INTRODUCTION TO IDEALS

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

AVANTHIKA P
DB20CMSR03

under the guidance of
Mrs. Najumunnisa K

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu, Iritty
March 2023

Examiner 1. **Examiner 2.**

CERTIFICATE

This is to certify that **"An Introduction To Ideals"** is a bona fide project of **AVANTHIKA P**, **DB20CMSR03** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Mrs.Najumunnisa.K
Project Supervisor

DECLARATION

I, **AVANTHIKA P**, hereby declare that the project **"An Introduction To Ideals"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Mrs. Najumunnisa.K**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

AVANTHIKA P
DB20CMSR03

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Mrs. Naju, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the facuty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

Contents

1 INTRODUCTION

In ring theory, a branch of abstract algebra an ideal of ring is a special subset of its element.Ernst Kummer invented the concept of ideal numbers to serve as the ”missing” factors in number ring in which unique factorisation fails.

Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. Addition and subtraction of even numbers preserves evenness, and multiplying an even number by any integer (even or odd) results in an even number; these closure and absorption properties are the defining properties of an ideal. An ideal can be used to construct a quotient ring in a way similar to how, in group theory, a normal subgroup can be used to construct a quotient group.

2 PRELIMINARIES

2.1 GROUP

A group is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

2.1.1 Example1

($\mathbb{Z}^+$) is a group:

Associativity: Let a,b,c $\in \mathbb{Z}$. Then (a+b)+c=a+b+c=a+(b+c) So $\mathbb{Z}^+$ is associative.

Identity: Let a $\in \mathbb{Z}$. Then let e be an element of $\mathbb{Z}$ such that a+e=e+a=a. Logically, this means that e=0. So 0 is the identity element of $\mathbb{Z}$ under addition.

Inverse: Let a $\in \mathbb{Z}$. Then there exist an element $-$a such that a+$-$a=$-$a+a=e.Therefore $-$ a is the inverse element of a.

We have proved all three properties; therefore, the ordered pair $(\mathbb{Z}^+)$ is a group.

2.2 SUBGROUP

A subgroup is a subset of a group that itself is a group. That means, if H is a non-empty subset of a group G, then H is called the subgroup of G if H is a group.

2.2.1 Example1

subgroups of $\mathbb{Z}_6$ are $\langle\ 0\ \rangle$, $\langle\ 3\ \rangle$, $\langle\ 2\ \rangle$, and $\mathbb{Z}_6$.

2.3 RING

A ring is a set having an addition that must be commutative (a + b = b + a for any a, b) and associative [a + (b + c) = (a + b) + c for any a, b, c], and a multiplication that must be associative [a(bc) = (ab)c for any a, b, c]. There must also be a zero (which functions as an identity element for addition), negatives of all elements (so that adding a number and its negative produces the ring's zero element),

and two distributive laws relating addition and multiplication [a(b + c) = ab + ac and (a + b)c = ac + bc for any a, b, c]. A commutative ring is a ring in which multiplication is commutative—that is, in which ab = ba for any a, b.

2.3.1 Example1

The simplest example of a ring is the collection of integers (. . . , 3, 2, 1, 0, 1, 2, 3, . . .) together with the ordinary operations of addition and multiplication.

2.4 SUBRING

A subring S of a ring R is a subset of R which is a ring under the same operations as R. Equivalently: The criterion for a subring. A non-empty subset S of R is a subring if a, b $\in$ S implies that a - b, ab $\in$ S. So S is closed under subtraction and multiplication.

2.4.1 Example1

$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$

2.5 FUNCTION

Let A and B be two sets. A binary relation f from A to B is called a function (or mapping) from A to B if each element of A is related to exactly one element of B.

2.6 KERNEL

The kernel is the set of all elements in G which map to the identity element in H. It is a subgroup in G and it depends on f. Different homomorphisms between G and H can give different kernels. If f is an isomorphism, then the kernel will simply be the identity element.

2.6.1 Example1

Let G be the cyclic group on 6 elements 0, 1, 2, 3, 4, 5 with modular addition, H be the cyclic on 2 elements 0, 1 with modular addition, and f the homomorphism that maps each element g in G to the element g modulo 2 in H. Then ker f = 0, 2, 4 , since all these elements are mapped to 0H.

2.7 RING HOMOMORPHISM

A ring homomorphism is a function f : R $\rightarrow$ S satisfying f(x + y) = f(x) + f(y) and f(xy) = f(x)f(y). That is, it is a semigroup homomorphism for multiplication and a group homomorphism for addition.

2.7.1 Example1

The mapping from n-square matrices to m-square matrices for m $>$ n which adds to a matrix m$-$n rows and columns of zero.

2.8 ISOMORPHISM

A group isomorphism is a function between two groups that sets up a one-to-one correspondence 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.

2.8.1 Example1

The group ($\mathbb{R}$, +) ($\mathbb{R}$,+) is isomorphic to the

group ($\mathbb{C}$,+) ($\mathbb{C}$,+) of all complex numbers under addition

2.9 INTEGRAL DOMAIN

An integral domain is a commutative ring with an identity (1 0) with no zero-divisors. That is ab = 0 a = 0 or b = 0.

2.9.1 Example1

The ring Z is an integral domain

2.9.2 Example2

If a, b are elements of a field with ab = 0 then if a 0 it has an inverse a-1 and so multiplying both sides by this gives b = 0. Hence there are no zero-divisors and we have: Every field is an integral domain.

2.10 COMMUTATIVE RING

A commutative ring is a ring R in which multiplication is commutative—that is, in which ab = ba for any a, b R

2.10.1 Example1

1. Z, Q, R,C are commutative rings.
2. Z=(a+bi: a,b Z)is a commutative ring
3. Z is a commutative ring.

2.11 FIELD

A field is a set F together with two binary operations on F called addition and multiplication.[1] A binary operation on F is a mapping $F \times F \rightarrow F$, that is, a correspondence that associates with each ordered pair of elements of F a uniquely determined element of F.satisfy the following property :

Associativity of addition and multiplication: a + (b + c) = (a + b) + c, and a (b c) = (a b) c.

Commutativity of addition and multiplication: a + b = b + a, and a b = b a.

Additive and multiplicative identity: there exist two different elements 0 and 1 in F such that a + 0 = a and a 1 = a.

Additive inverses: for every a in F, there exists an element in F, denoted a, called the additive inverse of a, such that a + (a) = 0.

Multiplicative inverses: for every a 0 in F, there exists an element in F, denoted by a1 or 1/a, called the multiplicative inverse of a, such that a a1 = 1.

Distributivity of multiplication over addition: a (b + c) = (a b) + (a c).

2.11.1 Example1

The set of real numbers, denoted ”R”, together with the regular addition (+) and multiplication (*) arithmetic operations is a field. Assuming we already know it is a ring (i.e., it’s closed and associative under both operations, commutative under addition, has additive and multiplicative identities, and has additive inverses)

2.12 HOMOMORPHISM

A homomorphism is a map between two algebraic structures of the same type (that is of the same name), that preserves the operations of the structures. This means a map $f : A \rightarrow$ B f:A $\rightarrow$ B between two sets $AA, BB\ equipped\ with\ the\ same\ structure\ such\ that, if$ $\cdot\ \cdot$ is an operation of the structure (supposed here, for simplification, to be a binary operation) , then
$f(x \cdot$ y)=f(x) $\cdot$ f(y)$f(x \cdot$ y)=f(x) $\cdot$ f(y)

2.13 CONSTANT FUNCTION

A constant function is a function which takes the same value for f(x) no matter what x is. When we are talking about a generic constant function, we usually write f(x) = c, where c is some unspecified constant. Examples of constant functions include f(x) = 0, f(x) = 1, f(x) = , f(x) = 0.

2.14 COSET

A subgroup H of a group G may be used to decompose the underlying set of G into disjoint, equal-size subsets called cosets. There are left cosets and right cosets. Cosets have the same number of elements as does H. Furthermore, H itself is both a left coset and a right coset.

gH = gh : h an element of H for g in G

Hg = hg : h an element of H for g in G.

2.14.1 Example1

Let G be the additive group of the integers,$\mathbb{Z} = (..., 2, 1, 0, 1, 2, ..., +)$ and H the subgroup $(3\mathbb{Z}, +) = (..., 6, 3, 0, 3, 6, ..., +)$. Then the cosets of H in G are the three sets 3$\mathbb{Z}$, $\mathbb{Z}$ + 1, and 3$\mathbb{Z}$ + 2, where $3\mathbb{Z} + a = ..., 6 + a, 3 + a, a, 3 + a, 6 + a, ...$ These three sets partition the set $\mathbb{Z}$, so there are no other right cosets of H. Due to the commutivity of addition H + 1 = 1 + H and H +

$2 = 2 + H$. That is, every left coset of H is also a right coset, so H is a normal subgroup. (The same argument shows that every subgroup of an Abelian group is normal.)

3 CHAPTER 1

BASICS OF IDEALS

3.1 IDEALS

An additive subgroup N of a ring R satisfying the properties

$$aN \subseteq N \text{ and } Nb \subseteq N; \text{ for all } a,b \in R$$

is an ideal

3.1.1 Example 1

We see that $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$ since we know it is a subring,and $s(nm)=(nm)s \in n\mathbb{Z}$ for all $s\in\mathbb{Z}$

3.1.2 Example 2

Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let C be the subring of F consisting of all constant function in F.Is C is an ideal in F? Why?

solution:

It is not true that the product of a constant function is again a constant function .For example ,the product of sinx and 2 is the function 2sinx .Thus C is not an ideal of F.

3.1.3 Example 3

Let F be the ring of all function mapping $\mathbb{R}$ into $\mathbb{R}$,and N be the subring of all function f such that f(2)=0.Is N an ideal in F?why or why not?

solution:

Let f$\in$N and let g$\in$N .Then
(fg)(2)=f(2)g(2)=0g(2)=0 ,so fg$\in$N.Similarly,we find that gf$\in$N.therefore N is an ideal of F.We could also have proved this by just observing that N is the kernel of the evaluation homomorphism 2:F$\longrightarrow$R

3.1.4 example 4

Ring
$\mathbb{Z}=\{..., -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, ...\}$
subset $2\mathbb{Z}=\{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\}$
Take 3 from $\mathbb{Z}$
$3(2\mathbb{Z})=6\mathbb{Z}=\{...., -12, -6, 0, 6, 12, ...\}$

That is 3(2$\mathbb{Z}$)$\subseteq$2$\mathbb{Z}$ $\Longrightarrow$aN $\subseteq$N
In general we can say that nZ is said to be an ideal of $\mathbb{Z}$.

3.2 LEFT AND RIGHT IDEAL

A subring I of R is a left ideal if a$\in$I,

$$\text{r}\in \text{R} \Longrightarrow \text{ra}\in\text{I}$$

A right ideal is defined similarly.
A subring I of R is a right ideal if a$\in$I,

$$\text{r}\in\text{R} \Longrightarrow \text{ar}\in\text{I}$$

3.3 COROLLARY:

Let N be an ideal of a ring R.Then the additive cosets of N from a ring R/N with the binary operation defined by

$$(a+N)+(b+N)=(a+b)+N$$

and

$$(a+N)(b+N)=ab+N$$

3.4 THEOREM 1.1:

Let N be an ideal of ring R .Then

y:R$\longrightarrow$R/N given by $y(x) = x + N$

is a ring homomorphism with kernal N

3.5 THEOREM 1.2:

Fundamental Homomorphism Theorem:
Let ϕ:$R\longrightarrow R'$ be a ring homomorphism with kernal N .Then [R] is a ring map μ:$R/N\longrightarrow$[R] $given\ by$ u(x+n)=p(x)$is\ an\ isomorphism.If$y:R$\longrightarrow$R/ we have $p(x)$ =μy(x).

3.6 Properties In Ideal

- In a ring R ,the set R itself forms a two sided ideal called unit ideal.
- The $\{0_R\}$ consisting of only the additive identity 0_R forms a two sided ideal called the zero ideal.
- An (left , right or two sided) ideal that is not the unit ideal is called a proper ideal.

Note:

A left ideal is a proper ideal if and only if it does not contain a unit element.

Remark:

- The even integers forms an ideal in a $\mathbb{Z}$ of all integers;it is usually denoted by $2\mathbb{Z}$ .This is because sum of any even number is even,and the product of any integer with an even integer is also even .Similarly ,the set of all integers divisible by a fixed integer n is an ideal $n\mathbb{Z}$.
- The of all polynomial with real coefficient which are divisible by the polynomial x^2+1 is an ideal in the ring of all polynomials.
- The set of all n$\times$n matrices whose last row is zero forms a right ideal in the ring of all n$\times$n matrices .It is not a left ideal .The set of all n$\times$n matrices whose last column is zero forms a left ideal but not a right ideal.
- A ring is called a simple ring if it is nonzero and has no two sided ideal other than (0),(1).

