Discrete Math Notes

B.Tech. CSE

Gurmukh Singh

Instructor:
Dr. Sanjay Kumar

Contents

1 UNIT 1

1.1 Set Theory

Schaum series- Lipscitz

1.1.1 Sets

Sets are well defined collection of mathematical objects.
Example:
The collection of best mathematicians in the world is not a set as there is no fixed criteria for being the best mathematicians.

Notation: Sets are denoted by capital letters such as A, B, X, Y.
the elements are denoted by small letters such as a, b, x, y.

Def^n :
A set A is called to be a subset of B iff

$$a \in A \implies a \in B$$

It is denoted by $A \subseteq B$.

1.1.2 Empty and Universal set

Def^n :
An empty set is a set which contains no elements. It is either denoted by empty braces or the greek letter ϕ.

Def^n :
A Universal set is a set which contains all the elements (in the context).

Def^n :
A set which contains only one element is called a singleton set.
for example: $\{5\}$.

Note:
for any set A, ϕ and A are always subsets called improper subsets.

1.1.3 Power Set

Def^n :
A power set of a set is the collection of all the subsets of A. It is denotes by 2^A.

1.2 Representation of Sets

There are 2 ways to represent sets:

1. Set builder form

2. Roaster form

1.2.1 Set builder form

Def^n :
It is based on the unique property of the collection. The iterator is set and a property is defined in curly braces

Example:

$$A = \{x : x = 2y, y \in \mathbb{Z}\}$$

OR

$$A = \{2x : x \in \mathbb{Z}\}$$

1.2.2 Roaster form

Def^n :
In this representation we list the elements in curly braces seperated by commas.

Example:

$$A = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

1.3 Operations on sets

We have defined the following functions on sets

1. Union
2. Intersection
3. Difference
4. Symmetric Difference

1.3.1 Union of Sets($\cup$)

Def^n :
Collection of all the elements of the sets

Example:

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

1.3.2 Intersection of Sets($\cap$)

Def^n :
Collection of all the elements in both the sets

Example:

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

1.3.3 Difference of Sets(-)

<u>*Def*^{n} :</u>
Collection of all the elements one set but not the other

Example:

$$A - B = \{x : x \in A \text{ and } x \notin B\}$$

1.3.4 Symmetric difference of Sets(Δ)

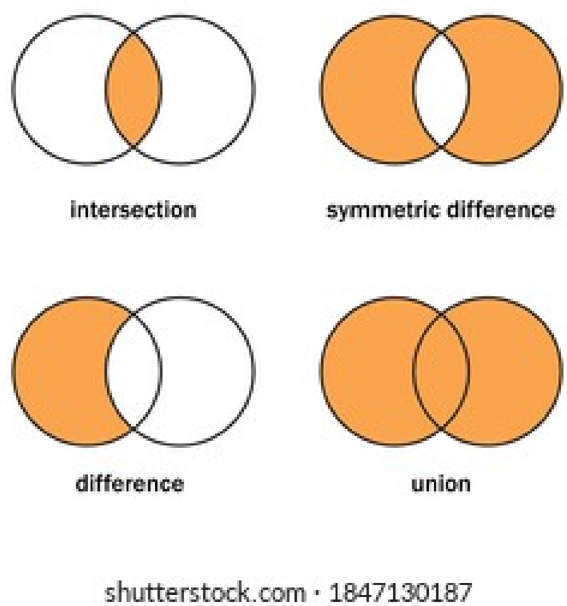
<u>*Def*^{n} :</u>
Collection of all the elements which exist in exactly one of the sets

Example:

$$A \Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

1.4 Venn diagram

A pictorial representation of sets is called a venn diagram



1.5 De-morgan's Law

Let A and B be two sets then

1. $(A \cup B)^c = A^c \cap B^c$
2. $(A \cap B)^c = A^c \cup B^c$

Proof: Let $x \in (A \cup B)^c$

$$\begin{aligned}
&\implies x \notin A \cup B \\
&\implies x \notin A, x \notin B \\
&\implies x \in A^c, x \in B^c \\
&\implies x \in A^c \cap B^c
\end{aligned}$$

Thus we can say that $(A \cup B)^c \subseteq A^c \cap B^c$
Similarly Let $x \in A^c \cap B^c$.

$$\begin{aligned}
&\implies x \in A^c, x \in B^c \\
&\implies x \notin A, x \notin B \\
&\implies x \notin A \cup B \\
&\implies x \in (A \cup B)^c
\end{aligned}$$

Thus we can say that $A^c \cap B^c \subseteq (A \cup B)^c$
This is possible iff $(A \cup B)^c = A^c \cap B^c$

Q.E.D.

1.6 Partition of sets

Let S be a non-empty set. Then S has the partition if it has a collection of subsets A_i such that:

1. $\forall a \in S, \exists$ unique i such that $a \in A_i$
2. $A_i \cup A_j = \phi, i \neq j$

Example:
Consider the set $S = \{1, 2, \ldots, 9\}$

1. $[\{1, 3, 5\}, \{2, 6\}, \{4, 9\}]$
2. $[\{1, 3, 5\}, \{2, 4, 6, 8\}, \{7, 9\}]$

then 1 is not a partition of S as the element 7 is missing. However 2 is a partition of the set S.

