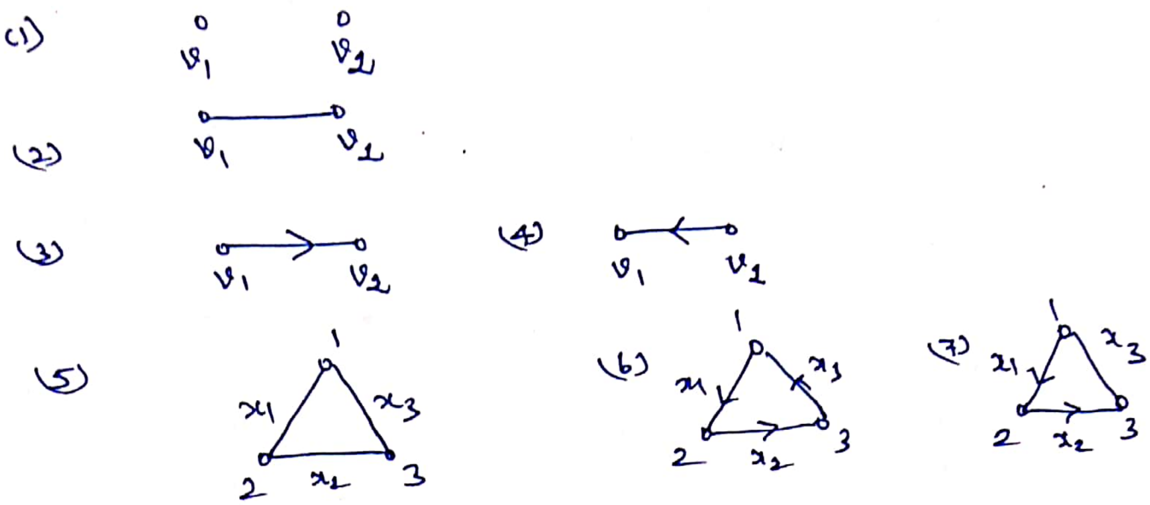
In a graph $G = \langle V, E \rangle$, an edge which is associated with an ordered pair of $V \times V$ is called a directed edge, while an edge which is associated with an unordered pair of nodes is called an undirected edge.

★ A graph in which every edge is directed is called a directed graph or digraph.

★ A graph in which every edge is undirected is called an undirected graph.

★ If some edges are directed and some are undirected in a graph, the graph is called mixed.

Examples



Here Example ① is considered as either directed or undirected graph.

② & ⑤ are undirected graph.

③ , ④ & ⑥ are directed graph

⑦ mixed graph.

Initial and Terminal Nodes

Let $G = \langle V, E \rangle$ be a graph and let $x \in E$ be a directed edge associated with the ordered pair of nodes $\langle u, v \rangle$. Then the edge 'x' is called as initiating or originating in the node 'u' and terminating or ending in the node v.

The nodes 'u' and 'v' are also called the initial and terminal nodes of the edge 'x'.

Incident on a node

An edge $x \in E$ which joins the nodes 'u' & 'v' either it be directed or undirected, is called to be incident to the nodes 'u' and 'v'.

Loop

An edge of a graph which joins a node to itself is called a loop in a graph.

Parallel edges

In a directed as well as undirected graphs, we may have certain pairs of nodes joined by more than one edge, such edges are called parallel edges

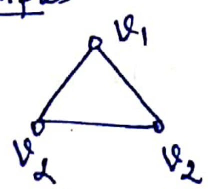
Multigraph

Any graph which contains some parallel edges is called multigraph.

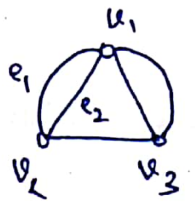
Simple graph

If there is no loops and parallel edges then the graph is called simple graph.

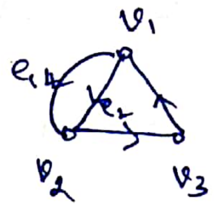
Examples



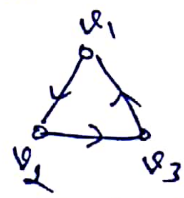
undirected & simple



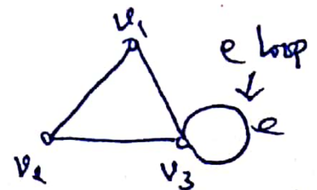
undirected multigraph.



