UNIT I – LOGIC AND PROOFS

==

Mathematical Logic is the science of reasoning used to represent the statements to communicate the facts. It provides rules by which one can determine whether any particular argument is valid or not.

A proposition is defined as **statement**, that is either true or false but not both. It is used to describe any Mathematical structure. Consider the following examples:

i. Delhi is the capital of India

ii. $0 > 1$

iii. The problem is simple

Here i. and ii. are true and false respectively. Hence they are called as proposition or statement. But iii. is neither true nor false. Hence it is not a statement.

There are two types of statements:

i. Simple Statement or atomic statement   ii. Compound statement or molecular statement

A statement which cannot be divided into further meaningful simple statements is called atomic statement. **Example:** i. 5 is a prime number   ii. Raja is a boy

A statement which consists of more than one atomic statements is called a compound statement. They are formed by combining atomic statements by the use of connectives like and, or, etc.

Example: Raja is a boy and he is studying B.E.

Truth value of a proposition:

English alphabets are used to represent simple statements and are called propositional variables. If a proposition is true then its truth value is T and if a proposition is false, its truth value is F, which are called propositional constants.

Connectives: The words by which atomic statements are combined to form a compound statements, with the help of 'or', 'and', 'not', 'if' are called connectives. We will discuss some of the connectives:

TRUTH TABLE

It is a way of summarizing the truth values of logical statements and indicates the truth values of compound propositions. The number of columns depends on the propositional variables and connectives used and number of rows depends on simple propositions. For n simple propositions the number of rows will be 2^n.

LOGICAL OPERATIONS

Negation: ($\sim$ or $\neg$) The negation of a statement P is written as $\neg P$ or $\sim P$ and read as 'not P'. The truth table for negation is given here.

P	$\neg P$ or $\sim P$
T	F
F	T

Example: Let P : Ram is a rich man

Then $\sim P$: Ram is not a rich man / Ram is a poor man / It is not the case Ram is rich man

Note: Negation is a unary operator

Conjunction: (AND $\wedge$) The conjunction of two statements P and Q is written as '$P \wedge Q$' and is read as 'P and Q'. It has truth value True only when both P and Q are True. Otherwise False. The truth table for conjunction is given here.

https://doi.org/10.5281/zenodo.15287507

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

Example: Let P: It is hot. Q: It is sunny

Then $P \wedge Q$: It is hot and it is sunny.

Note: Negation is a binary operator and it is symmetric.

To form $P \wedge Q$ the statements P and Q need not be related

Disjunction: (OR $\vee$) The disjunction of two statements P and Q is written as '$P \vee Q$' and is read as 'P or Q'. It has truth value False only when both P and Q are False. Otherwise True. The truth table for disjunction is given here.

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

Example: Let P: I will go to college. Q: I will go to cinema.

Then $P \vee Q$: I will go to college or cinema.

Note: Disjunction is a binary operator and it is symmetric.

Implication or Conditional Statement: ($\rightarrow$) Let P and Q be any two statements. Then '$P \rightarrow Q$' is read as 'if P then Q'. It has truth value False only when P is True and Q is False. Otherwise True. The truth table for the conditional statement is given here.

P	Q	$\mathrm{P} \rightarrow Q$
T	F	F
F	T	T
F	F	T
T	T	T

Example: Let P: There is a flood. Q: The crop will be destroyed.

Then $P \rightarrow Q$: If there is a flood, then the crop will be destroyed.

Note: $\rightarrow$is a binary operator and it is not symmetric

Equivalence of Biconditional Statement: ($\leftrightarrow$) Let P and Q be any two statements. Then '$P \leftrightarrow Q$' is read as 'P if and only if Q'. It has truth value True if both P and Q are identical. Otherwise False. The truth table for the biconditional statement is given here.

P	Q	$\mathrm{P} \leftrightarrow Q$
T	F	F
F	T	F
F	F	T
T	T	T

Example: Let P: x is even number. Q: x is divisible by 2.

Then $P \leftrightarrow Q$: x is even number iff x is divisible be 2.

Note: $\leftrightarrow$is a binary operator and it is symmetric.

Symbolic form of compound propositions

Example: Let P : He is rich, Q: He is happy.

Write the following in symbolic form.

He is neither rich nor happy.

Solution: $\neg P \wedge \neg Q$

Example: Let P be "Roses are red" and Q be "Violets are blue." Let S be the statement:

"It is not true that roses are red and violets are blue." Write S in symbolic form.The symbolic form is

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

Example: Let P : It is hot, Q : It is sunny.

Write the following in symbolic form.

It is not hot but it is sunny.

Solution: $\neg P \wedge Q$

Example: Let P : You will get a good job,

Q : You study Mathematics well.

Write the following in symbolic form.

You will get a good job if and only if you study Mathematics well.

Solution: $P \leftrightarrow Q$

Logical Equivalence:

Definition: Any two simple propositions P and Q are said to be logically equivalent iff they have the same truth values. It is denoted as $P \equiv Q$.

Example: P : 2 is even number Q: $3^2 + 4^2 = 5^2$. Then P and Q are equivalent, since both are true.

Definition: Any two compound propositions P and Q are said to be logically equivalent iff their truth values identical for each combination of the truth values of its components. It is denoted as $P \equiv Q$.

Example: P : $R \to S$ Q: $\neg S \to \neg R$. Then P and Q are equivalent. This can be verified by the truth table.

Statement Formula: A definite compound statements represented by variables like P, Q, R, ……. is called statement formula. Example: $P \wedge \neg P$, $(P \vee \neg Q)$.

Example: Express the statement "Good food is not safety" in symbolic form

Let P : Good food is cheap. Then $S \equiv \neg P$: Good food is not cheap.

Example : If P : Raja is poor and Q: Raja is happy, write the following statements in symbolic form.

i. Raja is rich but happy

ii. Raja is neither poor nor happy

iii. Raja is rich or he is both poor and unhappy

Solution: i. $\neg P \wedge Q$ ii. $\neg P \wedge \neg Q$ iii. $\neg P \vee (P \wedge \neg Q)$

Example : Write the negation of the following:

i. Mathematics is interesting and Logic is not easy

ii. If students do well in the examinations then they will not fail

i. Let P : Mathematics is interesting. Q: Logic is easy

Therefore given proposition is $P \wedge \neg Q$.

The negation is $\neg(P \wedge \neg Q) \equiv \neg P \vee Q$ i.e. Mathematics is not interesting or Logic is easy.

ii. Let P : Students do well in the examinations. Q: They will fail

Therefore given proposition is $P \to \neg Q$.

The negation is $\neg(P \to \neg Q) \equiv \neg(\neg P \vee \neg Q) \equiv P \wedge Q$ i.e. Students do well in the examinations and they will fail.

Example : Let P: It is hot and Q: It is humid. Give the verbal sentences for the following symbolic form: i. $\neg P$ ii. $P \wedge Q$ iii. $P \wedge \neg Q$ iv. $\neg(\neg Q)$

Solution:

i. It is not hot

ii. It is hot and humid

iii. It is hot and it is not humid

iv. It is humid

https://doi.org/10.5281/zenodo.15287507

Inverse, converse and contra positive of a statement

For any implication statement $P \to Q$, (Q whenever P)

i. $Q \to P$ is called converse

ii. $\neg P \to \neg Q$ is called inverse

iii. $\neg Q \to \neg P$ is called contra positive

Note:

1. $P \to Q \neq Q \to P$
2. $P \to Q \neq \neg P \to \neg Q$
3. $P \to Q \neq \neg Q \to \neg P$

Example: What are the contrapositive , converse and inverse of the conditional statement .
" If it is raining, then I get wet".

Let P : It is raining and Q : I get wet.

Contrapositive : $\neg Q \to \neg P$ If I don't get wet, then it is not raining

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

Inverse : $\neg P \to \neg Q$ If it is not raining, then I don't get wet

Example: What are the contrapositive , converse and inverse of the conditional statement .
"The Indian cricket team wins whenever it plays first batting".

Rewriting the statement as "If India plays first batting, then Indian cricket team wins"

Let P : India plays first batting and Q : Indian cricket team wins.

Contrapositive $\neg Q \to \neg P$: If Indian cricket team do not win, then it is not playing first batting

Converse $Q \to P$: If Indian cricket team wins, then it plays first batting

Inverse $\neg P \to \neg Q$: If India is not playing first batting, then Indian team don't win

Example: What are the contrapositive , converse and inverse of the conditional statement .

"If you are guilty, then you are punished"

Let P : You are guilty and Q : You are punished.

Contrapositive $\neg Q \to \neg P$: If you are not punished, then you are not guilty

Converse $Q \to P$: If you are punished, then you are guilty

Inverse $\neg P \to \neg Q$: If you are not guilty, then you are not punished

We can form the truth table for inverse, converse and contra positive as shown below:

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

Do you know? How many rows are needed for the truth table of the formula $(P \wedge \neg Q) \leftrightarrow [(\neg R \wedge S) \to T]$?

Construction of the truth table:

1. Construct the truth table for $(P \to Q) \to (P \wedge Q)$.

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

2. Construct the truth table for $(P \to Q) \vee (\neg P \wedge Q)$.

P	Q	$(P \to Q)$	$\neg P$	$(\neg P \wedge Q)$	$(P \to Q) \vee (\neg P \wedge Q)$
T	T	T	F	F	T
T	F	F	F	F	F
F	T	T	T	T	T
F	F	T	T	F	T

A statement formula which is true regardless of the truth values of the statements which replaces the variables in it is called a universally valid formula or a **Tautology**. Example: $P \vee \neg P$. A formula is a tautology if each entry in the final column of the truth table is T.

A statement formula which is false regardless of the truth values of the statements which replaces the variables in it is called a **contradiction.** Example: $P \wedge \neg P$. A formula is a contradiction if each entry in the final column of the truth table is F.

A statement formula which is neither a tautology or a contradiction is called a contingency.

Example: Prove that $(P \wedge Q) \wedge \neg (P \vee Q)$ is a contradiction.

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

Example: Using truth table prove that $(P \wedge Q) \vee (P \to R) \vee (\neg Q \to \neg R)$ is a tautology.

P	Q	R	$P \wedge Q$ 1	$P \to$R 2	$(1) \vee (2)$ 3	$\neg Q$	$\neg R$	$\neg Q \to \neg R$ 4	$(3) \vee (4)$
T	T	T	T	T	T	F	F	T	T
T	T	F	T	F	T	F	T	T	T
T	F	T	F	T	T	T	F	F	T
T	F	F	F	F	F	T	T	T	T
F	T	T	F	T	T	F	F	T	T
F	T	F	F	T	T	F	T	T	T
F	F	T	F	T	T	T	F	F	T
F	F	F	F	T	T	T	T	T	T

https://doi.org/10.5281/zenodo.15287507

Example: Obtain the truth table for the statement $(\neg P \to R)\wedge(Q\to P)\wedge(Q\to P)$ and comment on the statement.

P	Q	R	$\neg P$	$\neg P \to \mathrm{R}$ (1)	$Q\to P$ (2)	$(1)\wedge(2)$ (3)	$(3)\wedge(2)$
T	T	T	F	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	T	T	T	T
F	F	F	T	F	T	F	F

Above table implies that $(Q\to P)$, $(\neg P\to R)\wedge(Q\to P)$ are having equivalent truth values

Equivalence Formulas

Let A and B be two statement formulas. If the truth value of A is equal to truth value of B, then A and B are said to be **equivalent** and is denoted by $A\Leftrightarrow B$.

Example: $\neg\neg P\Leftrightarrow P$, $P\vee P\Leftrightarrow P$

Note: $\Leftrightarrow$ is not connective. If $A\Leftrightarrow B$, then $A\leftrightarrow B$ is a tautology.

Definition: A formula A is said to tautologically imply a formula B if and only if $A\to B$ is a tautology. In this case, we write $A\Leftrightarrow B$.

Example: Show that $(P\to Q)\Rightarrow(\neg Q\to\neg P)$ by using truth table.

P	Q	$(P\to Q)$	$\neg Q$	$\neg P$	$(\neg Q\to\neg P)$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Here the columns of $(P\to Q)$ and $(\neg Q\to\neg P)$ are identical.

Hence $(P\to Q)\to(\neg Q\to\neg P)$ is a tautology.

Hence we can write $(P\to Q)\Rightarrow(\neg Q\to\neg P)$.

Example: Show that $(P\vee Q)\Leftrightarrow\neg(\neg Q\wedge\neg P)$ by using truth table.

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

Here the columns of $(P\vee Q)$ and $\neg(\neg Q\wedge\neg P)$ are identical.

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

Hence we can write $(P\vee Q)\Leftrightarrow\neg(\neg Q\wedge\neg P)$.

Note: Now $(P \vee Q)$ and $\neg(\neg Q \wedge \neg P)$ are said to be equivalent.

Some Useful Equivalent Formulas:

$P \vee P \Leftrightarrow P$	and	$P \wedge P \Leftrightarrow P$	Idempotent Law
$P \vee F \Leftrightarrow P$	and	$P \wedge T \Leftrightarrow P$	Identity Law
$P \vee T \Leftrightarrow T$	and	$P \wedge F \Leftrightarrow F$	Domination Law
$P \vee \neg P \Leftrightarrow T$	and	$P \wedge \neg P \Leftrightarrow F$	Negation Law
$P \vee (P \wedge Q) \Leftrightarrow P$	and	$P \wedge (P \vee Q) \Leftrightarrow P$	Absorption Law
$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	and	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	Demorgan's Law
$(P \vee Q) \Leftrightarrow (Q \vee P)$	and	$(P \wedge Q) \Leftrightarrow (Q \wedge P)$	Commutative Law
$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	and	$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	Associative Law
$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	and	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	Distributive Law
$P \rightarrow Q \Leftrightarrow \neg P \vee Q$	and	$P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$	

$(A \vee B) \wedge (C \vee D) \Leftrightarrow (A \wedge C) \vee (A \wedge D) \vee (B \wedge C) \vee (B \wedge D)$	Extended Distributive Law
$(A \wedge B) \vee (C \wedge D) \Leftrightarrow (A \vee C) \wedge (A \vee D) \wedge (B \vee C) \wedge (B \vee D)$	Extended Distributive Law

Solved Problems on Simplification using Equivalences

Example: Is $[\neg P \wedge (P \vee Q)] \rightarrow Q$ a tautology.

$$
\begin{aligned}
[\neg P \wedge (P \vee Q)] \rightarrow Q &\Leftrightarrow (\neg P \wedge P) \vee (\neg P \wedge Q) \rightarrow Q \\
&\Leftrightarrow F \vee (\neg P \wedge Q) \rightarrow Q \\
&\Leftrightarrow (\neg P \wedge Q) \rightarrow Q \\
&\Leftrightarrow \neg(\neg P \wedge Q) \vee Q \\
&\Leftrightarrow (P \vee \neg Q) \vee Q \\
&\Leftrightarrow P \vee (\neg Q \vee Q) \\
&\Leftrightarrow P \vee T \\
&\Leftrightarrow T
\end{aligned}
$$

Example: Show that $[Q \vee (P \wedge \neg Q)] \vee (\neg P \wedge \neg Q)$ is a tautology.

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

$$\Leftrightarrow \left[(Q \vee P) \wedge T\right] \vee \neg(P \vee Q)$$

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

$$\Leftrightarrow \ T$$

Example: Show that $\left[(P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))\right] \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ is a tautology by using equivalences.

$$\left[(P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))\right] \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$$

$$\Leftrightarrow \left[(P \vee Q) \wedge \neg(\neg P \wedge \neg(Q \wedge R))\right] \vee \neg(P \vee Q) \vee \neg(P \vee R)$$

$$\Leftrightarrow \left[(P \vee Q) \wedge (P \vee (Q \wedge R))\right] \vee \neg\left[(P \vee Q) \wedge (P \vee R)\right]$$

$$\Leftrightarrow \left[(P \vee Q) \wedge (P \vee Q) \wedge (P \vee R)\right] \vee \neg\left[(P \vee Q) \wedge (P \vee R)\right]$$

$$\Leftrightarrow \left[(P \vee Q) \wedge (P \vee R)\right] \vee \neg\left[(P \vee Q) \wedge (P \vee R)\right]$$

$$\Leftrightarrow \ T$$

Example: Show that $(P \vee Q) \wedge \neg(\neg P \wedge Q) \Leftrightarrow P$ without using truth table.

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

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

$$\Leftrightarrow \ P \vee F$$

$$\Leftrightarrow \ P$$

Example: Show that $\neg(P \leftrightarrow Q)$ and $(P \vee Q) \wedge \neg(P \wedge Q)$ are equivalent.

$$\neg(P \leftrightarrow Q) \ \Leftrightarrow \neg\left[(P \rightarrow Q) \wedge (Q \rightarrow P)\right]$$

$$\Leftrightarrow \ \neg\left[(\neg P \vee Q) \wedge (\neg Q \vee P)\right]$$

$$\Leftrightarrow \ \left[\neg(\neg P \vee Q) \vee \neg(\neg Q \vee P)\right]$$

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

$$\Leftrightarrow \ \left[(P \wedge \neg Q) \vee Q\right] \wedge \left[(P \wedge \neg Q) \vee \neg P\right]$$

$$\Leftrightarrow \left[(P \vee Q) \wedge (\neg Q \vee Q)\right] \wedge \left[(P \vee \neg P) \wedge (\neg Q \vee \neg P)\right]$$

$$\Leftrightarrow \left[(P \vee Q) \wedge (\neg Q \vee Q)\right] \wedge \left[(P \vee \neg P) \wedge (\neg Q \vee \neg P)\right]$$

$$\Leftrightarrow \left[(P \vee Q) \wedge T\right] \wedge \left[T \wedge \neg(Q \wedge P)\right]$$

$$\Leftrightarrow \left[(P \vee Q)\right] \wedge \left[\neg(Q \wedge P)\right]$$

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

Example: Show that $(P \rightarrow Q) \wedge (R \rightarrow Q)$ and $(P \vee R) \rightarrow Q$ are equivalent.

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

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

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

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

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

Example: Prove without using truth table $\neg (P \leftrightarrow Q) \equiv (P \vee Q) \wedge \neg (P \wedge Q) \equiv (Q \wedge \neg P) \vee (P \wedge \neg Q)$.

In the previous example, we have proved that $\neg (P \leftrightarrow Q) \equiv (P \vee Q) \wedge \neg (P \wedge Q)$

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

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

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

$$\Leftrightarrow [F \vee (Q \wedge \neg P)] \vee [(P \wedge \neg Q) \vee F]$$

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

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

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

Example: Without using the truth table, prove that $\neg P \to (Q \to R) \equiv Q \to (P \vee R)$

$$\neg P \to (Q \to R) \Leftrightarrow P \vee (Q \to R)$$

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

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

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

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

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

Example: Show that $P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to R \Leftrightarrow P \to (\neg Q \vee R)$

$$P \to (Q \to R) \Leftrightarrow P \to (\neg Q \vee R) \text{.........(1)}$$

$$P \to (Q \to R) \Leftrightarrow \neg P \vee (Q \to R)$$

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

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

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

$$\Leftrightarrow (P \wedge Q) \to R \text{............(2)}$$

https://doi.org/10.5281/zenodo.15287507

From (1) and (2) $P\to(Q\to R)\Leftrightarrow(P\wedge Q)\to R\Leftrightarrow P\to(\neg Q\vee R)$

Example: Prove that $(P\to Q)\wedge(R\to Q)\Rightarrow(P\vee R)\to Q$

$$
\begin{aligned}
(P\to Q)\wedge(R\to Q) &\Leftrightarrow (\neg P\vee Q)\wedge(\neg R\vee Q)\\
&\Leftrightarrow (\neg P\wedge\neg R)\vee Q\\
&\Leftrightarrow \neg(P\vee R)\vee Q\\
&\Leftrightarrow (P\vee R)\to Q
\end{aligned}
$$

Example: Show that $(\neg P\wedge(\neg Q\wedge R))\vee(Q\wedge R)\vee(P\wedge R)\Leftrightarrow R$ without using truth table.

$$
\begin{aligned}
(\neg P\wedge(\neg Q\wedge R))\vee(Q\wedge R)\vee(P\wedge R) &\Leftrightarrow ((\neg P\wedge\neg Q)\wedge R)\vee(Q\vee P)\wedge R\\
&\Leftrightarrow (\neg(P\vee Q)\wedge R)\vee(P\vee Q)\wedge R\\
&\Leftrightarrow [\neg(P\vee Q)\vee(P\vee Q)]\wedge R\\
&\Leftrightarrow T\wedge R\\
&\Leftrightarrow R
\end{aligned}
$$

Functionally Set of Connectives

We introduce a new connective NAND $\uparrow$ (combination of NOT and AND) defined by $P\uparrow Q=\neg(P\wedge Q)$ and another connective NOR $\downarrow$ (combination of NOT and OR) defined by $P\downarrow Q=\neg(P\vee Q)$.
Thus the connectives $\uparrow$ and $\downarrow$ are defined in terms of $\wedge$, $\vee$ and $\neg$.

A set of connectives is said to be functionally complete if every formula can be expressed in terms of an equivalent formula containing the connectives only from this set.

Example: $\{\wedge,\neg\}$, $\{\uparrow\}$, $\{\downarrow\}$ and $\{\vee,\neg\}$ are functionally complete.

Duality Law: Two formulas A and A^* are said to be duals of each other if either one can be obtained from the other by replacing $\wedge$ by $\vee$, $\vee$ by $\wedge$, F by T, T by F.

Example: The dual of $(P\wedge\neg R)\vee T$ is $(P\vee\neg R)\wedge F$.

Note: If $A\Leftrightarrow B$ then $A^*\Leftrightarrow B^*$

Principal Disjunctive and Principal Conjunctive Normal Forms

Given a number of variables, the conjunction in which each variable or its negation, but not both, occurs only once are called minterms. For variables P, Q the minterms are $P\wedge Q,\neg P\wedge Q,\ P\wedge\neg Q,\neg P\wedge\neg Q$.

Given a number of variables, the disjunction in which each variable or its negation, but not both, occurs only once are called maxterms. For variables P, Q the maxterms are $P\vee Q,\neg P\vee Q,\ P\vee\neg Q,\neg P\vee\neg Q$.

A formula consisting disjunction of min terms and equivalent to a given formula is known as PDNF.

A formula consisting conjunction of max terms and equivalent to a given formula is known as PCNF.

Note:
To get min terms in the disjunction, the missing factors are introduced through the complement law $P \vee \neg P \equiv T$ and then apply distributive law.

To obtain PCNF of A, apply De Morgan's laws to the PDNF of $\neg A$.

$PCNF\ of\ S \equiv \neg(PDNF\ of\ \neg S)$ and $PDNF\ of\ S \equiv \neg(PCNF\ of\ \neg S)$

To obtain the PDNF of the statement S, write the disjunction of minterms corresponding to the truth value T and to find the PDNF of the statement $\neg S$, write the disjunction of minterms corresponding to the truth value F.

Example: Find the PDNF and PCNF of $(\neg P \vee \neg Q) \to (P \leftrightarrow \neg Q)$ using truth table.

Let $S \equiv (\neg P \vee \neg Q) \to (P \leftrightarrow \neg Q)$

P	Q	$\neg \mathrm{P}$	$\neg Q$	$\neg P \vee \neg Q$	$P \leftrightarrow \neg Q$	$(\neg P \vee \neg Q) \to (P \leftrightarrow \neg Q)$
T	T	F	F	F	F	T
T	F	F	T	T	T	T
F	T	T	F	T	T	T
F	F	T	T	T	F	F

PDNF of S is $(P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$

PDNF of $\neg S$ is $(\neg P \wedge \neg Q)$

PCNF of S is $\neg(PDNF\ of\ \neg S)$

PCNF of S is $\neg(\neg P \wedge \neg Q) \equiv (P \vee Q)$

Example: Obtain PCNF & PDNF of $(P \to (Q \wedge R)) \wedge (\neg P \to (\neg Q \wedge \neg R))$

Let $S \equiv (P \to (Q \wedge R)) \wedge (\neg P \to (\neg Q \wedge \neg R))$

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

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

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

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

PDNF of S is $(\neg P \wedge \neg Q \wedge \neg R) \vee (Q \wedge R \wedge P)$

PDNF of $\neg S$ is $(\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R)$

PCNF of S is $\neg(PDNF\ of\ \neg S)$

PCNF of S is $\neg[(\neg P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R)]$

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

Example: Obtain PDNF of $(P\wedge Q)\vee R\rightarrow\neg P$ & hence find its PCNF.

$$(P\wedge Q)\vee R\rightarrow\neg P \Leftrightarrow \neg\left[(P\wedge Q)\vee R\right]\vee\neg P$$

$$\Leftrightarrow \left[(\neg P\vee\neg Q)\wedge\neg R\right]\vee\neg P$$

$$\Leftrightarrow \left[(\neg P\vee\neg Q)\vee\neg P\right]\wedge(\neg R\vee\neg P)$$

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

$$\Leftrightarrow \left[(\neg P\vee\neg Q)\vee F\right]\wedge\left[(\neg R\vee\neg P)\vee F\right]$$

$$\Leftrightarrow \left[(\neg P\vee\neg Q)\vee(R\wedge\neg R)\right]\wedge\left[(\neg R\vee\neg P)\vee(Q\wedge\neg Q)\right]$$

$$\Leftrightarrow \left[(\neg P\vee\neg Q\vee R)\wedge(\neg P\vee\neg Q\vee\neg R)\right]\wedge\left[(\neg R\vee\neg P\vee Q)\wedge(\neg R\vee\neg P\vee\neg Q)\right]$$

$$\Leftrightarrow \left[(\neg P\vee\neg Q\vee R)\wedge(\neg P\vee\neg Q\vee\neg R)\right]\wedge\left[(\neg R\vee\neg P\vee Q)\wedge(\neg R\vee\neg P\vee\neg Q)\right]$$

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

PCNF of S is $(\neg P\vee\neg Q\vee R)\wedge(\neg P\vee\neg Q\vee\neg R)\wedge(\neg P\vee Q\vee\neg R)$

PCNF of $\neg S$ is $(P\vee\neg Q\vee\neg R)\wedge(P\vee Q\vee R)\wedge(\neg P\vee Q\vee R)\wedge(P\vee\neg Q\vee R)\wedge(P\vee Q\vee\neg R)$

PDNF of S is $\neg(PCNF\ of\ \neg S)$

PDNF of S is $\neg\left[(P\vee\neg Q\vee\neg R)\wedge(P\vee Q\vee R)\wedge(\neg P\vee Q\vee R)\wedge(P\vee\neg Q\vee R)\wedge(P\vee Q\vee\neg R)\right]$

$$\left[(\neg P\wedge Q\wedge R)\vee(\neg P\wedge\neg Q\wedge\neg R)\vee(P\wedge\neg Q\wedge\neg R)\vee(\neg P\wedge Q\wedge\neg R)\vee(\neg P\wedge\neg Q\wedge R)\right]$$

Example: Obtain the PDNF and PCNF of $(P\rightarrow Q)\wedge(Q\rightarrow P)$.

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

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

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

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

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

Therefore PDNF of S is $(\neg P\wedge\neg Q)\vee(Q\wedge P)$

Therefore PDNF of $\neg$S is $(\neg P\wedge Q)\vee(P\wedge\neg Q)$

Therefore PCNF of S is $\neg$(PDNF of $\neg$S) i.e. $\neg\left[(\neg P\wedge Q)\vee(P\wedge\neg Q)\right]$ *i.e.* $(P\vee\neg Q)\wedge(\neg P\vee Q)$

Another method using truth table:

P	Q	$P\rightarrow Q$	$Q\rightarrow P$	$(P\rightarrow Q)\wedge(Q\rightarrow P)$	Minterms

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

The rows 1 and 4 has the truth value T and the corresponding minterms are $(P \wedge Q)$ and $(\neg P \wedge \neg Q)$

Therefore PDNF of S is $(\neg P \wedge \neg Q) \vee (Q \wedge P)$ and hence PCNF of S is $(P \vee \neg Q) \wedge (\neg P \vee Q)$

Example: Obtain the PCNF of $(\neg P \rightarrow R) \wedge (Q \leftrightarrow P)$.

$$\begin{aligned}
(\neg P \rightarrow R) \wedge (Q \leftrightarrow P) &\Leftrightarrow (P \vee R) \wedge [(Q \rightarrow P) \wedge (P \rightarrow Q)] \\
&\Leftrightarrow (P \vee R) \wedge (\neg Q \vee P) \wedge (\neg P \vee Q) \\
&\Leftrightarrow (P \vee R \vee F) \wedge (\neg Q \vee P \vee F) \wedge (\neg P \vee Q \vee F) \\
&\Leftrightarrow (P \vee R \vee (Q \wedge \neg Q)) \wedge (\neg Q \vee P \vee (R \wedge \neg R)) \wedge (\neg P \vee Q \vee (R \wedge \neg R)) \\
&\Leftrightarrow (P \vee R \vee Q) \wedge (P \vee R \vee \neg Q) \wedge (\neg Q \vee P \vee R) \wedge (\neg Q \vee P \vee \neg R) \\
&\qquad \wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R) \\
&\Leftrightarrow (P \vee R \vee Q) \wedge (P \vee R \vee \neg Q) \wedge (\neg Q \vee P \vee \neg R) \\
&\qquad \wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R)
\end{aligned}$$

Therefore the PCNF is $(P \vee R \vee Q) \wedge (P \vee R \vee \neg Q) \wedge (\neg Q \vee P \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R)$

Another method using truth table:

P	Q	R	$Q \leftrightarrow$P	$\neg$P	$\neg$P$\rightarrow$R	$(\neg P \rightarrow R) \wedge (Q \leftrightarrow P)$	Maxterms
T	T	T	T	F	T	T	
T	T	F	T	F	T	T	
T	F	T	F	F	T	F	$(\neg P \vee Q \vee \neg R)$
T	F	F	F	F	T	F	$(\neg P \vee Q \vee R)$
F	T	T	F	T	T	F	$(P \vee \neg Q \vee \neg R)$
F	T	F	F	T	F	F	$(P \vee \neg Q \vee R)$
F	F	T	T	T	T	T	
F	F	F	T	T	F	F	$(P \vee Q \vee R)$

The rows 3, 4, 5, 6 and 8 have the truth values F . The corresponding maxterms are given above.

Therefore the PCNF is $(\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R)$

Example: Find the PCNF and PDNF of $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$ without using truth tables.

https://doi.org/10.5281/zenodo.15287507

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

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

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

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

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

The PDNF of S is $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge R \wedge Q) \vee (\neg P \wedge R \wedge \neg Q)$

The PDNF of $\neg$S is $(\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg R \wedge \neg Q) \vee (P \wedge R \wedge \neg Q)$

PCNF of S is $\neg$(PDNF of $\neg$S) :
$\neg\left[(\neg P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg R \wedge \neg Q) \vee (P \wedge R \wedge \neg Q)\right]$

$$\left[(P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (\neg P \vee R \vee Q) \wedge (\neg P \vee \neg R \vee Q)\right]$$

Example: Find the PDNF and PCNF of $\left[P \to (Q \wedge R)\right] \wedge \left[\neg P \to (\neg Q \wedge \neg R)\right]$ without using truth tables.

$$S \Leftrightarrow \left[P \to (Q \wedge R)\right] \wedge \left[\neg P \to (\neg Q \wedge \neg R)\right]$$

$$\Leftrightarrow \left[\neg P \vee (Q \wedge R)\right] \wedge \left[P \vee (\neg Q \wedge \neg R)\right]$$

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

$$\Leftrightarrow \left[(\neg P \vee Q) \vee (R \wedge \neg R)\right] \wedge \left[(\neg P \vee R) \vee (Q \wedge \neg Q)\right] \wedge \left[(P \vee \neg Q) \vee (R \wedge \neg R)\right] \wedge \left[(P \vee \neg R) \vee (Q \wedge \neg Q)\right]$$

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

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

PCNF of S is
$(\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (P \vee Q \vee \neg R)$

PCNF of $\neg S$ is $(P \vee Q \vee R) \wedge (\neg P \vee \neg Q \vee \neg R)$

PDNF of S is $\neg$(PCNF of $\neg S$) $= \neg\left[(P \vee Q \vee R) \wedge (\neg P \vee \neg Q \vee \neg R)\right]$
$= (\neg P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge R)$

Alternate Method:

$$S \Leftrightarrow \left[P \to (Q \wedge R)\right] \wedge \left[\neg P \to (\neg Q \wedge \neg R)\right]$$

$$\Leftrightarrow \left[\neg P \vee (Q \wedge R)\right] \wedge \left[P \vee (\neg Q \wedge \neg R)\right]$$

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

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

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

https://doi.org/10.5281/zenodo.15287507

PDNF of S is $(P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$

PDNF of $\neg S$ is
$(\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge \neg R)$

PCNF of S is $\neg$(PDNF of $\neg S$)
$\neg\left[(\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (P \wedge Q \wedge \neg R) \right]$
$(P \vee \neg Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee \neg Q \vee R)$

Example: Obtain the PDNF and PCNF of $\neg(P \to Q) \leftrightarrow (P \wedge \neg Q)$.

$$\begin{aligned}
\neg(P \to Q) \leftrightarrow (P \wedge \neg Q) &\Leftrightarrow \left[\neg(P \to Q) \to (P \wedge \neg Q)\right] \wedge \left[(P \wedge \neg Q) \to \neg(P \to Q)\right] \\
&\Leftrightarrow \left[\ (P \to Q) \ \vee \ (P \wedge \neg Q) \ \right] \ \wedge \ \left[\neg \ (P \wedge \neg Q) \vee \neg \ (P \to Q) \ \right] \\
&\Leftrightarrow \left[\ (\neg P \vee Q) \ \vee \ (P \wedge \neg Q) \ \right] \ \wedge \ \left[\neg \ (P \wedge \neg Q) \vee \neg \ (\neg P \vee Q) \ \right] \\
&\Leftrightarrow \left[\ (\neg P \vee Q) \ \vee \ (P \wedge \neg Q) \ \right] \ \wedge \ \left[\ (\neg P \vee Q) \vee \ (P \wedge \neg Q) \ \right] \\
&\Leftrightarrow \left[\ (\neg P \vee Q) \ \vee \ (P \wedge \neg Q) \ \right] \\
&\Leftrightarrow \left[\ (\neg P \vee Q) \ \vee \ \neg(\neg P \vee Q) \ \right] \\
&\Leftrightarrow T
\end{aligned}$$

Since the given formula is a tautology, we cannot obtain its PCNF. Since the result of the formula is T, the PDNF will contain all the 4 possible minterms. Therefore the PDNF is $(P \wedge Q) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$

Note: Similarly if a given formula is a contradiction, then only PCNF exists.

Theory of Inference:

Let A and B be two statement formulas. Then B logically follows from A (or) B is a valid conclusion of the premise A iff $A \to B$ is a tautology and is denoted as $A \Rightarrow B$.

A set of premises $H_1, H_2, \ldots\ldots H_n$ derives a conclusion C iff $H_1 \wedge H_2 \wedge \ldots\ldots \wedge H_n \Rightarrow C$. This can be verified by constructing the truth table.

Example: Determine whether the conclusion $C : Q$ follows from the premises $H_1 : \neg P$, $H_2 : P \vee Q$

P	$C : Q$	$H_1 : \neg P$	$H_2 : P \vee Q$
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

The premises $H_1 : \neg P$ and $H_2 : P \vee Q$ have truth value T in third row and the conclusion is also have the truth value T in the same row. Hence the conclusion $C : Q$ is valid from the given premises.

This method is tedious for large number of variables. So when a conclusion is derived from a set of premises by using the rules of reasoning, then such a process is called a formal proof and the argument is called valid argument. There are three rules of inference.

Rule P : A premises may be introduced at any stage of derivation
Rule T : A formula S may be introduced in a derivation if S is tautologically implied by the preceding formulae in the derivation
Rule CP : If Q is derived from P and a set of premises, then $P \to Q$ may be derived from the set of premises alone.

Note:

- Indirect method or proof by contradiction means, If C is the conclusion, introduce $\neg C$ as an additional premises and derive the conclusion as F.
- The premises are inconsistent, if the conclusion(their conjunction) is F. Otherwise consistent.

Example: Give indirect proof of the theorem "If $3n+2$ is odd, then n is odd"

Suppose n is even. Let $n = 2k$.

$3n+2 = 3(2k)+2 = 2(3k+1) = Even$, a contradiction.

Hence the given statement is true.

List of rules of implications:

I_1	$P,\ P \to Q \Rightarrow Q$ $\neg Q,\ P \to Q \Rightarrow \neg P$ $Q,\ P \to Q \Rightarrow Q$	*Modus Ponens* *Modus Tollens*
I_2	$P \to Q,\ Q \to R \Rightarrow P \to R$	*Hypothetical Syllogism*
I_3	$P \to Q \Leftrightarrow \neg P \vee Q$	*Equivalence*
I_4	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$ $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	*De Morgan's Law*
I_5	$P \to Q \Leftrightarrow \neg Q \to \neg P$	*Contra Positive*
I_6	$P, Q \Rightarrow P \wedge Q$	*Implication*
I_7	$P \to R,\ Q \to R \Rightarrow (P \vee Q) \to R$	*Implication*
I_8	$P \wedge Q \Rightarrow P$ $P \wedge Q \Rightarrow Q$	*Simplification*
I_9	$P \Rightarrow P \vee Q$ $Q \Rightarrow P \vee Q$	*Addition*
I_{10}	$\neg P,\ P \wedge Q \Rightarrow Q$	Disjunction Dilemma
I_{11}	$\neg P,\ P \vee Q \Rightarrow Q$ $\neg Q,\ P \vee Q \Rightarrow P$	Disjunctive Syllogism
I_{12}	$\neg P \Rightarrow P \to Q$ $Q \Rightarrow P \to Q$	

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

Worked Examples on Equivalence and Implication

Example: Show that $P \to Q$, $Q \to \neg R$, R, $P \vee (R \wedge S) \Rightarrow (R \wedge S)$.

Step	Premises	Rule	Reason
1	$P \to Q$	P	Given Premises
2	$Q \to \neg R$	P	Given Premises
3	$P \to \neg R$	T	(1),(2) Hypothetical
4	$R \to \neg P$	T	(3) Contrapositive
5	R	T	Given Premises
6	$\neg P$	T	(5),(4) Modus Ponens
7	$P \vee (R \wedge S)$	P	Given Premises
8	$\neg P \to (R \wedge S)$	T	(7) Implication
9	$R \wedge S$	T	(6), (8) Modus ponens

Example: Show that S is valid inference from the premises $P \to \neg Q$, $Q \vee R$, $\neg S \to P$ and $\neg R$.

Step	Premises	Rule	Reason
1	$Q \vee R$	P	Given Premise
2	$\neg Q \to R$	T	(1) Equivalent
3	$\neg R$	P	Given Premise
4	Q	T	(2), (3) Modus Tollens
5	$P \to \neg Q$	P	Given Premise
6	$\neg P$	T	(4), (5) Modus Tollens
7	$\neg S \to P$	P	(6), (7) Modus Tollens
8	S	P	Given Premises

Example: Show that $\neg(P \wedge \neg Q), \neg Q \vee R, \neg R \Rightarrow \neg P$

Step	Premises	Rule	Reason
1	$\neg(P \wedge \neg Q)$	P	Given Premises
2	$\neg P \vee Q$	T	De-Morgan's Law
3	$P \to Q$	T	(2) Equivalence
4	$\neg Q \vee R$	P	Given Premises
5	$Q \to R$	T	(4) Equivalence
6	$P \to R$	T	(3), (5) Hypothetical Syllogism
7	$\neg R$	P	Given Premises
8	$\neg P$	T	(6), (7) Modus Tollens

Example: Show that $R \vee S$ follows logically follows from the premises $C \vee D$, $(C \vee D) \to \neg H$, $\neg H \to (A \wedge \neg B)$, $(A \wedge \neg B) \to (R \vee S)$.

Step	Premises	Rule	Reason
1	$(C \vee D) \to \neg H$	P	Given Premises
2	$\neg H \to (A \wedge \neg B)$	P	Given Premises
3	$(C \vee D) \to (A \wedge \neg B)$	T	(1), (2) Hypothetical Syllogism
4	$(A \wedge \neg B) \to (R \vee S)$	P	Given Premises
5	$(C \vee D) \to (R \vee S)$	T	(3), (4) Hypothetical Syllogism
6	$C \vee D$	P	Given Premises
7	$R \vee S$	T	(5), (6) Modus Ponens

Example: Show that $R \to S$ is logically derived from the premises $P \to (Q \to S)$, $\neg R \vee P$ and Q.

Step	Premises	Rule	Reason
1	$\neg R \vee P$	P	Given Premises
2	R	AP	Additional Premises
3	P	T	(1), (2) Modus Ponens
4	$P \to (Q \to S)$	P	Given Premises
5	$Q \to S$	T	(3), (4) Modus Ponens
6	Q	P	Given Premises
7	S	T	(5), (6) Modus Ponens
	$R \to S$	CP	(2), (7)

Example: Show that $R \wedge (P \vee Q)$ is a valid conclusion from the premises $P \vee Q,\ Q \to R,\ P \to M,\ \neg M$.

Step	Premises	Rule	Reason
1	$\neg M$	P	Given Premises
2	$P \to M$	P	Given Premises
3	$\neg P$	T	(1), (2) Modus Tollens
4	$P \vee Q$	P	Given Premises
5	$\neg P \to Q$	T	(4)
6	Q	T	(3), (5) Modus Ponens
7	$Q \to R$	P	Given Premises
8	R	T	(6), (7) Modus Ponens
9	$R \wedge (P \vee Q)$	T	(4), (8)

Example: Show that D can be derived from the premises $(A \to B) \wedge (A \to C)$, $\neg(B \wedge C)$ and $(D \vee A)$.

https://doi.org/10.5281/zenodo.15287507

Step	Premises	Rule	Reason
1	$(A\to B)\wedge(A\to C)$	P	Given Premises
2	$(A\to B)$	T	(1) Simplification
3	$(A\to C)$	T	(1) Simplification
4	$\neg B\to\neg A$	T	(2) Contra positive
5	$\neg C\to\neg A$	T	(3) Contra positive
6	$(\neg B\vee\neg C)\to\neg A$	T	(4), (5) Simplification
7	$\neg(B\wedge C)\to\neg A$	T	(6) De Morgan's Law
8	$\neg(B\wedge C)$	P	Given Premises
9	$\neg A$	T	(7), (8) Simplification
10	$(D\vee A)$	P	Given Premises
11	$(D\vee A)\wedge\neg A$	T	(9), (10) Conjunction
12	$(D\wedge\neg A)\vee(A\wedge\neg A)$	T	(11) Distributive Law
13	$(D\wedge\neg A)\vee F$	T	(12) Simplification
14	$D\wedge\neg A$	T	(13) Simplification
15	D	T	(14) Simplification

Example: Show that $(P\to Q)\wedge(R\to S)$, $(Q\to T)\wedge(S\to U)$, $\neg(T\wedge U)$ and $P\to R\Rightarrow\neg P$.

Step	Premises	Rule	Reason
1	$(P\to Q)\wedge(R\to S)$	P	Given Premises
2	$P\to Q$	T	(1) Simplification
3	$R\to S$	T	(1) Simplification
4	$(Q\to T)\wedge(S\to U)$	P	Given Premises
5	$Q\to T$	T	(4) Simplification
6	$S\to U$	T	(4) Simplification
7	$P\to T$	T	(2), (5) Hypothetical Syllogism
8	$R\to U$	T	(3), (6) Hypothetical Syllogism
9	$P\to R$	P	Given Premises
10	$P\to U$	T	(9), (8) Hypothetical Syllogism
11	$\neg U\to\neg P$	T	(10) Contra positive
12	$\neg T\to\neg P$	T	(7) Contra positive
13	$(\neg T\vee\neg U)\to\neg P$	T	(11), (12) Implication
14	$\neg(T\wedge U)\to\neg P$	T	(13) De Morgan's Law
15	$\neg(T\wedge U)$	P	Given Premises
16	$\neg P$	T	(15), (14) Modus Ponens

https://doi.org/10.5281/zenodo.15287507

Example: Apply indirect method, to prove R is the conclusion from the premises $P \to Q$, $Q \to R$, $P \vee R$.

Step	Premises	Rule	Reason
1	$\neg R$	P	Added Premises
2	$Q \to R$	P	Premises
3	$\neg Q$	T	(2),(1) Modus Tollens
4	$P \to Q$	P	Given Premises
5	$\neg P$	T	(4), (3) Modus Tollens
6	$P \vee R$	P	Given Premises
7	$\neg P \to R$	T	(6) Implication
8	R	T	(5),(7) Modus ponens
9	F	T	(1),(8)

Example: Show that the premises $A \to (B \to C)$, $D \to (B \wedge \neg C)$ and $A \wedge D$ are inconsistent.

Step	Premises	Rule	Reason
1	$A \wedge D$	P	Given Premises
2	A	T	(1) Simplification
3	D	T	(1) Simplification
4	$A \to (B \to C)$	P	Given Premises
5	$(B \to C)$	P	(2), (4) Modus Ponens
6	$\neg B \vee C$	T	(5) Equivalent
7	$D \to (B \wedge \neg C)$	P	Given Premises
8	$\neg(B \wedge \neg C) \to \neg D$	T	(7) Contra positive
9	$(\neg B \vee C) \to \neg D$	T	(8) Simplification
10	$\neg D$	T	(6), (9) Modus Ponens
11	$D \wedge \neg D$	T	(3), (10)
12	F	T	(11) Implication

Example: Show that the premises $R \to \neg Q$, $R \vee S$, $S \to \neg Q$, $P \to Q \Rightarrow \neg P$ are inconsistent by indirect method.

Step	Premises	Rule	Reason
1	P	P	Added Premises
2	$R \to \neg Q$	P	Given Premises
3	$R \vee S$	P	Given Premises
4	$S \to \neg Q$	P	Given Premises
5	$P \to Q$	P	Given Premises
6	$\neg Q \to \neg P$	T	(5) Contra positive
7	$\neg R \to S$	T	(3) Implication

https://doi.org/10.5281/zenodo.15287507

8	$\neg R \to \neg Q$	T	(4), (7) Hypothetical Syllogism
9	$\neg R \to \neg P$	T	(6), (8) Hypothetical Syllogism
10	$P \to R$	T	(9) Contra positive
11	R	T	(1), (10) Modus ponens
12	Q	T	(1), (5) Modus ponens
13	$\neg R$	T	(2), (12) Modus Tollens
14	F	T	(11), (13) Implication

Example: Using derivation process prove that $S \to \neg Q$, $R \vee S$, $\neg R$, $\neg R \leftrightarrow Q \Rightarrow \neg P$.

Step	Premises	Rule	Reason
1	$S \to \neg Q$	P	Given Premises
2	$R \vee S$	P	Given Premises
3	$\neg R \to S$	T	(2) Equivalent
4	$\neg R \to \neg Q$	T	(3), (1) Hypothetical Syllogism
5	$\neg R$	P	Given Premises
6	$\neg Q$	T	(5), (4) Modus ponens
7	$\neg R \leftrightarrow Q$	P	Given Premises
8	$\neg R \to Q$	T	(7) Equivalent
9	$\neg Q \to R$	T	(8) Equivalent
10	R	T	(6), (9) Modus Ponens
11	$R \wedge \neg R = F$	T	(5), (10) Conjunction
12	$\neg P$	T	(11) Contradiction $\Rightarrow$ Any formula

Example: Prove that $A \to \neg D$ is a conclusion from the premises $A \to B \vee C$, $B \to \neg A$ and $D \to \neg C$ by using conditional proof.

Include A as an additional premise and derive $\neg D$.

Step	Premises	Rule	Reason
1	A	P	Additional Premises
2	$A \to B \vee C$	P	Given Premises
3	$B \vee C$	T	(1), (2) Modus Ponens
4	$\neg B \to C$	T	(3) Equivalence
5	$B \to \neg A$	P	Given Premises
6	$A \to \neg B$	T	(5) Contra positive
7	$A \to C$	T	(6), (4) Hypothetical Syllogism
8	$D \to \neg C$	P	Given Premises
9	$\neg D \vee \neg C$	T	(8) Equivalence
10	$\neg D$	T	(9) Addition
11	$A \to \neg D$	CP	(1), (10)

Example: Using conditional proof, prove that $\neg P \vee Q$, $\neg Q \vee R$, $R \to S \Rightarrow P \to S$.

Include P as an additional premise and derive S.

Step	Premises	Rule	Reason
1	P	P	Additional Premises
2	$\neg P \vee Q$	P	Given Premises
3	$P \to Q$	T	(2) Equivalent
4	Q	T	(1), (3) Modus Ponens
5	$\neg Q \vee R$	P	Given Premises
6	$Q \to R$	T	(5) Equivalent
7	R	T	(4), (6) Modus Ponens
8	$R \to S$	P	Given Premises
9	S	T	(7), (8) Modus Ponens
10	$P \to S$	CP	(1), (9)

Validity of Arguments

Often we come across arguments expressed in sentences. The premises can be represented in symbols and can be verified the validity of the arguments. An argument is valid if and only if the conjunction of premises implies the conclusion.

Method to test validity

- Construct truth table showing the truth values of premises and conclusion
- Find rows in which all premises and conclusion is true. Then the argument is valid.
- If at least one row contains T for premises and conclusion is F, then the argument is invalid.

Example: If 7 is a prime number, then 7 does not divide 35. 7 divides 35. 7 is not a prime number.

Let P : 7 is a prime number Q : 7 divides 35 $C : \neg P$: 7 is not prime

The premises are $P \to \neg Q$, Q and the conclusion is $\neg P$

Let us now construct truth table:

P	Q	$\neg Q$	$P \to \neg Q$	$\neg P$
T	T	F	F	F
T	F	T	T	F
F	T	F	T	T
F	F	T	T	T

$P \to \neg Q$ and Q are both true only in the third row and in that row $\neg P$ is also true. Hence $P \to \neg Q, Q \Rightarrow \neg P$

By using rules of Implications.

1	$P \to \neg Q$	Rule P
2	Q	Rule P
3	$\neg P$	Rule T(1) (2) Modus Tollens

Example: By using truth tables verify whether the following specifications are consistent:
Whenever the system software is being upgraded users cannot access the file system. If users can access the file system, then they can save new files. If users cannot save new files then the system software is not being upgraded.

Let P : The system software is upgraded

https://doi.org/10.5281/zenodo.15287507

Q : Users can access the system
R : Users can save the new files

The given premises are : $P \to \neg Q$, $Q \to R$, $\neg R \to \neg P$

We have to prove the statement $S \equiv (P \to \neg Q) \wedge (Q \to R) \wedge (\neg R \to \neg P)$ is consistent.

P	Q	R	$\neg P$	$\neg Q$	$\neg R$	$P \to \neg Q$ (1)	$Q \to R$ (2)	$\neg R \to \neg P$ (3)	$(1) \wedge (2) \wedge (3)$
T	T	T	F	F	F	F	T	T	F
T	T	F	F	F	T	F	F	F	F
T	F	T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T	F	F
F	T	T	T	F	F	T	T	T	T
F	T	F	T	F	T	T	F	T	F
F	F	T	T	T	F	T	T	T	T
F	F	F	T	T	T	T	T	T	T

Therefore the premises are consistent.

Example: Test the validity of the following argument: If I study, I will pass in the examination. If I watch TV, then I will not study. I failed in the exam. Therefore I watched TV.

Let P : I will pass in the examination S : I will study W : I watch TV

The given premises are : $S \to P$, $W \to \neg S$, $\neg P$, $C : W$

W	S	P	$\neg P$	$\neg S$	$S \to P$	$W \to \neg S$
T	T	T	F	F	T	F
T	T	F	T	F	F	F
T	F	T	F	T	T	T
T	F	F	T	T	T	T
F	T	T	F	F	T	T
F	T	F	T	F	F	T
F	F	T	F	T	T	T
F	F	F	T	T	T	T

In the last row, premises are True but the conclusion is false. Hence the arguments are not valid.

1	$S \to P$	Rule P
2	$\neg P$	Rule P
3	$\neg S$	Rule T (1), (2)
4	$W \to \neg S$	Rule P
5	¬W	Rule T (3), (4)

Therefore the given arguments are not valid.

Example: Test the validity of the arguments: If 5 is a prime number, then 5 does not divide 15. 5 divides 15. Conclusion: 5 is not a prime number.

P : 5 is a prime number Q : 5 divides 15

The given premises are : $P \to \neg Q$, Q & $C : \neg P$

1	Q	Rule P
2	P→¬QRule P	
3	Q→¬P	Rule T (2)

https://doi.org/10.5281/zenodo.15287507

4 ¬P Rule T (1), (3)

Therefore the given arguments are not valid.

Example: Prove that whenever $A \wedge B \Rightarrow C$, we also have $A \Rightarrow (B \to C)$ and vice versa.

Assume that $A \wedge B \Rightarrow C$ To prove $A \Rightarrow (B \to C)$ Suppose that A is true and $(B \to C)$ is false. Hence B must be true and C must be false. Thus $A \wedge B$ is true where as C is false. This contradicts our assumption.	Conversely assume that $A \Rightarrow (B \to C)$ To prove $A \wedge B \Rightarrow C$. Suppose that it is false. Hence $A \wedge B$ is true and C is false. Hence A is true and $B \to C$ is false. This contradicts our assumption.

Example: Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Suppose $\sqrt{2}$ is rational.

Therefore $\sqrt{2} = \dfrac{P}{Q}$ where P, Q are integers having no common divisor and $Q \neq 0$ ...... (1)

$i.e.\ \dfrac{P^2}{Q^2} = 4$

$P^2 = 2Q^2$.......(2)

$\therefore\ P^2 =$ Even Number

$i.e.\ P =$ Even Number

Let $P = m$ for some integer m.

From (2), $(2m)^2 = 2Q^2$

$Q^2 = 2m^2$

$Q^2 =$ Even Number

$Q =$ Even Number

Since P and Q are even number, they have common factor 2.

This is a contradiction to (1). Therefore $\sqrt{2}$ is irrational.

Example: Show that $3-\sqrt{2}$ is irrational number.

Suppose $3-\sqrt{2} = R$ is a rational number. Then $\sqrt{2} = 3-R$.
Since 3, R are rational, $3-R$ is rational and hence $\sqrt{2}$ is rational. This is a contradiction to the fact that $\sqrt{2}$ irrational. Therefore $3-\sqrt{2} = R$ is irrational.

Example: Show that the following premises are inconsistent. "If Ram misses many classes through illness then he fails high school. If Ram fails high school then he is uneducated. If Ram reads a lot of books then he is not uneducated. Ram misses many classes through illness and reads a lot of books.

Let P : Ram misses many classes Q: Ram fails high school
R : Ram reads lot of books S: Ram is uneducated

Premises are $P \to Q,\ Q \to S,\ R \to \neg S,\ P \wedge R$

Step	**Premises**	**Rule**	**Reason**

1	$P \to Q$	P	Given Premises
2	$Q \to S$	P	Given Premises
3	$P \to S$	T	(1), (2) Hypothetical Syllogism
4	$R \to \neg S$	P	Given Premises
5	$S \to \neg R$	T	(4) Contra Positive
6	$P \to \neg R$	T	(3), (5) Hypothetical Syllogism
7	$\neg P \vee \neg R$	T	(6) Implication
8	$\neg(P \wedge R)$	T	(7) Implication
9	$P \wedge R$	P	Given Premises
10	$(P \wedge R) \wedge \neg(P \wedge R)$	T	(8), (9)
11	F	T	(10) Implication

Example: Show that "It is rained" is a conclusion obtained from the statements. "If it does not rain or if there is no traffic dislocation, then the sports day will be held and the cultural will go on". "If the sports day is held, the trophy will be awarded" and "the trophy was not awarded."

Let P : It rained Q: There is a traffic dislocation

R : Sports day held S: Cultural programmes goes on T: The trophy is awarded

Premises are $(\neg P \vee \neg Q) \to (R \wedge S)$, $R \to T$, $\neg T$ and conclusion $C : P$

Step	Premises	Rule	Reason
1	$\neg T$	P	Given Premises
2	$R \to T$	P	Given Premises
3	$\neg R$	T	(1), (2) Modus Tollens
4	$(\neg P \vee \neg Q) \to (R \wedge S)$	P	Given Premises
5	$\neg(R \wedge S) \to \neg(\neg P \vee \neg Q)$	T	(4) Contra Positive
6	$(\neg R \vee \neg S) \to (P \wedge Q)$	T	(3), (5) Hypothetical Syllogism
7	$\neg R \vee \neg S$	T	(3) Addition
8	$P \wedge Q$	T	(6), (7) Modus Ponens
9	P	T	(8) Simplification

Example: Prove that the statements $P \wedge Q \Rightarrow R \to S$ and $P \wedge Q \wedge R \Rightarrow S$ are equivalent.

$$\begin{aligned} P \wedge Q \Rightarrow R \to S &\Leftrightarrow (P \wedge Q) \to (R \to S) \text{ is a tautology} \\ &\Leftrightarrow \left[(P \wedge Q) \wedge R\right] \to S \text{ is a tautology} \\ &\Leftrightarrow (P \wedge Q \wedge R) \Rightarrow S \end{aligned}$$

Example: If the premises P, Q and R are inconsistent, prove that $\neg R$ is a conclusion from P and Q.

Given that $P \wedge Q \wedge R = F$. We have to prove $P \wedge Q \Rightarrow \neg R$

Assume that $P \wedge Q$ is true and on the contrary $\neg R$ is false.

Therefore R is true and hence $P \wedge Q \wedge R$ is true, which is a contradiction.

Therefore $\neg R$ is true and hence $P \wedge Q \Rightarrow \neg R$.

Predicates:

Consider the statements of the form $x-5=0$, $x^2-2x-1=0$, $x>100$ *etc.* We can not conclude that these are true or false as the values of x are not known. If x is replaced by a real number, the above statements becomes propositions. Such statements are called predicates and the symbol x is called the variable.

Let us consider two statements: 1. Ramu is clever 2. Seetha is clever

It requires 2 different symbols to denote them. But it will not reveal the common features of these statements (clever). Now we introduce a common symbol to denote 'is clever' and a method to join it with names of individuals. The part 'is clever' is called 'predicate'. Predicate is denoted by capital letters and individual person is denoted by small letter.

Here the predicate 'is clever' is denoted by C and Ramu by r and Seetha by s. Now the given statements can be symbolized as $C(r)$ and $C(s)$. The predicate $C(x)$ is a statement only if x is assigned some names.

When a quantifier is used on a variable x? when we have to assign a value to this variable to get a proposition, the occurrence of the variable is said to be bound.

An occurrence of a variable that is not bound by a quantifier or that set is equal to a particular value is said to be free.

Statement Function and Variables

A simple statement function of one variable consisting of predicate symbol and an individual variable.
Example: $M(x)$: x is a man. $R(x)$: x is a rational number greater than 10.

We can also combine one or more statement function using logical connectives to form compound function.

Example: $M(x)$: x is a man, $H(x)$: x is mortal and $T(x)$: x is tall.
Then $M(x)\wedge H(x)$, $M(x)\rightarrow H(x)$, $\neg T(x)$ etc.

Example: $S(x,y)$: x is greater than y.

Quantifiers:

https://doi.org/10.5281/zenodo.15287507

Consider the following propositions involving a specified number of objects.

1. Some men are human 2. For every real number x, $x^2 \geq 0$ 3. At least one student is interested in logic 4. There exists a function whose integration is e^x.

The word of type "For every", "For at least", "There exists an", "Some" etc., are said to quantify the propositions.

Universal Quantifier

The expression for all, some, none, exists, at least one is called the Universal quantifier and is denoted by $\forall$. All men are mortal is denoted by $(\forall x)(M(x) \to H(x))$.

Existential Quantifier

The expression 'for some', 'there exists' is called existential quantified and is denoted by $\exists$. Some men are tall is denoted by $(\exists x)(M(x) \wedge T(x))$.

Connectives involving quantifiers

The predicate prefixed by a quantifier is called a quantified predicate. The connectives like negation, disjunction, conjunction, conditional and biconditional can be used in quantified predicates to form a new predicates.