1.7 Relations

A relation R from set A to set B is subset of $A \times B$ where :

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

$$R \subseteq A \times B = \{(a, b) : a \in A, b \in B\}$$

- Domain $\rightarrow$ All the elements of set A
- Codomain $\rightarrow$ All the elements of set B
- Range $\rightarrow$ All the second elements of R

Example:

$$\begin{aligned}
R =& \{(a,b) : b = 2a+1, a \in [1,10], b \in [1,10]\} \\
A =& [1,10] \\
R \subseteq& A \times A \\
=& \{(1,3),(2,5),(3,7),(4,9)\}
\end{aligned}$$

- Domain = $\{1,2,3,4\}$
- Range = $\{3,5,7,9\}$

1.7.1 Composition of Relations

Let R be a relation from A to B
Let S be a relation from B to C
then

$$R \circ S = \{(a,c) : \exists b \in B \ s.t. \ (a,b) \in R, (b,c) \in S\}$$

Example:

$$\begin{aligned}
\text{Let } A &= \{1,2,3,4\} \\
B &= \{a,b,c,d\} \\
C &= \{x,y,z\} \\
R &= \{(1,a),(2,a),(3,a),(4,d)\} \\
S &= \{(a,y),(b,x),(c,z)\} \\
\implies R \circ S &= \{(1,y),(2,y),(3,z)\}
\end{aligned}$$

1.7.2 Equivalence Relations

A relation R from A to A is said to be equivalence if it satisfies the following conditions:

1. Reflexivity
2. Transivity
3. Symmetricity

$\underline{Def^n:}$
A relation is said to be reflexive iff:

$$(a,a) \in R \ \forall a \in A$$

$\underline{Def^n:}$
A relation is said to be Transitive iff:

$$(a,b) \in R, (b,c) \in R \implies (a,c) \in R$$

Def^n :
A relation is said to be Symmetric iff:

$$(a, b) \in R \implies (b, a) \in R$$

Example:
Consider the relation R on $A = \{1, 2, 3, 4\}$

$$R_1 = \{(1,1), (1,2), (2,3), (1,3), (4,4)\}$$
$$R_2 = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)\}$$
$$R_3 = \{(1,3), (2,1)\}$$
$$R_4 = A \times A$$

Then

- R_1 is Transitive only
- R_2 is Equivalence
- R_3 is neither Symmetric, Reflexive or Transitive only
- R_4 is Equivalence

Def^n :
A relation on a set A is said to be Anti-symmetric if and only if:

$$(a, b) \in A, (b, a) \in A \implies a = b$$

1.8 Functions

A relation from set A to B such that each element of A has a unique mapping in B then it is called a function and is denoted as

$$f : A \to B$$

All functions are relations but not vice-versa.

1.8.1 Domin, Range and Codomain

for $f : A \to B$

- Domain: A
- Codomain: B
- Range: $\{b \in B : \exists a \in A \text{ such that } f(a) = b\}$

Note: Domain$(f) \subseteq A$
Range$(f) \subseteq B$

One-one	Each horizontal line cuts the graph at atmost one point
Onto	Each horizontal line cuts the graph at one or more points

1.8.2 One-one and Onto function

Let $f : A \to B$ be a funciton then f is called one-one if distinct elements of A have different image.
Mathematically:

$$f(x_1) = f(x_2) \implies x_1 = x_2$$

f is said to be onto if each element of B has a preimage in A.
Mathematically

$$\forall b \in B, \exists a \in A \text{ such that } f(a) = b$$

<u>*Def*^{n} :</u>
f is bijective iff it is both one-one and onto

1.8.3 Geometrical characterisation of one-one and onto functions

Example:
Let $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x^2$
One-one:

$$\begin{aligned}
&\text{Let } f(x_1) = f(x_2)\\
&\implies x_1^2 = x_2^2\\
&\implies x_1^2 - x_2^2 = 0\\
&\implies (x_1 - x_2)(x_1 + x_2) = 0\\
&\implies x_1 = x_2 \text{ or } x_1 = -x_2
\end{aligned}$$

Onto: We have $f(x) = x^2 \geq 0$
$\nexists x < 0 \in \mathbb{R}$ such that $f(x) = x^2$

1.9 Composition of Functions

Let $f : A \to B$ and $g : B \to C$ be two functions then
$g \circ f : A \to C$ is called composition of f and g.

$$g \circ f(x) = g(f(x))$$

Result:
Let $f : A \to B$ and $g : B \to C$ be two functions then

1. $g \circ f$ is one-one if both f and g are one-one
2. $g \circ f$ is onto if both f and g are onto

Proof:

1. Let $(g \circ f)(x_1) = (g \circ f)(x_2)$

$$\begin{aligned}
&\implies g(f(x_1)) = g(f(x_2)) \\
&\implies f(x_1) = f(x_2) \text{ as g is one-one} \\
&\implies x_1 = x_2 \text{ as f is one-one}
\end{aligned}$$

2. $g \circ f : A \to C$
   Let $z \in C$, we will show that $\exists x \in A$ such that $g \circ f(x) = z$
   Since g is onto $\implies \exists y \in B$ such that $g(y) = z$
   Since f is onto and $y \in B \implies \exists x \in A$ such that $f(x) = y$

Q.E.D.