3.7 THEOREM 1.3:

The intersection of two ideal of a ring R is again an ideal of the ring R.

proof

consider I_1 and I_2 are two ideal
$\Longrightarrow$ I_1 and I_2 are subgroup of $\langle$R,+$\rangle$
$\Longrightarrow$ $I_1 \cap I_2$ is also a subgroup of $\langle$R,+$\rangle$
Now,if a $\in$ $I_1 \cap I_2$ and r$\in$ R
$\Longrightarrow$ a$\in$ I_1 and a $\in$ I_2 ,r$\in$ R.
since a$\in$ I and r$\in$ R
$\Longrightarrow$ ar$\in$$I_1$ and ra$\in$$I_1$
and ra$\in$$I_2$ and ar$\in$$I_2$
$\Longrightarrow$ ar$\in$$I_1$ and ar$\in$$I_2$
$\Longrightarrow$ ar$\in$ $I_1 \cap I_2$

3.8 THEOREM 1.4:

If I_1 and I_2 are two ideals then I_1+I_2 such that I_1+I_2 =$\{a_1$+a_2:$a_1\in I_1$ and $a_2\in I_2\}$ is also an ideal containing both I_1 and I_2.

proof

x and y $\in$ $I_1 + I_2$
x-y $\in$ $I_1 + I_2$
x=$a_1 + a_2$
y=$b_1 + b_2$

a$\in I_1 \Longrightarrow a+0 \in I_1$
$\Longrightarrow a+0 \in I_1+I_2$
$I_1 \subseteq I_1+I_2$

3.9 THEOREM 1.5:

If R is a commutative ring then for every a $\in$ R,

$$\text{Ra}=\{r.a, r \in R\}$$

is an ideal.

proof

$r_1a \in R_2$ and $r_2a \in R_2$
$\text{r}_1a-r_2a=(r_1-r_2)a\in$ Ra
Ra is subgroup of $\langle$ R,+ $\rangle$
$\text{r}_1a\in$ Ra ,r$\in$ R
$\Longrightarrow r(r_1\ a)=(r\ r_1)a \in$ Ra
$\Longrightarrow (r_1\ a)r=r(a\ r_1)=r_1(r\ a)$
$=(r\ r_1)a \in$ Ra

3.10 Ideal Operation

- The sum and product of ideals are defined as follows .
  for a and b left(right) ideals of a ring R
  their sum is

$$a+b=\{a+b : a \in a and b \in b\},$$

which is a left(right) ideal, and if a,b are two sided

$$\text{ab}=\{a_1b_1 + ... + a_nb_n : a_i \in a and b_i \in b, i = 1, 2, 3...n for n = 1, 2...\}$$

That is the product is the ideal generated by all product of the form ab with a in a and b in b

- The distributive law holds for two sided ideal a,b,c

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc$$

If a product is replaced by an intersection ,a partial distributive law holds:

$$a \cap (b+c) \supset a \cap b + a \cap c$$

where the equality holds if a contains b or c

- If a,b are ideal of a commutative ring R ,then $a \cap b = ab$ in the following two cases (at least)

$$a + b = (1)$$

a is generated by elements that form a regular sequence modulo b

Example:

In $\mathbb{Z}$ we have
$(n) \cap (m) = lcm(n, m)\mathbb{Z}$
since $(n) \cap (m)$ is the set of integers which are divisible by both n and m.
Let $R = \mathbb{C}x, y, z, w$
and let
$a = (z, w), b = (x + z, y + w), c = (x + z, w).$
then,

- $a + b = (z, w, x + z, y + w =$
  $(x, y, z, w) and a + c = (z, w, x + z)$
- $ab = (z(x + z), z(y + w), w(x + z), w(y + w)) =$
  $(x^2 + xz, zy + wz, wx + wz, wy + w^2)$
- $ac = (xz + z^2, zw, xw + zw, w^2)$
- $a \cap b = ab\ while\ a \cap c = (w, zx + z^2) \neq ac$

4 CHAPTER 2

TYPES OF IDEALS

4.1 MAXIMAL IDEALS

DEFINITION:

A maximal ideal of a ring R is an ideal M different from R such that there is no proper ideal N of R properly containing M.

4.1.1 Example

The ideal (2,*) is a maximal ideal in a ring $\mathbb{Z}$[X]. **Example** If F is a field ,then the only maximal ideal is $\{0\}$

4.1.2 Example

$\mathbb{Z}_8$ =$\{0, 1, 2, 3, 4, 5, 6, 7\}$

$\frac{1}{8}$ = $< 1 >$ = $\mathbb{Z}_8$

$\frac{2}{8}$ = $< 2 >$ = $\{0, 2, 4, 6\}$

$\frac{4}{8}$ = $< 4 >$ = $\{0, 4\}$

$\frac{8}{8}$ = $< 8 >$ = $\{0\}$

$< 8 > \subseteq < 4 > \subseteq < 2 > \subseteq < 1 >$ = $\mathbb{Z}_8$

Therefore $< 2 >$ is the only maximal ideal of $\mathbb{Z}_8$

4.1.3 Example

$\mathbb{Z}_{36}$

$\frac{1}{36}$ = $< 1 >$ = $\mathbb{Z}_{36}$

$\frac{2}{36}$ = $< 2 >$ = $\{0, 2, 4, 6, 8, 10, .., 32, 34\}$

$\frac{3}{36}$ = $< 3 >$ = $\{0, 3, 6, 9, .., 30, 33\}$

$\frac{4}{36}$ = $< 4 >$ = $\{0, 4, 8, 12, 16, 20, 24, 28, 32\}$

$\frac{6}{36}$ = $< 6 >$ = $\{0, 6, 12, 18, 24, 30\}$

$\frac{9}{36}$ = $< 9 >$ = $\{0, 9, 18, 27\}$

$\frac{12}{36}$ = $< 12 >$ = $\{0, 12, 24\}$

$\frac{18}{36}$ = $< 18 >$ = $\{0, 18\}$

$\frac{36}{36}$ = $< 36 >$ = $\{0\}$

$< 12 > \subseteq < 4 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 2 >$

$< 18 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 3 >$

$< 18 > \subseteq < 9 > \subseteq < 3 >$

$< 12 > \subseteq < 3 >$

$< 12 > \subseteq < 6 >$

Therefore $< 2 >$ and $< 3 >$ are maximal ideals of $\mathbb{Z}_{36}$

4.2 MINIMAL IDEALS

DEFINITION:

A non-zero ideal is called minimal if it contains no other non zero ideal.

4.2.1 Example

In an integral domain the only minimal ideal is the zero ideal

4.3 PRIME IDEALS

DEFINITION:

An ideal $N \in R$ is a commutative ring R is a prime ideal if $ab \in N$ implies either $a \in N$ or $b \in N$ for a,b R.

Note that $\{0\}$ is a prime ideal in $\mathbb{Z}$ and, indeed in any integral domain

4.3.1 Example

Note that $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ for if $(a, b)(c, d) \in \mathbf{Z} \times \{0\}$. This implies that either

b = 0 so $(a, b) \in \mathbb{Z} \times \{0\}$ or d 0 so $(c, d) \in \mathbb{Z} \times \{0\}$ .Note that $(\mathbb{Z} \times \mathbb{Z})(\mathbb{Z} \times \{0\})$ is isomorphic to $\mathbb{Z}$ which is an integral domain.

4.3.2 Example

The prime ideals of $\mathbb{Z}$ are (0),(2),(3),(5),..

4.3.3 Example

2 $\mathbb{Z} \times 3\mathbb{Z}$ is not a prime ideal of $\mathbb{Z} \times \mathbb{Z}$. Since (2, 1) (1, 3) = (2, 3) $\in 2\mathbb{Z} \times 3\mathbb{Z}$ but (2,1) $\notin 2\mathbb{Z} \times 3\mathbb{Z}$ and (1,3)$\notin 2\mathbb{Z} \times 3\mathbb{Z}$

4.3.4 Example

12Z is not a prime ideal of $\mathbb{Z}$ since 3.8=24 $\in \{12\}$ but 3 $\notin \{12\}$ and 8 $\notin \{12\}$

4.3.5 Example

R = $\mathbb{Z}$= $\{ \pm 1, \pm 2, \pm 3, ..\}$
A = 2 $\mathbb{Z}$= $\{ 0, \pm 2, \pm 4, \pm 6, ..\}$
2 $\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$

5 CHAPTER 3

THEOREMS IN IDEALS

5.1 THEOREM

n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$ if and only if n is prime.

Proof

Let n$\mathbb{Z}$ be a prime ideal of $\mathbb{Z}$
Let if possible n is not a prime number
ie, n is composite
n=st ,$1 < s < n$,$1 < t < n$
n $\in$ n$\mathbb{Z}$
st $\in$ n$\mathbb{Z}$ and also s,t $\in \mathbb{Z}$
Since n$\mathbb{Z}$ is prime ideal
$\implies$ s $\in$ n$\mathbb{Z}$ or t $\in \mathbb{Z}$,which is not possible
$\therefore$ n is prime.
Conversely,
let n be a prime number
let a,b $\in \mathbb{Z}$ and ab $\in$ n$\mathbb{Z}$
$\implies$ n/ab
$\implies$ n/a or n/b ($\because$ n is prime)
$\implies$ $a = nk_1,\ or\ b = nk_2\ where\ k_1, k_2 \in \mathbb{Z}$
$\implies$ a $\in$ n$\mathbb{Z}$ or b $\in$ n$\mathbb{Z}$

$\Longrightarrow$ n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$.

5.2 THEOREM

Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof

If M is maximal in R,then R/M is a field. hence an integral domain, and therefore M is a prime ideal by theorem that let R be a commutative ring with unity,and let N $\notin$ R be an ideal in R. Then,R/N is an integral domain if and only if N is a prime ideal in R.

5.3 THEOREM

Let R is a commutative ring with unity, N is an ideal of R, N $\neq$ R
Then, N is a prime ideal of R if and only if R/N is an integral domain.

Proof

Given that R is a commutative ring with unity
N is an ideal of R, N $\neq$ R
Assume that N is a prime ideal of R

R is commutative ring with unity $\Longrightarrow$ R/N is also a commutative ring with unity
Now we have to show that R/N has no zero divisor
(a+N)(b+N)=N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ ab $\in$ N
$\Longrightarrow$ a $\in$ N or b $\in$ N (since N is a prime ideal)
$\Longrightarrow$ a+N=N or b+N=N
ie,(a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\therefore$ R/N has no divisors
ie, R/N is an integral domain
conversely,
Assume that R/N is an integral domain
we have to show that N is an prime ideal
ab $\in$ N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ (a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\Longrightarrow$ a $\in$ N or b $\in$ N
$\therefore$ N is an prime ideal

5.4 THEOREM

If A and B are two left ideals of a ring R, then A $\cap$ B is also a left ideal of R

Proof

let $x \in A \cap B$ and $r \in R$
since $x \in A \cap B \implies x \in A$ and $x \in B$
since $x \in A, r \in R \implies rx \in A$(since A is left ideal)
$x \in B, r \in R \implies rx \in B$(since B is left ideal)
since $rx \in A, rx \in B \implies rx \in A \cap B$
$\therefore A \cap B$ is a left ideal of R.

5.5 THEOREM

Let R be a commutaive ring with unity.
Then M is a maximal ideal of R if and only if R/M is a field.

Proof

suppose M is a maximal ideal in R.
Observe that if R is a commutative ring with unity,then R/M is also a nonzero commutative ring unity if $M \neq R$,which is the case if M is maximal.
Let $(a+M) \in R/M$,with $a \notin M$,so that a+M is not the addictive identity element of R/M.
Suppose a+M has no multiplicative inverse in R/M.

Then the set (R/M)(a+M)=(r+M)(a+M) (r+M) $\in$ R/M
we easily see that (R/M)(a+M) is an ideal of R/M.
It is nontrivial because a $\notin$ M,and it is a proper ideal because it does not contain 1+M
If γ :R $\longrightarrow$ R/M is the canonical
then $\gamma^{-}1$ [(R/M)(a+M)] is a proper ideal of R containing M.
But this contradicts our assumption that M is a maximal ideal, so a+M must have a multiplicative inverse in R/M.
conversely,
suppose that R/M is a field.
If N is any ideal of R such that M $\subseteq$ N $\subseteq$ R and γ is the canonical homomorphism of R onto R/M,then γ[N] is an ideal of R/M with [(0+M)] $\subseteq$ γ [N] $\subseteq$ R/M.
But this is contrary to that the field R/M contains no proper nontrivial ideals.
Hence if R/M is a field, M is maximal.

6 CONCLUSION

This project discusses the concept of ideals that is fundamental to ring theory.An ideal is an additive subgroup N of a ring R satisfying the properties $aN \subseteq N$ and $Nb \subseteq N$ for all $a,b \in R$.

In this project , the concept of an ideal is introduced and thus illustrated. It mostly includes the different types of ideals,its properties and different proofs related to this topic.

7 BIBILOGRAPHY

1. John B.Fraleigh ,***A First Course in Abstract Algebra*** Second Edition.
2. Gregory.T.Lee , ***Abstract Algebra*** An Introductory Course.
3. Joseph A.Gallian ,***Contemporary Abstract Algebra*** Ninth Edition.

INTRODUCTION TO IDEALS

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

JYOTHSNA C
DB20CMSR05

under the guidance of
Mrs. Najumunnisa K

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu, Iritty
March 2023

Examiner 1. **Examiner 2.**

CERTIFICATE

This is to certify that **"An Introduction To Ideals"** is a bona fide project of **JYOTHSNA C**, **DB20CMSR05** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Mrs.Najumunnisa.K
Project Supervisor

DECLARATION

I, **JYOTHSNA C**, hereby declare that the project **"An Introduction To Ideals"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Mrs. Najumunnisa.K**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

JYOTHSNA C
DB20CMSR05

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Mrs. Naju, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the facuty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

Contents

1 INTRODUCTION

In ring theory, a branch of abstract algebra an ideal of ring is a special subset of its element.Ernst Kummer invented the concept of ideal numbers to serve as the "missing" factors in number ring in which unique factorisation fails.

Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. Addition and subtraction of even numbers preserves evenness, and multiplying an even number by any integer (even or odd) results in an even number; these closure and absorption properties are the defining properties of an ideal. An ideal can be used to construct a quotient ring in a way similar to how, in group theory, a normal subgroup can be used to construct a quotient group.

2 PRELIMINARIES

2.1 GROUP

A group is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

2.1.1 Example1

($\mathbb{Z}^+$) is a group:

Associativity: Let a,b,c $\in \mathbb{Z}$. Then (a+b)+c=a+b+c=a+(b+c) So $\mathbb{Z}^+$ is associative.

Identity: Let a $\in \mathbb{Z}$. Then let e be an element of $\mathbb{Z}$ such that a+e=e+a=a. Logically, this means that e=0. So 0 is the identity element of $\mathbb{Z}$ under addition.

Inverse: Let a $\in \mathbb{Z}$. Then there exist an element $-$a such that a+$-$a=$-$a+a=e.Therefore $-$ a is the inverse element of a.

We have proved all three properties; therefore, the ordered pair $(\mathbb{Z}^+)$ is a group.

2.2 SUBGROUP

A subgroup is a subset of a group that itself is a group. That means, if H is a non-empty subset of a group G, then H is called the subgroup of G if H is a group.