Examples: $(\exists x)P(x) \vee (\forall x)Q(x)$, $(\forall x)P(x) \wedge (\exists x)Q(x)$, $(\exists x)P(x) \to (\forall x)Q(x)$

Negation of a quantified statement

The following rules are used to find the negation of a quantified predicates.

i. $\neg(\exists x)P(x) \equiv (\forall x)\neg P(x)$ *ii.* $\neg(\forall x)P(x) \equiv (\exists x)\neg P(x)$

Symbolic form of the quantified statements:

1. Some men are honest

$M(x)$: x is a man $H(x)$: x is honest

There exists a man who is honest $(\exists x)(M(x) \wedge H(x))$

2. No cats has a tail

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

For all x, if x is a cat then x has no tail. $(\forall x)(C(x) \to \neg T(x))$

3. Someone is teasing

$T(x)$: x is teasing $P(x)$: x x is person

There is one x such that x is a person and x is teasing $(\exists x)(P(x) \wedge T(x))$

4. All babies are innocent

$B(x)$: x is a baby $I(x)$: x is innocent

https://doi.org/10.5281/zenodo.15287507

For all x, if x is a baby then x is innocent. $\left(\forall x\right)\left(B(x)\rightarrow I(x)\right)$

5. Some people who trust others are rewarded

$P(x)$: x is a person $T(x)$: x trust others $R(x)$: x is rewarded

There is some x such that x is a person, x trust others and x is rewarded $\left(\exists x\right)\left(P(x)\wedge T(x)\wedge R(x)\right)$

6. If any one is good, then John is good

$P(x)$: x is a person $G(x)$: x is good $G(j)$: John is good

If there is one x such that x is a person and x is good, then John is good $\left(\exists x\right)\left(\left(P(x)\wedge G(x)\right)\rightarrow G(j)\right)$

7. He is ambitious or no one is ambitious

$A(x)$: x is ambitious $P(x)$: x is person

x is ambitious or for all x, if x is a person then x is not ambitious $A(x)\vee\left(\forall x\right)\left(P(x)\rightarrow\neg A(x)\right)$

8. It is not true that all roads leads to Rome.

$R(x)$: x is a road $L(x)$: x leads to Rome

Negation of all roads leads to Rome $\neg\left[\left(\forall x\right)\left(R(x)\rightarrow L(x)\right)\right]$

9. Express the statement "For every x there exists a y such that $x^2+y^2\geq 100$" in symbolic form.

$(\forall x)(\exists y)\left(x^2+y^2\geq 100\right)$

10. Write the statement "Every one who likes fun will enjoy each of these plays" in symbolic form.

$L(x)$: x likes fun $P(x)$: x is a play $E(x,y)$: x will enjoy y

There exists a man who is honest $\left(\forall x\right)\left(\forall y\right)\left(L(x)\wedge P(y)\rightarrow E(x,y)\right)$

11. Write the statement "Every one who is healthy can do all kinds of work" in symbolic form.

$H(x)$: x is healthy $W(x)$: x is a kind of work $D(x,y)$: x can do y

Symbolic form $\left(\forall x\right)\left(\forall y\right)\left(H(x)\wedge W(y)\right)\rightarrow D(x,y)$

12. Let $M(x)$: x is a mammal. Let $A(x)$: x is an animal. Let $W(x)$: x is warm blooded

Symbolize the statement:	Translate into a statement
"Every Mammal is warm blooded"	$(\exists x)\left(A(x)\wedge\neg M(x)\right)$
$(\forall x)\left[M(x)\rightarrow W(x)\right]$	There are some animals that are not mammals

Universe of discourse:

We can restrict our discussion to a particular set of objects or persons. Such a restricted class is called the universe discourse.

Example: Symbolize the following statements using and without using universe of discourse.

(a) All men are mortal (b) some men mortal

Without universe of discourse **With universe of discourse**

$M(x)$: x is a man

$H(x)$: x is mortal

Let S be the set of all human beings

$H(x)$: x is mortal

(a) Given ‘for all x, if x is a man then x is mortal’

$(\forall x)(M(x) \to H(x))$ $\qquad$ $(\forall x)H(x)$

(b) Given ‘There exists some x such that x is a man and x is mortal’

$(\exists x)(M(x) \wedge H(x))$ $\qquad$ $(\exists x)H(x)$

Example: Translate the following where the universe is the set of all people and
$C(x)$: x is a comedian $\quad$ $F(x)$: x is funny

$(\forall x)(C(x) \to F(x))$ = All comedians are funny

$(\forall x)(C(x) \wedge F(x))$ = All are comedians and funny

$(\exists x)(C(x) \to F(x))$ = Some comedians are funny

$(\exists x)(C(x) \wedge F(x))$ = Some are comedians and funny

Example: $R(x, y): x + y = y + x$. What is the truth value of the quantifier $(\forall x)(\forall y)R(x, y)$, where the Domain is the set of real numbers.

The condition $x + y = y + x$ for all real numbers. Therefore the truth value is T.

Example: Let $P(x)$ denotes the statement $x > 3$. What is the truth value of $P(2)$?

Here $P(2): 2 > 3$. It is False.

Example: Let $Q(x, y)$ denote the statement $x = y + 3$. What is the truth value of the proposition $Q(3, 0)$?

Given $Q(x, y) : x = y + 3$
$Q(3, 0) : 3 = 0 + 3$. It is True.

Example: For all x, there exists some y such that $x + y = 0$.
If $x = 2,\ y = -2,\ x + y = 0$. Hence the truth value is T.

Example: Let the universe of discourse be $E = \{5, 6, 7\}$. Let $A = \{5, 6\}$ and $B = \{6, 7\}$.
Let $P(x) : x$ is in A; $Q(x) : x$ is in B and $R(x, y) : x + y < 12$. Find the truth value of
$(\exists x)[P(x) \to Q(x)] \to R(5, 6)$.

$R(5, 6) : 5 + 6 = 11 < 12$ is true.

$P(5)$ is true and $Q(5)$ is false. Therefore $P(5) \to Q(5)$ is true.

$P(6)$ is true and $Q(6)$ is true. Therefore $P(6) \to Q(6)$ is true.

$P(7)$ is false and $Q(7)$ is true. Therefore $P(7) \to Q(7)$ is true.

$\therefore$ $(\exists x)[P(x) \to Q(x)]$ is true.

$\therefore$ $(\exists x)[P(x) \to Q(x)] \to R(5, 6)$ is true.

Example: Find the truth value of $(x)(P \rightarrow Q(x)) \vee (\exists x)R(x)$ where $P: 2>1,\ Q(x): x>3,\ R(x): x>4,$ with the universe of discourse E being $E=\{2,3,4\}$.

P is true and $Q(4)$ is false. Hence $P \rightarrow Q(4)$ is false. $\therefore\ (x)(P \rightarrow Q(x))$ is false.

Since $R(2), R(3), R(4)$ are all false $(\exists x)R(x)$ is also false.

Hence $(x)(P \rightarrow Q(x)) \vee (\exists x)R(x)$ is false.

Example: Give an example in which $(\exists x)[P(x) \rightarrow Q(x)]$ is true but $((\exists x)P(x)) \rightarrow ((\exists x)Q(x))$ is false.

Let the universe of discourse be $E=\{3, 4, 6\}$

Let $P(x): x<5;\quad Q(x): x>7$.

$P(3)$ is true. $(\exists x)P(x)$ is true. For any x in E, $Q(x)$ is false.

Hence $((\exists x)P(x)) \rightarrow ((\exists x)Q(x))$ is false.

$P(6)$ is false and $Q(6)$ is false. Therefore $P(6) \rightarrow Q(6)$ is true.

Therefore $(\exists x)[P(x) \rightarrow Q(x)]$ is true.

Demorgan's Law: $\neg(\forall x)P(x) \Leftrightarrow (\exists x)\neg P(x)$ **and** $\neg(\exists x)P(x) \Leftrightarrow (\forall x)\neg P(x)$

Negation of Quantified Statements

Example: Negate the following statements:

a. All cities in India are clean
b. Some men are honest
c. Some birds cannot fly
c. No dog is intelligent

a. For all x, x is a city in India, then x is clean.

$C(x): x$ is a city and $L(x): x$ is clean then $(\forall x)(C(x) \rightarrow L(x))$

$$\begin{aligned}\neg(\forall x)(C(x) \rightarrow L(x)) &\Leftrightarrow (\exists x)\neg(C(x) \rightarrow L(x))\\ &\Leftrightarrow (\exists x)\neg(\neg C(x) \vee L(x))\\ &\Leftrightarrow (\exists x)(C(x) \wedge \neg L(x))\end{aligned}$$ i.e. some cities in India are not clean

b. There exists some x, x is a man, and x is honest.

$M(x): x$ is a man and $H(x): x$ is honest then $(\exists x)(M(x) \wedge H(x))$

$$\begin{aligned}\neg(\exists x)(M(x) \wedge H(x)) &\Leftrightarrow (\forall x)\neg(M(x) \wedge H(x))\\ &\Leftrightarrow (\forall x)(\neg M(x) \vee \neg H(x))\\ &\Leftrightarrow (\forall x)(M(x) \rightarrow \neg H(x))\end{aligned}$$ i.e. All men are not honest.

c. There exists some x, x is a bird, and x cannot fly.

$B(x): x$ is a bird and $F(x): x$ can fly then $(\exists x)(B(x) \wedge \neg F(x))$

$$\begin{aligned}\neg(\exists x)(B(x) \wedge \neg F(x)) &\Leftrightarrow (\forall x)\neg(B(x) \wedge \neg F(x))\\ &\Leftrightarrow (\forall x)(\neg B(x) \vee F(x))\end{aligned}$$

https://doi.org/10.5281/zenodo.15287507

$\Leftrightarrow (\forall x)\big(B(x) \to F(x)\big)$ i.e. All birds can fly.

d. It is not true that, for all x, x is a dog, then x is intelligent.

$D(x)$: x is a dog and $I(x)$: x is intelligent then $\neg\big(\forall x\big)\big(D(x) \to I(x)\big)$

$\neg\neg\big(\forall x\big)\big(D(x) \to I(x)\big) \Leftrightarrow \big(\forall x\big)\big(D(x) \to I(x)\big)$ i.e. all dogs are intelligent

Example: Express the negations of the following statement using quantifiers and in statement form. "No one has done every problem in the exercise".

$D(x, y)$: x has done problem y.

Given statement is $(\neg\exists x)(\forall y)D(x, y)$

Negation of the statement: Someone has done every problem in the exercise.

Symbolic form: $(\exists x)(\forall y)D(x, y)$

Example: Symbolize the following statement with and without using the set of positive integers as the universe of discourse. "Give any positive integer, there is a greater positive integers".

Let UOD is the set of integers.
Let the variables x and y be in the set of integers.

Let $G(x, y)$: x is greater than y.
Symbolic form: $(\forall x)(\exists x)G(x, y)$

Suppose we do not impose the restriction on UOD
Let $P(x)$: x is positive integer

Symbolic form:
$(\forall x)\big(P(x) \to (\exists y)\big(P(y) \wedge G(x, y)\big)\big)$

Example: Use quantifiers to say that $\sqrt{5}$ is not a rational number.

Let $P(x)$: x is a prime number. Let $Q(x)$:$\sqrt{x}$ is square root of prime number

Let $R(x)$: Rational number for all x.

$Q(x) \Rightarrow \neg R(x)$ i.e. Square root of every prime number is not rational.

Theory of inference for predicate calculus:

The following equivalence formulas can be used to derive the conclusion.

$\big(\forall x\big)A(x) \Rightarrow A(y)$ Rule US $\qquad$ $A(y) \Rightarrow \big(\forall x\big)A(x)$ Rule UG

$\big(\exists x\big)A(x) \Rightarrow A(y)$ Rule ES $\qquad$ $A(y) \Rightarrow \big(\exists x\big)A(x)$ Rule EG

Example: Verify the validity of the inference: If one person is more successful than other, then he has worked harder to deserve success. John has not worked harder than Peter. Therefore, John is not successful than Peter.

Solution: Universe : All persons

$S(x, y)$: x is more successful than y

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

a: John and b: Peter

The premises are $\big(\forall x\big)\big(\forall y\big)\big[S(x, y) \to W(x, y)\big]$, $\neg W(a, b)$ and conclusion $C : \neg S(a, b)$

1	$\neg W(a,b)$	Premise
2	$(\forall x)(\forall y)\left[S(x,y)\rightarrow W(x,y)\right]$	Premise
3	$(\forall y)\left[S(a,y)\rightarrow W(a,y)\right]$	US and (2)
4	$\left[S(a,b)\rightarrow W(a,b)\right]$	US and (3)
5	$\neg S(a,b)$	From (1) & (4)

Example: Show that the premises "One student in this class knows how to write programmes in JAVA and everyone who knows how to write programmes in JAVA can get a high paying job" imply the conclusion "Someone in this class can get a high paying job".

Solution: Universe : All students

$C(x): x$ is in this class

$J(x): x$ knows JAVA programming

$H(x): x$ can get a high paying job

The premises are $(\exists x)\left[C(x)\wedge J(x)\right]$, $(\forall x)\left[J(x)\rightarrow H(x)\right]$ and conclusion $C:(\exists x)[C(x)\wedge H(x)]$

1	$(\exists x)\left[C(x)\wedge J(x)\right]$	Premise
2	$C(a)\wedge J(a)$	ES and (1)
3	$C(a)$	From (2)
4	$J(a)$	From (2)
5	$(\forall x)\left[J(x)\rightarrow H(x)\right]$	Premise
6	$J(a)\rightarrow H(a)$	US and (5)
7	$H(a)$	From (4) and (6)
8	$C(a)\wedge H(a)$	From (3) and (7)
9	$(\exists x)[C(x)\wedge H(x)]$	EG and (8)

Example: Verify the validity of the argument: Lions are dangerous animals. There are lions. Therefore there are dangerous animals.

Let $L(x): x$ is a lion and $D(x): x$ is a dangerous animal.
Then the premises are $(x)\left(L(x)\rightarrow D(x)\right)$ and $(\exists x)\,L(x)$ and the conclusion is $(\exists x)\,D(x)$

Step	**Premises**	**Rule**
1	$(x)\left(L(x)\rightarrow D(x)\right)$	P
2	$L(y)\rightarrow D(y)$	T , US , (1)
3	$(\exists x)\,L(x)$	P
4	$L(y)$	T , ES , (3)
5	$D(y)$	T , (2), (4)

6	$(\exists x)\,D(x)$	T , EG , (5)

Example: Verify the validity of the argument: All men are mortal. Socretes is a man Therefore Socretes is a mortal.

Let $M(x): x$ is a man and $R(x): x$ is a mortal. s: Socretes. Then the premises are

$(x)\big(M(x) \to R(x)\big)$, $M(s)$ and the conclusion is $R(s)$.

1	$(x)\big(M(x) \to R(x)\big)$	Rule P
2	$M(s) \to R(s)$	Rule US , (1)
3	$M(s)$	Rule P
4	$R(s)$	Rule T (2), (3)

Hence the given argument is valid.

Example: Show that $(\forall x)P(x) \to (\exists x)P(x)$ is logically valid statement.

If $(\forall x)P(x)$ is true in some particular universe, then the universe has at least one object a in it and $P(b)$ is true statement for every b in the universe. In particular $P(a)$ must be true. Then $(\exists x)P(x)$ is true. Therefore $(\forall x)P(x) \to (\exists x)P(x)$ is valid.

Example: Give an example to show that $(\exists x)\big(A(x) \wedge B(x)\big)$ need not be a conclusion from $(\exists x)A(x)$ and $(\exists x)B(x)$.

Let $A(x): x \in A$ and $B(x): x \in B$. Let $A = \{1\}$ and $B = \{2\}$. Since A and B are non empty, $(\exists x)A(x)$ and $(\exists x)B(x)$ are both true. But $(\exists x)\big(A(x) \wedge B(x)\big)$ is false since $A \cap B = \phi$.

Example: For the following set of premises, explain which rules of inferences are used to obtain conclusion from the premises. "Somebody in this class enjoys whale watching. Every person who enjoys whale watching cares about ocean pollution. Therefore, there is person in this class who cares about ocean pollution".

Universe of discourse : Set f students in the class
Let $E(x): x$ enjoys whale watching $O(x): x$ cares about ocean pollution
Then the premises are $(\exists x)E(x)$, $(\forall x)\big(E(x) \to O(x)\big)$ and conclusion is $(\exists x)O(x)$.

1	$(\exists x)E(x)$	Rule P
2	$E(a)$	ES, (1)
3	$(\forall x)\big(E(x) \to O(x)\big)$	Rule P
4	$E(a) \to O(a)$	US, (3)
5	$O(a)$	Rule T, (2), (4)
6	$(\exists x)O(x)$	EG, (5)

Example: Prove that $(\exists x)M(x)$ follows logically from the premises $(x)\big(H(x) \to M(x)\big)$ and $(\exists x)H(x)$.

1	$(\exists x)H(x)$	Rule P
2	$H(a)$	ES and (1)

3	$(x)\big(H(x)\to M(x)\big)$	Rule P
4	$H(a)\to M(a)$	US and (3)
5	$M(a)$	Rule T, (2), (4)
6	$(\exists x)M(x)$	EG and (5)

Example: Prove that $(\exists x)A(x)\to B \Leftrightarrow (\forall x)A(x)\to B$

Suppose that $(\exists x)A(x)\to B$ is true and assume that $(\forall x)A(x)\to B$ is false.

Hence $A(a)\to B$ is false for some a.

Therefore is $A(a)$ true and B is false.

Since $A(a)$ is true $(\exists x)A(x)$ is true.

Therefore $(\exists x)A(x)\to B$ must be false, which is contrary to our assumption.

This proves that $(\forall x)A(x)\to B$ is true.

For the reverse implication suppose that $(\forall x)A(x)\to B$ is true and assume that $(\exists x)A(x)\to B$ is false.

Therefore $(\exists x)A(x)$ is true and B is false.

Therefore $A(a)$ is true for some a.

Therefore $A(a)\to B$ is false

Hence $(\forall x)A(x)\to B$ is false, which is contrary to our assumption.

This proves that $(\exists x)A(x)\to B$ is true.

Example: Prove that $(x)[H(x)\to A(x)]\Rightarrow (x)(\exists y)\big(H(y)\wedge N(x,y)\big)\to(\exists y)\big(A(y)\wedge N(x,y)\big)$

Assume that $(x)[H(x)\to A(x)]$ is true and $(x)(\exists y)\big(H(y)\wedge N(x,y)\big)\to(\exists y)\big(A(y)\wedge N(x,y)\big)$ is false.

Hence for some a in the universe discourse $(\exists y)\big(H(y)\wedge N(a,y)\big)\to(\exists y)\big(A(y)\wedge N(a,y)\big)$ is false.

This is again implies that $(\exists y)\big(H(y)\wedge N(a,y)\big)$ is true and $(\exists y)\big(A(y)\wedge N(a,y)\big)$ false.

i.e. $\big(H(b)\wedge N(a,b)\big)$ is true for some b ……(1) and $(\forall y)\neg\big(A(y)\wedge N(a,y)\big)$ is true.

i.e. $\neg\big(A(b)\wedge N(a,b)\big)$ is true.

i.e. $\big(A(b)\wedge N(a,b)\big)$ is false…….(2)

From (1), $H(b)$ and $N(a,b)$ is true and from (2) $A(b)$ is false.

Therefore $H(b)\to A(b)$ must be false.

But this cannot happen since we assumed that $(x)[H(x)\to A(x)]$ is true. This proves the given statement.

Example: Show that $(x)\big(H(x)\to M(x)\big)\wedge H(s)\Rightarrow M(s)$

1	$(x)\big(H(x)\to M(x)\big)$	Rule P
2	$H(s)\to M(s)$	Rule US, (1)
3	$H(s)$	Rule P

4	$M(s)$	Rule T (2), (3)

Example: Show that $(x)(P(x) \to Q(x)) \wedge (x)(Q(x) \to R(x)) \Rightarrow (x)(P(x) \to R(x))$

1	$(x)(P(x) \to Q(x))$	Rule P
2	$P(y) \to Q(y)$	Rule US, (1)
3	$(x)(Q(x) \to R(x))$	Rule P
4	$Q(y) \to R(y)$	Rule US, (3)
5	$P(y) \to R(y)$	Rule T, (2), (4)
6	$(x)(P(x) \to R(x))$	Rule UG, (5)

Example: Show that $(\exists x)M(x)$ follows logically from the premises $(x)(H(x) \to M(x))$ and $(\exists x)H(x)$ (or) Is the following conclusion validly derivable from the premises given? If $(\forall x)(P(x) \to Q(x))$, $(\exists y)P(y)$ then $(\exists z)Q(z)$.

1	$(\exists x)H(x)$	Rule P
2	$H(y)$	Rule ES, (1)
3	$(x)(H(x) \to M(x))$	Rule P
4	$H(y) \to M(y)$	Rule US, (3)
5	$M(y)$	Rule T, (2), (4)
6	$(\exists x)M(x)$	Rule EG

Example: Prove that $(\exists x)(P(x) \to Q(x)) \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$

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

Example: Use conditional proof to prove that $(\forall x)[P(x) \to Q(x)] \Rightarrow (\forall x)P(x) \to (\forall x)Q(x)$

We assume $(\forall x)P(x)$ as an additional premise and derive $(\forall x)Q(x)$.

1	$(\forall x)P(x)$	Additional Premise
2	$P(a)$	US, (1)
3	$(\forall x)[P(x) \to Q(x)]$	Rule P

4	$P(a) \to Q(a)$	US, (3)
5	$Q(a)$	Rule T, (2), (4)
6	$(\forall x)Q(x)$	UG, (5)

Example: Prove that $(\exists x)P(x) \to (x)Q(x) \Rightarrow (x)\left[P(x) \to Q(x)\right]$

Assume that $(\exists x)P(x) \to (x)Q(x)$ is true and $(x)[P(x) \to Q(x)]$ is false.

i.e. $P(a) \to Q(a)$ is false for some a in the UOD.

i.e. $P(a)$ must be true and $Q(a)$ must be false.

i.e. $(\exists x)P(x)$ is true and $(x)Q(x)$ is false.

$\therefore$ $(\exists x)P(x) \to (x)Q(x)$ is false.

This proves that the given statement is true.

Alternate Method:

1	$(\exists x)P(x) \to (x)Q(x)$ Rule P	
2	$\neg\left((\exists x)P(x)\right) \vee \left((x)Q(x)\right)$	Rule T, (1)
3	$(\forall x)\neg P(x) \vee (x)Q(x)$	Rule T, (2)
4	$(\forall x)\left[\neg P(x) \vee Q(x)\right]$	Rule T, (3)
5	$(\forall x)\left[P(x) \to Q(x)\right]$	Rule T, (4)

Example: Prove that $(\exists x)\left(P(x) \vee Q(x)\right) \Leftrightarrow (\exists x)\left(P(x)\right) \vee (\exists x)\left(Q(x)\right)$

Assume $(\exists x)\left(P(x) \vee Q(x)\right)$ is true. $\Rightarrow P(a) \vee Q(a)$ is true for some a.

$\Rightarrow P(a)$ is true of $Q(a)$ is true.

$\Rightarrow (\exists x)P(x)$ or $(\exists x)Q(x)$

$\Rightarrow (\exists x)\left(P(x)\right) \vee (\exists x)\left(Q(x)\right)$

Conversely assume that $(\exists x)\left(P(x)\right) \vee (\exists x)\left(Q(x)\right)$ is true.

$\Rightarrow (\exists x)P(x)$ is true, or $(\exists x)Q(x)$ is true

If $(\exists x)P(x)$ is true, $P(a)$ is true for some a.

i.e. $P(a) \vee Q(a)$ is true

i.e. $(\exists x)\left(P(x) \vee Q(x)\right)$ is true

If $(\exists x)Q(x)$ is true, $Q(a)$ is true for some a.

i.e. $P(a) \vee Q(a)$ is true

i.e. $(\exists x)\left(P(x) \vee Q(x)\right)$ is true

Example: Prove that $(\exists x)\left(P(x) \wedge Q(x)\right) \Rightarrow (\exists x)\left(P(x)\right) \wedge (\exists x)\left(Q(x)\right)$

1	$(\exists x)\left(P(x) \wedge Q(x)\right)$	Rule P

2	$P(y)\wedge Q(y)$	ES, (1)
3	$P(y)$	From (2)
4	$Q(y)$	From (3)
5	$\exists x P(x)$	EG, (3)
6	$\exists x Q(x)$	EG, (4)
7	$(\exists x)\big(P(x)\big)\wedge(\exists x)\big(Q(x)\big)$	From (5), (6)

Example: Using indirect method of proof, prove that $(x)\big(P(x)\vee Q(x)\big)\Rightarrow (x)P(x)\vee(\exists x)Q(x)$

We assume $\neg\big[(x)P(x)\vee(\exists x)Q(x)\big]$ as additional premise and arrive at a contradiction

Step	**Premises**	**Rule**
1	$\neg\big[(x)P(x)\vee(\exists x)Q(x)\big]$	P , Additional Premise
2	$(\exists x)\neg P(x)\wedge(\forall x)\neg Q(x)$	T , De Morgan's Law, (1)
3	$(\exists x)\neg P(x)$	T , $P\wedge Q\Rightarrow P$, (2)
4	$(\forall x)\neg Q(x)$	T , $P\wedge Q\Rightarrow Q$, (2)
5	$\neg P(y)$	T , ES , (3)
6	$\neg Q(y)$	T , US , (4)
7	$\neg P(y)\wedge\neg Q(y)$	T , (5), (6)
8	$\neg\big[P(y)\vee Q(y)\big]$	T , De Morgan's Law, (7)
9	$(x)\big(P(x)\vee Q(x)\big)$	P
10	$P(y)\vee Q(y)$	T , US , (9)
11	$\neg\big[P(y)\vee Q(y)\big]\wedge\big[P(y)\vee Q(y)\big]$	T , (7), (10)
12	F	T , (11)

Example: Using indirect method of proof, prove that $(x)\big(P(x)\rightarrow Q(x)\big)\wedge(\exists y)Q(y)\Rightarrow(\exists z)Q(z)$

We assume $\neg(\exists z)Q(z)$ as additional premise and arrive at a contradiction

Step	**Premises**	**Rule**
1	$\neg(\exists z)Q(z)$	P , Additional Premise
2	$(\forall z)\neg Q(z)$	T , (1)
3	$\neg Q(a)$	T, US, (2)
4	$(\exists y)P(y)$	P
5	$P(a)$	T , ES , (4)
6	$P(a)\wedge\neg Q(a)$	T , (3), (5)

7	$\neg[P(a)\to Q(a)]$	T, (6),
8	$(x)(P(x)\to Q(x))$	P
9	$P(a)\to Q(a)$	T, US, (8)
10	$[P(a)\to Q(a)]\wedge\neg[P(a)\to Q(a)]$	T, (7), (9)
11	F	T, (10)

Example: Using CP obtain the following implication $(x)(P(x)\to Q(x)),\ (x)(R(x)\to\neg Q(x))$ $\Rightarrow (x)(R(x)\to\neg P(x))$

In conditional method, we assume $R(x)$ as additional premise and we derive $\neg P(x)$.

Step	Premises	Rule
1	$(x)(P(x)\to Q(x))$	P
2	$P(y)\to Q(y)$	T, US, (1)
3	$(x)(R(x)\to\neg Q(x))$	P
4	$R(y)\to\neg Q(y)$	T, US, (3)
5	$(x)R(x)$	P
6	$R(y)$	T, (5)
7	$\neg Q(y)$	T, (4), (6)
8	$\neg P(y)$	T, (2), (7)
9	$(x)\neg P(x)$	T, (8)

Example : Prove that $(x)(P(x)\to Q(x)),\ (x)(R(x)\to\neg Q(x))\ \Rightarrow (x)(R(x)\to\neg P(x))$

1	$(x)(P(x)\to Q(x))$	Rule P
2	$P(a)\to Q(a)$	US (1)
3	$(x)(R(x)\to\neg Q(x))$	Rule P
4	$R(a)\to\neg Q(a)$	US (3)
5	$Q(a)\to\neg R(a)$	$(4)\Leftrightarrow(5)$ Contra Positive
6	$P(a)\to\neg R(a)$	Rule T (2), (5)
7	$R(a)\to\neg P(a)$	$(6)\Leftrightarrow(7)$
8	$(x)(R(x)\to\neg P(x))$	UG (7)

Example : Prove that $(x)(P(x)\to(Q(y)\wedge R(x))),\ (\exists x)P(x)\ \Rightarrow Q(y)\wedge\exists x(P(x)\wedge R(x))$

1	$(x)(P(x)\to(Q(y)\wedge R(x)))$	Rule P

2	$\left(P(a) \rightarrow \left(Q(y) \wedge R(a)\right)\right)$	US, (1)
3	$\left(\exists x\right) P(x)$	Rule P
4	$P(a)$	ES, (3)
5	$Q(y) \wedge R(a)$	From (4), (2)
6	$Q(y)$	From (5)
7	$R(a)$	From (5)
8	$P(a) \wedge R(a)$	From (4), (7)
9	$\exists x\left(P(x) \wedge R(x)\right)$	EG, (8)
10	$Q\left(y\right) \wedge \exists x\left(P(x) \wedge R(x)\right)$	From (6), (9)

Example : Show that the conclusion $\left(\forall x\right) P(x) \rightarrow \neg Q(x)$ follows from the premises $\left(\exists x\right)\left(P(x) \wedge Q(x)\right) \rightarrow \left(\forall y\right)\left(R(y) \rightarrow S(y)\right)$ and $(\exists y)\left(R(y) \wedge \neg S(y)\right)$.

1	$(\exists y)\left(R(y) \wedge \neg S(y)\right)$	Rule P
2	$R(a) \wedge \neg S(a)$	ES, (1)
3	$\neg R(a) \rightarrow S(a)$	Rule T, (2)
4	$(\exists y) \neg\left(R(y) \rightarrow S(y)\right)$	EG, (3)
5	$\neg(\forall y)\left(R(y) \rightarrow S(y)\right)$	Rule T, (4)
6	$\left(\exists x\right)\left(P(x) \wedge Q(x)\right) \rightarrow \left(\forall y\right)\left(R(y) \rightarrow S(y)\right)$	Rule P
7	$\neg\left(\exists x\right)\left(P(x) \wedge Q(x)\right)$	Rule T, (5), (6)
8	$\left(\forall x\right) \neg\left(P(x) \wedge Q(x)\right)$	Rule T, (7)
9	$\neg P(x) \wedge Q(x)$	US, (8)
10	$P(x) \rightarrow Q(x)$	Rule T, (9)
11	$(\forall x)\left[P(x) \rightarrow \neg Q(x)\right]$	UG, (10)

EXERCISE

1. Show that $\left(\neg P \wedge \left(\neg Q \wedge R\right)\right) \vee \left(Q \wedge R\right) \vee \left(P \wedge R\right) \Leftrightarrow R$, without using truth table.

2. Show that $\left(P \vee Q\right) \wedge \neg\left(\neg P \wedge \left(\neg Q \vee \neg R\right)\right) \vee \left(\neg P \wedge \neg Q\right) \vee \left(\neg P \wedge \neg R\right)$ is a tautology without using truth table.

3. Show that $R \wedge \left(P \vee Q\right)$ is a valid conclusion from the premises $P \vee Q,\ Q \rightarrow R,\ P \rightarrow M,\ \square\ M$.

4. Show that $R \rightarrow S$ is logically derived from the premises $P \rightarrow \left(Q \rightarrow S\right),\ \neg R \vee P$ and Q.

5. Show that $\left(\left(P \vee Q\right) \wedge \neg\left(\neg P \wedge \left(\neg Q \vee \neg R\right)\right)\right) \vee \left(\neg P \wedge \neg Q\right) \vee \left(\neg P \wedge \neg R\right)$ is a tautology by using equivalences.

6. Using indirect method, show that $R \vee S,\ R \rightarrow \neg Q,\ S \rightarrow \neg Q,\ P \rightarrow Q \Rightarrow \neg P$.

7. Show that $R \to S$ is logically derived from the premises $P \to (Q \to S)$, $\neg R \vee P$ and Q.

8. Show that using Rule C.P., $\neg P \vee Q,\ \neg Q \vee R,\ R \to S \Rightarrow P \to S$

9. Show that $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ is a tautology by using equivalences.

10. Without constructing the truth tables, obtain the PDNF of $(\neg P \to R) \wedge (Q \leftrightarrow P)$.

11. Obtain the PCNF of the formula $(\neg P \to R) \wedge (P \to Q) \wedge (Q \to P)$

12. Find the PDNF form of $(P \wedge Q) \vee (\neg P \wedge R) \vee (Q \wedge R)$ without using truth table. Also find its PCNF form.

13. Obtain the PCNF and PDNF of $(\neg P \to R) \wedge (Q \leftrightarrow P)$ by using equivalences.

14. Find the PCNF of $(P \vee R) \wedge (P \vee \neg Q)$. Also find its PDNF, without using truth table.

15. Let $M(x): x$ is a man. $R(x): x$ is mortal. Produce the suitable English statement for the following: (1) $(\forall x)(M(x) \to \neg R(x))$ (2) $(\exists x)(M(x) \wedge R(x))$

16. Show that the following set of premises is inconsistent:

If war is near then the army would be mobilized. If the army has mobilized then the labor costs are high. However the war is near and yet the labor costs are not high.

17. Verify the validity of the argument. "Every living thing is a plant or an animal". John's gold fish is alive and it is not a plant. All animals has hearts therefore, John's gold fish has a heart.

18. Using CP rule, prove the following argument:
$(\forall x)P(x) \to Q(x),\ (\forall x)(R(x) \to \neg P(x)) \Rightarrow (\forall x)(R(x) \to \neg P(x))$.

19. Show that $(x)[P(x) \to Q(x)] \wedge (x)[Q(x) \to R(x)] \Rightarrow (x)[P(x) \to R(x)]$.

20. If the universe of discourse consists of all real numbers and if $p(x)$ and $q(x)$ are given by $p(x): x \geq 0$ and $q(x): x^2 \geq 0$, then determine the truth value of $(\forall x)(p(x) \to q(x))$.

21. Show that if x and y are integers and both xy and $x+y$ are even, then both x and y are even.

22. Let $K(x): x$ is a two wheeler, $L(x): x$ is a scooter, $M(x): x$ is manufactured by Bajaj. Express the following using quantifiers.

(1) Every two wheeler is a scooter

(2) There is a two wheeler that is not manufactured by Bajaj

(3) There is a two wheeler manufactured by Bajaj that is not a scooter

(4) Every two wheeler that is a scooter is manufactured by Bajaj.

UNIT II – COMBINATORICS

Method of Induction

Introduction:

Mathematical statements which cannot be easily derived by direct methods is sometimes derived by using mathematical induction. It is one of the basic methods of proof of a statement about all natural numbers. Consider the example: What is the formula for the sum of first n positive odd integers?.

$$1 = 1^2$$
$$1+3 = 4 = 2^2$$
$$1+3+5 = 9 = 3^2$$
$$1+3+5+7 = 16 = 4^2$$

Now any one can guess the sum of the first n positive odd integers is n^2. But to prove assertion of this type, Mathematical induction is a technique. The word induction is associated with the inductive, by which a conclusion is drawn from a large number of special cases.

Principle of Mathematical Induction:

Let $p(n)$ be the proposition involving the integral value of n.

(i) If $p(1)$ is true and

(ii) Under the assumption that $p(k)$ is true,

(iii) Then we have to prove $p(k+1)$ is true.

Then , we conclude that the statement $p(n)$ is true for all $n \in Z^+$.

Note: Here $p(1)$ is called the base step of the statement. Sometimes $p(0)$ or $p(2)$ may be the base steps.

Strong form of Principle of Mathematical Induction:

Let $p(n)$ be the proposition involving the integral value of n.

(i) Assume that $p(n)$ is true for $n = 1, 2, 3, \ldots\ldots, k$

(ii) Under the assumption, we have to prove $p(k+1)$ is true.

Then , we conclude that the statement $p(n)$ is true for all $n \in Z^+$.

Example 1: Prove by mathematical induction that $1+2+3+\ldots.+n = \dfrac{n(n+1)}{2}$.

Let $p(n):\ 1+2+3+\ldots.+n = \dfrac{n(n+1)}{2}$.

https://doi.org/10.5281/zenodo.15287608

Now $p(1):\ 1=\frac{1(1+1)}{2}=1.$ $p(2):\ 1+2=\frac{2(2+1)}{2}=3$ is true.

Hence assume that $p(k)$ is true. i.e. $p(k):\ 1+2+3+....+k=\frac{k(k+1)}{2}.$

Now we have to prove $p(k+1)$ is true.

$$\begin{aligned}1+2+3+....+k+(k+1) &= \frac{k(k+1)}{2}+(k+1)\\ &= \frac{k(k+1)+2(k+1)}{2}\\ &= \frac{(k+1)(k+2)}{2}\\ &= \frac{(k+1)[(k+1)+1]}{2}\end{aligned}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 2: Prove by mathematical induction that $1^2+2^2+3^2+....+n^2=\frac{n(n+1)(2n+1)}{6}.$

Let $p(n):\ 1^2+2^2+3^2+....+n^2=\frac{n(n+1)(2n+1)}{6}.$

Now $p(1):\ 1^2=\frac{1(1+1)(2+1)}{6}=1.$

$p(2):\ 1^2+2^2=\frac{2(2+1)(4+1)}{6}=\frac{30}{6}=5$ is true

Hence assume that $p(k)$ is true. i.e. $p(k):\ 1^2+2^2+3^2+....+k^2=\frac{k(k+1)(2k+1)}{6}.$

Now we have to prove $p(k+1)$ is true.

$$\begin{aligned}1^2+2^2+3^2+....+k^2+(k+1)^2 &= \frac{k(k+1)(2k+1)}{6}+(k+1)^2\\ &= \frac{k(k+1)(2k+1)+6(k+1)^2}{6}\\ &= \frac{(k+1)[(2k^2+k)+6k+6]}{6}\\ &= \frac{(k+1)(2k^2+7k+6)}{6}\\ &= \frac{(k+1)(k+2)(2k+3)}{6}\\ &= \frac{(k+1)\ [(k+1)+1)\ [2(k+1)+1]}{6}\end{aligned}$$

https://doi.org/10.5281/zenodo.15287608

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 3: Prove by mathematical induction that $1^2+3^2+5^2+....+(2n-1)^2=\frac{n(2n-1)(2n+1)}{3}$.

Let $p(n):1^2+3^2+5^2+....+(2n-1)^2=\frac{n(2n-1)(2n+1)}{3}$.

Now $p(1):\ 1^2=\frac{1(2\square 1-1)(2\square 1+1)}{3}=1.$

$p(2):\ 1^2+3^2=\frac{2(2\square 2-1)(2\square 2+1)}{3}=\frac{30}{3}=10$ is true

Hence assume that $p(k)$ is true. i.e. $p(k):1^2+3^2+5^2+....+(2k-1)^2=\frac{k(2k-1)(2k+1)}{3}$.

Now we have to prove $p(k+1)$ is true.

$$1^2+3^2+5^2+....+(2k-1)^2+(2k+1)^2=\frac{k(2k-1)(2k+1)}{3}+(2k+1)^2$$

$$=\frac{k(2k-1)(2k+1)+3(2k+1)^2}{3}$$

$$=\frac{(2k+1)[k(2k-1)+3(2k+1)]}{3}$$

$$=\frac{(2k+1)(2k^2+5k+3)}{3}$$

$$=\frac{(2k+1)(2k+3)(k+1)}{3}$$

$$=\frac{(k+1)\ [2(k+1)-1)\ [2(k+1)+1]}{3}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 4: Use mathematical induction to prove $1^3+2^3+3^3+....+n^3=\left[\frac{n(n+1)}{2}\right]^2=\frac{n^2(n+1)^2}{4}$.

Let $p(n):\ 1^3+2^3+3^3+....+n^3=\frac{n^2(n+1)^2}{4}$.

Now $p(1):\ 1^3=\frac{1^2(1+1)^2}{4}=1.$

$p(2):\ 1^3+2^3=\frac{2^2(2+1)^2}{4}=9$ is true.

Hence assume that $p(k)$ is true. i.e. $p(k): 1^3+2^3+3^3+....+k^3=\frac{k^2(k+1)^2}{4}$.

Now we have to prove $p(k+1)$ is true.

$$\begin{aligned}1^3+2^3+3^3+....+k^3+(k+1)^3 &= \frac{k^2(k+1)^2}{4}+(k+1)^3\\ &= \frac{k^2(k+1)^2+4(k+1)^3}{4}\\ &= \frac{(k+1)^2(k^2+4k+4)}{4}\\ &= \frac{(k+1)^2(k+2)^2}{4}\\ &= \frac{(k+1)^2[(k+1)+1]^2}{4}\end{aligned}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 5: Using mathematical induction, prove that 8^n-3^n is multiple of 5, $n\geq 0, n\in I$.

Let $p(n)$: 8^n-3^n is multiple of 5. i.e. $8^n-3^n=5X$

Now $p(1): 8^1-3^1=5=5\times 1$, multiple of 5.

$p(2): 8^2-3^2=64-9=55=5\times 11$, multiple of 5.

Hence assume that $p(k)$ is true. i.e. $p(k): 8^k-3^k=5X$. …………..(1)

Now we have to prove $p(k+1)$ is true.

$$\begin{aligned}8^{k+1}-3^{k+1} &= 8^k.8-3^k.3\\ &=(5X+3^k).8-3^k.3, \quad \textit{from}(1)\ 8^k=5X+3^k\\ &=5.8X+8.3^k-3^k.3\\ &=5.8X+3^k(8-3)\\ &=5[8X+3^k], \textit{multiple of } 5\end{aligned}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 6: Prove by mathematical induction that $3^{2n}+4^{n+1}$ is divisible by 5, $n\geq 0, n\in I$.

Let $p(n)$: $3^{2n}+4^{n+1}$ is multiple of 5. i.e. $3^{2n}+4^{n+1}=5X$

Now $p(1): 2^{2(1)}+4^{(1)+1}=4+16=20=5\times 4$, divisible by 5.

https://doi.org/10.5281/zenodo.15287608

$p(2):\ 2^{2(2)}+4^{(2)+1}=16+64=80=5\times 16$, multiple of 5.

Hence assume that $p(k)$ is true. i.e. $p(k):\ 3^{2k}+4^{k+1}=5X$. …………..(1)

Now we have to prove $p(k+1)$ is true.

$$\begin{aligned}3^{2(k+1)}+4^{(k+1)+1}&=3^{2k}.3^{2}+4^{k+1}.4\\&=(5X-4^{k+1}).9+4^{k+1}.4,\quad from(1)\ 3^{2k}=5X-4^{k+1}\\&=5.9X-9.4^{k+1}+4^{k+1}.4\\&=5.9X-4^{k+1}(9-4)\\&=5[9X-4^{k+1}],\mathit{divisible\ by}\ 5\end{aligned}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 7: Prove by mathematical induction that $\sum_{r=0}^{n}3^{r}=\frac{3^{n+1}-1}{2}$.

Let $p(n):\ \sum_{r=0}^{n}3^{r}=\frac{3^{n+1}-1}{2}$

$p(n):3^{0}+3^{1}+3^{2}+....+3^{n}=\frac{3^{n+1}-1}{2}$

Now , $p(0):\ 3^{0}=\frac{3^{0+1}-1}{2}=1$.

$p(1):\ 3^{0}+3^{1}=\frac{3^{1+1}-1}{2}=\frac{8}{2}=4$ is true.

Hence assume that $p(k)$ is true. i.e. $p(k):3^{0}+3^{1}+3^{2}+....+3^{k}=\frac{3^{k+1}-1}{2}$

Now we have to prove $p(k+1)$ is true.

$$\begin{aligned}3^{0}+3^{1}+3^{2}+....+3^{k}+3^{k+1}&=\frac{3^{k+1}-1}{2}+3^{k+1}\\&=\frac{3^{k+1}-1+2.3^{k+1}}{2}\\&=\frac{3.3^{k+1}-1}{2}\\&=\frac{3^{(k+1)+1}-1}{2}\end{aligned}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 8: Using mathematical induction, prove that $a^n - b^n$ is multiple of $(a-b)$, $n \in N$.

Let $p(n):\ a^n - b^n$ is multiple of $(a-b)$. i.e. $a^n - b^n = (a-b)X$

Now $p(1):\ a^1 - b^1 = (a-b) = (a-b)\times 1$, multiple of $(a-b)$.

$p(2):\ a^2 - b^2 = (a-b)(a+b) = (a-b)\times X$, multiple of $(a-b)$.

Hence assume that $p(k)$ is true. i.e. $p(k):\ a^k - b^k = (a-b)X$. ....(1)

Now we have to prove $p(k+1)$ is true.

$$a^{k+1} - b^{k+1} = a^k.a - b^k.b$$

$$=\left[(a-b)X + b^k\right].a - b^k.b, \quad from(1)\ a^k = (a-b)X + b^k$$

$$= (a-b).aX + a.b^k - b^k.b$$

$$= (a-b).aX + b^k(a-b)$$

$$= (a-b)[aX + b^k], multiple\ of\ (a-b)$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 9: Show by mathematical induction that $n^3 < 3^n,\ n \geq 4$.

Let $p(n):\ n^3 < 3^n,\ n \geq 4$

Now $p(4):\ 4^3 < 3^4 \quad i.e.\ 64 < 81$, which is true.

Hence assume that $p(k)$ is true. i.e. $p(k):\ k^3 < 3^k,\ k \geq 4$ ....(1)

Now we have to prove $p(k+1)$ is true. i.e. to prove $(k+1)^3 < 3^{k+1}$

$(k+1)^3 = k^3 + 3k^2 + 3k + 1$

Also we have $3k^2 < 4k^2 < k.k^2 = k^3 < 3^k$

$3k^2 < 3^k$ ....(2)

Adding (1) and (2), we have $k^3 + 3k^2 < 3^k + 3^k$ ....(3)

Also $3k + 1 < 3^4$ ....(4)

https://doi.org/10.5281/zenodo.15287608

Adding (3) and (4), we have $k^3+3k^2+3k+1<3^k+3^k+3^k$

$$(k+1)^3<3.3^k$$

$$(k+1)^3<3^{k+1}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 10: Prove by mathematical induction $\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+....+\frac{1}{n.(n+1)}=\frac{n}{n+1}.$

Let $p(n): \frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+....+\frac{1}{n.(n+1)}=\frac{n}{n+1}.$

Now $p(1): \frac{1}{1.2}=\frac{1}{1+1}$ is true.

$$p(2): \frac{1}{1.2}+\frac{1}{2.3}=\frac{2}{2+1}$$

$$\frac{1}{2}+\frac{1}{6}=\frac{2}{3}$$

$$\frac{4}{6}=\frac{2}{3}$$

Hence assume that $p(k)$ is true. i.e. $p(k): \frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+....+\frac{1}{k.(k+1)}=\frac{k}{k+1}.$

Now we have to prove $p(k+1)$ is true.

$$p(k+1): \frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+....+\frac{1}{k.(k+1)}+\frac{1}{(k+1).(k+2)}=\frac{k}{k+1}+\frac{1}{(k+1).(k+2)}$$

$$=\frac{k(k+2)+1}{(k+1).(k+2)}$$

$$=\frac{k^2+2k+1}{(k+1).(k+2)}$$

$$=\frac{(k+1)^2}{(k+1).(k+2)}$$

$$=\frac{(k+1)}{(k+2)}$$

Therefore $p(k+1)$ is true and hence $p(n)$ is true.

Example 11. Use mathematical induction to show that $n\ !\geq 2^{n+1},\quad n=5,6,....$

Let $P(n): \quad n!\geq 2^{n+1}\ n=5,6,....$

https://doi.org/10.5281/zenodo.15287608

Here $P(5)$: $5! \geq 2^{5+1}$ is true

Assume $P(k)$: $k! \geq 2^{k+1}$ is true .... (1)

Claim: $p(k+1)$ is true.

Using (1), We have, $P(k)$: $k! \geq 2^{k+1}$

Multiply both sides by 2, we have

$$2k! \geq 2*2^{k+1},$$

$$(k+1)k! \geq 2^{k+2}, \qquad \text{since } 2 < k+1 \text{ for all } k \geq 5$$

$$(k+1)! \geq 2^{k+2},$$

$p(k+1)$ is true

Hence, by the principle of mathematical induction, $n! \geq 2^{n+!}, \quad n = 5, 6, ...$

Example 12. Using induction principle, prove that $n^3 + 2n$ is divisible by 3.

Let P(n) : $n^3 + 2n$ is divisible by 3.

P(1) : $1 + 2(1) = 3$ is divisible by 3

Assume P(k) : $k^3 + 2k$ is divisible by 3 is true. .... (1)

Claim: $p(k+1)$ is true.

Now, $p(k+1)$: $(k+1)^3 + 2(k+1)$

$$= k^3 + 3k^2 + 3k + 1 + 2k + 2$$

$$= k^3 + 3k^2 + 3k + 2k + 3 = (k^3 + 2k) + 3(k^2 + k + 1) \text{ ....(2)}$$

$k^3 + 2k$ is divisible by 3. $3(k^2 + k + 1)$ is a multiple of 3 and hence divisible by 3.

$P(k+1) = (k^3 + 2k) + 3(k^2 + k + 1)$ is divisible by 3.

$p(k+1)$ is true.

By the principle of mathematical induction, P(n) : $n^3 + 2n$ is divisible by 3.

Example 13. Use mathematical induction to show that $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + ... + \frac{1}{\sqrt{n}} > \sqrt{n}, \quad n \geq 2.$

Let $P(n)$: $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + ... + \frac{1}{\sqrt{n}} > \sqrt{n}, \quad n \geq 2.$

Here $P(2)$: $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} = (1.707) > \sqrt{2} = (1.414)$ is true.

Assume $P(k)$: $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + ... + \frac{1}{\sqrt{k}} > \sqrt{k}$ ...... (1) is true.

Claim: $p(k+1)$ is true.

$$P(k+1):\ \frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+....+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}}$$

$$>\sqrt{k}+\frac{1}{\sqrt{k+1}}=\frac{\sqrt{k}\sqrt{k+1}+1}{\sqrt{k+1}}=\frac{\sqrt{k(k+1)}+1}{\sqrt{k+1}}$$

$$>\frac{\sqrt{k*k}+1}{\sqrt{k+1}}$$

$$>\frac{k+1}{\sqrt{k+1}}=\sqrt{k+1}$$

$$P(k+1)=\sqrt{k+1}$$

Therefore, $P(k+1)$ is true.

By the principle of mathematical induction, $\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+....+\frac{1}{\sqrt{n}}>\sqrt{n}.$

Example 14. Prove by mathematical induction that $6^{n+2}+7^{2n+1}$ is divisible by 43 for all positive integer *n*.

Let P(n) : $6^{n+2}+7^{2n+1}$ is divisible by 43.

Here P(1) is true i.e. 6^3+7^3 is divisible by 43.

Assume that P(k) is true.

$6^{k+2}+7^{2k+1}$ is divisible by 43.

$6^{k+2}+7^{2k+1}=43r$ where r is a positive integer .... (1)

Claim: P(k+1) is true.

To prove $6^{k+3}+7^{2k+3}$ is divisible by 43.

Now

$$6^{k+3}+7^{2k+3}=6*6^{k+2}+7^2*7^{2k+1}$$

$$=6*6^{k+2}+49*7^{2k+1}$$

$$=6*6^{k+2}+6*7^{2k+1}+43*7^{2k+1} \qquad .... (2)$$

$$=6*\left(6^{k+2}+7^{2k+1}\right)+43*7^{2k+1}$$

$6^{k+2}+7^{2k+1}$ is divisible by 43

$43*7^{2k+1}$ is divisible by 43.

Since RHS of equation(2) is a multiple of 43, it is divisible by 43.

$6^{k+3}+7^{2k+3}$ is divisible by 43.

P(k+1) is true.

https://doi.org/10.5281/zenodo.15287608

Example 15: Prove that a positive integers greater than 1 is either a prime number or it can be written as product of prime numbers.

Let the statement is true for $n=2$, because 2 is a prime number.
Assume that the statement is true for all numbers less than $n<k$. i.e. any number less than k is prime or it can be written as product of prime numbers.

Consider the number k.
Case (i): Suppose k is prime, the statement is true for $n=k$.

Case (ii): Suppose k is composite. Then we know that any composite number has two factors other than 1 & k.
Let $k=a\times b$, where $a<k$, $b<k$.
Therefore by our assumption a *and* b can be expressed as product of primes.
Therefore $a=p_1p_2...p_r$ and $b=q_1q_2....q_s$
But $k=ab=p_1p_2...p_rq_1q_2....q_s$, product of primes.

Example 16: Prove that the number of subsets of set having n elements is 2^n.

We know that a null set has 2^0 subsets. Hence $P(0)$ is true.
Now assume that $P(k)$ is true. i.e. any set with k elements has 2^k subsets.

Let A be a set with $k+1$elements. Choose an element $a\in A$.
Now any subset that does not contain a is a subset of $A-\{a\}$.
Therefore there are 2^k subsets of $A-\{a\}$.
Now any subset X of $A-\{a\}$ can be matched up any subset Y of $A-\{a\}\cup\{a\}=A$.
Consequently, there are as many subsets of A that contain a as do not.
Thus there are twice as many subsets of A as there are subsets of $A-\{a\}$.
i.e. number of subsets of A = $2\times$number of subsets of $A-\{a\}$.

$$= 2\times 2^k$$
$$= 2^{k+1}$$

Hence by induction hypothesis, the number of subsets of set having n elements is 2^n.

Example 17: Let m any odd positive integer. Then prove that there exists a positive integer n such that m divides 2^n-1.

Let $m_k=\left(2m_{k-1}+1\right)$ be the sequence of odd positive integers with $m_1=1$.
Let $P(n)$: 2^n-1 is divisible by $m_k=\left(2m_{k-1}-1\right)$ for some k.
$P(1)$: $2^1-1=1$ is divisible by $m_1=1$.
$P(2)$: $2^2-1=3$ is divisible by $m_1=1$ and $m_2=\left(2m_1+1\right)=3$.

https://doi.org/10.5281/zenodo.15287608

$P(3):\ \ 2^3-1=7$ is divisible by $m_1=1$ and $m_3=\left(2m_2+1\right)=7$.

Hence assume that $P(k):\ \ 2^k-1$ is divisible by $m_1=1$ and $m_k=\left(2m_{k-1}+1\right)$.

Therefore $2^k-1=m_k$.

To show that $P(k+1):$ is true.

Consider
$$\begin{aligned}2^{k+1}-1&=2\cdot 2^k-1\\&=2\cdot 2^k-2^k+2^k-1\\&=2^k(2-1)+\left(2^k-1\right)\\&=m_k+1+m_k\\&=2m_k+1\\&=m_{k+1}\end{aligned}$$

i.e. $P(k+1):\ \ 2^{k+1}-1$ is divisible by $m_1=1$ and $m_k=\left(2m_{k-1}+1\right)$.

Therefore $P(n):\ \ 2^n-1$ is divisible by $m_1=1$ and m_k for some k.

Well Ordering Principle

Every non negative set of integers has a smallest element.

Let us prove this statement by mathematical induction. A set containing one element (non negative integer) has a smallest element, namely the element itself.

Assume that the statement is true for a set containing k elements. i.e. a set containing k elements has a smallest element.

Consider a set S with $k+1$ elements. Now remove an element, say 'a' from S . Now the set has k elements and it has a least element, say 'b'.

The smallest of 'a' and 'b' is the smallest element of the set S . Therefore any finite set of non negative integers has a smallest element.

https://doi.org/10.5281/zenodo.15287608

Exercise

Use mathematical induction to show that

1 $1+3+5+.......+(2n-1)=n^2$

2. $1\cdot 2\cdot 3+2\cdot 3\cdot 4+3\cdot 4\cdot 5+.......+n(n+1)(n+2)=\frac{1}{4}n(n+1)(n+2)(n+3)$

3. $\frac{1\cdot 3\cdot 5.....(2n-1)}{2\cdot 3\cdot 4.........(2n)}\leq\frac{1}{\sqrt{n+1}}$ for all natural numbers

4. $1+\frac{1}{2}+\frac{1}{3}+.....+\frac{1}{2^n}\geq 1+\frac{n}{2}$ (or) If H_n denote harmonic numbers, then prove that $H_{2n}\geq 1+\frac{n}{2}$ using mathematical induction.

5. Using mathematical induction, show that $\sum_{r=0}^{n}3^r=\frac{3^{n+1}-1}{2}$.

6. 3^n+7^n-2 is divisible by 8 for $n\geq 1$.

7. $1\square 1!+2\square 2!+3\square 3!+.....+n\square n!=(n+1)!-1$ if $n\geq 1$

8. Show that $F_n\leq 2^n$ for every positive integer n, where $\{F_n\}$ is a Fibonacci sequence.

9. Use mathematical induction to prove the inequality $n<2^n$ for all positive integer n.

10. Use mathematical induction to show that $n!\geq 2^{n+1}$, $n=1,2,3,.......$

11. Prove, by mathematical induction, that $6^{n+2}+7^{2n+1}$ is divisible by 43 for each positive integer n.

Basics of counting

Combinatoric is a branch of discrete mathematics dealing with counting problems. Techniques for counting are important in Computer Science, especially in analysis of algorithms. For example, a computer password, normally contains eight strings consisting of alphabets, numerals and special characters. Suppose a password should contain minimum one special character, one numeral and one capital letter. Then how many such passwords can be generated?. Now the necessity of counting arises.

Principles of counting

The sum rule: If two tasks can be done in m, n ways respectively and if both cannot be done at the same time, (mutually exclusive) then there are $m+n$ ways to do both the works.

Equivalently If there are m different objects in the one set, n different objects in the another set and if the different sets are disjoint, then the number of ways to select an object from one of the 2 sets is $m+n$.
This can be extended to any number tasks.

Example: In how many ways a student can choose a project from the topics given as: Cryptography – 20 titles, Artificial Intelligence – 10 titles, Mobile Apps – 5 titles.

By sum rule, there are $20+10+5=35$ ways to select a project from one of these three lists.

The product rule: A task can be done in two successive steps, first step can be done in m ways and second step can be done in n ways Then the task can be done in $m \cdot n$ ways. This can be extended to any number tasks.

Example: A password consists of two alphabets followed by three digits. (i) How many passwords can be generated. (ii) If first digit is never zero, then how many passwords can be generated? (iii) If no letter or digit is repeated, how many passwords can be generated in both the cases?

If alphabets and digits are repeated	

(i) There are 26 options for alphabets and 10 options for digits. Therefore there are $26\times 26\times 10\times 10\times 10 = 6,76,000$ passwords can be generated.	(ii) There are 26 options for alphabets and 10 options for digits. Since first letter is nonzero digit, there are $26\times 26\times 9\times 10\times 10 = 6,08,400$ passwords can be generated.
(iii) No alphabets and digits are repeated	
Therefore there are $26\times 25\times 10\times 9\times 8 = 4,68,000$ passwords can be generated.	Since first letter is nonzero digit, there are $26\times 25\times 9\times 9\times 8 = 4,21,200$ passwords can be generated.

Example: A password consists of an English alphabet followed by 3 or 4 digits. Find (i) the total number of passwords created (ii) number of passwords in which no digit repeats.

