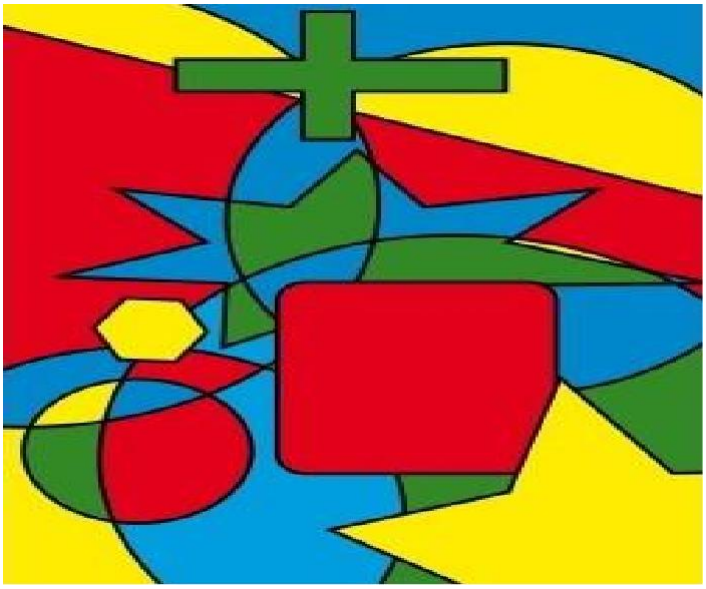
BCS405A

Discrete Mathematical Structures

(For the 4th Semester Computer Science and Engineering Stream)



Module 1

Mathematical Logic

Content

Module-1

Mathematical Logic

☻ **Syllabus:**

Fundamentals of Logic: Basic Connectives and Truth Tables, Logic Equivalence – The Laws of Logic, Logical Implication – Rules of Inference. The Use of Quantifiers, Quantifiers, Definitions and the Proofs of Theorems.

☻ Basic Connectives and Truth table:

Proposition:

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

Example:

1. 2 is a prime number. (true)
2. All sides are equal in scalene triangle. (false)
3. 2+3=4. (false)
4. What is the time now?
5. Read this carefully.

From the above examples we note that 1, 2, 3 are proposition, whereas 4 and 5 are not the propositions.

Logical Connectives and Truth table:

New propositions are obtained by starting with given propositions with the aid of words or phrases like 'not', 'and', 'if … then, and 'if and only if'. Such words or phrases are called **Logical connectives**.

1. Negation:

A proposition is obtained by inserting the word 'not' at an appropriate place in the given proposition is called the negation of the given proposition.

The negation of a Proposition p is denoted by ¬ p (read 'not p'). For any Proposition p, if p is true, then ¬ p is false, and if p is false, then ¬ p is true. i.e., If the truth value of a proposition p is 1 then the truth value of ¬ p is 0 and If the truth value of a proposition p is 0 then the truth value of ¬ p is 1.

Example:

p: 4 is an even number.

¬ p: 4 is not an even number.

Truth table for Negation

p	¬ p
0	1
1	0

2. <u>Conjunction:</u>

A compound proposition obtained by combining two given propositions by inserting the word 'and' in between them is called the conjunction of the given proposition.

The conjunction of two propositions p and q is denoted by $p \wedge q$ (read 'p and q'). The conjunction $p \wedge q$ is true only when p is true and q is true, in all other cases it is false. i.e., the truth value of the conjunction $p \wedge q$ is 1 only when the truth value of p is 1 and truth value of q is 1, in all other cases the truth value of $p \wedge q$ is 0.

Example:

p: $\sqrt{2}$ is an irrational number.

q: 9 is a prime number.

$p \wedge q$: $\sqrt{2}$ is an irrational number and 9 is a prime number.

Truth table for conjunction

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

3. <u>Disjunction:</u>

A compound proposition obtained by combining two given propositions by inserting the word 'or' in between them is called the disjunction of the given propositions.

The disjunction of two propositions p and q is denoted by $p \vee q$ (read 'p or q'). The disjunction $p \vee q$ is false only when p is false and q is false, in all other cases it is true. i.e., the truth value of the disjunction $p \vee q$ is 0 only when the truth value of p is 0 and truth value of q is 0, in all other cases the truth value of $p \vee q$ is 1.

Example:

p: All triangles are equilateral.

q: 2+5=7.

$p \vee q$: All triangles are equilateral or 2+5=7.

Truth table for Disjunction

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

4. <u>Exclusive Disjunction:</u>

We require that the compound proposition "p or q" to be true only when either p is true or q is true but not both. The exclusive or is denoted by the $\veebar$.

The compound proposition $p \veebar q$ (read as either p or q but not both) is called as exclusive disjunction of the propositions p and q. i.e., $p \veebar q = (p \wedge \neg q) \vee (q \wedge \neg p)$

Example:

p:9 is a prime number

q: all triangles are isosceles.

$p \veebar q$: Either 9 is prime number or all triangles are isosceles, but not both

Truth table for Exclusive Disjunction

p	q	$p \veebar q$
0	0	0
0	1	1
1	0	1
1	1	0

5. <u>Conditional:</u>

A compound proposition obtained by combining two given propositions by using the words 'if' and 'then' at appropriate places is called a conditional.

The Conditional "If p, then q" is denoted by $p \rightarrow q$ and the Conditional "If q, then p" is denoted by $q \rightarrow p$. The Conditional $p \rightarrow q$ is false only when p is true and q is false, in all other cases it is true. i.e., the truth value of the conditional $p \rightarrow q$ is 0 only when the truth value of p is 1 and the truth value of q is 0, in all other cases the truth value of $p \rightarrow q$ is 1.

Example:

p: 3 is a prime number.

q: 9 is a multiple of 6

Truth table for Conditional

6.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

<u>Biconditional:</u>

Let p and q be two sample propositions then the conjunction of the conditionals $p \rightarrow q$ and $q \rightarrow p$ is called the biconditional of p and q. It is denoted by $p \leftrightarrow q$ and it is same as $(p \rightarrow q) \wedge (q \rightarrow p)$ is read as "If p then q and if q then p".

Truth table for Biconditional

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

Problems:

1. Construct the truth tables for the following propositions.

(i). $p \wedge (\neg q)$ **(ii).** $(\neg p) \vee q$ **(iii).** $p \rightarrow (\neg q)$ **(iv).** $(\neg p) \veebar (\neg q)$

Solution:

The desired truth tables are obtained by considering all possible combinations of the truth values of p and q. the combined form of required truth table is given below

p	q	$\neg p$	$\neg q$	$p \wedge (\neg q)$	$(\neg p) \vee q$	$p \rightarrow (\neg q)$	$(\neg p) \veebar (\neg q)$
0	0	1	1	0	1	1	0
0	1	1	0	0	1	1	1
1	0	0	1	1	0	1	1
1	1	0	0	0	1	0	0

2. Let p, q and r be propositions having truth values 0, 0 and 1 respectively. Find the truth values if the following compound propositions:

(i). $(p \vee q) \vee r$ **(ii).** $(p \wedge q) \wedge r$ **(iii).** $(p \wedge q) \rightarrow r$

(iv). $p \rightarrow (q \wedge r)$ **(v).** $p \wedge (q \rightarrow r)$ **(vi).** $p \rightarrow (q \rightarrow \neg r)$

Solution:

(i) Since both p and q are false then $(p \vee q)$ is also false. Since r true it follows that $(p \vee q) \vee r$ is true. Thus, the truth value of $(p \vee q) \vee r$ is 1.

(ii) Since both p and q are false, $(p \wedge q)$ is false. Since $(p \wedge q)$ is false and r is true $(p \wedge q) \wedge r$ is false. Thus, the truth value of $(p \wedge q) \wedge r$ is 0.

(iii) Since $(p \wedge q)$ is false and r is true, $(p \wedge q) \rightarrow r$ is true. Thus, the truth value of $(p \wedge q) \rightarrow r$ is 1.

(iv) Since q is false and r is true, $(q \wedge r)$ is false. Also, p is false, therefore $p \rightarrow (q \wedge r)$ is true. Thus, the truth value of $p \rightarrow (q \wedge r)$ is 1.

(v) Since r is true and q is false $(q \rightarrow r)$ is true. Also, p is false. Therefore, $p \wedge (q \rightarrow r)$ is false. Thus, the truth value of $p \wedge (q \rightarrow r)$ is 0

(vi) Since r is true, $\neg r$ is false. Since q is false, $q \rightarrow (\neg r)$ is true. Also, p is false. Therefore, $p \rightarrow (q \rightarrow \neg r)$ is true. Thus, the truth value of $p \rightarrow (q \rightarrow \neg r)$ is 1.

3. Indicate how many rows are needed in the truth table for the compound proposition $(p \vee (\neg q)) \leftrightarrow ((\neg r) \wedge s) \rightarrow t$. Find the truth value of the proposition if p and r, are true and q, s, t, are false.

Solution:

The given compound proposition contains five primitives p, q, r, s, t. Therefore, the number of possible combinations of the truth values of these components which we have to consider is $2^5=32$. Hence 32 rows are needed in the truth table for the given compound proposition.

Next, suppose that p and r, are true and q, s, t are false, then $\neg q$ is true and $\neg r$ is false. Since p is true and $\neg q$ is true, $(p \vee (\neg q))$ is true on the other hand, since $\neg r$ is false and s is false, $\neg r \wedge s$ is false. Also, t is false. Hence $((\neg r) \wedge s) \rightarrow t$ is true.

Since $(p \vee (\neg q))$ is true and $((\neg r) \wedge s) \rightarrow t$ is true, it follows that the truth values of the given propositions $(p \vee (\neg q)) \leftrightarrow ((\neg r \wedge s) \rightarrow t$ is 1.

4. Let p: A circle is a conic, q: $\sqrt{5}$ is a real number, r: Exponential series is convergent. Express the following compound Proposition in words:

(i). $p \wedge (\neg q)$ **(ii).** $(\neg p) \wedge q$ **(iii)** $q \rightarrow (\neg p)$
(iv). $p \veebar (\neg q)$ **(v).** $p \rightarrow (q \veebar r)$ **(vi).** $\neg p \leftrightarrow q$

Solution:

(i) A circle is a conic and $\sqrt{5}$ is not a real number.

(ii) A circle is not a conic and $\sqrt{5}$ is a real number.

(iii) If $\sqrt{5}$ is a real number, then a circle is not a conic.

(iv) Either a circle is a conic or $\sqrt{5}$ is not a real number (but not both).

(v) If a circle is a conic then either $\sqrt{5}$ is a real number or the exponential series is convergent (but not both).

(vi) If a circle is not a conic then $\sqrt{5}$ is a real number and if $\sqrt{5}$ is a real number then a circle is not a conic.

5. Construct the truth table for the following compound propositions:

(i). $(p \wedge q) \rightarrow \neg r$ **(ii).** $q \wedge ((\neg r) \rightarrow p)$

Solution:

The required truth table are shown below in a combined form

p	q	r	$\neg r$	$p \wedge q$	$(p \wedge q) \rightarrow \neg r$	$(\neg r) \rightarrow p$	$q \wedge ((\neg r) \rightarrow p)$
0	0	0	1	0	1	0	0
0	0	1	0	0	1	1	0
0	1	0	1	0	1	0	0
0	1	1	0	0	1	1	1
1	0	0	1	0	1	1	0
1	0	1	0	0	1	1	0
1	1	0	1	1	1	1	1
1	1	1	0	1	0	1	1

☻ Tautology and Contradiction:

A compound proposition which is true for all possible truth values of its components is called a **tautology**.
A compound proposition which is false for all possible truth values of its components is called **Contradiction or an absurdity.**
A compound proposition that can be true or false is called a **contingency.** In other words, a contingency is a compound proposition which is neither a tautology nor a contradiction.

Problems:

1. Show that for any proposition p and q, the compound proposition $p \rightarrow (p \vee q)$ is a tautology and the compound proposition $p \wedge (\neg p \wedge q)$ is called contradiction.

Solution:

Let us first prepare the truth tables for $p \rightarrow (p \vee q)$ and $p \wedge (\neg p \wedge q)$. these truth tables are shown below in the combined form.

p	q	$p \vee q$	$p \rightarrow (p \vee q)$	$\neg p$	$(\neg p \wedge q)$	$p \wedge (\neg p \wedge q)$
0	0	0	1	1	0	0
0	1	1	1	1	1	0
1	0	1	1	0	0	0
1	1	1	1	0	0	0

From the above table we note that, for all possible values of p and q the compound proposition $p \rightarrow (p \vee q)$ is true and the compound proposition $p \wedge (\neg p \wedge q)$ is false.

Therefore $p \wedge (\neg p \wedge q)$ is **<u>contradiction</u>** and $p \rightarrow (p \vee q)$ is **<u>tautology</u>**.

2. Prove that, for any proposition p, q, r the compound proposition

$$(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r) \text{ is a tautology}$$

Solution:
The following truth table gives the required result.

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$p \to r$	$(p \to q) \wedge (q \to r) \to (p \to r)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

3. Prove that for any proposition p, q, r the compound proposition

$(p \vee q) \vee (p \to r) \wedge (q \to r)$ is tautology.

Solution:
The following truth table gives the required result.

p	q	r	$p \to r$	$q \to r$	$(p \to r) \wedge (q \to r)$	$p \vee q$	$(p \vee q) \vee (p \to r) \wedge (q \to r)$
0	0	0	1	1	1	0	1
0	0	1	1	1	1	0	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	1	1
1	0	1	1	1	1	1	1
1	1	0	0	0	0	1	1
1	1	1	1	1	1	1	1

4. Prove that for any proposition p, q, r the compound proposition
$(p \to q) \vee (p \to r) \leftrightarrow (p \to (q \vee r))$ is tautology.

Solution:
The following truth table gives the required result.

p	q	r	$p \to q$	$p \to r$	$(p \to q) \vee (p \to r)$	$q \vee r$	$p \to (q \vee r)$	$(p \to q) \vee (p \to r) \leftrightarrow (p \to (q \vee r))$
0	0	0	1	1	1	0	1	1
0	0	1	1	1	1	1	1	1
0	1	0	1	1	1	1	1	1
0	1	1	1	1	1	1	1	1
1	0	0	0	0	0	0	0	1
1	0	1	0	1	1	1	1	1
1	1	0	1	0	1	1	1	1
1	1	1	1	1	1	1	1	1

5. Prove that for any proposition p, q, r the compound proposition
$[(p \to q) \wedge (p \to r)] \to (p \to r))$ is tautology.

Solution:
The following truth table gives the required result.

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (p \to r)$	$p \to r$	$(p \to q) \wedge (p \to r) \to (p \to r)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

6. Prove that for any proposition p, q, r the compound proposition
$[(p \vee q) \wedge \{(p \to r) \wedge (q \to r)\}] \to r$ is tautology.

Solution:
The following truth table proves the gives result.

p	q	r	$p \to r$	$q \to r$	$(p \to r) \wedge (q \to r)$	$p \vee q$	$(p \vee q) \wedge \{(p \to r) \wedge (q \to r)\}$	$[(p \vee q) \wedge \{(p \to r) \wedge (q \to r)\}] \to r$
0	0	0	1	1	1	0	0	1
0	0	1	1	1	1	0	0	1
0	1	0	1	0	0	1	0	1
0	1	1	1	1	1	1	1	1
1	0	0	0	1	0	1	0	1
1	0	1	1	1	1	1	1	1
1	1	0	0	0	0	1	0	1
1	1	1	1	1	1	1	1	1

7. Verify the Compound Proposition $(p \vee q) \to r \leftrightarrow (\neg r \to \neg (p \vee q))$ is tautology or not.

p	q	r	$\neg r$	$p \vee q$	$(p \vee q) \to r$	$\neg (p \vee q)$	$\neg r \to \neg (p \vee q)$	$(p \vee q) \to r \leftrightarrow (\neg r \to \neg (p \vee q))$
0	0	0	1	0	1	1	1	1
0	0	1	0	0	1	1	1	1
0	1	0	1	1	0	0	0	1
0	1	1	0	1	1	0	1	1
1	0	0	1	1	0	0	0	1
1	0	1	0	1	1	0	1	1
1	1	0	1	1	0	0	0	1
1	1	1	0	1	1	0	1	1

Hence the compound Proposition $(p \vee q) \to r \leftrightarrow (\neg r \to \neg (p \vee q))$ is tautology

8. Prove that for any proposition p, q, r the compound proposition

$\{p \to (q \to r)\} \to \{(p \to q) \to (p \to r)\}$ is tautology.

Solution:

The following truth table gives the required result.

p	q	r	$p \to q$	$p \to r$	$q \to r$	$p \to (q \to r)$	$\{(p \to q) \to (p \to r)$	$\{p \to (q \to r)\} \to \{(p \to q) \to (p \to r)\}$
0	0	0	1	1	1	1	1	1
0	0	1	1	1	1	1	1	1
0	1	0	1	1	0	1	1	1
0	1	1	1	1	1	1	1	1
1	0	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1	1
1	1	0	1	0	0	0	0	1
1	1	1	1	1	1	1	1	1

☻ **Logic equivalence:**

Two statement s_1, s_2 are said to be logically equivalent, and we write $s_1 \leftrightarrow s_2$, when the statement s_1 is true (respectively false) if and only if the statement s_2 is true (respectively false). Or the biconditional $s_1 \leftrightarrow s_2$ is a tautology

Problems:

1. For any two propositions p, q Prove that $(p \rightarrow q) \Leftrightarrow (\neg p) \vee q$

Solution: The following truth table gives the required result.

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

From the column 4 and 5 of the above truth table, we find that $\neg p \vee q$ and $p \rightarrow q$ has the same truth values of p and q. Therefore $(p \rightarrow q) \Leftrightarrow (\neg p) \vee q$.

2. For any two propositions p, q Prove that $(p \rightarrow \neg q) \Leftrightarrow (q \rightarrow \neg p)$

Solution: The following truth table gives the required result.

p	q	$\neg p$	$\neg q$	$p \rightarrow \neg q$	$q \rightarrow \neg p$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	1	1
1	1	0	0	0	0

From the column 5 and 6 of the above truth table, we find that $p \rightarrow \neg q$ and $q \rightarrow \neg p$ has the same truth values of p and q. Therefore $(p \rightarrow \neg q) \Leftrightarrow (q \rightarrow \neg p)$.

3. For any two propositions p, q Prove that $(p \veebar q) \Leftrightarrow (p \vee q) \wedge \neg (p \wedge q)$.

Solution: The following truth table gives the required result.

p	q	$(p \vee q)$	$(p \veebar q)$	$(p \wedge q)$	$\neg (p \wedge q)$	$(p \vee q) \wedge \neg (p \wedge q)$
0	0	0	0	0	1	0
0	1	1	1	0	1	1
1	0	1	1	0	1	1
1	1	1	0	1	0	0

From the column 4 and 7 of the above truth table, we find that $(p \veebar q)$ and $(p \vee q) \wedge \neg (p \wedge q)$ has the same truth values of p and q. Therefore $(p \veebar q) \Leftrightarrow (p \vee q) \wedge \neg (p \wedge q)$.

4. For any propositions p, q, r. Prove that $[(p \rightarrow (q \rightarrow r)] \Leftrightarrow [(p \wedge \neg r) \rightarrow \neg q)]$

Solution: The following truth table gives the required result.

p	q	r	$\neg q$	$\neg r$	$q \rightarrow r$	$p \wedge \neg r$	$p \rightarrow (q \rightarrow r)$	$(p \wedge \neg r) \rightarrow \neg q)$
0	0	0	1	1	1	0	1	1
0	0	1	1	0	1	0	1	1
0	1	0	0	1	0	0	1	1
0	1	1	0	0	1	0	1	1
1	0	0	1	1	1	1	1	1
1	0	1	1	0	1	0	1	1
1	1	0	0	1	0	1	0	0
1	1	1	0	0	1	0	1	1

From the column 8 and 9 of the above truth table, we find that $[p \rightarrow (q \rightarrow r)]$ and $[(p \wedge \neg r) \rightarrow \neg q)]$ has the same truth values of p and q. Therefore $[(p \rightarrow (q \rightarrow r)] \Leftrightarrow [(p \wedge \neg r) \rightarrow \neg q)]$.

5. Show that the compound propositions $p \wedge ((\neg q) \vee r)$ and $p \vee (q \wedge (\neg r))$ are not logically equivalent.

Solution: The following truth table gives the required result

p	q	r	$\neg q$	$\neg r$	$\neg q \vee r$	$q \wedge \neg r$	$p \wedge ((\neg q) \vee r)$	$p \vee (q \wedge (\neg r))$
0	0	0	1	1	1	0	0	0
0	0	1	1	0	1	0	0	0
0	1	0	0	1	0	1	0	1
0	1	1	0	0	1	0	0	0
1	0	0	1	1	1	0	1	1
1	0	1	1	0	1	0	1	1
1	1	0	0	1	0	1	0	1
1	1	1	0	0	1	0	1	1

From the last two rows we note that $p \wedge ((\neg q) \vee r)$ and $p \vee (q \wedge (\neg r))$ do not have the same values in all possible situations. Therefore, they are not logically equivalent.

<u>The Laws of Logic:</u>

For any primitive statements p, q, r any tautology T_o and any contradiction F_o

Sl. No	Name of laws	Laws of logic
1	Laws of double negation	$\neg \neg p \Leftrightarrow p$
2	De Morgan's laws	$\neg (p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$ $\neg (p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$
3	Commutative laws	$(p \vee q) \Leftrightarrow (q \vee p)$ $(p \wedge q) \Leftrightarrow (q \wedge p)$
4	Associative laws	$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$ $p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$
5	Distributive laws	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$
6	Idempotent laws	$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$
7	Identity laws	$p \vee F_o \Leftrightarrow p$ $p \wedge T_o \Leftrightarrow p$
8	Inverse laws	$p \vee \neg p \Leftrightarrow T_o$ $p \wedge \neg p \Leftrightarrow F_o$
9	Domination laws	$p \vee T_o \Leftrightarrow T_o$ $p \wedge F_o \Leftrightarrow F_o$
10	Absorption laws	$p \vee (p \wedge q) \Leftrightarrow p$ $p \wedge (p \vee q) \Leftrightarrow p$

Problems:

1. Prove distributive law $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$

Solution:

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	0	1	1	1	1

From columns 5 and 8 of the above table, we find that $\{p \vee (q \wedge r)\}$ and $\{(p \vee q) \wedge (p \vee r)\}$ has same truth values in all possible situations. Therefore, $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$.

Similarly, we can prove $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$.

2. Prove De Morgan's law $\neg (p \vee q) \Leftrightarrow \neg p \wedge \neg q$

Solution:

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg (p \vee q)$	$\neg p \wedge \neg q$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

From columns 5 and 8 of the above table, we find that $\neg (p \vee q)$ and $\neg p \vee \neg q$ has same truth values in all possible situations. Therefore, $\neg (p \vee q) \Leftrightarrow \neg p \wedge \neg q$.

Similarly, we can prove $\neg (p \wedge q) \Leftrightarrow \neg p \vee \neg q$

Law for the negation of a conditional:

Given a conditional $p \rightarrow q$, its negation is obtained by using the following law.

$\neg (p \rightarrow q) \Leftrightarrow [p \wedge (\neg q)]$

Proof:

The following table gives the truth values of $\neg (p \rightarrow q)$ and $p \wedge (\neg q)$ for all possible truth values of p and q.

p	q	$p \rightarrow q$	$\neg (p \rightarrow q)$	$\neg q$	$p \wedge (\neg q)$
0	0	1	0	1	0
0	1	1	0	0	0
1	0	0	1	1	1
1	1	1	0	0	0

We note that $\neg (p \rightarrow q)$ and $p \wedge (\neg q)$ have same truth values in all possible situations. Hence, $\neg (p \rightarrow q) \Leftrightarrow [p \wedge (\neg q)]$.

Problems:

1. Simplify the following compounds propositions using the laws of logic.

(i) $p \vee q \wedge [\neg \{(\neg p) \wedge q\}]$ **(ii)** $p \vee q \wedge [\neg \{(\neg p) \vee q\}]$

(iii) $\neg [\neg \{(p \vee q) \wedge r\} \vee (\neg q)]$

Solution:

(i) $p \vee q \wedge [\neg \{(\neg p) \wedge q\}]$

$= p \vee q \wedge \{(\neg \neg p) \vee (\neg q)\}$ By De Morgan's law

$= p \vee q \wedge \{p \vee (\neg q)\}$ By Law of double negation

$= p \vee \{q \wedge (\neg q)\}$ By Distributive law

$= p \vee F_o$ By Inverse law

$= p$ By Identity law

(ii) $p \vee q \wedge [\neg \{(\neg p) \vee q\}]$

$= (p \vee q) \wedge \{p \wedge (\neg q)\}$

$= \{(p \vee q) \wedge p)\} \wedge (\neg q)$ Using Associative law

$= \{p \wedge (p \vee q)\} \wedge (\neg q)$ Using Commutative law

$= p \wedge (\neg q)$ Using Absorption law

(iii) $\neg [\neg \{(p \vee q) \wedge r\} \vee (\neg q)]$

$= \neg [\neg \{((p \vee q) \wedge r) \wedge q\}]$ Using De Morgan's law

$= ((p \vee q) \wedge r) \wedge q$ Law of Double negation

$= (p \vee q) \wedge (q \wedge r)$ Using Associative and Commutative law

$= \{(p \vee q) \wedge q\} \wedge r$ Using Associative law

$= q \wedge r$ Using Associative law

2. Prove the following logically without using truth table.

(i). $[p \vee q \vee (\neg p \wedge \neg q \wedge r)] \Leftrightarrow p \vee q \vee r$ **(ii).** $[(\neg p \vee \neg q) \rightarrow (p \wedge q \wedge r)] \Leftrightarrow p \wedge q$

(iii). $p \rightarrow (q \rightarrow r) \Leftrightarrow (p \wedge q) \rightarrow r$

Solution:

(i) $[p \vee q \vee (\neg p \wedge \neg q \wedge r)] \Leftrightarrow p \vee q \vee r$

We have, $\neg p \wedge \neg q \wedge r \Leftrightarrow \neg (p \vee q) \wedge r$ By De Morgan's law

Therefore, $[p \vee q \vee (\neg p \wedge \neg q \wedge r)] \Leftrightarrow (p \vee q) \vee (\neg (p \vee q) \wedge r)$

$\Leftrightarrow [(p \vee q) \vee \neg (p \vee q)] \wedge (p \vee q \vee r)$ By Distributive law

$\Leftrightarrow T_o \wedge (p \vee q \vee r)$ By Inverse and Associative law

$\Leftrightarrow (p \vee q \vee r)$ By Commutative law

(ii) $[(\neg p \vee \neg q) \rightarrow (p \wedge q \wedge r)] \Leftrightarrow p \wedge q$

We have, $[(\neg p \vee \neg q) \rightarrow (p \wedge q \wedge r)] \Leftrightarrow \neg (\neg p \vee \neg q) \vee (p \wedge q \wedge r)$

Because $(u \rightarrow v) \Leftrightarrow (\neg u \vee v)$

$\Leftrightarrow (p \wedge q) \vee [(p \wedge q) \wedge r]$ By De Morgan's law and Associative law

$\Leftrightarrow p \wedge q$ By Absorption law

(iii) we have, $p \rightarrow (q \rightarrow r) \Leftrightarrow \neg p \vee (\neg q \vee r)$ Because $(u \rightarrow v) \Leftrightarrow (\neg u \vee v)$

$\Leftrightarrow (\neg p \vee \neg q) \vee r$ Associative law

$\Leftrightarrow (p \wedge q) \vee r$ De-Morgan's law

$\Leftrightarrow (p \wedge q) \rightarrow r$ Because $(u \rightarrow v) \Leftrightarrow (\neg u \vee v)$

Duality:

Let s be a statement. If s contains no logical connectives other than $\wedge$ and $\vee$, the dual of s denoted by $\mathbf{s^d}$, is the statement obtained from s by replacing each occurrence of $\wedge$ and $\vee$ by $\vee$ and $\wedge$ respectively, and each occurrence of $\mathbf{T_o}$ and $\mathbf{F_o}$ by $\mathbf{F_o}$ and $\mathbf{T_o}$, respectively.

Example: Given the primitive statements p, q, r and the compound statements

s: $(p \wedge (\neg q)) \vee (r \wedge T_o)$

s^d: $(p \vee (\neg q)) \wedge (r \vee F_o)$

Principle of Duality:

Let s and t be two statements that contains no logical connections than $\wedge$ and $\vee$. If $s \Leftrightarrow t$, then $s^d \Leftrightarrow t^d$.

Problems:

1. Write duals of the following propositions.
(i). $p \rightarrow q$ **(ii).** $(p \rightarrow q) \rightarrow r$ **(iii).** $p \rightarrow (q \rightarrow r)$

Solution: we recall that $(u \rightarrow v) \Leftrightarrow (\neg u \vee v)$

Therefore, by the principle of duality we find that

(i) $(p \rightarrow q)^d \Leftrightarrow (\neg p \vee q)^d \Leftrightarrow \neg p \wedge q$

(ii) $[(p \rightarrow q) \rightarrow r]^d \Leftrightarrow [\neg(\neg p \vee q) \vee r]^d$

$\Leftrightarrow [(p \wedge \neg q) \vee r]^d$

$\Leftrightarrow (p \vee \neg q) \wedge r$

(iii) $[p \rightarrow (q \rightarrow r)]^d \Leftrightarrow [\neg p \vee (q \rightarrow r)]^d$
$\Leftrightarrow [\neg p \vee (\neg q \vee r)]^d$

$\Leftrightarrow \neg p \wedge (\neg q \wedge r)$

2. Write duals of the following propositions.
(i). $q \rightarrow p$ **(ii).** $(p \vee q) \wedge r$ **(iii).** $(p \wedge q) \vee T_0$
(iv). $p \rightarrow (q \wedge r)$ **(v).** $p \leftrightarrow q$ **(vi).** $p \veebar q$

Solution: we recall that $(u \rightarrow v) \Leftrightarrow (\neg u \vee v)$

Therefore, by the principle of duality we find that

(i) $(q \rightarrow p)^d \Leftrightarrow (\neg q \vee p)^d \Leftrightarrow \neg q \wedge p$

(ii) $[(p \vee q) \wedge r]^d \Leftrightarrow (p \wedge q) \vee r$

(iii) $[(p \wedge q) \vee T_0]^d \Leftrightarrow (p \vee q) \wedge F_0$

(iv) $[p \rightarrow (q \wedge r)]^d \Leftrightarrow [\neg p \vee (q \wedge r)]^d \Leftrightarrow \neg p \wedge (q \vee r)$

(v) $[p \leftrightarrow q]^d \Leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]^d \Leftrightarrow [(\neg p \vee q) \wedge (\neg q \vee p)]^d$

$\Leftrightarrow (\neg p \wedge q) \vee (\neg q \wedge p)$

(vi) $[p \veebar q]^d \Leftrightarrow [(p \wedge \neg q) \vee (q \wedge \neg p)]^d \Leftrightarrow [(p \vee \neg q) \wedge (q \vee \neg p)]$

<u>NAND and NOR</u>:

The compound proposition $\neg (p \wedge q)$ is read as "Not p and q" and also denoted by $(p \uparrow q)$. The symbol $\uparrow$ is called NAND connective.

The compound proposition $\neg (p \vee q)$ is read as "Not p or q" and also denoted by $(p \downarrow q)$. The symbol $\downarrow$ is called the NOR connective.

Truth table

p	q	$p \uparrow q$	$p \downarrow q$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

Where $p \uparrow q = \neg (p \wedge q) \Leftrightarrow \neg p \vee \neg q$ and $p \downarrow q = \neg (p \vee q) \Leftrightarrow \neg p \wedge \neg q$

<u>Problems:</u>

1. For any propositions p, q Prove the following
(i). $\neg (p \downarrow q) \Leftrightarrow \neg p \uparrow \neg q$ **(ii).** $\neg (p \uparrow q) \Leftrightarrow \neg p \downarrow \neg q$

Solution: Using definition, we find that

i. $\neg (p \downarrow q) \Leftrightarrow \neg [\neg (p \vee q)]$
$\Leftrightarrow \neg [\neg p \wedge \neg q]$
$\Leftrightarrow \neg p \uparrow \neg q$

ii. $\neg (p \uparrow q) \Leftrightarrow \neg [\neg (p \wedge q)]$
$\Leftrightarrow \neg [\neg p \vee \neg q]$
$\Leftrightarrow \neg p \downarrow \neg q$

2. For any propositions p, q, r Prove the following

(i). $p \uparrow (q \uparrow r) \Leftrightarrow \neg p \vee (q \wedge r)$ **(ii).** $(p \uparrow q) \uparrow r \Leftrightarrow (p \wedge q) \vee \neg r$

(iii). $p \downarrow (q \downarrow r) \Leftrightarrow \neg p \wedge (q \vee r)$ **(iv).** $(p \downarrow q) \downarrow r \Leftrightarrow (p \vee q) \wedge \neg r$

Solution: Using definition, we find that

(i). $p \uparrow (q \uparrow r) \Leftrightarrow \neg [p \wedge (q \uparrow r))]$

$\Leftrightarrow \neg [p \wedge \neg (q \wedge r)]$

$\Leftrightarrow \neg p \vee \neg [\neg (q \wedge r)]$

$\Leftrightarrow \neg p \vee (q \wedge r)$

(ii). $(p \uparrow q) \uparrow r \Leftrightarrow \neg [(p \uparrow q) \wedge r]$

$\Leftrightarrow \neg [\neg (p \wedge q) \wedge r]$

$\Leftrightarrow \neg [\neg (p \wedge q)] \vee \neg r$

$\Leftrightarrow (p \wedge q) \vee \neg r$

(iii). $p \downarrow (q \downarrow r) \Leftrightarrow \neg [p \vee (q \downarrow r))]$

$\Leftrightarrow \neg [p \vee \neg (q \vee r)]$

$\Leftrightarrow \neg p \wedge \neg [\neg (q \vee r)]$

$\Leftrightarrow \neg p \wedge (q \vee r)$

(iv). $(p \downarrow q) \downarrow r \Leftrightarrow \neg [(p \downarrow q) \vee r]$

$\Leftrightarrow \neg [\neg (p \vee q) \vee r]$

$\Leftrightarrow \neg [\neg (p \vee q)] \wedge \neg r$

$\Leftrightarrow (p \vee q) \wedge \neg r$

Converse, Inverse and Contrapositive:

Consider a conditional $p \rightarrow q$ then:

1. $q \rightarrow p$ is called the converse of $p \rightarrow q$.
2. $\neg p \rightarrow \neg q$ is called the inverse of $p \rightarrow q$.
3. $\neg q \rightarrow \neg p$ is called the contrapositive of $p \rightarrow q$.