1.10 Induction

Used to prove that a statement is true for all integers or natural numbers.

$$P(n) \text{ holds } \forall n$$

1.10.1 Principle of Mathematical Induction

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

1. <u>Basic Step</u>: $P(1)$ is true
2. <u>Induction Step</u>: $P(k) \implies P(k+1)$ is true

This causes a domino effect and effectively proves that $P(n)$ is true $\forall n$ *Example:*
Using Induction, Prove that:

$$1 + 2 + 3 + 4 + 5 + \cdots + n = \frac{n(n+1)}{2}, n \in \mathbb{Z}^+$$

1. Base Case:

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

Q.E.D.

2. Induction Step: Let $P(k)$ is true, then we have to show that $P(k+1)$ is true.

$$\begin{aligned}
1 + 2 + \cdots + k &= \frac{k(k+1)}{2} \\
\implies 1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\
\implies 1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
\implies 1 + 2 + \cdots + k + (k+1) &= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Q.E.D.

1.11 Recursion

This is used when we cannot explicitly represent any object or mathematical term. so we use recursion.

<u>*Def^n* :</u>
<u>Recursive function</u>
Let $\{a\}_n, n \in \mathbb{Z}_0^+$ such that $a_n \in \mathbb{Z} \forall n$ then:

1. Basic Step: a_n is given at $n = 0$
2. Recursive step: $a_n = f(a_{n-1}, a_{n-2} \dots)$

Well known examples of recursive expressions are:

1. Arithemetic progression
$$a_n = a_{n-1} + d$$
2. Geometric progression
$$a_n = ra_{n-1}$$
3. Factorial function
$$f(n) = n \times f(n-1)$$
$$f(0) = 1$$
4. Fibonacci function
$$f(n) = f(n-1) + f(n-2)$$
$$f(0) = 0$$
$$f(1) = 1$$

1.11.1 Linear recurrence relations with constant coefficients

Let $a_n = \phi(a_{n-1}, a_{n-2}, \dots, a_0, m)$
It can be written as:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_{n-1} a_1 + c_n a_0 + f(m)$$

If $f(m) = 0$ then the function is called homogeneous
If $f(m) \neq 0$ then the function is called non-homogeneous

HOMOGENEOUS SOLUTION
Note: kth order recurrence relation is one such that

$$a_n = \phi(a_{n-1}, a_{n-2}, \dots, a_{n_k}, m)$$

or

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} + f(m)$$

so a second order recurrence relation will look like:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + c_3 \tag{1}$$

Then characteristic equation of (1) is given by:

$$x^2 - c_1 x - c_2 = 0, c_1, c_2 \in \mathbb{R}$$

Come forth 3 cases:

1. When roots are real and distinct:

$$x^2 - c_1 x - c_2 = 0 \implies \begin{cases} x = r_1 \\ x = r_2 \end{cases} \quad r_1 \neq r_2$$

Then the solution of (1) is given by:

$$a_n = p_1 r_1^n + p_2 r_2^n$$

2. Roots are real and equal:

$$r_1 = r_2 = r$$

Then the solution of (1) is given by:

$$a_n = (p_1 + np_2) r^n$$

Example:
Solve $a_n = 2a_{n_1} + 3a_{n-2}$

$$\begin{aligned} a_n - 2a_{n-1} - 3a_{n-2} &= 0 \\ \implies x^2 - 2x - 3 &= 0 \\ \implies (x-3)(x+1) &= 0 \\ \implies x &= -1, 3 \end{aligned}$$

Solution:

$$a_n = p_1(-1)^n + p_2(3)^n$$

Suppose: $a_0 = 1, a_1 = 2$

$$\begin{aligned} n = 0 &\implies a_0 = p_1(-1)^0 + p_2(3)^0 \\ &\implies 1 = p_1 + p_2 \\ n = 1 &\implies a_1 = p_1(-1)^1 + p_2(3)^1 \\ &\implies 2 = -p_1 + 3p_2 \end{aligned}$$

From the above 2 equations we get:

$$p_1 = \frac{1}{4}$$
$$p_2 = \frac{3}{4}$$

$$\implies a_n = \frac{1}{4}(-1)^n + \frac{3}{4}(3)^n$$

Example:
Solve: $a_n = 6a_{n-1} - 9a_{n-2}$
with $a_1 = 3, a_2 = 27$

NON-HOMOGENEOUS SOLUTION

We have

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + f(n) \tag{2}$$

where $f(n) \neq 0$
From (2) the associated homogeneous linear recurrence relation is

$$a_n = c_1 a_{n-1} + \cdots + c_k a_{n-k} \tag{3}$$

We can get the solution of (3), Let say (a_n^c)
Let a_n^p is the particular solution of (2). Then the general solution of (2) can be written as

$$a_n = a_n^c + a_n^p$$

Theorem:
Suppose that a_n satisfies the relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + f(n)$$

where $c_i \in \mathbb{R} \forall i$ and

$$f(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n$$

where $b_i, s \in \mathbb{R} \forall i$
Then the following cases.