Directed multigraph



directed simple graph

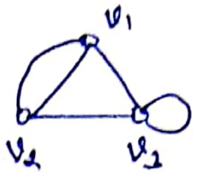


Undirected graph.

Pseudo graph:-

A graph in which loops and parallel edges are allowed is called a pseudo graph.

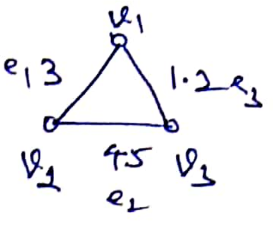
Example:-



Weighted graph

A graph in which a weight (numerical values) are assigned to every edge is called a weighted graph.

eg:

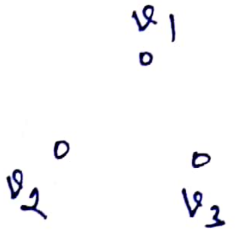


Isolated nodes and Null graph

In a graph a node which is not adjacent to any other node is called an isolated node.

A graph containing only isolated nodes is called a null graph.

Example:.



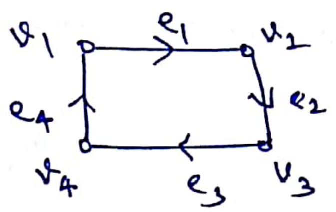
G = Null graph with isolated nodes $\{v_1, v_2, v_3\}$

Graph Isomorphic

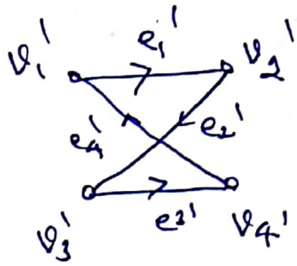
Two graphs are isomorphic if there exists a one to one correspondence between the nodes of the two graphs which preserves adjacency of the nodes as well as directions of the edges, if any.

ie, $G = \langle V_1, E_1, \phi_1 \rangle \cong G_2 = \langle V_2, E_2, \phi_2 \rangle$, If there exists a bijective function $f: V_1 \xrightarrow[\text{onto}]{1-1} V_2$ s.t which preserves the adjacency of the nodes and its direction (if any)

Examples:-

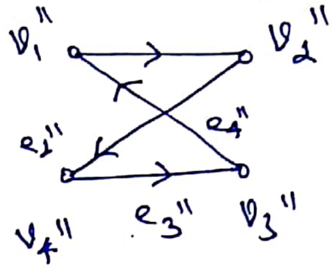


$\cong$



$G_1 \cong G_2$ $\quad \{v_1, v_2, v_3, v_4\} \xrightarrow[\text{onto}]{1-1} \{v_1', v_2', v_4', v_3'\}$

But



G_3

not isomorphic
$G_1 \not\cong G_3$.

Degree of a vertex in undirected graphs

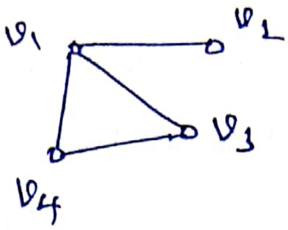
The degree of a vertex in an undirected graph is the number of edges incident with it. (only for simple undirected graph).

Note:- (1) The degree of a vertex 'v' is denoted by '$\deg(v)$'

(2) The degree of the isolated vertex is 'Zero'.

(3) If the $\deg(v) = 1$ is called a pendant vertex.

Example:-



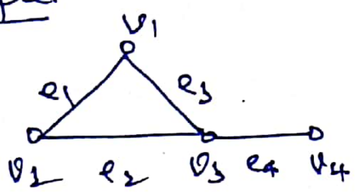
$deg(v_1) = 3$
$deg(v_2) = 1$ (pendant)
$deg(v_3) = 2 = deg(v_4)$.

Subgraph

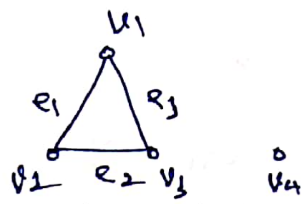
Let $G = \langle V_G, E_G, \Phi_G \rangle$ be a graph. A graph $H = \langle V_H, E_H, \Phi_H \rangle$ is called a subgraph of a graph G, if $V_H \subseteq V_G$ and $E_G \subseteq E_H$ (i.e., every edge of H is also a edge of G).