2.2.1 Example1

subgroups of $\mathbb{Z}_6$ are $\langle\ 0\ \rangle$, $\langle\ 3\ \rangle$, $\langle\ 2\ \rangle$, and $\mathbb{Z}_6$.

2.3 RING

A ring is a set having an addition that must be commutative (a + b = b + a for any a, b) and associative [a + (b + c) = (a + b) + c for any a, b, c], and a multiplication that must be associative [a(bc) = (ab)c for any a, b, c]. There must also be a zero (which functions as an identity element for addition), negatives of all elements (so that adding a number and its negative produces the ring's zero element),

and two distributive laws relating addition and multiplication [a(b + c) = ab + ac and (a + b)c = ac + bc for any a, b, c]. A commutative ring is a ring in which multiplication is commutative—that is, in which ab = ba for any a, b.

2.3.1 Example1

The simplest example of a ring is the collection of integers (. . . , 3, 2, 1, 0, 1, 2, 3, . . .) together with the ordinary operations of addition and multiplication.

2.4 SUBRING

A subring S of a ring R is a subset of R which is a ring under the same operations as R. Equivalently: The criterion for a subring. A non-empty subset S of R is a subring if a, b $\in$ S implies that a - b, ab $\in$ S. So S is closed under subtraction and multiplication.

2.4.1 Example1

$2\mathbb{Z}$ = $2n \text{ — } n \in \mathbb{Z}$ is a subring of $\mathbb{Z}$

2.5 FUNCTION

Let A and B be two sets. A binary relation f from A to B is called a function (or mapping) from A to B if each element of A is related to exactly one element of B.

2.6 KERNEL

The kernel is the set of all elements in G which map to the identity element in H. It is a subgroup in G and it depends on f. Different homomorphisms between G and H can give different kernels. If f is an isomorphism, then the kernel will simply be the identity element.

2.6.1 Example1

Let G be the cyclic group on 6 elements 0, 1, 2, 3, 4, 5 with modular addition, H be the cyclic on 2 elements 0, 1 with modular addition, and f the homomorphism that maps each element g in G to the element g modulo 2 in H. Then ker f = 0, 2, 4 , since all these elements are mapped to 0H.

2.7 RING HOMOMORPHISM

A ring homomorphism is a function f : R $\rightarrow$ S satisfying f(x + y) = f(x) + f(y) and f(xy) = f(x)f(y). That is, it is a semigroup homomorphism for multiplication and a group homomorphism for addition.

2.7.1 Example1

The mapping from n-square matrices to m-square matrices for m $>$ n which adds to a matrix m$-$n rows and columns of zero.

2.8 ISOMORPHISM

A group isomorphism is a function between two groups that sets up a one-to-one correspondence 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.

2.8.1 Example1

The group ($\mathbb{R}$, +) ($\mathbb{R}$,+) is isomorphic to the

group ($\mathbb{C}$,+) ($\mathbb{C}$,+) of all complex numbers under addition

2.9 INTEGRAL DOMAIN

An integral domain is a commutative ring with an identity (1 0) with no zero-divisors. That is ab = 0 a = 0 or b = 0.

2.9.1 Example1

The ring Z is an integral domain

2.9.2 Example2

If a, b are elements of a field with ab = 0 then if a 0 it has an inverse a-1 and so multiplying both sides by this gives b = 0. Hence there are no zero-divisors and we have: Every field is an integral domain.

2.10 COMMUTATIVE RING

A commutative ring is a ring R in which multiplication is commutative—that is, in which ab = ba for any a, b R

2.10.1 Example1

1. Z, Q, R,C are commutative rings.
2. Z=(a+bi: a,b Z)is a commutative ring
3. Z is a commutative ring.

2.11 FIELD

A field is a set F together with two binary operations on F called addition and multiplication.[1] A binary operation on F is a mapping $F \times F \to F$, that is, a correspondence that associates with each ordered pair of elements of F a uniquely determined element of F.satisfy the following property :

Associativity of addition and multiplication: a + (b + c) = (a + b) + c, and a (b c) = (a b) c.

Commutativity of addition and multiplication: a + b = b + a, and a b = b a.

Additive and multiplicative identity: there exist two different elements 0 and 1 in F such that a + 0 = a and a 1 = a.

Additive inverses: for every a in F, there exists an element in F, denoted a, called the additive inverse of a, such that a + (a) = 0.

Multiplicative inverses: for every a 0 in F, there exists an element in F, denoted by a1 or 1/a, called the multiplicative inverse of a, such that a a1 = 1.

Distributivity of multiplication over addition: a (b + c) = (a b) + (a c).

2.11.1 Example1

The set of real numbers, denoted "R", together with the regular addition (+) and multiplication (*) arithmetic operations is a field. Assuming we already know it is a ring (i.e., it's closed and associative under both operations, commutative under addition, has additive and multiplicative identities, and has additive inverses)

2.12 HOMOMORPHISM

A homomorphism is a map between two algebraic structures of the same type (that is of the same name), that preserves the operations of the structures. This means a map $f : A \to$ B f:A $\to$ B between two sets AA, BB *equipped with the same structure such that*, if $\cdot\,\cdot$ is an operation of the structure (supposed here, for simplification, to be a binary operation) , then
$f(x \cdot$ y)=f(x) $\cdot$ f(y)$f(x \cdot$ y)=f(x) $\cdot$ f(y)

2.13 CONSTANT FUNCTION

A constant function is a function which takes the same value for f(x) no matter what x is. When we are talking about a generic constant function, we usually write f(x) = c, where c is some unspecified constant. Examples of constant functions include f(x) = 0, f(x) = 1, f(x) = , f(x) = 0.

2.14 COSET

A subgroup H of a group G may be used to decompose the underlying set of G into disjoint, equal-size subsets called cosets. There are left cosets and right cosets. Cosets have the same number of elements as does H. Furthermore, H itself is both a left coset and a right coset.

gH = gh : h an element of H for g in G

Hg = hg : h an element of H for g in G.

2.14.1 Example1

Let G be the additive group of the integers,$\mathbb{Z} = (..., 2, 1, 0, 1, 2, ..., +)$ and H the subgroup $(3\mathbb{Z}, +) = (..., 6, 3, 0, 3, 6, ..., +)$. Then the cosets of H in G are the three sets $3\mathbb{Z}$, $\mathbb{Z}$ + 1, and $3\mathbb{Z}$ + 2, where $3\mathbb{Z} + a = ..., 6 + a, 3 + a, a, 3 + a, 6 + a, ...$ These three sets partition the set $\mathbb{Z}$, so there are no other right cosets of H. Due to the commutivity of addition H + 1 = 1 + H and H +

$2 = 2 + H$. That is, every left coset of H is also a right coset, so H is a normal subgroup. (The same argument shows that every subgroup of an Abelian group is normal.)

3 CHAPTER 1

BASICS OF IDEALS

3.1 IDEALS

An additive subgroup N of a ring R satisfying the properties

$$aN \subseteq N \text{ and } Nb \subseteq N; \text{ for all } a,b \in R$$

is an ideal

3.1.1 Example 1

We see that $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$ since we know it is a subring,and $s(nm)=(nm)s \in n\mathbb{Z}$ for all $s\in\mathbb{Z}$

3.1.2 Example 2

Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let C be the subring of F consisting of all constant function in F.Is C is an ideal in F? Why?

solution:

It is not true that the product of a constant function is again a constant function .For example ,the product of sinx and 2 is the function 2sinx .Thus C is not an ideal of F.

3.1.3 Example 3

Let F be the ring of all function mapping $\mathbb{R}$ into $\mathbb{R}$,and N be the subring of all function f such that f(2)=0.Is N an ideal in F?why or why not?

solution:

Let f$\in$N and let g$\in$N .Then
(fg)(2)=f(2)g(2)=0g(2)=0 ,so fg$\in$N.Similarly,we find that gf$\in$N.therefore N is an ideal of F.We could also have proved this by just observing that N is the kernel of the evaluation homomorphism 2:F$\longrightarrow$R

3.1.4 example 4

Ring
$\mathbb{Z}$=$\{..., -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, ...\}$
subset 2$\mathbb{Z}$=$\{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\}$
Take 3 from $\mathbb{Z}$
3(2$\mathbb{Z}$)=6$\mathbb{Z}$=$\{...., -12, -6, 0, 6, 12, ...\}$

That is $3(2\mathbb{Z}) \subseteq 2\mathbb{Z} \Longrightarrow$aN $\subseteq$N
In general we can say that nZ is said to be an ideal of $\mathbb{Z}$.

3.2 LEFT AND RIGHT IDEAL

A subring I of R is a left ideal if a$\in$I,

$$\text{r}\in \text{R} \Longrightarrow \text{ra}\in\text{I}$$

A right ideal is defined similarly.
A subring I of R is a right ideal if a$\in$I,

$$\text{r}\in\text{R} \Longrightarrow \text{ar}\in\text{I}$$

3.3 COROLLARY:

Let N be an ideal of a ring R.Then the additive cosets of N from a ring R/N with the binary operation defined by

$$(a+N)+(b+N)=(a+b)+N$$

and

$$(a+N)(b+N)=ab+N$$

3.4 THEOREM 1.1:

Let N be an ideal of ring R .Then

y:R$\longrightarrow$R/N given by $y(x) = x + N$

is a ring homomorphism with kernal N

3.5 THEOREM 1.2:

Fundamental Homomorphism Theorem:
Let ϕ:$R\longrightarrow R'$ be a ring homomorphism with kernal N .Then [R] is a ring map μ:$R/N\longrightarrow$[R] $given\ by$ u(x+n)=p(x)$is\ an\ isomorphism.If$y:R$\longrightarrow$R/ we have $p(x)$ =μy(x).

3.6 Properties In Ideal

- In a ring R ,the set R itself forms a two sided ideal called unit ideal.
- The $\{0_R\}$ consisting of only the additive identity 0_R forms a two sided ideal called the zero ideal.
- An (left , right or two sided) ideal that is not the unit ideal is called a proper ideal.

Note:

A left ideal is a proper ideal if and only if it does not contain a unit element.

Remark:

- The even integers forms an ideal in a $\mathbb{Z}$ of all integers;it is usually denoted by $2\mathbb{Z}$ .This is because sum of any even number is even,and the product of any integer with an even integer is also even .Similarly ,the set of all integers divisible by a fixed integer n is an ideal $n\mathbb{Z}$.
- The of all polynomial with real coefficient which are divisible by the polynomial x^2+1 is an ideal in the ring of all polynomials.
- The set of all n×n matrices whose last row is zero forms a right ideal in the ring of all n×n matrices .It is not a left ideal .The set of all n×n matrices whose last column is zero forms a left ideal but not a right ideal.
- A ring is called a simple ring if it is nonzero and has no two sided ideal other than (0),(1).

3.7 THEOREM 1.3:

The intersection of two ideal of a ring R is again an ideal of the ring R.

proof

consider I_1 and I_2 are two ideal
$\Longrightarrow$ I_1 and I_2 are subgroup of $\langle$R,+$\rangle$
$\Longrightarrow$ $I_1 \cap I_2$ is also a subgroup of $\langle$R,+$\rangle$
Now,if a $\in$ $I_1 \cap I_2$ and r$\in$ R
$\Longrightarrow$ a$\in$ I_1 and a $\in$ I_2 ,r$\in$ R.
since a$\in$ I and r$\in$ R
$\Longrightarrow$ ar$\in I_1$ and ra$\in I_1$
and ra$\in I_2$ and ar$\in I_2$
$\Longrightarrow$ ar$\in I_1$ and ar$\in I_2$
$\Longrightarrow$ ar$\in$ $I_1 \cap I_2$

3.8 THEOREM 1.4:

If I_1 and I_2 are two ideals then I_1+I_2 such that I_1+I_2 =$\{a_1$+a_2:$a_1 \in I_1$ and $a_2 \in I_2\}$ is also an ideal containing both I_1 and I_2.

proof

x and y $\in$ $I_1 + I_2$
x-y $\in$ $I_1 + I_2$
x=$a_1 + a_2$
y=$b_1 + b_2$

a$\in I_1 \Longrightarrow a+0 \in I_1$
$\Longrightarrow a+0 \in I_1+I_2$
$I_1 \subseteq I_1+I_2$

3.9 THEOREM 1.5:

If R is a commutative ring then for every a $\in$ R,

$$\text{Ra}=\{r.a, r \in R\}$$

is an ideal.

proof

$r_1a \in R_2$ and $r_2a \in R_2$
$\text{r}_1a - r_2a = (r_1 - r_2)a \in$ Ra
Ra is subgroup of $\langle$ R,+ $\rangle$
$\text{r}_1a \in$ Ra ,r$\in$ R
$\Longrightarrow r(r_1\ a) = (r\ r_1)a \in$ Ra
$\Longrightarrow (r_1\ a)r = r(a\ r_1) = r_1(r\ a)$
$= (r\ r_1)a \in$ Ra

3.10 Ideal Operation

- The sum and product of ideals are defined as follows .
  for a and b left(right) ideals of a ring R
  their sum is

$$a + b = \{a + b : a \in a and b \in b\},$$

which is a left(right) ideal, and if a,b are two sided

$$\text{ab} = \{a_1 b_1 + ... + a_n b_n : a_i \in a and b_i \in b, i = 1, 2, 3...n for n = 1, 2...\}$$

That is the product is the ideal generated by all product of the form ab with a in a and b in b

- The distributive law holds for two sided ideal a,b,c

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$

If a product is replaced by an intersection ,a partial distributive law holds:

$$a \cap (b + c) \supset a \cap b + a \cap c$$

where the equality holds if a contains b or c

- If a,b are ideal of a commutative ring R ,then $a \cap b = ab$ in the following two cases (at least)

$$a + b = (1)$$

a is generated by elements that form a regular sequence modulo b

Example:

In $\mathbb{Z}$ we have
$(n) \cap (m) = lcm(n, m)\mathbb{Z}$
since $(n) \cap (m)$ is the set of integers which are divisible by both n and m.
Let $R = \mathbb{C}x, y, z, w$
and let
$a = (z, w), b = (x + z, y + w), c = (x + z, w).$
then,

- $a + b = (z, w, x + z, y + w =$
  $(x, y, z, w) and a + c = (z, w, x + z)$
- $ab = (z(x + z), z(y + w), w(x + z), w(y + w)) =$
  $(x^2 + xz, zy + wz, wx + wz, wy + w^2)$
- $ac = (xz + z^2, zw, xw + zw, w^2)$
- $a \cap b = ab\ while\ a \cap c = (w, zx + z^2) \neq ac$

4 CHAPTER 2

TYPES OF IDEALS

4.1 MAXIMAL IDEALS

DEFINITION:

A maximal ideal of a ring R is an ideal M different from R such that there is no proper ideal N of R properly containing M.