1. If s is not the root of the characteristic equation then the particular solution of (2) is of the type
$$(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n$$
2. if s is root of the characteristic equation then the particular solution of (2) is of the type
$$n^m (p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) s^n$$
where m is the multiplicity of the root

Example:
Write the type of particular solution for the recurrence relation, $a_n = 6a_{n-1} - 9a_{n-2} + f(n)$

1. $f(n) = 3^n$
2. $f(n) = n3^n$
3. $f(n) = n^2 2^n$

Solution:
The associated homogeneous linear recurrence relation:

$$a_n - 6a_{n-1} + 9a_{n-2} = 0$$

So characteristic equation :

$$x^2 - 6x + 9 = 0$$

$$\implies (x-3)^2 = 0$$

$$\implies x = 3, 3$$

1. $f(n) = 3^n$
   comparing to $f(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n$ we get
   so
   $$b_0 = 1, b_i = 0 \forall i > 0$$

   $s = 3$ is root of the characteristic equation with multiplicity 2
   So particular solution would be:
   $$n^2 p_0 3^n$$

2. $f(n) = n3^n$
   comparing to $f(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n$ we get
   so
   $$b_0 = 1, b_1 = 1, b_i = 0 \forall i > 1$$

   $s = 3$ is root of the characteristic equation with multiplicity 2
   So particular solution would be:
   $$n^2 (p_1 n + p_0) 3^n$$

3. $f(n) = n^2 2^n$
   comparing to $f(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) s^n$ we get
   so
   $$b_0 = 1, b_1 = 1, b_2 = 1, b_i = 0 \forall i > 1$$

   $s = 2$ is root of the characteristic equation with multiplicity 2
   So particular solution would be:
   $$a_n^p = (p_2 n^2 + p_1 n + p_0) 2^n$$
   $$a_n^c = (c_1 + c_2 n) 3^n$$
   From the above 2 equations ;
   $$(p_2 n^2 c p_1 n + p_0) 2^n = 6(p_2(n-1)^2 + p_2(n-1) + p_0) 2^{n-1} - 9(p_2(n-2)^2 + p_1(n2) + p_0) 2^{n-2} + n^2 2^n$$

Example:
Solve:

$$a_n = 6a_{n-1} - 9a_{n-2} + n^2 2^n, a_0 = 1, a_1 = 2$$

Solution:
The associated homogeneous linear recurrence relation is $a_n = 6a_{n-1} - 9a_{n-2}$ So the characteristic equation is

$$\begin{aligned} x^2 - 6x + 9 &= 0 \\ \implies x &= 3, 3 \end{aligned}$$

So

$$a_n^c = (c_1 + c_2 n)3^n$$

for particular solution:

$$a_n^p = (b_2 n^2 + b_1 n + b_0)2^n$$

so the general solution :

$$a_n = (c_1 + c_2 n)3^n + (b_2 n^2 + b_1 n + b_0)2^n$$

putting the values of a_0 and a_1 we get

$$\begin{aligned} 1 &= c_1 3^0 + b_0 2^n \\ \implies 1 &= c_1 + b_0 \end{aligned}$$

$$\begin{aligned} 2 &= (c_1 + c_2)3 + (b_2 + b_1 + b_0)2 \\ \implies 2 &= 3c_1 + 3c_2 + 2b_2 + 2b_1 + 2b_0 \end{aligned}$$

Comparing the coefficients of 2^n and 3^n in both sides:

$$\begin{aligned} b_0 + b_1 + b_2 &= 1 \\ c_1 + c_2 &= 0 \\ c_1 &= 1 \\ b_0 &= 0 \\ c_2 &= -c_1 = -1 \end{aligned}$$

2 Logic and Proof Techniques

<u>*Def*^{n}</u> :
Proposition(statement): is a declarative sentence that is either true or false but not both.

Example:

1. Ice floats on water.
2. $2 - x = 3$

2.1 Proof Techniques

Def^n :
Conjecture: Any statement given is a conjecture.
Theorem: A statement which is to be proved true.

$$Conjecture + proof \to Theorem$$

Proof: The technique by which we check whether the given statement is true or not

There are the following proof techniques:

1. Direct Proof
2. Proof by Contrapositive
3. Proof by Contradiction
4. Proof by Counterexample
5. Proof by Cases

2.1.1 Direct Proof

If we are given $p \to q$, then take p and by implications of p, we arrive at q.
Example:
If n is even then prove that n^2 is even.

Given: n is even.
To prove: n^2 is even
Proof: let us say that

$$\begin{aligned} & n = 2k, k \in \mathbb{Z} \\ \implies & n^2 = 4k^2 \\ \implies & n^2 = 2(2k^2) \end{aligned}$$

Example:
For all integers a,b and c if $a|b$, and $b|c$ prove that $a|c$

2.1.2 Proof by Contrapositive

Suppose we have to prove that $p \implies q$, then it is equivalent to proving $\neg q \implies \neg p$
Example:
For all integers a and b if $a + b$ in odd then either a is odd or b is odd
$p : a + b$ is odd
$q : a$ is odd or b is odd

$\neg p : a + b$ is even
$\neg q : a$ is even and b is even

since $p \implies q \equiv \neg q \implies \neg p$
We have a is even and b is even

$$a = 2m, b = 2n, m, n \in \mathbb{Z}$$

$$\begin{aligned} \implies a + b &= 2m + 2n \\ &= 2(m + n) \\ &= 2k, k \in \mathbb{Z} \end{aligned}$$

Example:
For every prime number r, if $r \neq 2$ then r is odd

2.1.3 Proof by Contradiction

We have co prove $p \implies q$
Then it is equivalent to $\neg p \implies \neg q$

for that we take p is not true and then by implications, we arrive at some Contradiction.
Example:
$\sqrt{2}$ is irrational.

suppose $\sqrt{2}$ is a rational number.
Then we can represent it in form of $\frac{p}{q}$ such that p and q are coprimes

$$\begin{aligned} &\implies \sqrt{2} = \frac{p}{q} \\ &\implies 2 = \frac{p^2}{q^2} \\ &\implies 2q^2 = p^2 \end{aligned}$$

hence p is an even number. therefore we can write p as

$$p = 2k$$

$$p^2 = 4k^2$$

$$2q^2 = 4k^2$$

$$q^2 = 2k^2$$

thus q is also an even number.
this is a contradiction to the fact that p and q are coprime.