Truth table for converse, inverse and contrapositive

p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$q \rightarrow p$	$\neg p \rightarrow \neg q$	$\neg q \rightarrow \neg p$
0	0	1	1	1	1	1	1
0	1	1	0	1	0	0	1
1	0	0	1	0	1	1	0
1	1	0	0	1	1	1	1

Note: 1. A conditional and its contrapositive are logically equivalent i.e., $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$

2. A converse and the inverse of a conditional are logically equivalent

$$q \rightarrow p \Leftrightarrow \neg p \rightarrow \neg q$$

Logical implication:

Logical implication is a type of relationship between two statements or sentences. The relation translates verbally into "logically implies" or "if/then" and is symbolized by a double-lined arrow pointing toward the right ($\Rightarrow$). If p and q represent statements, then $p \Rightarrow q$ means "p implies q" or "If p, then q." The word "implies" is used in the strongest possible sense.

Example:

Suppose the sentences p and q are assigned as follows:

p = The sky is overcast.
q = The sun is not visible.

In this instance, $p \Rightarrow q$ is a true statement (assuming we are at the surface of the earth, below the cloud layer.) However, the statement $p \Rightarrow q$ is not necessarily true; it might be a clear night. Logical implication does not work both ways. However, the sense of logical implication is reversed if both statements are negated. i.e., $(p \Rightarrow q) \Rightarrow (\neg q \Rightarrow \neg p)$

Using the above sentences as examples, we can say that if the sun is visible, then the sky is not overcast. This is always true. In fact, the two statements $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$ are logically equivalent.

Necessary and Sufficient Conditions:

Consider two propositions p and q whose truth values are interrelated. Suppose that $p \Rightarrow q$. Then in order that q may be true it is sufficient that p is true. Also, if p is true then it is necessary that q is true. In view of this interpretation, all of the following statements are taken to carry the same meaning:

(i). $p \Rightarrow q$ (ii). p is sufficient for q (iii). q is necessary for p

Problems:

1. State the converse inverse and contrapositive of
i) If the triangle is not isosceles, then it is not equilateral
ii) If the real number x^2 is greater than zero, then x is not equal to zero.
iii) If a quadrilateral is a parallelogram, then its diagonals bisect each other.

Solution:

(i) p: Triangle is not isosceles and q: Triangle is not equilateral.

Implication: $p \rightarrow q$. if triangle is not isosceles then it is not equilateral.
Converse: $q \rightarrow p$. if a triangle is not equilateral then it is not isosceles.
Inverse: $\neg p \rightarrow \neg q$. if a triangle is isosceles then it is equilateral.
Contrapositive: $\neg q \rightarrow \neg p$: if a triangle is equilateral then it is isosceles.

(ii) p: A real number x^2 is greater than zero and q: x is not equal to zero.
Implication: $p \rightarrow q$. if a real number x^2 is greater than zero then, x is not equal to zero.
Converse: $q \rightarrow p$. if a real number x is not equal to zero then, x^2 is greater zero.
Inverse: $\neg p \rightarrow \neg q$. if a real number x^2 is not greater than zero then, x is equal to zero.
Contrapositive: If a real number x is equal to zero then, x^2 is not greater than zero

(iii) p: If Quadrilateral is a parallelogram and q: its Diagonals Bisects each other.

Implication: $p \rightarrow q$. If Quadrilateral is a parallelogram, then its diagonals bisects each other.
Converse: $q \rightarrow p$. If the diagonals of the Quadrilateral bisect each other, then it is a parallelogram.
Inverse: $\neg p \rightarrow \neg q$. If Quadrilateral is not a parallelogram, then its diagonals do not bisect each other.
Contrapositive: $\neg q \rightarrow \neg p$: If the diagonals of the Quadrilateral do not bisect each other, then it is a not a parallelogram.

2. Write down the following statements in the 'Necessary and Sufficient Condition' Language.
i) If the triangle is not isosceles, then it is not equilateral
ii) If the real number x^2 is greater than zero, then x is not equal to zero.
iii) If a quadrilateral is a parallelogram, then its diagonals bisect each other.

Solution:

Necessary Condition Language:

(i). For a triangle to be non-isosceles it is necessary that is not equilateral.

(ii). A necessary condition for a real number x^2 to be greater than zero is that x is not equal to zero.

(iii). A necessary condition for a quadrilateral to be a parallelogram is that its diagonals bisect each other.

Necessary Condition Language:

(i). A sufficient condition for a triangle to be not equilateral is that it is not isosceles.

(ii). For a real number x, the condition x^2 to be greater than zero is sufficient for x to be not equal to zero.

(iii). A sufficient condition for the diagonals of a quadrilateral to bisect each other is that the quadrilateral is a parallelogram.

☻ **<u>Rules of inference</u>:**

Let us consider the implication $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$

Here n is a positive integer, the statements $p_1, p_2, \ldots p_n$ are called the **premises of the argument** and q is called the **conclusion of the argument**.

We write the above argument in the following tabular form:

$$\begin{array}{c} p_1 \\ p_2 \\ p_3 \\ \vdots \\ \vdots \\ \underline{p_n} \\ \therefore q \end{array}$$

The preceding argument is said to be valid if whenever each of the premises $p_1, p_2, \ldots p_n$ is true, then the conclusion q is likewise true.
i.e., $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is valid when $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q$
It is to be emphasized that in an argument, the premises are always taken to be true whereas the conclusion may be true or false. The conclusion is true only in the case of valid argument. There exist rules of logic which can be employed for establishing the validity of arguments. These rules are called Rules of Inference.

Name of the rule and rule of inference

Sl.no	Rules of inference	Name of rule
1	$\begin{array}{c} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$	Rule of Detachment (modus pones)
2	$\begin{array}{c} p \rightarrow q \\ \underline{q \rightarrow r} \\ \therefore p \rightarrow r \end{array}$	Law of Syllogism
3	$\begin{array}{c} p \rightarrow q \\ \underline{\neg q} \\ \therefore \neg p \end{array}$	Modus Tollens
4	$\begin{array}{c} p \\ \underline{q} \\ \therefore p \wedge q \end{array}$	Rule of Conjunction
5	$\begin{array}{c} p \vee q \\ \underline{\neg p} \\ \therefore q \end{array}$	Rule of Disjunctive Syllogism
6	$\begin{array}{c} \underline{\neg p \rightarrow Fo} \\ \therefore p \end{array}$	Rule of Contradiction
7	$\begin{array}{c} \underline{p \wedge q} \\ \therefore p \end{array}$	Rule of Conjunctive Simplification
8	$\begin{array}{c} \underline{p} \\ \therefore p \vee q \end{array}$	Rule of Disjunctive Amplification

Problems:

1. Test whether the following is valid argument.

If Sachin hits a century, then he gets a free car.

Sachin hits a century.

∴ Sachin gets a free car.

Solution: Let p: Sachin hits a century.

q: Sachin gets a free car.

The given statement reads

$$\begin{array}{c} p \to q \\ \underline{\quad p \quad} \\ \therefore q \end{array}$$

In view of Modus Pones Rule, this is a valid argument.

2. Test the validity of the following arguments.
If Ravi goes out with friends, he will not study.
If Ravi does not study, his father will become angry.
His father is not angry.
∴ Ravi has not gone out with friends.

Solution: Let p: Ravi goes out with friends.

q: Ravi does not study.

r: His father gets angry.

Then the given argument reads.

$$\begin{array}{c} p \to q \\ q \to r \\ \underline{\quad \neg r \quad} \\ \therefore \neg p \end{array}$$

This argument is logically equivalent to (Using the rule of syllogism)

$$\begin{array}{c} p \to r \\ \underline{\quad \neg r \quad} \\ \therefore \neg p \end{array}$$

In view of Modus Tollens Rule, this is a valid argument.

3. Test whether the following is valid argument.

If Sachin hits a century, then he gets a free car.

Sachin does not get a free car.

∴ Sachin has not hit a century

Solution: Let p: Sachin hits a century.

q: Sachin gets a free car.

The given statement reads

$$\begin{array}{c} p \rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

In view of Modus Tollens Rule, this is a valid argument.

4. Test the validity of the following argument
If I study, then I'll not fail in the examination.
If I do not watch tv in the evenings, I will study.
<u>I failed in the examination.</u>
∴ I must have watched tv in the evenings.

Solution: Let p: I study

q: I fail in the examination

r: I watch tv in the evenings.

Then the given argument reads

$$\begin{array}{c} p \rightarrow \neg q \\ \neg r \rightarrow p \\ q \\ \hline \therefore r \end{array}$$

This argument is logically equivalent to

$$\begin{array}{c} q \rightarrow \neg p \\ \neg p \rightarrow r \\ q \\ \hline \therefore r \end{array}$$

(because $(p \rightarrow \neg q) \Leftrightarrow (\neg\neg q \rightarrow \neg p)$)

(because $(\neg r \rightarrow p) \Leftrightarrow (\neg p \rightarrow r)$)

This is equivalent to (Using rule of syllogism)

$$\begin{array}{c} q \rightarrow r \\ q \\ \hline \therefore r \end{array}$$

In view of Modus Pones Rule, this is a valid argument.

5. Test the validity of the following argument
I will become famous or I will not become a musician.
<u>I will become a musician.</u>
∴ I will become famous.

Solution: Let p: I will become famous

q: I will become a musician

Then the given argument reads

$$\begin{array}{c} p \vee \neg q \\ \underline{\quad q \quad} \\ \therefore p \end{array}$$

This argument is logically equivalent to

$$\begin{array}{c} q \rightarrow p \\ \underline{\quad q \quad} \\ \therefore p \end{array}$$

Because $p \vee \neg q \Leftrightarrow \neg q \vee p \Leftrightarrow q \rightarrow p$

In view of Modus Pones Rule, this is a valid argument.

6. Test the validity of the following argument
I will get grade A in this course or I will not graduate.
If I do not graduate, I will join army.
<u>I got grade A.</u>
∴ I will not join army.

Solution: Let p: I will get grad A in this course

q: I do not graduate.

r: I will join army.

Then the given argument reads

$$\begin{array}{c} p \vee q \\ q \rightarrow r \\ \underline{\quad p \quad} \\ \therefore \neg r \end{array}$$

This argument is logically equivalent to

$$\begin{array}{c} \neg q \rightarrow p \\ \neg r \rightarrow \neg q \\ \underline{\quad p \quad} \\ \therefore \neg r \end{array}$$

Because $p \vee \neg q \Leftrightarrow q \vee p \Leftrightarrow \neg q \rightarrow p$ and using Contrapositive.

This is equivalent to (Using rule of syllogism)

$$\begin{array}{c} \neg r \rightarrow p \\ \underline{\quad p \quad} \\ \therefore \neg r \end{array}$$

This is not a valid argument.

7. Test whether the following is valid argument.

If Sachin hits a century, then he gets a free car.

Sachin gets a free car.

∴ Sachin has hit a century.

Solution: Let p: Sachin hits a century.

q: Sachin gets a free car.

The given statement reads

$$\begin{array}{r} p \to q \\ q \\ \hline \therefore p \end{array}$$

We note that if $p \to q$ and q are true, there is no rule which asserts that p must be true. Indeed, p can be false when $p \to q$ and q are true. See the table below.

p	q	$p \to q$	$(p \to q) \wedge q$
0	1	1	1

Thus, $[(p \to q) \wedge q] \to p$ is not a tautology. Hence, this is not a valid argument.

8. Test the Validity of the following argument:

(i). $p \wedge q$
$p \to (q \to r)$
$\therefore\ r$

(ii). p
$p \to \neg q$
$\neg q \to \neg r$
$\therefore\ \neg r$

(iii). $p \to r$
$q \to r$
$\therefore\ (p \vee q) \to r$

Solution:

(i). Since $p \wedge q$ is true, both p and q are true. Since p is true and $p \to (q \to r)$ is true, $q \to r$ Should be true. Since q is true and $q \to r$ is true, r should be true. Hence the given argument is valid.

(ii). The premises $p \to \neg q$ and $\neg q \to \neg r$ together yields the premise $p \to \neg r$. since p is true, this premise $p \to \neg r$ establishes that $\neg r$ is true. Hence the given argument is valid.

(iii) We note that

$(p \to r) \wedge (q \to r) \Leftrightarrow (\neg p \vee r) \wedge (\neg q \vee r)$

$\Leftrightarrow (r \vee \neg p) \wedge (r \vee \neg q)$ By Commutative law

$\Leftrightarrow r \vee (\neg p \wedge \neg q)$ By Distributive law

$\Leftrightarrow \neg (p \vee q) \vee r$ By Commutative & De Morgan's Law

$\Leftrightarrow (p \vee q) \to r$

This Logical equivalence shows that the given argument is valid.

9. Test whether the following arguments are valid:

(i).

$p \to q$

$r \to s$

$\underline{p \vee r}$

$\therefore\ q \vee s$

(ii).

$p \to q$

$r \to s$

$\underline{\neg q \vee \neg s}$

$\therefore \neg (p \wedge r)$

Solution:

(i) We note that

$(p \to q) \wedge (r \to s) \wedge (p \vee r) \Leftrightarrow (p \to q) \wedge (r \to s) \wedge (\neg p \to r)$

$\Leftrightarrow (p \to q) \wedge (\neg p \to r) \wedge (r \to s)$ By Commutative law

$\Leftrightarrow (p \to q) \wedge (\neg p \to s)$ Using Rule of Syllogism

$\Leftrightarrow (\neg q \to \neg p) \wedge (\neg p \to s)$ Using Contrapositive

$\Leftrightarrow (\neg q \to s)$ Using Rule of Syllogism

$\Leftrightarrow q \vee s$

This Logical equivalence shows that the given argument is valid.

(ii) We note that

$(p \to q) \wedge (r \to s) \wedge (\neg q \vee \neg s) \Leftrightarrow (p \to q) \wedge (r \to s) \wedge (q \to \neg s)$

$\Leftrightarrow (p \to q) \wedge (q \to \neg s) \wedge (r \to s)$ By Commutative law

$\Leftrightarrow (p \to \neg s) \wedge (r \to s)$ Using Rule of Syllogism

$\Leftrightarrow (p \to \neg s) \wedge (\neg s \to \neg r)$ Using Contrapositive

$\Leftrightarrow (p \to \neg r)$ Using Rule of Syllogism

$\Leftrightarrow \neg p \vee \neg r)$

$\Leftrightarrow \neg (p \wedge r)$

This Logical equivalence shows that the given argument is valid.

10. Show that the following argument is not valid:

p

$p \vee q$

$q \to (r \to s)$

$\underline{t \to r}$

$\therefore \neg s \to \neg t$

Solution:

Here p is true (premise) and ($p \vee q$) is true (premise). Therefore, q may be true or false.

Suppose q is false. Then, since $q \rightarrow (r \rightarrow s)$ is true (premise), $r \rightarrow s$ must be false. This means that r must be true, and s must be false. Since r is true and $t \rightarrow r$ is true (premise), t may be true or false. Suppose t is true, then $\neg t$ is false. Since s must be false, $\neg s$ must be true. Consequently, $\neg s \rightarrow \neg t$ is false.

Thus, when q is false and t is true, the given conclusion does not follow from the given premise. As such, the given argument is not valid argument.

☻ **<u>Open statement</u>:**

A declaration statement is an open statement

i. If it contains one or more variables.
ii. If it is not statement.
iii. But it becomes statement when the variables in it are replaced by certain allowable choices.

Example: "The number x+2 is an even integer" is denoted by P(x) then ¬ P(x) may be read as "The number x+2 is not an even integer".

<u>Quantifiers</u>:

The words "all", "every", "some", "there exist" are associated with the idea of a quantity such words are called quantifiers.

1. **Universal quantifiers**:
   The symbol ∀ has been used to denote the phrases "for all" and "for every" in logic "for each" and "for any" are also taken up to equivalent to these. These equivalent phrases are called universal quantifiers.
2. **Existential quantifiers**:
   The symbol ∃ has been used to denote the phrases "there exist", "for some" and "for at least one" each of these equivalent phrases is called the existential quantifiers.

Example: 1. For every integer x, x^2 is a non-negative integer ∃ x ∈ s, P(x).

2. For the universe of all integers, let
   p(x): x>0.
   q(x): x is even.
   r(x): x is a perfect square.
   s(x): x is divisible by 3.
   t(x): x is divisible by 7.

<u>Problems</u>:

Write down the following quantified statements in symbolic form:

i) At least one integer is even.

ii) There exists a positive integer that is even.

iii) Some integers are divisible by 3.

iv) every integer is either odd or even.

v) if x is even and a perfect square, then is not divisible by 3.

vi) if x is odd or is not divisible by 7, then x is divisible by 3.

<u>Solution:</u>

Using the definition of quantifiers, we find that the given statement read as follows in symbolic form

i) $\exists x, q(x)$

ii) $\exists x, [\ p(x) \wedge q(x)]$

iii) $\exists x, [\ q(x) \wedge s(x)]$

vi) $\forall x, [\ q(x) \veebar \neg q(x)]$

v) $\forall x\ [\ \{q(x) \wedge r(x)\} \rightarrow s(x)]$

vi) $\forall x, [\{\neg q(x) \vee \neg t(x)\} \rightarrow s(x)]$

<u>Rules employed for determining truth value</u>:

Rule1: The statement "$\forall\ x \in s, p(x)$" is true only when $p(x)$ is true for each $x \in s$.

Rule2: The statement "$\exists\ x \in s, p(x)$" is false only when $p(x)$ is false for every $x \in s$.

*****<u>Rules of inference</u>:

Rule3: If an open statement $p(x)$ is known to be true for all x in a universe s and if $a \in s$ then $p(a)$ is true. (this is known as the rule of universal specification).

Rule4: if an open statement $p(x)$ is proved to be true for any (arbitrary) x chosen from a set s then the quantified statement $\forall\ x \in s, p(x)$ is true. (this is known as the rule of universal generalization)

*****<u>Logical equivalence</u>:

Two quantified statements are said to be logically equivalent whenever they have the same truth values in all possible situations.

The following results are easy to prove.

i) $\forall\ x\ [p(x) \wedge q(x)] \Leftrightarrow (\forall\ x, p(x)) \wedge (\forall\ x, q(x))$

ii) $\exists\ x\ [p(x) \vee q(x)] \Leftrightarrow (\exists\ x, p(x)) \vee (\exists\ x, q(x))$

iii) $\exists\ x, [p(x) \rightarrow q(x)] \Leftrightarrow \exists\ x, (\neg p(x) \vee q(x))$

*****<u>Rule for negation of a quantified statement</u>:

Rule5: To construct the negation of a quantified statement, change the quantifier from universal

to existential and vice versa.

i.e., $\neg\ [\forall\ x, p(x)] \equiv \exists\ x, [\ \neg p(x)]$

$\neg\ [(\exists\ x, p(x)] \equiv \forall\ x\ [\ \neg p(x)]$

Problems:

1. Consider the open statements with the set of real numbers as the universe.

$p(x): |x|>3$, $q(x): x>3$

Find the truth value of the statement $\forall x, [p(x) \rightarrow q(x)]$. Also, write down the converse, inverse and the contrapositive of this statement and find their truth values

Solution:

We readily note that

$p(-4) \equiv |-4|>3$ is true and $q(-4) \equiv -4>3$ is false

Thus, $p(x) \rightarrow q(x)$ is false for $x= -4$.

Accordingly, the given statement $\forall x, [p(x) \rightarrow q(x)]$ ..... (i) is false.

The converse of the statement (i) is $\forall x, [q(x) \rightarrow p(x)]$ .....(ii)

In words, this reads "For every real number x, $x>3$ then $|x|>3$"

Or Equivalently, "Every real number greater than 3 has its absolute value (magnitude) greater than 3"

This is a true statement.

Next, the inverse of the statement (i) is $\forall x, [\neg p(x) \rightarrow \neg q(x)]$ .....(iii)

In words this reads "For every real number x, if $|x| \leq 3$ then $x \leq 3$"

Or equivalently, "If the magnitude of a real number is less than or equal to 3, then the number is less than or equal to 3"

Since the converse and inverse of a conditional are logically equivalent the statements (ii) and (iii) have the same truth values. Thus iii) is a true statement.

Then the contrapositive of statement (i) is $\forall x, [\neg q(x) \rightarrow \neg p(x)]$.....(iv)

"Every real number which is less than or equal to 3 has its magnitude less than or equal to 3".

2. Let $p(x): x^2-7x+10$, $q(x): x^2-2x-3$, $r(x): x<0$.
Determine the truth or falsity of the following statements. When the universe U contains only the integers 2 and 5. If a statement is false. Provide a counter example or explanation.

(i). $\forall x, [p(x) \rightarrow \neg r(x)]$ **(ii).** $\forall x, [q(x) \rightarrow r(x)]$
(iii). $\exists x, [q(x) \rightarrow r(x)]$ **(iv).** $\exists x, [p(x) \rightarrow r(x)]$

Solution:

Here, the universe is $U= \{2, 5\}$.

We note that $x^2-7x+10 = (x-5)(x-2)$. Therefore, p(x) is true for x=5 and 2. That is p(x) is true for all $x \in U$.

Further, $x^2-2x-3 = (x-3)(x+1)$. Therefore, q(x) is only true for x=3 and x=-1. Since x=3 and x=-1 are not in the universe, q(x) is false for all $x \in U$

Obviously, r(x) is false for all $x \in U$.

Accordingly:

(i) Since p(x) is true for all $x \in U$ and $\neg$ r(x) is true for all $x \in U$, the statement $\forall$ x,

$[p(x) \rightarrow \neg r(x)]$ is true.

(ii) Since q(x) is false for all $x \in U$ and r(x) is false for all $x \in U$, the statement $\forall$ x,

$[q(x) \rightarrow r(x)]$ is true.

(iii) Since q(x) and r(x) are false for x=2, the statement $\exists$ x, $[q(x) \rightarrow r(x)]$ is true.

(iv) Since p(x) is true for all $x \in U$ but r(x) is false for all $x \in U$. the statement $p(x) \rightarrow r(x)$ is false for all $x \in U$. consequently, $\exists$ x, $[p(x) \rightarrow r(x)]$ is false.

3. Negate and simplify each of the following.

(i). $\exists$ x, $[p(x) \vee q(x)]$ **(ii).** $\forall$ x, $[p(x) \wedge \neg q(x)]$

(iii). $\forall$ x, $[p(x) \rightarrow q(x)]$ **(iv).** $\exists$ x, $[p(x) \vee q(x)] \rightarrow r(x)$

Solution:

By using the rule of negation for quantified statements and the laws of logic, we find that

(i) $\neg [\exists x, \{p(x) \vee q(x)\}] \equiv \forall x, [\neg \{p(x) \vee q(x)]$

$\equiv \forall x, [\neg p(x) \wedge \neg q(x)]$

(ii) $\neg [\forall x, \{p(x) \wedge \neg q(x)\}] \equiv \exists x, [\neg \{p(x) \wedge \neg q(x)\}]$

$\equiv \exists x, [\neg p(x) \vee q(x)]$

(iii) $\neg [\forall x, \{p(x) \rightarrow q(x)\}] \equiv \exists x, [\neg \{\neg p(x) \vee q(x)\}]$

$\equiv \exists x, [p(x) \wedge \neg q(x)\}]$

(iv) $\neg [\exists x, \{p(x) \vee q(x)\} \rightarrow r(x)] \equiv \forall x, [\neg \{\neg (p(x) \vee q(x)) \vee r(x)\}]$

$\equiv \forall x, [\{p(x) \vee q(x)\} \wedge \neg r(x)]$

4. Write down the following proposition in symbolic form, and find its negation:
"If all triangles are right angled, then no triangle is equiangular".

Solution:

Let T denote set of all triangles. Also, p(x): x is right angled, q(x): x is equiangular.

Then in symbolic form, the given proposition reads

$\{\forall x \in T, p(x)\} \rightarrow \{\forall x \in T, \neg q(x)\}$

The negation of this is

$\{\forall x \in T, p(x)\} \wedge \{\exists x \in T, q(x)\}$

In words, this reads "All triangles are right angled and some triangles are equiangular".

Logical implication involving quantifiers

5. Prove that $\exists x, [p(x) \wedge q(x)] \Rightarrow \exists x, p(x) \wedge \exists x, q(x)$

Is the converse true

Solution:

Let S denote the universe, we find that

$\exists x, [p(x) \wedge q(x)] \Rightarrow p(a) \wedge q(a)$ for some $a \in S$

$\Rightarrow p(a)$, for $a \in S$ and $q(a)$ for some $a \in S$

$\Rightarrow \exists x, p(x) \wedge \exists x, q(x)$

This proves the required implication.

Next, we observe that $\exists x, p(x) \Rightarrow p(a)$ for some $a \in S$ and $\exists x, q(x) \Rightarrow q(b)$ for some $b \leftarrow S$.

Therefore, $\exists x, p(x) \wedge \exists x, q(x) \Rightarrow p(a) \wedge q(b)$

$\not\Leftrightarrow p(a) \wedge q(a)$ because b need not be a

Thus, $\exists x, [p(x) \wedge q(x)]$ need not be true when $\exists x, p(x) \wedge \exists x, q(x)$ is true.

That is $\exists x, p(x) \wedge \exists x, q(x) \not\Leftrightarrow [p(x) \wedge q(x)]$

Accordingly, the converse of the given implication is not necessarily true.

6. Find whether the following arguments is valid:

No engineering student of first or second semester studies logic

<u>Anil is a student who studies logic</u>.

$\therefore$ Anil is not in second semester

Solution:

Let us take the universe to be the set of all engineering students

p(x): x is in first semester.

q(x): x is in second semester.

r(x): x studies logic.

Then the given argument reads

$$\frac{\begin{array}{c}\forall x, [\{p(x) \vee q(x)\} \rightarrow \neg r(x)] \\ r(a)\end{array}}{\therefore \neg q(a)}$$

We note that

$\forall x, [\{p(x) \vee q(x)\} \rightarrow \neg r(x)] \Rightarrow \{p(a) \vee q(a)\} \rightarrow \neg r(a)$

By rule of universal specification.

Therefore,

$[\forall x, \{p(x) \vee q(x)\} \rightarrow \neg r(x)] \wedge r(a)$

$\Rightarrow [\{p(a) \vee q(a)\} \rightarrow \neg r(a)] \wedge r(a)$

$\Rightarrow r(a) \wedge [r(a) \rightarrow \neg [p(a) \vee q(a)]]$, Using Commutative law and Contrapositive

$\Rightarrow \neg [p(a) \vee q(a)]$, By the Modus Pones law

$\Rightarrow \neg p(a) \wedge \neg q(a)$, By De Morgan's law

$\Rightarrow \neg q(a)$, by the rule of conjunctive specification,

This proves that the given argument is valid.

7. Find whether the following argument is valid.
If a triangle has 2 equal sides then, it is isosceles.
If the triangle is isosceles, then it has 2 equal angles.
<u>A certain triangle ABC does not have 2 equal angles.</u>
$\therefore$ the triangle ABC does not have 2 equal sides.

Solution:

Let the universe be set of all triangles

And let p(x):x has equal sides.

q(x): x is isosceles.

r(x): x has 2 equal angles.

Also let C denote the triangle ABC.

Then, in symbols, the given argument reads as follows:

$\forall x, [p(x) \rightarrow q(x)]$

$\forall x, [q(x) \rightarrow r(x)]$

$\underline{\neg r(c)}$

$\therefore p(c)$

We note that

$\forall x, [p(x) \rightarrow q(x)] \wedge \{\forall x, [q(x) \rightarrow r(x)]\} \wedge \neg r(c)$

$\Rightarrow \{\forall x, [p(x) \rightarrow r(x)] \wedge \neg r(c)\}$, By Rule of Syllogism

$\Rightarrow \{[p(c) \rightarrow r(c)] \wedge \neg r(c)\}$, By Rule of Universal Specification

$\Rightarrow \neg p(c)$ By Modus Tollens Rule

This proves that the given argument is valid.

8. Prove that the following argument is valid.

$\forall x, [p(x) \vee q(x)]$
$\exists x, \neg p(x)$
$\forall x, [\neg q(x) \vee r(x)]$
$\forall x, [s(x) \rightarrow \neg r(x)]$
$\therefore \exists x, \neg s(x)$

Solution:

We note that

$\{\forall x, [p(x) \vee q(x)]\} \wedge [\exists x, \neg p(x)]$
$\Rightarrow [p(a) \vee q(a)] \wedge \neg p(a)$ For some as in the universe
$\Rightarrow q(a)$ By Disjunctive Syllogism

Therefore, $\{\forall x, [p(x) \vee q(x)]\} \wedge [\exists x, \neg p(x)] \wedge \{\forall x, [\neg q(x) \vee r(x)]\}$
$\Rightarrow q(a) \wedge [\neg q(a) \vee r(a)]$
$\Rightarrow r(a)$ By Rule of Disjunctive Syllogism

Consequently,

$\{\forall x, [p(x) \vee q(x)]\} \wedge \{\exists x, \neg p(x)\} \wedge \{\forall x, [\neg q(x) \vee r(x)]\} \wedge \{\forall x, [s(x) \rightarrow \neg r(x)]\}$
$\Rightarrow r(a) \wedge \{s(a) \rightarrow \neg r(a)\}$
$\Rightarrow \neg s(a)$ By Modus Tollens rule
$\Rightarrow \exists x, \neg s(x)$.

This proves the given argument is valid.

Quantified statements with more than one variable

9. Determine the truth value of each of the following quantified statements. The universe being the set of all non-zero integer.

i) $\exists x, \exists y [xy=1]$
ii) $\exists x \forall y [xy=1]$
iii) $\forall x \exists y [xy=1]$
iv) $\exists x, \exists y, [(2x+y=5) \wedge (x-3y=-8)]$
v) $\exists x, \exists y, [(3x-y=17) \wedge (2x+4y=3)]$

Solution: (i) true (take x=1, y=1)

(ii) False (for specified x, xy=1 for every y is not true)

(iii) false (for x=2, there is no integer y such that xy=1)

(iv) true (take x=1, y=3)

(v) false (equation 3x-y=17 and 2x+4y=3 do not have a common integer solution)

☻ **Methods of proof and methods of disproof:**

Direct proof:

1. **Hypothesis:** first assume that p is true.
2. **Analysis:** starting with the hypothesis and employ the rules/ Laws of logic and other known facts infer that q is true.
3. **Conclusion:** $p \rightarrow q$ is true.

Indirect proof:

A conditional $p \rightarrow q$ and its contrapositive $\neg q \rightarrow \neg p$ is logically equivalent. In some situations, given a condition $p \rightarrow q$, a direct proof of the contrapositive $\neg q \rightarrow \neg p$ is easier. On the basis of this proof, we infer that the conditional $p \rightarrow q$ is true. This method of proving a conditional is called an indirect method of proof.

Proof by contradiction:

1. **Hypothesis:** assume that $p \rightarrow q$ is false, that is assume that p is true and q is false.
2. **Analysis:** starting with the hypothesis that q is false and employing the rules of logics and other known facts, this infer that p is false. This contradicts the assumption that p is true.
3. **Conclusion:** because of the contradiction arrived in the analysis, we infer that $p \rightarrow q$ is true.

Proof by exhaustion:

Recall that a proposition of the form "$\forall x \in S, p(x)$" is true if p(x) is true for every x in S. if S consists of only a limited number of elements, we can prove that the statement "$\forall x \in S, p(x)$" is true by considering p(a) for each a in S and verifying that p(a) is true (in each case). Such a method of proof is called the method of exhaustion.

Disproof by counter example:

The way of disproving a proposition involving the universal quantifiers is to exhibit just one case where the proposition is false. This method of disproof is called disproof by counter example.

Problems:

1. Prove that, for all integers k and l, if k and l are both odd the k+l is even and kl is odd.

Solution:

Take any two integers k and l, and assume that both of these are odd (hypothesis)

Then k=2m+1, l=2n+! for some integers m and n. therefore,

$k+1= (2m+1) +(2n+1) = 2(m+n+1)$

$kl= (2m+1)(2n+1) = 4mn+2(m+n)+1$

We observe that k+l is divisible by 2 and kl is not divisible by 2. Therefore k+l is an even integer and kl is an odd integer.

Since k and l are arbitrary integers, the proof of the given statement is complete.

2. For each of the following statements, provide an indirect proof by stating and proving the contrapositive of the given statement.
(i) for all integers k and l, if kl is odd then both k and l are odd.
(ii) for all integers k and l if k+l is even, then k and l are both even or both odd.

Solution:

The contrapositive of the given statement is

"For all integers k and l, if k is even or l is even then kl is even.

We now prove this contrapositive.

For any integers k and l, assume that k is even.

Then k=2m for some integer m, and kl=(2m)l=2(ml) which is evidently even. Similarly if l is even, then kl=k(2n)=2kn for some integer n so that kl is even. This proves the contrapositive.

This proof of contrapositive serves as an indirect proof of the given statement.

(ii). Here, the contrapositive of the given statement is

"for all integers k and l, if one of k and l and is odd and the other is even, then k+l is odd"

We now prove this contrapositive

For any odd integers k and l, assume that, one of k and l is odd and the other is even.

Suppose k is odd and l is even. Then k=2m+1 and l=2n for some integers m and n. consequently k+l=(2m+1)+2n which is evidently odd.

Similarly, if k is even and l is odd, we find that k+l is odd. This proves the contrapositive.

This proof of contrapositive serves as an indirect proof of the given statement.

3. Give (i) direct proof (ii) indirect proof (iii) proof by contradiction for the following statement: "if n is an odd integer, then n+9 is an even integer".