(i) The number of 4 character passwords is $26\times 10\times 10\times 10 = 26,000$ The number of 5 character passwords is $26\times 10\times 10\times 10\times 10 = 2,60,000$ Therefore, by sum rule, total number of passwords is $26,000 + 2,60,000 = 2,86,000$	(ii) The number of 4 character passwords is $26\times 10\times 9\times 8 = 18,720$ The number of 5 character passwords is $26\times 10\times 9\times 8\times 7 = 1,31,040$ Therefore, by sum rule, total number of passwords is $18,720 + 1,31,040 = 1,49,760$

Permutations and Combinations

Permutations	**Combinations**
For $n \geq r \geq 0$, an $r-$ permutation of an n- distinct element set is a linear ordering of r elements of the set. It is denoted by $n\mathrm{Pr} = P(n,r) = n(n-1)(n-2)...\left(n-(r-1)\right) = \dfrac{n!}{(n-r)!}$ Results: $n\mathrm{P}n = P(n,n) = n!,\quad n\mathrm{P}0 = P(n,0) = 1$ Note: It is about the number of arrangements of objects Ordering of objects matters abc, bac, cab are different	For $n \geq r \geq 0$, an unordered selection of $r-$ elements from an n element set is called a combination. It is denoted by $nC\mathrm{r} = C(n,r) = \dfrac{n!}{r!\,(n-r)!}$ Results: $nCn = C(n,n) = 1 \quad \& \quad C(n,r) = C(n,n-r)$ Note: It is about the number of selections of objects Ordering of objects does not matter abc, bac, cab are same

2 permutations of a, b, c are : ab, ba, bc, cb, ac, ca	2 combinations of a, b, c are : $ab,\ bc, ac$
For example, the set of elements a, b and C has six permutations. $3P3 = 3! = 6$. They are $abc, acb, bac, bca, cab, cba$. There are 3 ways to fill first place 2 ways to fill the second place 1 way to fill the third place By product rule, $3\times2\times1 = 3! = 6$ permutations.	For example, all the combinations of the set $\{a, b, c\}$ of sizes 0, 1, 2, 3 are $\{\}$, $\{a\}, \{b\}, \{c\}$, $\{a,b\}, \{b,c\}, \{c,a\}$, $\{a,b,c\}$ $3C0 = 1,\ 3C1 = 3,$ $3C2 = 3,\ 3C3 = 1$

Example: (a) How many different ways can three of the letters of the word VENUS be chosen and written in a row? (b) How many different ways can this be done if the first letter must be E?

(a) Required number of ways is given by the number of 3-permutations of a set of five elements.

$$i.e.\ 5P3 = 60$$

(b) Since the E is used in the first position, there are four letters available to fill the remaining two positions. Hence the number of 2-permutations of a set of four elements is $4P2 = 12$.

Example: (a) In how many of ways can the letters of the word VENUS be arranged? (b) How many of them begin with V and end with S? How many of them do not begin with V but end with S?

(a) The word VENUS consists of 5 letters which can be arranged in $5P5 = 5! = 120$ ways

(b) If V occupies first place and S the last place, then there are 3 letters left to be arranged in 3 places. This can be done in $3P3 = 3! = 6$ ways

(b) If V does not occupy first place but S occupies the last place, then the first place is filled by remaining 3 letters. For the second place, again 3 letters are available including V. The third and fourth place can be filled by 2, 1 ways. Therefore by product rule, required number of arrangements are $3\times3\times2\times1 = 18$ ways

Example: How many 4 digit numbers less than 10,000 can be made with the digits 1, 1, 2, 3, 4, 5, 6, 9?

The number of 4-digit numbers made with the give 8 digits is $= 8P4$. But these numbers include 0 in the 1000th place.

Hence the number of 4-digit numbers $= 8P4 - 7P3$

Similarly the number of 3-digit numbers $= 8P3 - 7P2$

The number of 2-digit numbers $= 8P2 - 7P1$

The number of 1-digit numbers $= 8$

Hence the required number is given by $= (8P4 - 7P3) + (8P3 - 7P2)\ (8P2 - 7P1) + 8$

Permutations with repetition

https://doi.org/10.5281/zenodo.15287608

Theorem: When repetition of n elements contained in a set is permitted in $r-$ permutations, then the number of $r-$ permutations is n^r.

The results of the discussion is summarized below: Number of ways to select(arrange) r objects from n items:

	Selection of distinct objects or Arrangement (Ordered outcome)	Selection of identical objects or Combination (Unordered outcome)
No repetition	$n\text{Pr}$	$nC\text{r}$
Repetition allowed	n^r	$(n+r-1)C\,\text{r}$

Example : Consider the word 'COMPUTER'.
No. of permutations/arrangements of the letters is $8P8=8!$
No. of permutations/arrangements of 5 letters is $8P5=6,720$
No. of permutations/arrangements of 10 letter sequence, repetitions are allowed is $=8^{10}$
Example : How many digits between 1 and 10000 contain exactly one 8 and one nine.

Of these 4 digits(first position 1 cannot be changed), 8 and 9 can be filled in (4×3) ways. The remaining 2 positions can be filled by any of the remaining 8 digits is 8^2 ways. Hence the required number of $(4\times3)\times8^2$

Example : In how many ways can 2 letters be selected from the set $\{a, b, c, d\}$ when repetition is allowed, if (i) the order of the letters matters (ii) the order does not matter?

When the order of letters matters (repetition is allowed)	**When the order of letters does not matter** (repetition is allowed)
The number of possible selections $=4^2=16$ They are aa, ab, ac, ad ba, bb, bc, bd ca, cb, cc, cd da, db, dc, dd	The number of possible selections $=(4+2-1)C2$ $=5C2=10$ They are aa, ab, ac, ad bb, bc, bd cc, cd dd

Example : In how many ways can 2 letters be selected from the set $\{a, b, c, d\}$ when repetition is not allowed, if (i) the order of the letters matters (ii) the order does not matter?

When the order of letters matters (repetition is not allowed)	**When the order of letters does not matter** (repetition is not allowed)
The number of possible selections $=4P2=12$ They are ab, ac, ad $ba, \quad bc, bd$ $ca, cb, \quad cd$ da, db, dc	The number of possible selections $=4C2=6$ They are ab, ac, ad bc, bd cd

Example : How many different bit strings are there of length nine?.

Each of the nine bits can be chosen in two ways (0 or 1).
Therefore, by the product rule there are $2^9 = 512$ bit strings

Example : How many times is the digit 5 written when listing all numbers from 1 to 100,000?

Numbers from 1 to 100,000It is same as numbers between 0 to 99,999. Let all numbers between them are 5-digit sequences (5-digit numbers with leading 0s allowed).

Number of times does a 5 occur in the first position in these 5-digit sequences 10^4. For all five positions the 5 digit sequence containing 5 is 5×10^4.

Example : Twelve students want to place order of different ice creams in a parlour, which has six type of ice creams. Find the number of orders that the twelve students can place.

Number of types of ice cream is $n = 6$.

Each order corresponds to a 12 combination with repetition from a set of 6 objects $(r = 12)$.

So the number of orders $(n+r-1)C\,\mathrm{r} = (6+12-1)C12 = 17C12 = 6{,}188$

Example : Determine the number of solutions of the equation $x_1+x_2+x_3+x_4=32$ where $x_i \geq 0, \forall\, i.$

Consider a solution $x_1=14,\ x_2=8,\ x_3=10,\ x_4=0$. Another set of solution is
$x_1=8,\ x_2=10,\ x_3=0,\ x_4=14$.
Even though the same integers are taken, they are different set of solutions. This can be restated as 32 identical items can be distributed to 4 distinct persons, repetitions allowed.

Hence, the number of solutions $= (4+32-1)C32$

$$= 35C32$$

$$= 6{,}545$$

Result: Consider the following three equivalent statements:

The number of integer solutions of $x_1+x_2+x_3+x_4=32$ where $x_i \geq 0, \forall\, i.$	The number of selections, with repetition, of size r from a collection of size n.	The number of ways r identical objects can be distributed among n distinct containers.

Example : In how many ways 10 identical balls be distributed in 6 boxes?.

From the above result, it is equivalent to finding the nonnegative integer solution of the equation $x_1+x_2+....+x_6=10$.

https://doi.org/10.5281/zenodo.15287608

That number is the number of selections of size 10, with repetition, from a collection of size 6.
i.e. $(6+10-1)C10 = 3,003$ ways.

Example : Determine the number of solutions of the equation $x_1 + x_2 + x_3 + x_4 = 32$ where $x_i > 0, \forall\, i.$

Given $x_i > 0, \forall\, i.$ i.e. $x_i \geq 1, \forall\, i.$

Put $y_i = x_i - 1,$ so that $y_i \geq 0, \forall\, i.$

Then the given equations becomes $y_1 + 1 + y_2 + 1 + y_3 + 1 + y_4 + 1 = 32$

$$y_1 + y_2 + y_3 + y_4 = 28$$

Hence, the number of solutions $= (4+28-1)C28$

$= 31C28$

$= 4,495$

Example : Determine the number of solutions of the equation $x_1 + x_2 + x_3 + x_4 = 32$ where $x_1,\, x_2 \geq 6 \;\&\; x_3,\, x_4 \geq 4.$

Put $y_1 = x_1 - 6,\; y_2 = x_2 - 6,\; y_3 = x_3 - 4,\; y_4 = x_4 - 4,$ then the equation becomes

$y_1 + 6 + y_2 + 6 + y_3 + 4 + y_4 + 4 = 32$ so that $y_i \geq 0, \forall\, i.$

$y_1 + y_2 + y_3 + y_4 = 12$

Hence, the number of solutions $= (4+12-1)C12$

$= 15C12$

$= 455$

Example : Determine the number of solutions of the equation $x_1 + x_2 + x_3 + x_4 = 32$ where $x_1,\, x_2,\, x_3 > 0 \;\&\; 0 < x_4 \leq 20.$

First we find the no. of solutions where $x_1,\, x_2,\, x_3 > 0 \;\&\; x_4 > 20$

Put $y_1 = x_1 - 1,\, y_2 = x_2 - 1,\; y_3 = x_3 - 1,\; \&\; y_4 = x_4 - 21,$ then the equation becomes

$y_1 + 1 + y_2 + 1 + y_3 + 1 + y_4 + 21 = 32$ so that $y_i \geq 0, \forall\, i.$

$y_1 + y_2 + y_3 + y_4 = 8$

Hence, the number of solutions $= (4+8-1)C8$

$= 11C8$

$= 165$

https://doi.org/10.5281/zenodo.15287608

No. of solutions where $x_1, x_2, x_3 > 0$ & $0 < x_4 \le 20$ = (No. of solutions where $x_1, x_2, x_3, x_4 \ge 0$) –

(No. of solutions where $x_1, x_2, x_3 > 0$ & $x_4 > 20$)

$= 6,545 - 165$

$= 6,380$

Example : Determine the number of solutions of the equation $x_1 + x_2 + x_3 + x_4 < 12$ where $x_1, x_2, x_3, x_4 \ge 0$.

Consider the equality form of the given inequality as $x_1 + x_2 + x_3 + x_4 + x_5 = 12$ where $x_5 \ge 1$.

Put $y_5 = x_5 - 1$, then the equation becomes $x_1 + x_2 + x_3 + x_4 + y_5 + 1 = 12$ so that $x_1, x_2, x_3, x_4, y_5 \ge 0$

$x_1 + x_2 + x_3 + x_4 + y_5 = 11$

Hence, the number of solutions $= (7 + 11 - 1)C11$

$= 17C11$

$= 17C6$

$= 12,376$

Restricted Cases

Restricted Permutations	Restricted Combinations
The number of permutations of n different objects taken r at a time in which k particular objects do not occur is $(n-k)\mathrm{Pr}$	The number of combinations of n different objects taken r at a time in which k particular objects are always occur is $(n-k)C(\mathrm{r}-k)$
The number of permutations of n different objects taken r at a time in which k particular objects are always occur is $(n-k)\mathrm{P}(\mathrm{r}-k) \times rPk$	The number of combinations of n different objects taken r at a time in which k particular objects do not occur is $(n-k)C\mathrm{r}$

Example: In how many ways a team of 10 members be chosen out of a batch of 15 students? How many of them will (a) include a particular student (b) exclude a particular student?

Here $n = 15,\ r = 10,\ k = 1$

(a) Number of ways of selecting a team of 10 members out of 15 is $= 15C10$

(b) Number of ways in which a particular player is included is $= 14C9$

(c) Number of ways in which a particular player is excluded is $= 14C10$

Circular Permutation

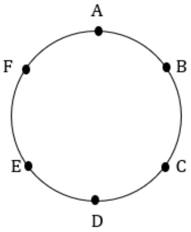
If the objects are arranged in a circle, we get circular permutation. Number of circular permutations of n objects is $(n-1)!$. If clockwise and counter clockwise arrangements are considered as same, then the number of permutations is $\frac{1}{2}(n-1)!$.

Example: If 6 people are seated about a round table, how many different circular arrangements are possible?

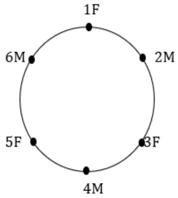
In the group, 3 are male and 3 are female, then how many arrangements do the sexes alternate?

https://doi.org/10.5281/zenodo.15287608

Let A, B, C, D, E, F be the 6 people. If one permutation is obtained from the other by rotation, they are considered as same. Therefore required number of circular arrangements is $(6-1)!=5!=120$



Note that rotation does not alter the circular arrangement.
Assume that a female occupies position1.
Positions 2, 4, 6 must be occupied by 3 male and there are $3P3=3!=6$ ways.
Positions 3, 5 must be occupied by the remaining female in $2P2=2!=2$ ways.
Therefore total number of such a circular arrangements $=6\times 2=12$



OR

Three male be seated along the round table in $(3-1)!=2!$ ways. Between any two male let a female be seated. Hence all 3 females can be seated in 3 intermediate places in $3P3=3!$ ways.
$\therefore$ by product rule required number of arrangements is $2!\times 3!=12$

Example: Find the number of ways in which 10 different beads can be arranged to form a chain.

This is a circular permutation with clockwise and counter clockwise arrangements are considered as same. Therefore required number of arrangements is $\frac{1}{2}(10-1)!=\frac{9!}{2}$.

Theorem: The number of different permutations of n objects which include n_1 identical objects of type I, n_2 identical objects of type II,………. and n_k identical objects of type K is equal to $\frac{n!}{n_1!\cdot n_2!\ldots n_k!}$ where $n_1+n_2+\ldots+n_k=n$.

Example: Consider 3-permutations of the three alphabets a, b, c.

The $3!$ permutations are $abc, acb, bac, bca, cab, cba$.
If b, c is replaced by β, then the permutations becomes $a\beta\beta, a\beta\beta, \beta a\beta, \beta\beta a, \beta a\beta, \beta\beta a$ which are not different.
Then the number of different permutations of 3 letters in which 2 are identical (type I) and 1 letter is (type II) is equal to $\frac{3!}{2!\cdot 1!}=3$. They are $a\beta\beta, \beta\beta a, \beta a\beta$.

Example: How many permutations are there on the word "MALAYALAM"?

Total number of letters 9 in which M occurs 2 times, A occurs 4 times, L occurs 2 times, Y occur 1 time. Hence there are $\frac{9!}{2!\times 4!\times 2!}=$ permutations on this word.

https://doi.org/10.5281/zenodo.15287608

Example: How many positive integers can be formed using the digits 3, 4, 4, 5, 5, 6, 7, whose value is above 50,00,000.

The first place must be occupied by the digits 5, 6 or 7.
When 5 becomes the first place, the remaining six places are to filled by the digits 3, 4, 4, 5, 6, 7.
Therefore required no. of such numbers $= \frac{6!}{2!}$ (digit 4 occurs twice)
$= 360$

When 6 becomes the first place, the remaining six places are to filled by the digits 3, 4, 4, 5, 5, 7.
Therefore required no. of such numbers $= \frac{6!}{2! \times 2!}$ (digit 4, 5 occurs twice)
$= 180$

When 7 becomes the first place, the remaining six places are to filled by the digits 3, 4, 4, 5, 5, 6.
Therefore required no. of such numbers $= \frac{6!}{2! \times 2!}$ (digit 4, 5 occurs twice)
$= 180$

Therefore No. of numbers exceeding 50,00,000 = 360 + 180 + 180 = 720

Example: How many bits of string of length 10 contain

i. exactly four 1's ii. at most four 1's
iii. at least four 1's iv. an equal number of 0's and 1's

This is permutation with repetition. Hence number of different permutations are $\frac{n!}{n_1! \cdot n_2! \ldots n_k!}$.

(i) The 10 bit string contains exactly four 1's and six 0's
Therefore required bit strings $= \frac{10!}{4! \times 6!} = 210$ ways

(iii) The 10 bit string contains at most four 1's
(four 1's and six 0's) or (three 1's and seven 0's) or (two 1's and eight 0's) or (one 1's and nine 0's) or (no 1's and ten 0's)
Therefore required bit strings $= \frac{10!}{4! \times 6!} + \frac{10!}{3! \times 7!} + \frac{10!}{2! \times 8!} + \frac{10!}{1! \times 9!} + \frac{10!}{0! \times 10!} = 386$ ways

(iii) The 10 bit string contains at least four 1's
(four 1's and six 0's) or (five 1's and five 0's) or (six 1's and four 0's) or (seven 1's and three 0's) or (eight 1's and two 0's) or (nine 1's and one 0's) or (ten 1's and no 0's)
Therefore required bit strings $= \frac{10!}{4! \times 6!} + \frac{10!}{5! \times 5!} + \frac{10!}{6! \times 4!} + \frac{10!}{7! \times 3!} + \frac{10!}{8! \times 2!} + \frac{10!}{9! \times 1!} + \frac{10!}{10! \times 0!} = 848$ ways

(iv) The 10 bit string contains an equal number of 0's and 1's (i.e. five 1's and 0's)

Therefore required bit strings $=\dfrac{10!}{5!\times 5!}=252$ ways

Problems on Permutations

Example: How many permutations can be made out of the letters of the word "Basic"? How many of these (1) Begin with B? (2) End with C? (3) B and C occupy the end places?

The given string contains 5 letters.

(1) Since all permutations (words) must begin with B, the remaining 4 letters can be arranged in $4P4=4!$ ways. Therefore total number of permutations with B as the starting letter is $4!=24$.	(2) Since all permutations (words) must end with C, the remaining 4 letters can be arranged in $4P4=4!$ ways. Therefore total number of permutations with C as the end letter is $4!=24$.	(3) Since all permutations (words) must begin with B and end with C, the remaining 3 letters can be arranged in $3P3=3!$ ways. Therefore total number of permutations with B as the starting letter is $3!=6$.

Example: If repetitions are not allowed,

(i) How many four digit numbers can be formed from the digits 1, 2, 4, 5, 7 and 9?
(ii) How many of these numbers are less than 5000?
(iii) How many of these numbers are odd?
(iv) How many of the numbers contain both the digits 2 and 7?

(i)

Position 1 can be filled by 6 numbers	Position 2 can be filled by 5 numbers	Position 3 can be filled by 4 numbers	Position 4 can be filled by 3 numbers

Therefore number of 4-permutations of 6-numbers = $6P4=6\times5\times4\times3=360$

(ii)

Position 1 can be filled by three ways by the numbers1, 2, 4	Position 2 can be filled by 5 numbers	Position 3 can be filled by 4 numbers	Position 4 can be filled by 3 numbers

Therefore number of 4-digit numbers less than 5000 = $3\times5P3=3\times\left(5\times4\times3\right)=180$

(iii) The required 4-digit number is odd, the last digit must be 1, 5, 7 and 9.

Position 1 can be filled by 5 numbers	Position 2 can be filled by 4 numbers	Position 3 can be filled by 3 numbers	Position 4 can be filled by 4 ways by the numbers 1, 5, 7, 9

Therefore number of 4-digit odd numbers $=5P3\times4=\left(5\times4\times3\right)\times4=240$

(iv)

The digits 2 and 7 can occupy any two of the 4 places. Therefore there are $4P2=4\times3=12$ ways	The remaining two places can be occupied by the numbers 1, 4, 5, 9. Therefore there are $4P2=4\times3=12$ ways

Therefore number of 4-digit numbers containing 2 and 7 = $4P2\times4P2=12\times12=144$

Example: There are 7 boys and 8 girls.	
(i) In how many ways can all the 7 boys and 8 girls sit in a row?	There are 15 persons(arranged in 15 places) Therefore number of ways $=15P15=15!$ ways
(ii) In how many ways can they sit in a row such that two boys can't sit together?	The 8 girls can be seated in $8P8=8!$ ways There are 8 places for 7 boys $\therefore$ The 7 boys can be seated in $8P7$ ways Hence required number of $=8!\times 8P7$
(ii) In how many ways can they sit in a row if the boys are to sit together?	Consider boys are one unit and hence there are $1+8=9$ persons. These 9 persons can be arranged in a row $9!$ ways. In any one of these $9!$ ways, the 7 boys can be arranged among themselves in $7!$ ways. Hence required number of ways $=9!\times 7!$
(iii) In how many ways can they sit in a row if the boys are to sit together and the girls are to sit together?	Consider boys are one unit and girls are another unit. These 2 units can be arranged in $2!$ ways. In any one of these $2!$ ways, the 7 boys can be arranged among themselves in $7!$ ways and the girls among themselves in $8!$ ways. Hence required number of ways $=2!\times 8!\times 7!$
(iv) In how many ways can they sit in a row if just the boys are to sit together?	No. of ways in which boys only sit together = (No. of ways in which boys sit together) – (No. of ways in which boys sit together and girls sit together) $=(9!\times 7!)-(2!\times 8!\times 7!)$

Example: A collection of eight books consists of two books on English, three books on Mathematics, and three books on Science.

(a) How many ways can the books be arranged on a shelf so that all books on a single subject are together?

(b) How many ways can the books be arranged on a shelf so that the three books on Mathematics are together?

(c) How many ways can the books be arranged on a shelf so that the two books on English occur at the right end of the arrangement?

(a) Let consider each subject books are considered together. Therefore there are 3 bunch of books. They can be arranged in $3P3=3!$ ways.

Among themselves, English books can be arranged in $2P2=2!$ ways.

Among themselves, Mathematics books can be arranged in $3P3=3!$ ways.

Among themselves, Science books can be arranged in $3P3=3!$ ways.

Therefore by multiplication rule, total number of arrangements $=3!\times(2!\cdot 3!\cdot 3!)=432$

(b) If Mathematics books are considered together, then there are 6 books. These 6 books can be arranged in $6P6=6!$ ways. In this arrangements, Mathematics books among themselves can be arranged in $3P3=3!$ ways.

Therefore by multiplication rule, total number of arrangements $=6!\times(3!)=4,320$

(c) If English books are considered together, then there are 6 books. These 6 books can be arranged in $6P6 = 6!$ ways, in which English books are placed at the right end. In this arrangements, English books among themselves can be arranged in $2P2 = 2!$ways.

Therefore by multiplication rule, total number of arrangements $= 6! \times (2!) = 1,440$

Example : A magnetic tape contains a collection of 5 lakh strings made up of four or fewer number of English letters. Can all the strings in the collection be distinct?

Total number of strings with four or fewer number of English letters

$$26P4 + 26P3 + 26P2 + 26P1 = (24\times 23\times 22\times 21) + (24\times 23\times 22) + (24\times 23) + (24)$$

$$= (24\times 23\times 22\times 21) + (24\times 23\times 22) + (24\times 23) + (24)$$

$$= 2,55,024 + 12,144 + 552 + 24$$

$$= 2,67,704$$

There can be only $2,67,704$ distinct strings. Since the magnetic tape contains 5 lakh strings, we conclude that the collection of the strings are not distinct.

Example : How many permutations of the letters ABCDEFGH contain the string ABC?

If the letter group ABC is treated as a unit, then there are effectively only six objects that are to be arranged in a row. Therefore there are $6! = 720$ permutations.

Problems on Combinations

Example : In how many ways a committee of 6 persons be formed from 7 men and 5 women so as to include 3 women at least?

The committee may consists of

(i) 3 men and 3 women in $7C3 \times 5C3 = 35\times 10 = 350$ ways

(ii) 2 men and 4 women in $7C2 \times 5C4 = 21\times 5 = 105$ ways

(iii) 1 man and 5 women in $7C1 \times 5C5 = 7\times 1 = 7$ ways

By sum rule, the number of possible ways of forming the committee $= 350 + 105 + 7 = 462$ ways.

Example: There are 7 men and 8 women. A committee should be formed with 6 members.

How many number of ways a committee can be formed with no gender partiality?(they can be of any sex)	$15C6=\frac{15\cdot14\cdot13\cdot12\cdot11\cdot10}{1\cdot2\cdot3\cdot4\cdot5\cdot6}=5005$
How many number of ways a committee with a captain, can be formed with no gender partiality?	A captain can be chosen in 15 ways The other 6 members can be chosen from 14 members $14C6=\frac{14\cdot13\cdot12\cdot11\cdot10\cdot9}{1\cdot2\cdot3\cdot4\cdot5\cdot6}=3003$ $\therefore$ total number of ways to select a team with a captain is $15\times3003=45045$
How many number of ways a committee can be formed with male members?	$7C6=7C1=7$
How many number of ways a committee can be formed with female members?	$8C6=8C2=\frac{8\cdot7}{1\cdot2}=28$
How many number of ways a committee can be formed with 4 male and 2 female members?	$7C4\times8C2=\frac{7\cdot6\cdot5\cdot4}{1\cdot2\cdot3\cdot4}\times\frac{8\cdot7}{1\cdot2}=980$
How many number of ways a committee can be formed with all of them are same sex?	i.e. all the 6 are either male or female $7C6+8C6=7C1+8C2=7+\frac{8\cdot7}{1\cdot2}=35$
How many number of ways a committee can be formed with at least 5 women?	(5W, 1M) or (6W, 0M) $(7C1\times8C5)+(7C0\times8C6)=(7\times40)+(1\times24)=304$
How many number of ways a committee can be formed with at most 2 men?	(0M, 6W) or (1M, 5W) or (2M, 4W) $(7C0\times8C6)+(7C1\times8C5)+(7C2\times8C4)$ $=(1\times24)+(7\times56)+(21\times70)=1886$

Example : Which regular polygon has the same number of diagonals as sides?

A regular polygon with n sides has n vertices. Any two vertices give either a side or a diagonal. Therefore the total sides and diagonals will be $nC2$. There are n sides.

Therefore number of diagonals is $=nC2-n$

$$=\frac{n(n-1)}{2}-n$$

$$=\frac{n(n-3)}{2}$$

https://doi.org/10.5281/zenodo.15287608

But given that $\frac{n(n-3)}{2}=n$

$$n^2-3n=2n$$
$$n^2-5n=0$$
$$n(n-5)=0$$

Since n cannot be 0, we have $n=5$. Thus the pentagon is the only polygon with the same number of diagonals as sides.

Example: How many number of arrangements are there on the word "JAMMAIASSUU"? How many of these arrangements have no adjacent to A'S?

Total number of arrangements of the letters of the given word $=\frac{11!}{3!\cdot 2!\cdot 2!\cdot 2!\cdot 1!\cdot 1!}=8,31,600$

Total number of arrangements of the letters of the word, omitting $A=\frac{8!}{2!\cdot 2!\cdot 2!\cdot 1!\cdot 1!}=5,040$

Consider one of the permutation, omitting A is *J * M * M * I * S * S * U * U *.
So, three A's can be inserted in any of the place nine places i.e. $9C3=84$ ways.
Therefore by product rule, there are $5,040\times 84=4,23,360$ arrangements that have no two A's are adjacent.

Example : Prove that if n and k are positive integers with $n=2k$, then $\frac{n!}{2^k}$ is an integer.

Consider the symbols $a_1, a_1, a_2, a_2, a_3, a_3,\ldots\ldots, a_k, a_k$. Here k symbols are repeated twice. Therefore $n=2k$.

The number of ways in which all these $n=2k$ symbols are arranged $=\frac{n!}{2!\times 2!\times 2!\times\ldots\ldots\times 2!(k\,times)}$

$=\frac{n!}{2^k}$, an integer.

Binomial Theorem

Consider the binomial expansion $(x+y)^n=nC0x^ny^0+nC1x^{n-1}y^1+nC2x^{n-2}y^2+\ldots.+nCnx^0y^n$. Here the coefficients are called binomial coefficients which are r combination from the set of n elements.

$$(x+y)^n=\sum_{r=0}^{n} nCrx^{n-r}y^6 \text{ and } (x-y)^n=\sum_{r=0}^{n}(-1)^r nCr\,x^{n-r}y^6$$

Example: Find the coefficient of x^5y^8 in $(x+y)^{13}$.

$$(x+y)^{13}=13C0x^{13}y^0+13C1x^{12}y^1+13C2x^{11}y^2+\ldots.+13C8x^5y^8+\ldots..+13C13x^0y^{13}$$

Therefore the coefficient of x^5y^8 is $13C18$.

https://doi.org/10.5281/zenodo.15287608

Example: Show that if n and k are positive integers then $\binom{n+1}{k}=(n+1)\binom{n}{k-1}/k$. Use this identity to construct an inductive definition of the binomial coefficients.

By definition

$$\begin{aligned}
\binom{n+1}{k} &= \frac{(n+1)!}{k!(n+1-k)!} \\
&= \frac{(n+1)\cdot n!}{k\cdot(k-1)!(n+1-k)!} \\
&= \frac{(n+1)}{k}\frac{n!}{(k-1)!(n-(k-1))!} \\
&= \frac{(n+1)}{k}\binom{n}{k-1}
\end{aligned}$$

Theorem: Prove that $\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$

Consider $R.H.S=\binom{n}{r-1}+\binom{n}{r}$

$$\begin{aligned}
&= \frac{n!}{(r-1)!(n-r+1)!}+\frac{n!}{r!(n-r)!} \\
&= \frac{r\cdot n!}{r\cdot(r-1)!(n-r+1)(n-r)!}+\frac{n!(n-r+1)}{r!(n-r+1)(n-r)!} \\
&= \frac{r\cdot n!}{r!\cdot(n-r+1)!}+\frac{n!(n-r+1)}{r!(n-r+1)!} \\
&= \frac{n!\cdot(r+n-r+1)}{r!(n-r+1)!} \\
&= \frac{(n+1)!}{r!(n+1-r)!} \\
&= \binom{n+1}{r} \\
&= L.H.S.
\end{aligned}$$

EXERCISE

1. How many different words are there in the word MATHEMATICS?

2. How many different words are there in the word MASSASAUGA?

3. How many permutations are there in the word MISSISSIPPI?

4. In how many ways can all the letters in MATHEMATICAL be arranged?

5. A box contains six white balls and five red balls. Fid the number of ways four balls can be drawn from the box if (1) they can be any color (2) two must be white and two red (3) they must all are of the same color.

https://doi.org/10.5281/zenodo.15287608

6. From a club consisting of six men and seven women, in how many ways we select a committee of (1) three men and four women (2) four person which has at least one women (3) four person that has at most one man (4) four persons that has children of both sexes?

7. There are 6 men and 5 women in a room. Find the number of ways four persons can be drawn from the room if (1) they can be male or female (2) two must be men and two women (3) they must all are of the same sex.

8. Suppose there are 9 faculty members in the mathematics department and 11 in the computer science department. How many ways are there to select a committee to develop a discrete mathematics course at a school if the committee is to consist of three faculty members from the mathematics department and four from the computer science department?

9. From a club consisting of 6 men and 7 women, in how many ways can we select a committee of 4 persons that has at most one woman?

10. How many solutions does the equation, $x_1 + x_2 + x_3 = 11$ have, where x_1, x_2 and x_3 are non-negative integers?.

11. Find the coefficient of $x^{10}y^{15}$ in $(x+y)^{25}$.

Pigeonhole Principle

If n pigeons are accommodated in m pigeon-holes and $n > m$ then at least one pigeonhole will contain two or more pigeons.

Generalization: If n pigeons are accommodated in m pigeon-holes and $n > m$ then at least one of the pigeonholes must contain at least $\left\lfloor \frac{n-1}{m} \right\rfloor + 1$ pigeons.

Note: If x is a real variable, the floor of x, denoted by $\lfloor x \rfloor$ is the greatest integer less than or equal to x.

https://doi.org/10.5281/zenodo.15287608

Example: If seven colors are used to paint 50 bicycles, then show that at least eight bicycles will be the same color.

Here $n=50$ and $m=7$. By generalized pigeonhole principle, $\left\lfloor \frac{50-1}{7} \right\rfloor +1=8$ bicycles will have the same color.

Example: Among 200 people, how many of them were born on the same month?

Here $n=200$ and $m=12$. By generalized pigeonhole principle, $\left\lfloor \frac{200-1}{12} \right\rfloor +1=17$ peoples were born in the same month.

Example: Prove that in a group of six people, at least three must be mutual friends or at least three must be mutual strangers.

Let *Ram* be one of the 6 people. Let the remaining 5 peoples be accommodated in two rooms namely, 'Friends to *Ram*' and 'Strangers to *Ram*'.
Let us treat the 5 people as 5 pigeons and 2 rooms as 2 pigeonholes. By the generalized pigeonhole principle, one of the room must contain $\left\lfloor \frac{5-1}{2} \right\rfloor +1=3$ people.

In the three people, if any two are mutually friends, then together with *Ram*, there is a set of 3 mutual friends. If no two are mutually friends, then these 3 are mutual strangers.

Example : Find the minimum number of students in a class to be sure that four out of them are born in the same month.

Consider each month as a pigeonhole, then $m=12$.
We have to find such that $\left\lfloor \frac{n-1}{m} \right\rfloor +1=4$.

$$\left\lfloor \frac{n-1}{12} \right\rfloor =3$$

$$n=37$$

Example: Show that among any group of six (not necessarily consecutive) integers there are two integers with the same remainder when divided by 5.

There are only 5 possible reminders when an integer is divided by 5, namely 0, 1, 2, 3, 4.

By Pigeon hole principle if we have 6 reminders then at least 2 must be same.

https://doi.org/10.5281/zenodo.15287608

Example: A bank requires customers to choose a four-digit code to use with an ATM card. The code must consist of two English alphabets in the first two positions and two numerals in the other two positions. The bank has 70,000 customers. Show that at least two customers choose the same four-digit code.

By multiplication rule the possibility for number of distinct codes is

$$\begin{aligned} &= \text{No. of choices of first alphabet} \times \text{No. of choices of second alphabet} \\ &\quad \text{No. of choices of first digit} \times \text{No. of choices of second digit} \\ &= 26 \times 26 \times 10 \times 10 \\ &= 67,600 \end{aligned}$$

Since there are 75,000 customers and only 67,600 codes, the Pigeon-Hole Principle implies that at least two of the customers choose the same code.

Example: If n pigeonholes are occupied by $kn+1$ pigeons, where k is a positive integer, prove that at least one pigeonhole is occupied by $k+1$ or more pigeons. Hence find the minimum number of m integers to be selected from $S = \{1,2,3,4,5,6,7,8,9\}$ so that the sum of two of the m integers are even.

Suppose one pigeonhole is not occupied by $k+1$ or more pigeons, then each pigeonhole contains at most k pigeons. Therefore, the total number of pigeons occupying the n pigeonholes is at most kn.

But there are $kn+1$ pigeons, which is a contradiction. Therefore, at least one pigeonhole is occupied by $k+1$ or more pigeons.

We know that sum of two even integers or two odd integers is even. Divide the given set into two subsets as $S_o = \{1,3,5,7,9\}$, $S_e = \{2,4,6,8\}$. Let them be pigeonholes. Therefore $n=2$.

Now at least two numbers must be chosen from the set S_o or S_e.
i.e. at least one pigeonhole must contain 2 pigeons. i.e. $k+1=2$ i.e. $k=1$.

Therefore the minimum number of pigeons required (minimum number of integers selected) is $kn+1=3$.

Example: How many cards must be selected from a standard deck of 52 cards (4 different suits of equal size) to guarantee that at least three cards of the same suit are chosen?

Suppose there are 4 boxes, one for each suit ($m=4$ pigeonholes). Now cards are selected and placed in the respective boxes reserved for that suit. Suppose n cards (pigeons) are selected to ensure at least 3 cards of the same suit. Then by general pigeonhole principle

$$\left\lfloor \frac{n-1}{m} \right\rfloor + 1 \geq 3$$

$$\left\lfloor \frac{n-1}{4} \right\rfloor + 1 \geq 3$$

https://doi.org/10.5281/zenodo.15287608

$$\frac{n-1}{4} \geq 2$$

$n \geq 9$, minimum 9 cards must be chosen.

Example: What is the maximum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade if there are five possible grades A, B, C, D and F?

Given that only 5 grades ($m=5$ pigeonholes) are available. Suppose n students (pigeons) are required to ensure at least 6 will receive the same grade. Then by general pigeonhole principle

$$\left\lfloor \frac{n-1}{m} \right\rfloor + 1 \geq 6$$

$$\left\lfloor \frac{n-1}{5} \right\rfloor + 1 \geq 6$$

$$\frac{n-1}{5} \geq 5$$

$n \geq 26$, minimum 26 students are required.

Example: What is the maximum number of students required in a discrete mathematics class to be sure that at least six will receive the same grade if there are five possible grades A, B, C, D and F?

Given that only 5 subjects ($m=5$ pigeonholes) are available. Suppose n students (pigeons) are required to ensure at least 5 students belongs to the same subject. Then by general pigeonhole principle

$$\left\lfloor \frac{n-1}{m} \right\rfloor + 1 \geq 5$$

$$\left\lfloor \frac{n-1}{5} \right\rfloor + 1 \geq 5$$

$$\frac{n-1}{5} \geq 4$$

$n \geq 21$, minimum 21 students are required.

Principle of Inclusion and Exclusion

When two jobs can be done at the same time we cannot use the sum rule. Because the addition leads to an overcount since the ways to do both jobs are counted twice. Therefore we add the number of ways to do each of the two jobs and then subtract the number of ways to do both jobs. This technique is known as the principle of inclusion – exclusion.

If A and B are finite subsets of a finite universal set U, then $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

If A, B and C are finite subsets of a finite universal set U, then

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(C \cap A) + n(A \cap B \cap C)$$

https://doi.org/10.5281/zenodo.15287608

This principle can be extended to any number of finite subsets.

Example: Find the number of integers between 1 and 500 that are not divisible by any of the integers 2, 3 and 5.

Let A, B, C be the set of integers that lies between 1 and 500 both inclusive and that are divisible by 2, 3 and 5 respectively.

Therefore $|A| = \left\lfloor \frac{500}{2} \right\rfloor = 250$, $|B| = \left\lfloor \frac{500}{3} \right\rfloor = 166$, $|C| = \left\lfloor \frac{500}{5} \right\rfloor = 100$

$$|A \cap B| = \left\lfloor \frac{500}{2\times 3} \right\rfloor = 83,\ |B \cap C| = \left\lfloor \frac{500}{3\times 5} \right\rfloor = 33,\ |A \cap C| = \left\lfloor \frac{500}{2\times 5} \right\rfloor = 50$$

$$|A \cap B \cap C| = \left\lfloor \frac{500}{2\times 3\times 5} \right\rfloor = 16$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

$$= (250 + 166 + 100) - (83 + 50 + 33) + (16) = 366$$

Therefore total number of integers not divisible by 2, 3, 5 = 500 – (no. of integers divisible by 2, 3, 5)
= 500 – 366 = 134

Example: Find the number of integers between 1 and 250 both inclusive that are divisible by any of the integers 2, 3, 5 and 7.

Let A, B, C, D be the set of integers that lies between 1 and 250 both inclusive and that are divisible by 2, 3, 5, 7 respectively.

Therefore $|A| = \left\lfloor \frac{250}{2} \right\rfloor = 125$, $|B| = \left\lfloor \frac{250}{3} \right\rfloor = 83$, $|C| = \left\lfloor \frac{250}{5} \right\rfloor = 50$, $|D| = \left\lfloor \frac{250}{7} \right\rfloor = 35$

$$|A \cap B| = \left\lfloor \frac{250}{2\times 3} \right\rfloor = 41,\ |B \cap C| = \left\lfloor \frac{250}{3\times 5} \right\rfloor = 16,\ |C \cap D| = \left\lfloor \frac{250}{5\times 7} \right\rfloor = 7,\ |A \cap D| = \left\lfloor \frac{250}{2\times 7} \right\rfloor = 17$$

$$|A \cap B \cap C| = \left\lfloor \frac{250}{2\times 3\times 5} \right\rfloor = 8,\ |A \cap B \cap D| = \left\lfloor \frac{250}{2\times 3\times 7} \right\rfloor = 5,\ |B \cap C \cap D| = \left\lfloor \frac{250}{3\times 5\times 7} \right\rfloor = 2, |A \cap C \cap D| = \left\lfloor \frac{250}{2\times 5\times 7} \right\rfloor = 3$$

$$|A \cap B \cap C \cap D| = \left\lfloor \frac{250}{2\times 3\times 5\times 7} \right\rfloor = 1$$

$$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D| - |A \cap B| - |B \cap C| - |C \cap D| - |A \cap D| - |A \cap C| - |B \cap D|$$

$$+|A\cap B\cap C|+|A\cap B\cap D|+|B\cap C\cap D|+|A\cap C\cap D|-|A\cap B\cap C\cap D|$$

$$=(125+83+50+35)-(41+25+17+16+11+7)+(8+5+3+2)-1=193$$

Example: Determine the number of positive integers n, $1\le n\le 1000$ that are divisible by 5, but not by 7 and not by 9.

Let A, B, C be the set of integers that lies between 1 and 1000 both inclusive and that are divisible by 5, 7 and 9 respectively.

Therefore $|A|=\left\lfloor \frac{1000}{5} \right\rfloor=200$, $|B|=\left\lfloor \frac{1000}{7} \right\rfloor=142$, $|C|=\left\lfloor \frac{1000}{9} \right\rfloor=111$

$|A\cap B|=\left\lfloor \frac{1000}{5\times 7} \right\rfloor=28$, $|B\cap C|=\left\lfloor \frac{1000}{7\times 9} \right\rfloor=15$, $|A\cap C|=\left\lfloor \frac{1000}{5\times 9} \right\rfloor=22$

$|A\cap B\cap C|=\left\lfloor \frac{1000}{5\times 7\times 9} \right\rfloor=3$

The number of integers divisible by all the numbers (5, 7, 9) $=3$

$|A\cap B|-|A\cap B\cap C|=28-3=25$, No. of integers divisible by 5 and 7 but not by all the three

$|A\cap C|-|A\cap B\cap C|=22-3=19$, No. of integers divisible by 5 and 9 but not by all the three

$|A|-25-19=200-25-19=153$, No. of integers divisible by 5 but not by 7 and not by 9.

Example: Determine the number of positive integers n, $1\le n\le 2000$ that are not divisible by 2, 3 or 5, but are divisible by 7.

Let A, B, C, D be the set of integers that lies between 1 and 2000 both inclusive and that are divisible by 2, 3, 5, 7 respectively.

Therefore $|A|=\left\lfloor \frac{2000}{2} \right\rfloor=1000$, $|B|=\left\lfloor \frac{2000}{3} \right\rfloor=666$, $|C|=\left\lfloor \frac{2000}{5} \right\rfloor=400$, $|D|=\left\lfloor \frac{2000}{7} \right\rfloor=285$

$|A\cap B|=\left\lfloor \frac{2000}{2\times 3} \right\rfloor=333$, $|B\cap C|=\left\lfloor \frac{2000}{3\times 5} \right\rfloor=133$, $|C\cap D|=\left\lfloor \frac{2000}{5\times 7} \right\rfloor=57$, $|A\cap D|=\left\lfloor \frac{2000}{2\times 7} \right\rfloor=142$

$|A\cap B\cap C|=\left\lfloor \frac{2000}{2\times 3\times 5} \right\rfloor=66$, $|A\cap B\cap D|=\left\lfloor \frac{2000}{2\times 3\times 7} \right\rfloor=47$

$|B\cap C\cap D|=\left\lfloor \frac{2000}{3\times 5\times 7} \right\rfloor=19$, $|A\cap C\cap D|=\left\lfloor \frac{2000}{2\times 5\times 7} \right\rfloor=28$

$$|A\cap B\cap C\cap D| = \left\lfloor \frac{2000}{2\times 3\times 5\times 7} \right\rfloor = 9$$

Also the number of integers divisible by all 2, 3, 5 and 7 is $=9$

$|A\cap B\cap D| - |A\cap B\cap C\cap D| = 47-9 = 38$, No. of integers divisible by 2, 3, 7 but not by all (2, 3, 5, 7)

$|B\cap C\cap D| - |A\cap B\cap C\cap D| = 19-9 = 10$, No. of integers divisible by 3, 5, 7 but not by all (2, 3, 5, 7)

$|A\cap C\cap D| - |A\cap B\cap C\cap D| = 28-9 = 19$, No. of integers divisible by 2, 5, 7 but not by all (2, 3, 5, 7)

$|D| - 38 - 10 - 19 = 285 - 38 - 10 - 19 = 218$, No. of integers divisible by 7 but not by 2, not by 3 and not by 5.

Note : The number of r combinations of n distinct things with unlimited number of repetitions
= The number of ways of distributing r similar balls in n number of boxes
=The number of non negative integer solutions of $x_1 + x_2 + \ldots + x_n = x_r$
$= (n-1+r)Cr$

Example: Use principle of inclusion and exclusion to determine how many solutions does the equation $x_1 + x_2 + x_3 = 11$ have?, where $0 \le x_1 \le 3,\ 0 \le x_2 \le 4, 0 \le x_3 \le 6$.

Let us find the total number of solutions of $x_1 + x_2 + x_3 = 11$ where $x_1 \ge 0,\ x_2 \ge 0, x_3 \ge 0$.

It is $N = (3+11-1)C11$
$= 13C11$
$= 13C2$
$= 78$

Let $A,\ B,\ C$ represents the set of solution with the property $x_1 > 3,\ x_2 > 4, x_3 > 6$ respectively.

Therefore required number of solutions is $N - |A\cup B\cup C|$

i.e. $N - \left(|A| + |B| + |C| - |A\cap B| - |B\cap C| - |C\cap A| + |A\cap B\cap C|\right)$….(1)

$|A|$ = No. of solutions when $x_1 = 4, 5, \ldots, 11$. Now $(x_2 \le 7,\ x_3 \le 7)$
$= (3+7-1)C7$
$= 9C7$
$= 36$

$|B|$ = No. of solutions when $x_2 = 5, 6, \ldots, 11$. Now $(x_1 \le 6,\ x_3 \le 6)$

https://doi.org/10.5281/zenodo.15287608

$= (3+6-1)C6$
$= 8C6$
$= 28$

$|C| =$ No. of solutions when $x_3 = 7,8,...,11$. Now $(x_2 \le 4,\ x_1 \le 4)$
$= (3+4-1)C4$
$= 6C4$
$= 15$

$|A \cap B| =$ No. of solutions when $x_1 \ge 4,\ x_2 \ge 5$. Now $(x_3 \le 2)$
$= (3+2-1)C2$
$= 4C2$
$= 6$

$|B \cap C| =$ No. of solutions when $x_2 \ge 5,\ x_3 \ge 7$. Now $(x_1 \le -1)$, not possible.
$= 0$

$|C \cap A| =$ No. of solutions when $x_3 \ge 7,\ x_1 \ge 4$. Now $(x_2 \le 0)$
$= (3+0-1)C0$
$= 2C0$
$= 1$

$|A \cap B \cap C| =$ No. of solutions when $x_1 \ge 4, x_2 \ge 5,\ x_3 \ge 7$, not possible.
$= 0$

From (1), required number of solutions = 78 – 36 – 28 – 15 + 6 + 0 + 1 – 0) = 6

Example: Use principle of inclusion and exclusion to determine how many bit strings of length 8 either start with a 1 bit or end with the two bits 00's?

Let A represents the set of strings of length 8 starting with 1.
Let B represents the set of strings of length 8 end with 00.
Therefore required number of strings is $|A \cup B|$
i.e. $|A \cup B| = |A| + |B| - |A \cap B|$

$|A| = 2^7 = 128$ {because first place is 1 and the remaining 7 places are filled by either 0 or 1}

$|B| = 2^6 = 64$ {because last two places is 00 and the remaining 6 places are filled by either 0 or 1}

$|A \cap B| = 2^5 = 32$ {because first place is 1 and last two places is 00 and the remaining 5 places are filled by either 0 or 1}

Therefore $|A \cup B| = 128 + 64 - 32 = 160$.

Euler's Phi Function:

For $n \in Z^+$, $n \geq 2$, let $\phi(n)$ be the number of positive integers m, where $1 \leq m < n$ and $\gcd(m, n) = 1$ that is, m, n are relatively prime.

Result: $\phi(p) = p - 1$ if p is prime.

$\phi(4) = 2$. Because $1 \leq m = 1, 3 < 4$ and $\gcd(1, 4) = 1$, $\gcd(3, 4) = 1$

$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) ... \left(1 - \frac{1}{p_m}\right)$ where $p_1, p_2, ..., p_m$ are distinct prime factors of n.

Example: Use the principle of inclusion-exclusion to derive a formula for $\phi(n)$ when the prime factorization of n is $n = p_1^{a_1} p_2^{a_2} .....p_m^{a_m}$.

Let $n = p_1^{a_1} p_2^{a_2} .....p_m^{a_m}$ where $p_1, p_2, ..., p_m$ are distinct prime factors of n and $\alpha_i \geq 1$.

Let $U = \{1, 2, 3, ..., n\}$.

Let A_i be the subset of U containing the integers that divisible by p_i.

Now the integers in U relatively prime to n are those in none of the subsets $A_1, A_2, ..., A_m$.

Therefore $\phi(n) = \overline{A_1} \cap \overline{A_2} \cap ..... \cap \overline{A_m} = |U| - |A_1 \cup A_2 \cup ... \cup A_m|$.

Also $|A_i| = \frac{n}{p_i}$, $|A_i \cap A_j| = \frac{n}{p_i \cdot p_j}$, ..., $|A_1 \cap A_2 \cap .... \cap A_m| = \frac{n}{p_1 \cdot p_2 \cdots\cdot p_m}$

Therefore by principle of inclusion and exclusion

$$\phi(n) = n - \sum_{i=1}^{m} \frac{n}{p_i} + \sum_{i,j}^{m} \frac{n}{p_i \cdot p_j} + ...(-1)^m \frac{n}{p_1 \cdot p_2 \cdots p_m}$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).....\left(1 - \frac{1}{p_m}\right)$$

https://doi.org/10.5281/zenodo.15287608

EXERCISE

1. In a class of 50 students, 20 students play foot ball and 16 students play hockey. It is found that 10 students play both the games. Find the number of students who play neither.

2. A total of 1232 students have taken a course in Spanish, 879 have taken a course in French and 114 have taken a course in Russian. Further, 103 have taken a courses in both Spanish and French, 23 have taken courses in both Spanish and Russian and 14 have taken courses in both French and Russian. If 2092 students have taken at least one of Spanish, French and Russian, how many students have taken a course in all three languages?
   Hint: Find $|S\cap F\cap R|$ from $|S\cup F\cup R|=|S|+|F|+|R|-|S\cap F|-|F\cap R|-|S\cap R|+|S\cap F\cap R|$

3. There are 2500 students in a college, of these 1700 have taken a course in C, 1000 have taken a course Pascal and 550 have taken a course in Networking. Further 750 have taken courses in both C and Pascal, 400 have taken courses in both C and networking and 275 have taken courses in both Pascal and networking. If 200 of these students have taken courses in C, Pascal, Networking (1) How many of these 2500 students have taken a course in any of these three courses C, Pascal and Networking? (2) How many of these 2500 students have not taken a course in any of these three courses C, Pascal and Networking?

4. Find the number of integers between 1 to 250 that are not divisible by any of the integers 2, 3, 5 and 7.

5. Find the number of integers between 1 to 100 that are not divisible by any of the integers 2, 3, 5 or 7.

6. Show that in any group of 8 people at least two have birthdays which falls on same day of the week in any given year.

https://doi.org/10.5281/zenodo.15287608

Recurrence Relations

Definition: A recurrence relation for the sequence $\{s_n\}$ is an equation that expresses s_n in terms of the previous terms, namely $s_0, s_1, s_2, \ldots.., s_{n-1}$, for all integers $n \geq n_0$, a non negative integer.

Example : Consider the Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, 13, ...

Here a term is equal to sum of its previous two terms with starting values 0 and 1.
Therefore the recurrence relation is $s_n = s_{n-1} + s_{n-2}$; subject to $s_0 = 0,\ s_1 = 1$.

Definition: If the terms of a sequence satisfy a recurrence relation, then the sequence is called a solution of the recurrence relation.

Example: Consider the sequence $2, 6, 18, 54, \ldots..$. If $\{a_n\}$ represents this sequence, then the recurrence relation is $\frac{a_{n+1}}{a_n} = 3$. i.e. $a_{n+1} = 3a_n,\ n \geq 0$.

Assuming $a_0 = 2$, we have $a_1 = 3a_0 = 3 \cdot 2^1,\ a_2 = 3a_1 = 3 \cdot 6 = 3^2 \cdot 2$ and so on. In general $a_n = 2 \cdot 3^n$. It is the general solution of the recurrence relation.

Example: Find the first four terms of the sequence defined by the recurrence relations and initial condition $a_n = a_{n-1}^2,\ a_1 = 2$.

The first four terms are $a_1 = 2,\ a_2 = a_1^2 = 4,\ a_3 = a_2^2 = 16,\ a_4 = a_3^2 = 256$.

Note: A recurrence relation of the form $a_0 y_n + a_1 y_{n-1} + a_2 y_{n-2} + \ldots.. + a_k y_{n-k} = f(n),\ n \geq k$ is called a linear recurrence relation, where $a_0, a_1, a_2, \ldots..a_k$ are real numbers.
It is of order k if $a_k \neq 0$ i.e. is y_n expressed in terms of the previous k terms.
If $f(n) = 0$, it is said to be homogeneous. Otherwise non homogeneous.
A recurrence relation may be denoted by various notations as $a_0 y(n) + a_1 y(n-1) + \ldots.. + a_k y(n-k) = f(n)$
Instead of y, any other dummy variable may be used.

Formation of Recurrence Relation

Example : Find the recurrence relation of the sequence $s(n) = a^n : n \geq 1$.

Given $s(n) = a^n$ and hence $s(n-1) = a^{n-1} = \frac{1}{a} a^n$

https://doi.org/10.5281/zenodo.15287608

$$a\,s(n-1)=a^n$$

Therefore $a\ s(n-1)=S(n)$

Example : Find the recurrence relation satisfying the equation $y_n = A(3)^n + B(-4)^n$

Given $y_n = A(3)^n + B(-4)^n$

Therefore $y_{n+1} = A(3)^{n+1} + B(-4)^{n+1} = 3A3^n - 4B(-4)^n$

$$y_{n+2} = A(3)^{n+2} + B(-4)^{n+2} = 9A3^n + 16B(-4)^n$$

Eliminating the constants 1, $A(3)^n$ and $B(-4)^n$ from the three equations, we get

$$\begin{vmatrix} y_n & 1 & 1 \\ y_{n+1} & 3 & -4 \\ y_{n+2} & 9 & 16 \end{vmatrix} = 0$$

$$y_n(48+36) - y_{n+1}(16-9) + y_{n+2}(-4-3) = 0$$

$$84y_n - 7y_{n+1} - 7y_{n+2} = 0$$

$$12y_n - y_{n+1} - y_{n+2} = 0, \quad for\ n \ge 0$$

Aliter: Given $y_n = A(3)^n + B(-4)^n$

Therefore $y_{n-1} = A(3)^{n-1} + B(-4)^{n-1} = \frac{1}{3}A3^n - \frac{1}{4}B(-4)^n$

$$12y_{n-1} = 4A3^n - 3B(-4)^n$$

$$y_{n-2} = A(3)^{n-2} + B(-4)^{n-2} = \frac{1}{9}A3^n + \frac{1}{16}B(-4)^n$$

$$144y_{n-2} = 16A3^n + 9B(-4)^n$$

Eliminating the constants 1, $A(3)^n$ and $B(-4)^n$ from the three equations, we get

$$\begin{vmatrix} y_n & 1 & 1 \\ 12y_{n-1} & 4 & -3 \\ 144y_{n-2} & 16 & 9 \end{vmatrix} = 0$$

$$y_n(36+48) - 12y_{n-1}(9-16) + 144y_{n-2}(-3-4) = 0$$

$$84y_n + 84y_{n-1} - 1008y_{n-2} = 0$$

$$y_n + y_{n-1} - 12y_{n-2} = 0, \quad for\ n \ge 2$$

Note: Therefore $12y_n - y_{n+1} - y_{n+2} = 0, \quad for\ n \ge 0$ is same as $y_n + y_{n-1} - 12y_{n-2} = 0, \quad for\ n \ge 2$

Solution of Linear Recurrence Relations

Consider a second order recurrence relation $a_0y_n + a_1y_{n-1} + a_2y_{n-2} = f(n), n \geq 2$

Let the solution is y_n = complementary solution + particular solution.

Write the characteristic equation by putting $y_n = m^2,\ y_{n-1} = m,\ y_{n-2} = 1$

$$a_0m^2 + a_1m + a_2 = 0$$

Let the roots of the characteristic equation be m_1, m_2.

Case (i)	Case (ii)	Case (iii)
If $m_1 \neq m_2$, then the complementary solution is $A \cdot m_1^n + B \cdot m_2^n$ where A, B are arbitrary constants	If $m_1 = m_2 = (m)$, then the complementary solution is $(A + B \cdot n)m^n$ where A, B are arbitrary constants	If $m_1 = m_2 = (r\cos\theta \pm i\sin\theta)$, then the complementary solution is $(A\cos n\theta + B\sin n\theta)m^n$ where A, B are arbitrary constants

If $f(n) \neq 0$, particular solution may be evaluated by assuming some standard substitutions which are given below.

Form of $f(n)$	Assumption of particular solution
C, Constant	A, a constant
n	$A_0n + A_1$
n^2	$A_0n^2 + A_1n + A_2$
a^n	$A \cdot a^n$
n^2a^n	$a^n\left(A_0n^2 + A_1n + A_2\right)$
$\cos n\theta / \sin n\theta$	$A\sin n\theta + B\cos n\theta$
$a^n \cos n\theta / a^n \sin n\theta$	$a^n\left(A\sin n\theta + B\cos n\theta\right)$

Example : Solve the recurrence relation $y(k) - 8y(k-1) + 16y(k-2) = 0 : k \geq 2$, where $y(2) = 16, y(3) = 80$

The characteristic equation is $m^2 - 8m + 16 = 0$

$$(m-4)(m-4) = 0$$

$$m = 4, 4$$

Therefore the general solution is $y(k) = (A + Bk) \cdot 4^k$

By using the initial conditions, we have

$y(2) = (A + 2B) \cdot 4^2$ $\qquad$ $y(3) = (A + 3B) \cdot 4^3$

$16 = 16A + 32B........(i)$ $\qquad$ $80 = 64A + 192B........(ii)$

Solving (i) and (ii)

$$64 = 64A + 128B$$

$$80 = 64A + 192B$$

$$\overline{}$$

Subtracting $16 = 64B$

$B = 4$

From (i), $16 = 16A + 32 \times 4$

$A = -7$

Therefore the general solution is $y(k) = \left(A + Bk\right)\cdot 4^k = \left(-7 + 4k\right)\cdot 4^k$

Example : Solve the recurrence relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ given that $a_0 = 5, a_1 = 9$ and $a_2 = 15$.

Given recurrence relation is $a_n + 3a_{n-1} + 3a_{n-2} + a_{n-3} = 0$

The characteristic equation is $m^3 + 3m^2 + 3m + 1 = 0$

Here $m = -1$ is a root. By synthetic division, we get $m^2 + 2m + 1 = 0$

$$\left(m+1\right)^2 = 0$$

$$m = -1, -1$$

Therefore the general solution is $a_n = \left(A + Bn + Cn^2\right)\cdot(-1)^n$

By using the initial conditions, we have

$a_0 = \left(A + B\cdot 0 + C\cdot 0^2\right)\cdot(-1)^0$

$5 = A$

$a_1 = \left(A + B\cdot 1 + C\cdot 1^2\right)\cdot(-1)^1$

$9 = -A - B - C$

$B + C = -14.....(i)$

$a_2 = \left(A + B\cdot 2 + C\cdot 2^2\right)\cdot(-1)^2$

$15 = A + 2B + 4C$

$2B + 4C = 10.....(ii)$

Solving (i) and (ii)

$$2B + 2C = -28$$

$$2B + 4C = 10$$

$$\overline{}$$

Subtracting $2C = 38$

$C = 19$

From (i), $B + 19 = -14$

$B = -33$

Therefore the general solution is $a_n = \left(5 - 33n + 19n^2\right)\cdot(-1)^n$

Example : Solve the recurrence relation $S(n) - 3S(n-1) = 5\left(3^n\right)$, with $S(0) = 2$

The auxiliary equation is $\alpha - 3 = 0$ and hence $\alpha = 3$.

Therefore the complementary function is $A□3^n$.