3 Lattice

3.1 Complement of an element

Let L be a Lattice then an element $b \in L$ is said to be complement of $a \in L$ if

$$a * b = 0$$

$$a \oplus b = 1$$

An element may have no complement, unique complement or more than one complements

Theorem:
The following conditions always hold true:

$$0' = 1$$

$$1' = 0$$

and these complements are unique

Def^n :
A lattice L is complemented if each element has atleast one complement.

Def^n :
A Lattice is said to be distributive if

$$a * (b \oplus c) = (a * b) \oplus (a * c)$$

$$a \oplus (b * c) = (a \oplus b) * (a \oplus c)$$

This is true if each element has atmost one complement.

3.2 Boolean Algebra

Def^n :
A Lattice is Boolean if it is both complementary and distributive i.e. each element of lattice has exactly one complement. Alternatively, A Lattice is Boolean if it is isomorphic to a D_n(divisors of n).

Example:

Theorem:
Here are some results to keep in mind.

1. If a lattice does not contain 2^n elements then it cannot be a boolean lattice.
2. if $|L| = 2^n$ Then it may or may not be boolean.
3. if $n = p_1 \times p_2 \times \dots p_k$ where each p_i is a distinct prime then L will be a boolean algebra.

4. Let $n \in \mathbb{Z}$ and $p^k | n$ for some $k > 1$ then D_n is not a boolean algebra

3.3 Logic Gates and Circuits

Basic type of logic gates:

1. OR Gate
2. AND Gate
3. NOT Gate

3.3.1 OR Gate

$$Y = A * B \equiv A + B$$

Y will be 0 if and only if A and B both are zero.

3.3.2 AND Gate

$$Y = A \oplus B \equiv A \cdot B$$

Y will be 1 if and only if A and B both are 1.

3.3.3 NOT Gate

$$Y = A' = \overline{A}$$

Y will just be the opposite of A.

3.3.4 Logic Circuit

Def^n :
Any combination of logic gates to get the desired output is called logic circuit.
Note that logic circuit follows the rules of boolean algebra.

3.3.5 NAND and NOR Gate

NAND Gate is the combination of AND and NOT Gate.
NOR Gate is the combination of OR and NOT Gate.

4 GROUP THEORY yeah imma kms

4.1 Binary Operations

Def^n :
Let A be a set then any operation $*$ on A is binary operation if $\forall a, b \in A, a * b \in A$. For example, $(\mathbb{Z}, +)$ is a group, but $(\mathbb{Z}, /)$ is not.

4.2 Group

Defⁿ :

Let G be a nonempty set with a defined binary operation $*$ then G is called group if it satisfies a certian condition.

1. Closure: $a * b \in G \forall a, b \in G$.
2. Associativity: $(a * b) * c = a * (b * c)$.
3. Existence of Identity: $\exists e \in G, a * e = a \forall a \in G$.
4. Existence of Inverse: $\forall a \in G\ \exists\ b \in G$ such that $a * b = e$

Example:
$(\mathbb{Z}, +)(\mathbb{Q}, +)(\mathbb{R}, +)$ are groups
$(\mathbb{Z}, -)$ is not a group because $-$ is not associative
$(\mathbb{N}, +)$ is not a group because there does not exist an identity in $\mathbb{N}$
$(\mathbb{Z}, \cdot)$ is not a group because there is no inverse for $a \in \mathbb{N}$
$(\mathbb{R}, \cdot)$ is not a group because there is no inverse for $0 \in \mathbb{R}$
$(\mathbb{R} \setminus \{0\}, \cdot)$ is a group.
Example:
let $X = \mathbb{M}(\mathbb{R})_{2\times 2}$, then $G = (X, +)$ is a group.
However $G' = (X, \cdot)$ is not a group as there may or may not exist an inverse for a real matrix.

4.3 Abelian Group

Let G be a group with binary operation * then G is abelian if

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

Example:
$(\mathbb{Z}, +)$ is a group where $a + b = b + a \forall a, b \in \mathbb{Z}$
Thus $(\mathbb{Z}, +)$ is an abelian group.
Example:
$GL(2, \mathbb{R})$ = group of non singular matrices of order 2 with real entities
note that it is not necessary that the product of two matrices be commutative.
Example:
$SL(2, \mathbb{R})$ = group of matrices of order 2 with real entities and determinant 1
note that it is not necessary that the product of two matrices be commutative.