Solution:

(i) Direct proof: assume that n is an odd integer. Then n=2k+1 for some integer k. This gives n+9 = (2k+1)+9 = 2(k+5) from which it is evident that n+9 is even. This establishes the truth of the given statement by a direct proof.

(ii) Indirect proof: assume that n+9 is not an even integer. Then n+9 = 2k+1 for some integer k. This gives n = (2k+1)-9=2(k-4), which shows that n is even. Thus, if n+9 is not even, then n is not odd. This proves the contrapositive of the given statement. This proof of the contrapositive serves as an indirect proof of the given statement.

(iii) proof by contradiction: assume that the given statement is false. That is, assume that n is odd and n+9 is odd, n+9=2k+1 for some integer k so that n=(2k+1)-9= 2(k-4) which shows that n is even. This contradicts the assumption that n is odd. Hence the given statement must be true.

4. Prove that every even integer n with $2 \leq n \leq 26$ can be written as a sum of most three perfect squares.

Solution:

Let S={2, 4, 6, …., 24, 26}. We have to prove that the statement: "$\forall$ x $\in$ S, p(x)" is true, where p(x): x is a sum of at most three perfect squares.

We observe that

$2=1^2+1^2$	$16=4^2$
$4=2^2$	$18=4^2+1^2+1^2$
$6=2^2+1^2+1^2$	$20=3^2+3^2+1^2+1^2$
$8=2^2+2^2$	$22=3^2+3^2+2^2$
$10=3^2+1^2$	$24=4^2+2^2+2^2$
$12=2^2+2^2+2^2$	$26=5^2+1^2$
$14=3^2+2^2+1^2$	

The above facts verify that each x in S is a sum of at most three-perfect square.

5. Prove or disprove that the sum of square of any four non-zero integers is an even integer.

Solution:

Here the proposition is

"For any four non-zero integers a, b, c, d and $a^2+b^2+c^2+d^2$ is an even integer".

We check that for a=1, b=1, c=1, d=2 the proposition is false. Thus, the given proposition is not a true proposition. This proposition is disproved through the counter example a=b=c=1 and d=2.

6. Consider the following statement for the universe of integers if n is an integer then $n^2=n$ or $\forall n \{n^2=n\}$.

Solution:

For n=0 it is true that $n^2=0^2=0=n$ and if n=1 is also true that $n^2=1^2=1=n$. however we cannot conclude that $n^2=n$ for every integer n.

The rule of universal generalisation does not apply here, for we cannot consider the choices of 0 (or 1) as an arbitrarily chosen integer. If n=2, $n^2=4 \neq n=2$, and this one counter example is enough to tell us that the given statement is false.

However, either replacement namely n=0 or n=1 is not enough to establish the truth of the statement. For some integer n, $n^2=n$ or $\exists$ n $\{n^2=n\}$.

7. For all positive integers x and y if the product xy exceeds 25, then x>5 or y>5.

Solution:

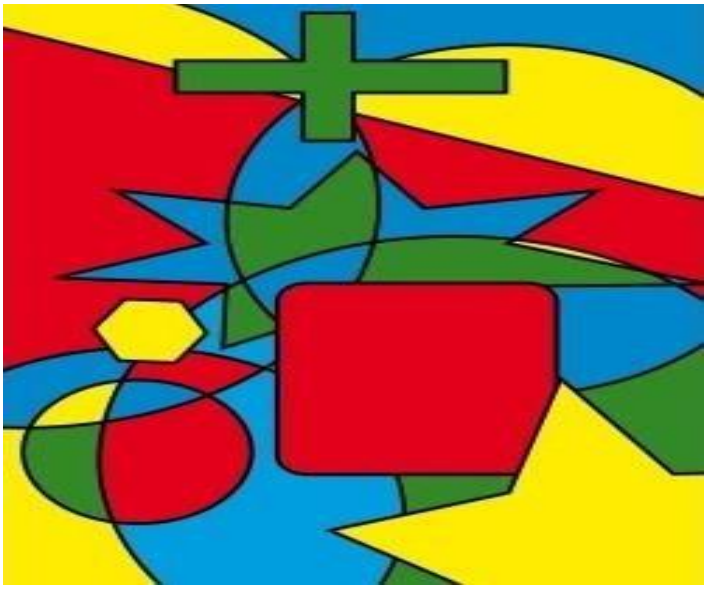
Consider the negation of the conclusion that is suppose that $0 < x \leq 5$ and $0 < y \leq 5$. Under these circumstances we find that $0 < x \cdot y < 5 \cdot 5 = 25$.

So, the product of xy does not exceed 25.

BCS405A

Discrete Mathematical Structures

(For the 4th Semester Computer Science and Engineering Stream)



Module 2

Properties of Integers & Principles of Counting

Content

MODULE 2

PROPERTIES OF INTEGERS & PRINCIPLES OF COUNTING

☻ **Syllabus:**

Properties of the Integers: The Well Ordering Principle – Mathematical Induction.

Fundamental Principles of Counting: The Rules of Sum and Product, Permutations, Combinations – The Binomial Theorem, Combinations with Repetition.

☻ Mathematical Induction:

Mathematical induction is a mathematical proof technique. It is essentially used to prove that a statement $P(n)$ holds for every natural number $n = 0, 1, 2, 3, \ldots \ldots$ i.e., the overall statement is a sequence of infinitely many cases $P(0), P(1), P(3), \ldots \ldots \ldots$

Well ordering principle:

Every non empty subset of Z^+contains a smallest element. (we often express this by saying that Z^+ is well ordered).

Finite induction principle (principle of Mathematical induction):

Let $S(n)$ denote an open mathematical statement that involves one or more occurrences of the variable n. Which represents a positive integer

(a) If $S(1)$ is true; and

(b) If whenever $S(k)$is true (for some particular but arbitrarily chosen $k \in Z^+$), then $S\ (k+1)$is true, then $S(n)$ is true for all $n \in Z^+$.

Proof:

Let $S(n)$ be such an open statement satisfying conditions (a) and (b) and let $F = \{t \in Z^+ / \ S(t)$ is false$\}$. We wish to prove that $F = \emptyset$ so to obtain a contradiction we assume that $F \neq \emptyset$. Then by the well-ordering Principle, F has a least element. Since $S(1)$ is true. It follows that $S \neq 1$. so $s > 10$, and consequently $s - 1 \in Z^+$. With $s - 1 \notin F$, $S(s-1)$ we have true. So, by condition (b) it follows that $S((s-1)+1) = S(s)$ is true, contradicting $s \in F$. This contradiction arose from the assumption that $F \neq \emptyset$. Consequently $F = \emptyset$.

Problems:

1. Prove by mathematical induction that, for all positive integers $n \geq 1$.

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

Solution:

Here, we have to prove the statement

$$S(n) = 1 + 2 + 3 + \cdots\cdots\cdots + n = \frac{1}{2}n(n+1) \text{ for all integers } n \geq 1.$$

Basic step: We note that $S(1)$ is the statement

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

Which is clearly true. thus, the statement $S(n)$is verified for $n = 1$.

Induction step: We assume that the statement $S(n)$ is true for $n = k$ where k is an integer ≥ 1; that is, we assume that the following statement is true:

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

Using this we find that (by adding $(k+1)$ to both side)

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

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

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

This is precisely the statement $S(k+1)$. Thus, on the basis of the assumption that $S(n)$ is true for $n = k \geq 1$, the truth ness of $S(n)$ for $n = k+1$ is established.

2. Prove that, for each $n \in Z^+$ $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

OR

Prove that, for each $n \in Z^+$, $1^2 + 2^2 + 3^2 + \cdots\cdots\cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Solution:

Let S(n) denote the given statement.

Basic step: We note that is $S(1)$ is the statement

$$1^2 = \frac{1}{6} \cdot 1 \cdot (1+1) \cdot (2+1) \text{ which is clearly true.}$$

Induction Step: We assume that the statement $S(n)$ is true for $n = k$ where k is an integer ≥ 1; that is, we assume that the following statement is true.

$$S(k) = 1^2 + 2^2 + 3^2 + \cdots\cdots\cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Adding $(k+1)^2$ to both sides of this, we obtain

$$S(k) = 1^2 + 2^2 + 3^2 + \cdots\cdots\cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$

$$= (k+1)\{\frac{k\,(2k+1)}{6} + (k+1)\}$$

$$= \frac{1}{6}(k+1)\{k(2k+1)+6(k+1)\}$$

$$= \frac{1}{6}(k+1)\{2k^2+k+6k+6\}$$

$$= \frac{1}{6}(k+1)\{2k^2+7k+6\}$$

$$= \frac{1}{6}(k+1)(k+2)(2k+3)$$

This is precisely the statement $S(k+1)$. Thus, on the basis of the assumption that $S(n)$ is true for $n = k \geq 1$, the truth ness of $S(n)$ for $n = k+1$ is established.

3. By mathematical induction, Prove That $(n!) \geq 2^{n-1}$ for all integers$n \geq 1$.

Solution:

<u>Basic step</u>: For $n = 1$, $S(n)$ reads $(1!) \geq 2^{1-1}$ which is obviously true. Thus $S(n)$ is verified for $n = 1$.

<u>Induction step</u>: We assume that $S(n)$ is true for $n = k$, where k is an integer ≥ 1; that is, we assume that

$(k!) \geq 2^{k-1}$, or $2^{k-1} \leq k!$ is true

$2^k = 2 \cdot 2^{k-1} \leq 2 \cdot k!$

$\leq (k+1) \cdot k!$, because $2 < (k+1)$ for $k \geq 1$

$= (k+1)!$

$(k+1)! \geq 2^k$

This is precisely the statement $S(n)$ for $n = k+1$. Thus, on the assumption that $S(n)$is true for $n = k \geq 1$, We have proved that $S(n)$ is true for $n = k+1$.

Hence, by mathematical induction, it follows that the statement $S(n)$ is true for all integers $n \geq 1$.

4. Prove that every positive integer $n \geq 24$ can be written as a sum of 5's and/or 7's.

Solution:

<u>Basic step</u>: We note that $24 = (7+7)+(5+5)$

This shows $S(24)$ is true.

<u>Induction step</u>: We assume that $S(n)$ is true for $n = k$ where $k \geq 24$. Then

$k = (7+7+\cdots\cdots)+(5+5+\cdots\cdots)$

Suppose this representation of k has r number of 7's and s number of 5's. Since $k \geq 24$ we should have $r \geq 2$ and $s \geq 2$.

Using this representation of k, we find that

$$k+1=\{\underbrace{(7+7+\cdots\cdots)}_{r}+\underbrace{(5+5+\cdots\cdots)}_{s}\}+1$$

$$=\{\underbrace{(7+7+\cdots\cdots)}_{r-2}+(7+7)+\underbrace{(5+5+\cdots\cdots)}_{s}\}+1$$

$$=\{\underbrace{(7+7+\cdots\cdots)}_{r-2}+\underbrace{(5+5+\cdots\cdots)}_{s+3}\}$$

This shows that $k+1$is sum of 7's and 5's. Thus, $S(k+1)$ is true.

5. Prove by mathematical induction that, for all positive integers $n \geq 1$.

$$1\cdot 2+2\cdot 3+3\cdot 4+\cdots\cdots\cdots+n(n+1)=\frac{1}{3}n(n+1)(n+2)$$

Solution:

Here, we have to prove the statement

$S(n)=1\cdot 2+2\cdot 3+3\cdot 4+\cdots\cdots\cdots+n(n+1)=\frac{1}{3}n(n+1)(n+2)$ for all integers $n \geq 1$.

<u>Basic step:</u> We note that $S(1)$ is the statement

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

Which is clearly true. thus, the statement $S(n)$is verified for $n=1$.

<u>Induction step</u>: We assume that the statement $S(n)$ is true for $n=k$ where k is an integer ≥ 1; that is, we assume that the following statement is true:

$$S(k)=1\cdot 2+2\cdot 3+3\cdot 4+\cdots\cdots\cdots+k(k+1)=\frac{1}{3}k(k+1)(k+2)$$

Using this we find that (by adding $(k+1)(k+2)$ to both side)

$$S(k)=1\cdot 2+2\cdot 3+3\cdot 4+\cdots\cdots\cdots+k(k+1)+(k+1)(k+2)$$

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

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

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

This is precisely the statement $S(k+1)$. Thus, on the basis of the assumption that $S(n)$ is true for $n=k\geq 1$, the truth ness of $S(n)$ for $n=k+1$ is established.

6. Prove, by mathematical induction that $1^2+3^2+5^2+\cdots\cdots\cdots+(2n-1)^2=\frac{n(2n-1)(2n+1)}{3}$ for all integers $n \geq 1$.

Solution:

Let S(n) denote the given statement.

<u>Basic step</u>: We note that is $S(1)$ is the statement

$$1^2 = \frac{1}{3} \cdot 1 \cdot (2-1) \cdot (2+1) \text{ which is clearly true.}$$

<u>Induction Step</u>: We assume that the statement $S(n)$ is true for $n = k$ where k is an integer ≥ 1; that is, we assume that the following statement is true.

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

Adding $(2k+1)^2$ to both sides of this, we obtain

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

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

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

$$= \frac{1}{3}((2k+1)\{2k^2 - k + 6k + 3\}$$

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

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

This is precisely the statement $S(k+1)$. Thus, on the basis of the assumption that $S(n)$ is true for $n = k \geq 1$, the truth ness of $S(n)$ for $n = k+1$ is established.

7. Prove by mathematical induction that, for all positive integers $n \geq 1$.

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots\cdots\cdots + n(n+2) = \frac{1}{6}n(n+1)(2n+7)$$

Solution:

Here, we have to prove the statement

$S(n) = 1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots\cdots\cdots + n(n+2) = \frac{1}{6}n(n+1)(2n+7)$ for all integers $n \geq 1$.

<u>Basic step:</u> We note that $S(1)$ is the statement

$$1 \cdot 3 = \frac{1}{6} \cdot 1 \cdot (1+1) \cdot (2+7)$$

Which is clearly true. thus, the statement $S(n)$is verified for $n = 1$.

<u>Induction step</u>: We assume that the statement $S(n)$ is true for $n = k$ where k is an integer ≥ 1; that is, we assume that the following statement is true:

$$S(k) = 1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots\cdots\cdots + k(k+2) = \frac{1}{6}k(k+1)(2k+7)$$

Using this we find that (by adding $(k+1)(k+3)$ to both side)

$$S(k) = 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots\cdots\cdots + k(k+2) + (k+1)(k+3) = \frac{1}{6}k(k+1)(2k+7) + (k+1)(k+3)$$

$$= (k+1)\{\frac{1}{6}k(2k+7) + (k+3)\}$$

$$= (k+1)\{2k^2 + 7k + 6k + 18\}$$

$$= (k+1)\{2k^2 + 13k + 18\}$$

$$= \frac{1}{6}(k+1)(k+2)(2k+9)$$

This is precisely the statement $S(k+1)$. Thus, on the basis of the assumption that $S(n)$ is true for $n = k \geq 1$, the truth ness of $S(n)$ for $n = k+1$ is established.

8. Prove that every positive integer greater than or equal to 14 can be written as a sum of 3's and/or 8's.

Solution:

<u>Basic step</u>: We note that $14 = (3+3) + 8$

This shows $S(14)$ is true.

<u>Induction step</u>: We assume that $S(n)$ is true for $n = k$ where $k \geq 14$. Then

$$k = (3 + 3 + \cdots\cdots) + (8 + \cdots\cdots)$$

Suppose this representation of k has r number of 3's and s number of 8's. Since $k \geq 14$ we should have $r \geq 2$ and $s \geq 2$.

Using this representation of k, we find that

$$k + 1 = \{\underbrace{(3 + 3 + \cdots\cdots)}_{r} + \underbrace{(8 + \cdots\cdots)}_{s}\} + 1$$

$$= \{\underbrace{(3 + 3 + \cdots\cdots)}_{r} + \underbrace{(8 + \cdots\cdots)}_{s-1} + 8\} + 1$$

$$= \{\underbrace{(3 + 3 + \cdots\cdots)}_{r+3} + \underbrace{(8 + \cdots\cdots)}_{s-1}\}$$

This shows that $k+1$is sum of 3's and 8's. Thus, $S(k+1)$ is true.

9. Prove by mathematical induction for any integer $n \geq 1$

$$\frac{1}{2 \cdot 5} + \frac{1}{5 \cdot 8} + \cdots\cdots\cdots + \frac{1}{(3n-1)(3n+2)} = \frac{n}{6n+4}$$

Solution:

Here, we have to prove the statement

$$S(n) = \frac{1}{2\cdot 5} + \frac{1}{5\cdot 8} + \cdots\cdots\cdots + \frac{1}{(3n-1)(3n+2)} = \frac{n}{6n+4} \text{ for all integers } n \geq 1.$$

<u>Basic step:</u> We note that $S(1)$ is the statement

$$\frac{1}{2\cdot 5} = \frac{1}{6\cdot 1+4}$$

Which is clearly true. thus, the statement $S(n)$is verified for $n = 1$.

<u>Induction step</u>: We assume that the statement $S(n)$ is true for $n = k$ where k is an integer ≥ 1; that is, we assume that the following statement is true:

$$S(k) = \frac{1}{2\cdot 5} + \frac{1}{5\cdot 8} + \cdots\cdots\cdots + \frac{1}{(3k-1)(3k+2)} = \frac{k}{6k+4}$$

Using this we find that (by adding $\frac{1}{(3k+2)(3k+5)}$ to both side)

$$S(k) = \frac{1}{2\cdot 5} + \frac{1}{5\cdot 8} + \cdots\cdots\cdots + \frac{1}{(3k-1)(3k+2)} + \frac{1}{(3k+2)(3k+5)} = \frac{k}{6k+4} + \frac{1}{(3k+2)(3k+5)}$$

$$= \frac{k(3k+2)(3k+5)+(6k+4)}{(6k+4)(3k+2)(3k+5)}$$

$$= \frac{9k^3+21k^2+16k+4}{(6k+4)(3k+2)(3k+5)}$$

$$= \frac{(k-1)(3k+2)^2}{(6k+4)(3k+2)(3k+5)}$$

$$= \frac{(k+1)(3k+2)}{(6k+4)(3k+5)}$$

This is precisely the statement $S(k+1)$. Thus, on the basis of the assumption that $S(n)$ is true for $n = k \geq 1$, the truth ness of $S(n)$ for $n = k+1$ is established.

10. Prove by mathematical induction that, for every positive integer n, 5 divides $n^5 - n$

Solution:

Let $S(n)$ be the given statement.

<u>Basic step:</u> We note that $S(1)$ is the statement

5 divides $1^5 - 1$

Since $1^5 - 1 = 0$, this statement is true

<u>Induction step</u>: We assume that the statement $S(n)$ is true for $n = k$ where k is an integer ≥ 1; that is, we assume that the following statement is true:

5 divides $k^5 - k$,

This means that $k^5 - k$ is a multiple of 5; that is $k^5 - k = 5m$, for some positive integer m.

Consequently, we find that

$$(k+1)^5 - (k+1) = (k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1) - (k+1)$$

$$= (k^5 - k) + 5(k^4 + 2k^3 + 2k^2 + k)$$

$$= 5m + 5(k^4 + 2k^3 + 2k^2 + k)$$

$$= 5(m + k^4 + 2k^3 + 2k^2 + k)$$

This shows that $(k+1)^5 - (k+1)$ is a multiple of 5; that is, 5 divides $(k+1)^5 - (k+1)$.

This is precisely the statement $S(n)$ for $n = k + 1$. Thus, on the assumption that $S(n)$is true for $n = k \geq 1$, We have proved that $S(n)$ is true for $n = k + 1$.

☻ **<u>Recursive Definition</u>:**

For describing a sequence, the two methods are commonly used.

(i) Explicit method (ii) Recursive method

In explicit method, the general term of the sequence is explicitly indicated

In recursive method, first few terms of the sequence must be indicated explicitly and in the second part the rule which will enable us to obtain new term if the sequence from the terms already known must be indicated.

Problems:

1. Find an explicit definition of the sequence defined recursively by

$a_1 = 7, a_n = 2a_{n-1} + 1$ for $n \geq 2$.

Solution: By repeated use of the given recursive definition we find that

$$a_n = 2a_{n-1} + 1 = 2\{2a_{n-2} + 1\} + 1$$

$$= 2\{2(2a_{n-3} + 1) + 1\} + 1 = 2^3 a_{n-3} + 2^2 + 2 + 1$$

$$\cdots\cdots\cdots$$

$$\cdots\cdots\cdots$$

$$= 2^{n-1} a_{n-(n-1)} + 2^{n-2} + 2^{n-3} + \cdots\cdots + 2^2 + 2 + 1$$

$$= 2^{n-1} a_1 + (1 + 2 + 2^2 + 2^3 + \cdots\cdots + 2^{n-3} + 2^{n-2})$$

Using $a_1 = 7$ and the standard result

$1 + a + a^2 + a^3 + \cdots\cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$ for $a > 1$

This becomes $a_n = 7 \cdot 2^{n-1} + \frac{2^{n-1} - 1}{2 - 1} = 8 \cdot 2^{n-1} - 1$

2. Obtain the recursive definition for the sequence $\{a_n\}$ is each of the following cases.

$(i). a_n = 5n$ $(ii). a_n = 6^n$ $(iii). a_n = 3n + 7$

$(iv). a_n = n(n + 2)$ $(v). a_n = n^2$ $(vi). a_n = 2 - (-1)^n$

Solution:

(i). Here $a_1 = 5, a_2 = 10, a_3 = 15, a_4 = 20, \ldots\ldots\ldots$

We can rewrite these as $a_1 = 5$ and $a_n = a_{n-1} + 5$ for $n \geq 2$.

This is the Recursive definition of the given sequence.

(ii). Here $a_1 = 6, a_2 = 6^2, a_3 = 6^3, a_4 = 6^4, \ldots\ldots\ldots$

We can rewrite these as $a_1 = 6$ and $a_{n+1} = 6a_n$ for $n \geq 1$.

This is the Recursive definition of the given sequence.

(iii). Here $a_1 = 10, a_2 = 13, a_3 = 16, a_4 = 19, \ldots \ldots \ldots$

We can rewrite these as $a_1 = 10$ and $a_n = a_{n-1} + 3$ for $n \geq 2$.

This is the Recursive definition of the given sequence.

(iv). Here $a_1 = 3, a_2 = 8, a_3 = 15, a_4 = 24, \ldots \ldots \ldots$

We observe that $a_2 - a_1 = 5 = 2 \cdot 1 + 3, a_3 - a_2 = 7 = 2 \cdot 2 + 3, a_4 - a_3 = 9 = 2 \cdot 3 + 3$

We can rewrite these as $a_{n+1} - a_n = 2n + 3$ then $a_{n+1} = a_n + 2n + 3$ for $n \geq 1$.

Hence $a_1 = 3$ and $a_{n+1} = a_n + 2n + 3$ for $n \geq 1$.

This is the Recursive definition of the given sequence.

(v). Here $a_1 = 1, a_2 = 4, a_3 = 9, a_4 = 16, \ldots \ldots \ldots$

We observe that $a_2 - a_1 = 3 = 2 \cdot 1 + 1, a_3 - a_2 = 5 = 2 \cdot 2 + 1, a_4 - a_3 = 7 = 2 \cdot 3 + 1$

We can rewrite these as $a_{n+1} - a_n = 2n + 1$ then $a_{n+1} = a_n + 2n + 1$ for $n \geq 1$.

Hence $a_1 = 1$ and $a_{n+1} = a_n + 2n + 1$ for $n \geq 1$.

This is the Recursive definition of the given sequence.

(vi). Here $a_1 = 3, a_2 = 1, a_3 = 3, a_4 = 1, \ldots \ldots \ldots$

We observe that $a_2 - a_1 = -2 = 2\,(-1), a_3 - a_2 = 2 = 2(1), a_4 - a_3 = -2 = 2(-1)$

We can rewrite these as $a_{n+1} - a_n = 2(-1)^n$ then $a_{n+1} = a_n + 2(-1)^n$

Hence $a_1 = 3$ and $a_{n+1} = a_n + 2(-1)^n$ for $n \geq 1$.

This is the Recursive definition of the given sequence.

3. The Fibonacci numbers are defined recursively by $F_0 = 0, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ Evaluate F_2 to F_{10}

Solution:

Given $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

$F_2 = F_1 + F_0 = 1 + 0 = 1$

$F_3 = F_2 + F_1 = 1 + 1 = 2$

$F_4 = F_3 + F_2 = 2 + 1 = 3$

$F_5 = F_4 + F_3 = 3 + 2 = 5$

$F_6 = F_5 + F_4 = 5 + 3 = 8$

$F_7 = F_6 + F_5 = 8 + 5 = 13$

$F_8 = F_7 + F_6 = 13 + 8 = 21$

$F_9 = F_8 + F_7 = 21 + 13 = 34$

$F_{10} = F_9 + F_8 = 34 + 21 = 55$

Note: The Sequence formed by the Fibonacci numbers is called the Fibonacci sequence.

4. The Lucas numbers are defined recursively by $L_0 = 2, L_1 = 1$ and $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$

Evaluate L_2 to L_{10}

Solution:

Given $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$

$L_2 = L_1 + L_0 = 1 + 2 = 3$

$L_3 = L_2 + L_1 = 3 + 1 = 4$

$L_4 = L_3 + L_2 = 4 + 3 = 7$

$L_5 = L_4 + L_3 = 7 + 4 = 11$

$L_6 = L_5 + L_4 = 11 + 7 = 18$

$L_7 = L_6 + L_5 = 18 + 11 = 29$

$L_8 = L_7 + L_6 = 29 + 18 = 47$

$L_9 = L_8 + L_7 = 47 + 29 = 76$

$L_{10} = L_9 + L_8 = 76 + 47 = 123$

Note: The Sequence formed by the Lucas numbers is called the Lucas sequence.

5. For the Fibonacci sequence $F_0, F_1, F_2, \ldots \ldots \ldots \ldots$ Prove that $F_n = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]$

Solution:

For $n = 0$ and $n = 1$, the required results read (respectively)

$F_0 = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^0 - (\frac{1-\sqrt{5}}{2})^0] = \frac{1}{\sqrt{5}}[1 - 1] = 0$

$F_1 = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2}) - (\frac{1-\sqrt{5}}{2})] = \frac{1}{\sqrt{5}}[\sqrt{5}] = 1$

Which is true.

Thus, the required result is true for $n = 0$ and $n = 1$. We assume that the result is true for $n = 0, 1, 2, \ldots . k$, where $k \geq 1$. Then, we find that

$F_{k+1} = F_k + F_{k-1}$

$F_{k+1} = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k} - (\frac{1-\sqrt{5}}{2})^{k}] + \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k-1} - (\frac{1-\sqrt{5}}{2})^{k-1}]$ using the assumption made

$F_{k+1} = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k-1}\{\frac{1+\sqrt{5}}{2} + 1\} - (\frac{1-\sqrt{5}}{2})^{k-1}\{\frac{1-\sqrt{5}}{2} + 1\}]$

$F_{k+1} = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k-1}\{\frac{3+\sqrt{5}}{2}\} - (\frac{1-\sqrt{5}}{2})^{k-1}\{\frac{3-\sqrt{5}}{2}\}]$

$F_{k+1} = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k-1}\{\frac{6+2\sqrt{5}}{4}\} - (\frac{1-\sqrt{5}}{2})^{k-1}\{\frac{6-2\sqrt{5}}{4}\}]$

$F_{k+1} = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^{k+1} - (\frac{1-\sqrt{5}}{2})^{k+1}]$

This shows that the required result is true for $n = k + 1$. Hence by mathematical induction, the result is true for all non – negative integers n.

☻ The Rules of Sum and Product:

Rule of sum:

Suppose two tasks T_1 and T_2 are to be performed. if the task T_1 can be performed in m different ways and the task T_2 can be performed in n different ways and if these two tasks cannot be performed simultaneously, then one of the two tasks (T_1 or T_2) can be performed in $m + n$ ways.

Example: Suppose T_1 is the task of selecting a prime no. < 10 and T_2 is the task of selecting an even number < 10. then T_1 can be performed in 4 ways and T_2 can be performed in 4 ways. But since 2 is both a prime and an even number < 10 the task T1 or T_2 can be performed in 4 + 4 – 1 = 7 ways.

Rule of product:

Suppose two tasks are to be performed one after the other. If T_1 can be performed in n_1 different ways, and for each of these ways T_2 can be performed in $n_2$different ways. then both of the tasks can be performed in $n_1 * n_2$ different ways.

Example: Suppose a person has 8 shirts and 5 ties. Then He has 8 * 4 = 40 different ways of choosing a shirt and a tie.

Problems:

1. Cars of a particular manufacturer come in 4 models, 12 colours, 3 engine sizes and 2 transmission types (a) how many distinct cars can be manufactured? (b) of these how many have the same colour?

Solution:

(a) By the product rule, it follows that the number of distinct cars that can be manufactured is 4*12*3*2 =288

(b) for any chosen colour, the number of distinct cars that can be manufactured is 4*3*2=24

2. A bit is either 0 or 1. A byte is a sequence of 8 bits. Find (i) the number of bytes. (ii) the number of bytes that begin with 11 and end with 11. (iii) The number of bytes that begin with 11 and do not end with 11. (iv) the number of bytes that begin with 11 or end with 11.

Solution:

(i) Since each byte contains 8 bits and each bit is 0 or 1, the number of bytes is $2^8 = 256$

(ii) In a byte beginning and ending with 11, there occur 4 open positions. These can be filled un $2^4 = 16$ ways. Therefore, there are 16 bytes which begin and end with 11.

(iii) These occur 6 open positions in a byte beginning with 11. these positions can be filled is $2^6 = 64$ ways. thus, there are 64 bytes that begin with 11. since there are 16 bytes that begin and end with 11, the number of bytes that begin with 11 but do not end with 11 is 64-16 = 48.

(iv) As in (iii) the numbers of bytes that end with 11 is 64. Also, the number of bytes that begin and end with 11 is 16. Therefore, the number of bytes that begin or end with 11 is 64 + 64 = 16 = 112.

3. Find the number of 3 digit even numbers with no repeated digits.

Solution:

Here we consider number of the form $x\ y\ z$, where each of x, y, z represents a digit under the given restrictions. Since $x\ y\ z$ has to be even, z has to be 0, 2, 4, 6 or 8. If z is 0, then x has 9 choices and $y\ z$ has 2, 4, 6, 8 (4 choices) then x has 8 choices (Note that x cannot be 0). Therefore, z and x can be chosen in $1 \times 9 + 4 \times 8 = 41$ ways. For each of these ways, y can be chosen in 8 ways.

Hence, the desired number is 41 * 8 = 328.

4. Find the number of proper divisors of 441000.

Solution:

We note that $441000 = 2^3 \times 3^2 \times 5^3 \times 7^2$. Therefore, every divisor of $n = 441000$ must be of the form $d = 2^p \times 3^q \times 5^r \times 7^s$ where $0 \leq p \leq 3, 0 \leq q \leq 2, 0 \leq r \leq 3, 0 \leq s \leq 2$.

Thus, for a divisor d, p can be chosen in 4 ways, q in 3 ways, r in 4 ways and s in 3 ways. Accordingly, the number of possible d's is $4 \times 3 \times 4 \times 3 = 144$. Of these, two divisors (namely 1 and n) are not proper divisors. Therefore, the number of proper divisors of the given number is $144 - 2 = 142$.

5. How many among the first 100,000 positive integers contain exactly one 3, one 4 and one 5 in their decimal representations?

Solution:

The number 100000 does not contain 3 or 4 or 5. Therefore, we have to consider all possible positive integers with 5 places that meet the given conditions. In a 5-place integer the digit 3 can be in any one of the 5 places. Subsequently, the digit 4 can be in any one of the 4 remaining places. Then the digit 5 can be in any one of the 3 remaining places. There are 2 places left and either of these may be filled by 5 digits (digits from 0 to 9 other tan 3, 4, 5). Thus, there are $5 \times 4 \times 3 \times 7 \times 7 = 2940$ integers of the required type.

☻ **<u>Permutations</u>:**

Suppose that we are given n distinct objects and wish to arrange r of these objects in a line. Since there are n ways of choosing the first object, and after this done $n-1$ ways of choosing the second object…. And finally, $n-r+1$ ways of choosing r^{th} object, it follows by the product rule of counting (stated in the preceding section) that the number of different arrangements, or permutations (as they are commonly called) is $n(n-1)(n-2)\cdots\cdots\cdots(n-r+1)$. We denote this number by $P(n,r)$ and is referred to as the number of permutations of size r of n objects.

$$\boldsymbol{P(n,r)=\frac{n!}{(n-r)!}}$$

<u>Generalization</u>

Suppose it is required to find the number of permutations that can be formed from a collection of n objects of which n_1 are of one type , n_2 are of a second type ,…… n_k are of kth type, with $n_1+n_2+\cdots\cdots+n_k=n$. Then, the number of permutations of the objects is

$$\boldsymbol{\frac{n!}{n_1!\,n_2!\cdots\cdots n_k!}}$$

Problems:

1. Four different mathematics books, five different computer science books and two different control theory books are to be arranged in a shelf. How many different arrangements are possible if (a) The books in each particular subject must be together? (b) Only mathematics books must be together?

Solution:

(a) The mathematics books can be arranged among themselves in 4! Ways, the computer science books in 5! Ways the control theory books in 2! Ways, and the three groups in 3! Ways. Therefore, the number of possible arrangements is 4! * 5! * 2! * 3! = 34560.

(b) Consider the 4 mathematics boos as one single book. Then we have 8 books which can be arranged in 8! Ways. In all of these ways the mathematics books are together. But the mathematics books can be arranged among themselves in 4! Ways. Hence, the number of arrangements is 8! * 4! = 967680

2. Find the number of permutations of the letters of the word MASSASAUGA. In how many of these, all four ‘A’s are together? How many of them begin with S?