Let the particular integral is of the form $S(n) = cn\left(3^n\right)$

Therefore given relation becomes $cn\left(3^n\right) - 3c(n-1)\left(3^{n-1}\right) = 5\left(3^n\right)$

Comparing the coefficient of $\left(3^n\right)$ on both sides, we get $cn\left(3^n\right) - c\ (n-1)\left(3^n\right) = 5\left(3^n\right)$

$$cn - c\ (n-1) = 5$$
$$c = 5$$

The solution is $S(n) = C.F + P.I = A3^n + 5n3^n$

Since $S(0) = 2$, $S(0) = A3^0 + 5(0)3^n$

$$2 = A$$

$$\therefore S(n) = 2\cdot 3^n + 5n3^n$$

Example : Solve $G(k) - 7G(k-1) + 10G(k-2) = 8k+6$, for $k \geq 2$.

The characteristic equation is $m^2 - 7m + 10 = 0$

$$(m-2)(m-5) = 0$$
$$m = 2,\ 5$$

Therefore the complementary function is $A\cdot 2^k + B\cdot 5^k$

Since RHS is of the form $8k+6$, let the particular integral be assumed as $G(k) = a_0 + a_1 k$.

Using this in the given recurrence relation, we have

$$\left(a_0 + a_1 k\right) - 7\left(a_0 + a_1(k-1)\right) + 10\left(a_0 + a_1(k-2)\right) = 8k+6$$
$$\left(a_0 + a_1 k\right) - 7\left(a_0 + a_1 k - a_1\right) + 10\left(a_0 + a_1 k - 2a_1\right) = 8k+6$$

Comparing the coefficients of k and constants, we get

$a_1 - 7a_1 + 10a_1 = 8$ and $a_0 - 7a_0 + 7a_1 + 10a_0 - 20a_1 = 6$

$4a_1 = 8$ and $4a_0 - 13a_1 = 6$

$a_1 = 2$ and $4a_0 - 13\times 2 = 6$

$$a_0 = 8$$

Therefore the solution is $G(k) = C.F + P.I = A\cdot 2^k + B\cdot 5^k + \left(8+2k\right)$

Example : Solve the recurrence relation $a_{n+1} - a_n = 3n^2 - n, n \geq 0,\ a_0 = 3.$

The auxiliary equation is $\alpha - 1 = 0$ and hence $\alpha = 1$.

Therefore the complementary function is $K\cdot 1^n$.

Here RHS is of the form $\left(3n^2 - n\right)\cdot 1^n$ and also characteristic root is 1,

https://doi.org/10.5281/zenodo.15287608

let the particular integral is of the form $a_n = \left(An^2 + Bn + C\right)n$. Hence $a_{n+1} = \left(A(n+1)^2 + B(n+1) + C\right)(n+1)$

Therefore given relation becomes $\left(A(n+1)^2 + B(n+1) + C\right)(n+1) - \left(An^2 + Bn + C\right)(n) = 3n^2 - n$

$$\left(A(n+1)^3 + B(n+1)^2 + C(n+1)\right) - \left(An^3 + Bn^2 + Cn\right) = 3n^2 - n$$

$$A\left(n^3 + 3n^2 + 3n + 1\right) + B\left(n^2 + 2n + 1\right) + Cn + C - An^3 - Bn^2 - Cn = 3n^2 - n$$

Comparing the like coefficients, we get

$$3A + B - B = 3 \qquad 3A + 2B + C - C = -1 \qquad A + B + C = 0$$
$$A = 1 \qquad 2B = -4 \qquad 1 - 2 + C = 0$$
$$B = -2 \qquad C = 1$$

Therefore particular integral $a_n = \left(n^2 - 2n + 1\right)n$

Therefore the general solution is $a_n = CF + PI = K \cdot 1^n + \left(n^2 - 2n + 1\right) \cdot n$

Example : Solve $a_{n+2} - 6a_{n+1} + 9a_n = 3\left(2^n\right) + 7\left(3^n\right), n \geq 0$ given that $a_0 = 1, a_1 = 4$.

The characteristic equation is $m^2 - 6m + 9 = 0$

$$\left(m - 3\right)^2 = 0$$
$$m = 3, 3$$

Therefore the complementary function is $\left(A + Bn\right) \cdot 3^n$

Let the particular integral be $a_n = C \cdot 2^n + Dn^2 \cdot 3^n$, since 3 is the double root.
Using this in the given recurrence relation, we have

$$\left(C \cdot 2^{n+2} + D(n+2)^2 \cdot 3^{n+2}\right) - 6\left(C \cdot 2^{n+1} + D(n+1)^2 \cdot 3^{n+1}\right) + 9\left(C \cdot 2^n + Dn^2 \cdot 3^n\right) = 3\left(2^n\right) + 7\left(3^n\right)$$

$$\left(4C \cdot 2^n + 9D(n+2)^2 \cdot 3^n\right) - 6\left(2C \cdot 2^n + 3D(n+1)^2 \cdot 3^n\right) + 9\left(C \cdot 2^n + Dn^2 \cdot 3^n\right) = 3\left(2^n\right) + 7\left(3^n\right)$$

$$\left(4C \cdot 2^n + 9D(n+2)^2 \cdot 3^n\right) - 6\left(2C \cdot 2^n + 3D(n+1)^2 \cdot 3^n\right) + 9\left(C \cdot 2^n + Dn^2 \cdot 3^n\right) = 3\left(2^n\right) + 7\left(3^n\right)$$

Comparing the like terms, we have

$$\left(4C - 12C + 9C\right) = 3 \qquad \& \qquad 9D(n+2)^2 - 18D(n+1)^2 + 9Dn^2 = 7$$
$$C = 3 \qquad 9Dn^2 + 36D + 36Dn - 18Dn^2 - 18D - 36Dn + 9Dn^2 = 7$$
$$18D = 7$$
$$D = \frac{7}{18}$$

Therefore the particular integral becomes $a_n = 3 \cdot 2^n + \frac{7}{18}n^2 \cdot 3^n$

https://doi.org/10.5281/zenodo.15287608

Hence the general solution is $a_n = CF + PI$

$$a_n = (A + Bn)\cdot 3^n + 3\cdot 2^n + \frac{7}{18}n^2\cdot 3^n$$

By using the initial conditions,

$$a_0 = (A + B\cdot 0)\cdot 3^0 + 3\cdot 2^0 + \frac{7}{18}0^2\cdot 3^0$$

$$1 = A + 3$$

$$A = -2$$

and

$$a_1 = (A + B\cdot 1)\cdot 3^1 + 3\cdot 2^1 + \frac{7}{18}1^2\cdot 3^1$$

$$4 = 3A + 3B + 6 + \frac{7}{6}$$

$$4 = -6 + 3B + 6 + \frac{7}{6}$$

$$B = \frac{17}{18}$$

Therefore $a_n = \left(-2 + \frac{17}{18}n\right)\cdot 3^n + 3\cdot 2^n + \frac{7}{18}n^2\cdot 3^n$

Example : A factory makes custom sports car at an increasing rate. In the first month only one car is made, in the second month two cars are made, and so on, with n cars made in the nth month.

i. Set up recurrence relation for the number of cars produced in the first n months by this factory.

ii. How many cars are produced in the first year?

Given that

End of month	1	2	3	.....	n	.....
No. of cars produced	1	2	3	.....	n	.....

Let a_n represents number of cars produced in n months. Then $a_n = a_{n-1} + 1,\ n \geq 1$ such that $a_0 = 0$.

Now we solve the recurrence relation.

The auxiliary equation is $\alpha - 1 = 0$ and hence $\alpha = 1$.

Therefore the complementary function is $A\cdot 1^n$.

Let the particular integral is of the form $a_n = Kn$, since RHS is 1 and 1 is a root of the auxiliary equation.

Therefore given relation becomes $Kn - K(n-1) = 1$

$$K = 1$$

The solution is $a_n = C.F + P.I = A\cdot 1^n + n$

Since $a_0 = 0$, $a_0 = A\cdot 1^0 + 0$

$$0 = A$$

Therefore $a_n = n$.

Number of cars produced in first year $(n = 12)$ is $a_{12} = 12$

EXERCISE

1. Find the recurrence relation of the sequence $s(n) = a^n : n \geq 1$

2. Solve : $a_k = 3a_{k-1}$, for $k \geq 1$ with $a_0 = 2$.

3. Write a particular solution of the recurrence relation $a_n = 6a_{n-1} - 9a_{n-2} + 3^n$.

4. Solve $a_n - 5a_{n-1} + 6a_{n-2} = 0$.

5. Solve the recurrence relation $a_n = 8a_{n-1} - 16a_{n-2}\ n \geq 2,$ for $a_0 = 16, a_1 = 80$.

6. Find the solution to the recurrence relation $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$, with the initial conditions $a_0 = 2, a_1 = 5$ and $a_2 = 15$.

https://doi.org/10.5281/zenodo.15287608

Generating Functions

Definition: The generating function for the sequence $s_0, s_1, s_2, \ldots\ldots, s_n, \ldots\ldots\ldots$ of real numbers is the infinite series $G(s,z) = s_0 + s_1 z^1 + s_2 z^2 + \ldots\ldots + s_n z^n + \ldots. = \sum_{k=0}^{\infty} s_k z^k$ where z is the dummy variable.

Note: The generating function for the sequence 1, 2, 3, 4, …. is given by

$$G(s,z) = 1 + 2z^1 + 3z^2 + \ldots\ldots = \sum_{n=0}^{\infty} (n+1) z^n = (1-2z)^{-2}$$

Example: Write the generating function for the sequence $1, a, a^2, a^3, \ldots\ldots.$

The generating function is $G(a,z) = 1 + az^1 + a^2 z^2 + \ldots\ldots + a^n z^n + \ldots\ldots$

$$= (1-az)^{-1} \text{ if } |az| < 1$$

$$= \frac{1}{(1-az)} \text{ if } |z| < \frac{1}{|a|}, a \neq 0$$

Solution of Recurrence Relation by Using Generating Functions

Example : Use generating function to solve the recurrence relation $S(n) - 7S(n-1) + 6S(n-2) = 0$, for $n \geq 2$ with $S(0) = 8, S(1) = 6.$

For our convenience, rewrite the given equation as $S_n - 7S_{n-1} + 6S_{n-2} = 0$ for $n \geq 2$ with $S_0 = 8, \quad S_1 = 6.$

Let $G(S,z) = \sum_{n=2}^{\infty} S_{n-2} z^{n-2} = S_0 + S_1 z^1 + S_2 z^2 + \ldots\ldots$ be the generating function of the sequence $\{S_n\}$.

Given that $S_n - 7S_{n-1} + 6S_{n-2} = 0$ for $n \geq 2$.

Therefore $\sum_{n=2}^{\infty} S_n z^n - 7\sum_{n=2}^{\infty} S_{n-1} z^n + 6\sum_{n=2}^{\infty} S_{n-2} z^n = 0$

$$\sum_{n=2}^{\infty} S_n z^n - 7z\sum_{n=2}^{\infty} S_{n-1} z^{n-1} + 6z^2\sum_{n=2}^{\infty} S_{n-2} z^{n-2} = 0$$

$$\left(S_2 z^2 + S_3 z^3 + \ldots\ldots\right) - 7z\left(S_1 z^1 + S_2 z^2 + \ldots\ldots\right) + 6z^2\left(S_0 + S_1 z^1 + S_2 z^2 + \ldots\ldots\right) = 0$$

https://doi.org/10.5281/zenodo.15287608

$$\left[G(S,z)-S_0-S_1z^1\right]-7z\left[G(S,z)-S_0\right]+6z^2G(S,z)=0$$

$$\left[G(S,z)-8-6z\right]-7z\left[G(S,z)-8\right]+6z^2G(S,z)=0$$

$$G(S,z)\left(1-7z+6z^2\right)-6z+56z-8=0$$

$$G(S,z)\left(6z^2-7z+1\right)=8-50z$$

$$G(S,z)=\frac{8-50z}{\left(6z^2-7z+1\right)}$$

$$G(S,z)=\frac{8-50z}{(6z-1)(z-1)}$$

$$G(S,z)=\frac{8-50z}{(1-6z)(1-z)}$$

$$\frac{8-50z}{(1-6z)(1-z)}=\frac{A}{(1-6z)}+\frac{B}{(1-z)}$$

$$8-50z=A(1-z)+B(1-6z)$$

$$\begin{array}{ll} When\ \ z=1 & z=\frac{1}{6} \\ -42=-5B & 8-\frac{50}{6}=A\left(1-\frac{1}{6}\right) \\ 42=5B & -\frac{2}{6}=\frac{5}{6}A \\ B=\frac{42}{5} & A=-\frac{2}{5} \end{array}$$

$$G(S,z)=\frac{8-50z}{(1-6z)(1-z)}=-\frac{2}{5}\frac{1}{(1-6z)}+\frac{42}{5}\frac{1}{(1-z)}$$

$$G(S,z)=-\frac{2}{5}(1-6z)^{-1}+\frac{42}{5}(1-z)^{-1}$$

$$G(S,z)=-\frac{2}{5}\left(1+(6z)+(6z)^2+\ldots\right)+\frac{42}{5}\left(1-(z)+(z)^2-\ldots\right)$$

Therefore the general solution is given by

$$S_n=coefficient\ of\ \ z^n\ \ in\ \ G(S,z)=-\frac{2}{5}6^n+\frac{42}{5}1^n$$

Example : Using the generating function, solve the difference equation $y_{n+2}-y_{n+1}-6y_n=0, n\geq 0$ with $y_0=2,\ y_1=1$

Let $G(y,z)=\sum_{n=0}^{\infty} y_n z_n = y_0 + y_1 z^1 + y_2 z^2 + ...$ be the generating function of the sequence $\{y_n\}$.

Given that $y_{n+2} - y_{n+1} - 6y_n = 0$ for $n \geq 0$.

Therefore $\sum_{n=0}^{\infty} \; y_{n+2} z^n - \sum_{n=0}^{\infty} \; y_{n+1} z^n - 6\sum_{n=0}^{\infty} \; y_n z^n = 0$

$$\frac{1}{z^2}\sum_{n=0}^{\infty} \; y_{n+2} z^{n+2} - \frac{1}{z}\sum_{n=0}^{\infty} \; y_{n+1} z^{n+1} - 6\sum_{n=0}^{\infty} \; y_n z^n = 0$$

$$\frac{1}{z^2}\left(y_2 z^2 + y_3 z^3 + ...\right) - \frac{1}{z}\left(y_1 z^1 + y_2 z^2 + ...\right) - 6G(y,z) = 0$$

$$\frac{1}{z^2}\left[G(y,z) - y_0 - y_1 z^1\right] - \frac{1}{z}\left[G(y,z) - y_0\right] - 6G(y,z) = 0$$

$$\frac{1}{z^2}\left[G(y,z) - 2 - z\right] - \frac{1}{z}\left[G(y,z) - 2\right] - 6G(y,z) = 0$$

$$G(y,z)\left(\frac{1}{z^2} - \frac{1}{z} - 6\right) - \frac{2}{z^2} - \frac{z}{z^2} + \frac{2}{z} = 0$$

$$G(y,z)\left(\frac{1}{z^2} - \frac{1}{z} - 6\right) = \frac{2}{z^2} + \frac{z}{z^2} - \frac{2}{z}$$

$$G(y,z)\left(\frac{1}{z^2} - \frac{1}{z} - 6\right) = \frac{2 + z - 2z}{z^2}$$

$$G(y,z)\left(\frac{1 - z - 6z^2}{z^2}\right) = \frac{2 - z}{z^2}$$

$$G(y,z) = \frac{2 - z}{1 - z - 6z^2}$$

$$G(y,z) = \frac{z - 2}{6z^2 + z - 1}$$

$$G(y,z) = \frac{z - 2}{(1-3z)(1+2z)}$$

$$\frac{z-2}{(1-3z)(1+2z)} = \frac{A}{(1-3z)} + \frac{B}{(1+2z)}$$

$$z - 2 = A(1+2z) + B(1-3z)$$

https://doi.org/10.5281/zenodo.15287608

$$z-2 = A(1+2z)+B(1-3z)$$

$$When \quad z=-\frac{1}{2} \qquad\qquad z=\frac{1}{3}$$

$$-\frac{1}{2}-2 = B\left(1+\frac{3}{2}\right) \qquad \frac{1}{3}-2 = A\left(1+\frac{2}{3}\right)$$

$$-\frac{5}{2}=\frac{5}{2}B \qquad\qquad -\frac{5}{3}=\frac{5}{3}A$$

$$B=-1 \qquad\qquad A=-1$$

$$\frac{z-2}{(1-3z)(1+2z)} = \frac{-1}{(1-3z)}+\frac{-1}{(1+2z)}$$

$$G(y,z) = \frac{2-z}{(1-3z)(1+2z)} = \frac{1}{(1-3z)}+\frac{1}{(1+2z)}$$

$$G(y,z) = (1-3z)^{-1}+(1+2z)^{-1}$$

$$G(y,z) = \left(1+(3z)+(3z)^2+\ldots\right)+\left(1-(2z)+(3z)^2-\ldots\right)$$

Therefore the general solution is $y_n = coefficient\ of\ z^n\ in\ G(y,z) = 3^n+(-2)^n$

Example : Solve the recurrence relation $a_n = 3a_{n-1}+2, n\geq 1$ with $a_0=1$ by the method of generating functions.

For our convenience, let us rewrite the recurrence relation as $y_n = 3y_{n-1}+2$ such that $y_0=1$.

Let $G(Y,z) = \sum_{n=0}^{\infty} y_n z_n = y_0+y_1z^1+y_2z^2+.....$ be the generating function of the sequence $\{y_n\}$.

Given that $y_n = 3y_{n-1}+2$ for $n \geq 1$.

Therefore $\sum_{n=1}^{\infty} y_n z^n = 3\sum_{n=1}^{\infty} y_{n-1}z^n + \sum_{n=1}^{\infty} 2z^n$

$$\left(y_1z^1+y_2z^2+y_3z^3+......\right) = 3\left(y_0z^1+y_1z^2+......\right)+2\left(z^1+z^2+z^3+......\right)$$

$$\left(y_0+y_1z^1+y_2z^2+y_3z^3+......-y_0\right) = 3z\left(y_0+y_1z^1+......\right)+2z\left(1+z^1+z^2+......\right)$$

$$\left(G(Y,z)-y_0\right) = 3zG(Y,z)+2z(1-z)^{-1}$$

$$\left(G(Y,z)-1\right) = 3zG(Y,z)+2z(1-z)^{-1}$$

$$G(Y,z)(1-3z) = \frac{2z}{1-z}+1$$

$$G(Y,z)(1-3z)=\frac{2z+1-z}{1-z}$$

$$G(Y,z)=\frac{z+1}{(1-3z)(1-z)}$$

By splitting in to partial fractions,

$$\frac{z+1}{(1-3z)(1-z)}=\frac{A}{(1-3z)}+\frac{B}{(1-z)}$$

$$z+1=A(1-z)+B(1-3z)$$

Put $z=1$ Put $z=0$

$B=-2$ $A=3$

$$G(Y,z)=\frac{3}{(1-3z)}-\frac{2}{(1-z)}$$

$$G(Y,z)=3(1-3z)^{-1}-2(1-z)^{-1}$$

$$G(Y,z)=3\left(1+(3z)+(3z)^2+....\right)-2\left(1+(z)+(z)^2+....\right)$$

Therefore the general solution is given by

$$y_n=\textit{coefficient of } z^n \textit{ in } G(Y,z)$$

$$y_n=3\cdot 3^n-2\cdot 1^n$$

Example : Use the method of generating function to solve the recurrence relation $a_n=4a_{n-1}-4a_{n-2}+4^n;\ n\geq 2$ given that $a_0=2,\ a_1=8$.

For our convenience, let us rewrite the recurrence relation as $y_n=4y_{n-1}-4y_{n-2}+4^n$ such that

$y_0=2,\ y_1=8$.

Let $G(y,z)=\sum_{n=0}^{\infty}y_n z_n=y_0+y_1z^1+y_2z^2+.....$ be the generating function of the sequence $\{y_n\}$.

Given that $y_n=4y_{n-1}-4y_{n-2}+4^n$ for $n\geq 2$.

Therefore $\sum_{n=2}^{\infty} y_nz^n=4\sum_{n=2}^{\infty} y_{n-1}z^n-4\sum_{n=2}^{\infty} y_{n-2}z^n+\sum_{n=2}^{\infty} 4^n z^n$

$$\left(y_2z^2+y_3z^3+......\right)=4\left(y_1z^2+y_2z^3+......\right)-4\left(y_0z^2+y_1z^3+......\right)+\left(4^2z^2+4^3z^3+......\right)$$

$$\left(G(Y,z)-y_0-y_1z\right)=4z\left(G(Y,z)-y_0\right)-4z^2G(Y,z)+\frac{1}{1-4z}-1-4z$$

$$\left(G(Y,z)-2-8z\right)=4z\left(G(Y,z)-2\right)-4z^2G(Y,z)+\frac{1}{1-4z}-1-4z$$

$$G(Y,z)\left(1-4z+4z^2\right)=\frac{1}{1-4z}-1-4z+2$$

$$G(Y,z)(1-2z)^2=\frac{1}{1-4z}+1-4z$$

$$G(Y,z)=\frac{1+(1-4z)^2}{(1-2z)^2(1-4z)}$$

https://doi.org/10.5281/zenodo.15287608

By splitting in to partial fractions,

$$G(Y,z)=-\frac{2}{(1-2z)^2}+\frac{4}{(1-4z)}$$

$$G(Y,z)=-2(1-2z)^{-2}+4(1-4z)^{-1}$$

$$G(Y,z)=-2\Big(1+2(2z)+3(2z)^2+....\Big)+$$

$$4\Big(1+(4z)+(4z)^2+....\Big)$$

Therefore the general solution is given by

$$y_n=\mathit{coefficient\ of}\ \ z^n\ \ \mathit{in}\ \ G(Y,z)$$

$$y_n=-2\cdot(n+1)\cdot 2^n+4\cdot 4^n$$

$$y_n=4^{n+1}-(n+1)\cdot 2^{n+1}$$

$$\frac{1+(1-4z)^2}{(1-2z)^2(1-4z)}=\frac{A}{(1-2z)}+\frac{B}{(1-2z)^2}+\frac{C}{(1-4z)}$$

$$1+(1-4z)^2=A(1-2z)(1-4z)+B(1-4z)+C(1-2z)^2$$

Put $2z=1$ Put $4z=1$ Put $z=0$

$$2=-B \qquad 1=\frac{C}{4} \qquad 2=A+B+C$$

$$B=-2 \qquad C=4 \qquad A=0$$

Example : Using generating function method solve the recurrence relation $a_{n+2}-2a_{n+1}+a_n=2^n$ where $n\geq 0,\ a_0=2$ and $a_1=1$.

For our convenience, let the recurrence relation be $y_{n+2}-2y_{n+1}+y_n=2^n,\ n\geq 0$ such that $y_0=2,\ y_1=1$.

Let $G(y,z)=\sum_{n=0}^{\infty}y_nz_n=y_0+y_1z^1+y_2z^2+.....$ be the generating function of the sequence $\{y_n\}$.

Given that $y_{n+2}-2y_{n+1}+y_n=2^n,\ n\geq 0$.

Therefore $\sum_{n=0}^{\infty}\ y_{n+2}z^n-2\sum_{n=0}^{\infty}\ y_{n+1}z^n+\sum_{n=0}^{\infty}\ y_nz^n=\sum_{n=0}^{\infty}\ 2^nz^n$

$$\left(y_2+y_3z^1+y_4z^2+......\right)-2\left(y_1+y_2z^1+y_3z^2+......\right)+\left(y_0+y_1z^1+y_2z^2+......\right)=\left(1+2^1z^1+2^2z^2+2^3z^3+......\right)$$

$$\frac{1}{z^2}\left(y_2z^2+y_3z^3+y_4z^4+......\right)-\frac{2}{z}\left(y_1z^1+y_2z^2+y_3z^3+......\right)+\left(y_0+y_1z^1+y_2z^2+......\right)=\Big(1+(2z)^1+(2z)^2+(2z)^3+......\Big)$$

$$\frac{1}{z^2}\left(G(Y,z)-y_0-y_1z^1\right)-\frac{2}{z}\left(G(Y,z)-y_0\right)+G(Y,z)=(1-2z)^{-1}$$

$$\frac{1}{z^2}\left(G(Y,z)-2-z^1\right)-\frac{2}{z}\left(G(Y,z)-2\right)+G(Y,z)=(1-2z)^{-1}$$

$$G(Y,z)\left(\frac{1}{z^2}-\frac{2}{z}+1\right)-\frac{2}{z^2}-\frac{1}{z}+\frac{4}{z}=\frac{1}{1-2z}$$

$$G(Y,z)\left(\frac{1-2z+z^2}{z^2}\right)+\frac{-2-z+4z}{z^2}=\frac{1}{1-2z}$$

$$G(Y,z)\left(\frac{1-2z+z^2}{z^2}\right)=\frac{1}{1-2z}-\frac{3z-2}{z^2}$$

$$G(Y,z)\frac{(1-z)^2}{z^2}=\frac{z^2-3z+2+6z^2-4z}{z^2(1-2z)}$$

$$G(Y,z)=\frac{7z^2-7z+2}{(1-z)^2(1-2z)}$$

By splitting in to partial fractions,

$$G(Y,z)=\frac{3}{(1-z)}-\frac{2}{(1-z)^2}+\frac{1}{(1-2z)}$$

$$G(Y,z)=3(1-z)^{-1}-2(1-z)^{-2}+(1-2z)^{-1}$$

$$G(Y,z)=3\left(1+z+z^2+.....\right)-2\left(1+2z+3z^2+....\right)$$
$$+\left(1+(2z)+(2z)^2+....\right)$$

Therefore the general solution is given by

$$y_n=coefficient\ of\ \ z^n\ \ in\ \ G(Y,z)$$

$$y_n=3\cdot n-2\cdot(n+1)+2^n$$

$$\frac{7z^2-7z+2}{(1-z)^2(1-2z)}=\frac{A}{(1-z)}+\frac{B}{(1-z)^2}+\frac{C}{(1-2z)}$$

$$7z^2-7z+2=A(1-z)(1-2z)+B(1-2z)+C(1-z)^2$$

Put $z=1$	Put $z=\frac{1}{2}$	Put $z=0$
$2=-B$ $B=-2$	$\frac{7}{4}-\frac{7}{2}+2=\frac{C}{4}$ $1=C$	$2=A+B+C$ $A=3$

Example : A valid code word is an n-digit decimal number containing even number of 0's. If a_n denotes the number of valid code words of length n then find an explicit formula for a_n using generating functions.

Let a_n be the number of valid n-digit codewords. Now $a_1=9$ because the string 0, is not valid.

To form a valid n-digit string from strings of $n-1$ digits.

Method 1:	Method 2:
A valid string of n digits can be obtained by appending a valid string of $n-1$ digits with a digit other than 0. This appending can be done in nine ways. Hence, a valid string with n digits can be formed in $9a_{n-1}$ ways.	A valid string of n digits can be obtained by appending a 0 to a string of length $n-1$ that has an odd number of 0 digits. The number of ways that this can be done equals the number of invalid $n-1$ digit strings. Because there are 10^{n-1} strings of length $n-1$, and a_{n-1} are valid, there are $10^{n-1}-a_{n-1}$ valid n-digit strings.

All valid strings of length n are produced in one of these two ways. Therefore

$$\begin{aligned} a_n &= 9a_{n-1} + \left(10^{n-1} - a_{n-1}\right) \\ &= 8a_{n-1} + 10^{n-1} \end{aligned}$$

To solve $a_n = 8a_{n-1} + 10^{n-1}$ subject to $a_0 = 1$(assumption), $a_1 = 9$ by generating function.

With usual notations, $y_n = 8y_{n-1} + 10^{n-1}$, $n \geq 1$ subject to $y_0 = 1,\ y_1 = 9$.

Let $G(y,z) = \sum_{n=0}^{\infty} y_n z^n = y_0 + y_1 z^1 + y_2 z^2 + ...$ be the generating function of the sequence $\{y_n\}$.

$$\sum_{n=1}^{n} y_n z^n = 8\sum_{n=1}^{n} y_{n-1} z^n + \sum_{n=1}^{n} 10^{n-1} z^n$$

$$\sum_{n=1}^{n} y_n z^n = 8z\sum_{n=1}^{n} y_{n-1} z^{n-1} + z\sum_{n=1}^{n} 10^{n-1} z^{n-1}$$

$$\left[y_1 z^1 + y_2 z^2 + y_3 z^3 .....\right] = 8z\left[y_0 z^0 + y_1 z^1 + y_2 z^2 .....\right] + z\left[10^0 z^0 + 10^1 z^1 + 10^2 z^2 + ...\right]$$

$$G(Y,z) - y_0 = 8zG(Y,z) + z[1-10z]^{-1}$$

$$(1-8z)G(Y,z) = 1 + \frac{z}{[1-10z]}$$

$$(1-8z)G(Y,z) = \frac{1-10z+z}{[1-10z]}$$

$$G(Y,z) = \frac{1-9z}{(1-8z)(1-10z)}$$

$$G(Y,z) = \frac{1}{2}\frac{1}{(1-8z)} + \frac{1}{2}\frac{1}{(1-10z)}$$

$$G(Y,z) = \frac{1}{2}(1-8z)^{-1} + \frac{1}{2}(1-10z)^{-1}$$

$$\begin{aligned} G(Y,z) = \frac{1}{2}&\left[1 + (8z) + (8z)^2 + ...\right] + \\ \frac{1}{2}&\left[1 + (10z) + (10z)^2 + ...\right] \end{aligned}$$

Therefore the general solution is given by
$y_n = coefficient\ of\ \ z^n\ \ in\ \ G(Y,z)$

By partial fraction

$$\frac{1-9z}{(1-8z)(1-10z)} = \frac{A}{(1-8z)} + \frac{B}{(1-10z)}$$

$$1-9z = A(1-10z) + B(1-8z)$$

$$y_n = \frac{1}{2}8^n + \frac{1}{2}10^n$$

$$1-9z = A\left(1-10z\right)+B\left(1-8z\right)$$

$$\begin{array}{ll}
When \quad z = \dfrac{1}{10} & z = \dfrac{1}{8} \\
1-\dfrac{9}{10} = B\left(1-\dfrac{8}{10}\right) & 1-\dfrac{9}{8} = A\left(1-\dfrac{10}{8}\right) \\
\dfrac{1}{10} = B\dfrac{2}{10} & -\dfrac{1}{8} = -\dfrac{2}{8}A \\
B = \dfrac{1}{2} & A = \dfrac{1}{2}
\end{array}$$

Example: Use generating function to determine how many solutions does the equation $x_1 + x_2 + x_3 = 11$ have?, when

(i) $x_1,\ x_2,\ x_3$ are non negative integers

(ii) Integers and $0 \le x_1 \le 3,\ 0 \le x_2 \le 4, 0 \le x_3 \le 6$

(iii) Integers and $x_1 \ge 2,\ \ x_2 \ge 3,\ x_3 \ge 4.$

Let $x^{x_1+x_2+x_3} = x^{11}$ and hence $x^{x_1} \cdot x^{x_2} \cdot x^{x_3} = x^{11}$

(i) $x_1,\ x_2,\ x_3$ are non negative integers

Therefore the generating function is $G(x) = \left(x^0 +\ x^1 + x^2 + \cdots\right)\left(x^0 +\ x^1 + x^2 + \cdots\right)\left(x^0 +\ x^1 + x^2 + \cdots\right)$

$$= \left(1 +\ x^1 + x^2 + \cdots\right)\left(1 +\ x^1 + x^2 + \cdots\right)\left(1 +\ x^1 + x^2 + \cdots\right)$$

$$= \left(1 - x\right)^{-3}$$

$$= \sum_{n=0}^{\infty} \binom{-3}{n}\left(-x\right)^n$$

$$= \sum_{n=0}^{\infty} \left(-1\right)^n \binom{3+n-1}{n}\left(x\right)^n\left(-1\right)^n$$

$$= \sum_{n=0}^{\infty} \binom{3+n-1}{n}\left(x\right)^n$$

The number of solutions for $x_1 + x_2 + x_3 = 11$ is the coefficient of x^{11} in $G(x)$.

Coefficient of x^{11} is $\binom{3+11-1}{11}=\binom{13}{11}=\binom{13}{2}=\frac{13\cdot 12}{1\cdot 2}=78$

(ii) $0\le x_1\le 3,\ 0\le x_2\le 4, 0\le x_3\le 6$

The generating function with the given condition is

$$\left(x^0+\ x^1+x^2+x^3\right)\left(x^0+\ x^1+x^2+x^3+x^4\right)\left(x^0+\ x^1+x^2+x^3+x^4+x^5+x^6\right)=x^{11}$$

The possible solutions are $\left(x^1,\ x^4,\ x^6\right),\ \left(x^2,\ x^4,\ x^5\right),\ \left(x^2,\ x^3,\ x^6\right),\ \left(x^3,\ x^3,\ x^5\right),\ \left(x^3,\ x^4,\ x^4\right)$

The solutions are $(1, 4, 6),\ (2, 4, 5),\ (2, 3, 6),\ (3, 3, 5),\ (3, 4, 4)$

(iii) $x_1\ge 2,\ \ x_2\ge 3,\ x_3\ge 4.$

The generating function with the given condition is

$$G(x)=\left(x^2+\ x^3+x^4+\cdots\right)\left(x^3+\ x^4+x^5+\cdots\right)\left(x^4+\ x^5+x^6+\cdots\right)$$

$$=x^2\left(1+\ x+x^2+\cdots\right)\cdot x^3\left(1+x+\ x^2+\cdots\right)\cdot x^4\left(1+x+\ x^2+\cdots\right)$$

$$=x^9\left(1-\ x\right)^{-3}$$

$$=x^9\sum_{n=0}^{\infty}\binom{-3}{n}\left(-1\right)^n x^n$$

$$=x^9\sum_{n=0}^{\infty}\left(-1\right)^n\binom{3+n-1}{n}\left(x\right)^n\left(-1\right)^n$$

$$=x^9\sum_{n=0}^{\infty}\binom{3+n-1}{n}\left(x\right)^n$$

The number of solutions for $x_1+x_2+x_3=11$ is the coefficient of $x^2\left(x^{11}=x^9\times x^2\right)$ in the expansion of $G(x)$.

Coefficient of x^2 is $\binom{3+2-1}{2}=\binom{4}{2}=\frac{4\cdot 3}{1\cdot 2}=6$

EXERCISE

1. Write the generating function for the sequence $1, a, a^2, a^3, ...$

2. Find the generating function of Fibonacci sequence.

3. Use the method of generating function, solve the recurrence relation $S_n + 3S_{n-1} - 4S_{n-2} = 0 : n \geq 2$ given $S_0 = 3$ and $S_1 = -2$.

4. Solve the recurrence relation $a_n - 7a_{n-1} + 6a_{n-2} = 0, n \geq 2$ with the initial conditions $a_0 = 8,\ a_1 = 6$ using generating function.

5. Solve the recurrence relations $S(n) = S(n-1) + 2S(n-2)$ with $S(0) = 3,\ S(1) = 1;\ n \geq 2$ using generating function.

6. Using generating function, solve the recurrence relation $a_n - 5a_{n-1} + 6a_{n-2} = 0$ where $n \geq 2, a_0 = 0$ and $a_1 = 1$.

7. Using generating function solve: $y_{n+2} - 5y_{n+1} + 6y_n = 0, n \geq 0$ with $y_0 = 1,\ y_1 = 1.$

8. Use generating functions to solve the recurrence relation $a_n - 2a_{n-1} - 3a_{n-2} = 0,\ n \geq 2$ with $a_0 = 3,\ a_1 = 1$.

https://doi.org/10.5281/zenodo.15287608

UNIT III – GRAPHS

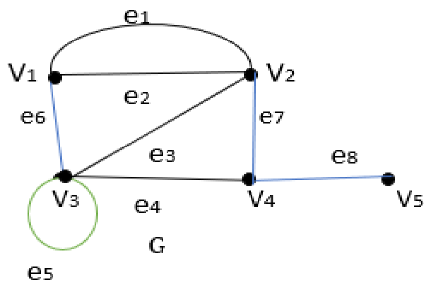
A **graph** $G=\{V,\ E\}$ consists of non empty set of vertices V and a set of edges E such that each edge is mapped to an unordered pair of vertices.

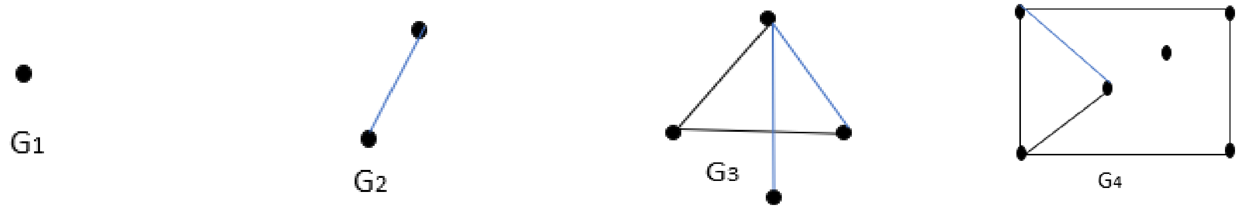
Note: To draw the graph, vertices are denoted by small dots and edges are denoted by a line joining the vertices. Each edge has either one or two vertices associated with it, called its endpoints

Example: Let $G=\{V,\ E\}$ where $V=\{v_1,\ v_2,\ v_3,\ v_4,\ v_5\}$ and $E=\{e_1,\ e_2,\ e_3,\ e_4,\ e_5,\ e_6,\ e_7,\ e_8\}$ such that

$e_1=(v_1,\ v_2)$ $e_2=(v_1,\ v_2)$ $e_3=(v_3,\ v_2)$ $e_4=(v_3,\ v_4)$

$e_5=(v_3,\ v_3)$ $e_6=(v_1,\ v_3)$ $e_7=(v_2,\ v_4)$ $e_8=(v_4,\ v_5)$



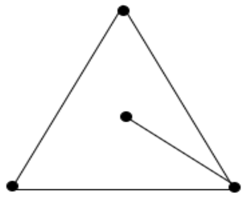


Examples of some Graphs

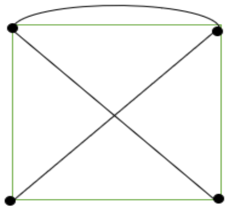
Note:

- A single vertex itself a graph (trivial) and a single edge itself a graph
- A pair of vertices that are connected by an edge is called adjacent vertices – $(v_1,\ v_2),\ (v_3,\ v_2)$
- If two edges are incident with a common vertex, then they are said to be adjacent edges – e_3 , e_4
- If the end vertices of an edge are same, it is called a self loop – e_5
- If more than one edges have the common end vertex, they are called parallel edges – e_1 , e_2

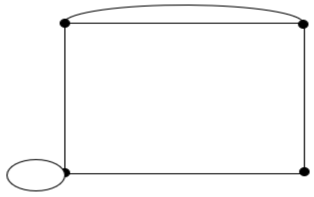
Definition: A graph which has neither self loop nor parallel edges is called a **simple graph**. A graph which contains parallel edges is called multigraph. A graph which has self loops and parallel edges is called pseudo graph.



Simple Graph



Multi Graph



Pseudo Graph

Definition: The number of edges incident on a vertex, counting self loop twice, is called the **degree** of the vertex.

In the above graph G, $\deg(v_1)=3$, $\deg(v_2)=4$, $\deg(v_3)=5$, $\deg(v_4)=3$, $\deg(v_5)=1$

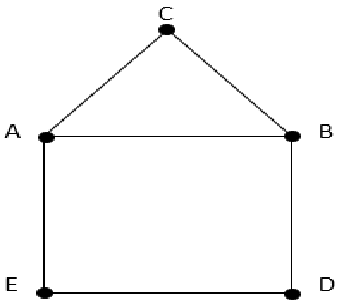
A vertex with degree 1 is called a pendant vertex.

A vertex with degree 0 is called isolated vertex. It is not adjacent to any other vertices

If there is an edge between two vertices, they are said to be adjacent.

A graph with only isolated vertices is called null graph.

Example: Draw the graph with 5 vertices A, B, C, D, E such that deg(A)=3, B is an odd vertex, deg(C)=2 and D and E are adjacent.



The Handshaking Theorem : The sum of degrees of all vertices of a graph is twice the number of edges.

Proof: Let G be a graph with n vertices and $'e'$ number of edges.

We know that each edge is incident on two vertices.

So each edge contributes two degrees.

Therefore $'e'$ number edges contributes $'2e'$ degrees.

i.e. $\sum_{i=1}^{n} d(v_i) = 2.e$

Example: If all the vertices of an undirected graph each of degree k, show that the number of edges of the graph is a multiple of k.

Let G be a graph with n vertices and $'e'$ number of edges.
Since all vertices each of degree k, the total degree of the graph is nk.

By the hand shacking theorem, $\sum_{i=1}^{n} d(v_i) = 2.e$

$$n.k = 2.e$$

$$e = k.\left(\frac{n}{2}\right)$$

i.e. the number of edges of the graph is multiple of k.

Do you know: In the above example, suppose all vertices are each of odd degree k, then $e =$....?

https://doi.org/10.5281/zenodo.15287638

Example: How many edges are there in a graph with 4 vertices each of degree three?

Sum of degrees of all vertices = $4 \times 3 = 12$

But sum of degrees = 2 (number of edges)

Therefore $12 = 2.e$

$$e = 6$$

Example: What is the largest possible number of vertices in a graph with 35 edges and all vertices of degree at least three.

Given number of edges 35. Therefore sum of degrees is $2 \times no.\ of\ \ edges = 70$

Let there are n vertices and each of degrees at least 3. Therefore $3n \geq 70$

$$n \geq \frac{70}{3} \approx 23$$

Therefore, largest possible number of vertices in the graph is 23.

Theorem: In any graph, the number of odd degree vertices is always even.

Proof: Let G be a graph with n vertices and $'e'$ number of edges

By previous theorem, we know that $\sum_{i=1}^{n} d(v_i) = 2.e$

We split the LHS as sum of odd degree vertices and even degree vertices. Then

$$\sum_{odd} d(v_i) + \sum_{even} d(v_j) = 2.e$$

$$\sum_{odd} d(v_i) + Even\ No. = Even\ No.$$

$$\sum_{odd} d(v_i) = Even\ No.$$

In LHS each $d(v_i)$ is odd number and its summation is even number.

Therefore number terms in LHS must be even number. i.e. the number of odd degree vertices is even.

Example: Show that there does not exist a graph with 5 vertices with degrees 1, 3, 4, 2, 3 respectively.

We know that in any graph the number of odd degree vertices are even. But in the given graph three odd degree vertices are given. Hence a graph with these degree sequence does not exist.

Example: Is there a simple graph with degree sequence 1, 1, 3, 3, 3, 4, 6, 7?

Sum of degrees = 28 which is even. Hence a graph exists with this degree sequence.

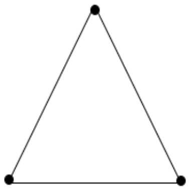
But a simple graph contains no self loop or parallel edges. Plot the eight vertices namely a, b, c, d, e, f, g, h.

The vertex, say a, with degree 7 is adjacent to all other vertices in which two vertices are of degree 1.

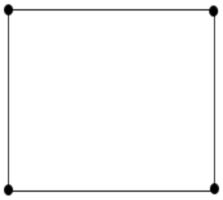
These pendent vertices may not be adjacent to any other vertices. The remaining vertices are only 5. Therefore a vertex with degree 6 is not possible and hence a simple graph is not possible.

Note: But a multigraph is possible with this degree sequence.

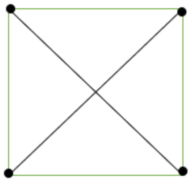
Definition: A graph in which the degree of all vertices are same is called **regular** graph.



Regular Graph with
3 vertices of degree 2



Regular Graph with
4 vertices of degree 2



Regular Graph with
4 vertices of degree 3

Example: How many vertices does a regular graph of degree four with 10 edges have?

Let n be the number of vertices.

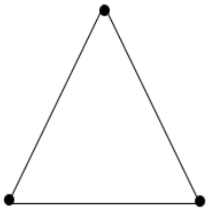
Since each vertex has degree 4, sum of degrees is $4n$

But sum of degrees is equal to two times number of edges

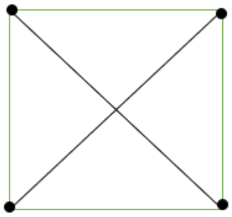
Therefore $4n = 2\times 20$

$n = 10$

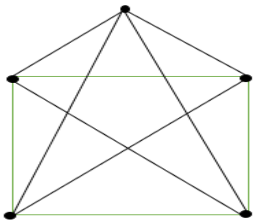
Definition: A graph with n vertices is said to be **complete** graph, if the degree of each vertices is $n-1$. It is denoted by K_n. Here all pair of vertices are adjacent.



K_3



K_4

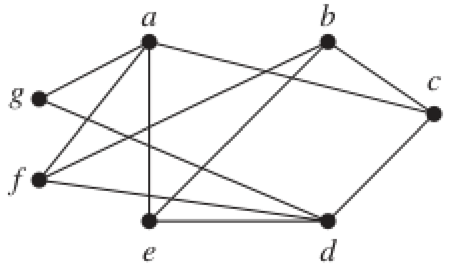


K_5

Do you know?: Can a complete graph be a regular graph ?

Definition: If the vertices set of a graph G can be partitioned into two disjoint sets such that $V_1 \cup V_2 = V$ and each edge has one end vertex in V_1 and another at V_2 is called a **bipartite graph**.

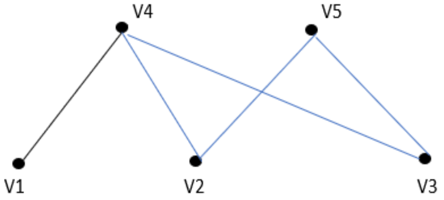
Example: Is the given graph bipartite?



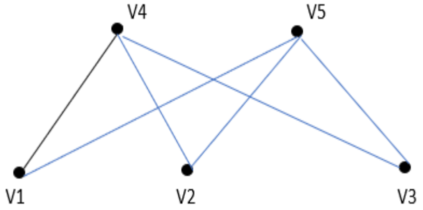
The Graph is bipartite because its vertex set is the union of two disjoint sets, $V_1 = \{a, b, d\}$ and $V_2 = \{c, e, f, g\}$, and each edge has one end vertex in V_1 and the other end vertex in V_2.

Do you know? : For which values of n are these graphs bipartite? a) K_n b) C_n c) W_n

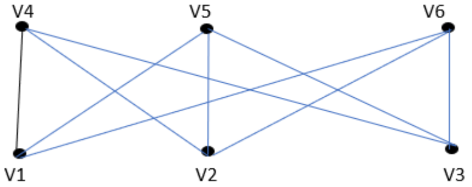
In a bipartite graph if all the vertices of V_1 is adjacent to all the vertices of V_2, it is said to be **complete bipartite**. It is denoted by $K_{m,n}$.



Bipartite Graph



Complete Bipartite Graph $K_{2,3}$



Complete Bipartite Graph $K_{3,3}$

Note: Complete bipartite graph $K_{2,3}$ have 2×3=6 edges.

Example: Prove that maximum number of edges in a bipartite graph with n vertices is $\frac{n^2}{4}$.

A bipartite graph with $|V_1| = n_1$ and $|V_2| = n_2$ vertices set have $n_1 \times n_2$ edges subject to $n_1 + n_2 = n$.

Therefore maximum number of edges is attained when number of vertices $n_1 = n_2 = \frac{n}{2}$ (if n is even)

Therefore maximum number of edges of a bipartite graph with n vertices is $\frac{n}{2} \times \frac{n}{2} = \frac{n^2}{4}$.

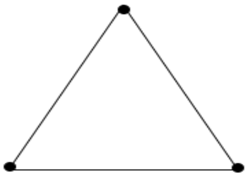
Note: If n is odd, then $n_1 = \frac{n-1}{2}$, $n_2 = \frac{n+1}{2}$

Therefore maximum number of edges of a bipartite graph with n vertices is $\frac{n-1}{2} \times \frac{n+1}{2} = \frac{n^2 - 1}{4} < \frac{n^2}{4}$.

Therefore maximum number of edges in a bipartite graph with n vertices is $\leq \frac{n^2}{4}$

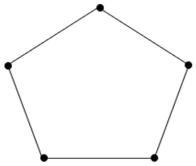
Definition: Alternating sequence of vertices and edges starting and ending with vertices such that no edge or vertex repeated more than once except the starting vertex is called a **cycle**. It is denoted by C_n.

Alternatively, A cycle C_n, $n \geq 3$, consists of n vertices $v_1, v_2, v_3, ...v_{n-1}, v_n$ and edges $(v_1, v_2), (v_2, v_3), (v_3, v_4), ..., (v_{n-1}, v_n), (v_n, v_1)$.



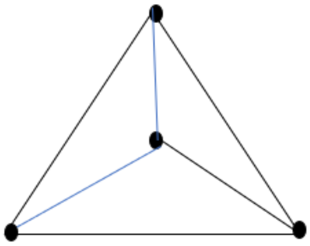
C_3

C_4

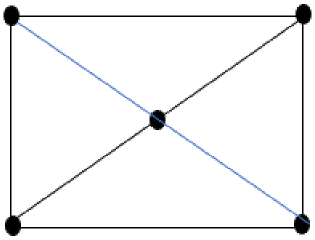


C_5

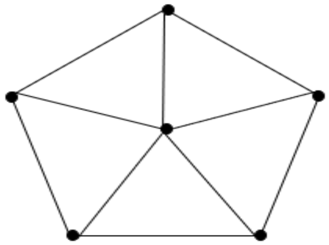
Definition: A **wheel** graph W_n contain an additional vertex to the cycle C_n and connect this new vertex to the n vertices of C_n by a new edges.



W_3



W_4



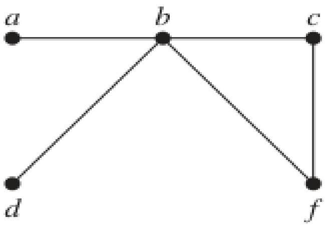
W_5

Do you know? : For which values of m, n are these graphs regular? a) K_n b) C_n c) W_n d) $K_{m,n}$

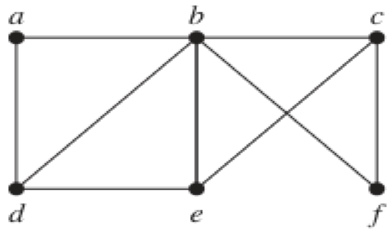
Definition: A graph H is said to be a **subgraph** of a graph G if all the vertices and all the edges of H are in G, and each edge of H has the same end vertices in H as in G. It is denoted by $H \subset G$.

Note:

- Every graph is its own subgraph.
- A single vertex in a graph G is a subgraph of G.
- A single edge in G, together with its end vertices, is also a subgraph of G.



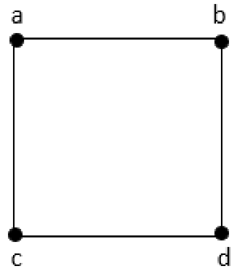
Subgraph H of G



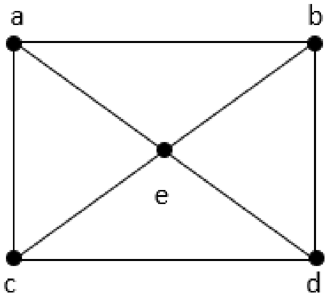
Graph G

A sub graph can be obtained by deleting a vertex from the given graph. **Deletion of a vertex** means the vertex and all edges incident on it.

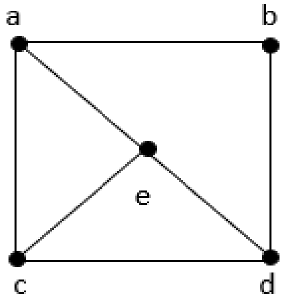
A sub graph can be obtained by deleting an edge from the given graph. **Deletion of an edge** means the edge only and not the end vertices.



Subgraph obtained by deleting an vertex e



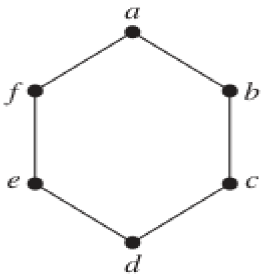
Given Graph



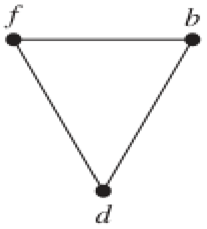
Subgraph obtained by deleting an edge (b, e)

Try this: Draw the complete graph K_5 with vertices A, B, C, D, E. Draw all complete sub graph of K_5 with 4 vertices.
(By deleting each vertices one by one, we get a complete subgraph with 4 vertices)

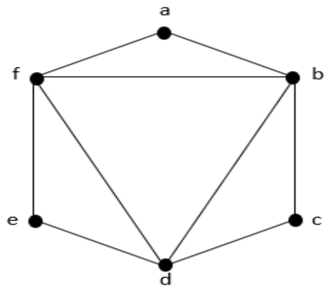
Definition: Let $G_1 = \{V_1, E_1\}$ and $G_2 = \{V_2, E_2\}$ be any two graphs. The union of two graphs is a graph G whose vertex set is $V = V_1 \cup V_2$ and edge set is $E = E_1 \cup E_2$.



$G_1 = \{V_1, E_1\}$

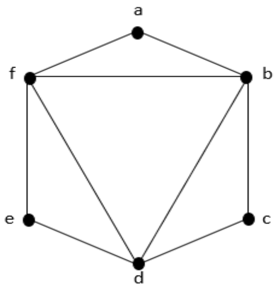


$G_2 = \{V_2, E_2\}$

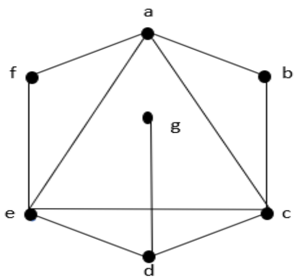


$G = G_1 \cup G_2$

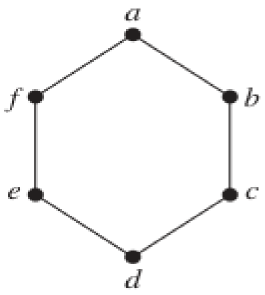
Definition: Let $G_1 = \{V_1, E_1\}$ and $G_2 = \{V_2, E_2\}$ be any two graphs. The intersection of two graphs is a graph G whose vertex is $V = V_1 \cap V_2$ and edge is $E = E_1 \cap E_2$.



$G_1 = \{V_1, E_1\}$



$G_2 = \{V_2, E_2\}$



$G = G_1 \cap G_2$

https://doi.org/10.5281/zenodo.15287638

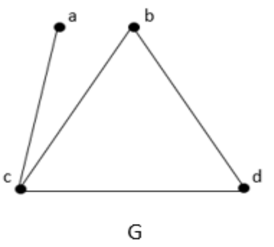
Matrix Representation of Graphs:

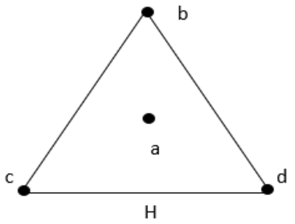
Adjacency Matrix : Suppose $G=\{V, E\}$ is a simple graph where $V=\{v_1, v_2, v_3, ...v_{n-1}, v_n\}$. The adjacency matrix $A(G)=\left[a_{ij}\right]$ is an $n \times n$ matrix, where

$$\begin{aligned} a_{ij} &= 1, \ \textit{if} \ \left(v_i, v_j\right) \ \textit{is and edge of} \ G \\ &= 0, \ \textit{otherwise} \end{aligned}$$

Note: For multigraph/pseudograph the $(i, j)^{th}$ entry of this matrix equals the number of edges that are associated to $\left(v_i, v_j\right)$.

Example: Use an adjacency matrix to represent the simple graphs shown here:

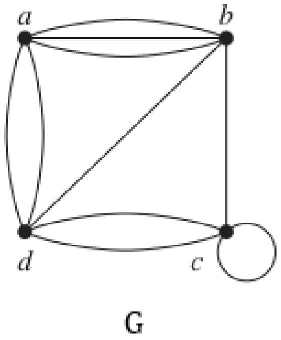




We order the vertices as a, b, c, d. The adjacency matrix representing the graph G and H is

$$A(G)=\begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\!\!\begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array} \quad \text{and} \quad A(H)=\begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\!\!\begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Example: Use an adjacency matrix to represent the pseudo graph shown here:



We order the vertices as a, b, c, d. The adjacency matrix representing the pseudograph G is

$$A(G)=\begin{array}{c} \\ a \\ b \\ c \\ d \end{array}\!\!\begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 \end{pmatrix} \end{array}$$

Some Observations of Adjacent Matrix

- Adjacency matrix of a graph is based on the ordering chosen for the vertices. Hence, there are n! different adjacency matrices for a graph with n vertices.

- The adjacency matrix of a graph is symmetric
- Entry 1 in the $(i,i)^{th}$ position represents the loop at the vertex v_i.
- Sum of elements of a row or column represents the degree of the vertex.
- Two graphs G and H are isomorphic if and only if their adjacency matrices $A(G)$ and $A(H)$ are related as $P^{-1}A(G)P = A(H)$ where P is a permutation matrix.

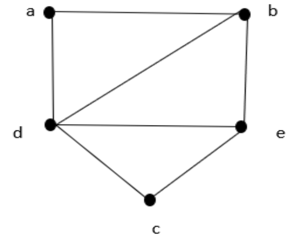
  (A matrix whose rows are the rows of the unit matrix, but not necessarily in the same order, is called a permutation matrix)

Example: Draw a graph with the adjacency matrix $A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

Let a, b, c, d, e be the ordering of vertices. Then the edges are given by the pairs of vertices (a,b), (a,d), (b,a), (b,d), (b,e), (c,d), (c,e), (d,a), (d,b), (d,c), (d,e), (e,b), (e,c), (e,d).

Because of symmetry, removing the repetitions, we have (a,b), (a,d), (b,d), (b,e), (c,d), (c,e), (d,e)

The graph is given here.



Theorem: If A is the adjacency matrix of a graph G with $V(G)=\{v_1, v_2, ..., v_n\}$, prove that for any $n \geq 1$, the $(i,j)^{th}$ entry of A^n is the number of $v_i - v_j$ walks of length n in G.

Proof: We prove this by mathematical induction.

Suppose G is a graph with vertices $v_1, v_2, ..., v_n$ and A is the adjacency matrix of G.

Let $P(n)$: For all integers $i, j = 1,2,3,.....,n$, the $(i,j)^{th}$ entry of A^n is the number of walks of length n from v_i *to* v_j in G.

To prove $P(1)$ is true:

The $(i,j)^{th}$ entry of A^1 = the $(i,j)^{th}$ entry of A

= number of edges connecting v_i *to* v_j (by definition of adjacency matrix)

= number of walks of length 1 from v_i *to* v_j (walk of length 1 is an edge)

Assume that $P(k)$ is true:

https://doi.org/10.5281/zenodo.15287638

$\therefore$ The $(i, j)^{th}$ entry of $A^k =$ number of walks of length k from v_i *to* v_j

To prove $P(k+1)$ is true:

Let $A = \left(a_{ij}\right)$ and $A^k = \left(b_{ij}\right)$. Also $A^{k+1} = A \,.\, A^k$

$\therefore$ $(i, j)^{th}$ entry of $A^{k+1} =$ $(i)^{th}$ row of A $\times$ $(j)^{th}$ column of A^k

$$= a_{i1}.b_{1j} + a_{i2}.b_{2j} + \ldots\ldots + a_{in}.b_{nj}$$

Here a_{i1} is the number of edges from v_i *to* v_1 and b_{1j} is the number of walks of length k from v_1 *to* v_j.

$\therefore$ combining these two edge and walk, we get

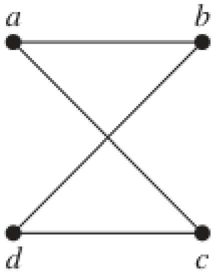
$a_{i1}.b_{1j} =$ the number of walks of length $k+1$ from v_i *to* v_j with v_1 as its second vertex.

In general, $a_{im}.b_{1m} =$ the number of walks of length $k+1$ from v_i *to* v_j with v_m as its second vertex.

$\therefore$ $(i, j)^{th}$ entry of $A^{k+1} =$ the number of walks of length $k+1$ from v_i *to* v_j.