4.1.1 Example

The ideal (2,*) is a maximal ideal in a ring $\mathbb{Z}$[X]. **Example** If F is a field ,then the only maximal ideal is $\{0\}$

4.1.2 Example

$\mathbb{Z}_8$ =$\{0, 1, 2, 3, 4, 5, 6, 7\}$

$\frac{1}{8}$ = $< 1 >$ = $\mathbb{Z}_8$

$\frac{2}{8}$ = $< 2 >$ = $\{0, 2, 4, 6\}$

$\frac{4}{8}$ = $< 4 >$ = $\{0, 4\}$

$\frac{8}{8}$ = $< 8 >$ = $\{0\}$

$< 8 > \subseteq < 4 > \subseteq < 2 > \subseteq < 1 >$ = $\mathbb{Z}_8$

Therefore $< 2 >$ is the only maximal ideal of $\mathbb{Z}_8$

4.1.3 Example

$\mathbb{Z}_{36}$

$\frac{1}{36}$ = $< 1 >$ = $\mathbb{Z}_{36}$

$\frac{2}{36}$ = $< 2 >$ = $\{0, 2, 4, 6, 8, 10, .., 32, 34\}$

$\frac{3}{36}$ = $< 3 >$ = $\{0, 3, 6, 9, .., 30, 33\}$

$\frac{4}{36}$ = $< 4 >$ = $\{0, 4, 8, 12, 16, 20, 24, 28, 32\}$

$\frac{6}{36}$ = $< 6 >$ = $\{0, 6, 12, 18, 24, 30\}$

$\frac{9}{36}$ = $< 9 >$ = $\{0, 9, 18, 27\}$

$\frac{12}{36}$ = $< 12 >$ = $\{0, 12, 24\}$

$\frac{18}{36}$ = $< 18 >$ = $\{0, 18\}$

$\frac{36}{36}$ = $< 36 >$ = $\{0\}$

$< 12 > \subseteq < 4 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 2 >$

$< 18 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 3 >$

$< 18 > \subseteq < 9 > \subseteq < 3 >$

$< 12 > \subseteq < 3 >$

$< 12 > \subseteq < 6 >$

Therefore $< 2 >$ and $< 3 >$ are maximal ideals of $\mathbb{Z}_{36}$

4.2 MINIMAL IDEALS

DEFINITION:

A non-zero ideal is called minimal if it contains no other non zero ideal.

4.2.1 Example

In an integral domain the only minimal ideal is the zero ideal

4.3 PRIME IDEALS

DEFINITION:

An ideal $N \in R$ is a commutative ring R is a prime ideal if $ab \in N$ implies either $a \in N$ or $b \in N$ for a,b R.

Note that $\{0\}$ is a prime ideal in $\mathbb{Z}$ and, indeed in any integral domain

4.3.1 Example

Note that $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ for if $(a, b)(c, d) \in \mathbf{Z} \times \{0\}$. This implies that either

b = 0 so $(a, b) \in \mathbb{Z}\times \{0\}$ or d 0 so $(c, d) \in \mathbb{Z} \times \{0\}$ .Note that $(\mathbb{Z} \times \mathbb{Z})(\mathbb{Z} \times\{0\})$ is isomorphic to $\mathbb{Z}$ which is an integral domain.

4.3.2 Example

The prime ideals of $\mathbb{Z}$ are (0),(2),(3),(5),..

4.3.3 Example

2 $\mathbb{Z} \times 3\mathbb{Z}$ is not a prime ideal of $\mathbb{Z} \times \mathbb{Z}$. Since (2, 1) (1, 3) = (2, 3) $\in 2\mathbb{Z} \times 3\mathbb{Z}$ but (2,1) $\notin 2\mathbb{Z} \times 3\mathbb{Z}$ and (1,3)$\notin 2\mathbb{Z} \times 3\mathbb{Z}$

4.3.4 Example

12Z is not a prime ideal of $\mathbb{Z}$ since 3.8=24 $\in \{12\}$ but 3 $\notin \{12\}$ and 8 $\notin \{12\}$

4.3.5 Example

R = $\mathbb{Z}$= $\{ \pm 1, \pm 2, \pm 3, ..\}$
A = 2 $\mathbb{Z}$= $\{ 0, \pm 2, \pm 4, \pm 6, ..\}$
2 $\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$

5 CHAPTER 3

THEOREMS IN IDEALS

5.1 THEOREM

n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$ if and only if n is prime.

Proof

Let n$\mathbb{Z}$ be a prime ideal of $\mathbb{Z}$
Let if possible n is not a prime number
ie, n is composite
n=st ,$1 < s < n$,$1 < t < n$
n $\in$ n$\mathbb{Z}$
st $\in$ n$\mathbb{Z}$ and also s,t $\in \mathbb{Z}$
Since n$\mathbb{Z}$ is prime ideal
$\implies$ s $\in$ n$\mathbb{Z}$ or t $\in \mathbb{Z}$,which is not possible
$\therefore$ n is prime.
Conversely,
let n be a prime number
let a,b $\in \mathbb{Z}$ and ab $\in$ n$\mathbb{Z}$
$\implies$ n/ab
$\implies$ n/a or n/b ($\because$ n is prime)
$\implies$ $a = nk_1,\ or\ b = nk_2\ where\ k_1, k_2 \in \mathbb{Z}$
$\implies$ a $\in$ n$\mathbb{Z}$ or b $\in$ n$\mathbb{Z}$

$\Longrightarrow$ n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$.

5.2 THEOREM

Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof

If M is maximal in R,then R/M is a field. hence an integral domain, and therefore M is a prime ideal by theorem that let R be a commutative ring with unity,and let N $\notin$ R be an ideal in R. Then,R/N is an integral domain if and only if N is a prime ideal in R.

5.3 THEOREM

Let R is a commutative ring with unity, N is an ideal of R, N $\neq$ R
Then, N is a prime ideal of R if and only if R/N is an integral domain.

Proof

Given that R is a commutative ring with unity N is an ideal of R, N $\neq$ R
Assume that N is a prime ideal of R

R is commutative ring with unity $\Longrightarrow$ R/N is also a commutative ring with unity
Now we have to show that R/N has no zero divisor
(a+N)(b+N)=N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ ab $\in$ N
$\Longrightarrow$ a $\in$ N or b $\in$ N (since N is a prime ideal)
$\Longrightarrow$ a+N=N or b+N=N
ie,(a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\therefore$ R/N has no divisors
ie, R/N is an integral domain
conversely,
Assume that R/N is an integral domain
we have to show that N is an prime ideal
ab $\in$ N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ (a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\Longrightarrow$ a $\in$ N or b $\in$ N
$\therefore$ N is an prime ideal

5.4 THEOREM

If A and B are two left ideals of a ring R, then A $\cap$ B is also a left ideal of R

Proof

let $x \in A \cap B$ and $r \in R$
since $x \in A \cap B \implies x \in A$ and $x \in B$
since $x \in A, r \in R \implies rx \in A$(since A is left ideal)
$x \in B, r \in R \implies rx \in B$(since B is left ideal)
since $rx \in A, rx \in B \implies rx \in A \cap B$
$\therefore A \cap B$ is a left ideal of R.

5.5 THEOREM

Let R be a commutaive ring with unity.
Then M is a maximal ideal of R if and only if R/M is a field.

Proof

suppose M is a maximal ideal in R.
Observe that if R is a commutative ring with unity,then R/M is also a nonzero commutative ring unity if $M \neq R$,which is the case if M is maximal.
Let $(a+M) \in R/M$,with $a \notin M$,so that a+M is not the addictive identity element of R/M.
Suppose a+M has no multiplicative inverse in R/M.

Then the set (R/M)(a+M)=(r+M)(a+M) (r+M) $\in$ R/M
we easily see that (R/M)(a+M) is an ideal of R/M.
It is nontrivial because a $\notin$ M,and it is a proper ideal because it does not contain 1+M
If γ :R $\longrightarrow$ R/M is the canonical
then $\gamma^{-}1$ [(R/M)(a+M)] is a proper ideal of R containing M.
But this contradicts our assumption that M is a maximal ideal, so a+M must have a multiplicative inverse in R/M.
conversely,
suppose that R/M is a field.
If N is any ideal of R such that M $\subseteq$ N $\subseteq$ R and γ is the canonical homomorphism of R onto R/M,then γ[N] is an ideal of R/M with [(0+M)] $\subseteq$ γ [N] $\subseteq$ R/M.
But this is contrary to that the field R/M contains no proper nontrivial ideals.
Hence if R/M is a field, M is maximal.

6 CONCLUSION

This project discusses the concept of ideals that is fundamental to ring theory.An ideal is an additive subgroup N of a ring R satisfying the properties $aN \subseteq N$ and $Nb \subseteq N$ for all $a,b \in R$.

In this project , the concept of an ideal is introduced and thus illustrated. It mostly includes the different types of ideals,its properties and different proofs related to this topic.

7 BIBILOGRAPHY

1. John B.Fraleigh ,***A First Course in Abstract Algebra*** Second Edition.
2. Gregory.T.Lee , ***Abstract Algebra*** An Introductory Course.
3. Joseph A.Gallian ,***Contemporary Abstract Algebra*** Ninth Edition.

INTRODUCTION TO IDEALS

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

PRINSHA P V
DB20CMSR06

under the guidance of
Mrs. Najumunnisa K

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu, Iritty
March 2023

Examiner 1. **Examiner 2.**

CERTIFICATE

This is to certify that **"An Introduction To Ideals"** is a bona fide project of **Prinsha P V**, **DB20CMSR06** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Mrs.Najumunnisa.K
Project Supervisor

DECLARATION

I, **Prinsha P V**, hereby declare that the project **"An Introduction To Ideals"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Mrs. Najumunnisa.K**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

Prinsha P V
DB20CMSR06

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Mrs. Naju, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the facuty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

Contents

1 INTRODUCTION

In ring theory, a branch of abstract algebra an ideal of ring is a special subset of its element.Ernst Kummer invented the concept of ideal numbers to serve as the ”missing” factors in number ring in which unique factorisation fails.

Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. Addition and subtraction of even numbers preserves evenness, and multiplying an even number by any integer (even or odd) results in an even number; these closure and absorption properties are the defining properties of an ideal. An ideal can be used to construct a quotient ring in a way similar to how, in group theory, a normal subgroup can be used to construct a quotient group.

2 PRELIMINARIES

2.1 GROUP

A group is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

2.1.1 Example1

($\mathbb{Z}^+$) is a group:

Associativity: Let a,b,c $\in \mathbb{Z}$. Then (a+b)+c=a+b+c=a+(b+c) So $\mathbb{Z}^+$ is associative.

Identity: Let a $\in \mathbb{Z}$. Then let e be an element of $\mathbb{Z}$ such that a+e=e+a=a. Logically, this means that e=0. So 0 is the identity element of $\mathbb{Z}$ under addition.

Inverse: Let a $\in \mathbb{Z}$. Then there exist an element $-$a such that a+$-$a=$-$a+a=e.Therefore $-$ a is the inverse element of a.

We have proved all three properties; therefore, the ordered pair $(\mathbb{Z}^+)$ is a group.

2.2 SUBGROUP

A subgroup is a subset of a group that itself is a group. That means, if H is a non-empty subset of a group G, then H is called the subgroup of G if H is a group.

2.2.1 Example1

subgroups of $\mathbb{Z}_6$ are $\langle\ 0\ \rangle$, $\langle\ 3\ \rangle$, $\langle\ 2\ \rangle$, and $\mathbb{Z}_6$.

2.3 RING

A ring is a set having an addition that must be commutative (a + b = b + a for any a, b) and associative [a + (b + c) = (a + b) + c for any a, b, c], and a multiplication that must be associative [a(bc) = (ab)c for any a, b, c]. There must also be a zero (which functions as an identity element for addition), negatives of all elements (so that adding a number and its negative produces the ring's zero element),

and two distributive laws relating addition and multiplication [a(b + c) = ab + ac and (a + b)c = ac + bc for any a, b, c]. A commutative ring is a ring in which multiplication is commutative—that is, in which ab = ba for any a, b.

2.3.1 Example1

The simplest example of a ring is the collection of integers (. . . , 3, 2, 1, 0, 1, 2, 3, . . .) together with the ordinary operations of addition and multiplication.

2.4 SUBRING

A subring S of a ring R is a subset of R which is a ring under the same operations as R. Equivalently: The criterion for a subring. A non-empty subset S of R is a subring if a, b $\in$ S implies that a - b, ab $\in$ S. So S is closed under subtraction and multiplication.

2.4.1 Example1

$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}$

2.5 FUNCTION

Let A and B be two sets. A binary relation f from A to B is called a function (or mapping) from A to B if each element of A is related to exactly one element of B.

2.6 KERNEL

The kernel is the set of all elements in G which map to the identity element in H. It is a subgroup in G and it depends on f. Different homomorphisms between G and H can give different kernels. If f is an isomorphism, then the kernel will simply be the identity element.

2.6.1 Example1

Let G be the cyclic group on 6 elements 0, 1, 2, 3, 4, 5 with modular addition, H be the cyclic on 2 elements 0, 1 with modular addition, and f the homomorphism that maps each element g in G to the element g modulo 2 in H. Then ker f = 0, 2, 4 , since all these elements are mapped to 0H.