Solution:

The given word has 10 letters of which 4 are A, 3 are S and 1 each are M, U and G. Therefore, the required number of permutations is

$$\frac{10!}{4!*3!*1!*1!*1!}=25200$$

It is a permutation all A’s are to be together, we treat all of A’s as one single letter. Then the letters to be permuted read (AAAA), S, S, S, M, U, G (which are 7 in number) and the number of permutations is

$$\frac{7!}{1! * 3! * 1! * 1! * 1!} = 840$$

For permutations beginning with S, there occur nine open positions to fill, where two are S, four are A, and one each of M, U, G. The number of such permutations is

$$\frac{9!}{2! * 4! * 1! * 1! * 1!} = 7560$$

3. (a) How many arrangements are there for all letters in the word SOCIOLOGICAL?

(b) In how many of these arrangements (i) A and G are adjacent? (ii) all the vowels are adjacent?

Solution:

(a) The given word has 12 letters of which three are O, two each are C, I, L and one each are S, A, G. Therefore, the number of arrangements of these letters is

$$\frac{12!}{3! * 2! * 2! * 2! * 1! * 1! * 1!} = 25200$$

(b)

(i) If, in an arrangement, A and G are to be adjacent, we treat A and G together as a single letter, say X so that we have three numbers of O's, two each of C, L, I and one each of S and X, totalling 11 letters. These can be arranged in $\frac{11!}{3!*2!*2!*2!*1!}$ Ways

Further the letters A and G can be arranged among themselves in two ways.

Therefore, the total number of arrangements in this case is

$$\frac{11!}{3! * 2! * 2! * 2! * 1!} \times 2 = 1663200$$

(ii) If, in an arrangement, all the vowels are to be adjacent, we treat all the vowels present in the given word (A, O, I) as a single letter, say Y, so that we have two each of C and L and one each of S, G & Y totalling to 7 letters. These can be arranged in $\frac{7!}{2!*2!*1!*1!*1!}$ ways

Further, since the given words contains 3 O's, two I's and one A, the letters A, O, I (clubbed as Y) can be arranged among themselves is $\frac{6!}{3!*2!*1!}$ Ways.

Therefore, the total number of arrangements in this case is $\frac{7!}{2!*2!*1!*1!*1!} \times \frac{6!}{3!*2!*1!} = 75600$

4. How many Positive integers n can we form using the digits 3, 4, 4, 5, 5, 6, 7 if we want n to exceed 5,000,000?

Solution:

Here n must be of the form $n = x_1x_2x_3x_4x_5x_6x_7$

Where $x_1, x_2, \dots\dots, x_7$ are the given digits with $x_1 = 5, 6\ or\ 7$. Suppose we take $x_1 = 5$. Then where $x_2x_3x_4x_5x_6x_7$ is an arrangement of the remaining 6 digits which contains two 4's and one each of 3, 5, 6, 7. The number of such arrangements is

$$\frac{6!}{1!\,2!\,1!\,1!\,1!} = 360$$

Similarly, we take $x_1 = 6$. Then where $x_2x_3x_4x_5x_6x_7$ is an arrangement of the remaining 6 digits which contains two each of 4 & 5 and one each of 3 & 7. The number of such arrangements is

$$\frac{6!}{1!\,2!\,2!\,1!} = 180$$

Similarly, we take $x_1 = 7$. Then where $x_2x_3x_4x_5x_6x_7$ is an arrangement of the remaining 6 digits which contains two each of 4 & 5 and one each of 3 & 6. The number of such arrangements is

$$\frac{6!}{1!\,2!\,2!\,1!} = 180$$

Accordingly, by the Sum Rule, the number of n's of the desired type is $360 + 180 + 180 = 720$.

5. How many numbers greater than 1,000,000 can be formed by using the digits 1, 2, 2, 2, 4, 4, 0?

Solution:

Here n must be of the form $n = x_1x_2x_3x_4x_5x_6x_7$

Where $x_1, x_2, \dots\dots, x_7$ are the given digits with $x_1 = 1, 2\ or\ 4$. Suppose we take $x_1 = 1$. Then where $x_2x_3x_4x_5x_6x_7$ is an arrangement of the remaining 6 digits which contains three 2's and two 4's. The number of such arrangements is

$$\frac{6!}{3!\,2!} = 60$$

Similarly, we take $x_1 = 2$. Then where $x_2x_3x_4x_5x_6x_7$ is an arrangement of the remaining 6 digits which contains two 2's and two 4's. The number of such arrangements is

$$\frac{6!}{2!\,2!} = 180$$

Similarly, we take $x_1 = 4$. Then where $x_2x_3x_4x_5x_6x_7$ is an arrangement of the remaining 6 digits which contains three 2's and one 4. The number of such arrangements is

$$\frac{6!}{3!\,1!} = 120$$

Accordingly, by the Sum Rule, the number of n's of the desired type is $60 + 180 + 120 = 360$.

☻ **<u>Combinations</u>:**

Suppose we are interested in selecting (choosing) a set of r objects from a set of $n \geq r$ objects without regard to order. The set of r objects being selected is traditionally called a Combination of r objects (or briefly r-combination).

The total number of combinations of r-different objects that can be selected from n different objects can be obtained by proceeding in the following way. Suppose this number is equal to C, say; that is, suppose there is a total of C number of combinations of r different objects chosen from n different objects. Take any one of these combinations. The r objects in this combination can be arranged in $r!$ Different ways. Since there are C combinations, the total number of permutations is $C \cdot r!$. But this is equal to $P(n,r)$. Thus,

$$\boldsymbol{C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{(n-r)!\,r!} \quad \text{for } 0 \leq r \leq n}$$

Problems:

1. A certain question paper contains two parts A and B each containing 4 questions. How many different ways a student can answer 5 questions by selecting at least 2 questions from each part?

Solution: The different ways a student can select his 5 questions are.

(i) 3 questions from part A and 2 questions from part B. this can be done in $C(4,3) * C(4,2) = 24$ ways.

(ii) 2 questions from part A and 3 questions from part B. this can be done in $C(4,2) * C(4,3) = 24$ ways.

Therefore, the total number of ways a student can answer 5 questions under given restrictions is 24 + 24 = 48.

2. Prove the following identities.

$$C(n,r-1) + C(n,r) = C(n+1,r)$$

$$C(m,2) + C(n,2) = C(m+n,2) - mn$$

Proof:

(i). $C(n,r-1) + C(n,r) = \frac{n!}{(r-1)!\,(n-r+1)!} + \frac{n!}{r!\,(n-r)!}$

$$= \frac{n!}{(r-1)!\,(n-r)!}\left\{\frac{1}{n-r+1} + \frac{1}{r}\right\}$$

$$= \frac{n!}{(r-1)!\,(n-r)!} \cdot \frac{n+1}{r\,(n-r+1)}$$

$$= \frac{(n+1)!}{r!\,(n-r+1)!}$$

$$= C(n+1,r)$$

(ii). $C(m,2) + C(n,2) = \frac{m!}{(m-2)! \cdot 2} + \frac{n!}{(n-2)! \cdot 2}$

$$= \frac{1}{2}\{m(m-1) + n(n-1)\}$$

$$= \frac{1}{2}\{m^2 + n^2 - m - n\}$$

$$= \frac{1}{2}(m+n)(m+n-1) - mn$$

$$= \frac{(m+n)!}{2\,(m+n-2)!} - mn$$

$$= C(m+n, 2) - mn$$

3. A woman has 11 close relatives and she wishes to invite 5 of them to dinner. In how many ways can she invite them in the following situations:

(i). There is no restriction on the choice.

(ii). Two particular persons will not attend separately.

(iii). Two particular persons will not attend together.

Solution:

(i). Since there is no restriction on the choice of invitees, five out of 11 can be invited in

$$C(11, 5) = \frac{11!}{6!\,5!} = 462 \text{ ways}$$

(ii). Since two particular persons will not attend separately, they should both be invited or not invited.

Suppose if both of them are invited, then three are more invitees are to be selected from the remaining 9 relatives. This can be done in

$$C(9, 3) = \frac{9!}{6!\,3!} = 84 \text{ ways}$$

Suppose if both of them are not invited, then five invitees are to be selected from the remaining 9 relatives. This can be done in

$$C(9, 5) = \frac{9!}{5!\,4!} = 126 \text{ ways}$$

Therefore, the total number of ways in which the invitees can be selected in this case is $84 + 126 = 210$.

(iii). Since two particular persons (Say P_1 & P_2) will not attend together, only one of them can be invited or none of them can be invited. The number of ways of choosing the invitees with P_1 invited is

$$C(9, 4) = \frac{9!}{5!\,4!} = 126 \text{ ways}$$

Similarly, the number of ways of choosing the invitees with P_2 invited is 126 ways

If both P_1 & P_2 are not invited, then the number of ways of inviting the invitees is

$$C(9, 5) = \frac{9!}{5!\,4!} = 126 \text{ ways}$$

Therefore, the total number of ways in which the invitees can be selected in this case is

$$126 + 126 + 126 = 378.$$

4. Find the number of arrangements of all the letters in TALLAHASSEE. How many of these arrangements have no adjacent A's?

Solution:

The number of letters in the given word is 11 of which 3 are A's, 2 each are L's, S's, E's and 1 each are T and H. Therefore, the number of arrangements (permutations) of the letters in the given word is

$$\frac{11!}{3!\,2!\,2!\,2!\,1!\,1!} = 831600$$

If we disregard the A's, the remaining 8 letters can be arranged in

$$\frac{8!}{2!\,2!\,2!\,1!\,1!} = 5040$$

In each of these arrangements, there are 9 possible locations for the three A's. These locations can be chosen in $C(9,3)$ ways. Therefore, the number of arrangements having no adjacent A's is

$$5040 \times C(9,3) = 5040 \times \frac{9!}{3!\,6!} = 5040 \times 84 = 423360$$

5. A committee of 12 is to be selected from 10 men and 10 women. In how many ways can the selection be carried out if
(a) there are no restrictions?
(b) there must be six men and six women?
(c) there must be an even number of women?
(d) there must be more women than men?
(e) there must be at least eight men?

Solution:

(a). If there is no restriction than it is a simple selection of 12 out of 20.

$$C(20,12) = \frac{20!}{12!\,8!} = 125970$$

(b). For 6 men out of 10 and 6 women out of 10. These are two different stages of selection that's why product rule is used

$$C(10,6) \times C(10,6) = \frac{10!}{6!\,4!} \times \frac{10!}{6!\,4!} = 44100$$

(c). 2, 4, 6, 8 or 10 can be the number of women in committee and corresponding to that men will be 10, 8, 6, 4 and 2.

$C(10,2) \times C(10,10) + C(10,4) \times C(10,8) + C(10,6) \times C(10,6) + C(10,8) \times C(10,4) + C(10,10) \times C(10,2) = 63090$

(d). Number of women can be 7, 8, 9 or 10 and number of men will be 5, 4, 3, 2 respectively.

$C(10,7) \times C(10,5) + C(10,8) \times C(10,4) + C(10,9) \times C(10,3) + C(10,10) \times C(10,2) = 40935$

(e). Number of men can be 8, 9 or 10 in this case and respectively number of women can be 4, 3 and 2.

$C(10,8) \times C(10,4) + C(10,9) \times C(10,3) + C(10,10) \times C(10,2) = 10695$

☻ Binomial and Multinomial Theorems:

Binomial Theorem:

On the basic properties of $C(n,r) = \binom{n}{r}$ is that it is the coefficient of $x^r y^{n-r}$ and $x^{n-r}y^r$ in the expansion of the expression $(x+y)^n$, where x and y are real numbers. In other words,

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r} = \sum_{r=0}^{n} \binom{n}{r} x^{r-n} y^r$$

This result is known as the binomial theorem for a positive integral index.

Multinomial Theorem:

For positive integers n and k the coefficient of $x_1^{n1} x_2^{n2} x_3^{n3} \dots\dots\dots x_k^{nk}$ in the expansion of $(x_1 + x_2 + x_3 + \cdots\cdots\cdots + x_k)^n$ is $\frac{n!}{n_1!\, n_2!\, n_3! \dots\dots n_k!}$

Problems:

1. Find the coefficient of

(i) x^9y^3 in the expansion of $(2x-3y)^{12}$

(ii) x^{12} in the expansion of $x^3(1-2x)^{10}$

(iii) x^0 in the expansion of $(3x^2 - \frac{2}{x})^{15}$

Solution:

By the Binomial theorem, we have $(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r} = \sum_{r=0}^{n} \binom{n}{r} x^{r-n} y^r$

(i). $(2x-3y)^{12} = \sum_{r=0}^{12} \binom{12}{r} (2x)^r (-3y)^{12-r}$

$$= \sum_{r=0}^{12} \binom{12}{r} 2^r (-3)^{12-r} x^r y^{12-r}$$

In the expansion, the coefficient of x^9y^3 (which corresponds to $r=9$) is

$$\binom{12}{9} 2^9 (-3)^{12-9} = -2^9 \times 3^3 \times \frac{12!}{9! \cdot 3!}$$

$$= -2^9 \times 3^3 \times \frac{12 \times 11 \times 10}{6}$$

$$= -(2^{10} \times 3^3 \times 11 \times 10)$$

(ii). $x^3(1-2x)^{10} = \sum_{r=0}^{10} \binom{10}{r} (-2x)^r 1^{10-r}$

$$x^3(1-2x)^{10} = \sum_{r=0}^{10} \binom{10}{r} (-2)^r x^{r+3}$$

In the expansion, the coefficient of x^{12} (which corresponds to $r=9$) is

$\binom{10}{9}(-2)^9 = -(10 \times 2^9) = -5120$

(iii). $(3x^2 - \frac{2}{x})^{15} = \sum_{r=0}^{15} \binom{15}{r} (3x^2)^r (-\frac{2}{x})^{15-r}$

$= \sum_{r=0}^{15} \binom{15}{r} 3^r (-2)^{15-r} x^{3r-15}$

In the expansion, the coefficient of x^9y^3 (which corresponds to $r = 5$) is

$\binom{15}{5} 3^5(-2)^{15-5} = (-2)^{10} \times 3^5 \times \frac{15!}{5! \cdot 10!}$

$= 2^{10} \times 3^5 \times 3003$

2. Determine the coefficient of

(i) xyz^2 in the expansion of $(2x - y - z)^4$

(ii) $x^{11}y^4$ in the expansion of $(2x^3 - 3xy^2 + z^2)^6$

(iii) $x^2y^2z^3$ in the expansion of $(3x - 2y - 4z)^7$

(iv) $a^2b^3c^2d^5$ in the expansion of $(a + 2b - 3c + 2d + 5)^{16}$

(v) $w^3x^2yz^2$ in the expansion of $(2w - x + 3y - 2z)^8$

Solution:

By the multinomial theorem, we have $(x_1 + x_2 + x_3 + \cdots\cdots\cdots + x_k)^n$ is $\frac{n!}{n_1!\, n_2!\, n_3! \ldots\ldots n_k!}$

(i). The general term is the expansion of $(2x - y - z)^4$ is $\binom{4}{n_1,\ n_2,\ n_3} (2x)^{n_1}(-y)^{n_2}(-z)^{n_3}$

For $n_1 = 1, n_2 = 1, n_3 = 2$ this becomes

$\binom{4}{1,\ 1,\ 2} (2x)^1(-y)^1(-z)^2 = \binom{4}{1,\ 1,\ 2} (2)(-1)(-1)^2xyz^2$

This shows that the required coefficient is $\binom{4}{1,\ 1,\ 2} (2)(-1)(-1)^2 = \frac{4!}{1!\,1!\,2!} \times (-2) = -12$

(ii). The general term is the expansion of $(2x^3 - 3xy^2 + z^2)^6$ is $\binom{6}{n_1,\ n_2,\ n_3} (2x^3)^{n_1}(-3xy^2)^{n_2}(z^2)^{n_3}$

For $n_3 = 0, n_2 = 2, n_1 = 3$ this becomes

$\binom{6}{3,\ 2,\ 0} (2x^3)^3(-3xy^2)^2(z^2)^0 = \binom{6}{3,\ 2,\ 0} (2)^3(-3)^2(1)^0x^{11}y^4$

This shows that the required coefficient is $\binom{6}{3,\ 2,\ 0} (2)^3(3)^2 = \frac{6!}{3!\,2!} \times 72 = 4320$

(iii). The general term is the expansion of $(3x - 2y - 4z)^7$ is $\binom{7}{n_1,\ n_2,\ n_3} (3x)^{n_1}(-2y)^{n_2}(-4z)^{n_3}$

For $n_1 = 2, n_2 = 2, n_3 = 3$ this becomes

$$\binom{7}{2,\ 2,\ 3}(3x)^2(-2y)^2(-4z)^3 = \binom{7}{2,\ 2,\ 3}(3)^2(-2)^2(-4)^3x^2y^2z^3$$

This shows that the required coefficient is

$$\binom{7}{2,\ 2,\ 3}(3)^2(-2)^2(-4)^3 = \frac{7!}{2!\,2!\,3!} \times 9 \times 4 \times (-64) = -483840$$

(iv). The general term is the expansion of $(a + 2b - 3c + 2d + 5)^{16}$ is

$$\binom{16}{n_1,\ n_2,\ n_3,\ n_4,\ n_5}(a)^{n_1}(2b)^{n_2}(-3c)^{n_3}(2d)^{n_4}(5)^{n_5}$$

For $n_1 = 2, n_2 = 3, n_3 = 2, n_4 = 5, n_5 = 16 - (2 + 3 + 2 + 5) = 4$, this becomes

$$\binom{16}{2,\ 3,\ 2,\ 5,\ 4}(a)^2(2b)^3(-3c)^2(2d)^5(5)^4 = \binom{16}{2,\ 3,\ 2,\ 5,\ 4}(2)^3(-3)^2(2)^5(5)^4a^2b^3c^2d^5$$

This shows that the required coefficient is

$$\binom{16}{2,\ 3,\ 2,\ 5,\ 4}(2)^3(-3)^2(2)^5(5)^4 = \frac{16!}{2!\,3!\,2!\,5!\,4!} \times 2^8 \times 3^2 \times 5^4 = \frac{16!}{(4!)^2} \times 2^5 \times 3 \times 5^3$$

(v). The general term is the expansion of $(2w - x + 3y - 2z)^8$ is

$$\binom{8}{n_1,\ n_2,\ n_3,\ n_4}(2w)^{n_1}(-x)^{n_2}(3y)^{n_3}(-2z)^{n_4}$$

For $n_1 = 3, n_2 = 2, n_3 = 1, n_4 = 2$ this becomes

$$\binom{8}{3,\ 2,\ 1,\ 2}(2w)^3(-x)^2(3y)^1(-2z)^2 = \binom{8}{3,\ 2,\ 1,\ 2}(2)^3(-1)^2(3)^1(-2)^2)\ w^3x^2yz^2$$

This shows that the required coefficient is

$$\binom{8}{3,\ 2,\ 1,\ 2}(2)^3(-1)^2(3)^1(-2)^2) = \frac{8!}{3!\,2!\,1!\,2!} \times 2^3 \times 3 \times 2^2 = 161280$$

☻ **<u>Combinations with repetitions</u>:**

Suppose we wish to select, with repetition, a combination of r objects from a set of n distinct objects. The number of such selections is given by $C(n+r-1,r) \equiv \frac{(n+r-1)!}{r!\ (n-1)!} \equiv C(r+n-1,n-1)$.

In other words, $C(n+r-1,r) \equiv C(r+n-1,n-1)$ represents the number of combinations of m distinct objects, taken r at a time, with repetition allowed.

The following are other interpretations of this number:

$C(n+r-1,r) \equiv C(r+n-1,n-1)$ represents the number of ways in which r identical objects can be distributed among n distinct containers.

$C(n+r-1,r) \equiv C(r+n-1,n-1)$ represents the number of nonnegative integer solutions of the equation.

Problems:

1. In how many ways we can distribute 10 identical marbles among 6 distinct containers?

Solution:

The selection consists in choosing with repetitions $r = 10$ marbles for $n = 6$ distinct containers

The required number is $C(6+10-1,10) = C(15,10) = \frac{15!}{10!\ 5!} = 3003$

2. Find the number of non-negative integer solutions of the inequality $x_1 + x_2 + x_3 + \cdots + x_6 < 10$

Solution:

We have to find the number of nonnegative integer solutions of the equation

$$x_1 + x_2 + x_3 + \cdots + x_6 = 9 - x_7$$

where $9 - x_7 \leq 9$ so that x_7 is non negative integer. Thus, the required number in the number of nonnegative solutions of the equation.

$$x1 + x2 + x3 + \ldots\ldots + x7 = 9$$

This number is $C(7+9-1,9) = C(15,9) = \frac{15!}{9!\ 6!} = 5005$

3. In How many ways can we distribute 7 apples and 6 oranges among 4 children so that each child gets at least 1 apple?

Solution:

Suppose we first give 1 apple to each child. This exhausts 4 apples. The remaining 3 apples can be distributed among 4 children in $C(4+3-1,3) = C(6,3)$ ways. Also, 6 oranges can be distributed among the 4 children in $C(4+6-1,6) = C(9,6)$ ways. Therefore, by the product rule, the number ways of distributing the given fruits under the given condition is

$C(6,3) \times C(9,6) = \frac{6!}{3!\,3!} \times \frac{9!}{6!\,3!} = 20 \times 84 = 1680$

4. A message is made up of 12 different symbols and it is to be transmitted through a communication channel. In addition to the 12 symbols, the transmitter will also send a total of 45 blank spaces between the symbols, with at least three spaces between each pair of consecutive symbols. In how many ways can the transmitter send such a message?

Solution:

The 12 symbols can be arranged in 12! Ways. For each of these arrangements, there are 11 positions between the 12 symbols. Since there must be at least three spaces between successive symbols, 33 of the 45 spaces will be used up. The remaining 12 spaces are to be accommodated in 11 positions. This can be done in $C(11+12-1,12) = C(22,12)$ ways. Consequently, by the product rule, the required number is

$$12! \times C(22,12) = 12! \times \frac{22!}{12! \times 10!} = 3.097445 \times 10^{14}$$

5. In how many ways can one distribute eight identical balls into four distinct containers so that (i) no container is left empty? (ii) the fourth container gets an odd number of balls?

Solution:

(i). First, we distribute one ball in to each container. Then we distribute the remaining 4 balls into 4 containers. The number of ways of doing this is the required number. This number is

$$C(4+4-1,4) = C(7,4) = \frac{7!}{4! \times 3!} = 35$$

(ii). If the fourth container has o get an odd number of balls, we have to put 1 or 3 or 5 or 7 balls into it.

Suppose we put 1 ball into the fourth container and the remaining 7 balls can be put into the remaining three containers in

$C(3+7-1,7) = C(9,7)$ ways

Similarly, we put 3 balls into the fourth container and the remaining 5 balls can be put into the remaining three containers in

$C(3+5-1,5) = C(7,5)$ ways

Similarly, we put 5 balls into the fourth container and the remaining 3 balls can be put into the remaining three containers in

$C(3+3-1,3) = C(5,3)$ ways

Similarly, we put 7 balls into the fourth container and the remaining 1 ball can be put into the remaining three containers in

$C(3+1-1,1) = C(3,1)$ ways

Thus, the total number of ways of distributing the given balls so that the fourth container gets an odd number of balls is

$C(9,7)+C(7,5)+C(5,3)+C(3,1)=\frac{9!}{7!\times 2!}+\frac{7!}{5!\times 2!}+\frac{5!}{3!\times 2!}+\frac{3!}{1!\times 2!}=36+21+10+3=70$

6. Find the number of integer solutions of $x_1+x_2+x_3+x_4=32$ where $x_i\geq 0, 1\leq i\leq 4$.

Solution:

Given $x_1+x_2+x_3+x_4=32$, where $x_i\geq 0, 1\leq i\leq 4$.

The required number is $C(4+32-1,32)=C(35,32)=\frac{35!}{32!\times 3!}=6545$

7. Find the number of positive integer solutions of the equation $x_1+x_2+x_3=17$

Solution:

Given $x_1+x_2+x_3=17$, we require $x_i\geq 1, 1\leq i\leq 3$.

Let us set $y_1=x_1-1,\ y_2=x_2-1, y_3=x_3-1$, then y_1, y_2, y_3 are all nonnegative integers.

Then the given equation is reads $(y_1+1)+(y_2+1)+(y_3+1)=17$ or $y_1+y_2+y_3=14$

The required number is $C(3+14-1,14)=C(16,14)=\frac{16!}{14!\times 2!}=120$

8. Find the number of positive integer solutions of the equation $x_1+x_2+x_3+x_4+x_5=30$ where $x_1\geq 2, x_2\geq 3, x_3\geq 4, x_4\geq 2, x_5\geq 0$

Solution:

Given $x_1+x_2+x_3+x_4+x_5=30$

Let us set $y_1=x_1-2,\ y_2=x_2-3,\ y_3=x_3-4, y_4=x_4-2,\ y_5=x_5$ then y_1, y_2, y_3, y_4, y_5 are all nonnegative integers.

Then the given equation is reads

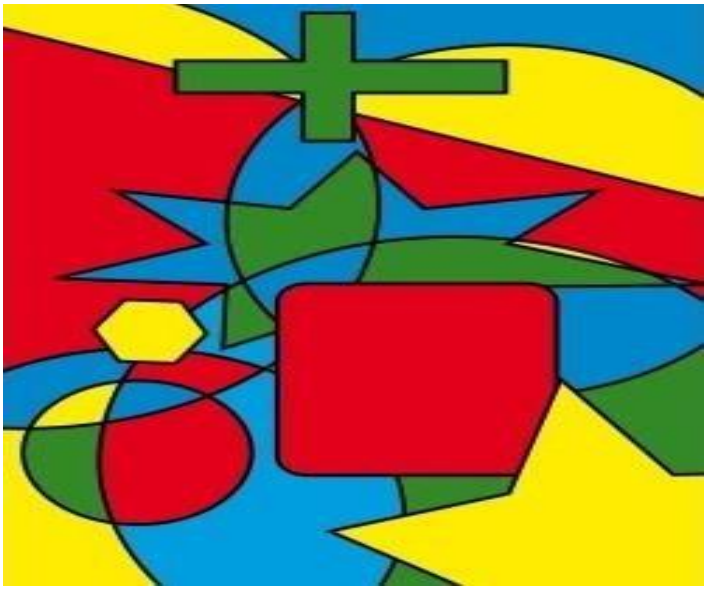
$(y_1+2)+(y_2+3)+(y_3+4)+(y_4+2)+(y_5+0)=30$ or $y_1+y_2+y_3+y_4+y_5=19$

The required number is $C(5+19-1,19)=C(23,19)=\frac{23!}{19!\times 4!}=8855$

BCS405A

Discrete Mathematical Structures

(For the 4th Semester Computer Science and Engineering Stream)



Module 3

Relations & Functions

Content

MODULE -3

RELATIONS AND FUNCTIONS

☻ **Syllabus:**

Relations and Functions: Cartesian Products and Relations, Functions – Plain and One-to One, Onto Functions. The Pigeon-hole Principle, Function Composition and Inverse Functions. **Relations:** Properties of Relations, Computer Recognition – Zero-One Matrices and Directed Graphs, Partial Orders – Hasse Diagrams, Equivalence Relations and Partitions.

☻ **<u>Cartesian Products</u>:**

For set $A, B \subseteq U$, the Cartesian product of A and B is denoted by $A \times B$ and equals $\{(a, b) \mid a \in A, b \in B\}$

Example: Let $U = \{1,2,3, \ldots .7\}, A = \{2,3,4\}, B = \{4,5\}$

Then (a). $A \times B = \{(2, 4), (2, 5), (3, 4), (3, 5), (4, 4), (4, 5)\}$

(b). $B^2 = B \times B = \{(4, 4), (4, 5), (5, 4), (5, 5)\}$

(c). $B^3 = B \times B \times B = \{(a, b, c) \mid a, b, c \in B\}$

☻ **<u>Relation</u>:**

For sets $A, B \subseteq U$ any subset of $A \times B$ is Called a Relation From A to B and any subset of $A \times A$ is called a Binary relation on A.

Example:

Let A and B be finite sets with $|B| = 3$. If there are 4096 relations from A to B what is $|A|$?

Solution: If $|A| = m$, $|B| = n$ then there are 2^{mn} relations from A to B.

Given $n = 3, 2^{mn} = 4096 \therefore m = 4 = |A|$.

☻ **<u>Functions</u>:**

Let **A** and **B** be two non-empty sets. Then a function **f** from **A** to **B** is a relation from A to B such that for each **a** in **A** there is a unique **b** in **B** such that $(\mathbf{a}, \mathbf{b})$ e **f**

<u>Types of Functions</u>:

(a). Floor function:

The function $f: R \to Z$, is given by

$f(x) = \lfloor x \rfloor =$ The greatest integer less than or equal to x.
$\lfloor 3.8 \rfloor = 3$
$\lfloor -3.8 \rfloor = -4$

(b). Ceiling Function:

The function $g: R \to Z$ is defined by $g(x) = \lceil x \rceil$

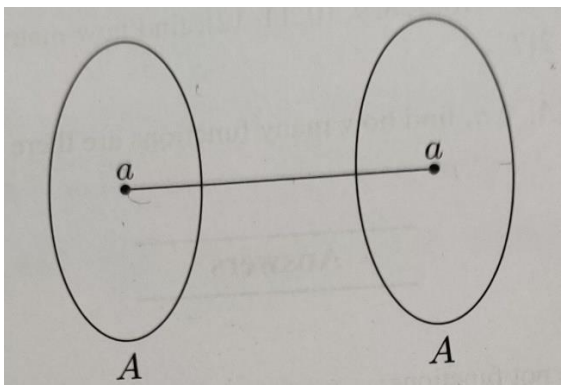
$\lceil 3 \rceil = 3, \lceil 3.01 \rceil = \lceil 3.7 \rceil = 4 = \lceil 4 \rceil$

$\lceil -3.01 \rceil = \lceil -3.7 \rceil = -3$

(c). Identity function:

A function $f: A \to A$ such that $f(a) = a$ for every $a \in A$ is called the identity function (or identity mapping) on A.

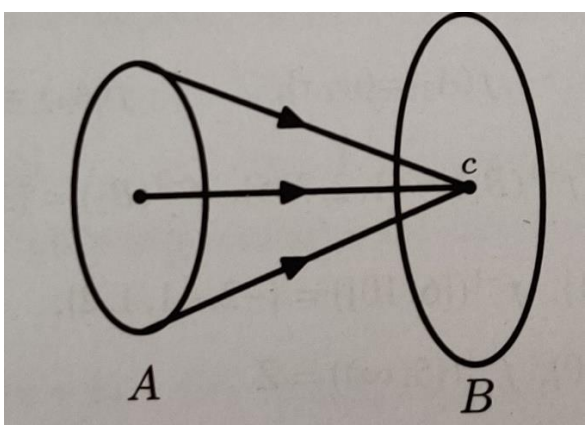
In other words, a function f on a set A is an identity function if the image of every element of A (under f) is itself.



(d). Constant function:

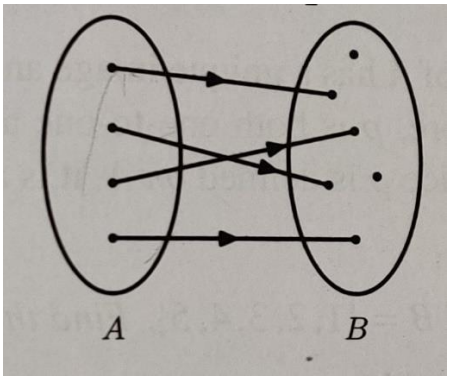
A function $f: A \to B$ such that $f(a) = c$ for every $a \in A$, where c is a fixed element of B, is called a Constant function.

In other words, a function f from A to B is a constant function if all elements of A have the same image (say c) in B.



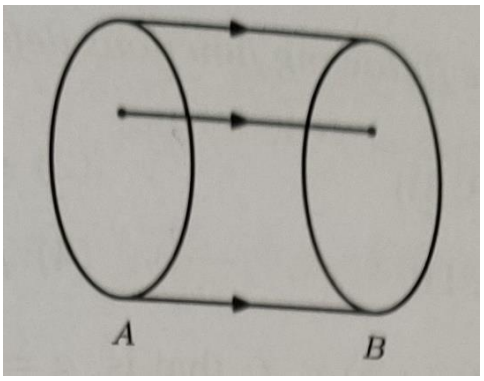
(e). Injective or one-to-one: A function $f: A \to B$ is called one-to-one, if each element of **B** appears at most once as the image of an element of **A**.

In other words, If different elements of A have different images in B under f; If whenever $f(a_1) = f(a_2)$ for $a_1, a_2 \in A$, then $a_1 = a_2$

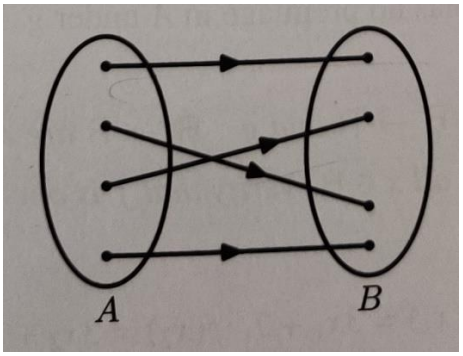


(f). Surjective or onto: A function $f: A \to B$ is called onto if for every element **b** of **B** there is an element **a** of **A** such that $f(a) = b$

In other words. f is an onto function from A to B if every element of B has a Preimage in A.



(g). Bijective or one-to-one correspondence: A function which is both one-to-one and onto is called Bijective.