Hence by induction hypothesis, $(i, j)^{th}$ entry of $A^n =$ the number of walks of length n from v_i *to* v_j.

Example: How many walks of length four are there from a *to* d in the following simple graph G.



The adjacency matrix of the given graph is

$$A(G) = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

https://doi.org/10.5281/zenodo.15287638

$$A^2 = A \times A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \end{bmatrix}$$

$$A^4 = A^2 \times A^2 = \begin{bmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \end{bmatrix} \times \begin{bmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 8 & 0 & 0 & \boxed{8} \\ 0 & 8 & 8 & 0 \\ 0 & 8 & 8 & 0 \\ 8 & 0 & 0 & 8 \end{bmatrix}$$

Hence there are 8 walks of length four from $a \ to \ d$. They are

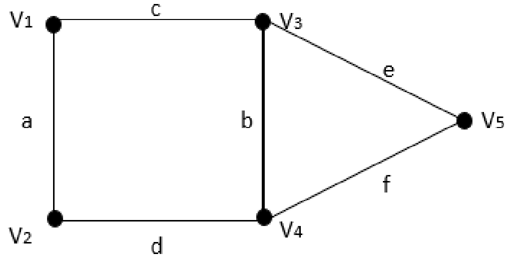
(1) $a\ b\ a\ b\ d$ (2) $a\ b\ a\ c\ d$ (3) $a\ b\ d\ b\ d$ (4) $a\ b\ d\ c\ d$

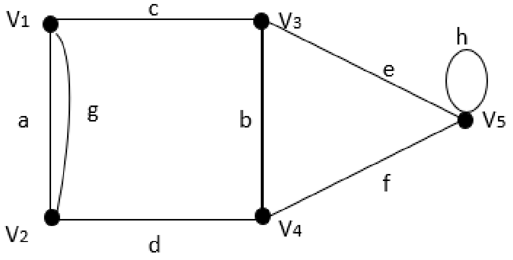
(5) $a\ c\ a\ b\ d$ (6) $a\ c\ a\ c\ d$ (7) $a\ c\ d\ b\ d$ (8) $a\ c\ d\ c\ d$

Incidence Matrix : Suppose $G = \{V, E\}$ is a simple graph where $E = \{e_1, e_2, e_3, ...e_{m-1}, e_m\}$ and $V = \{v_1, v_2, v_3, ...v_{n-1}, v_n\}$. The Incidence matrix $I(G) = \left[a_{ij}\right]$ is an $n \times m$ matrix, where

$$\begin{aligned} a_{ij} &= 1, \ if \ edge \ e_j \ is \ incident \ with \ v_i \\ &= 0, \ otherwise \end{aligned}$$

Example: Use an incidence matrix to represent the graphs shown here:





We order the vertices v_1, v_2, v_3, v_4, v_5 row wise and edges a, b, c, d, e, f column wise. The incidence matrix representing the graph is

$$I(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

We order the vertices v_1, v_2, v_3, v_4, v_5 row wise and edges a, b, c, d, e, f, g, h column wise. The incidence matrix representing the graph is

$$I(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} a & b & c & d & e & f & g & h \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

Some Observations of Incidence Matrix

- Since every edge is incident on exactly two vertices, each column of $I(G)$ has exactly two l′s.
- Only one 1's in a column represent a loop
- The number of l′s in each row equals the degree of the corresponding vertex(for simple graph)
- A row with all 0′s represents an isolated vertex
- Parallel edges in a graph produce identical columns in its incidence matrix
- Permutation of any two rows or columns in an incidence matrix simply corresponds to relabelling the vertices and edges of the same graph
- Two graphs G and H are isomorphic if and only if their incidence matrices $I(G)$ and $I(H)$ differ only by permutations of rows and columns

Example: Using the incidence matrix of a graph G, show that the sum of the degrees of vertices of a graph G is equal to twice the number of edges of G.

Let G be a simple graph and $I(G)$ represents its incidence matrix. We know that the number of l′s in each row equals the degree of the corresponding vertex. Therefore total degrees of all vertices is sum of all 1's in the incidence matrix.

By definition of incidence matrix, each column, representing an edge, contains exactly two 1's.

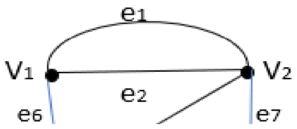
Therefore Total degrees of G = (Total number of 1's in incidence matrix)
= 2 (number of columns)
= 2 (edges)

Traversing a graph

Definition: A walk of a graph $G=\{V, E\}$ is a finite alternating sequence of vertices and edges $W=\{v_1\, e_1\, v_2\, e_2 \ldots e_{k-1}\, v_{k-1}\, e_k\, v_k\}$, starting and ending with vertices such that each edge is incident with the vertices preceding and succeeding it.

Note:

- In a walk vertices may be repeated but not edges.
- If starting and vertices are same vertex, it is called closed walk, otherwise, it is called open walk.
- A open walk is said to be a path, if the edges and vertices are distinct.
- The number of edges in a path is called the length of a path.
- A closed walk in which no vertex (except the initial and the final vertex) appears more than once is called a circuit.
- A circuit is a closed non intersecting walk



Open Walk $W=\{v_1\, e_6\, v_3\, e_5 v_3\, e_4\, v_4 e_7\, v_2\}$

Closed Walk $W=\{v_1\, e_6\, v_3\, e_5 v_3\, e_4\, v_4 e_7\, v_2 e_1\, v_1\}$

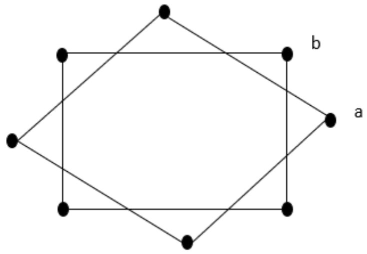
Open Path $P=\{v_1 e_6 v_3 e_4 v_4 e_7 v_2\}$

Closed Path/Circuit $P=\{v_1 e_6 v_3 e_4 v_4 e_7 v_2 e_2 v_1\}$

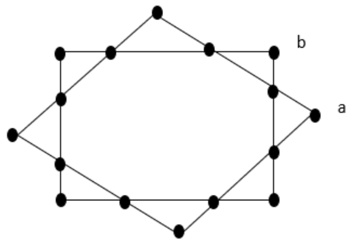
Can we say that a closed walk is a circuit?

Definition: A vertex u of a graph G is said to be reachable from a vertex v, if there is a path from u to v. A graph G is said to be connected if there is a path from every pair of vertices of G. Otherwise G is said to be disconnected.

Note: A disconnected graph comprised of components.



Disconnected Graph as there is no path between a and b.



Connected graph

Theorem: Prove that a graph G is disconnected if and only if its vertex set V can be partitioned into two non empty, disjoint subsets U and W such that there exists no edge in G whose one end vertex is in subset U and other in subset W.

Proof: Suppose that vertex set V of a graph G can be partitioned into two non empty disjoint subsets U and W as stated. Consider two arbitrary vertices $'a'$ & $'b'$ of G such that $a \in U$ and $b \in W$. No path can exists between vertices $'a'$ & $'b'$. Otherwise there would be at least one edge whose one end vertex be in U and the other in W. Hence if partition exists, G is disconnected.

Conversely, let G be a disconnected graph. Consider a vertex $'a'$ in G. Let U be the set of all vertices that are joined by paths to $'a'$. Since G is disconnected, U does not includes all the vertices of G. The remaining vertices will form a set W. No vertices in U is joined to any vertex in W by an edge. Hence the partition exists.

Theorem: Prove that the maximum number of edges in a simple graph with n vertices is $\dfrac{n(n-1)}{2}$.

Proof: We prove this by induction on number of vertices of a graph. Let $P(n) : \dfrac{n(n-1)}{2}$

Let $n=1$. Then the graph is isolated vertex and hence it has no edges. Also $P(1) : \dfrac{1(1-1)}{2}=0$ edges

Let $n=2$. Then the simple graph has one edge only. Also $P(2) : \dfrac{2(2-1)}{2}=1$ edge.

Assume that the statement is true for $n=k$ vertices. Then the graph has $P(k):\dfrac{k(k-1)}{2}=1$ edges.

Let the graph has $n=k+1$ vertices. We have to prove $P(k+1):\dfrac{(k+1)((k+1)-1)}{2}$

Now introduce the new vertex to the previous graph with k vertices and join it with new edges to the already existing k vertices i.e. k edges.

Therefore total number of edges is $=\dfrac{k(k-1)}{2}+k$

$$=\frac{k(k-1)+2k}{2}$$

$$=\frac{k^2+k}{2}$$

$$=\frac{k(k+1)}{2}$$

$$=\frac{(k+1)((k+1)-1)}{2}$$

Hence by induction, the statement is true for n vertices. i.e. $P(n):\dfrac{n(n-1)}{2}$

Alternate Proof:

Let G be a simple graph with n vertices. By hand shaking theorem, $\sum\deg(v_i)=2e$, where e is number of edges.

$$\deg(v_1)+\deg(v_2)+.....+\deg(v_n)=2e$$

$$(n-1)+(n-1)+.....+(n-1)=2e \text{ \{maximum edges possible for complete graph\}}$$

$$n(n-1)=2e$$

$$e=\frac{n(n-1)}{2}$$

Theorem: Prove that a simple graph with n vertices and k components can have at most $\dfrac{(n-k)(n-k+1)}{2}$ edges.

Proof: Let G be a simple graph with n vertices and k components.

Let n_1, n_2, n_3,........, n_k be the number of vertices of k components of the graph G.

Therefore $n_1+n_2+n_3+........+n_k=n$.

https://doi.org/10.5281/zenodo.15287638

Since G is simple, each component is simple. We know that a simple graph with n vertices can have maximum $\frac{n(n-1)}{2}$ edges.

Therefore total number of edges of $G =$ Sum of maximum of number of edges of each components

$$= \frac{n_1(n_1-1)}{2} + \frac{n_2(n_2-1)}{2} + \ldots.. + \frac{n_k(n_k-1)}{2}$$

$$= \sum_{i=1}^{k} \frac{n_i(n_i-1)}{2}$$

$$= \frac{1}{2}\sum_{i=1}^{k}\left(n_i^2 - n_i\right)$$

$$= \frac{1}{2}\sum_{i=1}^{k} n_i^2 - \frac{1}{2}\sum_{i=1}^{k} n_i$$

$$= \frac{1}{2}\sum_{i=1}^{k} n_i^2 - \frac{1}{2}n \ldots\ldots..(1)$$

Consider $\sum_{i=1}^{k}(n_i-1) = \sum_{i=1}^{k} n_i - \sum_{i=1}^{k} 1$

$$\sum_{i=1}^{k}(n_i-1) = n-k$$

Squaring on both sides

$$\left[(n_1-1)+(n_2-1)+\ldots..+(n_k-1)\right]^2 = (n-k)^2$$

$$\left[(n_1-1)^2+(n_2-1)^2+\ldots..+(n_k-1)^2 + \textit{positive terms}\right] = n^2+k^2-2nk$$

$$\left[\left(n_1^2+1-2n_1\right)+\left(n_2^2+1-2n_2\right)+\ldots..+\left(n_k^2+1-2n_k\right)\right] \le n^2+k^2-2nk$$

$$\sum_{i=1}^{k} n_i^2 - 2\sum_{i=1}^{k} n_i + k \le n^2+k^2-2nk$$

$$\sum_{i=1}^{k} n_i^2 - 2n + k \le n^2+k^2-2nk$$

$$\sum_{i=1}^{k} n_i^2 \le n^2+k^2-2nk+2n-k$$

$$\sum_{i=1}^{k} n_i^2 \le n^2+k^2-2nk+2n-k \ldots\ldots\ldots..(2)$$

Substitute (2) in (1)

https://doi.org/10.5281/zenodo.15287638

Total number of edges of $G \leq \frac{1}{2}\left(n^2+k^2-2nk+2n-k\right)-\frac{1}{2}n$

$$\leq \frac{1}{2}\left[n^2+k^2-2nk+2n-k-n\right]$$

$$\leq \frac{1}{2}\left[\left(n-k\right)^2+n-k\right]$$

$$\leq \frac{1}{2}\left(n-k\right)\left(n-k+1\right)$$

Example: Show that a simple graph G with n vertices is connected if it has more than $\frac{(n-1)(n-2)}{2}$ edges.

Let G be a simple graph with n vertices and $|E|$ number of edges.

Given that $|E| > \frac{(n-1)(n-2)}{2}$

Claim: To prove G is connected.

Suppose G is disconnected with 2 components.

Therefore by previous theorem, $|E| \leq \frac{\left(n-2\right)\left(n-2+1\right)}{2}$

$$|E| \leq \frac{\left(n-1\right)\left(n-2\right)}{2}$$

Thus if G is disconnected, then $|E| \leq \frac{\left(n-1\right)\left(n-2\right)}{2}$.

Therefore the contra positive statement is if $|E| \geq \frac{\left(n-1\right)\left(n-2\right)}{2}$ then G is connected.

Theorem: If G is a simple graph with $\delta(G) \geq \frac{|V(G)|}{2}$ then G is connected.

Proof: Let G be a simple graph with number of vertices is $|V(G)| = n$ and $\delta(G) =$ minimum degree of G.

Let degree of all vertices of G is $\geq \frac{n}{2}$. i.e. $\delta(G) \geq \frac{n}{2}$.

Claim: G is connected graph

Let u, v be any two vertices in G. Let X be the set of all vertices which are adjacent to u and Y be the set of vertices which are adjacent to v. Then $d(u) = |X|$ and $d(v) = |Y|$.

Therefore number of vertices of union of X and Y is $|X \cup Y| \leq n-2$ because $u, v \notin \left(X \cup Y\right)$.

https://doi.org/10.5281/zenodo.15287638

Then $\left|X\right| = d(u) \geq \delta(G) \geq \left\lfloor \frac{n}{2} \right\rfloor$ and $\left|Y\right| = d(v) \geq \delta(G) \geq \left\lfloor \frac{n}{2} \right\rfloor$

Therefore $\left|X\right| + \left|Y\right| \geq \left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor \geq n-1$

Consider

$$\left|X \cup Y\right| + \left|X \cap Y\right| = \left|X\right| + \left|Y\right|$$

$$\left|X \cap Y\right| = \left|X\right| + \left|Y\right| - \left|X \cup Y\right|$$

$$\geq (n-1) - (n-2) = 1$$

$$\left|X \cap Y\right| \geq 1$$

Since $X \cap Y \neq \phi$, choose a vertex $w \in \left(X \cap Y\right)$. Then uw and wv are edges, then uwv is an $u-v$ path in G.

Thus for every pair of distinct vertices in G there is a path between them, Hence G is connected.

Theorem: Let G be a graph (connected or disconnected) with exactly two vertices has odd degree. Then prove that there is a path between those two vertices.

Proof: Let G be a graph with all even vertices except vertices u and v, which are odd. We know that in any graph, the number of odd degree vertices are even. Since the given graph has exactly two odd degree vertices u & v, they belong to the same component. Hence there must be a path between u and v.

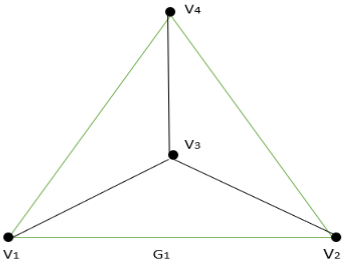
https://doi.org/10.5281/zenodo.15287638

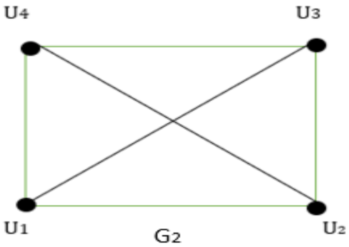
ISOMORPHISM

Two graphs G_1 and G_2 are said to isomorphic if there exists a one-to-one correspondence between their vertices, edges which preserves the incidence relationship.
i.e. the graphs must have

i. same number of edges
ii. same number of vertices
iii. incidence relationship.

Example 1: Establish an isomorphism for the following graphs.

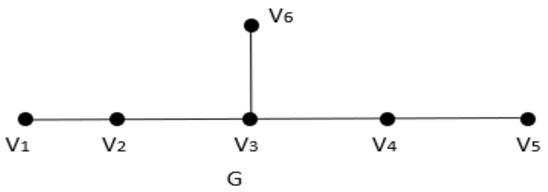


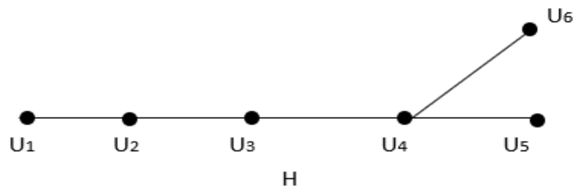


Let us compare the nature of both the graphs:

Description	G_1	G_2
Number of vertices	3	3
Number of edges	6	6
Vertex with degree	4 vertices with degree 3	4 vertices with degree 3
Circuits with length	4 circuits with length 3 3 circuits with length 4	4 circuits with length 3 3 circuits with length 4
Mapping	$f(v_1)$ *in* $G_1 = f(u_1)$ *in* G_2 $\quad$ $f(v_3)$ *in* $G_1 = f(u_3)$ *in* G_2 $f(v_2)$ *in* $G_1 = f(u_2)$ *in* G_2 $\quad$ $f(v_4)$ *in* $G_1 = f(u_4)$ *in* G_2	
In both the graphs, since all vertices are of same degree, adjacency relationship is preserved. Hence both the graphs are isomorphic		

Example 2: Establish the isomorphism of the following pairs of graphs.

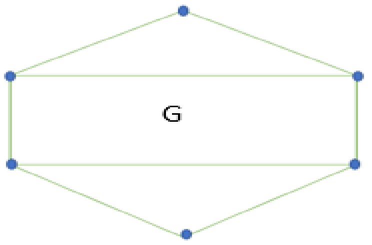


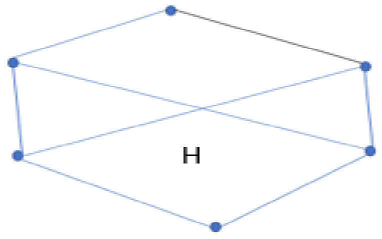


Let us compare the nature of both the graphs:

Description	G	H
Number of vertices	6	6
Number of edges	5	5
Vertex with degree	2 vertices with degree 2 3 vertices with degree 1 1 vertex with degree 3	2 vertices with degree 2 3 vertices with degree 1 1 vertex with degree 3
Circuits with length	No circuit exists	No circuit exists
Even though the above data are common in both the graphs, they are not isomorphic as the adjacency relationship is not preserved. Consider the vertices v_3 in G and u_4 in H. Both are of degree 3. Hence they are mapped. But the adjacent vertices of v_3 having the degrees 2, 2, 1. But the adjacent vertices of u_4 having the degrees 1, 1, 2. i.e. the adjacency relationship is not preserved. Hence both the graphs are **not isomorphic.**		

Example 3: Check whether the following graphs are isomorphic or not.





Let us compare the nature of both the graphs:

Description	G	H
Number of vertices	6	6
Number of edges	8	8
Vertex with degree	2 vertices with degree 2	2 vertices with degree 2

https://doi.org/10.5281/zenodo.15287638

	4 vertices with degree 3	4 vertices with degree 3
Circuits of length	2 circuits of length 3 1 circuit of length 4 1 circuit of length 6 2 circuits of length 5	0 circuit of length 3 5 circuits of length 4 3 circuit of length 6 0 circuits of length 5
Considering the above facts about the circuits, we conclude that both the graphs are **not isomorphic.**		

Example 4: Are the simple graphs with the following adjacency matrices isomorphic?

$$A(G_1)=\begin{pmatrix}0&0&1\\0&0&1\\1&1&0\end{pmatrix} \quad and \quad A(G_2)=\begin{pmatrix}0&1&1\\1&0&0\\1&0&0\end{pmatrix}$$

The degree sequence of both the matrices are 1, 1, 2 and 2, 1, 1. Therefore

Consider

$$A(G_1)=\begin{pmatrix}0&0&1\\0&0&1\\1&1&0\end{pmatrix}$$

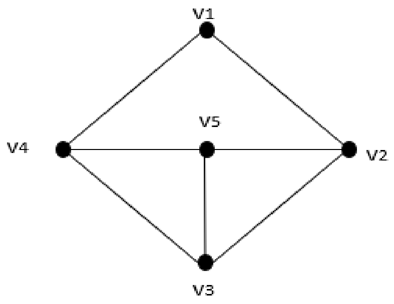
$$=\begin{pmatrix}1&0&0\\1&0&0\\0&1&1\end{pmatrix} \operatorname{int} erchanging\ C_1 \leftrightarrow C_3$$

$$=\begin{pmatrix}0&1&1\\1&0&0\\1&0&0\end{pmatrix} \operatorname{int} erchanging\ R_1 \leftrightarrow R_3$$

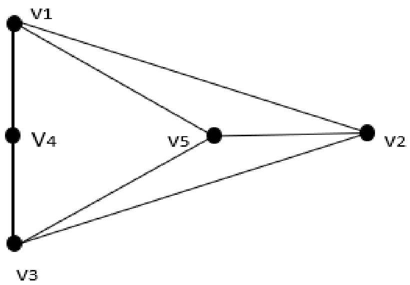
$$= A(G_2)$$

Hence G_1 and G_2 are isomorphic.

Example 5: Establish the isomorphism of the following pairs of graphs, by considering their adjacency matrices.



G1



G2

Example 6: Are the simple graphs with the following adjacency matrices isomorphic?

$$A(G_1)=\begin{pmatrix}1&1&0&0&0\\1&0&1&0&1\\0&0&0&1&1\\0&1&1&1&0\end{pmatrix}\quad and \quad A(G_2)=\begin{pmatrix}0&1&0&0&1\\0&1&1&1&0\\1&0&0&1&0\\1&0&1&0&1\end{pmatrix}$$

The degree sequence of both the matrices are 2, 3, 2, 3 and 2, 3, 2, 3. Therefore Consider

$$A(G_1)=\begin{pmatrix}1&1&0&0&0\\1&0&1&0&1\\0&0&0&1&1\\0&1&1&1&0\end{pmatrix}$$

$$=\begin{pmatrix}1&0&0&0&1\\1&1&1&0&0\\0&1&0&1&0\\0&0&1&1&1\end{pmatrix}\text{int}\, erchanging\ C_2 \leftrightarrow C_5$$

$$=\begin{pmatrix}0&1&0&0&1\\1&1&1&0&0\\1&0&0&1&0\\0&0&1&1&1\end{pmatrix}\text{int}\, erchanging\ C_1 \leftrightarrow C_2$$

$$=\begin{pmatrix}0&1&0&0&1\\0&1&1&1&0\\1&0&0&1&0\\1&0&1&0&1\end{pmatrix}\text{int}\, erchanging\ C_1 \leftrightarrow C_4$$

$$= A(G_2)$$

Hence G_1 and G_2 are isomorphic.

Example 7: The adjacency matrices of two pairs of graph as given below: Examine the isomorphism of G and H by finding a permutation matrix.

$$A_G = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, A_H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Solution: Let v_1, v_2, v_3 be the vertices of G and u_1, u_2, u_3 be the vertices of H.
Considering the degree of vertices of G and H, permutation matrix P can be obtained as follows:
Since $\deg(v_1) = \deg(u_2)$, the first row of I_3 can be taken as second row of P.
Also $\deg(v_2) = \deg(u_3)$, the second row of I_3 can be taken as third row of P.
And $\deg(v_3) = \deg(u_1)$, the third row of I_3 can be taken as first row of P.

$$\text{Hence } P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Consider

$$\begin{aligned} PGP^T &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\ &= H \end{aligned}$$

Therefore the graphs G and H are isomorphic.

Example 8: Are the simple graphs with the following adjacency matrices isomorphic?

$$A(G_1) = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad \textit{and} \quad A(G_2) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

The degree sequence of both the matrices are 2, 2, 1, 3 and 3, 2, 2, 3 and hence sum of degrees are not equal. Therefore given graphs G_1 and G_2 are not isomorphic

Definition: A property P is called an invariant for graph isomorphism if, and only if, given any graphs G_1 and G_2, if G_1 has property P and G_2 is isomorphic to G_1, then G_2 has property P.

The following properties is an invariant for graph isomorphism, where n, m and k are all nonnegative integers:

1. has n vertices	2. has m edges
3. has a vertex of degree k	4. has m vertices of degree k
5. has m circuits of length k	6. is connected
7. has an Euler circuit	8. has a Hamiltonian circuit.

Suppose G_1 and G_2 are two graphs which are isomorphic. Then there exists a $1-1$ function f between their vertex and edge set. Hence number of vertices and edges of both the graphs are equal.

By definition of isomorphism, the mapping f preserves incidence relationship so that both the graphs have equal number of vertices with a given degree. This can be verified by the adjacency matrix of the respective graphs. If $A(G_1) = A(G_2)$ it follows that f preserves edges and hence degree sequence and connectedness as well.

Refer example 3 for counter example for invariant property of circuit of a particular length.

Theorem: Show that isomorphism of simple graphs is an equivalence relation.

Proof: Let S be set of graphs and let R be the relation of graph isomorphism on S. Then R is an equivalence relation on S.

1. Reflexive

Given any graph G in S, define a graph isomorphism from G to G by using the identity functions on the set of vertices and on the set of edges of G. Hence isomorphism is reflexive.

Mapping: Define $f: V(G) \to V(G)$ by $f(v) = v$ and $g: E(G) \to E(G)$ by $g(e) = e$.

2. Symmetric

Let G_1, $G_2 \in S$ such that G_1 is isomorphic to G_2. Then there exists a one-to-one correspondence f from G_1 to G_2 that preserves adjacency and non adjacency. From this g is a one-to-one correspondence from G_2 to G_1 that preserves adjacency and non adjacency. Hence isomorphism is symmetric.

Mapping for vertices: $f: V(G_1) \to V(G_2)$ by $f(v) = w$ and $g: V(G_2) \to V(G_1)$ then $g(w) = f^{-1}(w)$. Therefore G_2 is isomorphic to G_1.

3. Transitive

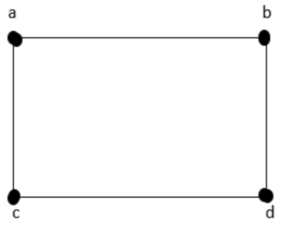
Let G_1, G_2, $G_3 \in S$ such that G_1 is isomorphic to G_2 and G_2 is isomorphic to G_3. Then there exists a one-to-one correspondence f from G_1 to G_2 and g from G_2 to G_3 that preserves adjacency and non adjacency. It follows that $g \circ f$ is a one-to-one correspondence from G_1 to G_3 that preserves adjacency and non adjacency. Hence isomorphism is transitive.

Mapping for vertices: $f:V(G_1)\rightarrow V(G_2)$, $g:V(G_2)\rightarrow V(G_3)$ by $f(u)=v,\ g(v)=w$ then $(g\circ f):V(G_1)\rightarrow V(G_3)$ defined by $(g\circ f)(u)=g\left[f(u)\right]=w$. Therefore G_1 is isomorphic to G_3.

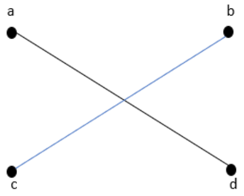
Definition: Let G be a simple graph and $\overline{G}$ is said to be **complement** of G, if vertices set of $\overline{G}$ is same as G and two vertices of $\overline{G}$ is adjacent if they are not adjacent in G.

Note:

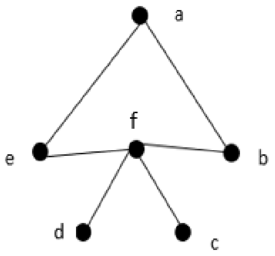
- Union of a graph and its complement is a complete graph i.e. $G\cup\overline{G}=K_n$
- If G and $\overline{G}$ are isomorphic, then G is said to be self complement.



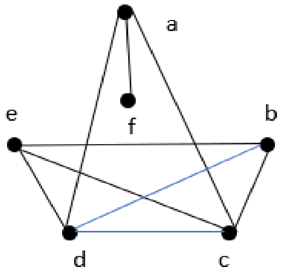
G



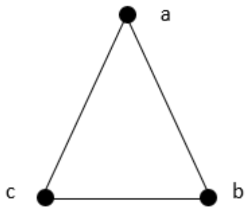
$\overline{G}$



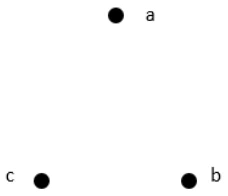
G



$\overline{G}$



G



$\overline{G}$

Theorem: Prove that the complement of a disconnected graph is connected.

Proof: Let G be a disconnected graph and let $\overline{G}$ be its complement. Consider two vertices $x,\ y$ in the complement. If $x\,\&\,y$ are not adjacent in G, then they will be adjacent in $\overline{G}$ and there exists a trivial $x-y$ path. If $x\,\&\,y$ are adjacent in G, then they must be in the same component. Let z be some vertex

https://doi.org/10.5281/zenodo.15287638

in another component of G. This means that the edges xz and yz were not in G. This implies that they both must be edges in $\overline{G}$. This gives us the path $x-z-y$. Therefore there exists a path between any two vertices and hence it is connected.

Example: If G is a simple graph with 15 edges and $\overline{G}$ has 13 edges, how many vertices does G have?

We know that G and $\overline{G}$ have same number of vertices, say n.

Union of G and $\overline{G}$ have 15 + 13 = 28 edges.

But Union of G and $\overline{G}$ is a complete graph with $\frac{n(n-1)}{2}$ edges

Therefore $\frac{n(n-1)}{2}=28$

$$n(n-1)=56$$

$$8\times 7=56$$

$$\therefore n=8$$

Do you know?: If the degree sequence of the simple graph G is 4, 3, 3, 2, 2, what is the degree sequence of $\overline{G}$?

Theorem: If G is self-complementary graph with n vertices, then G has $n\equiv 0$ (or) 1(mod 4) vertices.

Proof: We know that union of a graph and its complementary graph gives a complete graph which has $\frac{n(n-1)}{2}$ edges. Therefore n or $(n-1)$ must be even.

Also we know that a graph and its self complementary graph has equal number of vertices and edges.

Since G is self-complementary graph with n vertices, then G has $\frac{n(n-1)}{4}$ edges.

Therefore either 4 divides n or 4 divides $(n-1)$.

Therefore, $n\equiv 0(\text{mod}\,4)$ or $n\equiv 1(\text{mod}\,4)$

Example: Prove that C_5 is the only cycle graph isomorphic to its complement.

Solution: We know that a cycle graph of n vertices has n edges.

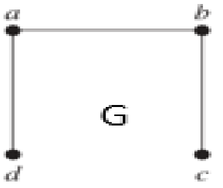
Also the complete graph of n vertices has $\frac{n(n-1)}{2}$ edges.

Therefore if C_n is isomorphic to its complement, its complement has $\frac{n(n-1)}{4}$ edges.

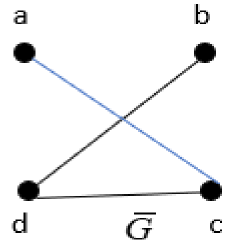
https://doi.org/10.5281/zenodo.15287638

Hence $\frac{n(n-1)}{4} = n$. i.e. $n-1=4$. i.e. $n=5$

Example: Show that the graph G is self-complementary.



The complementary of the graph is $\overline{G}$.

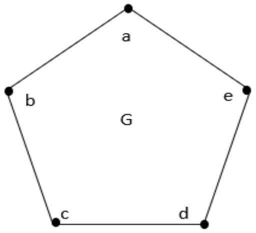


Let us establish the isomorphism between the graphs:

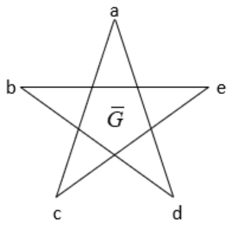
Description	G	$\overline{G}$
Number of vertices	4	4
Number of edges	3	3
Vertex with degree	2 vertices with degree 1 2 vertices with degree 2	2 vertices with degree 1 2 vertices with degree 2
Circuits of length	No circuit exists	No circuit exists
Mapping	$f(a)\ in\ \overline{G} = f(d)\ in\ G$ $f(b)\ in\ \overline{G} = f(c)\ in\ G$	$f(c)\ in\ \overline{G} = f(a)\ in\ G$ $f(d)\ in\ \overline{G} = f(b)\ in\ G$
Considering the above facts, we conclude that both the graphs are **isomorphic.** Hence the given graph G is **self complementary**.		

.

Example: Show that the graph G is self-complementary.



The complementary of the graph is $\overline{G}$.



Let us establish the isomorphism between the graphs:

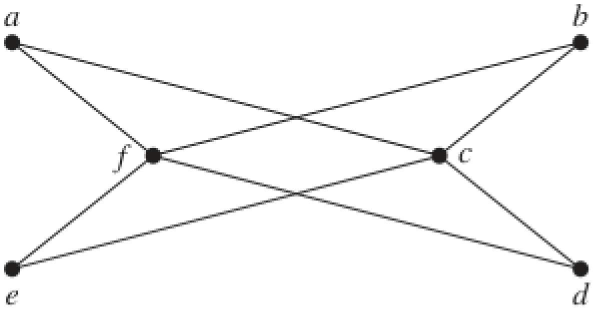
Description	G	$\overline{G}$

Number of vertices	5	5
Number of edges	5	5
Vertex with degree	5 vertices with degree 2	5 vertices with degree 2
Circuits of length	One circuit of length 5	One circuit of length 5
Mapping	$f(y)\ in\ \bar{G} = f(a)\ in\ G \qquad f(v)\ in\ \bar{G} = f(e)\ in\ G$ $f(x)\ in\ \bar{G} = f(d)\ in\ G \qquad f(w)\ in\ \bar{G} = f(b)\ in\ G \qquad f(u)\ in\ \bar{G} = f(c)\ in\ G$	
Considering the above facts, we conclude that both the graphs are **isomorphic.** Hence the given graph G is **self complementary**.		

https://doi.org/10.5281/zenodo.15287638

https://doi.org/10.5281/zenodo.15287638

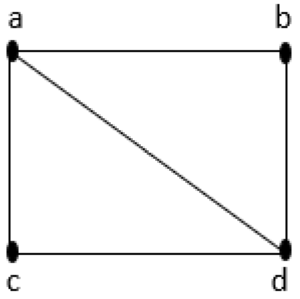
Definition: If some closed walk in a graph contains all the edges of the graph, then the walk is called an **Euler line** and the graph an **Euler graph**.



Closed walk: $\{a, c, d, f, e, c, b, f, a\}$

State the necessary and sufficient conditions for the existence of an Eulerian path in a connected graph.

A connected graph has an Euler path but not an Euler circuit if and only if it has exactly two vertices of odd degree



a and d are two vertices with odd degree.

Euler path is $a-b-d-a-c-d$

Necessary and sufficient condition for Euler graph: A connected graph G is an Euler graph if and only if all vertices of G is of even degree.

Proof: Assume that $G=\{V, E\}$ be an Euler Graph. We have to prove all vertices in V are of even degree. Since the graph is Euler, it has Euler circuit C with initial vertex u. Let v be an arbitrary internal vertex of the circuit C.

Each time a vertex v occurs as an internal vertex of C, then two of the edges incident with v, contributes 2 degrees.

Therefore $\deg(v) = 2\times$(number of times v occur inside the Euler circuit C)

= even degree.

Since u is the initial vertex, $\deg(u) = 2+2\times$(number of times u occur inside the Euler circuit C)

= even degree

$\therefore G$ has all vertices of even degree.

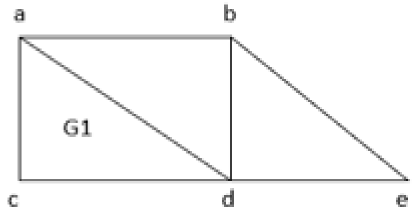
Conversely, assume that in $G=\{V, E\}$, all vertices of V are of even degree. We have to prove G is Euler.

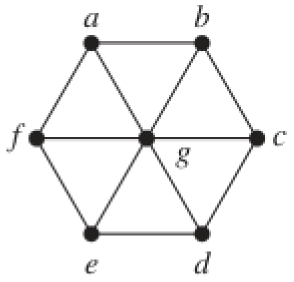
Let us trace a walk start from a vertex u and goes through all the edges without repeating any edge. Since every vertex is of even degree we can exit any vertex entered. The tracing is continued as far as possible and do not stop except the starting vertex u. If this tracing g_1 includes all edges of G, the graph is Euler. Otherwise, remove the edges of the closed walk just traced g_1 from G and obtain a sub graph say G_1.

Since the degrees of all vertices of G and g_1 are even, the degree of all vertices of G_1 is also even. Also G_1 must touch g_1 at least at one vertex a, because the graph is connected. Starting from a we can construct a closed walk g_2 in G_1 starting and ending at a. But this closed walk g_2 can be combined with g_1 to form a now closed walk starting and ending with u. Obviously this combined closed walk has more edges than g_1.

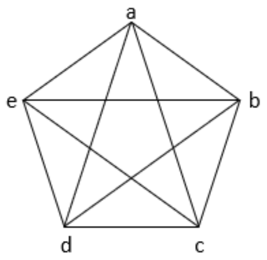
This process can be repeated until we obtain a closed walk that traverses all the edges of G. Thus G is an Euler graph.

Try this: Find an Euler path or Euler circuit, if it exists in each of the following three graphs. If it does not exist, explain why?





G2

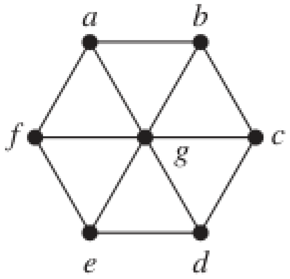


G3

Definition : A path in a graph G is said to be **Hamilton**, if it passes through every vertices of G exactly once.

Definition : A circuit in a graph G is said to be Hamilton, if it passes through every vertices of G exactly once. A graph is said to be **Hamiltonian** if it contains a Hamilton circuit.

https://doi.org/10.5281/zenodo.15287638



Hamilton Circuit: $a-b-c-d-e-f-g-a$.

Note:

- A Hamiltonian circuit in a graph of n vertices consists of exactly n edges
- The length of a Hamiltonian path (if it exists) in a connected graph of n vertices is $n-1$
- In K_n there are $\frac{(n-1)!}{2}$ Hamilton cycles (not edge disjoint).

  In a complete graph of n vertices K_n, every vertex is adjacent to every other vertex. Hence from any given vertex, there are Hamilton $(n-1)!$ cycles. Of these each pair of vertices which are adjacent both in the clock wise and anticlockwise direction, i.e. as $v_j v_i$ and $v_i v_j$. Hence there are $\frac{(n-1)!}{2}$ Hamilton cycles.

Example: Show that K_n has a Hamilton cycle for $n \geq 3$. What is the maximum number of edge disjoint cycles possible in K_n? Obtain all the edge disjoint cycles in K_7.

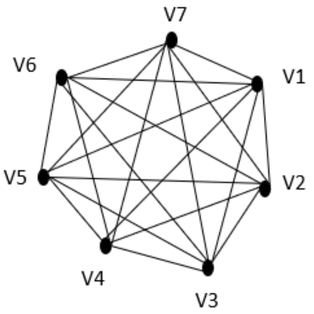
Proof: We know that K_n contains C_n for all $n \geq 3$. Therefore K_n has a Hamilton cycle for $n \geq 3$. Alternatively, in K_n there are edges between any two vertices. Therefore a circuit can be formed by visiting vertices in any order we choose, as long as the path begins and ends at the same vertex and traverse each vertex exactly once. This is a Hamilton circuit.

We know that each Hamilton cycle in K_n consists of n edges.

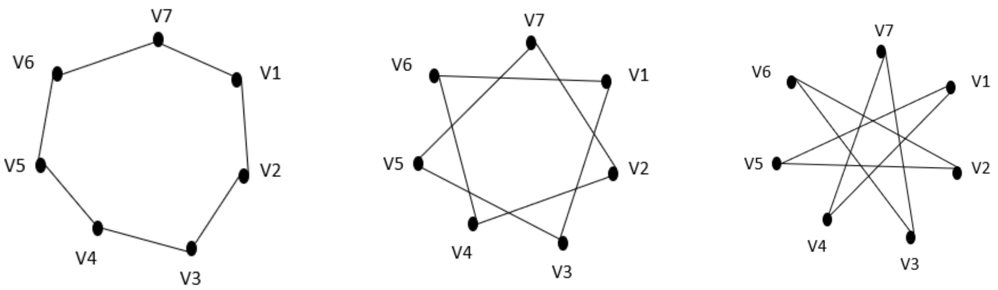
But complete graph K_n has $\frac{n(n-1)}{2}$ edges. Therefore K_n can have at most $\frac{n-1}{2}$ number of edge disjoint Hamilton Cycles.

K_7 and its edge disjoint Hamilton cycles.

https://doi.org/10.5281/zenodo.15287638



K_7

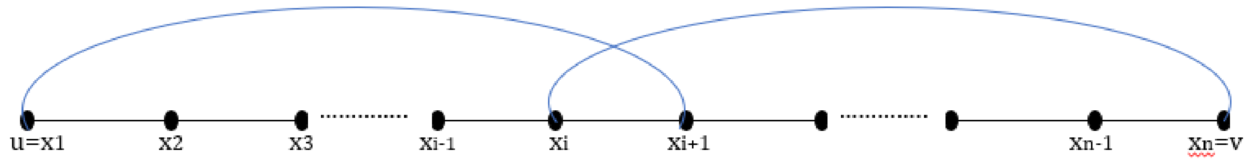


Edge Disjoint Hamilton Cycles of K_7

ORE'S THEOREM : If G is a simple graph with n vertices with $n \geq 3$ such that $d(u)+d(v) \geq n$ for every pair of nonadjacent vertices u and v in G. Then G is Hamiltonian if and only if $G+uv$ is Hamiltonian.

Proof: If G is Hamiltonian then obviously $G+uv$ is Hamiltonian.

Conversely suppose $G+uv$ is Hamiltonian but G is not.
Let us prove this theorem by contradiction.
Suppose that $d(u)+d(v) \geq n$ for all non adjacent vertices u , v in G for a non Hamilton circuit. Let G be such a maximal graph i.e. by adding an edge between u and v will result in a Hamilton circuit. Let the Hamilton path be $u = x_1,\ x_2,\ x_3, ...x_n = v$ as shown here.



Define two sets $S = \{\ x_u : \textit{It is adjacent to } u\ \}$ and $T = \{\ x_v : \textit{It is adjacent to } v\ \}$

Therefore $|S| = \deg(u)$ and $|T| = \deg(v)$. We claim that $S \cap T = \phi$ and $|S \cup T| \leq n-1$.

Thus if $x_i \in S \cap T$, then the edges $(u,\ x_i)$ and $(x_i,\ v)$ should be in G and the path

$u = x_1, x_2, \ldots x_{i-1}, x_i, x_{i+1}, \ldots x_n, x_{n-1}, \ldots, x_1$ will form a Hamiltonian circuit, which is a contradiction.

Also, since the vertex $u = x_1$ is neither adjacent to u nor adjacent to v, therefore $x_1 \notin S \cup T$ and hence $|S \cup T| \leq n-1$.
Therefore $d(u)+d(v) = |S|+|T| = |S \cup T| \leq n-1$, which is again a contradiction. Hence G is Hamiltonian.

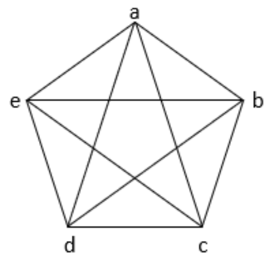
Dirac's Theorem: If G is connected simple graph with n vertices $n \geq 3$, such that the degree of every vertex in G is at least $\frac{n}{2}$, then prove that G has Hamilton cycle.

Proof: Given that G is connected simple graph with n vertices, such that the degree of every vertex is at least $\frac{n}{2}$.

Let u, v in G then $d(u) \geq \frac{n}{2}$ and $d(v) \geq \frac{n}{2}$ and hence $d(u)+d(v) \geq \frac{n}{2}+\frac{n}{2}=n$. This is true for all pair of non adjacent vertices u and v. Therefore by Ore's theorem, G has Hamiltonian circuit.

Example: Consider a complete graph K_5. Here $n=5$ and degree of each vertex is 4. Also $\deg(G)=4 \geq \frac{n}{2}$

Therefore by Dirac's theorem, K_5 has Hamilton Circuit which is $a-b-c-d-e-a$.



Direc's theorem is not necessary condition to have a Hamilton circuit.

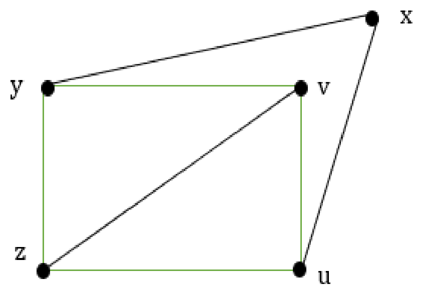
Example:
Consider the graph K_5. Here $n=5$ and degree of each vertex is 3 except the deg(x)=2 and hence $\deg(G)$ is not $\geq \frac{n}{2}$.

But the graph is Hamiltonian even the Dirac's theorem fails. Because it satisfies the conditions of Ore's theorem.

For the vertices x, v $\quad d(x)+d(v)=2+3=5 \geq n=5$

For the vertices u, y $\quad d(u)+d(y)=3+3=6 \geq n=5$

For the vertices x, z $\quad d(x)+d(z)=2+3=5 \geq n=5$



Hamilton Circuit: $x-y-v-z-u-x$.

Theorem: Complete bipartite graph $K_{m,n}$ with $m,n \geq 2$ is Hamiltonian if and only if $m=n$.

Proof: Let $K_{m,n}$ is a complete bipartite graph which is Hamiltonian.

Then the vertex set can be decomposed into two disjoint sets X and Y such that each edge in $K_{m,n}$ joins a vertex in X to a vertex in Y.

Conversely suppose $K_{m,n}$ is a complete bipartite graph with $m=n$.

Let the vertices sets are $X=\{x_1, x_2, ..., x_n\}$ and $Y=\{y_1, y_2, ..., y_n\}$

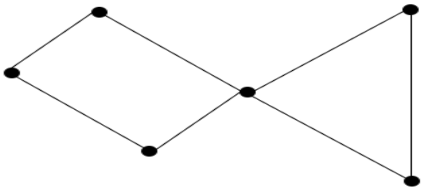
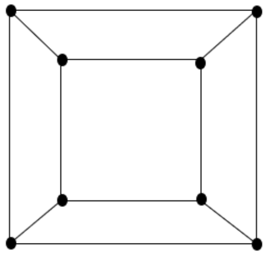
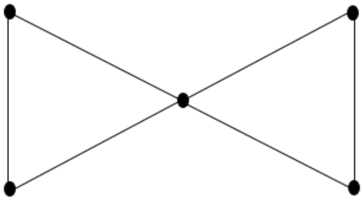
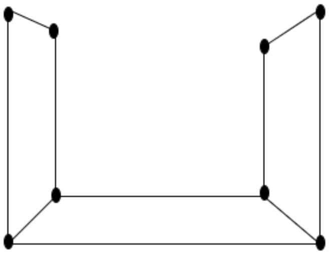
Consider a cycle

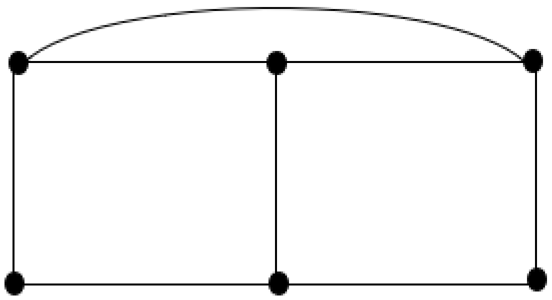
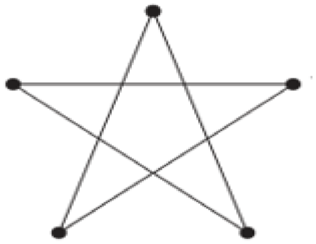
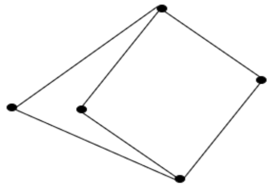
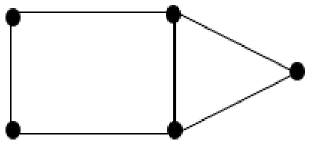
Since Hamilton circuit is a closed walk that traverses every vertices of the two sets exactly once alternatively. This is possible only the sets X and Y have the same number of vertices

i.e. $m=n\geq 2$.

$x_1,\ y_1,\ x_2,\ y_2,\ x_3,\ y_3,\ldots\ldots x_{n-1},\ y_{n-1},\ x_n,\ y_n,\ x_1$ which traverses all the vertices exactly once and hence it is Hamilton and the graph is said to be Hamiltonian

The following table gives examples for some Euler and Hamilton related graphs:

Types	**Example**
Euler Graph	
Hamilton Graph	
Euler but not Hamilton	
Hamilton but not Euler	

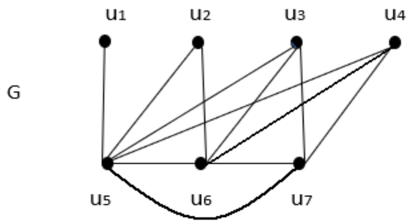
Neither Euler nor Hamilton	
Both Euler and Hamilton	
Contains Hamilton Path but not Hamilton Circuit	
Contains Euler line but not Euler Circuit	

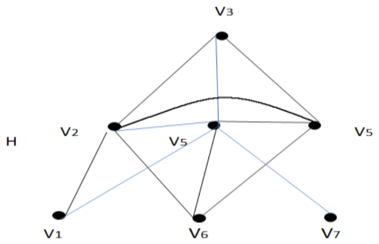
EXERCISE

1. What is the largest possible number of vertices in a graph with 35 edges and all vertices of degree at least three.

2. Draw a graph with the adjacency matrix $A = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

3. When do we say two simple graphs are isomorphic? Check whether the following two graphs are isomorphic or not. Justify your answer.





4. Write the adjacency matrix and incidence matrix of K_{22}.

5. How many edges are there in a graph with 10 vertices each of degree 3?

6. Give an example of self complementary graph.

7. Draw a graph with 5 vertices A, B, C, D and E such that deg(A)=3, B is an odd vertex, deg(C)=2 and D and E are adjacent.

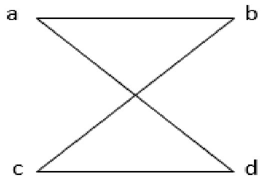
8. Show that there does not exist a graph with 5 vertices with degrees 1, 3, 4, 2, 3 respectively.

9. Define isomorphism between two graphs. Are the simple graphs with the adjacency matrices isomorphic?

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

10. Prove that a simple graph is bipartite if and only if it is possible to assign one of the two different colors to each vertex of the graph so that no two adjacent vertices are assigned the same color.

11. How many paths of length four are there from a to d in the simple graph G given below:



https://doi.org/10.5281/zenodo.15287638

UNIT IV – ALGEBRAIC STRUCTURES

An algebraic system is a pair of non empty set together with one or more operations on the set. It is also called an algebraic structure because the operations on the set define a structure of the elements of the set.

Definition: Let S be a nonempty set. A **binary operation** on S is a function $*$ from $S \times S$ into S and it is written as $a * b$ for all $a, b \in S$

Example: Let N be the set of natural numbers then the operation addition is a binary operation on N and is denoted by $(N,+)$.

But subtraction (–) is not binary operation on N . Because 3 – 4 = –1 $\notin N$.

Properties of Binary Operation

Let S be a nonempty set and $*$ be the binary operation on S .

1. **Closure Property**: The set S is closed under the binary operation $*$ if for all $a, b \in S$, $a * b \in S$

   Example: The set of natural numbers N is closed under addition but not closed under subtraction.

2. **Associative Property**: If for all $a, b, c \in S$, $a*(b*c)=(a*b)*c$, then $*$ is associative on S .

   Example: Multiplication is associative on the set of real numbers R .

3. **Commutative Property**: If for all $a, b \in S$, $(a*b)=(b*a)$, then $*$ is commutative on S .

   Example: The operation matrix addition is commutative but matrix multiplication on the set of square matrices in not commutative.

4. **Distributive Property**: If for all $a, b, c \in S$, $a*(b+c)=(a*b)+(a*c)$ or $(b+c)*a=(b*a)+(c*a)$, then $*$ is distributive over addition on S .

5. **Identity Property**: If for all $a \in S$ there exists $e \in S$, such that $(a*e)=(e*a)=a$, then e is the Identity element of the set with respect to the binary operation.

   Example: Zero is the additive identity on the set of integers and one is the multiplicative identity.

6. **Inverse Property**: If for all $a \in S$ there exists $a^{-1} \in S$, such that $(a*a^{-1})=(a^{-1}*a)=e$, then a^{-1} is the

https://doi.org/10.5281/zenodo.15287805

inverse element of a with respect to the binary operation.

Example: Consider the rational numbers Q. Under addition, 0 is the identity element.

Consider the set of natural numbers under the binary operation multiplication. Now inverse element does not exist.

7. **Idempotent Property**: A non empty set S together with the binary operation $*$ is said to have idempotent property if for $a \in S$, $(a*a) = a$.

Example: Find the idempotent elements of $G = \{1, -1, i, -i\}$ under the binary operation multiplication.

Here $1*1 = 1$. Hence 1 is the idempotent element of G.

8. **Cancellation Property**: A non empty set S together with the binary operation $*$ is said to have cancellation property if for a, b, $c \in S$, then $(a*b) = (a*c) \Rightarrow b = c$ (Left cancellation law) and $(b*a) = (c*a) \Rightarrow b = c$ (Right cancellation law).

Example: Addition on the set of integers satisfies cancellation property. But matrix multiplication does not satisfy cancellation law.

Consider the matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $C = \begin{pmatrix} 0 & -3 \\ 1 & 5 \end{pmatrix}$, $D = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$.

Here $AB = AC = D,\ but\ \ B \neq C.$

Definition: A non empty set S together with the binary operation $*$ is said to be **semi-group**, if it satisfies (1) Closure Property (2) Associative Property.

A semigroup $(M,*)$ with an identity element is called a **monoid.**

A semigroup/monoid with commutative property is called commutative semigroup/monoid.

Example: Consider the set of natural numbers N. Then

$(N,+)$ is a semi group But $(N,-)$ is not a semi group

$(N,\times)$ is a monoid But $(N,+)$ is not a monoid

$(P(S), \cap)$ is a commutative semi group But $(P(S), \cap)$ is not a monoid

$(P(S), \cup)$ is a commutative semi group But $(P(S), \cup)$ is a monoid

Definition : Let $(S,*)$ be a semi group. Let V be a sub set of S. If $(V,*)$ satisfies properties of semigroup, it is called sub semigroup.

Example: Let $(Z,+)$ be a semigroup. Let $V \subset Z$

Definition : Let $(S,*)$ be a monoid. Let V be a sub set of S. If $(V,*)$ satisfies properties of monoid, it is called submonoid.

Example: Let $(N,\times)$ be a monoid. Let $V \subset N$

Where V is the set of even positive integers. Then $(V,+)$ is a semigroup and hence sub semigroup.

Where V is the set of odd numbers. Then $(V,\times)$ is a monoid and hence submonoid.

Example: If S denotes the set of positive integers ≤ 100, for $x, y \in S$, define $x * y = \min\{x, y\}$. Verify whether $(S,*)$ is a Monoid assuming that $*$ associative.

Solution: It is enough to show that $(S,*)$ have identity element.

Here 100 is the identity element since $x*100 = \min\{x,100\} = x$ since $x \leq 100$ for all $x \in S$. Therefore it is a monoid..

Example: Show that the set N of natural numbers is a semigroup under the operation $x * y = Max(x, y)$. Is it a monoid?

Solution: Let $x,\ y,\ z \in N$.

$$x*(y*z) = x*Max(y,\ z) \qquad (x*y)*z = Max(x,y)*z$$

$$= Max\big(x,\ Max(y,\ z)\big) \qquad = Max\big(Max(x,\ y),\ z\big)$$

$$= Max(x,\ y,\ z) \qquad = Max(x,\ y,\ z)$$

Therefore $*$ is associative and hence $(N,*)$ is a semigroup.

Let $1 \in N$ and $x \in N$.

Then $x*1 = Max(x,\ 1) = Max(1,\ x) = 1*x = x.$

Therefore $1 \in N$ is the identity and hence $(N,*)$ is a monoid.

Example: Prove that $Z_5 = \{[0],\ [1],\ [2],\ [3],\ [4]\}$ is an commutative monoid under multiplication modulo 5.

Solution: Consider the following multiplication modulo 5 table:

$\times_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

The table shows z_5 is closed under multiplication modulo 5. Also associative law is satisfied under $\times_5$.

From the table, [1] is the identity element.

Also $[a]\times_5[b] = [b]\times_5[a]\ \forall\ [a],\ [b] \in Z_5$. Hence $(z_5,\times_5)$ is a commutative monoid.

Example: If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a,b)*(x,y) = (ax,\ ay+b)$, show that $(S,*)$ is a semi group. Is it commutative? Also find the identity element of S.

Solution: Let $(a,b),\ (x,y),\ (c,d) \in S$

$$\begin{aligned}\left[(a,b)*(x,y)\right]*(c,d) &= (ax,\ ay+b)*(c,d)\\ &= (acx,\ adx+ay+b)\end{aligned}$$

$$\begin{aligned}(a,b)*\left[(x,y)*(c,d)\right] &= (a,b)*(xc,\ xd+y)\\ &= (acx,\ adx+ay+b)\end{aligned}$$

Therefore $*$ is associative on S and hence $(S,*)$ is a semigroup.

Also $(a,b)*(x,y) = (ax,\ ay+b) \neq (x,y)*(a,b)$. Therefore $*$ is not commutative.

Let $\left(e_1,e_2\right)$ be the identity element on $(S,*)$. Then for $\left(a,b\right) \in S$,

$$\left(e_1,e_2\right)*\left(a,b\right) = \left(a,b\right)$$

$$\left(e_1 a,\ e_1 b+e_2\right) = \left(a,b\right)$$

$$\therefore\ e_1 a = a \ \Rightarrow\ e_1 = 1$$

$$\begin{aligned}\therefore\ e_1 b + e_2 &= b\\ b + e_2 &= b\\ e_2 &= 0\end{aligned}$$

Therefore the identity element is $\left(e_1,e_2\right) = \left(1,0\right)$

Example: If $*$ is the binary operation defined on R, set of real numbers defined by $a*b = a+b+2ab$. Is $\left(R,*\right)$ a semi group?. Find the identity element if it exists. Which elements have inverses and what are they?

Solution: Let $a,\ b,\ c \in S$

$$\begin{aligned}\left(a*b\right)*c &= \left(a+b+2ab\right)*c\\ &= \left(a+b+2ab+c+2ac+2bc+4abc\right)\\ &= \left(a+b+c+2\left(ab+bc+ca\right)+4abc\right)\end{aligned}$$

$$\begin{aligned}a*\left(b*c\right) &= a*\left(b+c+2bc\right)\\ &= \left(a+b+c+2bc+2ab+2ac+4abc\right)\\ &= \left(a+b+c+2\left(ab+bc+ca\right)+4abc\right)\end{aligned}$$

Therefore $*$ is associative on R and hence $\left(R,*\right)$ is a semigroup.

Also $a*b = a+b+2ab$ and $b*a = b+a+2ba = a+b+2ab = a*b$. Therefore $*$ is commutative on R

Let e be the identity element on R. Then for $a \in R$,

$$\begin{aligned}a*e &= a\\ a+e+2ae &= a\\ e\left(1+2a\right) &= 0\\ e &= 0, \quad \because 1+2a \neq 0\end{aligned}$$

Let a^{-1} be the inverse of an element $a \in R$. Then $a * a^{-1} = e$.

$$a + a^{-1} + 2aa^{-1} = 0$$

$$a^{-1}(1+2a) = -a$$

$$a^{-1} = \frac{-a}{(1+2a)}, \quad a \neq -\frac{1}{2}$$

Example: Prove that for any commutative monoid $(M, *)$, the set of idempotent elements of M form a submonoid.