4.4 Unitary group

Defⁿ :

$$U(n) = \{a : a \in \mathbb{Z}, gcd(a, n) = 1, a < n\}$$

Example:

$$U(10) = \{1, 3, 7, 9\}$$

Note that $(U(10), \odot_n)$
$\odot_n$ is multiplication moduolo

Note:
$$a \oplus_n b = a + b \pmod n$$
$$a \odot_n b = a \cdot b \pmod n$$

4.4.1 Cayley Table

It is a visual table representation of a group. we just multiply the group with itself to check for inverses

Example:

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

then $(\mathbb{Z}_n, \oplus_n)$ is a group with identity 0.
and $< \mathbb{Z}_n, \oplus_n >$ is an abelian group.

4.5 Properties of a group

1. Uniqueness of identity
   The identity of the group must be unique. To prove take two distinct identities and show that they are equal.
2. Cancellation Laws:-
   Let G be a group and $a, b, c \in G$. Then
   (a) $ab = ac \implies b = c$ (left cancellation law)
   (b) $ab = cb \implies a = c$ (right cancellation law)
3. Uniqueness of inverse
4. Let G be a group then $(ab)^{-1} = b^{-1}a^{-1}$
5. Let G be an abelian group then $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$

Proof:

1.
2. (a) To show: $ab = ac \implies b = c$
   Proof:

$$\begin{aligned}
ab &= ac \\
&\quad \text{since } G \text{ is a group } \exists a^{-1} \in G. \text{ So premultiply by } a^{-1} \\
a^{-1}ab &= a^{-1}ac \\
eb &= ec \\
b &= c
\end{aligned}$$

3. Let G be a group and $a \in G$. Let b, c be the inverses of a. since b is inverse of a:

$$ab = ba = e$$

similarly

$$ac = ca = e$$

From the two above statements we can infer that:

$$ab = ac = e$$

From the left cancellation law

$$b = c$$

Q.E.D.

4.6 Subgroups

Def^n :
The order of a group is the number of elements in a group.
Example:

$$G = U(10) = \{1, 3, 7, 9\}$$
$$O(G) = 4$$

Def^n :
The order of an element in a group
Let G be a group and $a \in G$ then oredr of a is defined as:

$$O(a) = \{n : a^n = e, a \in G\}(\cdot)$$

$$O(a) = \{n : na = e, a \in G\}(+)$$

then n is called order of a

Def^n :
Let H be subset of G then H is called subgroup of G if H itself is group under the same operation as that of G.
Notation: $H \leq G$

Example:
$(\mathbb{Z}, +) \leq (\mathbb{R}, +)$
Example:
$(\mathbb{Z}_{10}, \oplus_{10} \not\leq (\mathbb{R}, +)$ as the operation is not the same

4.6.1 One step subgroup test

Let H be subset of the group G. Then H is ssubgroup of G if

$$ab^{-1} \in H \forall a, b \in H (\text{wrt multiplication})$$

$$a - b \in H \forall a, b \in H (\text{wrt addition})$$

Example:
Let G be a Abelian group with identity e and $H = \{x \in G : x^2 = e\}$ then check for $H \leq G$ by one step test:

$$ab^{-1} \in H \forall a, b \in H (\text{wrt multiplication})$$

since $a, b \in H, a^2 = e, b^2 = e$
so $(ab^{-1})^2 = ab^{-1}ab^{-1} = aab^{-1}b^{-1} = a^2b^{-2} = ee^{-1} = e$
Therefore $H \leq G$ ■

4.6.2 Two step subgroup test

Let G be a group and $H \subseteq G$ then iff:

1. $ab \in H \forall a, b \in H$
2. $a \in H \forall a \in H$

Example:
Let $G = GL(2, \mathbb{Z})$ with addition.
Let $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + b + c + d = 0 \right\}$
Example:
$G = GL(2, \mathbb{R})$
$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z} \setminus \{0\} \right\}$
Then H will not be a subgroup because there may or may not exist an inverse of $a \in H$ in H

4.7 Cyclic groups

a group G is called cyclic if $G =< a >$ where

$$< a >= \{a^n : n \in \mathbb{Z}\} \text{ With respect to multiplication}$$

$$< a >= \{na : n \in \mathbb{Z}\} \text{ With respect to addtion}$$

Example:
$U(10) = \{1, 3, 7, 9\}$ under multiplication $\odot_{10}$

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

So $U(10)$ is cyclic

Note: in $\mathbb{Z}_n$, the generators are the numbers which are coprime to n. so $\mathbb{Z}_{10}$ has 1,3,7,9 as it's generators under addition modulo n

4.7.1 Euler's phi (totient) function

$$\phi(1) = 1$$

for $n > 1$

$$\phi(n) = \begin{cases} n-1, & n \text{ is prime} \\ p^m - p^{m-1}, & n = p^m \\ (p-1)(q-1), & n = pq \end{cases}$$

Note that $\mathbb{Z}$ has only 1 and -1 as it's generators. It is also the only infinite cyclic group