Note: Number of one-to-one functions from A to B is

$P(n, m) = \frac{n!}{(n-m)!}$ Where $|A| = m, |B| = n$ & $m >= n$

Number of onto functions from A to B is

$$P(n,m) = \sum_{k=0}^{n} (-1)^k \binom{n}{n-k} (n-k)^m$$

Problems:

1. Let $A = \{1,2,3,4,5,6,7\}, B = \{w,x,y,z\}$. Find the number of Onto Functions from A to B.

Solution: Given $m = |A| = 7$ & $n = |B| = 4$

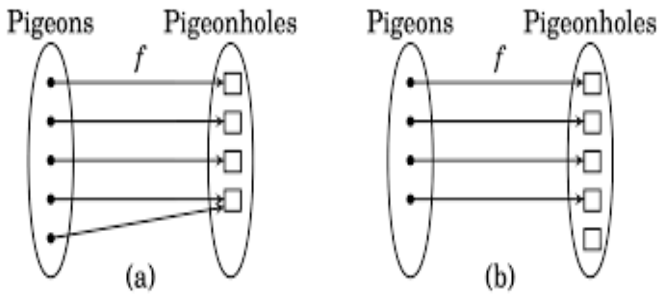
$$P(7,4) = \sum_{k=0}^{n} (-1)^k \binom{4}{4-k} (4-k)^7 = 8400$$

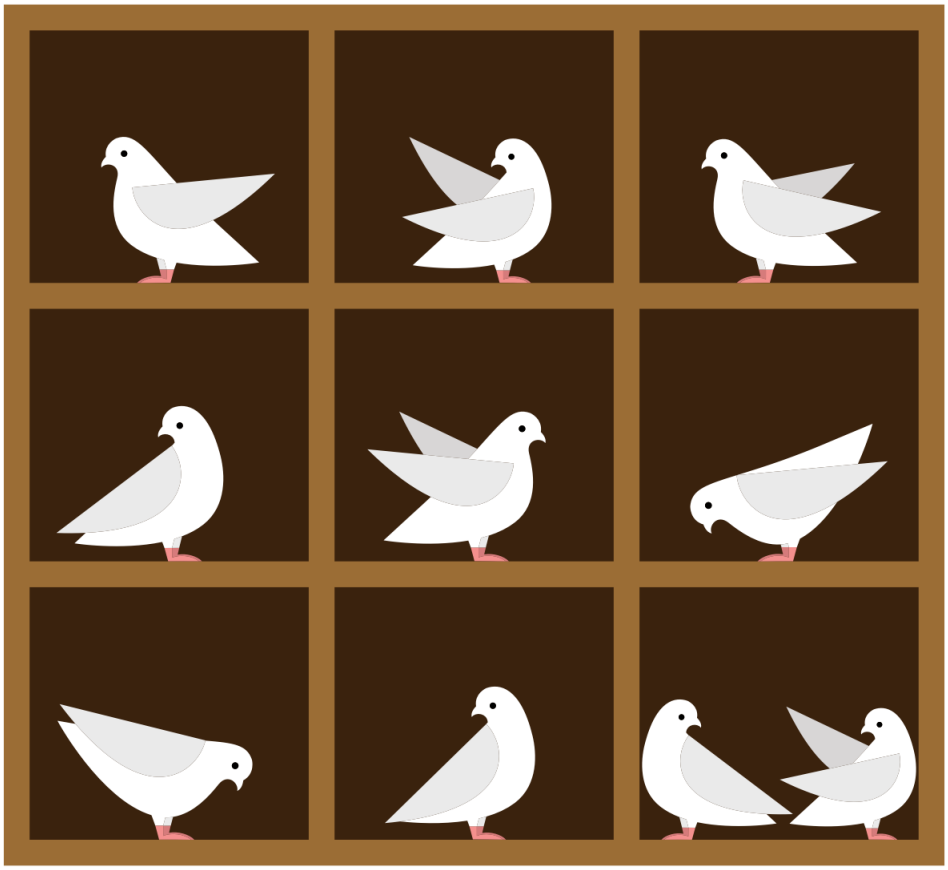
☻ **<u>Pigeonhole Principle</u>:**

If m pigeons occupy n pigeon holes and if $m > n$, then two or more pigeons occupy the same pigeonhole.

Generalization:

If m pigeons occupy n pigeonholes, then at least one pigeonhole must contain $(p + 1)$ or more pigeons, where $p = \lfloor \frac{(m-1)}{n} \rfloor$



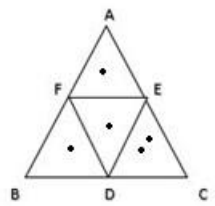


Problems:

1. ABC is an equilateral triangle whose sides are of length 1cm each. If we select 5 points inside the triangle, prove that at least 2 of these points are such that the distance between them is less than $\frac{1}{2}$ cm.

Solution:

Consider the triangle DEF formed by the mid points of the sides BC, CA and AB of the given triangle ABC. Then the triangle ABC is partition into 4 small equilateral triangles, each of which has sides equal to $\frac{1}{2}$ cm treating each of these four portions as a pigeonhole and 5 points chosen inside the triangle as pigeons, we find by using the pigeonhole principle that at least one portion must contain two or more points. Evidently the distance between such points is $< \frac{1}{2}$cm.



2. A magnetic tape contains a collection of 5 lakh strings made up to four or fewer number of English Letters can all the strings is the collection be distinct?

Solution:

Each place is an n letter string can be filled in 26 ways. Therefore, the possible number of strings made up of n letters is 26^n consequently, the total number of different possible strings made up of four or fewer letter is $26^4 + 26^3 + 26^2 + 26 = 4{,}75{,}254$.

Therefore, if there are 5 lakh strings in the tape, then at least one string is repeated. Thus, all the strings in the collection cannot be distinct.

3. Shirts numbered consecutively from 1 to 20 are worn by 20 students of a class. When any 3 of these students are chosen to be a debating team from the class, the sum of their shirt numbers is used as a code number of the team. Show that if any 8 of the 20 are selected, then from these 8 we may form at least two different teams having the same code number.

Solution:

From the 8 of the 20 students selected the numbers of teams of 3 students that can be formed is ${}^8C_3$=56. According to the way in which the code number of a team is determined, we note that the smallest possible code number is $1 + 2 + 3 = 6$ and the largest possible code number is $18 + 19 + 20 = 57$. Thus, the code number vary from 6 to 57, and these are 52 in number. As such only 52 code number are available for 56 possible teams, consequently by the pigeonhole principle, at least two different teams will have the same code number.

☻ **<u>Composition of functions</u>:**

Consider three non-empty sets A, B, C and the functions $f: A \to B$ and $g: B \to C$. the composition of these two functions is defined as the function $gof: A \to C$ with $(gof)(a) = g\{f(a)\}$ for all $a \epsilon A$.

Problems:

1. Consider the function f and g defined by $f(x) = x^3$ and $g(x) = x^2 + 1 \ \forall \ x \epsilon R$ find gof, fog, f^2 and g^2

Solution:

Here, both f and g are defined on R, therefore all of the functions $gof, fog, f^2 = fof$ and $g^2 = gog$ are defined on R and we find

$(gof)(x) = g\{f(x)\} = \ g(x^3) \ = \ (x^3)^2 + 1 = x^6 + 1$

$(fog)(x) = f\{g(x)\} = \ f(x^2 + 1) \ = \ (x^2 + 1)^3$

$f^2(x) = (fof)(x) = f\{f(x)\} = \ f(x^3) \ = \ (x^3)^3 = x^9$

$g^2(x) = (gog)(x) = g\{g(x)\} = g(x^2 + 1) = \ (x^2 + 1)^2 + 1$

2. Let f and g be function from R to R defined by $f(x) = ax + b$ and $g(x) = 1 - x + x^2$ if $(gof)(x) = 9x^2 - 9x + 3$ determine a, b.

Solution: We have $(gof)(x) = 9x^2 - 9x + 3 = g\{f(x)\}$

$= g\{ax + b\}$

$= 1 - (ax + b) + (ax + b)^{\ 2}$

$= a^2x^2 + (2ab - a)x + (1 - b + b^2)$

Comparing the corresponding coefficients

$$9 = a^2, 9 = a - 2ab, 3 = 1 - b + b^2.$$

$$a = \pm 3, \qquad b = -1,2$$

☻ **<u>Invertible Functions</u>:**

A function $f: A \to B$ is said to be invertible if there exists a function $g: B \to A$ such that $gof = I_A$ and $fog = I_B$ where I_A is the identity function on A and $I_B$is the identity function on B.

Problems:

1. Let $A = \{1,2,3,4\}$ and f and g be function From A to A given by $f = \{(1,4), (2,1), (3,2), (4,3)\}$ $g = \{(1,2), (2,3), (3,4), (4,1)\}$. Prove that f and g are inverse of each other.

Solution:

$$(gof)(1) = g\{f(1)\} = g(4) = 1 = I_A(1)$$

$$(gof)(2) = g\{f(2)\} = g(1) = 2 = I_A(2)$$

$$(gof)(3) = g\{f(3)\} = g(2) = 3 = I_A(3)$$

$$(gof)(4) = g\{f(4)\} = g(3) = 4 = I_A(4)$$

$$(fog)(1) = f\{g(1)\} = f(2) = 1 = I_B(1)$$

$$(fog)(2) = f\{g(2)\} = f(3) = 2 = I_B(2)$$

$$(fog)(3) = f\{g(3)\} = f(4) = 3 = I_B(3)$$

$$(fog)(4) = f\{g(4)\} = f(1) = 4 = I_B(4)$$

Thus, for all $x \epsilon A$, we have$(gof)(x) = I_A(x)$ and $(fog)(x) = I_B(x)$, therefore g is an inverse of f and f is an inverse of g.

2. Consider the function $f: R \to R$ defined by $f(x) = 2x + 5$. Let a function $g: R \to R$ be defined by $g(x) = \frac{1}{2(x-5)}$ Prove that g is an inverse of f.

Solution:

We check that for any $x \epsilon R$

$(gof)(x) = g[f(x)] = g(2x + 5)$

$= 1/2(2x + 5 - 5) = x = I_R(x)$

$(fog)(x) = f[g(x)] = f\{1/2(x - 5)\}$

$= 2\{1/2(x - 5)\} + 5 = x = I_R(x)$

☻ **Properties of Functions:**

<u>Theorem 1</u>: A function $f: A \to B$ is invertible if and only if one-to-one and onto.

Proof: Suppose that f is invertible then there exists a unique function $g: B \to A$ such that $gof = I_A$ and $fog = I_B$Take any a_1, $a_2 \epsilon A$ then

$$f(a_1) = f(a_2) \Rightarrow g\{f(a_1)\} = g\{f(a_2)\}$$

$$\Rightarrow (gof)(a_1) = (gof)(a2)$$

$$\Rightarrow I_A(a_1) = I_A(a_2)$$

$$\Rightarrow a_1 = a_2$$

This prove f is one-to-one

Next, take any $b \epsilon B$. Then $g(b) \epsilon A$ and $b = I_B(b)$

$$= (fog)(b) = f\{g(b)\}.$$

Thus, b is the image of an element $g(b) \epsilon A$ under f. therefore, f is onto as well.

Conversely, suppose that f is one-to-one and onto then for each $b \epsilon B$ there is a unique $a \epsilon A$ such that $b = f(a)$ now consider the function $g: B \to A$ defined by $g(b) = a$ then

$(gof)(a) = g\{f(a)\} = g(b) = a = I_A(a)$ and $(fog)(b) = f\{g(b)\} = f(a) = b = I_B(b)$

These show that f is invertible with g as the inverse. This completes the proof of the theorem.

<u>Theorem 2:</u> If $f: A \to B$ and $g: B \to C$ are invertible functions, then

$gof: A \to C$ is an invertible function and $(gof)^{-1} = f^{-1}og^{-1}$.

Proof: Since $\boldsymbol{f}$ and $\boldsymbol{g}$ are invertible functions; they are both one-to-one and onto consequently gof is both one-to-one and onto therefore, gof is invertible. Now the inverse f^{-1} of f is a function from B to A and the inverse g^{-1} of g is a function from C to B.

Therefore, if $h = f^{-1}og^{-1}$ then h is a function from C to A.

We find that

$$(gof)oh = (gof)o(f^{-1}og^{-1}) = go(fof^{-1})og^{-1} = goI_Bog^{-1}$$

$$= gog^{-1} = I_C$$

And

$$ho(gof) = (f^{-1}og^{-1})o(gof) = f^{-1}o(g^{-1}og)of = f^{-1}oI_Bof$$

$$= f^{-1}o\, f = I_A$$

The above expression show that h is the inverse of gof,

i.e., $h = (gof)^{-1}$. Thus $(gof)^{-1} = h = f^{-1}og^{-1}$ this completes the proof of the theorem.

☻ **<u>Zero-one matrices and Directed graphs</u>:**

Power of R:

Given a set A and a relation R on A we define the powers of R recursively by

(a) $RI = R$ (b) for $n \in Z^+, R^{n+1} = RoR^n$

Example:

If $A = \{1,2,3,4\}$ and $R = \{(1,2)\ (1,3)\ (2,4)\ (3,2)\}$ then $R^2 = \{(1,4),(1,2),(3,4)\}, R^3 = \{(1,4)\}$ and for $n \geq 4, R^n = \phi$.

Zero Matrix:

An $m \times n$ Zero-matrix $E = (e_{ij})_{m\times n}$ is a rectangular array of number arranged is m rows and n columns, where each e_{ij}, for $1 \leq i \leq m$ and $1 \leq i \leq n$ denote the entry is the i^{th}row and j^{th} column of E, and each such entry is 0 or 1.

$\boldsymbol{n \times n}$ $\boldsymbol{(0,1)}$ matrix:

For $n \in Z^+$, $I_n = (\delta_{ij})_{n\times \boldsymbol{n}}$ is the $n \times n$ (0,1)-matrix where

$$\delta_{ij} == \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

☻ **<u>Digraph of a relation</u>:**

Let V be a finite nonempty set. A directed graph G on V is made up of the elements of V, called the vertices or nodes of G, and a subset E, of $V \times V$ that contains the edges or arcs, of G. The set V is called the vertex set of G, the set E edge set. We then write $G = (V, E)$ to denote the graph.

If $a, b \in V$ and $(a, b) \in E$ then there is an edge from a to b vertex a is called the origin or source of the edge with b the terminus or terminating vertex and we say that b is adjacent from a and that a is adjacent to b. In addition, if $a \neq b$, then $(a, b) \neq (b, a)$. An edge of the form (a, a) is called a loop.

Problems:

1. Let $A = \{1,2,3,4\}$ and let R be the relation on A defined by xRy if and only if $y = 2x$.

   a) Write down R as asset of ordered pairs.

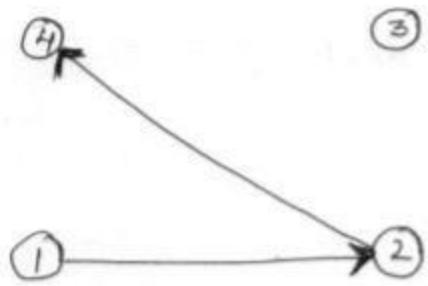
   b) Draw the digraph of R.

   c) Determine the in-degrees and out-degrees of the vertices in the digraph.

Solution:

a) We observe that for $x, y \in A, (x, y) \in R$ if and only if $y = 2x$. thus $R = \{(1,2),(2,4)\}$.

b) The digraph of R is as shown below



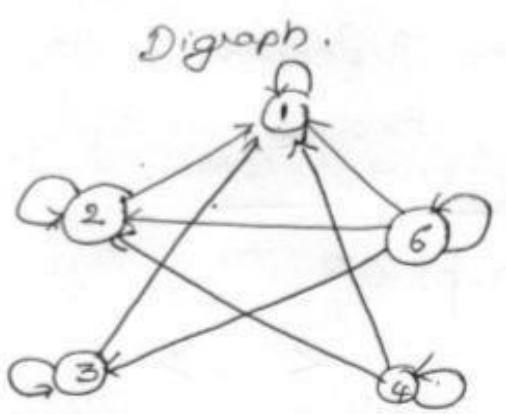
c) From the above digraph, we note that 3 is an isolated vertex and that for the vertex 1,2,4 the in-degrees and out-degrees are as shown in the table

Vertex	**1**	**2**	**4**
In-degree	0	1	1
Out-degree	1	1	0

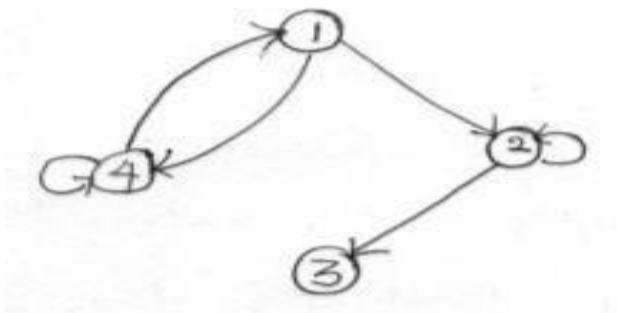
2. Let $A = \{1,2,3,4,6\}$ and R be a relation on A defined by aRb if and only if a is a multiple of b. Represent the relation R as a matrix and draw its digraph.

Solution: $R = \{(1,1),(2,1),(2,2),(3,1),(3,3),(4,1),(4,2),(4,4),(6,1),(6,2),(6,3),(6,6)\}$

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



3. Find the relation represented by the digraph given below. Also write down its matrix.



Solution:

By examining the given digraph which has 4 vertices, we note that the relation R represented by it is defined on the set $A = \{1,2,3,4\}$ and is given by $R = \{(1,2), (1,4), (2,2), (2,3), (4,1), (4,4)\}$. The matrix of R is

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

☻ **<u>Properties of Relations</u>:**

1. **Reflexive relation**:

A relation R on a set A is said to be reflexive, if $(a, a) \in R$, for all $a \in A$.

Example: $\leq$

2. **Irreflexive relation**:

A relation is said to be irreflexive, if $(a, a) \notin R$ for any $a \in A$.

Example: $<, >$

3. **Symmetric Relation:**

A relation R on a set is said to be symmetric, If $(b, a) \in R$ whenever $(a, b) \in R$ for all $a, b \in A$.

A relation which is not symmetric is called an **Asymmetric relation**.

Example: If $A = \{1,2,3\}$ and $R_1 = \{(1,1), (1,2), (2,1)\}$, $R_2 = \{(1,2), (2,1), (1,3)\}$

R_1 is symmetric and R_2 is asymmetric.

4. **Antisymmetric relation:**

A relation R on a set A is said to be antisymmetric, if whenever $(a, b) \in R$ and $(b, a) \in R$ then $a = b$.

Example: is less than or equal to.

5. **Transitive Relation:**

A relation on a set A is said to be transitive if whenever $(a, b) \in R$ and $(b, c) \in R$ then $(a, c\ ) \in R$ for all $a, b, c \in A$.

Examples:

1. Determine nature of the relations.

[1] $A = \{1,2,3\}$, $R_1 = \{(1,2), (2,1), (1,3), (3,1)\}$
- Symmetric but not reflexive.

[2] $R_2 = \{(1,1), (2,2), (3,3), (2,3)\}$
- Reflexive but not symmetric.

[3] $R_3 = \{(1,1), (2,2), (3,3)\}$
- Reflexive and symmetric.

[4] $R_4 = \{(1,1), (2,2), (3,3), (2,3), (3,2)\}$
- Both reflexive and symmetric.

[5] $R_5 = \{(1,1), (2,3), (3,3)\}$
- Neither reflexive nor symmetric

2. If $A = \{1,2,3,4\}$, $R_1 = \{(1,1),(2,3),(3,4),(2,4)\}$ is transitive $R_2 = \{(1,3),(3,2)\}$ is not transitive.

☻ **<u>Equivalence relation</u>:**

A relation that is reflexive, symmetric and transitive.

Problems:

1. A relation R on a set $A = \{a, b, c\}$ is represented by the following matrix.
   $M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ determine whether R is an Equivalence relation.

Solution: $R = \{(a,a),(a,c),(b,b),(c,c)\}$ we note that $(a,c) \in R$ but $(c,a) \notin R$

$\therefore$ R is not symmetric
$\therefore$R is not equivalence

2. For a fixed integer $n > 1$ prove that the relation congruent modulo n is an equivalence relation on the set of all integers Z.

Solution: For $a, b \in z$, we say that a is congruent to b modulo n if $a - b$ is a multiple of n or equivalently, $a - b = kn$ for some $k \in Z$.

Let us denote this relation by R so that aRb means $a \equiv b\ (mod\ n)$ we have to prove that R is an equivalence relation.

We note that for every $a \in Z$, $a - a = 0$ is a multiple of n ie, $a \equiv a(mod\ n), aRa$

R is reflexive. Next for all $a, b \in z$

$aRb \rightarrow a \equiv b\ mod\ n.$

$\rightarrow a - b$ is a multiple of n

$\rightarrow b - a$ is a multiple of n

$\rightarrow b \equiv a\ mod\ n$
$\rightarrow bRa$
R is symmetric.

Lastly, we note that for all $a, b, c \in Z$
aRb and $bRc \Rightarrow a \equiv b(mod\ n)$ and $b \equiv c(mod\ n)$
$= a - b$ and $b - c$ are multiples of n
$= (a - b) + (b - c) \ = \ (a - c)$ is a multiple of n
$= a \equiv c(\ mod\ n) \ = \ aRc$
R is transitive. This proves that R is equivalence relation.

☻ **<u>Equivalence Class</u>:**

Let R be an equivalence relation on a set A and $a \in A$. Then the set of all those elements x of A which are related to a by R is called the equivalence class of a with respect to R.

$$\bar{a} = [a] = R(a) = \{x \in A | (x, a) \in R\}$$

Example:

$R = \{(1,1), (1,3), (2,2), (3,1), (3,3)\}$ defined on the set $A = \{1,2,3\}$ we find elements x of A for which $(x, 1) \in R$ are $x = 1, x = 3$. Therefore $\{1,3\}$ is the equivalence class of 1

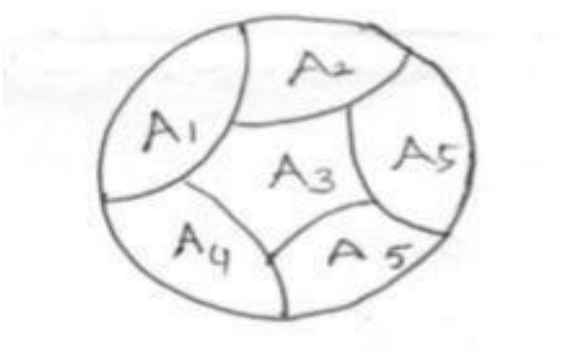
i.e., $[1] = \{1,3\}, [2] = [2], [3] = \{1,3\}$

☻ **<u>Partition of a set</u>:**

Let A be a non-empty set suppose that there exist non-empty subsets $A_1, A_2, A_3, \ldots\ldots A_K$ of A such that the following two conditions hold.

1) A is the union of $A_1, A_2, A_3, \ldots\ldots A_K$ that is $A = A_1 U A_2 U A_3, \ldots U A_K$
2) Any two of the subsets $A_1, A_2, A_3, \ldots\ldots A_K$ are disjoint i.e., $A_i \cap A_j = \phi$ for $i \neq j$ then the set $P = \{A_1, A_2, A_3, \ldots\ldots A_K\}$ is called a partition of A. also $A_1, A_2, A_3, \ldots\ldots A_K$ are called the blocks or cells of the partition.

A partition of a set A with 6 blocks is as shown below



$A = \{1,2,3,4,5,6,7,8\}$ and its following subsets $A_1 = \{1,3,5,7\}$, $A_2 = \{2,4\}$, $A_3 = \{6,8\}$

$P = \{A_1, A_2, A_3\}$ is a Partition of A with A_1 A_2 A_3 as blocks of the partition?

$A_4 = \{1,3,5\}$ then $P_1 = \{A_2, A_3, A_4\}$ in not a partition of the set A. Because although the subsets A_2, A_3 and A_4 are mutually disjoint A is not the union of these subsets. We find if $A_5 = \{5,6,8\}$ then $P_2 = \{A_1, A_2, A_5\}$ is also not a partition of A because A is the union of A_1, A_2, A_5. $A_1, A_5$are not disjoint.

Problems:

1. For the set A and the relation R on A

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

Defined on A find the partition of A induced by R.

Solution:

By examining the given R_1 we find that $[1] = \{1\}$, $[2] = \{2,3\}$, $[3] = \{2,3\}$, $[4] = \{4,5\}$, $[5] = \{4,5\}$ of these equivalence classes only $[1]$, $[2]$ and $[4]$ are distinct these constitute the partition P of A determined by R then

$P = \{[1], [2], [4]\}$ is the partition induced by R

$A = [1]\ U\ [2]\ U\ [4] = \{1\} U \{2,3\} U \{4,5\}$

☻ **Partial orders:**

A relation R on a set A is said to be a partial ordering relation or a partial order on A if (i) R is reflexive (ii) R is antisymmetric and (iii) R is transitive on A.

Poset:

A set with a partial order R defined on it is called a partially ordered set or Poset.

Example: less than or equal to. On set of integers.

Total Order:

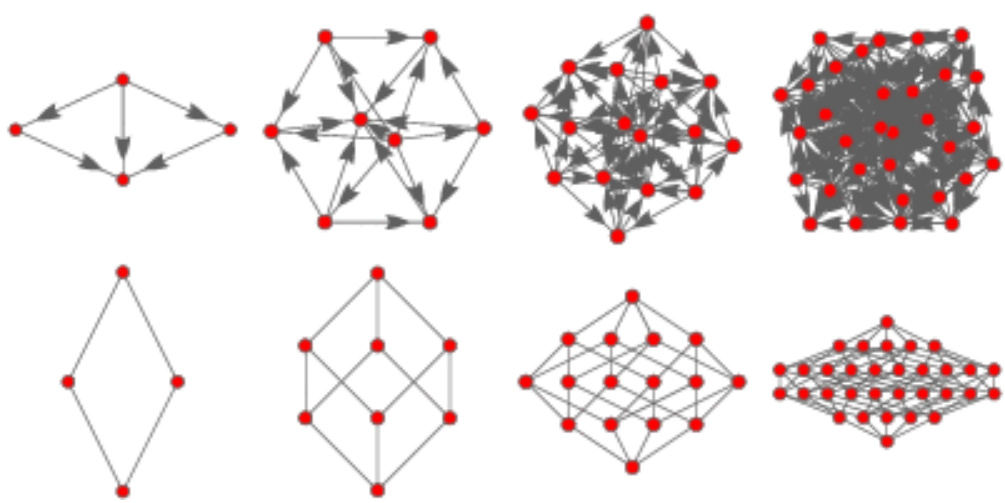
Let R be a partial order on a set A. Then R is called a total order on A. if for all $x, y \in A$ either xRy or yRx. In this case the poset (A, R) is called a totally ordered set.

Hasse Diagram:

A Hasse diagram is a graphical rendering of a partially ordered set displayed via the cover relation of the partially ordered set with an implied upward orientation. A point is drawn for each element of the poset, and line segments are drawn between these points according to the following two rules:

1. If $x < y$ in the poset, then the point corresponding to x appears lower in the drawing than the point corresponding to y.

2. The line segment between the points corresponding to any two elements x and y of the poset is included in the drawing iff x covers y or y covers x .



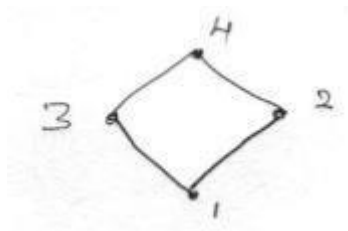
Problems:

1. Let $A = \{1,2,3,4\}$ and $R = \{(1,1), (1,2), (2,2), (2,4), (1,3), (3,3), (3,4), (1,4), (4,4)\}$. Verify that R is a partial order on A. also write down the Hasse diagram for R.

Solution:

We observe that the given relation R is reflexive and transitive. Further R does not contain ordered pairs of the form (a, b) and (b, a) with $b \neq a$. R is antisymmetric as such R is a partial order on A.

The Hasse diagram for R must exhibit the relationships between the elements of A as defined by R. if $(a, b) \in R$ there must be an upward edge from a to b.

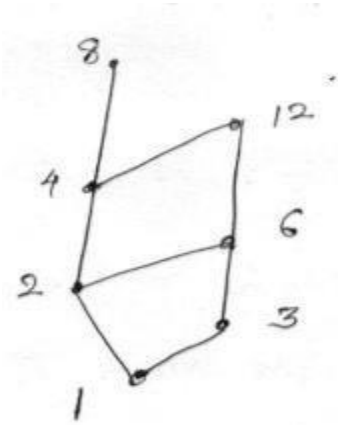


2. Let $A = \{1,2,3,4,6,8,12\}$ on A, define the partial ordering relation R by xRy if and only if x/y draw the Hasse diagram for R.

Solution:

$$R = \{(1,1), (1,2), (1,3), (1,4), (1,6), (1,8), (1,12), (2,2), (2,4), (2,6), (2,8), (2,12),$$
$$(3,3), (3,6), (3,12), (4,4), (4,8), (4,12), (6,6), (6,12), (8,8), (12,12)\}.$$

The Hasse diagram for this R is as shown below.



3. Draw the Hasse diagram representing the positive divisors of 36.

Solution:

The set of positive divisors of 36 is

$D_{36} = \{1,2,3,4,6,9,12,18,36\}$ The relation R of divisibility (that is aRb if and only if a divides b) is a partial order on this set. The Hasse diagram for this partial order is required here.

1 is related to all elements of D_{36}

2 is related to 2,4,6,12,18,36

3 is related to 3,6,9,12,18,36

4 is related to 4,12,36

6 is related to 6,12,18,36

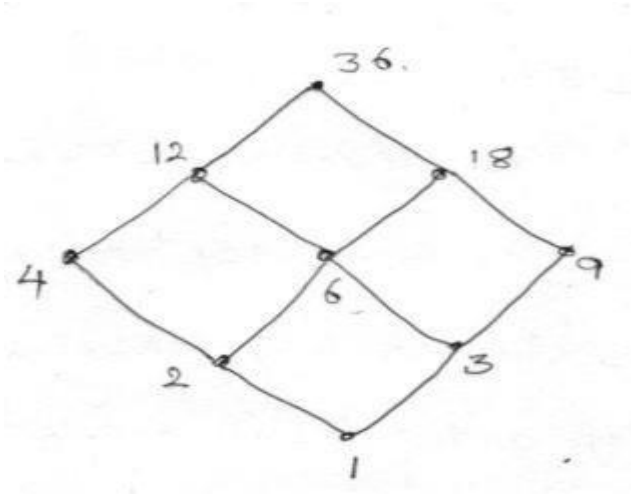
9 is related to 9,18,36

12 is related to 12 and 36

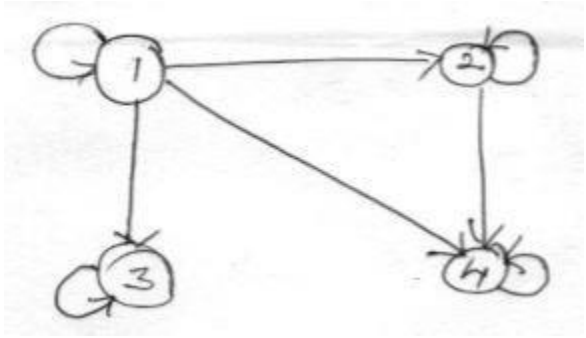
18 is related to 18 and 36

36 is related to 36.

The Hasse diagram for R must exhibit all of the above facts.

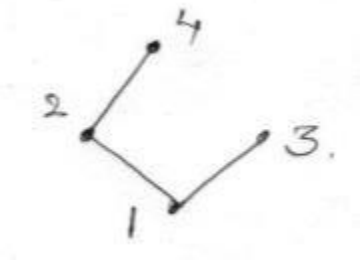


4. A partial order R on set $A = \{1,2,3,4\}$ is represented by the following diagraph. Draw the Hasse diagram for R.



Solution:
By observing the given diagraph, we note that

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



☻ **<u>External elements in Posets</u>:**

Upper bond of a subset B of A: an element $a \in A$ is called an upper bound of a subset B of A if xRa for all $x \in B$.
Lower bound of a subset B of A: an element $a \in A$ is called lower bound of a subset B is A if aRx for all $x \in B$.

Supremum (LUB): An element $a \in A$ is called the LUB of a subset B of A if the following two conditions hold.

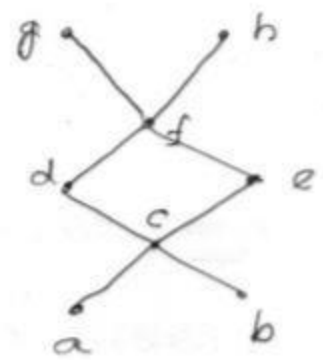
i) A is an upper bound of B.
ii) If a^l is an upper bound of B then aRa^l.

Infimum (GLB): An element $a \in A$ is called the GLB of a subset B of A if the following two conditions hold

i) A is a lower bound of B.
ii) If a^l is a lower bound of B then a^lRa.

Problems:

1. Consider the Hasse diagram of a Poset (A, R) given below.



If $B = \{c, d, e\}$ find (if they exist).

i) All upper bounds of B
ii) All lower bounds of B
iii) The least upper bound of B
iv) The greatest lower bound of B

Solution:

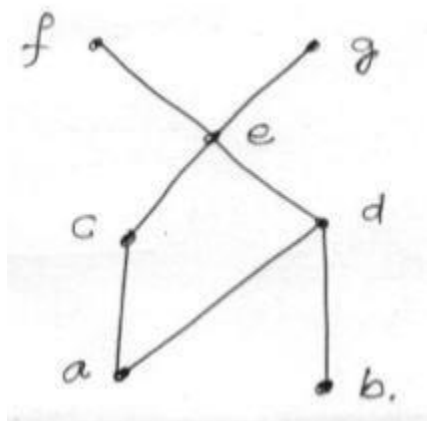
(i) All of c, d, e which are is B are related to f, g, h therefore f, g, h re upper bounds of B.

(ii) The elements a, b and c are related to all of c, d, e which are in B. therefore a, b and c are lower bounds of B.

(iii) The upper bound f of B is related to the other upper bounds g and h of B. Therefore, f is the LUB of B.

(iv) The lower bounds a and b of B are related to the lower bound c of B. therefore C is the GLB of B.

2. Consider the Poset whose Hasse diagram is shown below. Find LUB and GLB of $B = \{c, d, e\}$



By examining all upward paths from c, d, e is the given Hasse diagram. We find that LUB $(B) = e$. by examining all upward paths to c, d, e we find that $GLB(B) = a$.