2.7 RING HOMOMORPHISM

A ring homomorphism is a function f : R $\rightarrow$ S satisfying f(x + y) = f(x) + f(y) and f(xy) = f(x)f(y). That is, it is a semigroup homomorphism for multiplication and a group homomorphism for addition.

2.7.1 Example1

The mapping from n-square matrices to m-square matrices for m $>$ n which adds to a matrix m$-$n rows and columns of zero.

2.8 ISOMORPHISM

A group isomorphism is a function between two groups that sets up a one-to-one correspondence 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.

2.8.1 Example1

The group ($\mathbb{R}$, +) ($\mathbb{R}$,+) is isomorphic to the

group ($\mathbb{C}$,+) ($\mathbb{C}$,+) of all complex numbers under addition

2.9 INTEGRAL DOMAIN

An integral domain is a commutative ring with an identity (1 0) with no zero-divisors. That is ab = 0 a = 0 or b = 0.

2.9.1 Example1

The ring Z is an integral domain

2.9.2 Example2

If a, b are elements of a field with ab = 0 then if a 0 it has an inverse a-1 and so multiplying both sides by this gives b = 0. Hence there are no zero-divisors and we have: Every field is an integral domain.

2.10 COMMUTATIVE RING

A commutative ring is a ring R in which multiplication is commutative—that is, in which ab = ba for any a, b R

2.10.1 Example1

1. Z, Q, R,C are commutative rings.
2. Z=(a+bi: a,b Z)is a commutative ring
3. Z is a commutative ring.

2.11 FIELD

A field is a set F together with two binary operations on F called addition and multiplication.[1] A binary operation on F is a mapping $F \times F \rightarrow F$, that is, a correspondence that associates with each ordered pair of elements of F a uniquely determined element of F.satisfy the following property :

Associativity of addition and multiplication: a + (b + c) = (a + b) + c, and a (b c) = (a b) c.

Commutativity of addition and multiplication: a + b = b + a, and a b = b a.

Additive and multiplicative identity: there exist two different elements 0 and 1 in F such that a + 0 = a and a 1 = a.

Additive inverses: for every a in F, there exists an element in F, denoted a, called the additive inverse of a, such that a + (a) = 0.

Multiplicative inverses: for every a 0 in F, there exists an element in F, denoted by a1 or 1/a, called the multiplicative inverse of a, such that a a1 = 1.

Distributivity of multiplication over addition: a (b + c) = (a b) + (a c).

2.11.1 Example1

The set of real numbers, denoted ”R”, together with the regular addition (+) and multiplication (*) arithmetic operations is a field. Assuming we already know it is a ring (i.e., it’s closed and associative under both operations, commutative under addition, has additive and multiplicative identities, and has additive inverses)

2.12 HOMOMORPHISM

A homomorphism is a map between two algebraic structures of the same type (that is of the same name), that preserves the operations of the structures. This means a map $f : A \rightarrow$ B f:A $\rightarrow$ B between two sets $AA, BB\ equipped\ with\ the\ same\ structure\ such\ that, if$ $\cdot\ \cdot$ is an operation of the structure (supposed here, for simplification, to be a binary operation) , then
$f(x \cdot$ y)=f(x) $\cdot$ f(y)$f(x \cdot$ y)=f(x) $\cdot$ f(y)

2.13 CONSTANT FUNCTION

A constant function is a function which takes the same value for f(x) no matter what x is. When we are talking about a generic constant function, we usually write f(x) = c, where c is some unspecified constant. Examples of constant functions include f(x) = 0, f(x) = 1, f(x) = , f(x) = 0.

2.14 COSET

A subgroup H of a group G may be used to decompose the underlying set of G into disjoint, equal-size subsets called cosets. There are left cosets and right cosets. Cosets have the same number of elements as does H. Furthermore, H itself is both a left coset and a right coset.

gH = gh : h an element of H for g in G

Hg = hg : h an element of H for g in G.

2.14.1 Example1

Let G be the additive group of the integers,$\mathbb{Z} = (..., 2, 1, 0, 1, 2, ..., +)$ and H the subgroup $(3\mathbb{Z}, +) = (..., 6, 3, 0, 3, 6, ..., +)$. Then the cosets of H in G are the three sets 3$\mathbb{Z}$, $\mathbb{Z}$ + 1, and 3$\mathbb{Z}$ + 2, where $3\mathbb{Z} + a = ..., 6 + a, 3 + a, a, 3 + a, 6 + a, ...$ These three sets partition the set $\mathbb{Z}$, so there are no other right cosets of H. Due to the commutivity of addition H + 1 = 1 + H and H +

$2 = 2 + H$. That is, every left coset of H is also a right coset, so H is a normal subgroup. (The same argument shows that every subgroup of an Abelian group is normal.)

3 CHAPTER 1

BASICS OF IDEALS

3.1 IDEALS

An additive subgroup N of a ring R satisfying the properties

$$aN \subseteq N \text{ and } Nb \subseteq N; \text{ for all } a,b \in R$$

is an ideal

3.1.1 Example 1

We see that $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$ since we know it is a subring,and $s(nm)=(nm)s \in n\mathbb{Z}$ for all $s\in\mathbb{Z}$

3.1.2 Example 2

Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let C be the subring of F consisting of all constant function in F.Is Cis an ideal in F?Why?

solution:

It is not true that the product of a constant function is again a constant function .For example ,the product of sinx and 2 is the function 2sinx .Thus C is not an ideal of F.

3.1.3 Example 3

Let F be the ring of all function mapping $\mathbb{R}$ into $\mathbb{R}$,and N be the subring of all function f such that f(2)=0.Is N an ideal in F?why or why not?

solution:

Let f$\in$N and let g$\in$ .Then
(fg)(2)=f(2)g(2)=0g(2)=0 ,so fg$\in$N.Similarly,we find that gf$\in$N.therefore N is an ideal of F.We could also have proved this by just observing that N is the kernel of the evaluation homomorphism 2:F$\longrightarrow$R

3.1.4 example 4

Ring
$\mathbb{Z}=\{..., -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, ...\}$
subset $2\mathbb{Z}=\{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\}$
Take 3 from$\mathbb{Z}$
$3(2\mathbb{Z})=6\mathbb{Z}=\{...., -12, -6, 0, 6, 12, ...\}$

That is 3($2\mathbb{Z}$)$\subseteq 2\mathbb{Z} \Longrightarrow$aN $\subseteq$N
In general we can say that nZ is said to be an ideal of $\mathbb{Z}$.

3.2 LEFT AND RIGHT IDEAL

A subring I of R is a left ideal if a$\in$I,

$$\text{r}\in \text{R} \Longrightarrow \text{ra}\in\text{I}$$

A right ideal is defined similarly.
A subring I of R is a right ideal if a$\in$I,

$$\text{r}\in\text{R} \Longrightarrow \text{ar}\in\text{I}$$

3.3 COROLLARY:

Let N be an ideal of a ring R.Then the additive cosests of N from a ring R/N with the binary operation defined by

$$(a+N)+(b+N)=(a+b)+N$$

and

$$(a+N)(b+N)=ab+N$$

3.4 THEOREM 1.1:

Let N be an ideal of ring R .Then

y:R$\longrightarrow$R/N given by $y(x) = x + N$

is a ring homomorphism with kernal N

3.5 THEOREM 1.2:

Fundamental Homomorphism Theorem:
Let ϕ:$R\longrightarrow R'$ be a ring homomorphism with kernal N .Then [R] is a ring map μ:$R/N\longrightarrow$[R] $given\ by$ u(x+n)=p(x)$is\ an\ isomorphism.If$y:R$\longrightarrow$R/ we have $p(x)$ =μy(x).

3.6 Properties In Ideal

- In a ring R ,the set R itself forms a two sided ideal called unit ideal.
- The $\{0_R\}$ consisting of only the additive identity 0_R forms a two sided ideal called the zero ideal.
- An (left , right or two sided) ideal that is not the unit ideal is called a proper ideal.

Note:

A left ideal is a proper ideal if and only if it does not contain a unit element.

Remark:

- The even integers forms an ideal in a $\mathbb{Z}$ of all integers;it is usually denoted by $2\mathbb{Z}$ .This is because sum of any even number is even,and the product of any integer with an even integer is also even .Similarly ,the set of all integers divisible by a fixed integer n is an ideal $n\mathbb{Z}$.
- The of all polynomial with real coefficient which are divisible by the polynomial x^2+1 is an ideal in the ring of all polynomials.
- The set of all n$\times$n matrices whose last row is zero forms a right ideal in the ring of all n$\times$n matrices .It is not a left ideal .The set of all n$\times$n matrices whose last column is zero forms a left ideal but not a right ideal.
- A ring is called a simple ring if it is nonzero and has no two sided ideal other than (0),(1).

3.7 THEOREM 1.3:

The intersection of two ideal of a ring R is again an ideal of the ring R.

proof

consider I_1 and I_2 are two ideal
$\Longrightarrow$ I_1 and I_2 are subgroup of $\langle$R,+$\rangle$
$\Longrightarrow$ $I_1 \cap I_2$ is also a subgroup of $\langle$R,+$\rangle$
Now,if a $\in$ $I_1 \cap I_2$ and r$\in$ R
$\Longrightarrow$ a$\in$ I_1 and a $\in$ I_2 ,r$\in$ R.
since a$\in$ I and r$\in$ R
$\Longrightarrow$ ar$\in$$I_1$ and ra$\in$$I_1$
and ra$\in$$I_2$ and ar$\in$$I_2$
$\Longrightarrow$ ar$\in$$I_1$ and ar$\in$$I_2$
$\Longrightarrow$ ar$\in$ $I_1 \cap I_2$

3.8 THEOREM 1.4:

If I_1 and I_2 are two ideals then I_1+I_2 such that I_1+I_2 =$\{a_1$+a_2:$a_1\in I_1$ and $a_2\in I_2\}$ is also an ideal containing both I_1 and I_2.

proof

x and y $\in$ $I_1 + I_2$
x-y $\in$ $I_1 + I_2$
x=$a_1 + a_2$
y=$b_1 + b_2$

a$\in I_1 \Longrightarrow a+0 \in I_1$
$\Longrightarrow a+0 \in I_1+I_2$
$I_1 \subseteq I_1+I_2$

3.9 THEOREM 1.5:

If R is a commutative ring then for every a $\in$ R,

$$\text{Ra}=\{r.a, r \in R\}$$

is an ideal.

proof

$r_1a \in R_2$ and $r_2a \in R_2$
$\text{r}_1a-r_2a=(r_1-r_2)a\in$ Ra
Ra is subgroup of $\langle$ R,+ $\rangle$
$\text{r}_1a\in$ Ra ,r$\in$ R
$\Longrightarrow r(r_1\ a)=(r\ r_1)a \in$ Ra
$\Longrightarrow (r_1\ a)r=r(a\ r_1)=r_1(r\ a)$
$=(r\ r_1)a \in$ Ra

3.10 Ideal Operation

- The sum and product of ideals are defined as follows .
  for a and b left(right) ideals of a ring R
  their sum is

$$a+b=\{a+b : a \in a and b \in b\},$$

which is a left(right) ideal, and if a,b are two sided

$$\text{ab}=\{a_1b_1 + ... + a_nb_n : a_i \in a and b_i \in b, i = 1, 2, 3...n for n = 1, 2...\}$$

That is the product is the ideal generated by all product of the form ab with a in a and b in b

- The distributive law holds for two sided ideal a,b,c

$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc$$

If a product is replaced by an intersection ,a partial distributive law holds:

$$a \cap (b+c) \supset a \cap b + a \cap c$$

where the equality holds if a contains b or c

- If a,b are ideal of a commutative ring R ,then $a \cap b = ab$ in the following two cases (at least)

$$a + b = (1)$$

a is generated by elements that form a regular sequence modulo b

Example:

In $\mathbb{Z}$ we have
$(n) \cap (m) = lcm(n, m)\mathbb{Z}$
since $(n) \cap (m)$ is the set of integers which are divisible by both n and m.
Let $R = \mathbb{C}x, y, z, w$
and let
$a = (z, w), b = (x + z, y + w), c = (x + z, w).$
then,

- $a + b = (z, w, x + z, y + w =$
  $(x, y, z, w) and a + c = (z, w, x + z)$
- $ab = (z(x + z), z(y + w), w(x + z), w(y + w)) =$
  $(x^2 + xz, zy + wz, wx + wz, wy + w^2)$
- $ac = (xz + z^2, zw, xw + zw, w^2)$
- $a \cap b = ab\ while\ a \cap c = (w, zx + z^2) \neq ac$

4 CHAPTER 2

TYPES OF IDEALS

4.1 MAXIMAL IDEALS

DEFINITION:

A maximal ideal of a ring R is an ideal M different from R such that there is no proper ideal N of R properly containing M.

4.1.1 Example

The ideal (2,*) is a maximal ideal in a ring $\mathbb{Z}$[X]. **Example** If F is a field ,then the only maximal ideal is $\{0\}$

4.1.2 Example

$\mathbb{Z}_8$ =$\{0, 1, 2, 3, 4, 5, 6, 7\}$

$\frac{1}{8}$ = $< 1 >$ = $\mathbb{Z}_8$

$\frac{2}{8}$ = $< 2 >$ = $\{0, 2, 4, 6\}$

$\frac{4}{8}$ = $< 4 >$ = $\{0, 4\}$

$\frac{8}{8}$ = $< 8 >$ = $\{0\}$

$< 8 > \subseteq < 4 > \subseteq < 2 > \subseteq < 1 >$ = $\mathbb{Z}_8$

Therefore $< 2 >$ is the only maximal ideal of $\mathbb{Z}_8$

4.1.3 Example

$\mathbb{Z}_{36}$

$\frac{1}{36}$ = $< 1 >$ = $\mathbb{Z}_{36}$

$\frac{2}{36}$ = $< 2 >$ = $\{0, 2, 4, 6, 8, 10, .., 32, 34\}$

$\frac{3}{36}$ = $< 3 >$ = $\{0, 3, 6, 9, .., 30, 33\}$

$\frac{4}{36}$ = $< 4 >$ = $\{0, 4, 8, 12, 16, 20, 24, 28, 32\}$

$\frac{6}{36}$ = $< 6 >$ = $\{0, 6, 12, 18, 24, 30\}$

$\frac{9}{36}$ = $< 9 >$ = $\{0, 9, 18, 27\}$

$\frac{12}{36}$ = $< 12 >$ = $\{0, 12, 24\}$

$\frac{18}{36}$ = $< 18 >$ = $\{0, 18\}$

$\frac{36}{36}$ = $< 36 >$ = $\{0\}$

$< 12 > \subseteq < 4 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 2 >$

$< 18 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 3 >$

$< 18 > \subseteq < 9 > \subseteq < 3 >$

$< 12 > \subseteq < 3 >$

$< 12 > \subseteq < 6 >$

Therefore $< 2 >$ and $< 3 >$ are maximal ideals of $\mathbb{Z}_{36}$

4.2 MINIMAL IDEALS

DEFINITION:

A non-zero ideal is called minimal if it contains no other non zero ideal.