Note:-
If $V_H = V_G$, then H is called a spanning subgraph of G.
A spanning graph of G need not contain all its edges.

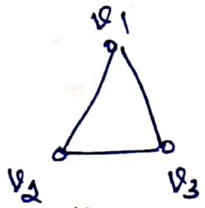
Example:-



G

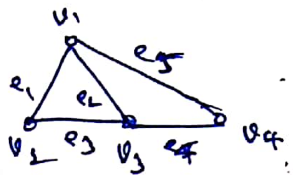


$H_1 = G - \{e_4\}$



H_2

H_1, H_2 are subgraphs
→ spanning
H_3 is not subgraph.



H_3

Some special simple graphs

Complete graph

A simple graph, in which there is exactly one edge between each pair of distinct vertices, is called a complete graph.

The complete graph on 'n' vertices is denoted by K_n.

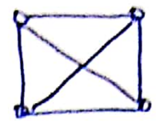
examples

K_1

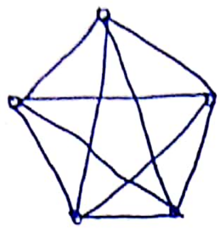
K_2

K_3

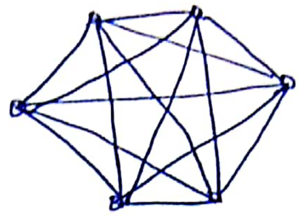
K_4



K_5



K_6



Results

1) The number of edges in K_n is nC_2 or $\frac{n(n-1)}{2}$

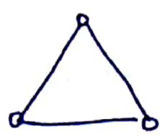
2) The maximum number of edges in a simple graph with 'n' vertices is $\frac{n(n-1)}{2}$.

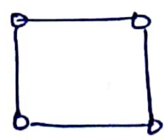
Regular graph

If every vertex of a simple graph has the same degree, then the graph is called a regular graph.

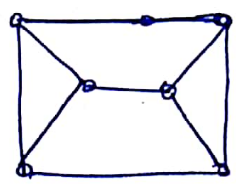
* If every vertex in a regular graph has degree 'n' then the graph is called n-regular.

Example:-

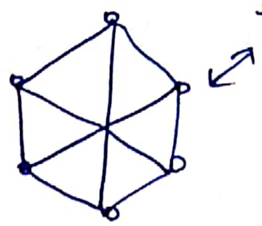




2-regular graph



3-regular graph.



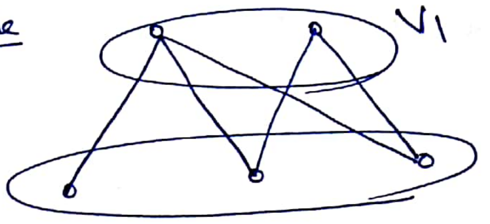
Result:- 1) Every complete graph is a regular graph.

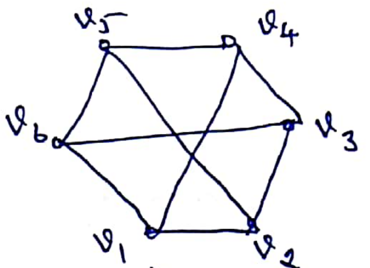
2) Every regular graph need not be a complete graph.

Bipartite graph

* If the vertex set V of a simple graph $G=(V,E)$ can be partitioned into two subsets V_1 and V_2 such that every edge of G connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or V_2), then G is called a bipartite graph.

* Example





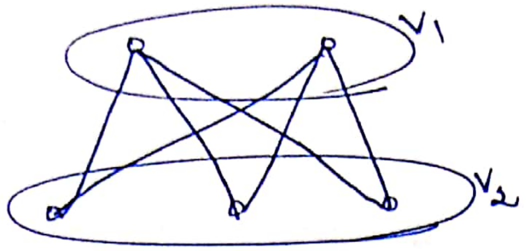
$V_1 = \{v_1, v_3, v_5\}$

$V_2 = \{v_2, v_4, v_5\}$

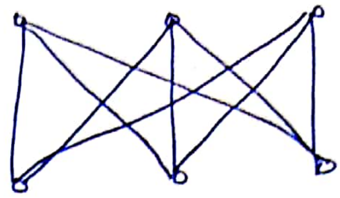
complete bipartite graph

If each vertex set V_1 is connected with every vertex of V_2 by an edge then G is called a complete bipartite graph. If V_1 have m vertices and V_2 have n vertices then the complete bipartite graph is denoted by $K_{m,n}$.