☻ **<u>Lattice</u>:**

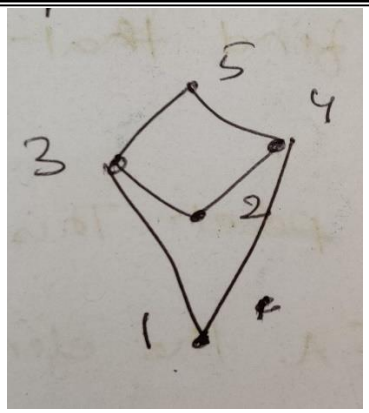
Let (A, R) be a Poset this Poset is called a lattice. For all $x, y \in A$ the elements $LUB\ \{x, y\}$ and $GLB\ \{x, y\}$ exist is A.

Example: Let (A, R) be Poset. The Poset is called a.

1). Consider the set N of all-natural numbers and let R be the partial order "less than or equal to" then for any $x, y \in N$, we note that $LUB\ \{x, y\} = Max\{x, y\}$ and $GLB\ \{x, y\} = min\{x, y\}$ and both of these belong to N. Therefore, the Poset $(N, \leq)$ is a lattice.

2). Consider the Poset $(Z^+, |)$ where Z^+ is set of all positive integer & | is the divisibility set. We can check that for any $a, b \in Z^+$, the least common multiple of a & b is the $LUB\ \{a, b\}$ & the GCD of a & b is $GLB\ \{a, b\}$. Since these belongs to Z^+ we infer that $(Z^+, |)$ is a lattice.

3). Consider the poset where Hasse Diagram is



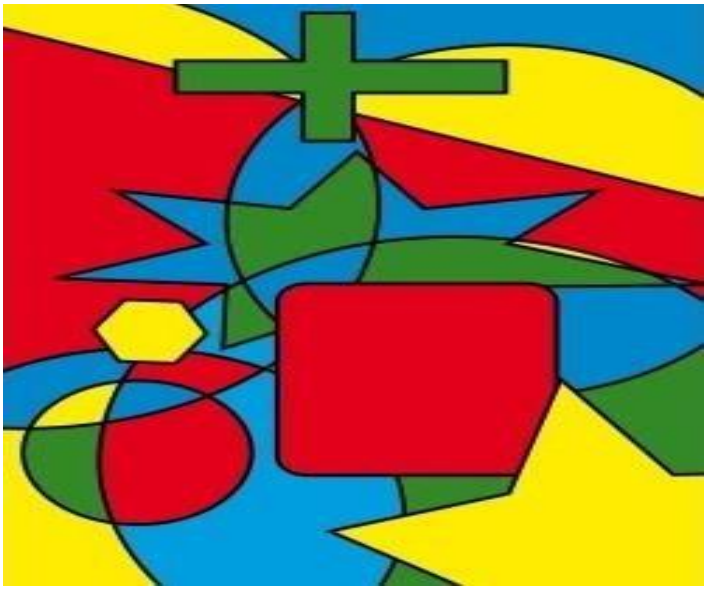
By examining the Hasse diagram, we note that $GLB\ \{3, 4\}$ does not exist.

$\therefore$ The poset is not a Lattice

BCS405A

Discrete Mathematical Structures

(For the 4th Semester Computer Science and Engineering Stream)



Module 4

THE PRINCIPLE OF INCLUSION & EXCLUSION, RECURRENCE RELATIONS

Content

MODULE-4

THE PRINCIPLE OF INCLUSION & EXCLUSION, RECURRENCE RELATIONS

☻ <u>The principle of Inclusion – Exclusion</u>:

If S is a finite set, then the number of elements in S is called the order (or the size, or the cardinality) of S and is denoted by |S|. If A and B are subsets of S, then the order od $A\ U\ B$ is given by the formula

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Thus, for determining the number of elements that are in $A\ U\ B$, we include all elements in A and B but exclude all elements common to A and B.

Principle of Inclusion – Exclusion for n sets.

Let S be a finite set and $A_1, A_2 \ldots\ldots\ldots\ldots A_n$ be subset of S. Then the principle of inclusion – exclusion for $A_1, A_2 \ldots\ldots\ldots\ldots A_n$ states that

$$|A_1 \cup A_2 \cup A_3 \ldots\ldots \cup A_n| = \Sigma|A_i| - \Sigma|A_i \cap A_j| + \Sigma|A_i \cap A_j \cap A_k| + \cdots + (-1)^{n-1}|A_1 \cap A_2 \ldots . \cap A_n|$$

<u>Generalization</u>:

The principle of inclusion – exclusion as given by expression

$$\bar{N} = S_0 - S_1 + S_2 - S_3 + \cdots + (-1)^n S_n$$

The number of elements in S that satisfy none of the conditions $C_1, C_2 \ldots\ldots C_n$. The following expression determines the number of elements in S that satisfy exactly m of the n conditions $(0 \le m \le n \le)$;

$$E_m = S_m - \binom{m+1}{1} S_{m+} + \binom{m+2}{2} S_{m+1} \ldots . + (-1)^{n-m} \binom{n}{n-m} S_n$$

Problems:

1. Out of 30 students in a hostel, 15 study History, 8 study Economics, and 6 study Geography. It is known that 3 students study all these subjects. Show that 7 or more students' study none of these subjects.

Solution:

Let 'S' denote the set of all students in the hostel and A_1, A_2, A_3 denotes the set of students who study History, Economics and Geography, respectively.

Given, $S_1 = \sum|Ai| = 15 + 8 + 6 = 29$ and

$S_3 = |A_1 \cap A_2 \cap A_3| = 3$

The number of students who do not study any of the three subjects is $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3|$

$$|A \cap \bar{A}_2 \cap \bar{A}_3| = |S| - \sum|A_i| + \sum|A_i \cap A_j| - \Sigma|A_1 \cap A_2 \cap A_3|$$

$$= |S| - S_1 + S_2 - S_3$$

$$= 30 - 29 - S_2 - 3 = S_2 - 2$$

Where, $S_2 = \sum|A_i \cap A_j|$

We know that $(A_1 \cap A_2 \cap A_3)$ is a subset of $(A_i \cap A_j)$ for $i, j = 1, 2, 3$. Therefore, each of $|A_i \cap A_j|$, which are 3 in number, is greater that (or) equal to $|A_1 \cap A_2 \cap A_3|$

$S_2 = \sum|A_i \cap A_j| \geq 3|A_1 \cap A_2 \cap A_3| = 9.$

$|A \cap \bar{A}_2 \cap \bar{A}_3| \geq 9 - 2 = 7.$

2. How many integers between 1 and 300(inclusive) are?

(i) divisible by at least one of $5, 6, 8$?

(ii) divisible by none of $5, 6, 8$?

Solution:

Let $S = \{1, 2, \ldots\ldots, 300\}$. So that, $|S| = 300$. Also, let A_1, A_2, A_3 be subset of whose elements are divisible by 5, 6, 8, resp.

(i) the number of elements of S that are divisible by at least one of 5, 6, 8 is, $|A_1 \cup A_2 \cup A_3|$

$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - \{|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|\} + |A_1 \cap A_2 \cap A_3|$

We know that

$|A_1| = 60$, $|A_2| = 50$, $|A_3| = 37$, $|A_1 \cap A_2| = 10$

$|A_1 \cap A_3| = 7$, $|A_2 \cap A_3| = 12$ $|A_1 \cap A_2 \cap A_3| = 2$

$|A_1 \cap A_2 \cap A_3| = (60 + 50 + 37) - (10 + 7 + 2) + 2 = 120.$

Thus 120 elements of S are divisible by at least one 5, 6, 8.

(ii) The number of elements of S that are divisible by none of 5, 6, 8. Is,

$|A \cap \bar{A}_2 \cap \bar{A}_3| = |S| - |A_1 \cup A_2 \cup A_3| = 300 - 120 = 180$

3. Find the number of non-negative integer solutions of the equation.

$$X_1 + X_2 + X_3 + X_4 = 18$$

Under the conditions $X_1 \leq 7, for\ 1 = 1, 2, 3, 4$

Solution:

Let S denote the set of all non-negative integer solutions of the given equation. The number of such solutions is, $C(4+18-1,18) = C(21,18)$

$|S| = C(21,18)$.

Let A, be the subset of S that contains the non-negative integer solutions of the given equation under the conditions $X_1 > 7, X_2 \geq 0, X_3 \geq 0, X_4 \geq 0$

$A_1 = \{ (X_1, X_2, X_3, X_4) \in S | X_1 > 7 \}$

Similarly, $A_2 = \{ (X_1, X_2, X_3, X_4) \in S | X_2 > 7 \}$

$A_3 = \{ (X_1, X_2, X_3, X_4) \in S | X_3 > 7 \}$

$A_4 = \{ (X_1, X_2, X_3, X_4) \in S | X_4 > 7 \}$

Therefore, the required solution, $|A \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4|$

Let us set $Y_1 = X_1 - 8$. Then, $X_1 > 7((ie)X \geq 8)$

Corresponds to $Y_1 \geq 0$, when written in terms of $Y_1, Y_1 + X_1 + X_2 + X_3 + X_4 = 10$.

The number of non-negative integer solutions of this equation is $C(4+10-1,10) = C(13,10)$.

$|A_1| = C(13,10)$

Similarly, $|A_2| = |A_3| = |A_4| = C(13,10)$

let us take $Y_1 = X_1 - 8$, $Y_2 = X_2 - 8$. Then $X_1 > 7$ and $X_2 > 7$ correspond to $Y_1 \geq 0$ and $Y_2 \geq 0$.

When written in terms of Y_1 and Y_2,

$Y_1 + Y_2 + X_3 + X_4 = 2$.

The number of non-negative integer solutions of this equation is $C(4+2-1,2) = C(5,2)$

$|A_1 \cap A_2|$, $\quad therfore\ |A_1 \cap A_2| = C(5,2)$

$|A_1 \cap A_3| = |A_1 \cap A_4| = |A_2 \cap A_3| = |A_2 \cap A_4| = |A_3 \cap A_4| = C(5,2)$.

The given equation, more than two X_i's cannot be greater than 7 simultaneously.

$$|A \cap \bar{A}_2 \cap \bar{A}_3| = |S| - \sum|A_i| + \sum|A_i \cap A_j| - \sum|A_i \cap A_j \cap A_k| + |A_1 \cap A_2 \cap A_3 \cap A_4|$$

$$= C(21,18) - \binom{4}{1} \times C(13,10) + \binom{4}{2} \times C(5,2) - 0 + 0$$

$$= 1330 - (4 \times 286) + (6 \times 30) = 366$$

4. In how many ways 5 number of a's, 4number of b's and 3 number of c's can be arranged so that all the identical letters are not in a single block?

Solution:

The given letters are 5+4+3 = 12 in number of which 5 are a's, 4are b's, and 3 are c's. If S is the set of all permutations (arrangements) of these letters, we've,

$$|S| = \frac{12!}{5!\,4!\,3!}$$

Let A_1 be the set of arrangements of the letters where the 5 a's are in a single block.

The number of such arrangements is,

$$|A_1| = \frac{8!}{4!\,3!}$$

Similarly, if A_2 is the set of arrangements of the letters where the 4 b's are in a single block and A_3 is the set of arrangements of the letters where the 3 c's are in a single block

We have,

$|A_2| = \frac{9!}{5!3!}$ and $|A_3| = \frac{10!}{5!4!}$

Likewise,

$$|A_1 \cap A_2| = \frac{5!}{3!}, \quad |A_1 \cap A_2| = \frac{6!}{4!}, \quad |A_2 \cap A_3| = \frac{7!}{5!}$$

$|A_1 \cap A_2 \cap A_3| = 3!$

The required number of arrangements is,

$$|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3|$$
$$= |S| - \{|A_1 \cup A_2 \cup A_3|\} + \{|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|\} - |A_1 \cap A_2 \cap A_3|$$

$$= \frac{12!}{5!\,4!\,3!} - \{\frac{8!}{4!\,3!} + \frac{9!}{5!\,3!} + \frac{10!}{5!\,4!}\} + \{\frac{5!}{3!} + \frac{6!}{4!} + \frac{7!}{5!}\}$$

$$= 27720 - (280 + 504 + 1260) + (20 + 30 + 42) - 6$$

= 25762.

5. In how many ways can the 26 letters of the English alphabet be permuted so that none of the patterns CAR, DOG, PUN (or) BYTE occurs?

Solution:

Let S denote the set of all permutations of the 26 letters. Then |S|= 26!

Let A_1 be the set of all permutations in which CAR appears. This word, CAR consists of three letters which from a single block.

The set A_1 therefore consists of all permutations which contains this single block and the 23 remaining letters. $|A_1| = 24!$

Similarly, if A_2 , A_3 , A_4 are the set of all permutations which contain DOG, PUN and BYTE respectively.

We have, $|A_2| = 24!$ $|A_3| = 24!$ $|A_4| = 23!$

Likewise, $|A_1 \cap A_2| = |A_1 \cap A_3| = |A_2 \cap A_3| = (26 - 6 + 2)! = 22!$

$|A_1 \cap A_4| = |A_2 \cap A_4| = |A_3 \cap A_4| = (26 - 7 + 2) = 21!$

$| A_1 \cap A_2 \cap A_3| = (26 - 9 + 3)! = 20!$

$| A_1 \cap A_2 \cap A_4| = | A_1 \cap A_3 \cap A_4| = | A_2 \cap A_3 \cap A_4| = (26 - 10 + 3)! = 19!$

$| A_1 \cap A_2 \cap A_3 \cap A_4| = (26 - 13 + 4)! = 17!$

Therefore, the required number of permutations is given by,

$$|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4| = |S| - \sum|A_i| + \sum|A_i \cap A_j| - \sum|A_i \cap A_j \cap A_k| + | A_1 \cap A_2 \cap A_3 \cap A_4|$$

$$= 26! - (3 \times 24! + 23!) + (3 \times 22! + 3 \times 21!) - (20! + 3 \times 19!) + 17!$$

6. In how many ways can one arrange the letters in the word CORRESPONDENTS so that

(i) There is no pair of consecutive identical letters?

(ii) There are exactly two pairs of consecutive identical letters?

(iii) There are at least three pairs of consecutive identical letters?

Solution:

In the word CORRESPONDENTS, there occur one each of C, P, D and T and two each of O, R, E, S, N. If S is the set of all permutations of these 14 letters, we've,

$$|S| = \frac{14!}{(2!)^5}$$

Let A_1 , A_2 , A_3 , A_4 , A_5 be the set of permutations in which O's, R's, E's, N's appear in pairs respectively.

Then, $|A_i| = \frac{13!}{(2!)^4}$ for i = 1, 2, 3, 4, 5

Also, $|A_i \cap A_j| = \frac{12!}{(2!)^3}$, $|A_i \cap A_j \cap A_k| = \frac{11!}{(2!)^2}$

$|A_i \cap A_j \cap A_k \cap A_p| = \frac{10!}{(2!)}$, $| A_1 \cap A_2 \cap A_3 \ldots\ldots \cap A_5| = 9!$

From these,

$$S_0 = N = |S| = \frac{14!}{(2!)^5}, \qquad S_1 = C(5,1) \times \frac{13!}{(2!)^4}$$

$$S_2 = C(5,2) \times \frac{12!}{(2!)^3}, \qquad S_3 = C(5,3) \times \frac{11!}{(2!)^2}$$

$$S_4 = C(5,4) \times \frac{10!}{(2!)^1}, \qquad S_5 = C(5,5) \times 9!$$

Accordingly, the number of permutations where these is no pair of consecutive identical letter is,

$$E_0 = S_0 - \binom{1}{1} S_1 + \binom{2}{2} S_2 - \binom{3}{3} S_3 + \binom{4}{4} S_4 - \binom{5}{5} S_5$$

$$= \frac{14!}{(2!)^5} - \binom{5}{1} \times \frac{13!}{(2!)^4} + \binom{5}{2} \times \frac{12!}{(2!)^3} - \binom{5}{3} \times \frac{11!}{(2!)^2} + \binom{5}{4} \times \frac{10!}{(2!)^1} - \binom{5}{5} \times 9!$$

The number of permutations where there are exactly two pairs of consecutive identical letters,

$$E_2 = S_2 - \binom{3}{1} S_3 + \binom{4}{2} S_4 - \binom{5}{3} S_5$$

$$= \binom{5}{2} \times \frac{12!}{(2!)^3} - \binom{3}{1}\binom{5}{3} \times \frac{11!}{(2!)^2} + \binom{4}{2}\binom{5}{4} \times \frac{10!}{(2!)^1} - \binom{5}{3}\binom{5}{5} \times 9!$$

The number of permutations where there are at least three pair of consecutive identical letter is,

$$E_3 = S_3 - \binom{3}{2} S_4 + \binom{4}{3} S_5$$

$$= \binom{5}{3} \times \frac{11!}{(2!)^2} + \binom{3}{2}\binom{5}{4} \times \frac{10!}{(2!)^1} - \binom{4}{2}\binom{5}{5} \times 9!$$

☻ **<u>Derangements</u>:**

A permutation of n distinct objects in which none of the objects is in its natural place is called a derangement.

Formula for d_n

The following is the formula for d_n for $n \geq 1$:

$$d_n = n!\{1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\}$$

$$= n! \times \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

For example, $D_2 = 2!\,[1 - \frac{1}{1!} + \frac{1}{2!}] = 1$

$D_3 = 3!\,[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!}] = 1\,(1 - 1 + \frac{1}{2} - \frac{1}{6}) = 2$

$D_4 =,\quad D_5 = 4^4,\quad D_6 = 26^5,\quad D_7 = 1854$

Problems:

1. Evaluate d_5, d_6, d_7, d_8

Solution:

$d_5 = 5!\{1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!}\}$

$= 120\{\frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120}\} = 44$

$d_6 = 6!\{1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \frac{1}{6!}\}$

$= 720\{\frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120} - \frac{1}{720}\} = 256$

Similarly, $d_7 \approx [7! \times e^{-1}] \approx [5040 \times 0.3679] \approx 1854$

$d_8 \approx [8! \times e^{-1}] \approx [40320 \times 0.3679] \approx 14833$

2. From the set of all permutations of n distinct objects, one permutation is chosen at random. What is the probability that it is not a derangement?

Solution:

The number of permutations of n distinct objects is $n!$. The number of derangements of these objects is d_n.

The probability that a permutation chosen is not a derangement,

$$P = 1 - \frac{dn}{n!} = 1 - \{1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\}$$

$$= 1 - \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$$

3. In how many ways can the integers 1, 2, 3….10 be arranged in a line so that no even integer is in its natural place.

Solution:

Let A_1 be the set of all permutations of the given integer where 2 is in its natural place. A_2 be the set of all permutations in which 4 is in its natural place, and so on. The number of permutations where no even integer is in its natural place is $|A \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4 \cap \bar{A}_5|$. This is given by,

$$|A \cap \bar{A}_2 \ldots \ldots \cap \bar{A}_5| = |S| - S_1 + S_2 - S_3 + S_4 - S_5$$

We note that |S|=10!

Now, the permutations in A1 are all of the form $b_1, b_3, b_4 \ldots b_{10}$ where $b_1 b_3 b_4 \ldots . b_{10}$is a permutation of 1,3, 4, 5, …. 10 as such |A1| = 9!

Similarly, $|A_2| = |A_3| = |A_4| = |A_5| = 9!$

So that, $S_1 = \Sigma|A_i| = 5 \times 9! = C(5,1) \times 9!$

The permutations in $A_1 \cap A_2$ are all of the form $b_1\ 2\ b_3\ 4\ b_5\ b_6 \ldots b_{10}$ where $b_1 b_3 b_5\ b_6 \ldots . b_{10}$ is a permutations of 1, 3, 5, 6, …10 . As such $|A_1 \cap A_2| = 8!$

Similarly, each of $|A_i \cap A_j| = 8!$ Are there are $C(10,2)$ such terms, $S_2 = \Sigma|A_i \cap A_j| = C(5,2) \times 8!$

Like wise $S_3 = C(5,3) \times 7!$, $S_4 = C(5,4) \times 6!$, $S_5 = C(5,5) \times 5!$

Accordingly, Expression (1) gives the required number as,

$$|\bar{A}_1 \cap \bar{A}_2 \ldots \ldots \cap \bar{A}_5|$$
$$= 10! - C(5,1) \times 9! + C(5,2) \times 8! - C(5,3) \times 7! + C(5,4) \times 6! - C(5,5) \times 5!$$

= 2170680

4. Prove that, for any positive integer n, $n! = \sum_{k=0}^{n} \binom{n}{k} d_k$

Solution:

For any positive integer n, the total number of permutations of $1, 2, 3, \ldots . N$ is $n!$. In each such permutations there exists K (where $0 \le k \le n$) elements which are in their natural positions called fixed elements, and n-k elements which are not in their original positions. The k element ca be chosen in $\binom{n}{k}$ ways and the remaining n-k elements can then be chosen in d_{n-k} ways.

Hence there are $\binom{n}{k} d_{n-k}$ permutations of 1, 2, 3, …. n with k fixed elements and n-k deranged elements. As k varies from 0 to n, we count all of the n! permutations of $1, 2, 3 \ldots . n$.

Thus, $n! = \sum_{k=0}^{n} \binom{n}{k} d_{n-1}$

$$= \binom{n}{0} d_n + \binom{n}{1} d_{n-1} + \binom{n}{2} d_{n-2} + \cdots + \binom{n}{n} d_0$$

$$= \sum_{k=0}^{n} \binom{n}{n-k} d_k -= \sum_{k=0}^{n} \binom{n}{k} d_k$$

☻ **<u>Rook Polynomials</u>:**

Consider a board that resembles a full chess board or a part of chess board. Let n be the number of squares present in the board. Pawns are placed in the squares of the board such that not more than one pawn occupies a square.

Then, according to the pigeonhole principle, not more than n pawns ca be used. Two pawns placed on a board having 2 (or) more squares are said to capture (or take) each other if they (pawns) are in the same row or in the same column of the board. For $2 \leq k \leq n$, let r_k denote the number of ways in which k paws can be placed on a board such that no two pawns capture each other – that is, no two pawns are in the same row or in the same column of the board.

Then the polynomial: $1 + r_1\, x + r_2\, x^2 + \cdots + r_n\, x^n$ is called the rook polynomial for the board considered. If the board is denoted by $r(c, x)$. thus, by definition,

$r(c, x) = 1 + r_1\, x + r_2\, x^2 + \cdots + r_n\, x^n$ … … … … …(1)

While defining this polynomial, it has been assumed that $n \geq 2$. In the trivial case where $n = 1$ (i.e., in the case where a board contains only one square), r_2, r_3 …are identically zero and the rook polynomial $r(c, x)$ is defined by,

$r(c, x) = 1 + x$ … … … … . . (2)

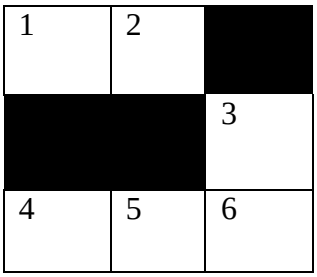
the expression (1) and (2) can be put in the following combined form which holds for a board c with $n \geq 1$ squares.

$r(c, x) = 1 + r_1\, x + r_2\, x^2 + \cdots + r_n\, x^n$ … … … … …(3)

Here, $r_1 = n =$ number of squares in the board.

Problems:

1. Consider the board containing 6 squares,



Solution:

For this board $r_1 = 6$ we observed that 2 non- capturing rooks can have the following positions: $(1, 3), (1, 5), (1, 6), (2, 3), (2, 4), (2, 6), (3, 4), (3, 5)$. These positions are 8 in number. therefore $r_2 = 8$.

Next, 3 mutually non-capturing rooks can be placed only in the following two positions: $(1, 3, 5), (2, 3, 4)$.

Thus $r_3 = 2$ we find that four (or) more mutually non-capturing rooks cannot be placed on the board.

Thus $r_4 = r_5 = r_6 = 0$. Accordingly, for this board, the rook polynomial is,

$$r^0(c, x) = 1 + 6x + 8x^2 + 2x^3$$

2. Consider the board containing 8 squares (marked 1 to 8)

1	2	3
4		5
6	7	8

Solution:

For this board, $r_1 = 8$

In this board, the positions of 2 non-capturing rooks are
$(1,5), (1,7), (2,4), (2,5), (2,6), (2,8), (3,4), (3,6), (3,7), (4,8), (5,6), (5,7)$.

These are 14 numbers, therefore $r_2 = 14$. The positions of 3 mutually non-capturing rooks are $(1,5,7), (2,4,8), (2,5,6), (3,4,7)$.

These are 4 in number, therefore $r_3 = 4$.

We check that the board has no positions for more than 3 mutually non-capturing rooks.

Hence, $r_4 = r_5 = r_6 = r_7 = r_8 = 0$.

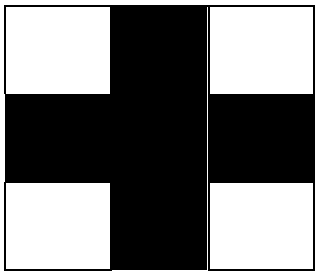
Thus, for this board, the rook polynomial is,

$$r(c, x) = 1 + 8x + 14x^2 + 4x^3.$$

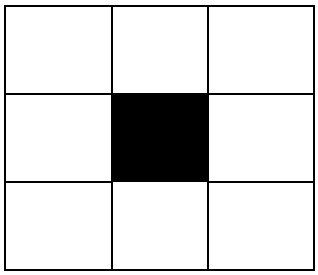
3. Find the rook polynomial for the 3 * 3 board by using the expansion formula.

Solution:

The 3 X 3 board let us mark the square which is at the centre of the board. The boards D and E appear as shown below (the shaded parts are the deleted parts),



D



E

For the board D, we find that $r_1 = 4, r_2 = 2, r_3 = r_4 = 0$

$$r(D, x) = 1 + 4x + 2x^2$$

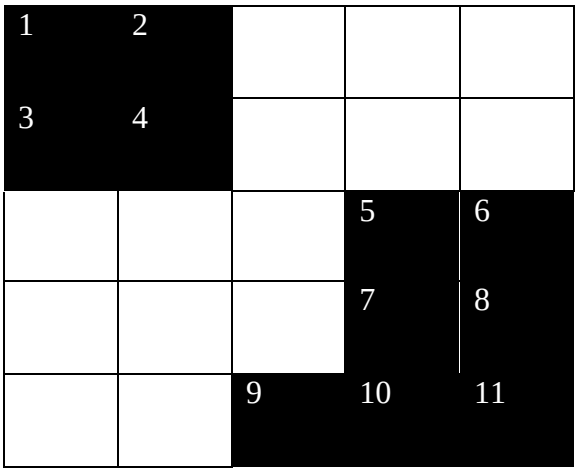
The board E is the same as the one considered (3 X 3) As such for this board,

$$r(E, x) = 1 + 8x + 14x^2 + 4x^3$$

Now, the expansion formula gives

$$\begin{aligned} r(c_{3\times3}, x) &= xrD(x) + r(E, x) \\ &= x(1 + 4x + 2x^2) + (1 + 8x + 14x^2 + 4x^3) \\ &= 1 + 9x + 18x^2 + 6x^3 \end{aligned}$$

4. Find the rook polynomial for the board shown below (shaded part)



Solution:

We note that the given board C is made up of two disjoint sub-boards C_1 and C_2, where C_1 is the 2 X 2 board with squares numbered 1 to 4 and C_2, is the board with squares numbered 5 to 11.

Since C_1 is the 2 X 2 board we've.

$$r(C_1, x) = 1 + 4x + 2x^2$$

We note that C_2 is the same as the board considered (3 X 3 board). We've,

$$r(C_2, x) = 1 + 7x + 10x^2 + 2x^3$$

Therefore, the product formula yields the rook polynomials for the given board as,

$$r(C_1, x) = r(C_1, x) \times r(C_2, x)$$

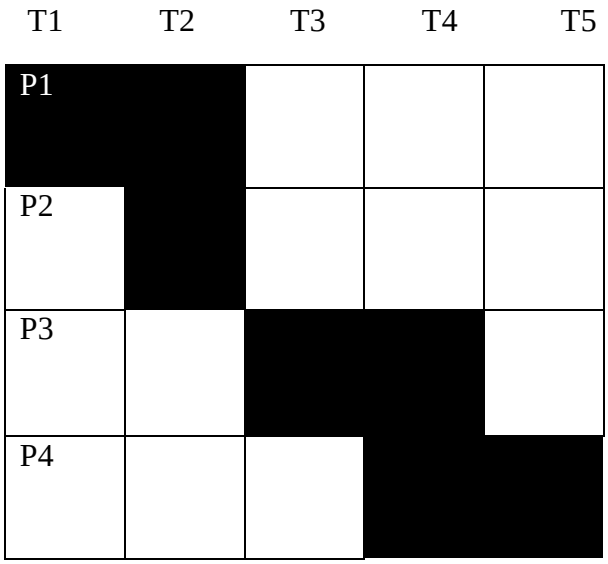
$$= (1 + 4x + 2x^2)(1 + 7x + 10x^2 + 2x^3$$

$$= 1 + 11x + 40x^2 + 56x^3 + 28x^4 + 4x^5$$

5. Four persons P_1, P_2, P_3, P_4 who arrive late for a dinner party find that only one chair at each of five tables T_1, T_2, T_3, T_4 and T_5 is vacant. P_1will not sit at T_1 or T_2, P_2 will not sit at T_2, P_3 will not sit at T_3 or T_4, and P_4 will not sit at T_4 or T_5. Find he number of ways they can occupy the vacant chairs.

Solution:

Consider the board shown below, representing the situation. The shaded in the first now indicate that tables T_1, and T_2 are forbidden for P_1 and so on.



For the board made up of shaded squares in the above figure. The rook polynomial is given by,

$$r(C, x) = 1 + 7x + 16x^2 + 13x^3 + 3x^4$$

Thus, here, $r_1 = 7, r_2 = 16, r_3 = 13, r_4 = 3$

$$S_0 = 5! = 120, \quad S_1 = (5-1)! \times r_1 = 168$$

$$S_2 = (5-2)! \times r_2 = 96, \quad S_3 = (5-3)! \times r_3 = 26$$

$$S_4 = (5-4)! \times r_4 = 3$$

Consequently, the number of ways which the four persons can occupy the chair is

$$S_0 - S_1 + S_2 - S_3 + S_4 = 120 - 168 + 96 - 26 + 3 = 25$$

☻ Recurrence Relations:

First-order recurrence relations: -

We consider for solution recurrence relations of the form,

$a_n = ca_{n-1} + f(n), \quad for\ n \geq 1 \ \dots\dots\dots\dots (1)$

Where c is a known constant and f(n) is a known function. Such a relation is called a linear recurrence relation of first-order with constant co-efficient, if $f(n) = 0$, the relation is called homogeneous, otherwise, it is called non-homogeneous

The relation (1) can be solved in a trivial way. First, we note that this relation may be rewritten as (by changing n to n+1)

$a_{n+1} = ca_n + f(n+1), \quad for\ n \geq 1 \dots\dots\dots\dots (2)$

For, $n = 0, 1, 2, 3, \dots$..This relation yields, respectively

$a_1 = ca_0 + f(1)$

$a_2 = ca_1 + f(2) = c\{ca_0 + f(1)\} + f(2)$

$\quad = c^2a_0 + cf(1) + f(2)$

$a_3 = ca_2 + f(3) = c\{c^2a_0 + cf(1) + f(2)\} + f(3)$

$\quad = c^2a_0 + c^2f(1) + cf(2) + f(3)$

And so on. Examining these, we obtain, by induction

$a_n = c^na_0 + c^{n-1}f(1) + c^{n-2}f(2) + \cdots + cf(n-1) + f(n)$

$= c^na_0 + \sum_{k=0}^{n} c^{n-k}f(k), \qquad for\ n \geq 1 \dots\dots\dots\dots\dots\dots\dots (3)$

This is the general solution of the recurrence relation (2) which is equivalent to the relation (1)

If f(n) = 0. That is if the recurrence relation is homogeneous, the solution (3) becomes

$a_n = c^na_0 \qquad for\ n \geq 1 \ \dots\dots\dots (4)$

The solutions (3) and (4) yield particular solutions if a_0 is specified value of $a_0$is called the initial condition.

Problems:

1. Solve the recurrence relation $a_n = na_{n-1}\ for\ n \geq 1$ given the $a_0 = 1$

Solution:

From the given relation, we find that,

$a_1 = 1 \times a_0, \quad a_2 = 2a_1 = (2 \times 1)a_0,$

$a_3 = 3 \times a_2 = (3 \times 2 \times 1)a_0,$

$a_4 = 4 \times a_3 = (4 \times 3 \times 2 \times 1)a_0$ and so on.

Evidently, the general solution is (by induction)

$a_n = (n!)a_0 \; for \; n \geq 1$

Using the given initial condition $a_0 = 1$

Therefore, $a_n = n!$

2. Solve the recurrence relation $a_n - 3a_{n-1} = 5 \times 3^n$ for $n \geq 1$ given that $a_0 = 2$

Solution:

The given relation may be rewritten as

$a_{n+1} = 3a_n + 5 \times 3^{n+1} \; for \; n \geq 0$

$= 3a_n + f(n+1) \; where \; f(n) = 5 \times 3^n$

The general solution for this relation is,

$a_n = 3^n a_0 + \sum_{k=1}^{n} 3^{n-k} f(k)$

$= 3^n a_0 + 3^{n-1} f(1) + 3^{n-2} f(2) + 3^{n-3} f(3) + \cdots + 3^0 f(n)$

Substituting for a_0 and f(n), n = 1, 2, …n in this we get

$a_n = 2 \times 3^n \times 3^{n-1} \times (5 \times 3^1) + 3^{n-2} \times (5 \times 3^2) + 3^{n-3} \times (5 \times 3^3) + \cdots + 3^0 \times (5 \times 3^n)$

$= 2 \times 3^n + 5 \times (3^n + 3^n + 3^n + \cdots + 3^n) \qquad (n \; terms)$

$= 2 \times 3^n + 5 \times (n3^n)$

$= (2 + 5n)3^n$

This is the required solution.

3. Find the recurrence relation and the initial condition for the sequence, $2, 10, 50, 250$.....Hence find the general term of the sequence.

Solution:

The given sequence is $< a_r >$, where $a_0 = 2, a_1 = 10, a_2 = 10, a_2 = 50, a_3 = 250$ ... .