4.2.1 Example

In an integral domain the only minimal ideal is the zero ideal

4.3 PRIME IDEALS

DEFINITION:

An ideal $N \in R$ is a commutative ring R is a prime ideal if $ab \in N$ implies either $a \in N$ or $b \in N$ for a,b R.

Note that $\{0\}$ is a prime ideal in $\mathbb{Z}$ and, indeed in any integral domain

4.3.1 Example

Note that $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ for if $(a, b)(c, d) \in \mathbf{Z} \times \{0\}$. This implies that either

b = 0 so $(a, b) \in \mathbb{Z} \times \{0\}$ or d 0 so $(c, d) \in \mathbb{Z} \times \{0\}$ .Note that $(\mathbb{Z} \times \mathbb{Z})(\mathbb{Z} \times \{0\})$ is isomorphic to $\mathbb{Z}$ which is an integral domain.

4.3.2 Example

The prime ideals of $\mathbb{Z}$ are(0),(2),(3),(5),..

4.3.3 Example

2 $\mathbb{Z} \times 3\mathbb{Z}$ is not a prime ideal of $\mathbb{Z} \times \mathbb{Z}$. Since (2, 1) (1, 3) = (2, 3) $\in 2\mathbb{Z} \times 3\mathbb{Z}$ but (2,1) $\notin 2\mathbb{Z} \times 3\mathbb{Z}$ and (1,3)$\notin 2\mathbb{Z} \times 3\mathbb{Z}$

4.3.4 Example

12Z is not a prime ideal of $\mathbb{Z}$ since 3.8=24 $\in \{12\}$ but 3 $\notin \{12\}$ and 8 $\notin \{12\}$

4.3.5 Example

R = $\mathbb{Z}$= $\{ \pm 1, \pm 2, \pm 3, ..\}$
A = 2 $\mathbb{Z}$= $\{ 0, \pm 2, \pm 4, \pm 6, ..\}$
2 $\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$

5 CHAPTER 3

THEOREMS IN IDEALS

5.1 THEOREM

n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$ if and only if n is prime.

Proof

Let n$\mathbb{Z}$ be a prime ideal of $\mathbb{Z}$
Let if possible n is not a prime number
ie, n is composite
n=st ,$1 < s < n$,$1 < t < n$
n $\in$ n$\mathbb{Z}$
st $\in$ n$\mathbb{Z}$ and also s,t $\in \mathbb{Z}$
Since n$\mathbb{Z}$ is prime ideal
$\implies$ s $\in$ n$\mathbb{Z}$ or t $\in \mathbb{Z}$,which is not possible
$\therefore$ n is prime.
Conversly,
let n be a prime number
let a,b $\in \mathbb{Z}$ and ab $\in$ n$\mathbb{Z}$
$\implies$ n/ab
$\implies$ n/a or n/b ($\because$ n is prime)
$\implies$ a=nk1, or b=nk2 where k1,k2 $\in \mathbb{Z}$
$\implies$ a $\in$ n$\mathbb{Z}$ or b $\in$ n$\mathbb{Z}$

$\Longrightarrow$ n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$.

5.2 THEOREM

Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof

If M is maximal in R,then R/M is a field. hence an integral domain, and therefore M is a prime ideal by theorem that let R be a commutative ring with unity,and let N $\notin$ R be an ideal in R. Then,R/N is an integral domain if and only if N is a prime ideal in R.

5.3 THEOREM

Let R is a commutative ring with unity, N is an ideal of R, N $\neq$ R
Then, N is a prmie ideal of R if and only if R/N is an integral domain.

Proof

Given that R is a commutative ring with unity N is an ideal of R, N $\neq$ R
Assume that N is a prime ideal of R

R is commutative ring with unity $\Longrightarrow$ R/N is also a commutative ring with unity
Now we have to show that R/N has no zero divisor
(a+N)(b+N)=N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ ab $\in$ N
$\Longrightarrow$ a $\in$ N or b $\in$ N (since N is a prime ideal)
$\Longrightarrow$ a+N=N or b+N=N
ie,(a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\therefore$ R/N has no divisors
ie, R/N is an integral domain
conversely,
Assume that R/N is an integral domain
we have to show that N is an prime ideal
ab $\in$ N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ (a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\Longrightarrow$ a $\in$ N or b $\in$ N
$\therefore$ N is an prime ideal

5.4 THEOREM

If A and B are two left ideals of a ring R, then A $\cap$ B is also a left ideal of R

Proof

let $x \in A \cap B$ and $r \in R$
since $x \in A \cap B \implies x \in A$ and $x \in B$
since $x \in A, r \in R \implies rx \in A$(since A is left ideal)
$x \in B, r \in R \implies rx \in B$(since B is left ideal)
since $rx \in A, rx \in B \implies rx \in A \cap B$
$\therefore A \cap B$ is a left ideal of R.

5.5 THEOREM

Let R be a commutaive ring with unity.
Then M is a maximal ideal of R if and only if R/M is a field.

Proof

suppose M is a maximal ideal in R.
Observe that if R is a commutative ring with unity,then R/M is also a nonzero commutative ring unity if $M \neq R$,which is the case if M is maximal.
Let $(a+M) \in R/M$,with $a \notin M$,so that a+M is not the addictive identity element of R/M.
Suppose a+M has no multiplicative inverse in R/M.

Then the set (R/M)(a+M)=(r+M)(a+M) (r+M) $\in$ R/M
we easily see that (R/M)(a+M) is an ideal of R/M.
It is nontrivial because a $\notin$ M,and it is a proper ideal because it does not contain 1+M
If γ :R $\longrightarrow$ R/M is the canonical
then $\gamma^{-}1$ [(R/M)(a+M)] is a proper ideal of R containing M.
But this contradicts our assumption that M is a maximal ideal, so a+M must have a multiplicative inverse in R/M.
conversely,
suppose that R/M is a field.
If N is any ideal of R such that M $\subseteq$ N $\subseteq$ R and γ is the canonical homomorphism of R onto R/M,then γ[N] is an ideal of R/M with [(0+M)] $\subseteq$ γ [N] $\subseteq$ R/M.
But this is contrary to that the field R/M contains no proper nontrivial ideals.
Hence if R/M is a field, M is maximal.

6 CONCLUSION

This project discusses the concept of ideals that is fundamental to ring theory.An ideal is an additive subgroup N of a ring R satisfying the properties $aN \subseteq N$ and $Nb \subseteq N$ for all $a,b \in R$.

In this project , the concept of an ideal is introduced and thus illustrated. It mostly includes the different types of ideals,its properties and different proofs related to this topic.

7 BIBILOGRAPHY

1. John B.Fraleigh ,***A First Course in Abstract Algebra*** Second Edition.
2. Gregory.T.Lee , ***Abstract Algebra*** An Introductory Course.
3. Joseph A.Gallian ,***Contemporary Abstract Algebra*** Ninth Edition.

INTRODUCTION TO IDEALS

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

SHILPA K K
DB20CMSR07

under the guidance of
Mrs. Najumunnisa K

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu, Iritty
March 2023

Examiner 1. **Examiner 2.**

CERTIFICATE

This is to certify that **"An Introduction To Ideals"** is a bona fide project of **SHILPA K K**, **DB20CMSR07** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Mrs.Najumunnisa.K
Project Supervisor

DECLARATION

I, **SHILPA K K**, hereby declare that the project **"An Introduction To Ideals"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Mrs. Najumunnisa.K**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

SHILPA K K
DB20CMSR07

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Mrs. Naju, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the facuty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

Contents

1 INTRODUCTION

In ring theory, a branch of abstract algebra an ideal of ring is a special subset of its element.Ernst Kummer invented the concept of ideal numbers to serve as the "missing" factors in number ring in which unique factorisation fails.

Ideals generalize certain subsets of the integers, such as the even numbers or the multiples of 3. Addition and subtraction of even numbers preserves evenness, and multiplying an even number by any integer (even or odd) results in an even number; these closure and absorption properties are the defining properties of an ideal. An ideal can be used to construct a quotient ring in a way similar to how, in group theory, a normal subgroup can be used to construct a quotient group.

2 PRELIMINARIES

2.1 GROUP

A group is a finite or infinite set of elements together with a binary operation (called the group operation) that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

2.1.1 Example1

($\mathbb{Z}^+$) is a group:

Associativity: Let a,b,c $\in \mathbb{Z}$. Then (a+b)+c=a+b+c=a+(b+c) So $\mathbb{Z}^+$ is associative.

Identity: Let a $\in \mathbb{Z}$. Then let e be an element of $\mathbb{Z}$ such that a+e=e+a=a. Logically, this means that e=0. So 0 is the identity element of $\mathbb{Z}$ under addition.

Inverse: Let a $\in \mathbb{Z}$. Then there exist an element $-$a such that a+$-$a=$-$a+a=e.Therefore $-$ a is the inverse element of a.

We have proved all three properties; therefore, the ordered pair $(\mathbb{Z}^+)$ is a group.

2.2 SUBGROUP

A subgroup is a subset of a group that itself is a group. That means, if H is a non-empty subset of a group G, then H is called the subgroup of G if H is a group.

2.2.1 Example1

subgroups of $\mathbb{Z}_6$ are $\langle\ 0\ \rangle$, $\langle\ 3\ \rangle$, $\langle\ 2\ \rangle$, and $\mathbb{Z}_6$.

2.3 RING

A ring is a set having an addition that must be commutative (a + b = b + a for any a, b) and associative [a + (b + c) = (a + b) + c for any a, b, c], and a multiplication that must be associative [a(bc) = (ab)c for any a, b, c]. There must also be a zero (which functions as an identity element for addition), negatives of all elements (so that adding a number and its negative produces the ring's zero element),

and two distributive laws relating addition and multiplication [a(b + c) = ab + ac and (a + b)c = ac + bc for any a, b, c]. A commutative ring is a ring in which multiplication is commutative—that is, in which ab = ba for any a, b.

2.3.1 Example1

The simplest example of a ring is the collection of integers (. . . , 3, 2, 1, 0, 1, 2, 3, . . .) together with the ordinary operations of addition and multiplication.

2.4 SUBRING

A subring S of a ring R is a subset of R which is a ring under the same operations as R. Equivalently: The criterion for a subring. A non-empty subset S of R is a subring if a, b $\in$ S implies that a - b, ab $\in$ S. So S is closed under subtraction and multiplication.

2.4.1 Example1

$2\mathbb{Z}$ = $2n \text{ — } n \in \mathbb{Z}$ is a subring of $\mathbb{Z}$

2.5 FUNCTION

Let A and B be two sets. A binary relation f from A to B is called a function (or mapping) from A to B if each element of A is related to exactly one element of B.

2.6 KERNEL

The kernel is the set of all elements in G which map to the identity element in H. It is a subgroup in G and it depends on f. Different homomorphisms between G and H can give different kernels. If f is an isomorphism, then the kernel will simply be the identity element.

2.6.1 Example1

Let G be the cyclic group on 6 elements 0, 1, 2, 3, 4, 5 with modular addition, H be the cyclic on 2 elements 0, 1 with modular addition, and f the homomorphism that maps each element g in G to the element g modulo 2 in H. Then ker f = 0, 2, 4 , since all these elements are mapped to 0H.

2.7 RING HOMOMORPHISM

A ring homomorphism is a function f : R $\rightarrow$ S satisfying f(x + y) = f(x) + f(y) and f(xy) = f(x)f(y). That is, it is a semigroup homomorphism for multiplication and a group homomorphism for addition.

2.7.1 Example1

The mapping from n-square matrices to m-square matrices for m $>$ n which adds to a matrix m$-$n rows and columns of zero.

2.8 ISOMORPHISM

A group isomorphism is a function between two groups that sets up a one-to-one correspondence 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.

2.8.1 Example1

The group ($\mathbb{R}$, +) ($\mathbb{R}$,+) is isomorphic to the

group ($\mathbb{C}$,+) ($\mathbb{C}$,+) of all complex numbers under addition

2.9 INTEGRAL DOMAIN

An integral domain is a commutative ring with an identity (1 0) with no zero-divisors. That is ab = 0 a = 0 or b = 0.

2.9.1 Example1

The ring Z is an integral domain

2.9.2 Example2

If a, b are elements of a field with ab = 0 then if a 0 it has an inverse a-1 and so multiplying both sides by this gives b = 0. Hence there are no zero-divisors and we have: Every field is an integral domain.

2.10 COMMUTATIVE RING

A commutative ring is a ring R in which multiplication is commutative—that is, in which ab = ba for any a, b R

2.10.1 Example1

1. Z, Q, R,C are commutative rings.
2. Z=(a+bi: a,b Z)is a commutative ring
3. Z is a commutative ring.

2.11 FIELD

A field is a set F together with two binary operations on F called addition and multiplication.[1] A binary operation on F is a mapping $F \times F \to F$, that is, a correspondence that associates with each ordered pair of elements of F a uniquely determined element of F.satisfy the following property :

Associativity of addition and multiplication: a + (b + c) = (a + b) + c, and a (b c) = (a b) c.

Commutativity of addition and multiplication: a + b = b + a, and a b = b a.

Additive and multiplicative identity: there exist two different elements 0 and 1 in F such that a + 0 = a and a 1 = a.