Example:-



$K_{2,3}$



$K_{3,3}$

Theorem (Fundamental theorem of Graph theory)

(The Handshaking theorem)

In any graph the sum of degrees of its vertices is equal to twice the number of edges.

i.e., $\sum_{i=1}^{n} d(v_i) = 2e$

Proof:-

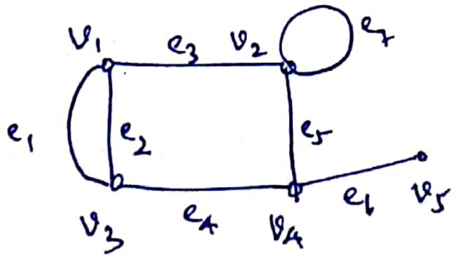
Let us consider a graph G with e edges and n vertices.

$v_1, v_2, \ldots, v_n$ are its vertices.

Since each edge contributes two degrees, the sum of the degrees of all vertices in G is twice the number of edges in G.

i.e., $\sum_i d(v_i) = 2e$.

Example: Verify the theorem



$d(v_1) = 3$ $\quad d(v_4) = 3$

$d(v_2) = 4$ $\quad d(v_5) = 1$

$d(v_3) = 3$

$\therefore \sum d(v_i) = 14$

$2e = 2 \times 7 = 14$ //.

Theorem The number of vertices of odd degree in an undirected graph is even. (or)

The number of odd vertices is always even.

Proof:- Let $G = \langle V, E \rangle$ be the undirected graph.

Let V_1 and V_2 be the sets of vertices of G of even and odd degrees respectively.

Then by previous theorem

$$2e = \sum_{v_i \in V_1} \deg(v_i) + \sum_{v_j \in V_2} \deg(v_j)$$

(even) (even)

$$\therefore \sum_{v_j \in V_2} \deg(v_j) = 2e - \sum_{v_i \in V_1} \deg(v_i)$$

$$= \text{even}$$

Since each $\deg(v_j)$ is odd, the number of terms contained in $\sum_{v_j \in V_2} \deg(v_j)$ is even.

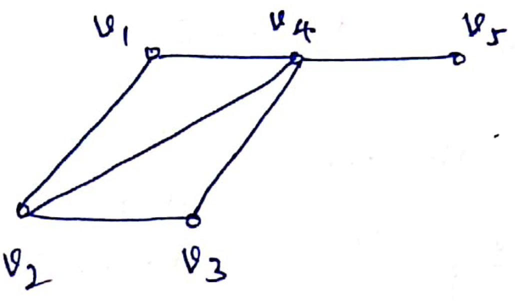
Example:-

(1)

$d(v_1) = 1$ $d(v_2) = 1$.

$\therefore$ The no. of odd vertices is even.

(2)



$d(v_1) = 2$ $d(v_2) = 3$

$d(v_3) = 2$ $d(v_4) = 4$

and $d(v_5) = 1$.

$\therefore$ even (v_2, v_5).

Matrix Representation of Graphs

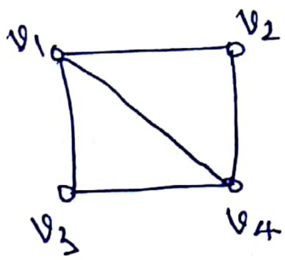
Adjacency matrix

When G is a simple graph with n vertices $v_1, v_2, \ldots, v_n$ the matrix A or $(A_G) \equiv [a_{ij}]$,

where $a_{ij} = \begin{cases} 1 & \text{if } (v_i, v_j) \text{ is an edge of } G \\ 0 & \text{otherwise} \end{cases}$

is called the adjacency matrix of G.

Example :



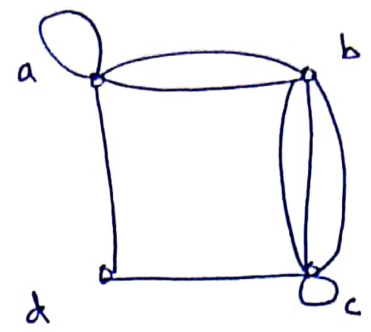
$$A = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

Remarks ① Since a simple graph has no loops, each diagonal entry of A viz $a_{ii} = 0$, for $i = 1, 2, \ldots n$.