Let $(M, *)$ be the commutative monoid.
Therefore the elements of M satisfies the closure, associative property under the binary operation * and has identity element $e \in M$.
Consider a set $N = \{e\}$ and hence $N \subset M$.
Here the elements of N satisfies closure and associative property. Also it has identity element under the binary operation *. Therefore N is monoid and hence submonoid.

Example: Let $\langle S, * \rangle$ be a semi group such that for $x, y \in S,\ x * x = y$, where $S = \{x, y\}$. Then prove that

(1) $x * y = y * x$ (2) $y * y = y$

Proof: Let $\langle S, * \rangle$ be a semi group such that for $x, y \in S,\ x * x = y$, where $S = \{x, y\}$.

(i) $LHS = x * y$

$$= x * (x * x)$$

$$= (x * x) * x$$

$$= y * x$$

$$= RHS$$

(ii) Since the binary operation *is associative

$x * y = x \ \ or \ \ y$, because only two elements in $x,\ y \in S$.

Let $x * y = x$

Consider $y * y = (x * x) * y$, by definition

$= x * (x * y)$, associative law

$= x * x$, by assumption

$= y$, by definition

Example: Show that a semigroup with more than one idempotent cannot be a group.

Solution: Let $(S, *)$ be a semigroup. Let $a,\ b \in S$ be two idempotent elements.

Then $a * a = a$ and $b * b = b$. Assume that $(S, *)$ is a group.

Then each element has its inverse i.e. $a * a^{-1} = e$. By associative property, we have

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

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

$$e = a$$

But in a group we cannot have two identities and hence $(S,*)$ cannot be a group.

Example: If $S=N\times N$, the set of ordered pairs of positive integers with the operation * defined by $(a,b)*(c,d)=(ad+bc,bd)$ and if $f:(S,*)\to(Q,+)$ is defined by $f(a,b)=\dfrac{a}{b}$, then show that f is a semigroup homomorphism.

Solution: Let $(a,b),\ (c,d),\ (e,f)\in S=N\times N$

$$\begin{aligned}\left[(a,b)*(c,d)\right]*(e,f)&=(ad+bc,\ bd)*(e,f)\\&=\left((ad+bc)f+bde,\ bdf\right)\\&=(adf+bcf+bde,\ bdf)\end{aligned}$$

$$\begin{aligned}(a,b)*\left[(c,d)*(e,f)\right]&=(a,b)*(cf+de,\ df)\\&=\left(adf+b(cf+de),\ bdf\right)\\&=(adf+bcf+bde,\ bdf)\end{aligned}$$

Therefore * is associative on S and hence it is a semigroup.

$$\begin{aligned}f\left((a,b)*(c,d)\right)&=f\left(ad+bc,\ bd\right)\\&=\frac{ad+bc}{bd}\\&=\frac{a}{b}+\frac{c}{d}\\&=f(a,b)+f(c,d)\end{aligned}$$

Therefore f is a semigroup homomorphism.

Theorem: Let $(M,*)$ be a monoid. Prove that there exists a subset $T\subseteq M^M$ such that $(M,*)$ is isomorphic to the monoid $(T,\circ)$; here M^M denotes the set of all mappings from M to M and $\circ$ denotes the composition of mappings.

Proof: Given that $(M,*)$ be a monoid.

For each $a\in M$, we define a function $f_a:M\to M$ such that $f_a(x)=a*x,\ \forall\ x\in M$.

Therefore $f_a\in T\subseteq M^M$.

Define a mapping $g:M\to T$ such that $g(a)=f_a,\ \ \forall\ a\in M$.

Let $a,\ b\in M$. Then $a*b\in M$. Therefore $g(a*b)=f_{a*b}$.

But for $x\in M$, $f_{a*b}(x)=(a*b)*x$

$$\begin{aligned}&=a*(b*x)\\&=f_a(b*x)\\&=f_a\left(f_b(x)\right)\end{aligned}$$

$$=(f_a \circ f_b)(x)$$

Therefore $f_{a*b} = (f_a \circ f_b)$ and hence $g(a*b) = f_{a*b} = f_a \circ f_b = g(a) \circ g(b)$

Therefore g is a homomorphism of $(M,*)$ into $(T,\circ)$.

Suppose $a,b \in M$ such that $a = b$. Then there exists a mapping f_a, f_b such that

$$f_a = f_b$$

$$g(a) = g(b)$$

Therefore g is one-to-one and also by definition it is onto. Hence g is isomorphic.

GROUPS

Definition : Let G be a nonempty set with a binary operation $*$. Then $(G,*)$ is called a group if the axioms (i) associative law (ii) existence of identity (iii) existence of inverse hold.

A group G is said to be **abelian** if it satisfies commutative property.

Definition: The number of elements in a group G, denoted by $|G|$ or $O(G)$, is called the **order** of G. The order of an infinite group is infinity.

Example : Let p be a prime number. Then $Z_p - \{0\}$ is a finite group with respect to multiplication modulo p. Its order is $p-1$.

Definition: Suppose a is an element of a group G. Then the least positive integer n such that $a^n = e$, the identity, is called the order of the element a. If no such positive integer exists, then a is said to be of infinite order.

Example : Let $Q^* = \{Q - \{0\}\}$ be the set of all nonzero rational number. Then it is a group with respect to multiplication.

The group Q^* is of infinite order. Also $O(1) = 1$, $O(-1) = 2$. All other elements are of infinite order.

Problems on Groups

Example : Show that $(Z,+)$ is a group.

(i) Let $a,\ b \in Z$, the set of integers.

Now $a+b \in Z$

i.e. Z is closed under addition

Example : Show that $(Q \setminus \{0\}, \times)$ is a group.

(i) Let $a,\ b \in Q \setminus \{0\}$, the set of non zero rationals.

Now $a \times b \in Q \setminus \{0\}$

i.e. $Q \setminus \{0\}$ is closed under multiplication

(ii) Let $a, b, c \in Z$,

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

i.e. Z is associative under addition

(iii) Let $a \in Z$, then there exists $0 \in Z$ such that

$a+0 = 0+a = a$

i.e. Z has the identity element

(iv) Let $a \in Z$, then there exists $-a \in Z$ such that

$a+(-a) = (-a)+a = 0$

i.e. all elements of Z has inverse element

Therefore $(Z,+)$ is a group.

Also, Let $a, b \in Z$, then

$a+b = b+a$

i.e. Addition is commutative in Z and hence $(Z,+)$ is an abelian group.

(ii) Let $a, b, c \in Q\setminus\{0\}$,

Now $(a\times b)\times c = a\times(b\times c)$

i.e. $Q\setminus\{0\}$ is associative under multiplication

(iii) Let $a \in Q\setminus\{0\}$, then there exists $1 \in Q\setminus\{0\}$ such that

$a\times 1 = 1\times a = a$

i.e. $Q\setminus\{0\}$ has the identity element

(iv) Let $a \in Q\setminus\{0\}$, then there exists $\frac{1}{a} \in Q\setminus\{0\}$ such that

$a\times\frac{1}{a} = \frac{1}{a}\times a = 1$

i.e. all elements of $Q\setminus\{0\}$ has inverse element

Therefore $(Q\setminus\{0\},\times)$ is a group.

Also, Let $a, b \in Q\setminus\{0\}$, then

$a\times b = b\times a$

i.e. Multiplication is commutative in $Q\setminus\{0\}$ and hence $(Q\setminus\{0\},\times)$ is an abelian group.

.

Example : Prove that $G = \{1, -1, i, -i\}$ is a group under multiplication.

Consider the following multiplication table:

×	**1**	**–1**	***i***	***–i***
1	1	–1	*i*	–*i*
–1	–1	1	–*i*	*i*
i	*i*	–*i*	–1	1
–i	–*i*	*i*	1	–1

The table shows G is closed under multiplication.

Also G is associative under multiplication.

From the first column/row, we conclude that 1 is the identity element of G.

Inverse of 1 is 1. Inverse of -1 is -1

Inverse of *i* is $-I$ Inverse of $-i$ is i

Symmetric Group S_n

A one-to-one mapping σ of the set $\{1,2,\ldots,n\}$ onto itself is called a permutation. Such a permutation may be denoted as follows where $J_i = \sigma(i)$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots.. & n \\ J_1 & J_2 & J_3 & \ldots.. & J_n \end{pmatrix}$$

https://doi.org/10.5281/zenodo.15287805

The set of all such permutations $(n!\ numbers)$ is denoted by S_n forms a group under the binary operation composition. It is called symmetric group of degree n.

Example : Prove that the set of permutations on the set $\{1,2,3\}$ is a group under composition of functions.

Let the elements of S_3 are $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

Consider the composition table of S_3

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_4	σ_6	σ_5	σ_2	σ_1
σ_4	σ_4	σ_3	σ_2	σ_1	σ_6	σ_5
σ_5	σ_5	σ_6	σ_4	σ_3	σ_1	σ_2
σ_6	σ_6	σ_5	σ_1	σ_2	σ_4	σ_3

The table shows S_3 is closed under composition.

Also S_3 is associative under composition.

From the first column/row, we conclude that σ_1 is the identity element of S_3.

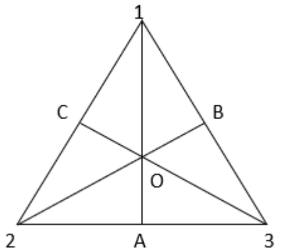
Inverse of σ_1 is σ_1. Inverse of σ_2 is σ_2 Inverse of σ_3 is σ_6

Inverse of σ_4 is σ_4 Inverse of σ_5 is σ_5 Inverse of σ_6 is σ_3

Dihedral Groups

By considering the symmetries of regular polygons, we obtain certain permutation groups known as dihedral groups.

Consider an equilateral triangle with vertices 1, 2, 3. Consider all possible rotations and reflections which keeps the position of the triangle unchanged except the renaming the vertices. The effect of the rotation/reflection can be expressed as the permutation.



Let P_1 be the rotation of the triangle about the origin O through $0°$ or $360°$. Then $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Let P_2 be the rotation of the triangle about the origin O through $120°$. Then $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Let P_3 be the rotation of the triangle about the origin O through $240°$. Then $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Let P_4 be the reflection of the triangle about the line $1A$. Then $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Let P_5 be the reflection of the triangle about the line $2B$. Then $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Let P_6 be the reflection of the triangle about the line $3C$. Then $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

The set of permutations $S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ together with composition $\circ$ forms a group. This is denoted by $(D_3, \circ)$

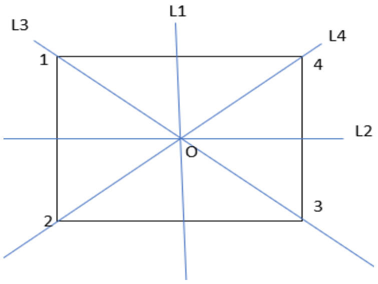
To find the dihedral group $(D_4, \circ)$ by considering the symmetries of a square

Let P_1 be the rotation of the square about the origin O through $90°$.

Then $P_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

Let P_2 be the rotation of the square about the origin O through $180°$.

Then $P_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$



Let P_3 be the rotation of the square about the origin O through $270°$.

Then $P_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

Let P_4 be the rotation of the square about the origin O through $0°$ or $360°$.

Then $P_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

Let P_5 be the reflection of the square about the line $L1$.

Then $P_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

Let P_6 be the reflection of the square about the line $L2$. Then $P_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Let P_7 be the reflection of the square about the line $L3$. Then $P_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

https://doi.org/10.5281/zenodo.15287805

Let P_8 be the reflection of the square about the line $L4$. Then $P_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

The composition table for $(D_4, \circ)$.

$\circ$	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_1	P_2	P_3	P_4	P_1	P_8	P_7	P_5	P_6
P_2	P_3	P_4	P_1	P_2	P_6	P_5	P_8	P_7
P_3	P_4	P_1	P_2	P_3	P_7	P_8	P_6	P_5
P_4	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_5	P_7	P_6	P_8	P_5	P_4	P_2	P_1	P_3
P_6	P_8	P_5	P_7	P_6	P_2	P_4	P_3	P_1
P_7	P_6	P_8	P_5	P_7	P_3	P_1	P_4	P_2
P_8	P_5	P_7	P_6	P_8	P_1	P_3	P_2	P_4

Example: Prove that $G = \{[1], [2], [3], [4]\}$ is an abelian group under multiplication modulo 5.

Consider the following multiplication modulo 5 table:

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

The table shows G is closed under multiplication modulo 5.

Also G is associative under multiplication modulo 5.

From the first column/row, we conclude that [1] is the identity element of G.

Inverse of [1] is [1]　　　Inverse of [2] is [3]

Inverse of [3] is [2]　　　Inverse of [4] is [4]

Also $a \times_5 b = b \times_5 a \ \forall \ a, b \in G$. Therefore G is abelian.

Example: Let Q be the set of all rational numbers other than 1 with the binary operation * defined by $a * b = a + b - ab$. Prove that $G = \{Q \backslash 1, *\}$ is a group.

(i) Let $G = \{Q \backslash 1, *\}$. Let $a, b \in G$. Then $a \neq 1, b \neq 1$. To prove $a * b = 1$.

Suppose $a * b = 1$. Then $a + b - ab = 1$

$$a + b - ab - 1 = 0$$

$$(a-1)-b(a-1)=0$$

$$(a-1)(1-b)=0$$

$$\therefore a=1 \ or \ b=1, \text{ a contradiction.}$$

Therefore $a*b \neq 1$

Since a, b are rational, $a+b-ab$ is also rational. Therefore $a, b \in G$ then $a*b \in G$.

Therefore $*$ is a binary operation on G.

(ii) To prove $*$ is associative.

$$\begin{aligned} a*(b*c) &= a*(b+c-bc) \\ &= a+b+c-bc-a(b+c-bc) \\ &= a+b+c-bc-ab-ac+abc \end{aligned}$$

$$\begin{aligned} (a*b)*c &= (a+b-ab)*c \\ &= a+b-ab+c-(a+b-ab)c \\ &= a+b+c-bc-ab-ac+abc \end{aligned}$$

(iii) If e is the identity. Then $a*e=e*a=a$.

Let $a*e=a$

Then $a+e-ae=a$

$$e(1-a)=0$$

$$\therefore \ e=0 \in G$$

(iv) If b is the inverse of a, then

$$a*b=b*a=e.$$

Let $a*b=e$

$$a+b-ab=0$$

$$a+b(1-a)=0$$

$$\therefore \ b=\frac{a}{a-1} \in G$$

Therefore $(G,*)$ is a group.

Example: Let Z be the group of integers with the binary operation * defined by $a*b=a+b-2$, for all $a, b \in Z$. Find the identity element of the group $(Z,*)$.

Given Z be the group of integers. The binary operation * is defined as $a*b=a+b-2$, for all $a, b \in Z$.

Let e be the identity element of G. Then, by definition of identity, $a * e = a$

$$a + e - 2 = a$$

$$e \ = a+2-a$$

$$e \ = 2$$

Example: Show that $(Q^+,*)$ is an abelian group, where * is defined by $a*b=\frac{ab}{2}$, $\forall \ a, b \in Q^+$.

https://doi.org/10.5281/zenodo.15287805

Given Q^+ is a set of positive rational numbers. The binary operation * is defined by $a*b=\frac{ab}{2}, \forall\ a, b\in Q^+$.

(i) Let $a, b\in Q^+$. Then $a*b=\frac{ab}{2}\in Q^+$. Because product of two rational is rational and a rational divided by 2 is also rational. Hence Q^+ is closed under the binary operation.

(ii) Obviously Q^+ is associative under the binary operation. Because

$$a*(b*c)=a*\frac{bc}{2} \qquad (a*b)*c=\frac{ab}{2}*c$$

$$=\frac{abc}{4} \qquad =\frac{abc}{4}$$

(iii) Let e be the identity element of G. Then $a * e = a$

$$\frac{a\ e}{2}=a$$

$$e=2\ \in Q^+$$

(iv) Let a^{-1} be the inverse element of $a\in G$. Then, by definition of inverse, $a * a^{-1} = e$

$$\frac{a\ a^{-1}}{2}=2$$

$$a^{-1}=\frac{4}{a}\in Q^+$$

Also $a*b=\frac{ab}{2}=\frac{ba}{2}=b*a$

Therefore $(Q^+,*)$ is an abelian group.

Example: Examine whether $G=\left\{\begin{pmatrix} a & a\\ a & a\end{pmatrix}: a\neq 0\in R\right\}$ is a commutative group under matrix multiplication, where R is the set of all real numbers.

Solution: Let G be the set of all 2×2 matrices of the form $\begin{pmatrix} a & a\\ a & a\end{pmatrix}: a\neq 0\in R$ and the binary operation is matrix multiplication.

Let $A=\begin{pmatrix} a & a\\ a & a\end{pmatrix}$, $B=\begin{pmatrix} b & b\\ b & b\end{pmatrix}\in G$ where a, b are non zero real numbers.

https://doi.org/10.5281/zenodo.15287805

Then $A\times B=\begin{pmatrix} a & a \\ a & a \end{pmatrix}\times\begin{pmatrix} b & b \\ b & b \end{pmatrix}=\begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix}\in G$. Hence G is closed under the matrix multiplication.

Clearly matrix multiplication is associative.

Let $E=\begin{pmatrix} e & e \\ e & e \end{pmatrix}\in G$ be the identity matrix where $e\neq 0$. Then $A\times E=A$

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix}\times\begin{pmatrix} e & e \\ e & e \end{pmatrix}=\begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

$$\begin{pmatrix} 2ae & 2ae \\ 2ae & 2ae \end{pmatrix}=\begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

Therefore $2ae=a$

$$e=\frac{1}{2}$$

Therefore identity matrix $E=\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}\in G$

Let $A^{-1}=\begin{pmatrix} a^{-1} & a^{-1} \\ a^{-1} & a^{-1} \end{pmatrix}\in G$ be the inverse element of $A=\begin{pmatrix} a & a \\ a & a \end{pmatrix}$. Then $A\times A^{-1}=E$

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix}\times\begin{pmatrix} a^{-1} & a^{-1} \\ a^{-1} & a^{-1} \end{pmatrix}=\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$$\begin{pmatrix} 2aa^{-1} & 2aa^{-1} \\ 2aa^{-1} & 2aa^{-1} \end{pmatrix}=\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Therefore $2aa^{-1}=\frac{1}{2}$

$$a^{-1}=\frac{1}{4a}$$

https://doi.org/10.5281/zenodo.15287805

Therefore inverse element $A^{-1}=\begin{pmatrix}\frac{1}{4a} & \frac{1}{4a}\\ \frac{1}{4a} & \frac{1}{4a}\end{pmatrix}\in G$

Also $A\times B=\begin{pmatrix}a & a\\ a & a\end{pmatrix}\times\begin{pmatrix}b & b\\ b & b\end{pmatrix}=\begin{pmatrix}2ab & 2ab\\ 2ab & 2ab\end{pmatrix}=\begin{pmatrix}2ba & 2ba\\ 2ba & 2ba\end{pmatrix}=B\times A$

Hence given G is commutative group under matrix multiplication.

Example: Prove that $G=\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\}$ forms an abelian group under matrix multiplication.

Let $A=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, B=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, C=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, D=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$

$AB=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=B$. Similarly $BA=B, CA=C,\ AC=C,\ DA=D,\ AD=D,\ AA=A$

$BB=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=A$ and $CC=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=A$

$DD=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=A$

$BC=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=D$ and $CB=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=D$

$BD=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=C$ and $DB=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=C$

$CD=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=B$ and $DC=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=B$

Consider the composition table.
From the table the matrix multiplication is closure and associative.
Also the matrix A is the identity element.
Inverse of each element is itself.
Also matrix multiplication is commutative. Hence $(G,\times)$ is an abelian group.

×	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

https://doi.org/10.5281/zenodo.15287805

Example: Let S be a nonempty set and $P(S)$ denote the power set of S. Verify whether $\left(P(S),\cap\right)$ is a group.

Solution: Let $P(S)$ is the power set of a non empty set S. Given binary operation is $\cap$.

Clearly intersection of any two sets of $P(S)$ is in $P(S)$. Therefore $\cap$ is closure on $P(S)$.

Obviously $\cap$ is associative. Since $A\cap S=A$ for any set A, S is the identity.

Therefore $\left(P(S),\cap\right)$ is a monoid.

Consider the empty set ϕ. Here we cannot find a set A in $P(S)$ such that $A\cap\phi=\phi\cap A=S$.

Hence ϕ has no inverse in $P(S)$. Hence $\left(P(S),\cap\right)$ is not a group.

Properties of Groups

Theorem: Let $(G,*)$ be a group. Then (i) Identity element of G is unique.
(ii) For any $a\in G$, inverse of a is unique. (iii) If an element $a\in G$ such that $a*a=a$, then $a=e$.

Proof: (i) Let there be two identity elements e_1 , e_2 of G.

If e_1 is the identity, then $e_1 * e_2 = e_2$.

If e_2 is the identity, then $e_1 * e_2 = e_1$. Therefore $e_1 = e_1 * e_2 = e_2$. i.e. identity element is unique.

(ii) Let e be the identity element of and let $a\in G$

Let a_1 , a_2 be two inverses of a. Then $a*a_1 = e = a_1 * a$ and $a*a_2 = e = a_2 * a$

Consider $a*a_1 = e$

$$a_2*\left(a*a_1\right) = a_2*e, \text{ pre multiply by } a_2$$

$$\left(a_2*a\right)*a_1 = a_2*e, \text{ by associative law}$$

$$e*a_1 = a_2*e, \text{ by identity}$$

$$a_1 = a_2$$

Therefore, the inverse element is unique.

(iii) Let a^{-1} be the inverses of the element a. Then $a*a^{-1} = e = a^{-1}* a$.

Let $a\in G$ such that $a*a=a$.

$$a^{-1}*\left(a*a\right)=a^{-1}*a, \text{ pre multiply by } a^{-1}$$

$$\left(a^{-1}*a\right)*a=a^{-1}*a, \text{ by associative law}$$

$$e*a=e, \qquad \text{by inverse law}$$

$$a=e$$

https://doi.org/10.5281/zenodo.15287805

Theorem : In any graph $(G,*)$, show that $(a*b)^{-1} = b^{-1}*a^{-1}$, for all $a,b \in G$.

We know that, if $a,b \in G$ such that $a*b = e$, then b is the inverse of a. i.e. $b = a^{-1}$.

Consider

$$\begin{aligned}\left(b^{-1}*a^{-1}\right)*(a*b) &= b^{-1}*\left(a^{-1}*a\right)*b \\ &= b^{-1} * e * b \\ &= b^{-1} * b \\ &= e\end{aligned}$$

Consider

$$\begin{aligned}(a*b)*\left(b^{-1}*a^{-1}\right) &= a*\left(b*b^{-1}\right)*a^{-1} \\ &= a * e * a^{-1} \\ &= a * a^{-1} \\ &= e\end{aligned}$$

Therefore, $\left(b^{-1}*a^{-1}\right)$ *and* $(a*b)$ are inverses to each other. i.e. $(a*b)^{-1} = b^{-1}*a^{-1}$

Theorem: Show that if every element in a group is its own inverse, then the group must be abelian.

Let $a,\ b \in G$. Then $a\,b \in G$.

Given that $a^{-1} = a,\ \ b^{-1} = b,\ (ab)^{-1} = ab.$

But $(ab)^{-1} = b^{-1}a^{-1}$

$$a\,b = b\,a$$

Therefore G is abelian.

Note: Converse of the theorem is not true.

Theorem: If G is a group such that $a^2 = e$ for all $a \in G$, show that G must be abelian.

Given $a^2 = e$. Premultiply by a^{-1}.

Then $a^{-1}a^2 = a^{-1}e$

$$a = a^{-1} \text{ for all } a \in G.$$

Let $a,\ b \in G$. Then $a\,b \in G$.

Therefore $a^{-1} = a,\ \ b^{-1} = b,\ (ab)^{-1} = ab.$

But $(ab)^{-1} = b^{-1}a^{-1}$

$$a\,b = b\,a$$

Therefore G is abelian.

Theorem: Show that in a group $(G,*)$ if for any $a,b \in G$, $(a*b)^2 = a^2*b^2$, then $(G,*)$ is abelian.

Given that $(a*b)^2 = a^2*b^2$ for any $a,b \in G$.

$$\begin{aligned}RHS &= a^2*b^2 \\ &= (a*a)*(b*b) \\ &= \left[(a*a)*b\right]*b \\ &= \left[a*(a*b)\right]*b \\ &= a*(a*b)*b\end{aligned}$$

$$\begin{aligned}LHS &= (a*b)^2 \\ &= (a*b)*(a*b) \\ &= \left[(a*b)*a\right]*b \\ &= \left[a*(b*a)\right]*b \\ &= a*(b*a)*b\end{aligned}$$

Therefore $a*\left(a*b\right)*b = a*\left(b*a\right)*b$

$$\left(a*b\right)=\left(b*a\right), \text{ by left and right cancellation law.}$$

Therefore $\left(G,*\right)$ is abelian.

Theorem: If $\left(G,*\right)$ is abelian group, show that $(a*b)^n = a^n * b^n$ for all $a,b \in G$ where n is a positive integer.

Proof: Since $(a*b)^1 = a^1 * b^1$, let the statement is true for $n=1$.

Assume that the statement is true for $n=k$ i.e. $(a*b)^k = a^k * b^k$

Consider

$$\begin{aligned}(a*b)^{k+1} &= (a*b)^k*(a*b)\\ &= (a^k*b^k)*(a*b)\\ &= a^k*(b^k*a)*b\\ &= a^k*(a*b^k)*b\\ &= (a^k*a)*(b^k*b)\\ &= a^{k+1}*b^{k+1}\end{aligned}$$

Therefore the statement is true for $n=k+1$ and hence it is true for $n \in N$.

Hence $(a*b)^n = a^n * b^n$

Theorem: If G is a finite group, show that there exists a positive integer n such that $a^n = e$ for $a \in G$.

Let $a \in G$. Consider $a, a^2, a^3, \ldots\ldots$ These are elements of G. Since G is finite, these elements cannot all be distinct. Hence there exists integers r, s with $r>0, s>0$ such that $a^r = a^s$.

Therefore $a^r a^{-s} = a^s a^{-s}$

$$a^r a^{-s} = e, \text{ where } r-s>0.$$

Let $S=\left\{q : a^q = e, q \in Z^+\right\}$. Here $r-s \in S$. Hence S is a non empty set of natural numbers and therefore by well ordering principle S has a least element say n. Hence $a^n = e$.

Theorem: Prove that identity is the only idempotent element in a group.

Clearly, $e^2 = e.e = e$. Hence e is the idempotent element.

Suppose let $x^2 = x$.

$$x.x = x.e$$

$$x = e$$

Therefore, identity is the only idempotent element in a group.

https://doi.org/10.5281/zenodo.15287805

SUBGROUPS AND CYCLIC GROUPS

SUBGROUP

A nonempty subset H of a group G is called a subgroup of G if H itself is a group under the same binary operation of G.

Example: $(Z,+)$ is a sub group of $(Q,+)$.

$(2Z,+)$ is a sub group of $(Z,+)$.

Example: Find all the non trivial sub groups of $(z_6,+_6)$.

Consider the elements of the set $Z_6=\{[0],[1],[2],[3],[4],[5]\}$ and $O(Z_6)=6$

Let H be the subgroup of Z_6 then $O(H)|6$. Therefore the possible values of $O(H)$ are 1, 2, 3 or 6.

$O(H)=1 \Rightarrow H=\{[0]\}$

$O(H)=2 \Rightarrow H=\{[0],[x]\}$ where $[2x]=0 \Rightarrow x=3. \therefore H=\{[0],[3]\}$

$O(H)=3 \Rightarrow H=\{[0],[x],[2x]\}$ where $[3x]=0 \Rightarrow x=2. \therefore H=\{[0],[2],[4]\}$

$O(H)=6 \Rightarrow H=Z_6$

Example: Find all the non trivial sub groups of $(z_{12},+_{12})$.

Consider the elements of the set $Z_{12}=\{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]\}$

Trivial subgroups are Z_{12} and $[0]$ under the binary operation $+_{12}$.

The non trivial subgroups are $H_1=\{[0],[4],[8]\}$, $H_2=\{[0],[6]\}$, $H_3=\{[0],[3],[6],[9]\}$,

$H_4=\{[0],[2],[4],[6],[8],[10]\}$

Properties of subgroup

Theorem: Prove that the identity of a subgroup is same as that of the group.

Proof: Let G be the group with identity e. Let H be the subgroup of G.

Suppose e' be the identity of the subgroup H.

Let $a\in H$. Then $a.e'=a$.

Also $a\in G$. Then $a.e=a$

Therefore $a.e=a.e'$

https://doi.org/10.5281/zenodo.15287805

$$e = e'$$

Theorem: (Necessary and Sufficient Condition) Show that a non empty subset H of a group $(G,*)$ is a subgroup of G if and only if $a*b^{-1} \in H$ for all $a,b \in H$.

Proof: Suppose $(H,*)$ is a subgroup of $(G,*)$. i.e. $(H,*)$ is a group.

Therefore for any $a,\ b \in H$, their inverses $a^{-1},\ b^{-1}$ are in H.

Consider $a,\ b^{-1} \in H$. Then by closure property, $a*b^{-1} \in H$

Conversely, suppose that H is a subset of $(G,*)$ and $a*b^{-1} \in H$ for all $a,b \in H$.

Associate law is inherited by H from G.

So, for two elements $a,\ a \in H$ then $a*a^{-1} = e \in H$.

Also, for two elements $e,\ a \in H$ then $e*a^{-1} = a^{-1} \in H$.

Hence $(H,*)$ is a group.

Theorem: The intersection of any two subgroups of a group G is again a subgroup of G.

Proof: Let H, K be two subgroups of G and e is the identity.

By definition, $e \in H$ and $e \in K$, then $e \in H \cap K$. Hence $H \cap K$ is non empty.

Let $a,\ b \in H \cap K$. Then $a,\ b \in H$ and $a,\ b \in K$.

Since H, K are subgroups, $a*b^{-1} \in H$ and $a*b^{-1} \in K$. Therefore $a*b^{-1} \in H \cap K$

Hence $H \cap K$ is a subgroup of G.

Theorem: The union of two subgroups of a group G is a subgroup if and only if one is contained in the other group.

Proof: Let H, K be two subgroups of G and let $H \cup K$ is also a subgroup of G.

To prove of $H \subseteq K$ or $K \subseteq H$. Suppose assume that $H \not\subset K$ and $K \not\subset H$

Now $H \not\subset K$ implies there is an element $a \in H$ such that $a \notin K$.

Also $H \not\subset K$ implies there is an element $b \in K$ such that $b \notin H$.

Clearly $a,b \in H \cup K$ and hence $ab \in H \cup K$

i.e. $ab \in H$ or $ab \in K$

Suppose $ab \in H$.

Then $a \in H$ implies $a^{-1} \in H$.

Suppose $ab \in K$.

Then $b \in K$ implies $b^{-1} \in K$.

$\therefore\ a^{-1}(ab) = b \in H$ which is a contradiction.

$\therefore\ (ab)b^{-1} = a \in K$ which is a contradiction.

Thus our assumption is wrong. Therefore $H \subseteq K$ or $K \subseteq H$.

Conversely, suppose that $H \subseteq K$ or $K \subseteq H$.

Now $H \subseteq K$ implies $H \cup K = K$ and $K \subseteq H$ implies $H \cup K = H$.

But H, K are sub groups. Hence $H \cup K$ is also a subgroup of G.

Example: Consider the group $(Z,+)$. Then $2Z = \{.....,-4,\ -2,\ 0,\ 2,\ 4,.....\}$ and $3Z = \{....,-6,\ -3,\ 0,\ 3,\ 6,.....\}$ are the subgroups of $(Z,+)$.
Let $H = 2Z \cup 3Z = \{....,-6,\ -4,\ -3,\ -2,\ 0,\ 2,\ 3,\ 4,\ ....\}$.

Here H is not closed . Hence H is not a subgroup.

Definition: Let $(H,*)$ be the subgroup of $(G,*)$ and a be any arbitrary element of G. Then the set $a*H = \{a*h : h \in H\}$ is called the left coset of H determined by a in G. Similarly, the set $H*a = \{h*a : h \in H\}$ is called the right coset of H determined by a in G.

Note: $a*H$ is denoted as aH and $H*a$ is denoted as Ha.

(Number of cosets)(Number of elements of H) = Number of elements of G.

Example: Consider the group $G = \{1,-1,i,-i\}$ under multiplication.

Let $H = \{1,-1\}$ be the subset of G and clearly H is a subgroup of G.

Let $1 \in G$ and hence $1 \times H = \{1\times 1,\ 1\times(-1)\} = \{1,\ -1\}$ is a left coset

Let $-1 \in G$ and hence $-1 \times H = \{(-1)\times 1,\ (-1)\times(-1)\} = \{-1,\ 1\}$ is a left coset

Let $i \in G$ and hence $i \times H = \{i \times 1,\ i \times (-1)\} = \{i,\ -i\}$ is a left coset

Let $-i \in G$ and hence $-i \times H = \{(-i)\times 1,\ (-i)\times(-1)\} = \{-i,\ i\}$ is a left coset

Note that the left cosets are either identical or disjoint and the union of left cosets is G.

Example : Let $(Z,+)$ be the additive group of integers. Let $H = \{.....,-9,\ -6,\ -3,\ 0,\ 3,\ 6,\ 9,\ ......\}$.
Clearly H is a subgroup of G.

Let $0 \in Z$ and hence $H + 0 = \{.....,-9,\ -6,\ -3,\ 0,\ 3,\ 6,\ 9,\ ......\} = H$ is a right coset

Let $1 \in Z$ and hence $H + 1 = \{.....,-8,\ -5,\ -2,\ 1,\ 4,\ 7,\ 10,\ ......\}$ is a right coset

Let $2 \in Z$ and hence $H + 2 = \{.....,-7,\ -4,\ -1,\ 2,\ 5,\ 8,\ 11,\ ......\}$ is a right coset

Let $3 \in Z$ and hence $H+3=\{.....,-6,\ -3,\ 0,\ 3,\ 6,\ 9,\ 12,\ ......\}$ is a right coset

Let $4 \in Z$ and hence $H+4=\{.....,-5,\ -2,\ 1,\ 4,\ 7,\ 10,\ 13,\ ......\}$ is a right coset

Let $5 \in Z$ and hence $H+5=\{.....,-4,\ -1,\ 2,\ 5,\ 8,\ 11,\ 14,\ ......\}$ is a right coset

Let $6 \in Z$ and hence $H+6=\{.....,-3,\ 0,\ 3,\ 6,\ 9,\ 12,\ 15,\ ......\}$ is a right coset

We observe that

$H+0=H+3=H+6=............$

$H+1=H+4=H+7=............$

$H+2=H+5=H+8=............$

Similarly

$H-1=H+2=H+5=............$

$H-2=H+1=H+4=............$

$H-3=H+0=H+3=............$

Therefore the only three right cosets of H in Z are $H,\ H+1,\ H+2$

Example: Find the left cosets of $\{[0],\ [3]\}$ in the group $(Z_6,\ +_6)$.

Clearly $H=\{[0],\ [3]\}$ is a subgroup of $(Z_6,\ +_6)$ where $Z_6=\{[0],\ [1],\ [2],\ [3],\ [4],\ [5]\}$

Let $[0] \in Z_6$ and hence $[0]+_6 H=\{[0],\ [3]\}=H$ is a left coset

Let $[1] \in Z_6$ and hence $[1]+_6 H=\{[1],\ [4]\}$ is a left coset

Let $[2] \in Z_6$ and hence $[2]+_6 H=\{[2],\ [5]\}$ is a left coset

Let $[3] \in Z_6$ and hence $[3]+_6 H=\{[3],\ [0]\}$ is a left coset

Let $[4] \in Z_6$ and hence $[4]+_6 H=\{[4],\ [1]\}$ is a left coset

Let $[5] \in Z_6$ and hence $[5]+_6 H=\{[5],\ [2]\}$ is a left coset

Therefore $\{[0],\ [3]\}$, $\{[1],\ [4]\}$, $\{[2],\ [5]\}$ are the three left cosets of H in Z_6.

Lagrange's Theorem: If G is finite group and H is a subgroup of G, then prove that the order of H divides the order of G.

Proof: The number of elements in a group is the order of elements of the group. Let $n,\ m$ be the orders of $G,\ H$ respectively.

Case (i): Suppose $m=1$. Then $H=\{e\}$. Here 1 divides n. i.e. $O(H)$ divides $O(G)$.

Case (ii): Suppose $m=n$. Then $H=G$. Here m divides n. i.e. $O(H)$ divides $O(G)$.

Case (ii): Suppose $m<n$. Then H is a proper subgroup of G.

Let $H=\{h_1, h_2, ,,,,,, h_m\}$ contains m distinct elements i.e. $O(H)=m$.

Let $a \in G$, and $aH=\{a*h_1, a*h_2, ..., a*h_m\}$ is the left coset of H in G.

We know that any two left cosets are either identical or disjoint. Since G finite, let there be k left cosets of H in G. The distinct left cosets are $a_1H, a_2H, ..., a_kH$.

Also the union of elements of these left cosets is equal to G.
i.e. $G=a_1H \cup a_2H \cup a_3H \cup ..... \cup a_kH$
i.e. $O(G)=O(a_1H)+O(a_2H)+O(a_3H)+ .....+O(a_kH)$
i.e. $n=m+m+m+ .....+m\ (k\ times)$
i.e. $n=mk$
i.e. $\frac{n}{m}=k$
i.e. $O(H)$ divides $O(G)$.

Do you know: In general, converse of Lagrange's theorem is not true.
The converse of the Lagrange's theorem is true in case of finite cyclic group.
Any group of prime order has no proper subgroups.
Any group of order 8 cannot have subgroup of order 3, 5, 6 or 7

Example: Let G be a group with subgroups H and K. If $|G|=660, |K|=66$ and $K \subset H \subset G,$ what are the possible values of $|H|$?.

Solution: From the given data, we observe that $\frac{O(G)}{O(H)}, \frac{O(G)}{O(K)}, \frac{O(H)}{O(K)}.$

$$\text{i.e. } \frac{660}{O(H)}, \frac{660}{66}, \frac{O(H)}{66}.$$

Therefore $O(H)$ must be multiple of 66 and less than 660.

Therefore the possible values of $|H|$ are 66, 132, 198, 264, 330, 396, 462, 528, 594.

Theorem: The order of any element of a finite group G divides the order of G.

Proof: Let G be a group of order n. Let $a \in G$ be an element of order m.

Then the order of 'a' is same as the order of cyclic subgroup $H=\langle a \rangle$.

By Lagrange's theorem, $O(H)$ divides $O(G)$. i.e. m divides n.

https://doi.org/10.5281/zenodo.15287805

Theorem: Let G be a group and let $a \in G$ be of order n. Then for any integer m, $a^m = e$ then n divides m.

Proof: Given $a^m = e$. Since $O(a) = n$, n is the least positive integer such that $a^n = e$.

Divide n by m. By division algorithm, $m = qn + r$, $0 \leq r < n$.

Now $e = a^m = a^{qn+r} = a^{qn}a^r = \left(a^n\right)^q a^r = e^q a^r = a^r$.

If $0 < r < n$, then $a^r = e$, a contradiction that n is least such that $a^n = e$.

Hence $r = 0$. Therefore $m = qn$ i.e. n divides m.

Theorem: If G is a group of order n and H is a subgroup of G of order m, then prove the following results:

(i) $a \in G$ is any element, then the left coset aH of H in G consists of as many elements as in H.

(ii) Any two left cosets of H in G is either equal or disjoint.

(iii) The index of H in G is an integer.

Proof : (i) Let G is a group of order n and H is a subgroup of G of order m.

Let $H = \{h_1, h_2, ,,,,,, h_m\}$ contains m distinct elements……..(1)

Let $a \in G$, and $aH = \{a*h_1, a*h_2, \ldots\ldots, a*h_m\}$ is the left coset of H in G.

Now we have to prove the left coset aH contains m elements. i.e. all elements of aH are distinct.

On the contrary, suppose $a*h_i = a*h_j$.

Then by left cancellation law, $h_i = h_j$. This is contradicts to (1).

Therefore we conclude that H and aH have same number of elements say, m.

(ii) To prove any two left cosets of H in G is either equal or disjoint .

Let aH and bH be two left cosets of H in G. Then aH and bH are either disjoint or equal.

If aH and bH are disjoint, there is nothing to prove.

If aH and bH are not disjoint, then there is at least one element say $'c'$ which belongs to both aH and bH.

$$i.e.\ c \in aH \ \ and \ \ c \in bH$$

$$\therefore\ c = a.h_1 \text{ and } c = b.h_2 \text{ for some } h_1, h_2 \in H$$

$$\therefore\ a.h_1 = b.h_2$$

https://doi.org/10.5281/zenodo.15287805

$$i.e.\ \ a.h_1.h_1^{-1} = b.h_2.h_1^{-1}$$

$$i.e.\ \ a.e = b.\left(h_2.h_1^{-1}\right)$$

$$i.e.\ \ a = b.h_3 \text{ where } h_3 = h_2.h_1^{-1} \in H$$

$$\therefore\ \ a.H = bh_3.H$$

$$\therefore\ \ a.H = b\left(h_3.H\right)$$

$$\therefore\ \ a.H = b.H\,, \text{ since } h_3 \in H, \text{ then } h_3H = H$$

Therefore aH and bH are either disjoint or equal.

(iii) The number of distinct right(left) cosets of a subgroup H of a group G is called the Index of the subgroup H in G.

Index of H in G = Number of distinct left(right cosets)

$= k$

$= \frac{n}{m}$, By Lagrange's theorem

$= \frac{O(G)}{O(H)}$

= an integer

Remark: (Index of H in G) × $O(H) = O(G)$

CYCLIC GROUP

A group $(G,*)$ is said to be cyclic group generated by an element $a \in G$ if every element of G is an integral power of a. i.e. $G = \left\{a^n : n \in Z\right\}$.

Note: The cyclic group G generated by the element a is denoted by $G = \langle a \rangle$.

A cyclic group may have more than one generator.

Theorem: If a is a generator of a cyclic group, then a^{-1} is also a generator.

Proof: Suppose G is a cyclic group generated by a. Then $x \in G$ implies $x = a^n : n \in Z$.

Also $x = a^n = \left(a^{-1}\right)^{-n}$. Therefore each element $x \in G$ is of the form $\left(a^{-1}\right)^m$ for some integer m.

Therefore a^{-1} is also a generator of G.

Example: Consider the group $G = \{1, -1, i, -i\}$ under multiplication.

Here $i^1 = 1$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$. Therefore i is the generator and hence $G = \langle i \rangle$.

https://doi.org/10.5281/zenodo.15287805

i.e. G is cyclic group with generator i.

Note: Here $-i$ is also another generator.

Example: The additive group of integers $(Z,+)$ is a cyclic group generated by 1.

Example: Is it true that $(\mathbf{Z}_5,\times_5)$ a cyclic group? Justify your answer.

Let $\mathbf{Z}_5=\{[0],[1],[2],[3],[4]\}$ and let $a=[4]\in\mathbf{Z}_5$

$a^1=[4]\times_5 1=[4]$ $\quad$ $a^2=[4]\times_5 2=[8]=[3]$ $\quad$ $a^3=[4]\times_5 3=[12]=[2]$

$a^4=[4]\times_5 4=[16]=[1]$ $\quad$ $a^5=[4]\times_5 5=[20]=[0]$

Therefore $a=\langle[4]\rangle$ is the generator of $\mathbf{Z}_5$ and hence $(\mathbf{Z}_5,\times_5)$ is a cyclic group.

Properties of cyclic group

Theorem: Prove that any cyclic group is abelian

Proof: Suppose G is a cyclic group generated by a. Then $G=\{a^n : n\in Z\}$.

Let $x,\ y$ be any two elements in G. Then there exists integers $m,\ n$ such that $x=a^m,\ y=a^n$.

Now $x.y=a^m\,a^n = a^{m+n} = a^n\,a^m = y.x$

Therefore G is abelian.

Do you know? The converse is not true.

Theorem: Prove that a subgroup of a cyclic group is cyclic.

Proof: Suppose G is a cyclic group generated by a. Then $G=\{a^n : n\in Z\}$.

Let H be a sub group of G. Certainly the elements of H are integrals powers of a. Of these powers, let m be the least positive integer.

Let b be any element in H. Then b is an integral power of a, say a^n. Divide n by m. Let q be the quotient and r be the remainder. Then $n=qm+r,\ 0\le r<m.$.

Now a^m is an element of H. Therefore $(a^m)^q$ and its inverse $(a^m)^{-q}$ are in H. But we have taken $b=a^n\in H$. Therefore by closure property, $(a^m)^{-q}.a^n=(a^m)^{-q}.a^{qm+r}=a^r\in H$.

But is the element with least positive power and $0\le r<m$. This implies that $r=0$, that is $n=mq$. i.e. $b=a^{mq}$, an integral powers of a^m. Therefore H is cyclic.

Theorem: Prove that any group of prime order is cyclic.

https://doi.org/10.5281/zenodo.15287805

Proof: Let G be a group of order p, where p is a prime number. Then $p = 1$ *or* 2 *or* 3*or* ....

If $p = 1$, then $G = \{e\}$ which trivially cyclic.

If $p \geq 2$, there is at least one more element a in G.

In this case, let H be the cyclic subgroup of G generated by a i.e. $H = \langle a \rangle$.

Now by Lagrange's theorem, $O(H)$ divides $O(G)$, namely, p.

Since p is prime, $O(H) = p.$ Thus $H = \langle a \rangle = \{a, a^2, \ldots.., a^p\}$.

Therefore H is a subgroup of G and both H and G have the same order p.

This implies that H is an improper subgroup of G, that is $G = \langle a \rangle = \{a, a^2, \ldots.., a^p\}$ which is cyclic.

Theorem: The order of an element of a finite group divides the order of G.

Proof: Let G be a finite group of order n.

i.e. $O(G) = n$

Let $a \in G$ and let $O(a) = m.$ Then $a^m = e$.

Let H be the cyclic group generated by a.

Therefore $O(a) = O(H) = m.$

But H is the cyclic subgroup of G.

By Lagrange's theorem, $O(H)$ divides $O(G)$.

i.e. $O(a)$ divides $O(G)$.

i.e. m divides n.

Theorem: Let G be a finite group of order n and $a \in G$. Then $a^n = e$.

Proof: Since G is finite group, a is of finite order.

Let $O(a) = m$

Then m is the least positive integer such that $a^m = e$.

By previous theorem, $O(a)$ divides $O(G)$.

i.e. m divides n.

Therefore $n = mq$ (for some integer q)

Now $a^n = a^{mq} = (a^m)^q = e^q = e$.

i.e. $a^n = e$.

Theorem: Let $(G,*)$ be a finite cyclic group generated by an element $a \in G$. If G is of order n, that is, $|G| = n$, then $a^n = e$, so that $G = \{a, a^2, \ldots., a^{n-1}, a^n = e\}$. Further more n is a least positive integer for which $a^n = e$.

Proof: Given $(G,*)$ is a finite cyclic group generated by an element $a \in G$ and $|G| = n$.

To prove n is a least positive integer for which $a^n = e$.

On the contrary, suppose there exists a positive integer $m < n$ such that $a^m = e$.
Since G is cyclic, any element of G can be expressed as a^k for some $k \in Z$.

https://doi.org/10.5281/zenodo.15287805

Divide k by m, let q be the quotient and r be the remainder such that $0 \le r < m$. Then $k = mq + r$.

$$\begin{aligned} a^k &= a^{mq+r} \\ &= a^{mq} * a^r \\ &= \left(a^m\right)^q * a^r \\ &= e^q * a^r \\ &= e * a^r \\ &= a^r \end{aligned}$$

This means that every element of G can be expressed as a^r, where $0 \le r < m$.

i.e. G has at most m elements or order of $G = m < n$, which is a contradiction.

i.e. $a^m = e$, for $m < n$ is not possible.

Hence $a^n = e$, where n is the least positive integer.

Now let us prove that the elements $a, a^2, ..., a^{n-1}, a^n = e$ are distinct.

Suppose $a^i = a^j$, *for* $i < j \le n$

$$a^{-i} * a^i = a^{-i} * a^j$$

$e = a^{j-i}$, $j - i < n$, which is a contradiction.

Hence the elements of G are distinct.

Normal Subgroup

A subgroup H of a group G is said to be normal subgroup of G if and only if $a * H = H * a$ for all $a \in G$.

or

A subgroup H of a group G is said to be normal subgroup of G if $a * h * a^{-1} \in H$ for all $h \in H$, $a \in G$.

Note: If G is abelian, then every subgroup of G is normal.

Example: Every subgroup of $\left(Z_{12}, +_{12}\right)$ is normal.

Let $Z_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}$ and $H_4 = \{[0], [2], [4], [6], [8], [10]\}$ is a subgroup of Z_{12} and hence normal subgroup.

Example: Let $G = \{1, -1, i, -i\}$ is a group under multiplication and $H = \{1, -1\}$ is a subgroup of G.

To prove H is normal subgroup.

https://doi.org/10.5281/zenodo.15287805

Let $a=1,\ a^{-1}=1\in G$ Let $h=1\in H$ Now $aha^{-1}=1\times1\times1=1\in H$	Let $a=1,\ a^{-1}=1\in G$ Let $h=-1\in H$ Now $aha^{-1}=1\times(-1)\times1=-1\in H$	Let $a=-1,\ a^{-1}=-1\in G$ Let $h=1\in H$ Now $aha^{-1}=(-1)\times1\times(-1)=1\in H$	Let $a=-1,\ a^{-1}=-1\in G$ Let $h=-1\in H$ Now $aha^{-1}=$ $(-1)\times(-1)\times(-1)=-1\in H$
Let $a=i,\ a^{-1}=-i\in G$ Let $h=1\in H$ Now $aha^{-1}=$ $i\times1\times(-i)=1\in H$	Let $a=i,\ a^{-1}=-i\in G$ Let $h=-1\in H$ Now $aha^{-1}=$ $i\times(-1)\times(-i)=-1\in H$	Let $a=-i,\ a^{-1}=i\in G$ Let $h=1\in H$ Now $aha^{-1}=$ $(-i)\times1\times(i)=1\in H$	Let $a=-i,\ a^{-1}=i\in G$ Let $h=-1\in H$ Now $aha^{-1}=$ $(-i)\times(-1)\times(i)=-1\in H$

Therefore H is a normal subgroup of G since $a*h*a^{-1}\in H$ for all $h\in H$, $a\in G$.

Properties of normal subgroup

Theorem: A subgroup H of a group G is a normal subgroup in G iff each left coset of H in G is equal to the right coset of H in G.

Proof: Suppose a subgroup H of a group G is a normal subgroup in G. Then by definition, $a*h*a^{-1}\in H$ for all $h\in H$, $a\in G$. Therefore $a*h*a^{-1}=H$ $\left(a*H*a^{-1}\right)*a=H*a$ $\left(a*H\right)*\left(a^{-1}*a\right)=H*a$ $\left(a*H\right)*e=H*a$ $a*H=H*a$ i.e. left and right cosets are equal	Conversely, suppose each left coset of H in G is equal to the right coset of H in G $a*H=H*a$ for all $a\in G$. $a*H*a^{-1}=H*a*a^{-1}$ $a*H*a^{-1}=H*e$ $a*H*a^{-1}=H$ Therefore $a*h*a^{-1}\in H$ for all $h\in H$, $a\in G$. i.e. subgroup H of a group G is a normal subgroup in G.

Theorem: Prove that every subgroup of an abelian group is a normal subgroup.

Proof: Let $\left(G,*\right)$ be an abelian group and let $\left(H,*\right)$ be the subgroup of G.

Let $a,\ a^{-1}\in G$ and let $h\in H$.

Consider $a*h*a^{-1}=a*a^{-1}*h$ {since G is abelian}

$=e*h$ {identity law}

$$= h \in H$$

Therefore $(H,*)$ is the normal subgroup of G.

Theorem: Prove that the intersection of two normal subgroups of a group G is again a normal subgroup of G.

Proof: Let H and K be two normal subgroups of G. Therefore H and K are two subgroups of G. Therefore $H \cap K$ is a subgroups of G.

Let $a,\ a^{-1} \in G$ and let $h \in H \cap K$.

Since H is a normal subgroup, $a*h*a^{-1} \in H$. Also since K is a normal subgroup, $a*h*a^{-1} \in K$.

Therefore $a*h*a^{-1} \in H \cap K$, for $a,\ a^{-1} \in G$ and $h \in H \cap K$.

Hence $H \cap K$ is a normal subgroup of G.

Example: If H is a subgroup of G such that $x^2 \in H$ for every $x \in G$ prove that H is a normal subgroup of G.

Solution: Let H is a subgroup of G such that $x^2 \in H$ for every $x \in G$.

For any $a \in G$ and $h \in H$, we have $a*h \in G$ then $(a*h)^2 \in H$ .....(1)

Since $a^{-1} \in G$, then $\left(a^{-1}\right)^2 \in H$. Also $h^{-1}, a^{-2} \in H$, then $h^{-1}*a^{-2} \in H$ ......(2)

From (1) and (2), $(a*h)^2 * h^{-1} * a^{-2} \in H$

$$a*h*a*h*h^{-1}*a^{-2} \in H$$

$$a*h*a*e*a^{-2} \in H$$

$$a*h*a*a^{-2} \in H$$

$$a*h*a^{-1} \in H$$

$$a^{-1}*h*a \in H$$

Therefore H is a normal subgroup.

HOMOMORPHISM OF GROUPS

Definition: Let $\langle G,* \rangle$ and $\langle H,\bullet \rangle$ be two groups. A mapping $f : G \to H$ is called group homomorphism from $\langle G,* \rangle$ to $\langle H,\bullet \rangle$ if for any $a,\ b \in G$, $f(a*b) = f(a)$□$f(b)$.

Note: If f is both one to one and onto, then f called isomorphism.

Example: Define $f:\left(R^{+},\times\right)\rightarrow\left(R,+\right)$ by $f(x)=\log_{10}x$.

Consider

$$f(x\times y)=\log_{10}(x\times y)$$

$$=\log_{10}(x)+\log_{10}(x)$$

$$=\ f(x)\ +\ f(y)$$

Therefore f is a homomorphism.

Example: Let G be the group of integers under addition and $H=\{1,-1\}$ is a group under multiplication.

Define $f:\left(G,+\right)\rightarrow\left(H,\times\right)$ by $f(x)=\left|\begin{array}{l}1,\ \textit{if}\ \ x\ \textit{is even}\\ -1,\ \textit{if}\ \ x\ \textit{is odd}\end{array}\right.$.

Case 1: Let $x,\ y\in G$. Suppose both x and y are even. Then $x+y$ is also even.

Therefore $f(x)=1,\ f(y)=1\ \textit{and}\ \ f(x+y)=1$.

Now $f(x+y)=f(x)\times f(y)$ and hence f is a homomorphism

Case 2: Let $x,\ y\in G$. Suppose both x and y are odd. Then $x+y$ is even.

Therefore $f(x)=-1,\ f(y)=-1\ \textit{and}\ \ f(x+y)=1$.

Now $f(x+y)=f(x)\times f(y)$ and hence f is a homomorphism

Case 3: Let $x,\ y\in G$. Suppose x is odd and y is even. Then $x+y$ is odd.

Therefore $f(x)=-1,\ f(y)=1\ \textit{and}\ \ f(x+y)=-1$.

Now $f(x+y)=f(x)\times f(y)$ and hence f is a homomorphism

Example: Define $f:\left(Z,+\right)\rightarrow\left(2Z,+\right)$ by $f(x)=2x$.

Let $x=y$

$$2x=2y$$

$$f(x)=f(y)$$

$\therefore\ f$ is one-to-one

Let $y\in 2Z$. Then y is even.

Then there exists $x\in Z$ such that $f(x)=y$

$$2x=y$$

$$x=\frac{y}{2}\in Z$$

$\therefore\ f$ is onto

Consider

$$f(x+y)=2(x+y)$$

$$=2x+2y$$

$$=\ f(x)\ +\ f(y)$$

$\therefore\ f$ is a homomorphism and hence it is isomorphism.

Example: Define $f:(R,+)\rightarrow(R^{+},\times)$ by $f(x)=e^{x}$.

Let $x=y$

$e^{x}=e^{y}$

$f(x)=f(y)$

$\therefore\ f$ is one-to-one

Let $y\in R^{+}$. Then y is positive.

Then there exists $x\in R$ such that $f(x)=y$

$e^{x}=y$

$x=\log y\in R$

$\therefore\ f$ is onto

Consider

$$f(x+y)=e^{(x+y)}$$

$$=e^{x}\times e^{y}$$

$$=f(x)\times f(y)$$

$\therefore\ f$ is a homomorphism and hence it is isomorphism.

Example: Show that a mapping $f:(S,+)\rightarrow(T,\times)$ defined by $f(x)=3^{x}$, where S is the set of all rational numbers and T is the set of all nonzero real numbers is a homomorphism but not an isomorphism.

Solution: Given $f(x)=3^{x}$ for all $x\in S$.

Let $x,y\in S$.

Then $f(x+y)=3^{x+y}=3^{x}\times3^{y}=f(x)\times f(y)$. Therefore f is a homomorphism.

Let $f(x)=f(y)$

$3^{x}=3^{y}$

$x=y$

Therefore f is one-to-one.

But range of f has no negative numbers and hence it is not onto. i.e. for $-3\in T$ there is no rational number $x\in S$ such that $3^{x}=-3$.

Therefore f is not an isomorphism

Theorem: The group $(Z_{n},+_{n})$ is isomorphic to every cyclic group of order n.

Proof: Let G be a finite cyclic group of order n. Let $a\in G$ be the generator.

Therefore $G=\langle a\rangle=\{e,\ a,\ a^{2},\ ....,\ a^{n-1}\}$.

Now define a map $f:Z_{n}\rightarrow G$ by $f(k)=a^{k}$, for all $k\in Z_{n}$.

Suppose $f(r)=f(s)$ where $r,\ s\in Z_{n}$

$a^{r}=a^{s}$

$a^{r}a^{-s}=a^{s}a^{-s}$

$a^{r-s}=e$

Since $O(a)=n$, it follows that n divides $r-s$.

But $r<n$ and $s<n,$ we get $r=s$ and hence f is one-to-one.

Clearly f is onto.

Consider $f(r+_n s)=a^{r+s}=a^r a^s = f(r)f(s)$. Therefore f is homomorphism.

Thus we conclude that $\left(Z_n, +_n\right)$ is isomorphic to G.

Theorem: Let $f:(G,*)\to f:(G',\Delta)$ be a group homomorphism. Then prove that

(1) $\left[f(a)\right]^{-1}=f\left(a^{-1}\right), \forall\ a\in G$ (2) $f(e)$ is an identity of G', when e is an identity of G.

Proof: Let $a\in G$. Let $e,\ e'$ be the identities of G and G' respectively.

(1) To prove $\left[f(a)\right]^{-1}=f\left(a^{-1}\right), \forall\ a\in G$

Let $a\in G$. Then $a*a^{-1}=e$. Also $a^{-1}*a=e$

Therefore $f\left(a*a^{-1}\right)=f\left(e\right)=e'$ Therefore $f\left(a^{-1}*a\right)=f\left(e\right)=e'$

$f\left(a\right)\Delta f\left(a^{-1}\right)=e'$ $f\left(a^{-1}\right)\Delta f\left(a\right)=e'$

Therefore, we have $f\left(a\right)\Delta f\left(a^{-1}\right)=f\left(a^{-1}\right)\Delta f(a)$

i.e. $f\left(a^{-1}\right)$ is the inverse of $f(a)$. i.e. $\left[f(a)\right]^{-1}=f\left(a^{-1}\right)$

i.e. group homomorphism preserves inverses.

(2) To prove $f(e)$ is an identity of G', when e is an identity of G.

$f(a)=f\left(a*e\right)$

$= f(a)\Delta f(e).......(1) \quad f\ is\ a\ \text{hom}\,omorphism$

Also $f(a)=f(a)\Delta\ e'$ .... (2)

From (1) and (2), $f(a)\Delta f(e)=f(a)\Delta e'$

$f(e)=e'$, {by left cancellation law}

i.e. group homomorphism preserves identities.