Additive inverses: for every a in F, there exists an element in F, denoted a, called the additive inverse of a, such that a + (a) = 0.

Multiplicative inverses: for every a 0 in F, there exists an element in F, denoted by a1 or 1/a, called the multiplicative inverse of a, such that a a1 = 1.

Distributivity of multiplication over addition: a (b + c) = (a b) + (a c).

2.11.1 Example1

The set of real numbers, denoted "R", together with the regular addition (+) and multiplication (*) arithmetic operations is a field. Assuming we already know it is a ring (i.e., it's closed and associative under both operations, commutative under addition, has additive and multiplicative identities, and has additive inverses)

2.12 HOMOMORPHISM

A homomorphism is a map between two algebraic structures of the same type (that is of the same name), that preserves the operations of the structures. This means a map $f : A \to$ B f:A $\to$ B between two sets AA, BB *equipped with the same structure such that*, if $\cdot\,\cdot$ is an operation of the structure (supposed here, for simplification, to be a binary operation) , then
$f(x \cdot$ y)=f(x) $\cdot$ f(y)$f(x \cdot$ y)=f(x) $\cdot$ f(y)

2.13 CONSTANT FUNCTION

A constant function is a function which takes the same value for f(x) no matter what x is. When we are talking about a generic constant function, we usually write f(x) = c, where c is some unspecified constant. Examples of constant functions include f(x) = 0, f(x) = 1, f(x) = , f(x) = 0.

2.14 COSET

A subgroup H of a group G may be used to decompose the underlying set of G into disjoint, equal-size subsets called cosets. There are left cosets and right cosets. Cosets have the same number of elements as does H. Furthermore, H itself is both a left coset and a right coset.

gH = gh : h an element of H for g in G

Hg = hg : h an element of H for g in G.

2.14.1 Example1

Let G be the additive group of the integers,$\mathbb{Z} = (..., 2, 1, 0, 1, 2, ..., +)$ and H the subgroup $(3\mathbb{Z}, +) = (..., 6, 3, 0, 3, 6, ..., +)$. Then the cosets of H in G are the three sets $3\mathbb{Z}$, $\mathbb{Z}$ + 1, and $3\mathbb{Z}$ + 2, where $3\mathbb{Z} + a = ..., 6 + a, 3 + a, a, 3 + a, 6 + a, ...$ These three sets partition the set $\mathbb{Z}$, so there are no other right cosets of H. Due to the commutivity of addition H + 1 = 1 + H and H +

$2 = 2 + H$. That is, every left coset of H is also a right coset, so H is a normal subgroup. (The same argument shows that every subgroup of an Abelian group is normal.)

3 CHAPTER 1

BASICS OF IDEALS

3.1 IDEALS

An additive subgroup N of a ring R satisfying the properties

$$aN \subseteq N \text{ and } Nb \subseteq N; \text{ for all } a,b \in R$$

is an ideal

3.1.1 Example 1

We see that $n\mathbb{Z}$ is an ideal in the ring $\mathbb{Z}$ since we know it is a subring,and $s(nm)=(nm)s \in n\mathbb{Z}$ for all $s\in\mathbb{Z}$

3.1.2 Example 2

Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let C be the subring of F consisting of all constant function in F.Is C is an ideal in F? Why?

solution:

It is not true that the product of a constant function is again a constant function .For example ,the product of sinx and 2 is the function 2sinx .Thus C is not an ideal of F.

3.1.3 Example 3

Let F be the ring of all function mapping $\mathbb{R}$ into $\mathbb{R}$,and N be the subring of all function f such that f(2)=0.Is N an ideal in F?why or why not?

solution:

Let f$\in$N and let g$\in$N .Then
(fg)(2)=f(2)g(2)=0g(2)=0 ,so fg$\in$N.Similarly,we find that gf$\in$N.therefore N is an ideal of F.We could also have proved this by just observing that N is the kernel of the evaluation homomorphism 2:F$\longrightarrow$R

3.1.4 example 4

Ring
$\mathbb{Z}$=$\{..., -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, ...\}$
subset 2$\mathbb{Z}$=$\{..., -8, -6, -4, -2, 0, 2, 4, 6, 8, ...\}$
Take 3 from $\mathbb{Z}$
3(2$\mathbb{Z}$)=6$\mathbb{Z}$=$\{...., -12, -6, 0, 6, 12, ...\}$

That is $3(2\mathbb{Z}) \subseteq 2\mathbb{Z} \Longrightarrow$aN $\subseteq$N
In general we can say that nZ is said to be an ideal of $\mathbb{Z}$.

3.2 LEFT AND RIGHT IDEAL

A subring I of R is a left ideal if a$\in$I,

$$\text{r}\in \text{R} \Longrightarrow \text{ra}\in\text{I}$$

A right ideal is defined similarly.
A subring I of R is a right ideal if a$\in$I,

$$\text{r}\in\text{R} \Longrightarrow \text{ar}\in\text{I}$$

3.3 COROLLARY:

Let N be an ideal of a ring R.Then the additive cosets of N from a ring R/N with the binary operation defined by

$$(a+N)+(b+N)=(a+b)+N$$

and

$$(a+N)(b+N)=ab+N$$

3.4 THEOREM 1.1:

Let N be an ideal of ring R .Then

y:R$\longrightarrow$R/N given by $y(x) = x + N$

is a ring homomorphism with kernal N

3.5 THEOREM 1.2:

Fundamental Homomorphism Theorem:
Let ϕ:$R\longrightarrow R'$ be a ring homomorphism with kernal N .Then [R] is a ring map μ:$R/N\longrightarrow$[R] $given\ by$ u(x+n)=p(x)$is\ an\ isomorphism.If$y:R$\longrightarrow$R/ we have $p(x)$ =μy(x).

3.6 Properties In Ideal

- In a ring R ,the set R itself forms a two sided ideal called unit ideal.
- The $\{0_R\}$ consisting of only the additive identity 0_R forms a two sided ideal called the zero ideal.
- An (left , right or two sided) ideal that is not the unit ideal is called a proper ideal.

Note:

A left ideal is a proper ideal if and only if it does not contain a unit element.

Remark:

- The even integers forms an ideal in a $\mathbb{Z}$ of all integers;it is usually denoted by $2\mathbb{Z}$ .This is because sum of any even number is even,and the product of any integer with an even integer is also even .Similarly ,the set of all integers divisible by a fixed integer n is an ideal $n\mathbb{Z}$.
- The of all polynomial with real coefficient which are divisible by the polynomial x^2+1 is an ideal in the ring of all polynomials.
- The set of all n×n matrices whose last row is zero forms a right ideal in the ring of all n×n matrices .It is not a left ideal .The set of all n×n matrices whose last column is zero forms a left ideal but not a right ideal.
- A ring is called a simple ring if it is nonzero and has no two sided ideal other than (0),(1).

3.7 THEOREM 1.3:

The intersection of two ideal of a ring R is again an ideal of the ring R.

proof

consider I_1 and I_2 are two ideal
$\Longrightarrow$ I_1 and I_2 are subgroup of $\langle$R,+$\rangle$
$\Longrightarrow$ $I_1 \cap I_2$ is also a subgroup of $\langle$R,+$\rangle$
Now,if a $\in$ $I_1 \cap I_2$ and r$\in$ R
$\Longrightarrow$ a$\in$ I_1 and a $\in$ I_2 ,r$\in$ R.
since a$\in$ I and r$\in$ R
$\Longrightarrow$ ar$\in I_1$ and ra$\in I_1$
and ra$\in I_2$ and ar$\in I_2$
$\Longrightarrow$ ar$\in I_1$ and ar$\in I_2$
$\Longrightarrow$ ar$\in$ $I_1 \cap I_2$

3.8 THEOREM 1.4:

If I_1 and I_2 are two ideals then I_1+I_2 such that I_1+I_2 =$\{a_1$+a_2:$a_1 \in I_1$ and $a_2 \in I_2\}$ is also an ideal containing both I_1 and I_2.

proof

x and y $\in$ $I_1 + I_2$
x-y $\in$ $I_1 + I_2$
x=$a_1 + a_2$
y=$b_1 + b_2$

a$\in I_1 \Longrightarrow a+0 \in I_1$
$\Longrightarrow a+0 \in I_1+I_2$
$I_1 \subseteq I_1+I_2$

3.9 THEOREM 1.5:

If R is a commutative ring then for every a $\in$ R,

$$\text{Ra}=\{r.a, r \in R\}$$

is an ideal.

proof

$r_1a \in R_2$ and $r_2a \in R_2$
$\text{r}_1a - r_2a = (r_1 - r_2)a \in$ Ra
Ra is subgroup of $\langle$ R,+ $\rangle$
$\text{r}_1a \in$ Ra ,r$\in$ R
$\Longrightarrow r(r_1\ a) = (r\ r_1)a \in$ Ra
$\Longrightarrow (r_1\ a)r = r(a\ r_1) = r_1(r\ a)$
$= (r\ r_1)a \in$ Ra

3.10 Ideal Operation

- The sum and product of ideals are defined as follows .
  for a and b left(right) ideals of a ring R
  their sum is

$$a + b = \{a + b : a \in a and b \in b\},$$

which is a left(right) ideal, and if a,b are two sided

$$\text{ab} = \{a_1 b_1 + ... + a_n b_n : a_i \in a and b_i \in b, i = 1, 2, 3...n for n = 1, 2...\}$$

That is the product is the ideal generated by all product of the form ab with a in a and b in b

- The distributive law holds for two sided ideal a,b,c

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc$$

If a product is replaced by an intersection ,a partial distributive law holds:

$$a \cap (b + c) \supset a \cap b + a \cap c$$

where the equality holds if a contains b or c

- If a,b are ideal of a commutative ring R ,then $a \cap b = ab$ in the following two cases (at least)

$$a + b = (1)$$

a is generated by elements that form a regular sequence modulo b

Example:

In $\mathbb{Z}$ we have
$(n) \cap (m) = lcm(n, m)\mathbb{Z}$
since $(n) \cap (m)$ is the set of integers which are divisible by both n and m.
Let $R = \mathbb{C}x, y, z, w$
and let
$a = (z, w), b = (x + z, y + w), c = (x + z, w).$
then,

- $a + b = (z, w, x + z, y + w =$
  $(x, y, z, w) and a + c = (z, w, x + z)$
- $ab = (z(x + z), z(y + w), w(x + z), w(y + w)) =$
  $(x^2 + xz, zy + wz, wx + wz, wy + w^2)$
- $ac = (xz + z^2, zw, xw + zw, w^2)$
- $a \cap b = ab\ while\ a \cap c = (w, zx + z^2) \neq ac$

4 CHAPTER 2

TYPES OF IDEALS

4.1 MAXIMAL IDEALS

DEFINITION:

A maximal ideal of a ring R is an ideal M different from R such that there is no proper ideal N of R properly containing M.

4.1.1 Example

The ideal (2,*) is a maximal ideal in a ring $\mathbb{Z}$[X]. **Example** If F is a field ,then the only maximal ideal is $\{0\}$

4.1.2 Example

$\mathbb{Z}_8$ =$\{0, 1, 2, 3, 4, 5, 6, 7\}$

$\frac{1}{8}$ = $< 1 >$ = $\mathbb{Z}_8$

$\frac{2}{8}$ = $< 2 >$ = $\{0, 2, 4, 6\}$

$\frac{4}{8}$ = $< 4 >$ = $\{0, 4\}$

$\frac{8}{8}$ = $< 8 >$ = $\{0\}$

$< 8 > \subseteq < 4 > \subseteq < 2 > \subseteq < 1 >$ = $\mathbb{Z}_8$

Therefore $< 2 >$ is the only maximal ideal of $\mathbb{Z}_8$

4.1.3 Example

$\mathbb{Z}_{36}$

$\frac{1}{36}$ = $< 1 >$ = $\mathbb{Z}_{36}$

$\frac{2}{36}$ = $< 2 >$ = $\{0, 2, 4, 6, 8, 10, .., 32, 34\}$

$\frac{3}{36}$ = $< 3 >$ = $\{0, 3, 6, 9, .., 30, 33\}$

$\frac{4}{36}$ = $< 4 >$ = $\{0, 4, 8, 12, 16, 20, 24, 28, 32\}$

$\frac{6}{36}$ = $< 6 >$ = $\{0, 6, 12, 18, 24, 30\}$

$\frac{9}{36}$ = $< 9 >$ = $\{0, 9, 18, 27\}$

$\frac{12}{36}$ = $< 12 >$ = $\{0, 12, 24\}$

$\frac{18}{36}$ = $< 18 >$ = $\{0, 18\}$

$\frac{36}{36}$ = $< 36 >$ = $\{0\}$

$< 12 > \subseteq < 4 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 2 >$

$< 18 > \subseteq < 2 >$

$< 12 > \subseteq < 6 > \subseteq < 3 >$

$< 18 > \subseteq < 9 > \subseteq < 3 >$

$< 12 > \subseteq < 3 >$

$< 12 > \subseteq < 6 >$

Therefore $< 2 >$ and $< 3 >$ are maximal ideals of $\mathbb{Z}_{36}$

4.2 MINIMAL IDEALS

DEFINITION:

A non-zero ideal is called minimal if it contains no other non zero ideal.

4.2.1 Example

In an integral domain the only minimal ideal is the zero ideal

4.3 PRIME IDEALS

DEFINITION:

An ideal $N \in R$ is a commutative ring R is a prime ideal if $ab \in N$ implies either $a \in N$ or $b \in N$ for a,b R.

Note that $\{0\}$ is a prime ideal in $\mathbb{Z}$ and, indeed in any integral domain

4.3.1 Example

Note that $\mathbb{Z} \times \{0\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ for if $(a, b)(c, d) \in \mathbf{Z} \times \{0\}$. This implies that either

b = 0 so $(a, b) \in \mathbb{Z}\times \{0\}$ or d 0 so $(c, d) \in \mathbb{Z} \times \{0\}$ .Note that $(\mathbb{Z} \times \mathbb{Z})(\mathbb{Z} \times\{0\})$ is isomorphic to $\mathbb{Z}$ which is an integral domain.