② The adjacency matrix of simple graph is symmetric.

③ $\deg(v_i)$ is equal to the number of 1's in the i^{th} row or i^{th} column.

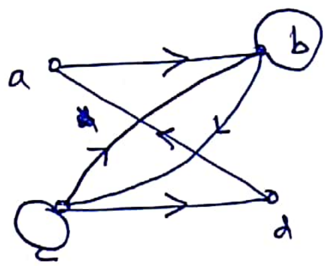
Pseudograph



$$A = \begin{array}{c|cccc} & a & b & c & d \\ \hline a & 1 & 2 & 0 & 1 \\ b & 2 & 0 & 3 & 0 \\ c & 0 & 3 & 1 & 1 \\ d & 1 & 0 & 1 & 0 \end{array}$$

Directed graph

$$A = \begin{array}{c|cccc} & a & b & c & d \\ \hline a & 0 & 1 & 0 & 0 \\ b & 0 & 1 & 1 & 0 \\ c & 0 & 1 & 1 & 1 \\ d & 1 & 0 & 0 & 0 \end{array}$$



out going vertices

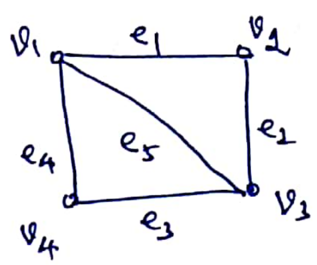
Definition **Incidence matrix**

If $G = (V, E)$ is an undirected graph with n vertices and m edges $e_1, e_2, \ldots e_m$, then the $(n \times m)$ matrix

$$B = [b_{ij}] \quad \text{where} \quad b_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ is incident on } v_i \\ 0 & \text{otherwise} \end{cases}$$

is called incidence matrix.

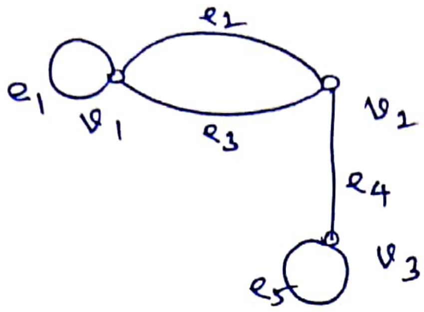
Ex:-



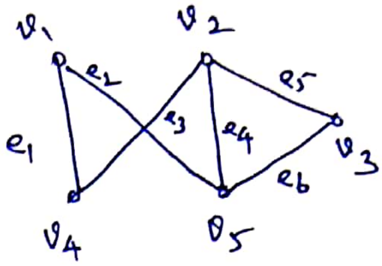
$$\begin{array}{c|ccccc} & e_1 & e_2 & e_3 & e_4 & e_5 \\ \hline v_1 & 1 & 0 & 0 & 1 & 1 \\ v_2 & 1 & 1 & 0 & 0 & 0 \\ v_3 & 0 & 1 & 1 & 0 & 1 \\ v_4 & 0 & 0 & 1 & 1 & 0 \end{array}$$

1. Write the incidence matrix of the graph

(i)

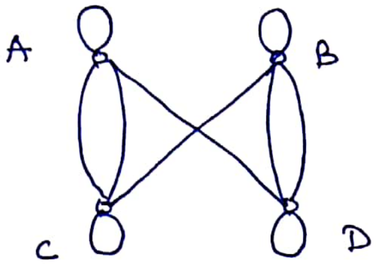


(ii)

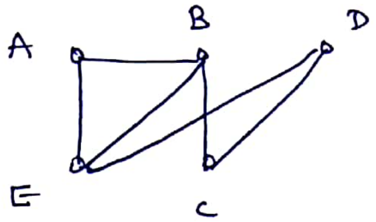


2. Write adjacency matrix

(i)



(ii)



3. Draw the graphs represented by the following adjacency matrices

(i) $\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

(ii) $\begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

(iii) $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

4. Draw the graphs represented by the following incidence matrix

(i)

$$\begin{array}{c c} & \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{array}{c} A \\ B \\ C \\ D \end{array} & \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

(ii)

$$\begin{array}{c c} & \begin{array}{ccccc} e_1 & e_2 & e_3 & e_4 & e_5 \end{array} \\ \begin{array}{c} A \\ B \\ C \\ D \end{array} & \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}$$