Theorem: Let $f:G\to G'$ be a group homomorphism. Then if H is a subgroup of G, then $f(H)=\left\{f(h):h\in H\right\}$ is a subgroup of G'.

https://doi.org/10.5281/zenodo.15287805

Proof: Let $e,\ e'$ be the identities of G and G' respectively.
Let $f(H)=\{f(h): h\in H\}$.
Since H is a sub group of G, $e\in H$. Therefore $f(e)\in f\left(H\right)$.

To prove $f\left(H\right)$ is a sub group, chose $a, b\in f\left(H\right)$ and show that $ab^{-1}\in f\left(H\right)$

Let $a, b\in f\left(H\right)$. Then there exists $x,\ y\in H$ such that $a=f(x), b=f(y)$.

Therefore $ab^{-1}=f(x)\left[f(y)\right]^{-1}=f(x)f\left(y^{-1}\right)=f\left(xy^{-1}\right)$

Since H is a sub group of G, $x,\ y\in H\ \Rightarrow\ xy^{-1}\in H$. Therefore $ab^{-1}=f\left(xy^{-1}\right)\in f\left(H\right)$.

Therefore $f\left(H\right)$ is a subgroup of G'.

Definition: Let $f:G\to H$ is a group homomorphism. The **kernel** is defined as $K=\{\ x\in G:\ f(x)=e'\ \}$ where e' is the identity element of H.

Theorem: Let $f:G\to H$ be a homomorphism with kernal K. Then prove that K is a sub group of G.

Proof: Let $e,\ e'$ be the identities of G and H respectively. Let $K=\{\ x\in G:\ f(x)=e'\ \}$.

Now $e\in G$ and $f(e)=e'$. Therefore $e\in K$ and hence K is non empty.
Let $a, b\in K$. Then $f(a)=e'$ and $f(b)=e'$.

Consider

$$\begin{aligned}f\left(ab^{-1}\right)&=f(a)f\left(b^{-1}\right)\\&=f(a)f(b)^{-1}\\&=e'\left(e'\right)^{-1}\\&=e'e'\\&=e'\end{aligned}$$

Therefore $a, b\in K\ \Rightarrow ab^{-1}\in K$ and hence K is a subgroup of G.

Theorem: Prove that the Kernal of a homomorphisms f from $\langle G,*\rangle$ to $\langle H,\bullet\rangle$ is a normal sub group of $\langle G,*\rangle$.

Proof : Let $f:\langle G,*\rangle\to\langle H,\bullet\rangle$ be a group homomorphism with kernel K. Then K is a subgroup of G.

Let $e,\ e'$ be the identities of G and H respectively.

By definition kernel $K=\{\ x\in G:\ f(x)=e'\ \}$

https://doi.org/10.5281/zenodo.15287805

Now $e \in G$ and $f(e) = e'$. Therefore $e \in K$ and hence K is non empty.

Let $a, b \in K$. Then $f(a) = e'$ and $f(b) = e'$.

Consider $f\left(a * b^{-1}\right) = f\left(a\right)\square f\left(b^{-1}\right)$ {since f is a homomorphism}

$$= f\left(a\right)\square\left[f\left(b\right)\right]^{-1}$$

$$= e'\square\left(e'\right)^{-1}$$

$$= e'\square e'$$

$$= e'$$

Therefore $a * b^{-1} \in K$ and hence K is a subgroup of G.

Now let $a, a^{-1} \in G$ and let $k \in K$.

Consider $f\left(a * k * a^{-1}\right) = f\left(a\right)\square f\left(k\right) \bullet f\left(a^{-1}\right)$

$$= f\left(a\right)\square e' \bullet f\left(a^{-1}\right)$$

$$= f\left(a\right) \bullet \left[f\left(a\right)\right]^{-1}$$

$$= e'$$

Therefore $a * k * a^{-1} \in K$ for all $a \in G$ and for all $k \in K$. Therefore K is a normal subgroup of G.

Theorem: (Fundamental theorem of homomorphism) Let $f : G \to G'$ be a homomorphism of G onto G' with kernel K. Then $G / K \square G'$.

Proof: Let $f : G \to G'$ be a homomorphism of G onto G'. Let Ker f = K. $\therefore f(x) = e', \ for \ x \in K \subseteq G$

Let e, e' be the identities of G and G' respectively.

Let $\phi : G \to G / K$ be a homomorphism defined by $\phi(g) = Kg, \ \forall \ g \in G$.

Define a mapping $\psi : G / K \to G'$ by $\psi\left(Kg\right) = f(g), \ \forall \ g \in G$

$$\begin{tikzcd}
g \in G \arrow[rr, "f"] \arrow[dr, "\phi"'] & & G' \\
& Kg \in G/K \arrow[ur, "\psi"'] &
\end{tikzcd}$$

(i) To prove ψ is well defined.

Suppose $Kg_1 = Kg_2 \Rightarrow g_1 \in Kg_2$

$\Rightarrow g_1 = kg_2$ for some $k \in K$

$\Rightarrow f\left(g_1\right) = f\left(kg_2\right)$

$\Rightarrow f\left(g_1\right) = f\left(k\right) f\left(g_2\right)$, since f is a homomorphism

$\Rightarrow f\left(g_1\right) = e' \ f\left(g_2\right)$, since $k \in K$

https://doi.org/10.5281/zenodo.15287805

$$\Rightarrow\ f(g_1) = f(g_2)$$

$$\Rightarrow\ \psi(Kg_1) = \psi(Kg_2)$$

(ii) To prove ψ is one-to-one.

Suppose $\psi(Kg_1) = \psi(Kg_2) \Rightarrow\ f(g_1) = f(g_2)$

$$\Rightarrow\ f(g_1)\left[f(g_2)\right]^{-1} = e'$$

$$\Rightarrow\ f(g_1)\, f\left(g_2^{-1}\right) = e'$$

$$\Rightarrow\ f\left(g_1 g_2^{-1}\right) = e'$$

$$\Rightarrow\ g_1 g_2^{-1} \in K$$

$$\Rightarrow\ g_1 \in Kg_2$$

$$\Rightarrow Kg_1 = Kg_2$$

(iii) To prove ψ is onto.

Let $g' \in G'$. Since f is onto, there exists $g \in G$ such that $f(g) = g'$.

Therefore there exists $Kg \in G/K$ such that $\psi(Kg) = f(g) = g'$.

Therefore ψ is onto.

(iii) To prove ψ is a homomorphism.

$$\begin{aligned}\psi\left[(Kg_1)(Kg_2)\right] &= \psi\left[Kg_1g_2\right]\\ &= f\left[g_1g_2\right]\\ &= f(g_1)\, f(g_2)\\ &= \psi(Kg_1)\psi(Kg_2)\end{aligned}$$

Thus ψ is an isomorphism and hence $G/K \cong G'$

Theorem: Let $(G, *)$ be a group and let H be a normal subgroup of G. If G/H be the set $\{aH \mid a \in G\}$ then show that $(G/H, \otimes)$ is a group, where $aH \otimes bH = (a*b)H$, for all $a*H,\ b*H \in G/H$. Further, show that there exists a natural homomorphism $f : G \to G/H$.

Proof: Given quotient group $G/H = \{a*H \mid a \in G\}$

(i) To prove the operation $\otimes$ defined by $a*H \otimes b*H = (a*b)H$ is well defined.

Let $a' \in aH$ and $b' \in bH$. Then $a'H = aH$ and $b'H = bH$.

To prove : $(aH)\otimes(bH) = (a'H)\otimes(b'H)$ i.e. $(a*b)H = (a'*b')H$

Since $a' \in aH$ and $b' \in bH$, we have $a' = ah_1,\ b' = bh_2$ for some $h_1, h_2 \in H$.

Therefore

$$\begin{aligned} a'b' &= ah_1 bh_2 \\ &= ab\left(b^{-1}h_1 b\right)h_2,\ \{\because N \textit{ is normal subgroup of } G,\ h_1 \in N,\ a \in G \textit{ then } b^{-1}h_1 b = h_3 \in N\} \\ &= abh_3h_2 \\ &= abh_4,\ \ \textit{where } h_3h_2 = h_4 \in N \end{aligned}$$

Therefore $a'b' \in abH$. Also $a'b' \in a'b'H$.

Since any two cosets are either identical or disjoint, $abH = a'b'H$

i.e. $(a*b)H = (a'*b')H$

Therefore the operation $\otimes$ is well defined.

(ii) To prove $\otimes$ is associative.

Let $a*H, b*H, c*H \in G/H$. Then

$$\begin{aligned} (a*H)\otimes\left[(b*H)\otimes(c*H)\right] &= (a*H)\otimes(b*c*H) \\ &= \left(a*(b*c)*H\right) \\ &= \left((a*b)*c*H\right) \\ &= \left((a*b)*H\right)\otimes(c*H) \\ &= \left[(a*H)\otimes(b*H)\right]\otimes(c*H) \end{aligned}$$

(iii) Let e be the identity of G. Then $H = e*H \in G/H$.

Then $(a*H)\otimes H = (a*H)\otimes(e*H) = (a*e)H = a*H$.

Similarly $H\otimes(a*H) = a*H$

Therefore H is the identity element of G/H.

(iv) Consider $(a*H)\otimes\left(a^{-1}*H\right) = \left(a*a^{-1}*H\right) = (e*H) = H$.

Similarly $\left(a^{-1}*H\right)\otimes(a*H) = H$.

https://doi.org/10.5281/zenodo.15287805

Therefore the inverse of $\left(a*H\right)\in G/H$ is $\left(a^{-1}*H\right)\in G/H$.

Therefore G/H is a group.,

Existence of homomorphism:

Consider the mapping $f:G\to G/H$ defined as $f(a)=a*H \;:\; a\in G$.

$$f(a*b)=\left(a*b\right)*H=\left(a*H\right)\otimes\left(b*H\right)=f(a)\otimes f(b)$$

Theorem: Prove that every finite group of order n is isomorphic to a permutation group of degree n.

Proof: Step 1: To find the set of permutations.

Let G be a finite group of order n. Let $a\in G$. Define $f_a:G\to G$ by $f_a(x)=ax$.

Here f_a is one to one function. Because $f_a(x)=f_a(y)$

$$ax=ay$$

$$x=y$$

Also f_a is on to function. Let $y=f_a(x)=ax$ and hence $x=a^{-1}y$

Therefore if $y\in G$, then there exists $x=a^{-1}y$ such that $f_a(x)=f_a\left(a^{-1}y\right)=aa^{-1}y=y$.

Therefore f_a is bijective and also is a permutation of n elements of G .

Let $G^{'}=\left\{f_a:a\in G\right\}$

Step 2: To prove $G^{'}$ is a group. Let $f_a,\ f_b\in G$.

Consider $(f_a\circ f_b)(x)=f_a\left[f_b(x)\right]=f_a(bx)=(ab)(x)=f_{ab}(x)\in G'$.

Therefore G' is closed under composition of mapping and hence it is associative.

Since $e\in G$ be the identity element of G , $f_e\in G'$ is the identity element of G' .

Because $f_e(e)=e.e=e$.

Consider $\left(f_{a^{-1}}\circ f_a\right)(x)=f_{a^{-1}}\left[f_a(x)\right]=f_{a^{-1}}(ax)=(a^{-1})(ax)=\left(a^{-1}a\right)x=ex=f_e(x)$.

Hence $f_{a^{-1}}$ is the inverse of f_a.

Hence G' is a group of permutation.

To prove G is isomorphic to G'. Define $g:G\to G'$ by $g(a)=f_a$.

Let $g(a)=g(b)$

$$f_a=f_b$$

$$f_a(x)=f_b(x)$$

https://doi.org/10.5281/zenodo.15287805

$ax = bx$

$a = b$. Hence g is one to one function.

Also for all $f_a \in G'$ there is $a \in G$ such that $g(a) = f_a$. Hence g is onto.

Consider $g(ab) = f_{ab}$

$= f_{ab}(x)$

$= (ab)x$

$= (ax)(bx)$

$= f_a(x)\, f_b(x)$

$= g(a)\, g(b)$

Hence g is one-one, onto homomorphism and hence g is isomorphic.

Algebraic Systems With Two Binary Operations

Definition: A non empty set R together with the binary operations + and • is said to a Ring if,

(1) $(R,+)$ is an abelian group

(2) • is associative

(3) • is distributive over addition

Definition: A ring R is said to be commutative if the binary operation • is commutative.

Example: $(R,+,\bullet)$, $(Z,+,\bullet)$, $(Q,+,\bullet)$ are commutative rings.

Example: Prove that the set $Z_4 = \{[0], [1], [2], [3]\}$ is a commutative ring with respect to the binary operation $+_4$ and $\times_4$.

To prove $(Z_4, +_4)$ is an abelian group.

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

From the table, $+_4$ is closure and associative.
[0] is the identity under $+_4$.

Inverse of [0] is [0]. Inverse of [1] is [3].

To prove $\times_4$ is associative

$\times_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

From the table $\times_4$ is associative.

For example consider

Inverse of $[2]$ is $[2]$. Inverse of $[3]$ is $[1]$.

Also $a +_4 b = b +_4 a$.
Therefore $(Z_4, +_4)$ is an abelian group.

$$[1]\times_4 ([2]\times_4 [3]) = ([1]\times_4 [2])\times_4 [3]$$
$$[1]\times_4 [2] = [2]\times_4 [3]$$
$$[2] = [2]$$

Also from the table $\times_4$ is commutative

To prove $\times_4$ is distributive over addition i.e. $a \times_4 (b +_4 c) = (a \times_4 b) +_4 (a \times_4 c)$

For example Consider,

$$[1]\times_4 ([2] +_4 [3]) = ([1]\times_4 [2]) +_4 ([1]\times_4 [3])$$
$$[1]\times_4 [1] = [2] +_4 [3]$$
$$[1] = [1]$$

Therefore Z_4 is a commutative ring with respect to the binary operation $+_4$ and $\times_4$.

Example: Prove that the set M of all $n \times n$ matrices with real elements is a non commutative ring with respect to matrix addition and matrix multiplication as binary operation.

Solution: Let M be the set of all $n \times n$ matrices with real elements.

Closure : Sum of any two $n \times n$ matrices is also a $n \times n$ matrix

Associative : Matrix addition is associative

Identity : $(0)_{n\times n}$ is the identity element

Inverse : For any $A \in M$ then $-A \in M$ such that $A + (-A) = (0)_{n\times n}$

Commutative: For all $A, B \in M$, $A + B = B + A$

Therefore $(M, +)$ is an abelian group.

Also matrix multiplication is associative and hence $(M, \times)$ is a semi group.

To prove matrix multiplication is distributive over matrix addition.

i.e. $A \times (B + C) = (A \times B) + (A \times C)$

For example Consider,

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\times\left(\begin{pmatrix}1 & 0\\2 & 1\end{pmatrix}+\begin{pmatrix}0 & 1\\0 & 1\end{pmatrix}\right)=\left(\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\times\begin{pmatrix}1 & 0\\2 & 1\end{pmatrix}\right)+\left(\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\times\begin{pmatrix}0 & 1\\0 & 1\end{pmatrix}\right)$$

$$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\times\begin{pmatrix}1 & 1\\2 & 2\end{pmatrix}=\begin{pmatrix}3 & 1\\2 & 1\end{pmatrix}+\begin{pmatrix}0 & 2\\0 & 1\end{pmatrix}$$

$$\begin{pmatrix}3 & 3\\2 & 2\end{pmatrix}=\begin{pmatrix}3 & 3\\2 & 2\end{pmatrix}$$

Since matrix multiplication is not commutative, $(M,+,\times)$ is non commutative ring.

Definition: A ring R is said to be a ring with identity if there exists an element $a\in R$ such that $a\bullet e=e\bullet a=a$ for all $e\in R$.

Example: $(R,+,\bullet)$, $(Z,+,\bullet)$, $(Q,+,\bullet)$ are rings with identity.

Definition: A non zero element $a\in R$ is a zero divisor if there exists a nonzero element $b\in R$ such that $ab=0$.

Example: In the Ring Z_{12}, $[3]$ is a zero divisor because $[3]\times_{12}[4]=0$.

Definition: A commutative ring R with a identity element e is an integral domain if R has no zero divisors..

Example: Z *and* Z_7 are integral domain.

Example: Show that $(Z,+,\times)$ is an integral domain where Z is the set of all integers.

Solution: Let Z be the set of all integers and addition is the binary operation

Let $a, b, c\in Z$

Closure: Sum of two integers is again an integer

Associative: Addition is associative on Z

Identity : 0 is the additive identity

Inverse : For any $a\in Z$ there is $-a\in Z$ such that $a+(-a)=0$

Commutative: $a+b=b+a$ for all $a,b\in Z$

$\therefore$ $(Z,+)$ is an abelian group.

Multiplication is associative on Z and 1 is the identity with respect to multiplication.

$\therefore$ $(Z,\times)$ is a Monoid.

Also multiplication is commutative on Z and it is distributive over addition.

There is no non zero integers a & b such that $a\times b=0$ and $a+b=0$.

https://doi.org/10.5281/zenodo.15287805

Therefore $(Z,+,\times)$ is without zero divisors and hence an integral domain.

Example: If $(R, +, .)$ is a ring then prove that $a.0 = 0, \forall a \in R$ and 0 is the identity element in R under addition.

Proof: Consider

$$a \bullet 0 = a \bullet 0 + 0$$

$$= a \bullet 0 + a \bullet 0 \ \{distributive \ \ property\}$$

$$0 = a \bullet 0$$

Definition: A field is a system $(F, +, .)$ satisfying the following conditions:

(i) $(F, +)$ is an abelian group

(ii) $(F - \{0\}, \ .)$ is an abelian group

(iii) $a.(b+c) = a.b + a.c \ \forall \ a, \ b, \ c \in F$

Example: $(R,+,\bullet)$, $(C,+,\bullet)$, $(Q,+,\bullet)$ are fields under usual addition and multiplication.

Example: Give an example of an integral domain which is not a field.

Consider the Ring of integers. It is an infinite integral domain but not a field.

Also Z is an infinite integral domain but not a field.

Note: A finite integral domain is a field.

EXERCISE

1. Find all the left co-sets of $H = \{1, -1\}$ in the group $(G,.)$ where $G = \{1, -1, i, -i\}$.
2. Is it true that $\left(\mathbf{Z}^{*}_{55},\times_{5}\right)$ a cyclic group? Justify your answer.
3. Show that $\left(Q^{+},*\right)$ is an abelian group, where * is defined by $a*b = \dfrac{ab}{2}, \ \forall\, a, \ b \in Q^{+}$.
4. Let Z be the group of integers with the binary operation * defined by $a*b = a+b-2$, for all $a, \ b \in Z$. Find the identity element of the group $(Z,*)$.
5. Give an example of an integral domain which is not a field.
6. Prove that $G = \{[1], \ [2], \ [3], \ [4]\}$ is an abelian group under multiplication modulo 5.
7. Prove that the set $Z_4 = \{[0], \ [1], \ [2], \ [3]\}$ is a commutative ring with respect to the binary operation $+_4$ and $\times_4$.
8. Examine whether $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \neq 0 \in R \right\}$ is a commutative group under matrix multiplication, where R is the set of all real numbers.
9. Find the left cosets of $\{[0], \ [3]\}$ in the group $(Z_6, \ +_6)$.
10. Find the idempotent elements of $G = \{1, \ -1, \ i, \ -i\}$ under the binary operation multiplication.

11. Find all the subgroups of $(Z_9, +_9)$.

12. If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a,b)*(x,y) = (ax,\ ay+b)$, show that $(S,*)$ is a semi group. Is it commutative? Also find the identity element of S.

13. Show that $(Z,+,\times)$ is an integral domain where Z is the set of all integers.

14. If $(Z,+)$ and $(E,+)$ where Z is the set of all integers and E is the set of all even integers. Show that the two semigroups $(Z,+)$ and $(E,+)$ are isomorphic.

https://doi.org/10.5281/zenodo.15287805

UNIT V – LATTICES AND BOOLEAN ALGEBRA

Relation is a fundamental concept in Set theory. Equivalence relation, partial ordering and functions are special types of relations. Recall the definition that a non empty set P together with a relation ≤ which is reflexive, anti-symmetric and transitive is called partially ordered set or poset, denotd by $(P,\leq)$. In a poset if $a\leq b$, then $(a,b)\in R$. In this chapter we introduce lattice as a partially ordered set with some additional characteristics and study its properties.

Example: Show that $(N,\leq)$ is a partially ordered set where N is set of all positive integers and ≤ is defined by $m\leq n$ if and only if $n-m$ is a non negative integer.

Given $N=\{0,1,2,3,..........\}$.

The relation $R(\leq)$ is defined by $m\leq n$ if and only if $n-m$ is a non negative integer.

Here for all $a\in N$, $a-a=0$ is a non negative integer and $(a,a)\in R$. Therefore the relation is reflexive.

Suppose that for $a,b\in N$, $b-a=k$, a non negative integer. But $a-b=-k$, a negative integer. If $a-b=b-a=k$, a non negative integer then $a=b$. Therefore if $(a,b)\in R$ *and* $(b,a)\in R$, then $a=b$. Therefore relation is antisymmetric.

Suppose that $(a,b),(b,c)\in R$, then $b-a=k$, a non negative integer and $c-b=l$, a non negative integer.

Adding, we have $(b-a)+(c-b)=k+l$

$(c-a)=k+l$, a non negative integer

Therefore $(a,c)\in R$

Therefore $(N,\leq)$ is a partially ordered set

Definition: Let $(P,\leq)$ be a poset. The elements $a,b\in A$ are said to be comparable if $a\leq b$ or $b\leq a$.

Example: Consider the poset $(\mathrm{Z}^+,|)$. Here 3, 8 are not comparable but 3, 9 are comparable.

Definition: Let $(P,\leq)$ be a poset. If every pair of elements of P are comparable, then P is called totally ordered set and the relation ≤ is called total order. A totally ordered set is called a **chain**.

Example: The set of real numbers with usual order ≤ is a totally ordered set.

Hasse Diagrams of Partially Ordered Sets

A partial order $(P,\leq)$ can be represented by means of a diagram called Hasse diagram. We discuss the procedure for constructing the Hasse diagram.

https://doi.org/10.5281/zenodo.15287996

Let $(P, \leq)$ be a poset and $a, b \in P$. Then the element a is an immediate predecessor of b then $a < b$ and no element $c \in P$ that lies between a and b.

Equivalently this can be stated as b is an immediate successor of a or b covers a denoted by $a << b$.

The Hasse diagram of a finite partially ordered set P is a directed graph whose vertices are elements of P and there is an directed edge from a to b whenever $a << b$ in P.

Instead of drawing an directed edge from a to b, it is customary to place b higher than a and draw undirected line between them. So the Hasse diagram of a finite poset is a undirected self loop free graph.

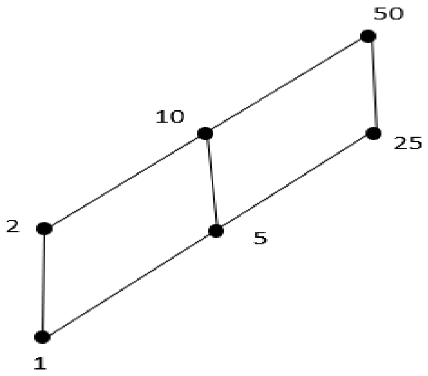
Hint: To obtain the Hasse diagram of a poset, first draw the directed graph of the relation ad then delete all loops and all edges implied by transitive property. Incomparable elements are placed in horizontal line.

Example: Draw the Hasse diagram of D_{50} , the set of all positive divisors of 50.

The elements of D_{50} are $\{1,\ 2,\ 5,\ 10,\ 25,\ 50\}$

Here 2, 5 and 10, 25 pairs are incomparable and hence they are on the same level.

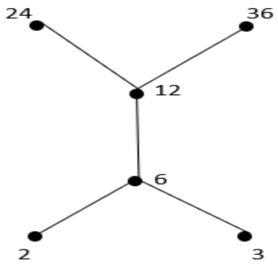
Also 1<<2, 1<<5, 2<<10, 5<<10, 5<<25, 10<<50, 25<<50



.

Example: Draw the Hasse diagram of the poset $(P, \leq)$ where $P = \{2,\ 3,\ 6,\ 12,\ 24,\ 36\}$ and $x \leq y$ if $x \mid y$.

Here the pairs 2, 3 and 24, 36 are incomparable and hence they are on the same level.
Also 2<<6, 3<<6, 6<<12, 12<<24, 12<<36



.**Example:** Draw the Hasse diagram of the poset $(P(S), \leq)$ where $P(S)$ is the power set of $S = \{a,\ b,\ c\}$ and $A \leq B$ if $A \subseteq B$

.

Here $P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}$

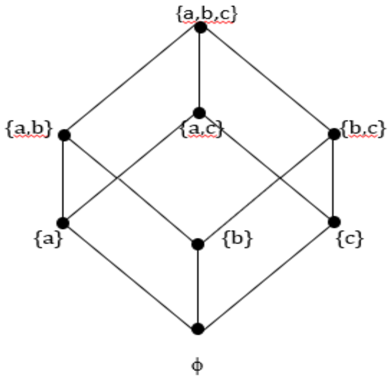
The triplets $\{a\}, \{b\}, \{c\}$ and $\{a,b\}, \{b,c\}, \{a,c\}$ are incomparable and hence they are on the same level. Also

$\phi << \{a\}$, $\phi << \{b\}$, $\phi << \{c\}$ and

$\{a\} << \{a,b\}$, $\{a\} << \{a,c\}$, $\{b\} << \{a,b\}$, $\{b\} << \{b,c\}$,

$\{c\} << \{a,c\}$, $\{c\} << \{b,c\}$.

Also $\{a,b\} << \{a,b,c\}$, $\{a,c\} << \{a,b,c\}$, $\{b,c\} << \{a,b,c\}$



https://doi.org/10.5281/zenodo.15287996

Special Elements in Posets

Let $(P,\leq)$ be a poset. An element $a \in P$ is the **greatest element** of P if $x \leq a$ for all $x \in P$.

A element $a \in P$ is called **maximal element** if $a < x$ for no $x \in P$.

Let $(P,\leq)$ be a poset. An element $a \in P$ is the **least element** of P if $a \leq x$ for all $x \in P$.

A element $a \in P$ is called **minimal element** if $x < a$ for no $x \in P$.

Results:

- The greatest (or least) element, if it exists, is unique.
- A maximal (or minimal) element need not be unique
- Maximal element need not be greatest element
- Minimal element need not be least element
- Maximal elements are at the top of the Hasse diagram
- Minimal elements are at the bottom of the Hasse diagram

Example: Let $S = \{a, b,c\}$. Then $(P(S), \subseteq)$ is a poset.

Let $A = \{\phi, a, b, \{a,c\}\}$
Then $(A, \subseteq)$ is a poset.

Here ϕ is the least element Because
$\phi \subseteq \phi, \quad \phi \subseteq \{a\},$
$\phi \subseteq \{b\}, \quad \phi \subseteq \{a,c\}$

A has no greatest element. Because $b \not\subset \{a,c\}$

But $\{a,c\}$ is the maximal element. Because there is no $x \in A$ such that $\{a,c\} \subset x$.

Also ϕ is the minimal element. Because there is no $x \in A$ such that $x \subset \phi$.

Let $A = \{a, b, \{a,c\},\{a,b,c\}\}$
Then $(A, \subseteq)$ is a poset.

There is no least element Because
$\{a\} \not\subset \{b\}, \; b \not\subset \{a,c\}$

But A has greatest element $\{a,b,c\}$. Because
$\{a\} \subseteq \{a,b,c\}, \quad \{b\} \subseteq \{a,b,c\},$
$\{a,c\} \subseteq \{a,b,c\}, \; \{a,b,c\} \subseteq \{a,b,c\}$

Here $\{a,b,c\}$ is the maximal element. Because there is no $x \in A$ such that $\{a,b,c\} \subset x$.

But $\{a\}$ and $\{b\}$ are the minimal elements. Because there is no $x \in A$ such that $x \subset \{a\}$ and $x \subset \{b\}$.

Let $A = \{\phi, a, b, \{a,b\}\}$
Then $(A, \subseteq)$ is a poset.

Here ϕ is the least element Because
$\phi \subseteq \phi, \quad \phi \subseteq \{a\},$
$\phi \subseteq \{b\}, \quad \phi \subseteq \{a,b\}$

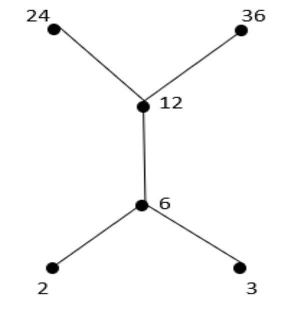
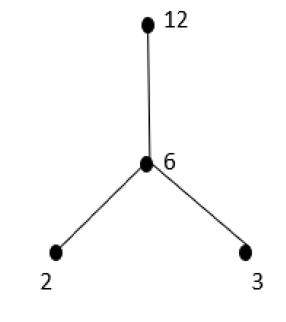
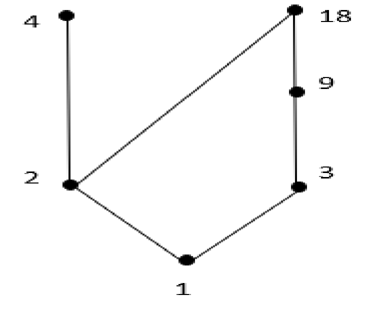
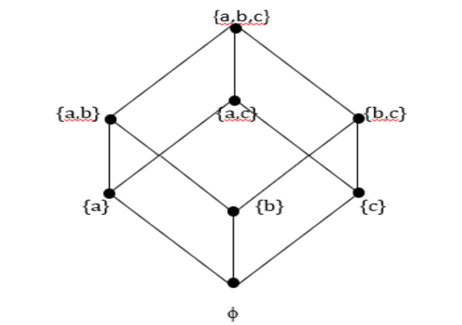
Also A has greatest element $\{a,b\}$. Because
$\{a\} \subseteq \{a,b\}, \quad \{b\} \subseteq \{a,b\},$
$\phi \subseteq \{a,b\}, \quad \{a,b\} \subseteq \{a,b\}$

Here $\{a,b\}$ is the maximal element. Because there is no $x \in A$ such that $\{a,b\} \subset x$.

Also ϕ is the minimal element. Because there is no $x \in A$ such that $x \subset \phi$.

https://doi.org/10.5281/zenodo.15287996

Example: Determine whether the posets P represented by Hasse diagram have a greatest and least element, minimal and maximal elements.

			 {a,b,c}
			{a,b}
			{a,c}
			{b,c}
			{a}
			{b}
			{c}
			ϕ

2,3 have no predecessor and hence they are the minimal elements	2,3 have no predecessor and hence they are the minimal elements	1 has no predecessor and hence it is the minimal element	ϕ has no predecessor and hence it is the minimal element
24, 36 have no successor and hence they are the maximal elements	12 has no successor and hence it is the maximal element	4, 18 have no successor and hence they are the maximal elements	$\{a,b,c\}$ has no successor and hence it is the maximal element
There is no element $a \in P$ such that $a \leq x$ for all $x \in P$ and hence P has no least element	There is no element $a \in P$ such that $a \leq x$ for all $x \in P$ and hence P has no least element	The element $1 \in P$ such that $1 \leq x$ for all $x \in P$ and hence 1 is the least element	The element $\phi \in P$ such that $\phi \leq x$ for all $x \in P$ and hence ϕ is the least element
There is no element $a \in P$ such that $x \leq a$ for all $x \in P$ and hence P has no greatest element	The element $12 \in P$ such that $x \leq 12$ for all $x \in P$ and hence 12 is the greatest element	There is no element $a \in P$ such that $x \leq a$ for all $x \in P$ and hence P has no greatest element	The element $\{a,b,c\} \in P$ such that $x \leq \{a,b,c\}$ for all $x \in P$ and hence $\{a,b,c\}$ is the greatest element

Definition: A set with an ordering relation is **well order** if every non empty subset of the set has a least element.

Example: The set of positive integers with ordering ≤ is well ordered.
But the set of integers with ordering ≤ is not well ordered, because the subset of negative integers has no least element.

Lower and Upper Bound

Definition: Let P be a poset and $a,b \in P$. An element $c \in P$ is the **lower bound** of a and b if $c \le a$ and $c \le b$, i.e. c precedes a and b.	**Definition:** Let P be a poset and $a,b \in P$. An element $c \in P$ is the **upper bound** of a and b if $a \le c$ and $b \le c$, i.e. c succeeds a and b.
Example: Consider the poset $P=\{3,4,5,6,7\}$ with the partial order relation ≤. Let $A=\{4,6\}$ be a sub set of P. Here $3 \le 4, 3 \le 6$ & $4 \le 4, 4 \le 6$ Therefore the lower bounds of A are 3, 4.	**Example:** Consider the poset $P=\{3,4,5,6,7\}$ with the partial order relation ≤. Let $A=\{4,6\}$ be a sub set of P. Here $4 \le 6$, $6 \le 6$ & $4 \le 7$, $6 \le 7$ Therefore the upper bounds of A are 6, 7.
Definition: An element $g \in A$ is called greatest lower bound(glb) of a and b if and only if $g \le a$ and $g \le b$ and $c \le g$ whenever c is a lower bound of P.	**Definition:** An element $l \in A$ is called least upper bound(lub) of a and b if and only if $a \le l$ and $b \le l$ and $l \le c$ whenever c is a lower bound of P.
Note: In the above example 4 is the greatest lower bound of P.	**Note:** In the above example 6 is the least upper bound of P.
Note: The greatest lower bound of $\{a,b\}$ is denoted by $a \wedge b$ or $a * b$ and is called meet or product. In the above example, $a \wedge b = 4$ or $a * b = 4$	**Note:** The least upper bound of $\{a,b\}$ is denoted by $a \vee b$ or $a \oplus b$ and is called join or sum. In the above example, $a \vee b = 6$ or $a \oplus b = 6$

Result:

- A sub set A of a poset may or may not have upper or lower bounds
- An upper or lower bound may or may not belong to the subset A itself.
- More than one upper or lower bound may exist
- The greatest element is always the least upper bound but the converse is not true.
- The least element is always the greatest lower bound but the converse is not true
- The LUB and GLB of a subset of a poset, if they exist, are unique.

Theorem: Show that least upper bound of a sub set B in a poset $(A,\le)$ is unique if it exist.

Let $B=\{a,b\}$. Let u_1, u_2 be two different least upper bounds of B.

By definition of upper bound, $a \le u_1, a \le u_2, b \le u_1, b \le u_2$.

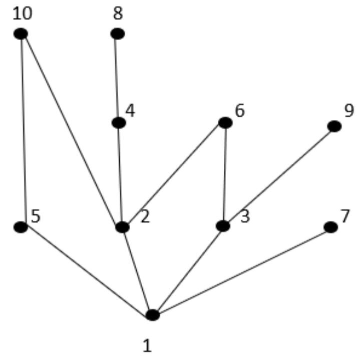
Suppose u_1 is a LUB of $B=\{a,b\}$ then $u_1 \le u_2$ for any other upper bound u_2

Suppose u_2 is a LUB of $B=\{a,b\}$ then $u_2 \le u_1$ for any other upper bound u_1

Therefore by antisymmetric, $u_1 = u_2$.

Note: The proof for uniqueness of GLB is analogous as LUB.

Example: Let $P = \{1,2,3,.....,9,10\}$ and the partial ordered relation be ‘divides’. Discuss the lower and upper bounds of the given subsets. $A = \{5, 8\}$, $A = \{2, 5\}$, $A = \{1, 2, 3\}$, $A = \{1, 2, 4\}$.



(i) Let $A = \{5, 8\}$ be a sub set of P.

Here $1 \le 5$ and $1 \le 8$. Hence $1 \in P$ precedes every element of A and it is the lower bound of A.

But there is no element $a \in P$ such that $5 \le a$ and $8 \le a$. Hence the set A has no upper bound.

(ii) Let $A = \{2, 5\}$ be a sub set of P.

Here $2 \le 10$ and $5 \le 10$. Hence $10 \in P$ succeeds every element of A and it is the upper bound od A.

Also $1 \le 2$ and $1 \le 5$. Hence $1 \in P$ precedes every element of A and it is the lower bound of A.

(iii) Let $A = \{1, 2, 3\}$ be a sub set of P.

Clearly $1 \in P$ precedes every element of A and it is the lower bound of A.

Clearly $6 \in P$ succeeds every element of A and it is the upper bound of A.

(iv) Let $A = \{1, 2, 4\}$ be a sub set of P.

Clearly $1 \in P$ precedes every element of A and it is the lower bound of A. Therefore $glb\{1,2,4\} = 1$

Also $1 \le 4,\ 2 \le 4,\ 4 \le 4$ and $1 \le 8,\ 2 \le 8,\ 4 \le 8$. Hence $4, 8 \in P$ succeeds every element of A and hence 4, 8 are the upper bound of A. Therefore $lub\{1,2,4\} = 4$

Example: Let $D_{30} = \{1,2,3,5,6,10,15,30\}$ and let the relation R be divisor on D_{30}. Find

i. all the lower bounds of 10 and 15
ii. the glb of 10 and 15
iii. all upper bound of 10 and 15
iv. the lub of 10 and 15
v. draw the Hasse diagram

(i) Let $A = \{10, 15\}$ be a sub set of D_{30}. Let the relation be divides

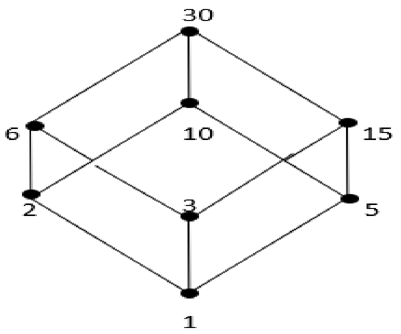
Here $1|10,\ 1|15$ and $5|10,\ 5|15$. Hence $1,5 \in D_{30}$ precedes every element of A and hence 1, 5 are the lower bounds of A.

(ii) $glb\{10, 15\} = 5$

(iii) Here $10 \mid 30,\ 15 \mid 30$. Hence $30 \in D_{30}$ succeeds every element of A and hence 30 is the upper bounds of A.

(iv) $lub\{10, 15\} = 30$

(v) The Hasse diagram



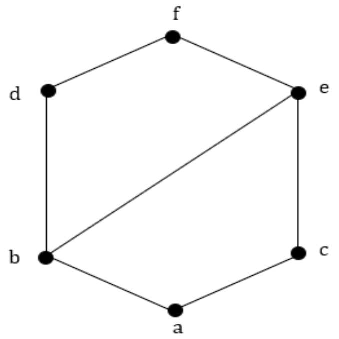
Note: If the partial order is 'divides' then $gcd(x,y) = glb(x,y)$ & $lcm(x,y) = lub(x,y)$.

Example: Verify the above note, with the poset or Hasse diagram of the previous example.

Let $A = \{3, 5\}$ Multiples of 3,5 are 3, 6, 9, 12, 15, 18,… 5, 10, 15, 20, 25,….. Least common multiple of A is 15 Upper bounds of A are 15, 30 Because 3|15, 5|15 and 3|30, 5|30 Least upper bound of A is 15.	Let $A = \{5, 6\}$ Multiples of 5,6 are 5, 10, 15, 20, 25, 30,… 6, 12, 18, 24, 30, 36….. Least common multiple of A is 30 Upper bound of A is 30 Because 5|30, 6|30 Least upper bound of A is 30.
Let $A = \{6, 15\}$ Divisors of 6, 15 are 1, 2, 3, 6 1, 3, 5, 15 Greatest common divisors of A is 3 Lower bounds of A are 1, 3 Because 1|6, 1|15 and 3|6, 3|15 Greatest lower bound of A is 3.	Let $A = \{2, 30\}$ Divisors of 2, 30 are 1, 2 1, 2, 3, 5, 6, 10, 15, 30 Greatest common divisors of A is 2 Lower bounds of A are 1, 2 Because 1|2, 1|30 and 2|2, 2|30 Greatest lower bound of A is 2.

.

Example: Find the lower bound, GLB for $B = \{d, e\}$ and upper bound, LUB for $A = \{a, b, c\}$ of the posets whose Hasse diagrams is given here.

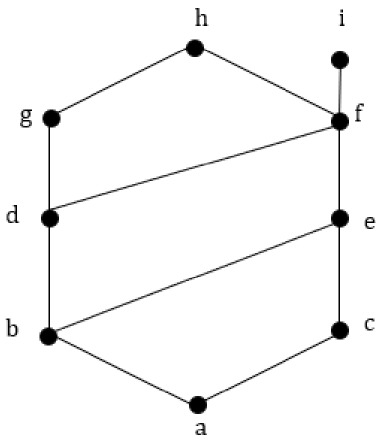


Let $A = \{a, b, c\}$.
The upper bounds of A are $e,\ f$.
Therefore the LUB of A is e.

Let $B = \{d, e\}$
The lower bounds of A are a, b.
Therefore the GLB of A is b.

.

Example: Find the lower and upper bounds of the sub sets $A=\{a,b,c\}$, $B=\{i,\ h\}$ and $C=\{a,c,d,\ f\}$ in the poset with the Hasse diagram given here.
Also find the LUB and GLB of the sub set $D=\{b,d,g\}$, if they exist.



Let $A=\{a,b,c\}$.
The upper bounds of A are $e,\ f,\ i,\ h.$
The lower bound of A is $a.$

Let $B=\{i,\ h\}$
The upper bound of B does not exist.
The lower bounds of B are $a,\ b,\ c,\ d,\ e,\ f.$

Let $C=\{a,c,d,\ f\}$.
The upper bounds of C are $f,\ i,\ h.$
The lower bound of C is $a.$

Example: For the poset $\{(3,5,9,15,24,45),|\}$, draw the Hasse diagram and find

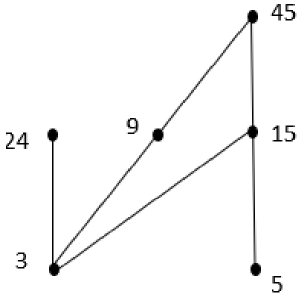
(i) The maximal and minimal elements
(ii) The greatest and least elements
(iii) The upper bounds and LUB of {3,5}
(iv) The lower bounds and GLB of {15, 45}

(i) The minimal elements are 3, 5 and the maximal element is 45

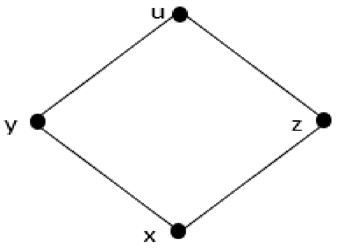
(ii) There exists no least or greatest elements

(iii) Upper bounds of {3, 5} are 15, 45 and hence LUB of {3, 5} is 15

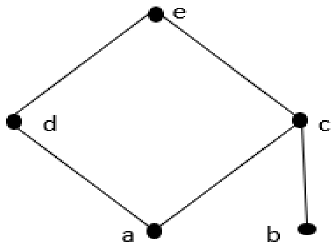
(iv) Lower bounds of {15, 45} are 3, 5 and hence GLB of {15, 45} is 5



Example: Identify the maximal elements, minimal elements, least and greatest (if they exist) of the POSETs given by the following Hasse diagrams.



POSET 1



POSET 2

https://doi.org/10.5281/zenodo.15287996

	POSET 1	POSET 2
Maximal Elements	u	e
Minimal Elements	x	a, b
Least Element	x	Does not exist
Greatest Element	u	e

LATTICE

A lattice is a poset $(L,\leq)$ in which every two element subset has a LUB and GLB. It is denoted as $(L,\wedge,\vee)$.

Example: Let I be the set of all positive integers and R be the relation divides i.e. aRb iff $a\,|\,b$.

Then the poset $(I,|)$ is a lattice in which join and meet of every pair of elements a and b is $a\vee b=lcm(a,b)$ and $a\wedge b=gcd(a,b)$

Example: Let $P(S)$ be the power set of a non empty set S and R be the relation subset i.e. ARB iff $A\subseteq B$.

Then the poset $(P(S),\subseteq|)$ is a lattice in which join and meet of every pair of elements A and B is $A\vee B=A\cup B$ and $A\wedge B=A\cap B$

Example: If $P(S)$ is the power set of S and $\cup,\cap$ are taken as join and meet, prove that $(P(S),\subseteq)$ is a lattice.

Let S be a given set and $P(S)$ be its power set. Let $A,\ B\in P(S)$.
Define a relation ARB on $P(S)$ if AÍ B. Clearly the relation is reflexive, anti-symmetric and transitive. Hence $(P(S),\subseteq)$ is a partially ordered set.

To find the $LUB\{A,\ B\}$.
We know that $A\subseteq(A\cup B)$ and $B\subseteq(A\cup B)$.
Therefore $(A\cup B)$ is the upper bound of $\{A,\ B\}$.
Suppose $A\subseteq C$ and $B\subseteq C$, then $A\cup B\subseteq C$.
Hence $(A\cup B)$ is the least upper bound of $\{A,\ B\}$.

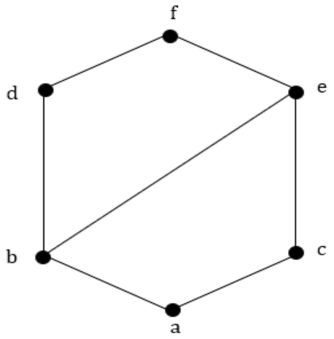
To find the $GLB\{A,\ B\}$.
We know that $(A\cap B)\subseteq A$ and $(A\cap B)\subseteq B$.
Therefore $(A\cap B)$ is the lower bound of $\{A,\ B\}$.
Suppose $C\subseteq A$ and $C\subseteq B$, then $C\subseteq A\cap B$.
Hence $(A\cap B)$ is the greatest lower bound of $\{A,\ B\}$.

i.e. every pair of elements of $P(S)$ has both LUB and GLB under $\subseteq$. Hence $(P(S),\subseteq)$ is a lattice.

Example : Consider the set $S=\{2,3,6,12,24,36\}$ with a binary operation division. Clearly $(S,\ |)$ is a poset. But $GLB(2,\ 3)$ and $LUB(24,\ 36)$ does not exist in S. Hence it is not a lattice.

Example: Consider the following Hasse diagrams of posets. Check whether the poset is a lattice.

https://doi.org/10.5281/zenodo.15287996



Here for any pair of elements of the poset LUB and GLB exists and hence the given poset is a lattice.

For example:

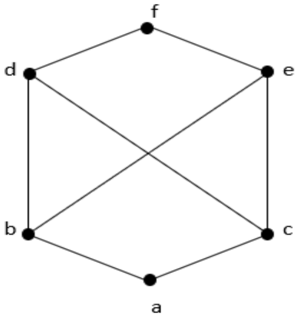
Let $A = \{b, c\}$ be a subset of the given poset

Now upper bounds of A are e, f.

$\therefore$ LUB $\{b, c\} = b \vee c = e$.

Now lower bounds of A is a.

$\therefore$ GLB $\{b, c\} = b \wedge c = a$.



Let $A = \{b, c\}$ be a subset of the given poset

Now upper bounds of A are d, e, f.

But LUB $\{b, c\} = b \vee c =$ does not exist.

Similarly consider a subset $B = \{d, e\}$

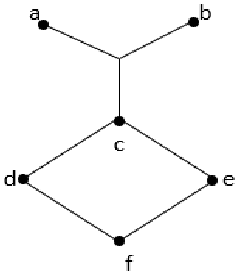
Now lower bounds of B are a, b, c.

But GLB $\{d, e\} = d \wedge e =$ does not exist.

Therefore the given poset is not a lattice.

Note: The Hasse diagram of a lattice is always a combination of closed polygons because any two of its elements have a common predecessor and a common successor.

Here given hasse diagram does not represent a lattice because $a \vee b$ does not exist.



Theorem: Every chain is a lattice.

Proof: Let $(L, \leq)$ be a chain and let $a, b \in L$. In a chain any pair of elements are comparable. Without loss of generality assume that $a \leq b$.

Clearly b is a the upper bound of a and b ……..(1)

Suppose u is any other upper bound of a and b .

Then $a \leq u$ and $b \leq u$ ……(2)

From (1) and (2), we conclude that b is a the least upper bound of a and b .

Therefore $a \vee b = b.$

Also a is a the lower bound of a and b ……..(3)

Suppose l is any other lower bound of a and b .

Then $l \leq a$ and $l \leq b$ ……(4)

From (3) and (4), we conclude that a is a the greatest lower bound of a and b .

Therefore $a \wedge b = a.$

Since both LUB and GLB exists for any pair of elements, the chain $(L, \leq)$ is a lattice.

Definition: A lattice L is said to be **complete** if every subset of it has a LUB and GLB in L.

Example : The lattice $L=\left(P(S),\cup,\cap\right)$ is complete.

The lattice $(R,\leq)$ is not complete because each subset does not posses a unique GLB.

Note: Every complete lattice is bounded
Every finite lattice is complete
Dual of the complete lattice is complete

Principle of Duality

When $\leq$ is a partial ordering relation on a set, the converse $\geq$ is also a partial ordering relation on the same set. For example, if 'divisor of' is a partial ordering relation then 'multiple of' is also a partial ordering.

Note: LUB(A) with respect to $\leq$ is same as GLB(A) with respect to $\geq$ and vice versa.
If $(L,\leq)$ is a lattice, then $(L,\geq)$ is also a lattice. Also the operations $\wedge,\vee$ in $(L,\leq)$ becomes the operations $\wedge,\vee$ in $\vee,\wedge$ in $(L,\leq)$.

Therefore any statement involving $\wedge,\vee$ in $(L,\leq)$ remains true if $\wedge$ is replaced by $\vee$ and $\vee$ is replaced by $\wedge$ and $\leq$ is replaced by $\geq$.

Properties: Let $(L,\leq)$ be a lattice, then for $a,b,c\in L$, the following properties are hold.

$i.$	$a\vee a=a$	and	$a\wedge a=a$	Idempotent
$ii.$	$a\vee b=b\vee a$	and	$a\wedge b=b\wedge a$	Commutative
$iii.$	$a\vee(b\vee c)=(a\vee b)\vee c$	and	$a\wedge(b\wedge c)=(a\wedge b)\wedge c$	Associative
$iv.$	$a\vee(a\wedge b)=a$	and	$a\wedge(a\vee b)=a$	Absorption

Theorem: Show that every ordered lattice $(L,\leq)$ satisfies the above properties of the algebraic lattice.

We know that $(L,\leq)$ is said to be ordered lattice if for every $a,b\in L$ both $a\wedge b,\ a\vee b$ exists. The lattice $(L,\wedge,\vee)$ is called algebraic lattice.

1. **Idempotent Property:**

$a\vee a=LUB(a,a)=LUB(a)=a$	$a\wedge a=GLB(a,a)=GLB(a)=a$

2. **Commutative Property**

$a\vee b=LUB(a,b)=LUB(b,a)=b\vee a$	$a\wedge b=GLB(a,b)=GLB(b,a)=b\wedge a$

3. **Associative Property**

$(a\vee b)\vee c$ is the LUB of $(a\vee b)$ and c	$a\vee(b\vee c)$ is the LUB of a and $(b\vee c)$
Therefore $(a\vee b)\leq(a\vee b)\vee c$ .....(1)	Therefore $a\leq a\vee(b\vee c)$.....(9)
$c\leq(a\vee b)\vee c$ .....(2)	$b\vee c\leq a\vee(b\vee c)$.....(10)

Also $\left(a \vee b\right)$ is the LUB of a and b

Therefore $a \leq \left(a \vee b\right)$ .....(3)

$b \leq \left(a \vee b\right)$ .....(4)

From (1), (3) by transitivity $a \leq \left(a \vee b\right) \vee c$ .....(5)

From (1), (4) by transitivity $b \leq \left(a \vee b\right) \vee c$ .....(6)

From (2), (6) by join $b \vee c \leq \left(a \vee b\right) \vee c$ .....(7)

From (5), (7) by join $a \vee \left(b \vee c\right) \leq \left(a \vee b\right) \vee c$ .....(8)

Also $\left(b \vee c\right)$ is the LUB of b and c

Therefore $b \leq \left(b \vee c\right)$.....(11)

$c \leq \left(b \vee c\right)$.....(12)

From (10), (11) by transitivity $b \leq a \vee \left(b \vee c\right)$..(13)

From (10), (12) by transitivity $c \leq a \vee \left(b \vee c\right)$..(14)

From (9), (13) by join $a \vee b \leq a \vee \left(b \vee c\right)$.....(15)

From (14), (15) by join $\left(a \vee b\right) \vee c \leq a \vee \left(b \vee c\right)$..(16)

Combining (8) and (16), we have $a \vee \left(b \vee c\right) = \left(a \vee b\right) \vee c$

Similarly we can prove the associative property for 'meet' or from the principle of duality it can be obtained.

4. **Absorption Property**

$\left(a \wedge b\right)$ is the GLB of a and b

Therefore $\left(a \wedge b\right) \leq a$ .....(1)

Also $a \leq a$ ....(2)

From (1) and (2) by join, $a \vee \left(a \wedge b\right) \leq a$ .....(3)

But $a \vee \left(a \wedge b\right)$ is the LUB of a and $\left(a \wedge b\right)$.

Therefore $a \leq a \vee \left(a \wedge b\right)$.....(4)

From (3), (4) $a = a \vee \left(a \wedge b\right)$

$\left(a \vee b\right)$ is the LUB of a and b

Therefore $a \leq \left(a \vee b\right)$ .....(5)

Also $a \leq a$ ....(6)

From (1) and (2) by meet, $a \leq a \wedge \left(a \vee b\right)$.....(7)

But $a \wedge \left(a \vee b\right)$ is the GLB of a and $\left(a \vee b\right)$.

Therefore $a \wedge \left(a \vee b\right) \leq a$.....(8)

From (7), (8) $a \wedge \left(a \vee b\right) = a$

5. Property: If $\left(L, \leq\right)$ be a lattice, for any $a, b \in L$ (i) $a \vee b = b$ *iff* $a \leq b$ (ii) $a \wedge b = a$ *iff* $a \leq b$

Let $a \leq b$
Also $b \leq b$
Therefore $a \vee b \leq b$ .....(1)
Since $a \vee b$ is the LUB of (a,b),
we have $b \leq a \vee b$ ....(2)
From (1) and (2) $a \vee b = b$

Conversely, suppose $a \vee b = b$
Since $a \vee b$ is the LUB of (a,b), $a \leq a \vee b$
i.e. $a \leq b$

Proof of (ii) is analogous to proof of (i)

6. Isotonic Property: If $(L,\leq)$ be a lattice, for any $a, b, c \in L$ if $b \leq c$, then $(ii)\ a \wedge b \leq a \wedge c$

we know that if $x \leq y \Rightarrow x \vee y = y$ ......(1)

$$\text{Since } b \leq c \Rightarrow b \vee c = c$$

$$\text{Also } a = a \vee a$$

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

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

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

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

Therefore from (1), $a \vee b \leq a \vee c$

we know that if $x \leq y \Rightarrow x \wedge y = x$ ......(1)

$$\text{Since } b \leq c \Rightarrow b \wedge c = b$$

$$\text{Also } a = a \wedge a$$

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

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

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

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

Therefore from (1), $a \wedge b \leq a \wedge c$

Example: Let $(L,\leq)$ be a lattice. If $a \leq b \leq c$, then (i) $a \vee b = b \wedge c$.
(ii) $(a \wedge b) \vee (b \wedge c) = b = (a \vee b) \wedge (a \vee c)$

Since $a \leq b$, by property (5), we have $a \vee b = b$ and $a \wedge b = a$
Since $b \leq c$, by property (5), we have $b \vee c = c$ and $b \wedge c = b$

Therefore combining the above, $a \vee b = b = b \wedge c$, we get the first result

Consider $(a \wedge b) \vee (b \wedge c) = a \vee b = b$ ....(1) {given above}
Since $a \leq c$ by transitivity, by property (5), we have $a \vee c = c$ and $a \wedge c = a$
Therefore $(a \vee b) \wedge (a \vee c) = b \wedge c = b$ ....(2)

Thus from (1) and (2), we get the second result.

Example: Show that in a lattice if $a \leq b$ and $c \leq d$, then $a * c \leq b * d$ and $a \oplus c \leq b \oplus d$.

Let $(L,\leq)$ be a lattice and assume that $a \leq b$ and $c \leq d$.

$\because$ $a \leq b$, we have $a * c \leq b * c$ (Isotonic)

$\because$ $c \leq d$, we have $b * c \leq b * d$ (Isotonic)

$\therefore$ $a * c \leq b * d$, by transitive property.

$\because$ $a \leq b$, we have $a \oplus c \leq b \oplus c$ (Isotonic)

$\because$ $c \leq d$, we have $b \oplus c \leq b \oplus d$ (Isotonic)

$\therefore$ $a \oplus c \leq b \oplus d$, by transitive property.

Theorem: Let $(L,\leq)$ be a lattice in which $*$ and $\oplus$ denote the operation of meet and join respectively.
For any $a, b \in L$, $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.

Proof: With usual notations, we have to prove that for any $a,b \in L,\ a \le b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b$.

$(i)\quad a \le b \Rightarrow a \vee b = b$

Given $\quad a \le b$

Also $\quad b \le b$ (reflexive)

Therefore $a \vee b \le b$ (definition).........(1)

But $\quad b \le a \vee b$ ....(2)

Because $a \vee b$ is LUB of (a,b)

Combining (1) & (2), we have $a \vee b = b$

$(ii)\quad a \vee b = b \Rightarrow a \wedge b = a$

Given $a \vee b = b$

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

$= a$ (absorption)

$(iii)\quad a \wedge b = a \Rightarrow a \le b$

Given $a \wedge b = a$

Therefore a is the greatest lower bound of a and b.

In particular $a \le b$.

Theorem: In a lattice $(L,\le)$, then for any $a,b,c \in L$, prove that $a \wedge (b \vee c) \ge (a \wedge b) \vee (a \wedge c)$

We know that $a \wedge b \le a$

Also $a \wedge b \le b \le b \vee c$

Therefore $a \wedge b$ is the lower bound of $\{a,\ b \vee c\}$. i.e. $a \wedge b \le a \wedge (b \vee c)$....(1)

Similarly $a \wedge c \le a$

Also $a \wedge c \le c \le b \vee c$

Therefore $a \wedge c$ is the lower bound of $\{a,\ b \vee c\}$. i.e. $a \wedge c \le a \wedge (b \vee c)$....(2)

Equations (1) and (2) shows that $a \wedge (b \vee c)$ is the upper bound of $\{a \wedge b, a \wedge c\}$

$$\text{i.e. } (a \wedge b) \vee (a \wedge c) \le a \wedge (b \vee c)$$

$$\text{i.e. } a \wedge (b \vee c) \ge (a \wedge b) \vee (a \wedge c)$$

Theorem: In a lattice $(L,\le)$, prove that $a \vee (b \wedge c) \le (a \vee b) \wedge (a \vee c)$

We know that $a \le a \vee b$

Also $b \wedge c \le b \le a \vee b$

Therefore $a \vee b$ is the upper bound of $\{a,\ b \wedge c\}$. i.e. $a \vee (b \wedge c) \le a \vee b$....(1)

Similarly $a \le a \vee c$

Also $b \wedge c \le c \le a \vee c$

Therefore $a \vee c$ is the upper bound of $\{a,\ b \wedge c\}$. i.e. $a \vee (b \wedge c) \le a \vee c$....(2)

Equations (1) and (2) shows that $a \vee (b \wedge c)$ is the lower bound of $\{a \vee b,\ a \vee c\}$

$$\text{i.e. } a \vee (b \wedge c) \le (a \vee b) \wedge (a \vee c)$$

Another Method:

We know that $a \le a \vee b$ and $a \le a \vee c$

i.e. a is the lower bound of $a \vee b$ and $a \vee c$

Therefore $a \le (a \vee b) \wedge (a \vee c)$ ....(1)

Also we know that $b \wedge c \le b \le a \vee b$ and $b \wedge c \le c \le a \vee c$

i.e. $b \wedge c$ is the lower bound of $a \vee b$ and $a \vee c$

Therefore $b \wedge c \le (a \vee b) \wedge (a \vee c)$ .....(2)

From (1) & (2), $(a \vee b) \wedge (a \vee c)$ is the upper bound of $\{a, \ b \wedge c\}$

i.e. $a \vee (b \wedge c) \le (a \vee b) \wedge (a \vee c)$

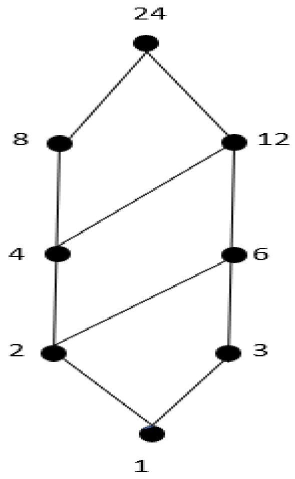
Special Lattices

Definition: A non empty subset M of a lattice $(L, \ \wedge, \ \vee)$ is called a **sublattice** of L, if M is closed under both the operations $\wedge, \vee$. i.e. if $a, b \in M$ then $a \wedge b \in M$, $a \vee b \in M$.