$a_1 = 5a_0, a_2 = 5a_1, a_3 = 5a_2 \; and \; so \; on.$

From these, we readily note that the recurrence relation for the given sequence is $a_n = 5a_{n-1} \; for \; n \geq 1$

With $a_0 = 2$ as the initial condition

This solution of this relation is, $a_n = 5^n a_0 = 5^n \times 2$

This is the general term of the given sequence

4. Suppose that there are $n \geq 2$ persons at a party and that each of these persons shakes hands (exactly once) with all of the other persons present. Using a recurrent relation find the number of handshakes.

Solution:

Let a_{n-2} denotes the number of hand shakes among the $n \geq 2$ persons present. (If $n = 2$, the number of handshakes is 1; that is $a_0 = 1$). If a new person joins the party, he will shake hands with each of the n persons already present. Thus, the number of handshakes increases by n when the number of persons changes to n+1 from n. Thus,

$a_{(n+1)} = a_{n-2} + n$ for $n \geq 2$

(or) $a_{m+1} = a_m + (m+2)$ for $m \geq 0$, where $m = n - 2$ setting f(m) = m+1,

$a_{m+1} = a_m + f(m+1)$ for $m \geq 0$

The general solution of this non homogenous recurrence relation is,

$$a_m = (1^m \times a_0) + \sum_{k=1}^{n} 1^{n-k} f(k) = a_0 + \sum_{k=1}^{n} (k+1)$$

Since, $a_0 = 1$, this becomes,

$a_m = 1 + \{2 + 3 + 4 + \cdots + m + (m+1)\}$

$= \frac{1}{2}(m+1)(m+2)\ for\ m \geq 0$

(or) $a_{n-2} = \frac{1}{2}(n-1)n \quad for\ n \geq 2$

this is the number of handshakes in the party when $n \geq 2$ persons are present.

<u>Second order homogenous Recurrence Relations</u>:

We now consider a method of solving recurrence relations of the form

$c_n a_n + c_{n-1} a_{n-1} + c_{n-2} a_{n-2} = 0 \quad for\ n \geq 2 \ldots\ldots\ldots..(1)$

where c_n, c_{n-1} and c_{n-2} are real constants with $c_n \neq 0$. A relation of this type is called a second order linear homogenous recurrence relation with constant co-efficient.

$c_n k^2 + c_{n-1} k + c_{n-2} = 0 \ldots\ldots\ldots..(2)$

Thus, $a_n = ck^n$ is a solution of (1) if k satisfies the quadraric equation (2). This quadratic equation is the auxiliary equation or the characteristic equation for the relation (1).

<u>Case 1</u>: The two roots k1 and k2 of equation (2) are real and distinct. Then we take,

$a_n = Ak_1^n + Bk_2^n \ldots\ldots\ldots\ (3)$

Where A and B are arbitrary real constants as the general equation of the relation (1).

<u>Case 2</u>: The two roots k1 and k2 of equation (2) are equal and real, with k as the common value. Then we take,

$a_n = (A + Bn)k^n \ldots\ldots\ldots(4)$

where A and B are arbitrary real constants, as the general solution of the relation (1).

<u>case 3</u>: The two roots k1 and k2 of equations (2) are complex. Then k1 and k2 are complex

conjugates of each other, so that if $k_1 = p + iq$, then $k_2 = p + iq$ and we take,

$a_n = r^n(A\cos n\theta + b\sin n\theta)$..... (5)

where A and B are arbitrary complex constants,

$r = |k_1| = |k_2| = \sqrt{p^2 + q^2}\ and\ \theta = tan^{-1}\left(\frac{a}{b}\right)$ as the general solution of the relation (1).

Problems:

1. Solve the recurrence relation

$$a_n - 6a_{n-1} + 9a_{n-2} = 0 \qquad for\ n \geq 2, \quad given\ that\ a_o = 5, \qquad a_1 = 12$$

Solution:

The characteristics equation for the given relation is,

$$k^2 - 6k + 9 = 0, \quad (or)\ (k-3)^2 = 0$$

Whose roots are $k_1 = k_2 = 3$. Therefore, the general solution for $a_n$is,

$$a_n = (A + Bn)3^n$$

Where A and B are arbitrary constants using the given initial conditions $a_0 = 5$ and $a_1 = 12$ in equation, we get $5 = A$ and $12 = 3(A + B)$ solving these we get, $A = 5$ and $B = -1$

Putting these values in equation we get,

$$a_n = (5 - n)3^n$$

This is the solution of the given relation, under the given initial condition.

2. Solve the recurrence relation

$$a_n = 2(a_{n-1} - a_{n-2}), \qquad for\ n \geq 2$$

Given that $a_0 = 1\ and\ a_1 = 2$

Solution:

For the given relation, the characteristic equation is $k^2 - 2k + 2 = 0$

The roots are,

$$k = \frac{(2 \pm \sqrt{4-8})}{2} = 1 \pm i$$

Therefore, the general solution for a_n is,

$$a_n = r^n[A\ cosn\theta + Bsin\theta]$$

Where A and B are arbitrary constants,

$$r = |1 \pm i| = \sqrt{2}, \quad and\ tan\theta = 1, \theta = \frac{\pi}{4}$$

$$a_n = (\sqrt{2})^n [A \cos \frac{n\pi}{4} + B \sin \frac{n\pi}{4}]$$

Using the given initial conditions $a_0 = 1$ and $a_1 = 2$ we get, 1 = A and

$$2 = (\sqrt{2})[A \cos\frac{\pi}{4} + B \sin\frac{\pi}{4}]$$

$$= A + B$$

$A = 1, B = 1$ putting these values of A and B

$$a_n = (\sqrt{2})^n [\cos \frac{n\pi}{4} + \sin \frac{n\pi}{4}]$$

This is the solution of the given relation under the given conditions.

3. If $a_0 = 0, a_1 = 1, a_2 = 4 \quad and\ a_3 = 37$ satisfy the recurrence realtion

$$a_{n+2} + ba_{n+1} + ca_n = 0 \qquad for\ n \geq 0$$

Determine the constant b and c and then solve the relation for a_n.

Solution:

For $n = 0$ and $n = 1$, the given relation,

$$a_2 + ba_1 + ca_0 = 0 \ \ and \ \ a_3 + ba_2 + ca_1 = 0$$

Substituting the given values of $a_0, a_1, a_2\ and\ a_3$ in this we get

$$4 + b + 0 = 0 \quad and\ 37 + 4b + c = 0$$

$$=> b = -1\ and\ c = -21$$

With these values of b and c, the given recurrence relation

$$a_{n+2} - 4a_{n-1} - 21a_n = 0 \qquad for\ n \geq 0$$

(or)

$$a_n - 4a_{n-1} - 21a_{n-2} = 0 \qquad for\ n \geq 2$$

The characteristic equation for this relation is $k^2 - 4k - 21 = 0$ whose roots are $k_1 = 7\ \ and\ \ k_2 = -3$.

The general solutions for a_n is,

$$a_n = A \times 7^n + B \times (-3)^n$$

A and B are arbitrary constants.

Using the given conditions $a_0 = 0, a_1 = 1$ in this we get,

$$0 = A + B, \qquad 1 = 7A - 3B$$

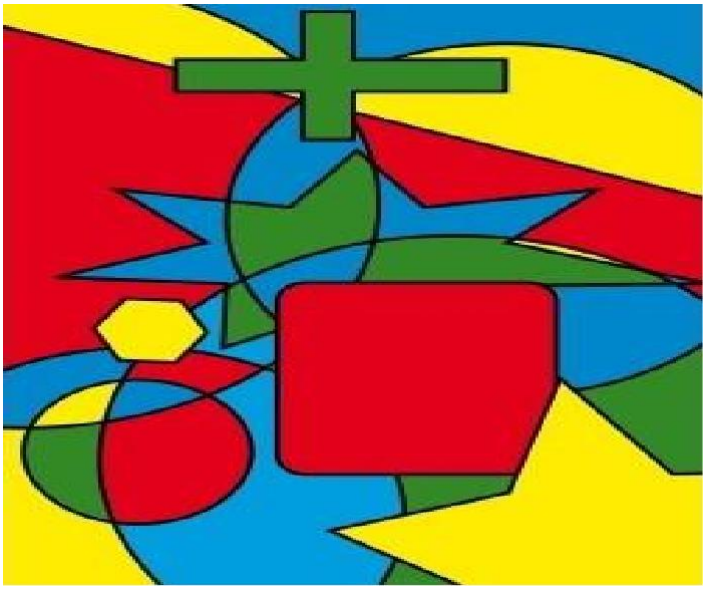
$$=> A = -B = \frac{1}{10}$$

$$therefore, \quad a_n = \frac{1}{10}[7^n - (-3)^n$$

BCS405A

Discrete Mathematical Structures

(For the 4th Semester Computer Science and Engineering Stream)



Module 5

INTRODUCTION TO GROUP THEORY

Content

Groups:

- Definitions, properties,
- Homomrphisms,
- Isomorphisms,
- Cyclic Groups,
- Cosets, and Lagrange's Theorem.

Coding Theory and Rings:

- Elements of CodingTheory,
- The Hamming Metric,
- The Parity Check, and Generator Matrices.

Group Codes:

- Decoding with Coset Leaders,
- Hamming Matrices.

Rings and Modular Arithmetic:

- The Ring Structure – Definition and Examples,

GROUPS

Introduction:

Definitions, Examples, and Elementary Properties:

In m athematics, a **discrete group** is a group *G* equipped with the discrete topology. With this topology *G* becomes a topological group. A **discrete subgroup** of a topological group *G* is a subgroup *H* whose relative topology is the discrete one. For example, the integers, **Z**, form a discrete subgroup of the reals, **R**, but the rational numbers, **Q**, do not.

Any group can be given the discrete topology. Since every map from a discrete space is continuous, the topological homomorphisms between discrete groups are exactly the group homomorphisms between the underlying groups. Hence, there is an isomorphism between the category of groups and the category of discrete groups. Discrete groups can therefore be identified with their underlying (non-topological) groups. With this in mind, the term **discrete group theory** is used to refer to the study of groups without topological structure, in contradistinction to topological or Lie group theory. It is divided, logically but also technically, into finite group theory, and infinite group theory.

There are some occasions when a topological group or Lie group is usefully endowed with the discrete topology, 'against nature'. This happens for example in the theory of the Bohr com pactification, and in group cohomology theory of Lie groups.

Properties:

Since topological groups are homogeneous, one need only look at a single point to determine if the group is discrete. In particular, a topological group is discrete if and only if the singleton containing the identity is an open set.

A discrete group is the same thing as a zero-dimensional Lie group (uncountable discrete groups are not second-co untable so authors who require Lie groups to satisfy this axiom do not regard these groups as Lie groups). The identity component of a discrete group is just the trivial subgroup while the group of components is isomorphic to the group itself.

Since the only Hausdorff topology on a finite set is the discrete one, a finite Hausdorff topological group must necessarily be discrete. It follows that every finite subgroup of a Hausdorff group is discrete.

A discrete subgroup *H* of *G* is co compact if there is a compact subset *K* of *G* such that $HK = G$.

Discrete normal subgroups play an important role in the theory of covering groups and locally isomorphic groups. A discrete normal subgroup of a connected group G necessarily lies in the center of G and is therefore abelian.

Other properties:

- every discrete group is totally disconnected
- every subgroup of a discrete group is discrete.
- every quotient of a discrete group is discrete.
- the product of a finite number of discrete groups is discrete.
- a discrete group is compact if and only if it is finite.
- every discrete group is locally compact.
- every discrete subgroup of a Hausdorff group is closed.
- every discrete subgroup of a compact Hausdorff group is finite.

Examples:

- Frieze groups and wallpaper groups are discrete subgroups of the i sometry group of the Euclidean plane. Wallpaper groups are cocompact, but Frieze groups are not.

- A space group is a discrete subgroup of the i sometry group of Euclidean space of some dimension.
- A crystallographic group usually means a cocompact, discrete subgroup of the isometries of some Euclidean space. Sometimes, however, a crystallographic group can be a cocompact discrete subgroup of a n ilpotent or solvable Lie group.
- Every triangle group T is a discrete subgroup of the isometry group of the sphere (when T is finite), the Euclidean plane (when T has a $\mathbf{Z} + \mathbf{Z}$ subgroup of finite index), or the hyperbolic plane.

Fuchsian groups are, by definition, discrete subgroups of the isometry group of the hyperbolic plane.

o A Fuchsian group that preserves orientation and acts on the upper half-plane model of the hyperbolic plane is a discrete subgroup of the Lie group

o A Fuchsian group that preserves orientation and acts on the upper half-plane model of the hyperbolic plane is a discrete subgroup of the Lie PSL(2,**R**), the group of orientation preserving isometries of the upperhalf-plane model of the hyperbolic plane.

A Fuchsian group is sometimes considered as a s pecial case of a Kleinian group, by embedding the hyperbolic plane isometrically into three dimensional hyperbolic space and ex tending the group action on the plane to the whole space.

The modular group is PSL(2,**Z**), thought of as a discrete subgroup of PSL(2,**R**). The modular group is a lattice in PSL(2,**R**), but it is not cocompact.
Kleinian groups are, by definition, discrete subgroups of the isometry group of hyperbolic 3-space. These include quasi- Fuchsian groups.
A Kleinian group that preserves orientation and acts on the upper half space model of h yperbolic 3-space is a discrete s ubgroup of the Lie group PSL(2,**C**), the group of o rientation preserving isometries of the upper half- space model of h yperbolic 3-space.
A lattice in a Lie group is a discrete subgroup such that the Haar measure of thequotient space is finite.

Group homomorphism:

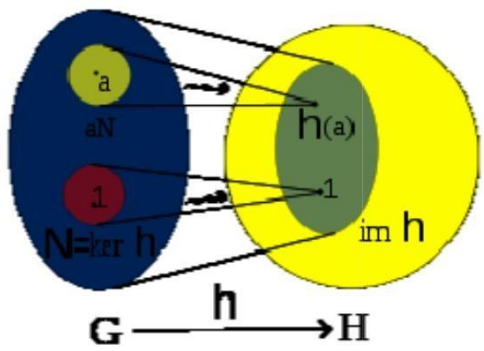


Image of a Group homomorphism(**h**) from **G**(left) to **H**(right). The smaller oval inside **H** is the image of **h**. **N** is the kernel of **h** and **aN** is a coset of **h**.

In mathematics, given two groups (G, *) and (H, ·), a **group homomorphism** from (G, *) to (H, ·) is a function $h : G \to H$ such that for all u and v in G it holds that

$$h(u * v) = h(u) \cdot h(v)$$

where the group operation on the left hand side of the equation is that of G and on the right hand side that of H.

From this property, one can deduce that h maps the identity element e_G of G to the identity element e_H of H, and it also maps inverses to inverses in the sense that

$$h(u^{-1}) = h(u)^{-1}.$$

Hence one can say that h "is compatible with the group s tructure".

Older notations for the homomorphism $h(x)$ may be x_h, though this may be confused as an index or a general subscript. A more recent trend is to write group homomorphisms on the right of their arguments, omitting brackets, so that $h(x)$ becomes simply $x\,h$. This approach is especially prevalent in areas of group theory where automata play a role, since it accords better with the convention that automata read words from left to right.

In areas of mathematics where one considers groups endowed with additional structure, a *homomorphism* sometimes means a map which respects not only the group structure (as above) but also the extra structure. For example, a homomorphism of topological groups is often required to be continuous.

The category of groups

If $h : G \to H$ and $k : H \to K$ are group homomorphisms, then so is $k \circ h : G \to K$. This shows that the class of all groups, together with group homomorphisms as morphisms, forms a category.

Types of homomorphic maps

If the homomorphism h is a bijection, then one can show that its inverse is also a group homomorphism, and h is called a *group isomorphism*; in this case, the groups G and H are called *is omorphic*: they differ only in the notation of their elements and are identical for all p ractical purposes.

If h: $G \to G$ is a group h omomorphism, we call it an *endomorphism* of G. If furthermore it is bijective and hence an isomorphism, it is called an *automorphism*. The set of all automorphisms of a group G, with functional composition as operation, forms itself a group, the *automorphism group* of G. It is denoted by Aut(G). As an example, the automorphism group of ($\mathbf{Z}$, +) contains only two elements, the identity transformationand multiplication with -1; it is isomorphic to $\mathbf{Z}/2\mathbf{Z}$.

An **epimorphism** is a surjective homomorphism, that is, a homomorphism which is *onto* as a function. A **monomorphism** is an injective homomorphism, that is, a homomorphism which is *one-to-one* as a function.

Homomorphisms of abelian groups

If G and H are abelian (i.e. commutative) groups, then the set Hom(G, H) of all group homomorphisms from G to H is itself an abelian group: the sum $h + k$ of two homomorphisms is defined by

$$(h + k)(u) = h(u) + k(u) \quad \text{for all } u \text{ in } G.$$

The commutativity of H is needed to prove that $h + k$ is again a group homomorphism. The addition of homomorphisms is compatible with the composition of homomorphisms in the following sense: if f is in Hom(K, G), h, k are elements of Hom(G, H), and g is in Hom(H,L), then

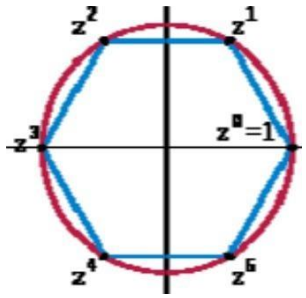
$$(h + k) \circ f = (h \circ f) + (k \circ f) \quad \text{and} \quad g \circ (h + k) = (g \circ h) + (g \circ k).$$

This shows that the set End(G) of all endomorphisms of an abelian group forms a ring, the *endomorphism ring* of G. For example, the endomorphism ring of the abelian group consisting of the direct sum of m copies of **Z**/**nZ** is isomorphic to the ring of m-by-m matrices with entries in **Z**/n**Z**. The above compatibility also shows that the category of all abelian groups with group ho momorphisms forms a preadditive category; the existence of direct sums and well-behaved kernels makes this category the prototypical example of an abelian category.

Cyclic group

In group theory, a **cyclic group** is a group that can be generated by a single element, in the sense that the group has an element g (called a "generator" of the group) such that, when written multiplicatively, every element of the group is a power of g (a multiple of g when the notation is additive).

Definition



The six 6th complex roots of unity form a cyclic group under multiplication. z is a primitive element, but z^2 is not, because the odd powers of z are not a power of z^2.

A group G is called cyclic if there exists an element g in G such that $G = \langle g \rangle = \{ g^n \mid n$ is an integer $\}$. Since any group generated by an element in a group is a subgroup of that group, showing that the only subgroup of a group G that contains g is G itself suffices to show that G is cyclic.

For example, if $G = \{ g^0, g^1, g^2, g^3, g^4, g^5 \}$ is a group, then $g^6 = g^0$, and G is cyclic. In fact, G is essentially the same as (that is, isomorphic to) the set { 0, 1, 2, 3, 4, 5 } with addition modulo 6. For example, 1 + 2 = 3 (mod 6) cor responds to $g^1 \cdot g^2 = g^3$, and 2 + 5 = 1 (mod 6) corresponds to $g^2 \cdot g^5 = g^7 = g^1$, and so on. One can use the isomorphism φ defined by $\varphi(g^i) =$ i.

For every positive integer n there is exactly one cyclic group (up to isomorphism) whose order is n, and there is exactly one infinite cyclic group (the integers under addition). Hence, the cyclic groups are the simplest groups and they are completely classified.

The name "cyclic" may be m isleading: it is possible to generate infinitely many elements and not form any literal cycles; that is, every g^n is distinct. (It can be said that it has one infinitely long cycle.) A group generated in this way is called an **infinite cyclic group**, and is isomorphic to the additive group of integers **Z**.

Furthermore, the circle group (whose elements are uncountable) is *not* a cyclic group—a cyclic group always has countable elements.

Since the cyclic groups are abelian, they are often written additively and denoted $\mathbf{Z}_n$. However, this notation can be problematic for number theorists because it conflicts with the usual notation for *p*-adic number rings or localization at a prime ideal. The quotient notations $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Z}/n$, and $\mathbf{Z}/(n)$ are standard alternatives. We adopt the first of these here to avoid the collision of notation. See also the section Subgroups and notation below.

One may write the group multiplicatively, and denote it by C_n, where n is the order (which can be ∞). For example, $g^3g^4 = g^2$ in C_5, whereas $3 + 4 = 2$ in $\mathbf{Z}/5\mathbf{Z}$.

Properties

The fundamental theorem of cyclic groups states that if G is a cyclic group of order n then every subgroup of G is cyclic. Moreover, the order of any subgroup of G is a divisor of n and for each positive divisor k of n the group G has exactly one subgroup of order k. This property characterizes finite cyclic groups: a group of order n is cyclic if and only if for every divisor d of n the group has at most one subgroup of order d. Sometimes the e quivalent s tatement is used: a group of order n is cyclic if and only if for every divisor d of n the group has exactly one subgroup of order d.

Every finite cyclic group is i somorphic to the group { [0], [1], [2], ..., [n - 1] } of integers modulo n under addition, and any infinite cyclic group is isomorphic to $\mathbf{Z}$ (the set of all integers) under addition. Thus, one only needs to look at such groups to understand the properties of cyclic groups in general. Hence, cyclic groups are one of the simplest groups to study and a number of nice p roperties are known.

Given a cyclic group G of order n (n may be infinity) and for every g in G,

- G is abelian; that is, their group operation is com mutative: $gh = hg$ (for all h in G). This is so since $g + h \bmod n = h + g \bmod n$.
- If n is finite, then $g^n = g^0$ is the identity element of the group, since $kn \bmod n = 0$ for any integer k.
- If $n = \infty$, then there are exactly two elements that generate the group on their own: namely 1 and -1 for $\mathbf{Z}$
- If n is finite, then there are exactly $\varphi(n)$ elements that generate the group on their own, where φ is the Euler totient function
- Every subgroup of G is cyclic. Indeed, each finite subgroup of G is a group of { 0,

1, 2, 3, ... m - 1} with addition m odulo m. And each infinite subgroup of G is $m\mathbf{Z}$ for some m, which is bijective to (so is omorphic to) **Z**.

- G_n is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ (factor group of **Z** over $n\mathbf{Z}$) since $\mathbf{Z}/n\mathbf{Z} = \{0 + n\mathbf{Z}, 1 + n\mathbf{Z}, 2 + n\mathbf{Z}, 3 + n\mathbf{Z}, 4 + n\mathbf{Z}, ..., n - 1 + n\mathbf{Z}\}$ $\cong \{0, 1, 2, 3, 4, ..., n - 1\}$ under addition modulo n.

More generally, if d is a divisor of n, then the number of elements in $\mathbf{Z}/n$ which have order d is $\varphi(d)$. The order of the residue class of m is n / gcd(n,m).

If p is a prime number, then the only group (up to isomorphism) with p elements is the cyclic group C_p or $\mathbf{Z}/p\mathbf{Z}$.

The direct product of two cyclic groups $\mathbf{Z}/n\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z}$ is cyclic if and only if n and m are coprime. Thus e.g. $\mathbf{Z}/12\mathbf{Z}$ is the direct product of $\mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$, but not the direct product of $\mathbf{Z}/6\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z}$.

The definition immediately implies that cyclic groups have very simple group presentation $C_\infty = < x \mid >$ and $C_n = < x \mid x^n >$ for finite n.

A primary cyclic group is a group of the form $\mathbf{Z}/p^k$ where p is a prime number. The fundamental theorem of abelian groups states that every finitely generated abelian group is the direct p roduct of finitely many finite primary cyclic and infinite cyclic groups.

$\mathbf{Z}/n\mathbf{Z}$ and **Z** are also commutative rings. If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a finite field, also denoted by $\mathbf{F}_p$ or $\mathbf{GF}(p)$. Every field with p elements is isomorphic to this one.

The units of the ring $\mathbf{Z}/n\mathbf{Z}$ are the numbers coprime to n. They form a group under multiplication modulo n with $\varphi(n)$ elements (see above). It is written as $(\mathbf{Z}/n\mathbf{Z})^\times$. For example, when $n = 6$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,5\}$. When $n = 8$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,3,5,7\}$.

In fact, it is known that $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic if and only if n is 1 or 2 or 4 or p^k or 2 p^k for an odd prime number p and $k \geq 1$, in which case every generator of $(\mathbf{Z}/n\mathbf{Z})^\times$ is called a primitive root modulo n. Thus, $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic for $n = 6$, but not for $n = 8$, where it is instead i somorphic to the Klein four-group.

The group $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic with p - 1 elements for every prime p, and is also written $(\mathbf{Z}/p\mathbf{Z})^*$ because it consists of the non-zero elements. More generally, every *finite*

s ubgroup of the mu ltiplicative group of any field is cyclic.

Examples

In 2D and 3D the symmetry group for n-fold rotational symmetry is C_n, of abstract group type Z_n. In 3D there are also other symmetry groups which are algebraically the same, see *Symmetry groups in 3D that are cyclic as abstract group*.

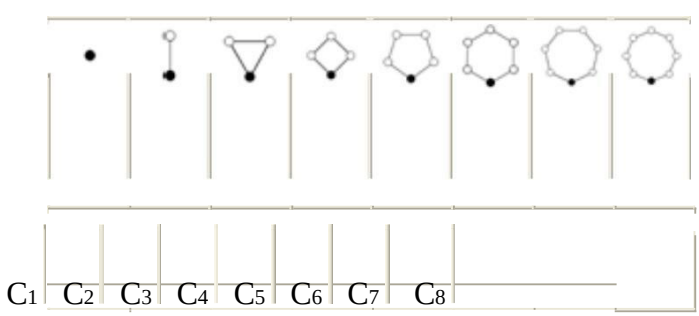
Note that the group S^1 of all rotations of a circle (the circle group) is *not* cyclic, since it is not even countable.

The nth roots of unity form a cyclic group of order n under multiplication. e.g., $0 = z^3 - 1 = (z - s^0)(z - s^1)(z - s^2)$ where $s^i = e^{2\pi i / 3}$ and a group of $\{s^0, s^1, s^2\}$ under mul tiplication is cyclic.

The Galois group of every finite field extension of a finite field is finite and cyclic; conversely, given a finite field F and a finite cyclic group G, there is a finite field extension of F whose Galois group is G.

Representation

The cycle graphs of finite cyclic groups are all n-sided polygons with the elements at the vertices. The dark vertex in the cycle graphs below stand for the identity element, and the other vertices are the other elements of the group. A cycle consists of successive powers of either of the elements connected to the identity element.



The rep resentation theory of the cyclic group is a critical base case for the representation theory of more general finite groups. In the complex case, a representation of a cyclic group d ecomposes into a direct sum of linear c haracters, making the connection between

character theory and repre sentation theory transparent. In the positive ch aracteristic case, the indecomposable repre sentations of the cyclic group form a model and inductive basis for the rep resentation theory of groups with cyclic Sylow subgroups and more generally the representation theory of blocks of cyclic defect.

Subgroups and notation

All subgroups and quotient groups of cyclic groups are cyclic. Specifically, all subgroups of **Z** are of the form $m\mathbf{Z}$, with m an integer ≥ 0. All of these subgroups are different, and apart from the trivial group (for $m=0$) all are isomorphic to **Z**. The lattice of subgroups of **Z** is isomorphic to the dual of the lattice of natural numbers ordered by divisibility. All factor groups of **Z** are finite, except for the trivial exception $\mathbf{Z}/\{0\} = \mathbf{Z}/0\mathbf{Z}$. For every positive divisor d of n, the quotient group $\mathbf{Z}/n\mathbf{Z}$ has precCSEly one subgroup of order d, the one generated by the residue class of n/d. There are no other subgroups. The lattice of subgroups is thus isomorphic to the set of divisors of n, ordered by divisibility. In particular, a cyclic group is simple if and only if its order (the number of its elements) is prime.

Using the quotient group formalism, $\mathbf{Z}/n\mathbf{Z}$ is a standard notation for the additive cyclic group with n elements. In ring terminology, the s ubgroup $n\mathbf{Z}$ is also the ideal (n), so the quotient can also be written $\mathbf{Z}/(n)$ or $\mathbf{Z}/n$ without abuse of notation. These alternatives do not conflict with the notation for the p-adic integers. The last form is very common in informal calculations; it has the additional advantage that it reads the same way that the group or ring is often described verbally, "Zee mod en".

As a p ractical problem, one may be given a finite subgroup C of order n, generated by an element g, and asked to find the size m of the subgroup generated by g^k for some integer k. Here m will be the smallest integer > 0 such that mk is divisible by n. It is therefore n/m where $m = (k, n)$ is the greatest common divisor of k and n. Put another way, the index of the subgroup generated by g^k is m. This reasoning is known as the **index calculus algorithm**, in number theory.

Endomorphisms

The endomorphism ring of the abelian group $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ itself as a ring. Under this isomorphism, the number r corresponds to the endomorphism of $\mathbf{Z}/n\mathbf{Z}$ that maps each element to the sum of r copies of it. This is a bijection if and only if r is

coprime with n, so the automorphism group of $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to the unit group $(\mathbf{Z}/n\mathbf{Z})^\times$ (see above).

Similarly, the endomorphism ring of the additive group $\mathbf{Z}$ is isomorphic to the ring $\mathbf{Z}$. Its automorphism group is iso morphic to the group of units of the ring $\mathbf{Z}$, i.e. to $\{-1, +1\} \cong C_2$.

Virtually cyclic groups

A group is called **virtually cyclic** if it contains a cyclic subgroup of finite index (the number of cosets that the subgroup has). In other words, any element in a virtually cyclic group can be arrived at by applying a member of the cyclic subgroup to a member in a certain finite set. Every cyclic group is virtually cyclic, as is every finite group. It is known that a finitely generated discrete group with exactly two *ends* is virtually cyclic

(for instance the product of $\mathbf{Z}/n$ and $\mathbf{Z}$). Every abelian subgroup of a Gromov hyperbolic group is virtually cyclic.

Group isomorphism

In abstract algebra, a **group isomorphism** is a function between two groups that sets up a one-to-one corre spondence between the elements of the groups in a way that respects the given group operations. If there exists an isomorphism between two groups, then the groups are called **isomorphic**. From the standpoint of group theory, isomorphic groups have the same p roperties and need not be distinguished.

Definition and notation

Given two groups $(G, *)$ and $(H, \odot)$, a *group isomorphism* from $(G, *)$ to $(H, \odot)$ is a bijective group homomorphism from G to H. Spelled out, this means that a group i somorphism is a bijective function $f : G \to H$ such that for all u and v in G it holds that

$$f(u * v) = f(u) \odot f(v)$$

The two groups $(G, *)$ and $(H, \odot)$ are isomorphic if an isomorphism exists. This is

written:

$$(G,*) \cong (H,\odot)$$

Often shorter and more simple notations can be used. Often there is no ambiguity about the group operation, and it can be omitted:

$$G \cong H$$

Sometimes one can even simply write $G = H$. Whether such a notation is possible without confusion or ambiguity depends on context. For example, the equals sign is not very suitable when the groups are both subgroups of the same group. See also the examples.

Conversely, given a group (G, *), a set H, and a bijection $f : G \to H$, we can make H a group (H, $\odot$) by defining

$$f(u) \odot f(v) = f(u * v)$$

If $H = G$ and $\odot = *$ then the bijection is an automorphism (*q.v.*)

In tuitively, group theorists view two iso morphic groups as follows: For every element g of a group G, there exists an element h of H such that h 'behaves in the same way' as g (operates with other elements of the group in the same way as g). For instance, if g generates G, then so does h. This implies in particular that G and H are in bijective cor respondence. So the definition of an isomorphism is quite natural.

An i somorphism of groups may equivalently be defined as an i nvertible morphism in the category of groups.

Examples

- The group of all real numbers with addition, ($\mathbb{R}$,+), is isomorphic to the group of all positive real numbers with multiplication ($\mathbb{R}^+$,×):

$$(\mathbb{R},+) \cong (\mathbb{R}^+,\times)$$

via the isomorphism

$$f(x) = e^x$$

(see ex ponential function).

- The group $\mathbb{Z}$ of integers (with addition) is a subgroup of $\mathbb{R}$, and the factor group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the group S^1 of complex numbers of absolute value 1 (with mul tiplication):

$$\mathbb{R}/\mathbb{Z} \cong S^1$$

An isomorphism is given by

$$f(x + \mathbb{Z}) = e^{2\pi x i}$$

for every x in $\mathbb{R}$.

The Klein four-group is isomorphic to the direct product of two copies of $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ (see modular arithmetic), and can therefore be written $\mathbb{Z}_2 \times \mathbb{Z}_2$. Another notation is Dih_2, because it is a dihedral group.

- Generalizing this, for all odd n, Dih_{2n} is isomorphic with the direct product of Dih_n and Z_2.

- If $(G, *)$ is an infinite cyclic group, then $(G, *)$ is isomorphic to the integers (with the addition operation). From an algebraic point of view, this means that the set of all integers (with the addition operation) is the 'only' infinite cyclic group.

Some groups can be proven to be isomorphic, relying on the axiom of choice, while it is even theoretically impossible to construct concrete isomorphisms. Examples:

- The group $(\mathbb{C}, +)$ is isomorphic to the group $(\mathbb{C}, +)$ of all <u>complex numbers</u> with addition.
- The group $(\mathbb{C}^*, \cdot)$ of non-zero complex numbers with multiplication as operation is isomorphic to the group S^1 mentioned above.

<u>Properties</u>

- The <u>kernel</u> of an isomorphism from $(G, *)$ to $(H, \bar{*})$ is always $\{e_G\}$ where e_G is the identity of the group $(G, *)$
- If $(G, *)$ is isomorphic to $(H, \bar{*})$ and if G is <u>abelian</u> then so is H.
- If $(G, *)$ is a group that is isomorphic to $(H, \bar{*})$ [where f is the isomorphism], then if a belongs to G and has <u>order n</u>, then so does $f(a)$.
- If $(G, *)$ is a <u>locally finite group</u> that is isomorphic to $(H, \bar{*})$, then $(H, \bar{*})$ is also locally finite.
- The previous examples illustrate that 'group properties' are always preserved by isomorphisms.