4.8 Subgroups of $\mathbb{Z}_n$

For any divisor k of n, the set $\langle \frac{n}{k} \rangle$ is a unique subgroup of order k and thees are the only subgroup of $\mathbb{Z}_n$.
Example:
Let us take $\mathbb{Z}_{30}$

$$\begin{aligned}
\langle \frac{30}{1} \rangle &= \langle 30 \rangle = \{0\} \\
\langle \frac{30}{2} \rangle &= \langle 15 \rangle = \{0, 15\} \\
\langle \frac{30}{3} \rangle &= \langle 10 \rangle = \{0, 10, 20\} \\
\langle \frac{30}{5} \rangle &= \langle 6 \rangle = \{0, 6, 12, 18, 24\} \\
\langle \frac{30}{6} \rangle &= \langle 5 \rangle = \{0, 5, 10, 15, 20, 25\} \\
\langle \frac{30}{10} \rangle &= \langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\} \\
\langle \frac{30}{15} \rangle &= \langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, \ldots, 28\} \\
\langle \frac{30}{30} \rangle &= \langle 1 \rangle = \{0, 1, 2, 3, 4, 5, 6, \ldots, 29\}
\end{aligned}$$

4.9 Center of a group

$$Z(G) = \{x \in G; xa = ax \forall a \in G\}$$

in leyman terms, collection of all elements which commute with each other

Note: if G is abelian then $Z(G) = G$

Example:

if $G = GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R} \right\}$

$Z(G) = \left\{ \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} : e \in \mathbb{R} \right\}$

$\boxed{\text{Note: } Z(G) \leq G}$

4.10 Centralizer of an element

for an element $a \in G$

$$C(a) = \{x \in G : xa = ax\}$$

Note: if G is abelian then $C(a) = G$

Example:

$$G = GL(2,\mathbb{R})$$

find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$

Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$

$$\begin{pmatrix} a & b \\ c & b \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & b \end{pmatrix}$$

$$\begin{pmatrix} a+b & a \\ c+d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ a & b \end{pmatrix}$$

4.11 Partition of numbers

Let n be a pasitive integer then teh ways in which the number can be written form partition of n.

Example:

$$\begin{aligned} n &= 1, 1 \\ n &= 2, 2 \\ &\quad , 1+1 \\ n &= 3, 3 \\ &\quad , 2+1 \\ &\quad , 1+1+1 \\ n &= 4, 4 \\ &\quad , 3+1 \\ &\quad , 2+2 \\ &\quad , 2+1+1 \\ &\quad , 1+1+1+1 \end{aligned}$$

Formula:

$$P(n+1) = \sum_{r=0}^{n} \binom{n}{r} P(r)$$

given $P(0) = 1$

So

$$\begin{aligned} P(4) &= P(3+1) \\ &= \sum_{r=0}^{3} \binom{3}{r} P(r) \\ &= \binom{3}{0}P(0) + \binom{3}{1}P(1) + \binom{3}{2}P(2) + \binom{3}{3}P(3) \\ &= 1 + 3\times 1 + 3\times 2 + 1\times 3 && = 13 \end{aligned}$$

4.12 Order of elements in S_n

Take n and make the partitions of n.

Example:

$$S_4 \qquad \begin{aligned} 4 &\to LCM = 4 \\ 1+3 &\to LCM = 3 \\ 2+2 &\to LCM = 2 \\ 1+1+2 &\to LCM = 1 \\ 1+1+1+1 &\to LCM = 1 \end{aligned}$$

It means that S_4 has elements of order 1, 2, 3, 4.

To find the number of elements of order m in S_n.

Let $n = p_1 + p_2 + \dots$

$$\frac{n!}{p_1^{m_1} \cdot m_1! \times p_2^{m_2} \cdot m_2!}$$

5 Cosets of H in G

Let G be a group and $H \leq G, a \in G$

then

$$aH = \{ah : h \in H\}$$

and

$$Ha = \{ha : h \in H\}$$

are called left and right cosets of H in G

Example:

$G = S_3$, $H = \{I, (13)\}$. Find all the left cosets of H in G

Left Coset:

$$aH = \{ah : h \in H\}$$

$$
\begin{aligned}
G = S_3 &= \{I, (12), (23), (13), (123), (132)\} \\
IH &= \{I, (13)\} = H \\
(12)H &= \{(12), (12)(13)\} = \{(12), (132)\}
\end{aligned}
$$

$$
\begin{aligned}
IH &= \{I, (13)\} = H \\
(23)H &= \{(23), (23)(13)\} = \{(23), (123)\}
\end{aligned}
$$

$$
\begin{aligned}
IH &= \{I, (13)\} = H \\
(13)H &= \{(13), (13)(13)\} = \{(13), I\}
\end{aligned}
$$

$$
\begin{aligned}
IH &= \{I, (13)\} = H \\
(123)H &= \{(123), (123)(13)\} = \{(123), (23)\}
\end{aligned}
$$

$$
\begin{aligned}
IH &= \{I, (13)\} = H \\
(132)H &= \{(132), (132)(13)\} = \{(132), (12)\}
\end{aligned}
$$

So there are 3 distinct left cosets of H in G

Example:

Let $G = \mathbb{Z}_9$ under addition
and $H = \{0, 3, 6\}$
Then find all the right cosets of H in G

$$
\begin{aligned}
H + a &= \{h + a, h \in H\} \\
H + \{0\} &= \{0, 3, 6\} \\
H + \{1\} &= \{1, 4, 7\} \\
H + \{2\} &= \{2, 5, 8\} \\
H + \{3\} &= \{3, 6, 9\} = \{0, 3, 6\} \\
H + \{4\} &= \{4, 7, 10\} = \{1, 4, 7\} \\
H + \{5\} &= \{5, 8, 11\} = \{2, 5, 8\} \\
H + \{6\} &= \{6, 9, 12\} = \{0, 3, 6\} \\
H + \{7\} &= \{7, 10, 13\} = \{1, 4, 7\} \\
H + \{8\} &= \{8, 11, 14\} = \{2, 5, 8\}
\end{aligned}
$$