Example: $(Z^+, |)$ is a lattice. Then $(D_n, |)$ is a sublattice where $D_n \subset Z^+$, n is a positive integer.

Example: If S_n is the set of all divisors of the positive integers n and aDb if and only if a divides b, prove that $\{S_{24}, D\}$ is a lattice. Find also all the sublattices of D_{24} that contain 5 or more elements.

Here $S_4 = D_{24} = \{1, 2, 3, 4, 6, 12, 24\}$ and the Hasse Diagram is given here.



Consider the poset $\{D_{24}, |\}$. Clearly it is reflexive, anti-symmetric and transitive and hence it is a poset.

To prove $\{D_{24}, |\}$ is a lattice. i.e. to prove any pair $(x, y) \in D_{24}$ has LUB and GLB.

For $x, y \in S_{42}$, we define $x * y =$ GLB = gcd (x,y) and

$x \oplus y =$ LUB = lcm(x,y)

Hence for any pair, GLB and LUB exists. Therefore $\{D_{24}, |\}$ is a lattice.

The sublattices of D_{24} that contain 5 or more elements are {1, 2, 3, 6, 12}, {1, 2, 4, 6, 12}, {1, 2, 4, 8, 24}, {1, 2, 3, 6, 12, 24}, {1, 2, 4, 6, 12, 24}, {1, 2, 3, 4, 6, 12} and {2, 4, 6, 8, 12, 24}.

Definition: A lattice $(L, \ \wedge, \ \vee)$ is said to have a lower bound, denoted by 0, if $0 \le a$ for all $a \in L$. Similarly, a lattice $(L, \ \wedge, \ \vee)$ is said to have a upper bound, denoted by 1, if $a \le 1$ for all $a \in L$. A lattice is said to be **bounded** if it has both a lower bound and upper bound.

Note: $a \vee 0 = a$, $a \vee 1 = 1$, $a \wedge 0 = 0$, $a \wedge 1 = a$

https://doi.org/10.5281/zenodo.15287996

Example:
The lattice $P(S)$ of all subsets of S is a bounded lattice with ϕ as a lower bound and S as an upper bound.

The set of non negative integers with usual ordering $0 < 1 < 2 < \cdots$ has a lower bound 0 but there is no upper bound. Hence it is not bounded.

Example: Every finite lattice is bounded

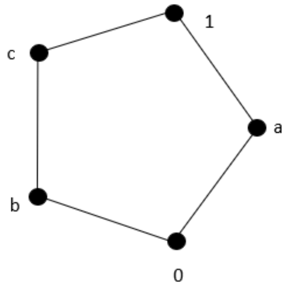
Let $L = \{a_1, a_2, ...a_n\}$ is a finite lattice. Then $a_1 \wedge a_2 \wedge .....\wedge a_n$ and $a_1 \vee a_2 \vee .....\vee a_n$ are the lower and upper bounds of L respectively. Hence it is bounded.

Definition: If $(L, \wedge, \vee, 0, 1)$ is a bounded lattice and $a \in L$. An element $b \in L$ is called **complement** of a, if $a \vee b = 1,\ a \wedge b = 0.$

Note: Lower and upper bounds are complements to each other.
An element $a \in L$ may have more than one complement
An element $a \in L$ may or may not have complement
A lattice is called complemented lattice, if every element of L has at least one complement.

Here $a \vee b = 1,\ a \wedge b = 0.$
Also $a \vee c = 1,\ a \wedge c = 0.$

Therefore the complement of a is b and c.



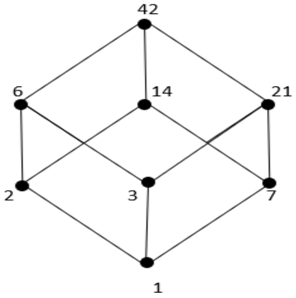
Example: Show that the lattice $P(S)$, where $P(S)$ is the power set of a finite set S is complemented.

We know that the complement of any subset A of S is given by $\bar{A} = S - A$.

Now $A \vee (S - A) = 1$ and $A \wedge (S - A) = 0$. Because
$A \cup (S - A) = S$ and $A \cap (S - A) = \phi$

Example: If S_{42} is the set of all divisors of 42 and D is the relation "divisor of" on S_{42}, prove that $\{S_{42}, D\}$ is a complemented lattice.

Given $S_{42} = \{1, 2, 3, 6, 7, 14, 21, 42\}$. For $x, y \in S_{42}$,
we define $x * y = \text{GLB} = \gcd(x, y)$ and $x \oplus y = \text{LUB} = \text{lcm}(x, y)$



The zero element of the lattice is 1 and the unit element of the lattice is 42.

Therefore if y is a complement of x, then $x * y = 1$ and $x \oplus y = 42$.

https://doi.org/10.5281/zenodo.15287996

Consider the elements 1, 42 in S_{42}

$1 * 42 = \gcd\,(x,y) = 1$

$1 \oplus 42 = \text{lcm}\,(x,y) = 42$

Therefore the complement of 1 is 42.

Similarly the complement of 42 is 1.

Consider the elements 3, 14 in S_{42}

$3 * 14 = \gcd\,(x,y) = 1$

$3 \oplus 14 = \text{lcm}\,(x,y) = 42$

Therefore the complement of 3 is 14.

Similarly the complement of 14 is 21.

Consider the elements 2, 21 in S_{42}

$2 * 21 = \gcd\,(x,y) = 1$

$2 \oplus 21 = \text{lcm}\,(x,y) = 42$

Therefore the complement of 2 is 21.

Similarly the complement of 21 is 2.

Consider the elements 6, 7 in S_{42}

$6 * 7 = \gcd\,(x,y) = 1$

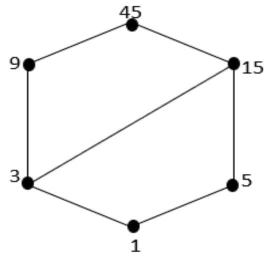
$6 \oplus 7 = \text{lcm}\,(x,y) = 42$

Therefore the complement of 6 is 7.

Similarly the complement of 7 is 6.

Since every element of S_{42} has a complements, it is a complemented lattice.

Example: If D_{45} denotes the set of all divisors of 45 under divisibility ordering, find which elements have complements and which do not have complements.



Given $D_{45} = \{1, 3, 5, 9, 15, 45\}$.

For $x, y \in D_{45}$, we define $x * y = GLB = \gcd\,(x,y)$ and $x \oplus y = LUB =$ lcm (x,y)

Also we know that if y is a complement of x,

then $x * y = 1$, the least element and $x \oplus y = 45$, the greatest element of D_{45} .

.

Consider the elements 1, 45 in D_{45}

$1 * 45 = \gcd\,(x,y) = 1$

$1 \oplus 45 = \text{lcm}\,(x,y) = 45$

Therefore the complement of 1 is 45.

Similarly the complement of 45 is 1.

Consider the elements 5, 9 in D_{45}

$5 * 9 = \gcd\,(x,y) = 1$

$5 \oplus 9 = \text{lcm}\,(x,y) = 45$

Therefore the complement of 5 is 9.

Similarly the complement of 9 is 5.

Consider the elements 3, 15 in D_{45}

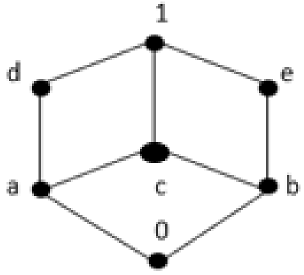
$3 * 15 = \gcd\,(x,y) = 3 \neq 1$

$3 \oplus 15 = \text{lcm}\,(x,y) = 15 \neq 45$

Therefore 3 and 15 have no complements

Example : Find the complements, if they exist, of the elements of the a,b,c of the lattice, whose Hasse diagram is given below. Can the lattice be complemented?

If y is a complement of x, then $x \wedge y = 0$ and $x \vee y = 1$.



Clearly 0 and 1 are complements to each other.

Let $x = a$. Then $a \wedge y = 0$ and $a \vee y = 1$.

i.e. $a \wedge b = 0$ and $a \vee b = 1$.

Therefore a and b are complements to each other.

Let $x = d$. Then $d \wedge y = 0$ and $d \vee y = 1$.

i.e. $d \wedge e = 0$ and $d \vee e = 1$.
Therefore d and e are complements to each other.

Let $x = c$. Then there exists no y such that $c \wedge y = 0$ and $c \vee y = 1$.

Because $c \vee a = c, c \vee b = c, c \vee d = 1, c \vee e = 1$ and $c \wedge a = a, c \wedge b = b, c \wedge d = a, c \wedge e = b$

Therefore c has no complement and hence the lattice is not complemented.

Note: Here a and e are complements to each other. Also b and d are complements to each other

Theorem: Show that a chain with three or more elements is not complemented.

Let $(L,\leq)$ be a chain with 3 or more elements. Let $0, x, 1$ be any three elements in the chain with least element 0 and greatest element 1.

Since L is a chain, it is totally ordered lattice. Therefore any two elements are comparable with least and greatest element. i.e. $0 \leq x \leq 1$.

Now $0 \wedge x = 0$ and $0 \vee x = x$. Also $1 \wedge x = x$ and $1 \vee x = 1$.
This shows that x has no complement and hence L is not complemented.

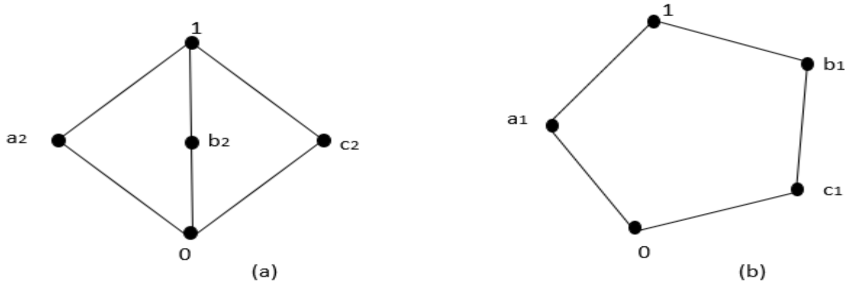
Definition: A lattice $(L, \wedge, \vee)$ is said to **distributive,** if for all $a, b, c \in L$. Then

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

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

https://doi.org/10.5281/zenodo.15287996

Example: Verify whether the lattices given by the Hasse diagrams in following are distributive.



(a) (b)

Consider the lattice L given in (a)

Let $a_2, b_2, c_2 \in L$

$$a_2 \wedge (b_2 \vee c_2) = (a_2 \wedge b_2) \vee (a_2 \wedge c_2)$$
$$a_2 \wedge 1 = 0 \vee 0$$
$$a_2 = 0$$
$$a_2 \vee (b_2 \wedge c_2) = (a_2 \vee b_2) \wedge (a_2 \vee c_2)$$
$$a_2 \vee 0 = 1 \wedge 1$$
$$a_2 = 1$$

Since distributive laws are not valid, it is not distributive lattice

Consider the lattice L given in (b)

Let $a_1, b_1, c_1 \in L$

$$a_1 \wedge (b_1 \vee c_1) = (a_1 \wedge b_1) \vee (a_1 \wedge c_1)$$
$$a_1 \wedge b_1 = 0 \vee 0$$
$$0 = 0$$
$$a_1 \vee (b_1 \wedge c_1) = (a_1 \vee b_1) \wedge (a_1 \vee c_1)$$
$$a_1 \vee c_1 = 1 \wedge 1$$
$$1 = 1$$

Here distributive laws are valid.

But Consider

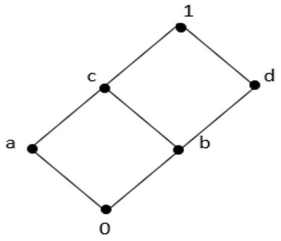
$$b_1 \wedge (a_1 \vee c_1) = (b_1 \wedge a_1) \vee (b_1 \wedge c_1)$$
$$b_1 \wedge 1 = 0 \vee c_1$$
$$b_1 \neq c_1$$

Hence it is not distributive lattice.

Example: Give an example of a distributive lattice but not complemented.

No complement exists for $0, b, c, d, 1$.

But it is distributive.



Theorem: Every chain is a distributive lattice.

Let $(L, \leq)$ be a chain, then every elements are comparable. Let $a, b, c \in L$. Then $a \leq b$ *and* $a \leq c$ or $b \leq a$ *and* $c \leq a$

Case(1) $a \leq b$ *and* $a \leq c$

Therefore we have $a \wedge b = a$

$$a \wedge c = a$$

Case(2) $b \leq a$ *and* $c \leq a$

Therefore we have $a \wedge b = b$

$$a \wedge c = c$$

https://doi.org/10.5281/zenodo.15287996

$$a \le b \vee c$$

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

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

Equating LHS, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

$$b \vee c \le a$$

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

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

Equating LHS, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

Therefore the chain $(L, \le)$ is a distributive lattice.

Theorem: Show that cancellation laws are valid in a distributive lattice.

Let $(L, \ \wedge, \ \vee)$ be a distributive lattice and $a, b, c \in L.$

We have to show that if $a \vee b = a \vee c$ and $a \wedge b = a \wedge c$ then $b = c$.

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

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

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

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

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

$$c = b$$

Theorem: In a distributive lattice prove that $a * b = a * c$ and $a \oplus b = a \oplus c$ imply $b = c$.

Let $(L, \le)$ be a distributive lattice. Given that

$a * b = a * c$ and $a \oplus b = a \oplus c$

Let $b = b * (a \oplus b)$ (Absorption law)

$= b * (a \oplus c)$ (Given)

$= (b * a) \oplus (b * c)$ (Distributive)

$= (a * b) \oplus (b * c)$ (Commutative)

$= (a * c) \oplus (b * c)$ (Given)

$= (c * a) \oplus (c * b)$ (Commutative)

$= c * (a \oplus c)$ (Distributive)

$= c$ (Absorption)

Theorem: In a distributive and complemented lattice, prove that complement of each element is unique

Let $(L, \ \wedge, \ \vee)$ be a distributive, complemented lattice. Suppose a and b are two complements to $x \in L$.

Then by definition, $x \vee a = 1$, $x \wedge a = 0$ and $x \vee b = 1$ *and* $x \wedge b = 0$.

Now $a = a \vee 0$

$= a \vee (x \wedge b)$ {by assumption}

$= (a \vee x) \wedge (a \vee b)$ {distributive}

$= 1 \wedge (a \vee b)$ {by assumption}

$= (a \vee b)$

Similarly $b = b \vee 0$

$= b \vee (x \wedge a)$ {by assumption}

$= (b \vee x) \wedge (b \vee a)$ {distributive}

$= 1 \wedge (b \vee a)$ {by assumption}

$= (b \vee a)$

Since $(b \vee a) = (a \vee b)$, we get $a = b$

Example: In a distributive complemented lattice, show that the following are equivalent.

$(1)\ a \le b \quad (2)\ a \wedge \bar{b} = 0 \quad (3)\ \bar{a} \vee b = 1 \quad (4)\ \bar{b} \le \bar{a}$

Let $(L, \ \wedge, \ \vee)$ be a distributive, complemented lattice. i.e. the lattice is distributive and each element has at least a complement.

To Prove $(1) \Rightarrow (2)$

Let $a, b \in L$. Given $a \le b$.

Then $a \vee b = b$ *and* $a \wedge b = a$

$$a \vee b = b$$
$$(a \vee b) \wedge \bar{b} = b \wedge \bar{b}$$
$$(a \wedge \bar{b}) \vee (b \wedge \bar{b}) = b \wedge \bar{b}$$
$$(a \wedge \bar{b}) \vee 0 = 0$$
$$(a \wedge \bar{b}) = 0$$

To Prove $(2) \Rightarrow (3)$

Let $a, b \in L$. Given $(a \wedge \bar{b}) = 0$.

Taking complement on both sides, we have

$$\overline{(a \wedge \bar{b})} = \bar{0}$$
$$\bar{a} \vee \bar{\bar{b}} = 1$$
$$\bar{a} \vee b = 1$$

To Prove $(3) \Rightarrow (4)$

Let $a, b \in L$. Given $\bar{a} \vee b = 1$.

$$(\bar{a} \vee b) \wedge \bar{b} = 1 \wedge \bar{b} \ \{\text{cancellation law}\}$$
$$(\bar{a} \wedge \bar{b}) \vee (b \wedge \bar{b}) = \bar{b}$$
$$(\bar{a} \wedge \bar{b}) \vee 0 = \bar{b}$$
$$(\bar{a} \wedge \bar{b}) = \bar{b}$$
$$\bar{b} \le \bar{a}$$

To Prove $(4) \Rightarrow (1)$

Let $a, b \in L$. Given $\bar{b} \le \bar{a}$.

Therefore $(\bar{a} \wedge \bar{b}) = \bar{b}$

$$\overline{(\bar{a} \wedge \bar{b})} = \bar{\bar{b}}$$
$$\bar{\bar{a}} \vee \bar{\bar{b}} = b$$
$$a \vee b = b$$
$$a \le b$$

Theorem: Establish De Morgan's laws in a complemented, distributive lattice.

We know that if x' is the complement of x, then $x \vee x' = 1$ and $x \wedge x' = 0$.

To prove $a' \wedge b'$ is the complement of $a \vee b$, we have to prove $(a \vee b) \vee (a' \wedge b') = 1$ and $(a \vee b) \wedge (a' \wedge b') = 0$.

Law (i) $(a \vee b)' = a' \wedge b'$

Consider $(a \vee b) \vee (a' \wedge b') = [(a \vee b) \vee a'] \wedge [(a \vee b) \vee b']$

$$= [(a \vee a') \vee b] \wedge [(b \vee b') \vee a]$$
$$= [1 \vee b] \wedge [1 \vee a]$$
$$= 1 \wedge 1$$
$$= 1$$

Consider $(a \vee b) \wedge (a' \wedge b') = [a \wedge (a' \wedge b')] \vee [b \wedge (a' \wedge b')]$

$$= [(a \wedge a') \wedge b'] \vee [(b \wedge b') \wedge a']$$

$$= [0 \wedge b'] \vee [0 \wedge a']$$

$$= 0 \vee 0$$

$$= 0$$

This shows that $a' \wedge b'$ is the complement of $a \vee b$. Hence $(a \vee b)' = a' \wedge b'$

Law (ii) $(a \wedge b)' = a' \vee b'$

To prove $a' \vee b'$ is the complement of $a \wedge b$, we have to prove $(a \wedge b) \vee (a' \vee b') = 1$ and $(a \wedge b) \wedge (a' \vee b') = 0$.

Consider $(a \wedge b) \vee (a' \vee b') = [a \vee (a' \vee b')] \wedge [b \vee (a' \vee b')]$

$$= [(a \vee a') \vee b'] \wedge [(b \vee b') \vee a']$$

$$= [1 \vee b'] \wedge [1 \vee a']$$

$$= 1 \wedge 1$$

$$= 1$$

Consider $(a \wedge b) \wedge (a' \vee b') = [(a \wedge b) \wedge a'] \vee [(a \wedge b) \wedge b']$

$$= [(a \wedge a') \wedge b] \vee [(b \wedge b') \wedge a]$$

$$= [0 \wedge b] \vee [0 \wedge a]$$

$$= 0 \vee 0$$

$$= 0$$

This shows that $a' \vee b'$ is the complement of $a \wedge b$. Hence $(a \wedge b)' = a' \vee b'$

Definition: Let $(L, *, \oplus)$, $(S, \wedge, \vee)$ be two lattices. Then the direct product of L and S is $L \times S$ and the operations are defined by

$$(a_1, b_1) \bullet (a_2, b_2) = (a_1 * a_2, b_1 \wedge b_2)$$
$$(a_1, b_1) + (a_2, b_2) = (a_1 \oplus a_2, b_1 \vee b_2)$$

The operations $+$ and $\bullet$ are idempotent, commutative, associative and satisfy the absorption law because they are defined in terms of the operations $*, \oplus$ and $\wedge, \vee$. Therefore is $(L \times S, \ \bullet, \ +)$ a lattice.

Theorem: The direct product of any two distributive lattices is a distributive lattice.

Let $(L, *, \oplus)$, $(S, \wedge, \vee)$ be distributive lattices. Then

$$a * (b \oplus c) = (a * b) \oplus (a * c)$$

https://doi.org/10.5281/zenodo.15287996

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

Let $(a_1,\ b_1),(a_2,\ b_2),(a_3,\ b_3)\in L\times S$

Now $(a_1,b_1)\bullet[(a_2,b_2)+(a_3,b_3)]=(a_1,b_1)\bullet(a_2\oplus a_3,b_2\vee b_3)$

$$=(a_1*(a_2\oplus a_3),b_1\wedge(\ b_2\vee b_3))$$
$$=((a_1*a_2)\oplus(a_1*a_3),(b_1\wedge b_2)\vee(\ b_1\wedge b_3))$$
$$=(a_1*a_2,b_1\wedge b_2)+(a_1*a_3,b_1\wedge b_3)$$
$$=[(a_1,b_1)\bullet(a_2,b_2)]+[(a_1,b_1)\bullet(a_3,b_3)]$$

Also $(a_1,b_1)+[(a_2,b_2)\bullet(a_3,b_3)]=(a_1,b_1)+(a_2*a_3,b_2\wedge b_3)$

$$=(a_1\oplus(a_2*a_3),b_1\vee(b_2\wedge b_3))$$
$$=((a_1\oplus a_2)*(a_1\oplus a_3),(b_1\vee b_2)\wedge(b_1\vee b_3))$$
$$=(a_1\oplus a_2,b_1\vee b_2)\bullet(a_1\oplus a_3,b_1\vee b_3)$$
$$=[(a_1,b_1)+(a_2,b_2)]\bullet[(a_1,b_1)+(a_3,b_3)]$$

Therefore $(L\times S,\ \bullet,\ +\ )$ is a distributive lattice.

Definition: Let $(L,\ \wedge,\ \vee)$ and $(M,\ \cap,\ \cup)$ are two lattices. A mapping $f:L\to M$ is called a lattice homomorphism, if for any $a,b\in L$,

$$f(a\wedge b)=f(a)\cap f(b)$$
$$f(a\vee b)=f(a)\cup f(b)$$

Note: A one-to-one homomorphism is said to be isomorphism.

Example: Show that the lattice $(L,|)$ where $L=\{1,2,3,6\}$ and the lattice $(M(S),\le)$ where $M=\{a_1,a_2\}$ are isomorphic.

Here $M(S)=\phi,\{a_1\},\{a_2\},\{a_1,a_2\}$

Define a mapping $f:L\to M(S)$ such that $f(1)=\phi,\ f(2)=\{a_1\},\ f(3)=\{a_2\},\ f(6)=\{a_1,a_2\}$

Then obviously f is one-to-one and onto.

Here f is a homomorphism. Because

$$f(1\wedge 2)=f(1)\wedge f(2) \qquad f(1\vee 2)=f(1)\vee f(2)$$
$$f(1)=\phi\wedge f(2) \qquad f(2)=\phi\vee f(2)$$
$$\phi=\phi\wedge\{a_1\} \qquad \{a_1\}=\phi\vee\{a_1\}$$
$$\phi=\phi \qquad \{a_1\}=\{a_1\}$$

https://doi.org/10.5281/zenodo.15287996

Hence f is an isomorphism.

Modular Inequality: If $(L, \leq)$ is a lattice, then for any $a, b, c \in L,\ a \leq c$ then $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

Since $a \leq c,\ a \vee c = c$

By distributive property, $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$

$$a \vee (b \wedge c) \leq (a \vee b) \wedge c \text{ .....(1)}$$

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

$$a \leq c \text{ .....(2)}$$

From (1) and (2), $a \leq c \Leftrightarrow a \vee (b \wedge c) \leq (a \vee b) \wedge c$

Definition: A lattice L is said to be **modular** if $a \leq c$ then $a \vee (b \wedge c) = (a \vee b) \wedge c$ for all $a, b, c \in L,$.

Theorem: Every distributive lattice is modular but not conversely.

Let $(L, \leq)$ be a distributive lattice, then for any $a, b, c \in L,\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

If $a \leq c$ *then* $a \vee c = c$.

Therefore $a \vee (b \wedge c) = (a \vee b) \wedge c$. Hence $(L, \leq)$ is modular.

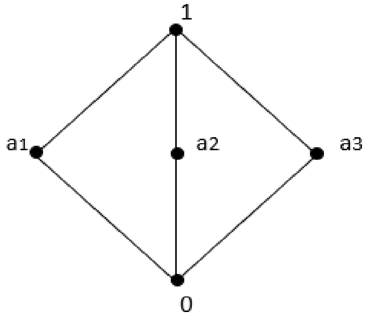
Consider the Diamond lattice M_5 which is modular.

Distributive Law : $a_1 \vee (a_2 \wedge a_3) = (a_1 \vee a_2) \wedge (a_1 \vee a_3)$

From the diagram $a_1 \vee (a_2 \wedge a_3) = (a_1 \vee 0) = a_1$

$$(a_1 \vee a_2) \wedge (a_1 \vee a_3) = 1 \wedge 1 = 1$$

Since $a_1 \vee (a_2 \wedge a_3) \neq (a_1 \vee a_2) \wedge (a_1 \vee a_3)$, the lattice is not distributive.



Hasse diagram of M_5

To prove diamond lattice M5 is Modular.

For any $a,b,c \in L, a \leq c$ then $a \vee (b \wedge c) = (a \vee b) \wedge c$

Suppose $a = c$.

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

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

$$c = c$$

Hence the result is true.

Suppose $a < c$. Since the diamond lattice is symmetric with respect to a_1, a_2, a_3 it is enough to prove the result with respect to one of them, say a_1.

https://doi.org/10.5281/zenodo.15287996

The condition $a < c$ for a_1 will be $a_1 < 1$ and $0 < a_1$.

Let $a_1 < 1$.

Then $a = a_1, c = 1$.

Therefore the condition becomes

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

$a_1 \vee (b \wedge 1) = (a_1 \vee b) \wedge 1$

$a_1 \vee b = a_1 \vee b$

Hence the result is true

Let $0 < a_1$.

Then $a = 0, c = a_1$.

Therefore the condition becomes

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

$0 \vee (b \wedge a_1) = (0 \vee b) \wedge a_1$

$b \wedge a_1 = b \wedge a_1$

Hence the result is true

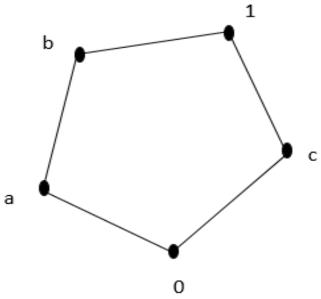
Therefore the lattice is modular

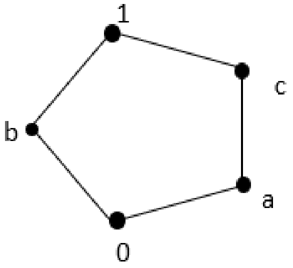
Example: Prove that the lattice whose Hasse diagram is not modular

For this lattice, when $a \le c,\ a \vee (b \wedge c) \ne (a \vee b) \wedge c$.

Because $a \vee (b \wedge c) = a \vee (0) = a$

and $(a \vee b) \wedge c = (1) \wedge c = c$





Note: If a lattice is not modular, it is not distributive.
A modular lattice need not be distributive.
Every chain is a modular lattice, because we cannot find $a, b, c \in L$ such that $a \le c$ and b is not comparable with a or c.

Boolean Algebra

A lattice which is distributive and complemented is called a Boolean Algebra. In Boolean Algebra, it is customary to use the symbol $+$ *and* $\bullet$ instead of $\vee$ *and* $\wedge$. It is denoted as $\{B, +, \square, ', 0, 1\}$.

If $\{B, +, \square, ', 0, 1\}$ is a Boolean Algebra, then the following properties are hold for $a, b, c \in B$.

Identity Laws: $a + 0 = a$ and $a \square 1 = a$

Commutative Laws: $a + b = b + a$ and $a \square b = b \square a$

Associative Laws: $(a + b) + c = a + (b + c)$ and $(a \square b) \square c = a \square (b \square c)$

Distributive Laws: $a \square (b + c) = (a \square b) + (a \square c)$ and $a + (b \square c) = (a + b) \square (a + c)$

Complement Laws: $a \cdot a' = 0$ and $a + a' = 1$

Note: Here 0 and 1 are symbolic form of lower and upper bounds
If a variable x takes on only the values , it is called Boolean variable
Sometimes $a \cdot b$ may be written as ab
The distributive law $a + (b \cdot c) = (a+b) \cdot (a+c)$ does not hold good in ordinary algebra

Example: If $B = \{0, 1\}$ and the operations $+$, $\bullet$, $'$ are defined as follows:

Identity Laws: $0+0=0,\ 1+0=1$ and $0 \cdot 1 = 0,\ 1 \cdot 1 = 1$

Commutative Laws: $1+1=1+1=1,\ 1+0=0+1=1$ and $0 \cdot 0 = 0 \cdot 0 = 0,\ 0 \cdot 1 = 1 \cdot 0 = 0$

Associative Laws: $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

Distributive Laws: Obvious

Complement Laws: $1' = 0$ and $0' = 1$

Therefore $B = \{0, 1\}$ is the (only) two element Boolean Algebra.

Note: This is the only Boolean Algebra whose Hasse diagram is a chain.

Example: If $P(S)$ is the power set of a set S, then $\{P(S), \cup, \cap, \square\}$ is a Boolean Algebra with $0 = \phi, 1 = S$.

Let A, B and C be any three elements of $P(S)$. Now $A \cup \phi = A$ and $A \cap S = A$.
Hence the zero element is ϕ and unit element is S and identity laws are satisfied……….(1)

Since $A \cup B = B \cup A$ and $A \cap B = B \cap A$, the commutative laws are satisfied…..(2)

Since $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$, associative laws are satisfied……..(3)

Since $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, distributive laws are satisfied……….(4)

Let the complement of any set $A \subseteq S$ is considered as $S \setminus A$ or $S - A$, the relative complement of A with respect to S.

Therefore $A \cup (S - A) = S$ and $A \cap (S - A) = \phi$, the complement laws are satisfied.

Theorem: In a Boolean Algebra, prove that the complement of every element is unique.

Let $\{B, +, \cdot, ', 0, 1\}$ be a Boolean Algebra. Suppose $a \in B$ has two complements b and $c \in B$.
Then by definition

$a \cdot b = 0$ and $a + b = 1$
$a \cdot c = 0$ and $a + c = 1$

Consider $b = b \cdot 1$
$= b \cdot (a + c)$
$= (b \cdot a) + (b \cdot c)$
$= 0 + (b \cdot c)$
$= (b \cdot c)$

Similarly $c = c \cdot 1$
$= c \cdot (a + b)$
$= (c \cdot a) + (c \cdot b)$
$= 0 + (c \cdot b)$
$= (c \cdot b)$

Hence, from the above $b = c$

Example: Show that D_n is a Boolean Algebra if n is a square free, i.e. n is a product of distinct primes.

Here D_n is a set of divisors of the number n and let the relation be |, divides.

Clearly, the relation is reflexive, antisymmetric and transitive and hence a partial order relation on D_n.

Therefore $(D_n, |)$ is a poset.

Let $x \in D_n$ and let $x' = \frac{m}{x}$. Since m is a product of distinct primes, x and x' have different prime divisors. Hence $x \cdot x' = \gcd(x, x') = 1$ and $x + x' = lcm(x, x') = n$. Therefore complement exists.
Also LUB and GLB exists. Hence $(D_n, |)$ is a complemented distributive lattice.
Therefore D_n is a Boolean algebra.

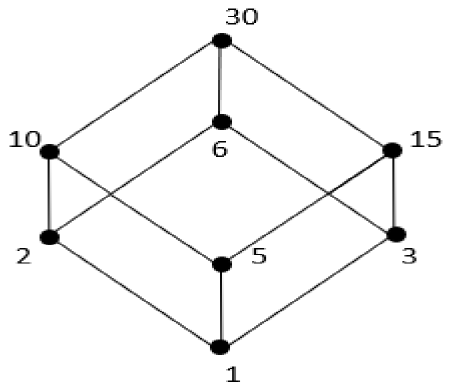
Note: The atoms of D_n are the prime divisors of n.

Example: Show that the lattice of positive divisors of 30 is a Boolean Algebra.

Let $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and let the relation be |, divides.

Clearly, the relation is reflexive, antisymmetric and transitive and hence a partial order relation on D_{30}.

Therefore $(D_{30}, |)$ is a poset.
Define $a \cdot b = \gcd(a, b)$ and $a + b = lcm(a, b)$ for all $a, b \in D_{30}$.
Since GLB and LUB exists, $(D_{30}, |)$ is a lattice.
From the Hasse diagram, it is distributive lattice.



https://doi.org/10.5281/zenodo.15287996

Here 1 is the least element and 30 is the greatest element.

Here $2\cdot 15 = \gcd(2,15) = 1$ and $2+15 = lcm(2,15) = 30$. Hence 2 and 15 are complements to each other. Similarly 3, 10 are complements to each other and 5, 6 are complements to each other.

Therefore $(D_{30}, |)$ is complemented distributive lattice i.e. Boolean Algebra.

Example: Is a lattice of divisors of 32 a Boolean Algebra?

The divisors of 32 is a chain. We know that a chain with three or more elements is not complemented. Therefore the lattice is not complemented and hence not Boolean Algebra.

Some Boolean Identities

Idempotent Laws: $x+x=x, \quad x\cdot x = x$

$$\begin{aligned}
x &= x+0 && \{\text{Identity}\}\\
x &= x+x.\bar{x} && \{\text{Complement}\}\\
x &= (x+x).(x+\bar{x}) && \{\text{Distributive}\}\\
x &= (x+x).1 && \{\text{Complement}\}\\
x &= (x+x) && \{\text{Identity}\}
\end{aligned}$$

$$\begin{aligned}
x &= x\cdot 1 && \{\text{Identity}\}\\
x &= x\cdot(x+\bar{x}) && \{\text{Complement}\}\\
x &= (x\cdot x)+(x\cdot\bar{x}) && \{\text{Distributive}\}\\
x &= (x\cdot x)+0 && \{\text{Complement}\}\\
x &= (x\cdot x) && \{\text{Identity}\}
\end{aligned}$$

Dominant Laws: $x+1=1, \quad x\cdot 0 = 0$

$$\begin{aligned}
x+1 &= (x+1)\cdot 1 && \{\text{Identity}\}\\
&= (x+1)\cdot(x+\bar{x}) && \{\text{Complement}\}\\
&= x+(1\cdot\bar{x}) && \{\text{Distributive}\}\\
&= x+\bar{x} && \{\text{Identity}\}\\
&= 1 && \{\text{Complement}\}
\end{aligned}$$

$$\begin{aligned}
x\cdot 0 &= (x\cdot 0)+0 && \{\text{Identity}\}\\
&= (x\cdot 0)+(x\cdot\bar{x}) && \{\text{Complement}\}\\
&= x\cdot(0+\bar{x}) && \{\text{Distributive}\}\\
&= x\cdot\bar{x} && \{\text{Identity}\}\\
&= 0 && \{\text{Complement}\}
\end{aligned}$$

Absorption Laws: $x\cdot(x+y)=x, \quad x+(x\cdot y)=x$

$$\begin{aligned}
x\cdot(x+y) &= (x+0)\cdot(x+y)\\
&= x+(0\cdot y)\\
&= x+0\\
&= x
\end{aligned}$$

$$\begin{aligned}
x+(x\cdot y) &= (x\cdot 1)+(x\cdot y)\\
&= x\cdot(1+y)\\
&= x\cdot 1\\
&= x
\end{aligned}$$

De Morgan's Laws: $\overline{(x+y)} = \bar{x}\cdot\bar{y}, \quad \overline{x\cdot y} = \bar{x}+\bar{y}$

Proof: We know that if x' is the complement of x, then $x+x'=1$ and $x\bullet x'=0$.

To prove $a' \bullet b'$ is the complement of $a+b$, we have to prove $(a+b) \vee (a' \bullet b') = 1$ and $(a+b) \bullet (a' \bullet b') = 0$.

Law (i) $(a+b)' = a' \bullet b'$

Consider $(a+b)+(a' \bullet b') = [(a+b)+a'] \bullet [(a+b)+b']$

$$= [(a+a')+b] \bullet [(b+b')+a]$$

$$= [1+b] \bullet [1+a]$$

$$= 1 \bullet 1$$

$$= 1$$

Consider $(a+b) \bullet (a' \bullet b') = [a \bullet (a' \bullet b')] + [b \bullet (a' \bullet b')]$

$$= [(a \bullet a') \bullet b'] + [(b \bullet b') \bullet a']$$

$$= [0 \bullet b'] + [0 \bullet a']$$

$$= 0 + 0$$

$$= 0$$

This shows that $a' \bullet b'$ is the complement of $a+b$. Hence $(a+b)' = a' \bullet b'$

By duality, $(a \bullet b)' = a' + b'$ is true.

Definition: If A is a non empty sub set of a Boolean Algebra B such that A it self is a Boolean Algebra with respect to the operation of B, then A is called a **subalgebra** of B.

Note: if $m \mid n$, then D_m is a sublattice of D_n. This is true for subalgebra also.

Definition: A non least element a in a Boolean algebra is called an atom if for every $x \in B,\ x \wedge a = a \ or \ x \wedge a = 0$.

Note: (1) $x \wedge a = a \Rightarrow a \le x$. (2) $x \wedge a = 0 \Rightarrow$ a and x are not connected.

(3) Any element $x \neq 0$ of B can expressed uniquely as a sum of atoms.

Example: Consider the lattice D_{105} with the partial ordered relation divides, then

i. Draw the Hasse diagram of D_{105}

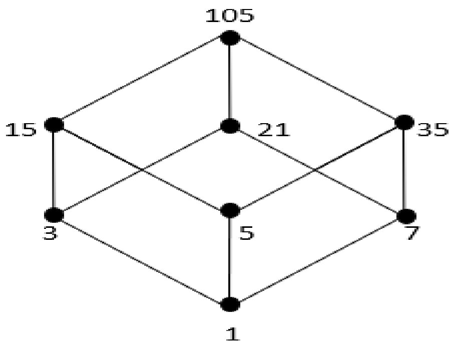
ii. Find the complement of each elements of D_{105}

iii. Find the set of atoms of D_{105}

iv. Find the number of sub algebras of D_{105}

The elements of $D_{105} = \{1, 3, 5, 7, 15, 21, 35, 105\}$

https://doi.org/10.5281/zenodo.15287996



Here $3 \wedge 35 = lcm(3,35) = 1$ and $3 \vee 35 = \gcd(3,35) = 105$. Hence Complement of 3 is 35
Similarly Complement of 5 is 21
Complement of 7 is 15 and Complement of 1 is 105

We know that a non least element a in a Boolean algebra is called an atom if for every $x \in B,\ x \wedge a = a \ or \ x \wedge a = 0$. Therefore set of atoms is { 3, 5, 7 }

To find sub algebras:

Here $O\left(D_{105}\right) = 8$. Therefore subalgebras must contain 2 or 4 or 8 elements.
D_{105} is a Boolean algebra with least element 1 and greatest element 105.
Therefore Sub algebra with 2 elements is { 1, 105 }
Also sub algebras with 8 elements is D_{105}

Subalgebra with 4 elements is of the form $\{1,\ x,\ x',\ 105\}$. Then may be either 3 or 5 or 7.

Sub algebras with 4 elements is {1, 3, 35, 105}, {1, 5, 21, 105}, {1, 7, 15, 105}
{number of subalgebras with 4 elements equals (number of non bound elements/2)}

Hence there are 5 sub algebras

Definition: Two Boolean algebras B_1 and B_2 are said to be isomorphic if there is a one-to-one correspondence $f : B_1 \to B_2$ if (i) $f\left(x+y\right) = f(x) + f(y)$ (ii) $f(xy) = f(x)\, f(y)$ (iii) $f\left(x'\right) = \left(f(x)\right)'$

Theorem: Let B be a finite Boolean Algebra and let A be the set of all atoms of B. Then prove that the Boolean Algebra B is isomorphic to the Boolean Algebra $P(A)$, where $P(A)$ is the power set of A.

Let B be a finite Boolean Algebra and let A be the set of all atoms of B.

$$A = \left\{a_1, a_2, ..., a_r, b_1, b_2, ..., b_s, c_1, c_2, ..., c_t, d_1, d_2, ..., d_k\right\}$$

Let $P(A)$ be the power set of A.
Define a mapping $f : B \to f(A)$ such that $f(x) = \left\{a_1, a_2, ..., a_r\right\}$ where $a_1 + a_2 + ... + a_r$ is the unique representation of sum of atoms.

By definition of atom, we have $a_i \square a_i = a_i$ and $a_i \square a_j = 0$.

Let $x, y \in B$ where $x = a_1 + a_2 + ... + a_r + b_1 + b_2 + ... + b_s$ and $y = b_1 + b_2 + ... + b_s + c_1 + c_2 + ... + c_t$

Then $x + y = a_1 + a_2 + ... + a_r + b_1 + b_2 + ... + b_s + c_1 + c_2 + ... + c_t$

$xy = b_1 + b_2 + ... + b_s$

Now $f(x+y) = \{a_1, a_2, ..., a_r, b_1, b_2, ..., b_s, c_1, c_2, ..., c_t\}$

$= \{a_1, a_2, ..., a_r, b_1, b_2, ..., b_s\} \cup \{b_1, b_2, ..., b_s, c_1, c_2, ..., c_t\}$

$= f(x) \cup f(y)$

Also $f(xy) = \{b_1, b_2, ..., b_s\}$

$= \{a_1, a_2, ..., a_r, b_1, b_2, ..., b_s\} \cap \{b_1, b_2, ..., b_s, c_1, c_2, ..., c_t\}$

$= f(x) \cap f(y)$

If $z = c_1 + c_2 + ... + c_t + d_1 + d_2 + ... + d_k$, then $x + y = 1$ and $xy = 0$. Hence z is the complement of x.

Also $f(x') = \{c_1, c_2, ..., c_t, d_1, d_2, ..., d_k\}$

$= \{a_1, a_2, ..., a_r, b_1, b_2, ..., b_s\}'$

$= (f(x))'$

Since this representation is unique, f is one-to-one and onto. Hence f is a Boolean algebra isomorphism.

Note: If a set A has n elements, then its power set $P(A)$ has 2^n elements. Thus a finite Boolean algebra has 2^n elements for some positive integer n.

Example: Is there a Boolean algebra with 5 elements?

No. Because each Boolean algebra is isomorphic to powerset algebra. Therefore it must have 2^n elements for some integer n and $5 \neq 2^n$.

Definition: A mapping $f : L \to S$ is said to be order preserving map from the Lattice $(L, *, \oplus, \leq)$ to the Lattice $(S, \wedge, \vee, \leq')$ if, $a \leq b \Rightarrow f(a) \leq' f(b), \forall a, b \in L.$

Theorem: Let $(L, *, \oplus)$ and $(S, \wedge, \vee)$ be any two lattices with the partial ordering $\leq$ and $\leq'$ respectively. If g is a lattice homomorphism, then g preserves the partial ordering. (or) Any Lattice homomorphism is order preserving. (or) Show that a lattice homomorphism on a Boolean Algebra which preserves 0 and 1 is a Boolean homomorphism.

Let $f : L \to S$ be a Lattice homomorphism. Let $a, b \in L$ such that $a \leq b$.

https://doi.org/10.5281/zenodo.15287996

Then $GLB\{a,b\} = a * b = a$ ……..(1)

Now $f(a*b) = f(a)$, using (1)

$f(a)* f(b) = f(a)$, since f is a homomorphism

i.e. greatest lower bound of $f(a)$ & $f(b)$ is $f(a)$.

i.e. $f(a)\wedge f(b) = f(a)$.

Therefore $f(a)\leq' f(b)$.

Therefore f is order preserving.

Then $LUB\{a,b\} = a \oplus b = b$ ……..(2)

Now $f(a\oplus b) = f(b)$, using (2)

$f(a)\oplus f(b) = f(b)$, since f is a homomorphism

i.e. least upper bound of $f(a)$ *and* $f(b)$ is $f(b)$.

i.e. $f(a)\vee f(b) = f(b)$.

Therefore $f(a)\leq' f(b)$.

Therefore f is order preserving.

Boolean Expression and Boolean Functions

A Boolean expression in n Boolean variables $x_1, x_2, \ldots, x_n$ is a finite string of symbols formed recursively. Example: (i) $f(x,y) = xy + x$ (ii) $f(x,y) = x + x\overline{y}$ (iii) $f(x,y,z) = xy + y + z$ (iv) $f(x,y,z) = xz + x$

A function $f : B^n = \{x_1, x_2, \ldots, x_n\} \to B\{0, 1\}$ is called a Boolean function of degree n. i.e. each Boolean expression represents a Boolean function, which is evaluated by substituting the values 0 or 1 for each variables. The values of the function may be obtained by the truth tables.

x	y	$x+y$	xy
1	1	1	1
1	0	1	0
0	1	1	0
0	0	0	0

Note: The number of different Boolean function $f : B^n \to B$ is 2^{2^n}.

Boolean product of all variables and its complements that appear exactly once is called minterm. Set of minterms in 2 variables: $ab,\ a'b,\ ab',\ a'b'$	Boolean sum of all variables and its complements that appear exactly once is called maxterm. Set of maxterms in 2 variables: $a+b,\ a'+b,\ a+b',\ a'+b'$
When a Boolean expression is expressed as a sum of minterms only is called disjunctive normal form(DNF). Example: $f(a,b,c) = abc + a'bc + a'b'c$	When a Boolean expression is expressed as a product of maxterms only is called conjunctive normal form(CNF). Example: $f(a,b,c) = (a+b+c)(a'+b+c)$

If a Boolean function is expressed by all its minterms, it is called complete DNF	If a Boolean function is expressed by all its maxterms, it is called complete CNF

Note: Boolean expression expressed in terms of CNF or DNF is called canonical form.
Canonical form is obtained by either truth table method or algebraic method.

Truth Table Method: Form the truth table for the given Boolean function $f(x, y, z)$, say.

To find the DNF: Note down the rows in which f column entry is 1. While writing the minterm corresponding to a row, entry 1 is replaced by the variable and entry 0 is replaced by the complement of the variables.

To find the CNF: Note down the rows in which f column entry is 0. While writing the maxterm corresponding to a row, entry 0 is replaced by the variable and entry 1 is replaced by the complement of the variables.

x	y	z	f
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	1

DNF : $xy\overline{z}+x\overline{y}z+\overline{x}y\overline{z}+\overline{x}\overline{y}\overline{z}$

CNF: $\left(\overline{x}+\overline{y}+\overline{z}\right)\left(\overline{x}+y+z\right)\left(x+\overline{y}+\overline{z}\right)\left(x+y+\overline{z}\right)$

Algebraic Method:

To find DNF: Express the function as a sum of product of variables. In a product, if a term, say a, is missing, multiply by $(a+\overline{a})$ which is equal to 1. Then apply distributive law, if necessary. Finally if a factor is repeated, it may be omitted because $a+a=a$.

To find CNF: Express the function as a product of sum of variables. In a sum, if a term, say a, is missing, add $(a\square\overline{a})$ which is equal to 0. Then apply distributive law, if necessary. Finally if a factor is repeated, it may be omitted because $a\square a=a$.

Example: What values of the Boolean variables x and y satisfy $xy=x+y$?

Let us find the values of the Boolean function from the following table with the use of Boolean sum and Boolean product.

x	y	xy	$x+y$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

https://doi.org/10.5281/zenodo.15287996

Compare the columns of xy and $x+y$. The values in the respective columns are equal when $x=1,\ y=1$ or $x=0,\ y=0$.
Therefore we get $xy=x+y$ if and only if $x=1,\ y=1$ or $x=0,\ y=0$.

Example: Verify De Morgan's Law with the use of Boolean sum and product.

To verify: (1) $\overline{(x+y)}=\bar{x}\cdot\bar{y}$ (2) $\overline{x\cdot y}=\bar{x}+\bar{y}$

x	y	$\bar{x}$	$\bar{y}$	$x\cdot y$	$\overline{x\cdot y}$	$\bar{x}+\bar{y}$	$x+y$	$\overline{x+y}$	$\bar{x}\cdot\bar{y}$
1	1	0	0	1	0	0	1	0	0
1	0	0	1	0	1	1	1	0	0
0	1	1	0	0	1	1	1	0	0
0	0	1	1	0	1	1	0	1	1

From column 9 and 10 (1) $\overline{(x+y)}=\bar{x}\cdot\bar{y}$ is proved and from columns 6 and 7 (2) $\overline{x\cdot y}=\bar{x}+\bar{y}$ is proved.
Example: In any Boolean Algebra, show that $(a+b')(b+c')(c+a')=(a'+b)(b'+c)(c'+a)$

$$\begin{aligned}(a+b')(b+c')(c+a')&=(a+b'+0)(b+c'+0)(c+a'+0)\\&=(a+b'+c.c')(b+c'+a.a')(c+a'+b.b')\\&=(a+b'+c).(a+b'+c').(b+c'+a).(b+c'+a').(c+a'+b).(c+a'+b')\\&=[(a'+b+c)(a'+b+c')].[(b'+c+a)(b'+c+a')].[(c'+a+b)(c'+a+b')]\\&=(a'+b+c.c').(b'+c+a.a').(c'+a+b.b')\\&=(a'+b+0).(b'+c+0).(c'+a+0)\\&=(a'+b).(b'+c).(c'+a)\end{aligned}$$

Example: In any Boolean Algebra, show that $(a\cdot b')+(b\cdot c')+(c\cdot a')=(a'\cdot b)+(b'\cdot c)+(c'\cdot a)$

$$\begin{aligned}(a\cdot b')+(b\cdot c')+(c\cdot a')&=(a\cdot b'\cdot 1)+(b\cdot c'\cdot 1)+(c\cdot a'\cdot 1)\\&=(a\cdot b'\cdot(c+c'))+(b\cdot c'\cdot(a+a'))+(c\cdot a'\cdot(b+b'))\\&=(a\cdot b'\cdot c)+(a\cdot b'\cdot c')+(b\cdot c'\cdot a)+(b\cdot c'\cdot a')+(c\cdot a'\cdot b)+(c\cdot a'\cdot b')\\&=\left[(b\cdot c'\cdot a')+(c\cdot a'\cdot b)\right]+\left[(a\cdot b'\cdot c)+(c\cdot a'\cdot b')\right]+\left[(a\cdot b'\cdot c')+(b\cdot c'\cdot a)\right]\\&=(a'\cdot b)\cdot(c+c')+(b'\cdot c)\cdot(a+a')+(c'\cdot a)\cdot(b+b')\\&=(a'\cdot b)\cdot 1+(b'\cdot c)\cdot 1+(c'\cdot a)\cdot 1\\&=(a'\cdot b)+(b'\cdot c)+(c'\cdot a)\end{aligned}$$

Example: In any Boolean algebra show that $a=0 \Leftrightarrow ab'+a'b=b$.

Let B be a Boolean algebra and let $a,b\in B$.

Suppose $a=0$. Then $ab'+a'b=0.b'+1.b=0+b=b$

Conversely, suppose $ab'+a'b=b$ ....(1)

Now

$$\begin{aligned}0&=b'.b\\&=b'.(ab'+a'b)\\&=ab'b'+a'bb'\\&=ab'+a'0\\&=ab'....(2)\end{aligned}$$

Applying De Morgan's law to (1), we have $b'=(a'+b)(a+b')$

Therefore $0=ab'$

$$\begin{aligned}&=a.(a'+b)(a+b')\\&=(aa'+ab)(a+b')\\&=(0+ab)(a+b')\\&=ab.(a+b')\\&=(aba+abb')\\&=(ab+0)\\&=ab\end{aligned}$$

Therefore $0=ab=ab'$

Therefore $0=ab+ab'=a(b+b')=a.1=a$

Hence $a=0$.

Example: If x, y are elements in a Boolean algebra, prove that $x\le y \quad \Leftrightarrow \quad y'\le x'$.

Since $x\le y$ implies $x\wedge y=x$ and $x\vee y=y$

$x'\wedge y'=(x\vee y)'=y'$ and $x'\vee y'=(x\wedge y)'=x'$.

Hence $x'\ge y'$

Conversely $y'\le x'$ implies $y'\wedge x'=y'$ and

$y'\vee x'=x'$.

Taking complements on both sides, we have

$$\begin{array}{ccc}(y'\wedge x')'=(y')' & \text{and} & (y'\vee x')'=(x')' \\ y\vee x=y & & y\wedge x=x\end{array}.$$

Hence $x'\ge y'$

Example: In any Boolean Algebra, prove the following statements are equivalent.

$(1)\ a+b=b \qquad (2)\ a\bullet b=a \qquad (3)\ a'+b=1 \qquad (4)\ a\bullet b'=0$

Let (1) $a+b=b$ is true.

Consider $a\bullet b=a\cdot(a+b)$ {Given}

$=a$ {absorption law}

Therefore $(1)\Leftrightarrow(2)$

Let (2) $a\bullet b=a$ is true.

Adding a' on both sides, we get

$$a'+a\bullet b=a'+a$$

$(a'+a)\bullet(a'+b)=1$ Distributive

$$1\bullet(a'+b)=1$$

$$(a'+b)=1$$

Therefore $(2)\Leftrightarrow(3)$

Let (3) $a'+b=1$ is true.

Taking complement

$$(a'+b)'=1'$$

$$a\cdot b'=0$$

Therefore $(3)\Leftrightarrow(4)$

Suppose (4) $a\cdot b'=0$ is true

Adding b on both sides, we have

$$a\cdot b'+b=0+b$$

$$(a+b)\cdot(b'+b)=b$$

$$(a+b)\cdot 1=b$$

$$(a+b)=b$$

Therefore $(4)\Leftrightarrow(1)$

.

Example: Simplify the Boolean expression $a'.b'.c+a.b'.c+a'.b'.c'$ using Boolean algebra identities.

$$a'\cdot b'\cdot c+a\cdot b'\cdot c+a'\cdot b'\cdot c'=(a+a')\cdot b'\cdot c+a'\cdot b'\cdot c'$$

$$=1\cdot b'\cdot c+a'\cdot b'\cdot c'$$

$$=b'\cdot c+a'\cdot b'\cdot c'$$

$$=b'\cdot(c+a'\cdot c')$$

$$=b'\cdot[(c+a')\cdot(c+c')]$$

$$=b'\cdot[(c+a')\cdot 1]$$

$$=b'\cdot(c+a')$$

$$=b'\cdot c+b'\cdot a'$$

Example: Simplify the Boolean expression $a'\cdot b'\cdot c+a\cdot b'\cdot c+a\cdot b'\cdot c'$ using Boolean algebra identities.

$$a'\cdot b'\cdot c+a\cdot b'\cdot c+a\cdot b'\cdot c'=(a'\cdot b'\cdot c)+a\cdot b'\cdot(c+c')$$

$$=(a'\cdot b'\cdot c)+a\cdot b'\cdot 1$$

$$=(a'\cdot b'\cdot c)+a\cdot b'$$

$$=b'\cdot(a+a')\cdot(a+c)$$

$$=b'\cdot 1\cdot(a+c)$$

$$=b'\cdot a+b'\cdot c$$

.

Example: In any Boolean Algebra, show that $a.b'+a'.b=0$ if and only if $a=b$.

https://doi.org/10.5281/zenodo.15287996

Let $a=b$. Then

$$a.b'+a'.b=a.a'+a'.a$$
$$=0+0$$
$$=0$$

Suppose $a\cdot b'+a'\cdot b=0$. Then

$$a+0=a$$
$$a+a\cdot b'+a'\cdot b=a$$
$$\left(a+a\cdot b'\right)+a'\cdot b=a$$
$$a+a'\cdot b=a \quad \text{\{absorption law\}}$$
$$\left(a+a'\right)\cdot\left(a+b\right)=a \quad \text{\{Distributive\}}$$
$$1\cdot\left(a+b\right)=a$$
$$\left(a+b\right)=a \text{ ....(1)}$$

Similarly

$$b+0=b$$
$$b+a\cdot b'+a'\cdot b=b$$
$$\left(b+a'\cdot b\right)+a\cdot b'=b$$
$$b+a\cdot b'=b \quad \text{\{absorption law\}}$$
$$\left(b+a\right)\cdot\left(b+b'\right)=b \quad \text{\{Distributive\}}$$
$$\left(b+a\right)\cdot 1=b$$
$$\left(b+a\right)=b \text{ ....(2)}$$

From (1) and (2) , we have $a=b$

Example: In a Boolean Algebra, show that $a.\left(a+b\right)=a$ for $a,b\in B$.

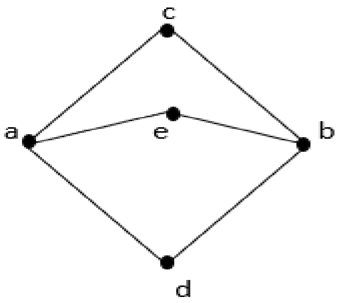
$$a\cdot\left(a+b\right)=a\cdot a+a\cdot b \quad \textit{Distributive}$$
$$=a+a\cdot b \quad \textit{Identity}$$
$$=a\cdot 1+a\cdot b \quad \textit{Complement}$$
$$=a\cdot\left(1+b\right) \quad \textit{Distributive}$$
$$=a\cdot 1 \quad \textit{Complement}$$
$$=a \quad \textit{Complement}$$

Example: In any Boolean Algebra prove that $a\cdot b'+a'\cdot b=\left(a+b\right)\left(a'+b'\right)$

$$\left(a+b\right)\cdot\left(a'+b'\right)=\left(a+b\right)\cdot a'+\left(a+b\right)\cdot b'$$
$$=a\cdot a'+b\cdot a'+a\cdot b'+b\cdot b'$$
$$=0+b\cdot a'+a\cdot b'+0$$
$$=a\cdot b'+a'\cdot b$$

EXERCISE

1. The following is the Hasse diagram of a partially ordered set. Verify whether it is a Lattice.



2. Let $D(12)$ denote the set of all positive divisors of 12. Draw the Hasse diagram of $D(12)$

3. Draw the Hasse diagram for (1) $P_1 = \{2,3,6,12,24\}$ (2) $P_2 = \{1,2,3,4,6,12\}$ and $\leq$ is a relation such that $x \leq y$ if and only if $x \mid y$.

4. Check whether the posets $\{(1,3,6,9),D\}$ and $\{(1,5,25,125),D\}$ are lattices or not. Justify your claim.

5. Draw the Hasse diagram of $(X,\leq)$, where $X = \{2,4,5,10,12,20,25\}$ and the relation $\leq$ be such that $x \leq y$ if x divides y .

6. Prove that D_{110}, the set of all positive divisors of a positive integer 110, is a Boolean Algebra and find all its sub algebras.

https://doi.org/10.5281/zenodo.15287996

7. Let $(L,*,\oplus)$ and $(S,\wedge,\vee)$ be any two lattices with the partial ordering $\leq$ and $\leq'$ respectively. If g is a lattice homomorphism, then g preserves the partial ordering.

8. Show that a complemented, distributive lattice is a Boolean Algebra.

9. Show that every non empty subset of a lattice has a least upper bound and greatest lower bound.

10. Show that every totally ordered set is a lattice.

11. Show that every non empty subset of a lattice has a least upper bound and greatest lower bound.

12. Is a Boolean Algebra contains six elements? Justify your answer.

13. Show that in any Boolean Algebra $(a+b)(a'+c)=ac+a'b+bc$.

https://doi.org/10.5281/zenodo.15287996