<u>Cyclic groups</u>

All cyclic groups of a given order are isomorphic to $\mathbb{Z}_n, +_n$.
Let G be a cyclic group and n be the order of G. G is then the group generated by $< x > = \{e, x, ..., x^{n-1}\}$. We will show that

$$G \cong \mathbb{Z}_n, +_n$$

Define

$\varphi : G \to \mathbb{Z}_n = \{0, 1, ..., n-1\}$ so that $\varphi(x^a) = a$. Clearly, φ is bijective.

Then

$$\varphi(x^a \cdot x^b) = \varphi(x^{a+b}) = a + b = \varphi(x^a) +_n \varphi(x^b)$$

which proves that $G \cong \mathbb{Z}_n, +_n$

<u>Consequences</u>

From the definition, it follows that any isomorphism $f : G \to H$ will map the identity element of *G* to the identity element of *H*,

$$f(e_G) = e_H$$

that it will map inverses to inverses,

$$f(u^{-1}) = [f(u)]^{-1}$$

and more generally, *n*th powers to *n*th powers,

$$f(u^n) = [f(u)]^n$$

for all *u* in *G*, and that the inverse map $f^{-1} : H \to G$ is also a group isomorphism.

The relation "being isomorphic" satisfies all the axioms of an equivalence relation. If *f* is an isomorphism between two groups *G* and *H*, then everything that is true about *G* that is only related to the group s tructure can be translated via *f* into a true ditto s tatement about *H*, and vice versa.

<u>Automorphisms</u>

An isomorphism from a group (G,*) to itself is called an automorphism of this group. Thus it is a bijection $f : G \to G$ such that

$$f(u) * f(v) = f(u * v).$$

An au tomorphism always maps the identity to itself. The image under an au tomorphism of a conjugacy class is always a conjugacy class (the same or another). The image of an element has the same order as that element.

The composition of two automorphisms is again an automorphism, and with this operation the set of all automorphisms of a group G, denoted by Aut(G), forms itself a group, the *au tomorphism group* of G.

For all Abelian groups there is at least the automorphism that replaces the group elements by their inverses. However, in groups where all elements are equal to their inverse this is the trivial automorphism, e.g. in the Klein four-group. For that group all permutations of the three non-identity elements are automorphisms, so the automorphism group is i somorphic to S_3 and Dih_3.

In Z_p for a prime number p, one non-identity element can be replaced by any other, with cor responding changes in the other elements. The automorphism group is isomorphic to Z_{p-1}. For example, for $n = 7$, multiplying all elements of Z_7 by 3, modulo 7, is an automorphism of order 6 in the automorphism group, because $3^6 = 1$ (modulo 7), while lower powers do not give 1. Thus this automorphism generates Z_6. There is one more automorphism with this property: multiplying all elements of Z_7 by 5, modulo 7. Therefore, these two correspond to the elements 1 and 5 of Z_6, in that order or conversely.

The automorphism group of Z_6 is isomorphic to Z_2, because only each of the two elements 1 and 5 generate Z_6, so apart from the identity we can only interchange these.

The automorphism group of $Z_2 \times Z_2 \times Z_2 = \mathrm{Dih}_2 \times Z_2$ has order 168, as can be found as follows. All 7 non-identity elements play the same role, so we can choose which plays the role of (1,0,0). Any of the remaining 6 can be chosen to play the role of (0,1,0). This determines which corresponds to (1,1,0). For (0,0,1) we can choose from 4, which determines the rest. Thus we have $7 \times 6 \times 4 = 168$ automorphisms. They correspond to those of the Fano plane, of which the 7 points correspond to the 7 non-identity elements

The lines connecting three points correspond to the group operation: a, b, and c on one line means a+b=c, a+c=b, and b+c=a. See also general linear group over finite fields.

For Abelian groups all automorphisms except the trivial one are called outer automorphisms.

Non-Abelian groups have a non-trivial inner automorphism group, and possibly also outer automorphisms.

Coding Theory and Rings

Elements of Coding Theory

Coding theory is studied by various scientific di sciplines — such as info rmation theory, electrical engineering, mathematics, and computer science — for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of r edundancy and the correction (or detection) of errors in the transmitted data. It also includes the study of the properties of codes and their fitness for a specific application.

Thus, there are es sentially two aspects to Coding theory:

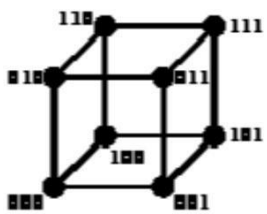
1. Data compression (or, *source coding*)
2. Error correction (or, *channel coding')*

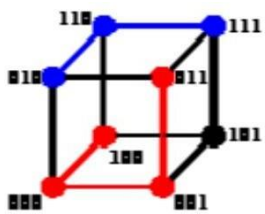
These two aspects may be studied in combination.

The first, source encoding, attempts to compress the data from a source in order to transmit it more efficiently. This practice is found every day on the Internet where the common "Zip" data compression is used to reduce the network load and make files smaller. The second, channel encoding, adds extra data bits to make the transmission of
data more robust to dis turbances present on the transmission channel. The ordinary user may not be aware of many applications using channel coding. A typical music CD uses the Reed-Solomon code to correct for scratches and dust. In this application the transmission channel is the CD itself. Cell phones also use coding techniques to correct

for the fading and noCSE of high frequency radio transmission. Data modems, t elephone transmissions, and NASA all employ channel coding techniques to get the bits through, for example the turbo code and LDPC codes.

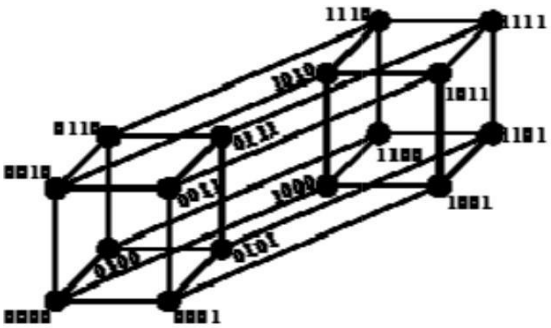
The hamming metric:



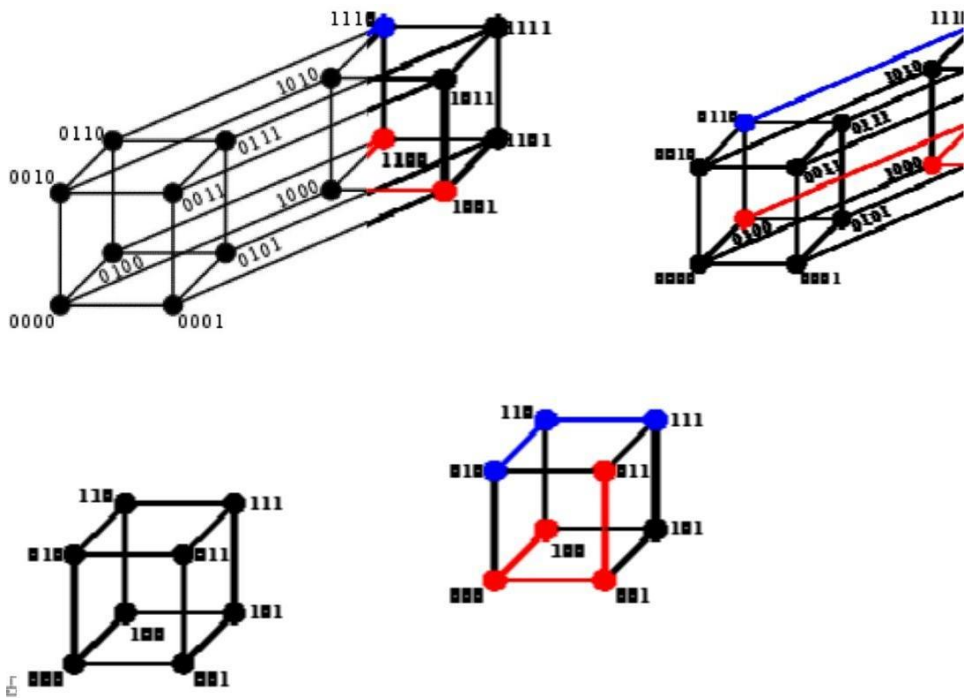


3-bit binary cube for finding Hamming distance

Two example distances: 100->011 has distance 3 (red path); 010->111 has distance 2 (blue path)



4-bit binary h ypercube for finding Hamming distance



Two example dis tances: 0100->1001 has distance 3 (red path); 0110->1110 has distance 1 (blue path)

In information theory, the **Hamming distance** between two strings of equal length is the number of positions at which the corresponding symbols are different. Put another way, it

Parity-check matrix

In coding theory, a **parity-check matrix** of a linear block code **C** is a generator matrix of the dual code. As such, a codeword c is in **C** if and only if the matrix-vector product $\mathbf{H}^{\mathbf{T}}c=\mathbf{0}$.

The rows of a parity check matrix are parity checks on the codewords of a code. That is, they show how linear combinations of certain digits of each codeword equal zero. For example, the parity check matrix

specifies that for each codeword, digits 1 and 2 should sum to zero and digits 3 and 4 should sum to zero.

Creating a parity check matrix

The parity check matrix for a given code can be derived from its generator matrix (and vice-versa). If the generator matrix for an [*n*,*k*]-code is in standard form

$$G = \left[I_k | P\right],$$

then the parity check matrix is given by

$$H = \left[-P^T | I_{n-k}\right],$$

because

$GH^T = P - P = 0.$

Negation is performed in the finite field mod *q*. Note that if the characteristic of the underlying field is 2 (i.e., 1 + 1 = 0 in that field), as in binary codes, then - *P* = *P*, so the negation is unnecessary.

For example, if a binary code has the generator matrix

$$G = \begin{bmatrix} 10|101 \\ 01|110 \end{bmatrix}$$

The parity check matrix becomes

$$H = \begin{bmatrix} 11|100 \\ 01|010 \\ 10|001 \end{bmatrix}$$

For any valid codeword x, $Hx = 0$. For any invalid codeword $\tilde{x}$, the syndrome S satisfies

$$H\tilde{x} = S$$

Parity check

If no error occurs during transmission, then the received codeword r is identical to the t ransmitted codeword x:

$$\mathbf{r} = \mathbf{x}$$

The receiver multiplies H and r to obtain the **syndrome** vector $\mathbf{z}$, which indicates whether an error has occurred, and if so, for mul which codeword bit. Performing this tiplication (again, entries modulo 2):

$$\mathbf{z} = \mathbf{H}\mathbf{r} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Since the syndrome z is the null vector, the receiver can conclude that no error has occurred. This conclusion is based on the observation that when the data vector is multiplied by $\mathbf{G}$, a change of basis occurs into a vector subspace that is the kernel of $\mathbf{H}$. As long as nothing happens during transmission, $\mathbf{r}$ will remain in the kernel of $\mathbf{H}$ and the mul tiplication will yield the null vector.

Coset

In mathematics, if G is a group, H is a subgroup of G, and g is an element of G, then

$gH = \{gh : h$ an element of H is$\}$ a **left coset of *H*** in G, and

$Hg = \{hg : h$ an element of H is$\}$ a **right coset of *H*** in G.

Only when H is normal will the right and left cosets of H coincide, which is one definition of normality of a subgroup.

A **coset** is a left or right coset of *some* subgroup in G. Since $Hg = g(g^{-1}Hg)$, the right cosets Hg (of H) and the left cosets $g(g^{-1}Hg)$ (of the conjugate subgroup $g^{-1}Hg$) are the same. Hence it is not meaningful to speak of a coset as being left or right unless one first specifies the underlying s ubgroup.

For abelian groups or groups written additively, the notation used changes to $g+H$ and $H+g$ respectively.

Examples

The additive cyclic group $\mathbf{Z}_4 = \{0, 1, 2, 3\} = G$ has a subgroup $H = \{0, 2\}$ (isomorphic to $\mathbf{Z}_2$). The left cosets of H in G are

$0 + H = \{0, 2\} = H$

$1 + H = \{1, 3\}$

$2 + H = \{2, 0\} = H$

$3 + H = \{3, 1\}$.

There are therefore two distinct cosets, H itself, and $1 + H = 3 + H$. Note that every element of G is either in H or in $1 + H$, that is, $H \cup (1 + H) = G$, so the distinct cosets of H in G partition G. Since $\mathbf{Z}_4$ is an abelian group, the right cosets will be the same as the left.

Another example of a coset comes from the theory of vector spaces. The elements

(vectors) of a vector space form an Abelian group under vector addition. It is not hard to show that subspaces of a vector space are subgroups of this group. For a vector space *V*, a s ubspace *W*, and a fixed vector *a* in *V*, the sets

$$\{x \in V : x = a + n, n \in W\}$$

are called affine subspaces, and are cosets (both left and right, since the group is Abelian). In terms of geometric vectors, these affine subspaces are all the "lines" or "planes" parallel to the subspace, which is a line or plane going through the origin.

General properties

We have $gH = H$ if and only if g is an element of H, since as H is a subgroup, it must be closed and must contain the identity.

Any two left cosets of H in G are either identical or disjoint — i.e., the left cosets form a partition of G such that every element of G belongs to one and only one left coset.[1] In particular the identity is in precCSEly one coset, and that coset is H itself; this is also the only coset that is a subgroup. We can see this clearly in the above examples.

The left cosets of H in G are the eq~~uivalence classes und~~er the equ~~ivalence relation on G~~ given by $x \sim y$ if and only if $x^{-1}y$?H. Similar statements are also true for right cosets.

A **coset representative** is a representative in the equivalence class sense. A set of representatives of all the cosets is called a transversal. There are other types of equivalence relations in a group, such as conjugacy, that form different classes which do not have the properties discussed here. Some books on very applied group theory erroneously identify the conjugacy class as 'the' equivalence class as opposed to a particular type of equivalence class.

Index of a subgroup

All left cosets and all right cosets have the same order (number of elements, or cardinality in the case of an infinite H), equal to the order of H (because H is itself a coset). Furthermore, the number of left cosets is equal to the number of right cosets and is

known as the **index** of H in G, written as $[G : H]$ Lagrange's theorem allows us to compute the index in the case where G and H are finite, as per the formula:

$$|G| = [G : H] \, |H|$$

This equation also holds in the case where the groups are infinite, although the meaning may be less clear.

Cosets and normality

If H is not normal in G, then its left cosets are different from its right cosets. That is, there is an a in G such that no element b satisfies $aH = Hb$. This means that the partition of G into the left cosets of H is a different partition than the partition of G into right cosets of H. (It is important to note that *some* cosets may coincide. For example, if a is in the center of G, then $aH = Ha$.)

On the other hand, the subgroup N is normal if and only if $gN = Ng$ for all g in G. In this

Lagrange's theorem (group theory)

Lagrange's theorem, in the mat hematics of group theory, states that for any finite group G, the order (number of elements) of every subgroup H of G divides the order of G. The theorem is named after Joseph Lagrange.

Proof of Lagrange's Theorem

This can be shown using the concept of left cosets of H in G. The left cosets are the equivalence classes of a certain equivalence relation on G and therefore form a partition of G. Specifically, x and y in G are related if and only if there exists h in H such that $x = yh$. If we can show that all cosets of H have the same number of elements, then each coset of H has precCSEly $|H|$ elements. We are then done since the order of H times the number of cosets is equal to the number of elements in G, thereby proving that the order H divides the order of G. Now, if aH and bH are two left cosets of H, we can define a map $f : aH \to bH$ by setting $f(x) = ba^{-1}x$. This map is b ijective because its inverse is given by

$f^{-1}(y) = ab^{-1}y$.

This proof also shows that the quotient of the orders $|G| / |H|$ is equal to the index $[G : H]$

(the number of left cosets of H in G). If we write this statement as

$$|G| = [G : H] \cdot |H|,$$

then, seen as a statement about cardinal numbers, it is equivalent to the Axiom of choice.

Using the theorem

A consequence of the theorem is that the order of any element a of a finite group (i.e. the smallest positive integer number k with $a^k = e$, where e is the identity element of the group) divides the order of that group, since the order of a is equal to the order of the cyclic subgroup generated by a. If the group has n elements, it follows

$$a^n = e.$$

This can be used to prove Fermat's little theorem and its generalization, Euler's theorem. These special cases were known long before the general theorem was proved.

The theorem also shows that any group of prime order is cyclic and simple.

E xistence of subgroups of given order

Lagrange's theorem raCSEs the converse question as to whether every divisor of the order of a group is the order of some subgroup. This does not hold in general: given a finite group G and a divisor d of $|G|$, there does not necessarily exist a subgroup of G with order d. The smallest example is the alternating group $G = A_4$ which has 12 elements but no subgroup of order 6. A *CLT group* is a finite group with the property that for every divisor of the order of the group, there is a subgroup of that order. It is known that a CLT group must be solvable and that every supersolvable group is a CLT group: however there exists solvable groups which are not CLT and CLT groups which are not super solvable.

There are partial converses to Lagrange's theorem. For general groups, Cauchy's theorem guarantees the existence of an element, and hence of a cyclic subgroup, of order any prime dividing the group order; Sylow's theorem extends this to the existence of a s ubgroup of order equal to the maximal power of any prime dividing the group order. For s olvable groups, Hall's theorems assert the existence of a subgroup of order equal to any

unitary divisor of the group order (that is, a divisor coprime to its cofactor).

Group Co des: Deco ding wthi Coset L ead ers, Hamming Matrices

R ings a nd Mod ular Arithmetic: The Ring Structure – Definition and E xampl es, Ring P ro pe rt ies and Sub str uctures, The I ntegers Mod ulo n

In computer science, **group codes** are a type of code. Group codes consist of *n* linear block cod~~es which are~~ subgroups of G^n, where G is a finite Abelian group.

A systematic group code C is a code over G_n of order defined by $|G|^k$ n - k homomorphisms which determine the parity check bits. The remaining k bits are the in formation bits themselves.

Construction

Group codes can be constructed by special generator matrices which resemble generator matrices of linear block codes except that the elements of those matrices are endomorphisms of the group instead of symbols from the code's alphabet. For example, consider the generator matrix

$$G = \begin{pmatrix} \begin{pmatrix} 00 \\ 11 \end{pmatrix} & \begin{pmatrix} 01 \\ 01 \end{pmatrix} & \begin{pmatrix} 11 \\ 01 \end{pmatrix} \\ \begin{pmatrix} 00 \\ 11 \end{pmatrix} & \begin{pmatrix} 11 \\ 11 \end{pmatrix} & \begin{pmatrix} 00 \\ 00 \end{pmatrix} \end{pmatrix}$$

The elements of this matrix are 2*x*2 matrices which are endomorphisms. In this scenario, each codeword can be represented as $g_1^{m_1} g_2^{m_2} \cdots g_r^{m_r}$ where $g_1,\ldots g_r$ are the generators of G.

Decoding with Coset leader

In the field of coding theory, a **coset leader** is defined as a word of minimum weight in any particular coset - that is, a word with the lowest amount of non-zero entries. Sometimes there are several words of equal minimum weight in a coset, and in that case,

any one of those words may be chosen to be the coset leader.

Coset leaders are used in the construction of a standard array for a linear code, which can then be used to decode received vectors. For a received vector y, the decoded message is $y - e$, where e is the coset leader of y. Coset leaders can also be used to construct a fast decoding strategy. For each coset leader u we calculate the syndrome uH'. When we receive v we evaluate vH' and find the matching syndrome. The corresponding coset leader is the most likely error pattern and we assume that $v+u$ was the codeword sent.

Example

A standard array for an $[n,k]$-code is a q^{n-k} by q^k array where:

1. The first row lists all codewords (with the 0 codeword on the extreme left)
2. Each row is a coset with the coset leader in the first column
3. The entry in the i-th row and j-th column is the sum of the i-th coset leader and the j-th codeword.

For example, the $[n,k]$-code C_3 = {0, 01101, 10110, 11011} has a standard array as follows:

0	01101	10110	11011
10000	11101	00110	01011
01000	00101	11110	10011
00100	01001	10010	11111
00010	01111	10100	11001
00001	01100	10111	11010
11000	10101	01110	00011
10001	11100	00111	01010

Note that the above is only one possibility for the standard array; had 00011 been chosen as the first coset leader of weight two, another standard array rep resenting the code would have been con structed.

Note that the first row contains the 0 vector and the codewords of C_3 (0 itself being a codeword). Also, the leftmost column contains the vectors of minimum weight enumerating vectors of weight 1 first and then using vectors of weight 2. Note also that each possible vector in the vector space appears exactly once.

Because each possible vector can appear only once in a standard array some care must be taken during cons truction. A s tandard array can be created as follows:

1. List the codewords of *C*, starting with 0, as the first row
2. Choose any vector of minimum weight not already in the array. Write this as the first entry of the next row. This vector is denoted the '**coset leader**'.
3. Fill out the row by adding the coset leader to the codeword at the top of each column. The sum of the i-th coset leader and the j-th codeword becomes the entry in row i, column j.
4. Repeat steps 2 and 3 until all rows/cosets are listed and each vector appears exactly once.

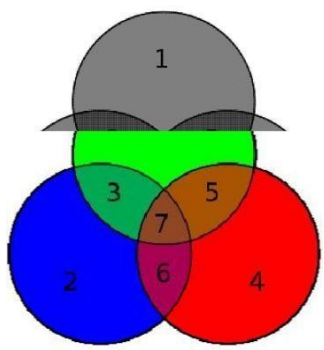
Hamming matrices

Hamming codes can be computed in linear algebra terms through matrices because Hamming codes are linear codes. For the purposes of Hamming codes, two **Hamming matrices** can be defined: the **code generator matrix** and the **parity-check matrix**:

$$\mathbf{G} := \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$\mathbf{H} := \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$



Bit position of the data and parity bits

As mentioned above, rows 1, 2, & 4 of $\mathbf{G}$ should look familiar as they map the data bits to their parity bits:

- p_1 covers d_1, d_2, d_4
- p_2 covers d_1, d_3, d_4
- p_3 covers d_2, d_3, d_4

The remaining rows (3, 5, 6, 7) map the data to their position in encoded form and there is only 1 in that row so it is an identical copy. In fact, these four rows are linearly independent and form the identity matrix (by design, not coincidence).

Also as mentioned above, the three rows of $\mathbf{H}$ should be familiar. These rows are used to compute the **syndrome vector** at the receiving end and if the s yndrome vector is the null

vector (all zeros) then the received word is error-free; if non-zero then the value indicates which bit has been flipped.

The 4 data bits — assembled as a vector — is pre-multiplied by (i.e.,) and taken modulo 2 to yield the encoded value that is transmitted. The original 4 data bits are converted to 7 bits (hence the name "Hamming(7,4)") with 3 parity bits added to ensure even parity using the above data bit coverages. The first table above shows the mapping between each data and parity bit into its final bit position (1 through 7) but this can also be presented in a Venn diagram. The first diagram in this article shows three circles (one for each parity bit) and encloses data bits that each parity bit covers. The second diagram (shown to the right) is identical but, instead, the bit positions are marked.

For the remainder of this section, the following 4 bits (shown as a column vector) will be used as a running example:

$$\mathbf{p} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Rings and Modular Arithmetic

Ring theory

In mathematics, **ring theory** is the study of rings— algebraic s tructures in which addition and multiplication are defined and have similar properties to those familiar from the integers. Ring theory studies the structure of rings, their representations, or, in different language, modules, special classes of rings (group rings, division rings, universal enveloping algebras), as well as an array of properties that proved to be of interest both within the theory itself and for its applications, such as homological properties and pol ynomial identities.

Commutative rings are much better understood than noncommutative ones. Due to its intimate connections with algebraic geometry and algebraic number theory, which provide many natural examples of co mmutative rings, their theory, which is considered to

be part of commutative algebra and field theory rather than of general ring theory, is quite different in flavour from the theory of their nonco mmutative counterparts. A fairly recent trend, started in the 1980s with the development of noncommutative geometry and with the discovery of quantum groups, attempts to turn the situation around and build the theory of certain classes of noncom mutative rings in a geometric fashion as if they were rings of functions on (non-existent) 'noncommutative spaces'.

Elementary introduction

Definition

Formally, a ring is an Abelian group (R, +), together with a second binary operation * such that for all a, b and c in R,

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

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

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

also, if there exists a *mult iplicative identity* in the ring, that is, an element e such that for all a in R,

$$a * e = e * a = a$$

then it is said to be a *ring with unity*. The number 1 is a common example of a unity.

The ring in which e is equal to the additive identity must have only one element. This ring is called the trivial ring.

Rings that sit inside other rings are called subrings. Maps between rings which respect the ring operations are called ring homomorphisms. Rings, together with ring homomorphisms, form a category (the category of rings). Closely related is the notion of ideals, certain subsets of rings which arCSE as kernels of homomorphisms and can serve to define factor rings. Basic facts about ideals, homomorphisms and factor rings are recorded in the i somorphism theorems and in the Chinese remainder theorem.

A ring is called *commutative* if its multiplication is commutative. Commutative rings

resemble familiar number systems, and various definitions for commutative rings are designed to recover properties known from the integers. Commutative rings are also important in algebraic geometry. In co mmutative ring theory, numbers are often replaced by ideals, and the definition of prime ideal tries to capture the essence of prime numbers. Integral domains, non-trivial commutative rings where no two non-zero elements multiply to give zero, generalize another property of the integers and serve as the proper realm to study divisibility. Principal ideal domains are integral domains in which every ideal can be generated by a single element, another property shared by the integers. E uclidean domains are integral domains in which the E uclidean algorithm can be carried out. Important ex amples of co mmutative rings can be constructed as rings of pol ynomials and their factor rings. Summary: Euclidean domain => p rincipal ideal domain => unique factorization domain => integral domain => Com mutative ring.

Non-commutative rings resemble rings of matrices in many respects. Following the model of algebraic geometry, attempts have been made recently at defining non-commutative geometry based on non-commutative rings. Non-commutative rings and associative algebras (rings that are also vector spaces) are often studied via their categories of modules. A module over a ring is an Abelian group that the ring acts on as a ring of endomorphisms, very much akin to the way fields (integral domains in which every non-zero element is invertible) act on vector spaces. Examples of non- commutative

rings are given by rings of square matrices or more generally by rings of endomorphisms of Abelian groups or modules, and by monoid rings.

The congruence relation

Modular ar ithmetic can be handled mathematically by introducing a con gruence relation on the integers that is compatible with the operations of the ring of integers: addition, s ubtraction, and mult iplication. For a positive integer *n*, two integers *a* and *b* are said to be **congruent modulo** *n*, written:

$$a \equiv b \pmod{n},$$

if their dif ference *a* - *b* is an integer multiple of *n*. The number *n* is called the **modulus** of the co ngruence. An equivalent definition is that both numbers have the same remainder when divided by *n*.

For example,

$$38 \equiv 14 \pmod{12}$$

because 38 - 14 = 24, which is a multiple of 12. For positive *n* and non-negative *a* and *b*, congruence of *a* and *b* can also be thought of as asserting that these two numbers have the same remainder after dividing by the modulus *n*. So,

$$38 \equiv 2 \pmod{12}$$

because both numbers, when divided by 12, have the same remainder (2). E quivalently, the fractional parts of doing a full division of each of the numbers by 12 are the same: 0.1666... (38/12 = 3.1666..., 2/12 = 0.1666...). From the prior definition we also see that their difference, $a - b = 36$, is a whole number (integer) multiple of 12 ($n = 12$, 36/12 = 3).

The same rule holds for negative values of *a*:

$$-3 \equiv 2 \pmod{5}.$$

A remark on the notation: Because it is common to consider several congruence relations for different moduli at the same time, the modulus is incorporated in the notation. In spite of the ternary notation, the congruence relation for a given modulus is binary. This would have been clearer if the notation $a \equiv_n b$ had been used, instead of the common traditional notation.

The properties that make this relation a congruence relation (respecting addition, s ubtraction, and mult iplication) are the following.

If

$$a_1 \equiv b_1 \pmod{n}$$

and

$$a_2 \equiv b_2 \pmod{n},$$

then:

- $(a_1 + a_2) \equiv (b_1 + b_2) \pmod{n}$
- $(a_1 - a_2) \equiv (b_1 - b_2) \pmod{n}$
- $(a_1 a_2) \equiv (b_1 b_2) \pmod{n}.$

Multiplicative group of integers modulo n

In modular arithmetic the set of congruence classes relatively prime to the modulus n form a group under multiplication called the **multiplicative group of integers modulo *n***. It is also called the group of **primitive residue classes modulo *n*.** In the theory of rings, a branch of abstract algebra, it is described as the group of units of the ring of integers modulo n. (Units refers to elements with a multiplicative inverse.)

This group is fundamental in number theory. It has found applications in cryptography, integer factorization, and primality testing. For example, by finding the order (ie. the size) of the group, one can determine if n is prime: n is prime if and only if the order is $n - 1$.

Group axioms

It is a straightforward exercCSE to show that under multiplication the congruence classes (mod n) which are relatively prime to n satisfy the axioms for an abelian group.
Because $a \equiv b \pmod{n}$ implies that $\gcd(a, n) = \gcd(b, n)$, the notion of congruence classes (mod n) which are relatively prime to n is well- defined.

Since $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ implies $\gcd(ab, n) = 1$ the set of classes relatively prime to n is closed under multiplication.

The natural mapping from the integers to the congruence classes (mod n) that takes an integer to its congruence class (mod n) is a ring homomorphism. This implies that the class containing 1 is the unique multiplicative identity, and also the associative and commutative laws.

Given a, $\gcd(a, n) = 1$, finding x satisfying $ax \equiv 1 \pmod{n}$ is the same as solving $ax + ny = 1$, which can be done by Bézout's lemma.

Notation

The ring of integers (mod n) is denoted $\mathbb{Z}/(n)$ or (i.e., the ring of integers modulo the ideal $n\mathbf{Z} = (n)$ consisting of the multiples of n) or by $\mathbb{Z}_n$. Depending on the author its group of units may be written $(\mathbb{Z}/n\mathbb{Z})^*$, $(\mathbb{Z}/n\mathbb{Z})^\times$, $U(\mathbb{Z}/n\mathbb{Z})$, $E(\mathbb{Z}/n\mathbb{Z})$ (for German *Einheit* = unit) or similar notations. This article uses

Structure

Powers of 2

Modulo 2 there is only one relatively prime congruence class, 1, so $(\mathbb{Z}/2\mathbb{Z})^\times \cong \{1\}$ is trivial.

Modulo 4 there are two relatively prime congruence classes, 1 and 3, so $(\mathbb{Z}/4\mathbb{Z})^\times \cong C_2$, the cyclic group with two elements.

Modulo 8 there are four relatively prime classes, 1, 3, 5 and 7. The square of each of these is 1, so $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$, the Klein four-group.

Modulo 16 there are eight relatively prime classes 1, 3, 5, 7, 9, 11, 13 and 15. $\{\pm 1, \pm 7\} \cong C_2 \times C_2$ is the 2-torsion subgroup (ie. the square of each element is 1), so is not cyclic. The powers of 3, {1,3,9,11} are a subgroup of order 4, as are the powers of 5, {1,5,9,13}. Thus $(\mathbb{Z}/16\mathbb{Z})^\times \cong C_2 \times C_4$.

The pattern shown by 8 and 16 holds[1] for higher powers 2^k, $k > 2$: $\{\pm 1, 2^{k-1} \pm 1\} \cong C_2 \times C_2$ is the 2-torsion subgroup (so $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is not cyclic) and the powers of 3 are a subgroup of order 2^{k-2}, so $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong C_2 \times C_{2^{k-2}}$.

Powers of odd primes

For powers of odd primes p^k the group is cyclic:[2] $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong C_{p^{k-1}(p-1)} \cong C_{\varphi(p^k)}$.

General composite numbers

The Chinese remainder theorem[3] says that if $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots,$ then the ring $\mathbb{Z}/n\mathbb{Z}$ is the direct product of the rings cor responding to each of its prime power factors:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \mathbb{Z}/p_3^{k_3}\mathbb{Z} \ldots$$

Similarly, the group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ is the direct p roduct of the groups corresponding to each of the prime power factors:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^\times \times (\mathbb{Z}/p_3^{k_3}\mathbb{Z})^\times \ldots .$$

Order

The order of the group is given by Euler's totient function: $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n).$ This is the product of the orders of the cyclic groups in the direct product.

Exponent

The exponent is given by the Carmichael function λ(*n*), the least common multiple of the orders of the cyclic groups. This means that if *a* and *n* are relatively prime,

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Generators

$(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $\varphi(n) = \lambda(n).$ This is the case precCSEly when *n* is 2, 4, a power of an odd prime, or twice a power of an odd prime. In this case a generator is called a **primitive root modulo n**.

Since all the $(\mathbb{Z}/n\mathbb{Z})^\times,$ *n* = 1, 2, ..., 7 are cyclic, another way to state this is: If *n* < 8 then $(\mathbb{Z}/n\mathbb{Z})^\times$ has a primitive root. If *n* ≥ 8 $(\mathbb{Z}/n\mathbb{Z})^\times$ has a primitive root unless *n* is divisible by 4 or by two distinct odd primes.

In the general case there is one generator for each cyclic direct factor.

Table

This table shows the structure and generators of for small values of *n*. The generators are not unique (mod *n*); e.g. (mod 16) both {-1, 3} and {-1, 5} will work. The generators are listed in the same order as the direct factors.

For example take $n = 20$. $\varphi(20) = 8$ means that the order of $(\mathbb{Z}/20\mathbb{Z})^\times$ is 8 (i.e. there are 8 numbers less than 20 and coprime to it); $\lambda(20) = 4$ that the fourth power of any number relatively prime to 20 is $\equiv 1 \pmod{20}$; and as for the generators, 19 has order 2, 3 has order 4, and every member of $(\mathbb{Z}/20\mathbb{Z})^\times$ is of the form $19^a \times 3^b$, where a is 0 or 1 and b is 0, 1, 2, or 3.

The powers of 19 are {±1} and the powers of 3 are {3, 9, 7, 1}. The latter and their negatives (mod 20), {17, 11, 13, 19} are all the numbers less than 20 and prime to it. The fact that the order of 19 is 2 and the order of 3 is 4 implies that the fourth power of every member of $\mathbb{Z}_{20}^\times$ is $\equiv 1 \pmod{20}$.