Thus we get 3 distinct cosets

Example:

Find all the left cosets of $\{1, 11\}$ in $U(30)$

$$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$$

$$
\begin{aligned}
\{1\}H &= \{1, 11\} = H \\
\{7\}H &= \{7, 77\} = \{7, 17\} \\
\{11\}H &= \{11, 121\} = \{1, 11\} \\
\{13\}H &= \{13, 143\} = \{13, 23\} \\
\{17\}H &= \{17, 187\} = \{7, 17\} \\
\{19\}H &= \{19, 209\} = \{19, 29\} \\
\{23\}H &= \{23, 253\} = \{13, 23\} \\
\{29\}H &= \{29, 309\} = \{19, 29\}
\end{aligned}
$$

Thus we get 4 distinct cosets

5.1 Normal Subgroup

Let G be a group and $H \leq G$. Then H is called normal in G if $aH = Ha \forall a \in G$. If means if $a \in G$ and $h \in H$ then there exists $h' \in H$ such that $ah' = ha$

Notation: $H \triangleleft G$
Example:
$G = S_3$ and $H = \{I, (12)\}$
Is H normal to G?

Let $a = (13) \in S_3$
and $h = (12) \in H$

Note: We have $aH = Ha \forall a \in G$

$$\implies a^{-1}Ha \subseteq H$$

By counterexample we can show that H is not normal in $G = S_3$.

$$H \ntriangleleft G$$

Example:

$$G = GL(2, \mathbb{R})$$

and

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} a, b, d \in \mathbb{R}, ad \neq 0 \right\}$$

$$\text{Let } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R})$$

$$\text{Then } \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ab - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \in H$$

$$\text{so } \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} =$$

In the end, H is not normal to G

6 Graph Theory

A graph is a pair of set (V, E) where V is the set of vertices and E is the set of edges. Here vertices are represented by dots and edges are represented by lines/curves joining the vertices.

6.1 Types of graph

1. Directed graph
2. Undirected graph

6.1.1 Directed graph

The graph in which the edge set is an ordered pair of vertices.
Here (v_i, v_j) repersents the edge from v_i to v_j

6.1.2 Undirected graph

The graph in which the edge set is an unordered pair of vertices.
Here $\{v_i, v_j\}$ repersents the edge from v_i to v_j and vice-versa.

6.2 Null graph

A graph having zero edges.

6.3 Self loop

An edge joining a vertex to itself is called self loop.

6.4 Degree of a vertex in an undirected graph

Let G be a graph and v be any vertex . Then degree of v is number of edges incident with it and denoted by $deg_G(v)$

Note:

1. if $deg_G(v) = 0 \implies$ isolated vertex
2. if $deg_G(v) = 1 \implies$ pendent vertex
3. any self loop in counted twice.

6.5 Degree of a vertex in a directed graph

1. Indegree ($deg_G^+(v)$):
   The number of edges incident to it (towards vertex)

2. Outdegree ($deg_G^-(v)$):
   The number of edges incident from it (away from vertex)

Note:
Self loop is conted each time in both cases.

6.6 Path

In an undirected graph a path is a sequence of zero or more edges of type:

$$\{v_0, v_1\}, \{v_1, v_2\}, \ldots \{v_{n-1}, v_n\}$$

OR

$$v_0, v_1, \ldots, v_n$$

where $v_0 \rightarrow$ initial vertex
$v_n \rightarrow$ final vertex
Note:

1. In a path edges and vertices may be seen multiple times.

2. The number of odgesa in a path is called length of path.

3. If the length if path is zero then it is called trivial path.

6.6.1 Types of path

1. Open path

2. Closed path

If the inital and final vertices are same then it is closed path otherwise open.

1. Simple Path

A path is simple if all the vertices are different except initial or final vertices.

6.7 Representation of graph

A matrix is a convenient way to describe a graph.
We can use the preperties of matrix algebra to find out many useful characteristics of a graph.
There are 3 types of matrix:

1. adjacency matrix

2. path matrix

3. incidence matrix

6.8 Matrix representation by Adjacency matrix

In case of undirected graph the adjacency matrix A will be defined as:

$$a_{ij} = \begin{cases} 1 & \text{, If } v_i \text{ and } v_j \text{ are adjacent to each other} \\ 0 & \text{, Otherwise} \end{cases}$$

In case of directed graph the adjacency matrix A will be defined as:

$$a_{ij} = \begin{cases} 1 & , (v_i, v_j) \in G \\ 0 & \text{, Otherwise} \end{cases}$$

6.9 Bipartite graph $(G(V_1, V_2, E)$

Let G be a graph whith vertex set V. Then if we can write V as disjoint union of two vertex sets V_1 and V_2 such that each edge of E has one vertex in V_1 and other vertex in V_2 then the graph is called bipartite graph.

A bipartite graph is called complete bipartite graph $K_(m, n)$ if each element of V_1 is connected to each element of V_2, here m and n are the number of elements in set one and two respectively.

$K_(3, 3)$