4.3.2 Example

The prime ideals of $\mathbb{Z}$ are (0),(2),(3),(5),..

4.3.3 Example

2 $\mathbb{Z} \times 3\mathbb{Z}$ is not a prime ideal of $\mathbb{Z} \times \mathbb{Z}$. Since (2, 1) (1, 3) = (2, 3) $\in 2\mathbb{Z} \times 3\mathbb{Z}$ but (2,1) $\notin 2\mathbb{Z} \times 3\mathbb{Z}$ and (1,3)$\notin 2\mathbb{Z} \times 3\mathbb{Z}$

4.3.4 Example

12Z is not a prime ideal of $\mathbb{Z}$ since 3.8=24 $\in \{12\}$ but 3 $\notin \{12\}$ and 8 $\notin \{12\}$

4.3.5 Example

R = $\mathbb{Z}$= $\{ \pm 1, \pm 2, \pm 3, ..\}$
A = 2 $\mathbb{Z}$= $\{ 0, \pm 2, \pm 4, \pm 6, ..\}$
2 $\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$

5 CHAPTER 3

THEOREMS IN IDEALS

5.1 THEOREM

n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$ if and only if n is prime.

Proof

Let n$\mathbb{Z}$ be a prime ideal of $\mathbb{Z}$
Let if possible n is not a prime number
ie, n is composite
n=st ,$1 < s < n$,$1 < t < n$
n $\in$ n$\mathbb{Z}$
st $\in$ n$\mathbb{Z}$ and also s,t $\in \mathbb{Z}$
Since n$\mathbb{Z}$ is prime ideal
$\implies$ s $\in$ n$\mathbb{Z}$ or t $\in \mathbb{Z}$,which is not possible
$\therefore$ n is prime.
Conversely,
let n be a prime number
let a,b $\in \mathbb{Z}$ and ab $\in$ n$\mathbb{Z}$
$\implies$ n/ab
$\implies$ n/a or n/b ($\because$ n is prime)
$\implies$ $a = nk_1,\ or\ b = nk_2\ where\ k_1, k_2 \in \mathbb{Z}$
$\implies$ a $\in$ n$\mathbb{Z}$ or b $\in$ n$\mathbb{Z}$

$\Longrightarrow$ n$\mathbb{Z}$ is prime ideal of $\mathbb{Z}$.

5.2 THEOREM

Every maximal ideal in a commutative ring R with unity is a prime ideal.

Proof

If M is maximal in R,then R/M is a field. hence an integral domain, and therefore M is a prime ideal by theorem that let R be a commutative ring with unity,and let N $\notin$ R be an ideal in R. Then,R/N is an integral domain if and only if N is a prime ideal in R.

5.3 THEOREM

Let R is a commutative ring with unity, N is an ideal of R, N $\neq$ R
Then, N is a prime ideal of R if and only if R/N is an integral domain.

Proof

Given that R is a commutative ring with unity N is an ideal of R, N $\neq$ R
Assume that N is a prime ideal of R

R is commutative ring with unity $\Longrightarrow$ R/N is also a commutative ring with unity
Now we have to show that R/N has no zero divisor
(a+N)(b+N)=N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ ab $\in$ N
$\Longrightarrow$ a $\in$ N or b $\in$ N (since N is a prime ideal)
$\Longrightarrow$ a+N=N or b+N=N
ie,(a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\therefore$ R/N has no divisors
ie, R/N is an integral domain
conversely,
Assume that R/N is an integral domain
we have to show that N is an prime ideal
ab $\in$ N $\Longrightarrow$ ab+N=N
$\Longrightarrow$ (a+N)(b+N)=N
$\Longrightarrow$ a+N=N or b+N=N
$\Longrightarrow$ a $\in$ N or b $\in$ N
$\therefore$ N is an prime ideal

5.4 THEOREM

If A and B are two left ideals of a ring R, then A $\cap$ B is also a left ideal of R

Proof

let $x \in A \cap B$ and $r \in R$
since $x \in A \cap B \implies x \in A$ and $x \in B$
since $x \in A, r \in R \implies rx \in A$(since A is left ideal)
$x \in B, r \in R \implies rx \in B$(since B is left ideal)
since $rx \in A, rx \in B \implies rx \in A \cap B$
$\therefore A \cap B$ is a left ideal of R.

5.5 THEOREM

Let R be a commutaive ring with unity.
Then M is a maximal ideal of R if and only if R/M is a field.

Proof

suppose M is a maximal ideal in R.
Observe that if R is a commutative ring with unity,then R/M is also a nonzero commutative ring unity if $M \neq R$,which is the case if M is maximal.
Let $(a+M) \in R/M$,with $a \notin M$,so that a+M is not the addictive identity element of R/M.
Suppose a+M has no multiplicative inverse in R/M.

Then the set (R/M)(a+M)=(r+M)(a+M) (r+M) $\in$ R/M
we easily see that (R/M)(a+M) is an ideal of R/M.
It is nontrivial because a $\notin$ M,and it is a proper ideal because it does not contain 1+M
If γ :R $\longrightarrow$ R/M is the canonical
then $\gamma^{-}1$ [(R/M)(a+M)] is a proper ideal of R containing M.
But this contradicts our assumption that M is a maximal ideal, so a+M must have a multiplicative inverse in R/M.
conversely,
suppose that R/M is a field.
If N is any ideal of R such that M $\subseteq$ N $\subseteq$ R and γ is the canonical homomorphism of R onto R/M,then γ[N] is an ideal of R/M with [(0+M)] $\subseteq$ γ [N] $\subseteq$ R/M.
But this is contrary to that the field R/M contains no proper nontrivial ideals.
Hence if R/M is a field, M is maximal.

6 CONCLUSION

This project discusses the concept of ideals that is fundamental to ring theory.An ideal is an additive subgroup N of a ring R satisfying the properties $aN \subseteq N$ and $Nb \subseteq N$ for all $a,b \in R$.

In this project , the concept of an ideal is introduced and thus illustrated. It mostly includes the different types of ideals,its properties and different proofs related to this topic.

7 BIBILOGRAPHY

1. John B.Fraleigh ,***A First Course in Abstract Algebra*** Second Edition.
2. Gregory.T.Lee , ***Abstract Algebra*** An Introductory Course.
3. Joseph A.Gallian ,***Contemporary Abstract Algebra*** Ninth Edition.

NUMBERS OF SPECIAL FORMS

Project report submitted to
KANNUR UNIVERSITY
for the award of the degree
of
Bachelor of science
by
ABHIRAMI PS
DB20CMSR10
Under the guidance of
Ms.REMYA RAJ

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu
March 2023

CERTIFICATE

It is to certify that this project report **'NUMBERS OF SPECIAL FORMS'** is the bonafide project of **Abhirami P S** and that this project has been carried out by supervision.

Mrs.Riya Baby
Head Of The Department

Ms.Remya Raj
Supervisor

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu

DECLARATION

I Abhirami P S hereby declare that the project **'NUMBERS OF SPECIAL FORMS'** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms.Remya Raj, Department Of Mathematics,Don Bosco Arts And Science College,Angadikkadavu and has not submitted by me elsewhere for the award of my degree,diploma,title or recognition before.

ABHIRAMI P S
DB20CMSR10

Department Of Mathematics
Don Bosco Arts And Science College
AngadikkadavU

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude to everyone involved in this initiative.Many people have aided me in finishing this job successfully.

I'd like to express my heartfelt thanks to my supervisor Ms.Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for providing invaluable guidance, suggestions and for helping me complete my project.

I also express my sincere gratitude towards all the faculty members of the Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu.

I owe and respectfully offer my thanks to the principal and staff of Don Bosco Arts And Science College, Angadikkadavu for their constant moral support and mellifluous affection provided to me.

And i will be greatfull to all who directly or indirectly helped me to complete this project.Their guidance and support was very helpful in bringing this work to a conclusion.

CONTENTS

INTRODUCTION

Number theory(or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions.German mathematician Carl Friedrich Gauss (1777-1855) said, "Mathematics is the queen of the sciences - and number theory is the queen of mathematics.
In accordance with the research methods and objectives, we briefly divide number theory into four classes; Elementary number theory, Analytic number theory, Algebraic number theory and Geometric number theory. Here we only deals with the Elementary number theory.

Elementary number theory is also known as classical number theory.It is the basic theory for studying divisibility,congruences , diophantine equations etc, mainly by means of the four fundamental rules. It requires no long preliminary training, the content is tangible and more than any other path of mathematics, the methods of inquiry adhere to the scientific approach.

Applications of number theory:
Here are some of the most important applications of number theory. Number theory is used to find some of the important divisibility tests, whether a given integer m divides the integer n. Number theory have countless applications in mathematics as well in practical applications such as :
1) Security system like in banking securities.
2) E-commerce websites.
3) Coding theory.
4) Bar codes.
5) Making of modular designs.
6) Memory management system.
7) Authentication system.

It is also defined in hash functions, linear congruences, pseudo random numbers and fast arithmetic operations.

PRELIMINARIES

DIVISOR:

A divisor is a number that divides another number either completely or with a remainder.

GEOMETRIC PROGRESSION:

A geometric progression or a geometric sequence is the sequence , in which each term is varied by another by a common ratio. The next term of the sequence is produced when we multiply a constant(which is non-zero) to the preceding term. It is represented by:

$a, ar, ar2, ar3, ar4$ and so on.

where a is the first term and r is the common ratio.

GCD:

The greatest common divisor of two or more numbers is the greatest common factor number that divides them, exactly.
It is also called called the highest common factor (HCF).

Suppose $4, 8$ and 16 are three numbers .Then the factors of $4, 8$ and 16 are:

$4 - 1, 2, 4$
$8 - 1, 2, 4, 8$
$16 - 1, 2, 4, 8, 16$

Therefore we can conclude that 4 is the highest common factor among all three numbers.

COMPOSITE:

In mathematics composite numbers are that have more than two factors.
example:
factors of 6 are 1,2,3 and 6, which are four factors in total

PRIME:

Prime numbers are the positive integers having only two factors, 1 and the integer itself.
For example:
factors of 7 are only 1 and 7, totally two.

HYPOTHESIS:

Hypothesis is a proposition that is consistent with known data , but has been neither verified nor shown to be false.

RELATIVELY PRIME:

Two integers a and b, not both of which are zero, are said to be relatively prime whenever $gcd(a, b) = 1$.

example:
$4 - 1, 2, 4$
and $15 - 1, 3, 5$
Here $gcd(4, 15) = 1$.

Hence they are relatively prime.

CONGRUENT MODULO n:

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b(mod\ n)$ if n divides the difference $a - b$; that is provided that $a - b = kn$ for some integer k.

AMICABLE NUMBER:

Two numbers are amicable if each is equal to the sum of the proper divisors of the other (for example, 220 and 284).

PRIMALITY:

Primality:the property of being a prime number.

EULER'S CRITERION

Euler's criterion is a formula for determining whether an integer is a quadratic residue modulo a prime. Precisely,
Let p be an odd prime and a be an integer coprime to p. Then

$$a^{(p-1)/2} \equiv \begin{cases} 1\ (mod\ p)\ if\ there\ is\ an\ integer\ x\ such\ that\ a \equiv x^2\ (mod\ p), \\ -1\ (mod\ p)\ if\ there\ is\ no\ such\ integer. \end{cases}$$

Euler's criterion can be concisely reformulated using the Legendre symbol: $(a/p) = a^{(p-1)/2}\ \ (mod\ \ p)$

FERMAT'S THEOREM:

Let p be a prime and suppose that p doesn't divide a. Then $a^{p-1} \equiv 1 (mod\ p)$.

PURE MATHEMATICS:

Pure mathematics is the study of mathematical concepts independently of any application outside mathematics.

CHAPTER 1

PERFECT NUMBERS

1 Perfect Numbers

The history of the theory of numbers abounds with famous conjectues and open questions. this topic focuses on some of the intriguing congectures associated with perfect numbers.
A few of these have been satisfactorily answered, but most remain unresolved.

Example 1.1. *The pythagoreans considered it rather remarkable that the number 6 is equal to the sum of its positive* ***divisors,other than itself.***

6=1+2+3

The next number after 6 having this feature is 28; for the positive divisors of 28 are found to be 1,2,4,7,14 and 28.

28=1+2+4+7+14

And the pythagoreans called such numbers **'perfect'**.

definition 1.1. *A positive integer n is said to be perfect if n is equal to the sum of all its positive divisors,excluding n itself.*

The sum of the positive divisors of an integer n,each of them less than n, is given by $\sigma(n) - n = n$. Thus, the condition "n is perfect" amounts to asking that $\sigma(n) - n = n$ or equivalently that $\sigma(n) = 2n$

EXAMPLE

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 * 6$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 * 28$$

it was partially solved by Euclid when he proved that if the sum

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = p$$

is a prime number, then $2^{k-1}p$ is a perfect number(of necessity even). For instance, 1+2+4=7 is a prime. Hence 4*7=28 is a perfect number. Euclid's arguments makes use of the formula for the sum of a geometric progression

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = 2^{k-1}.$$

in this notation, the result reads as follows:

If 2^{k-1} is prime $(k > 1)$, then n = $2^{k-1}(2^k - 1)$ is a perfect number.

Theorem 1.1. *If $2^k - 1$ is prime $(k > 1)$, then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.*

proof

Let $2^k - 1 = p$, a prime, and consider the integer $n = 2^{k-1}p$. In as much as $gcd(2^{k-1}, p) = 1$, the multiplicativity of σ entails that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}p) \\ &= \sigma(2^{k-1})\sigma(p) \\ &= (2^{k-1})(p + 1)\end{aligned}$$

$$(2^k - 1)(2^k) = 2n$$

making n a perfect number. Now conversely assume that n is an even perfect number. we may write n as $n = 2^{k-1}m$, where m is an odd integer and $k \geq 2$. It follows from $gcd(2^{k-1}, m) = 1$ that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}m) \\ &= \sigma(2^{k-1})\sigma(m) \\ &= (2^{k-1})\sigma(m)\end{aligned}$$

whereas the requirement for a number to be perfect gives

$$\sigma(n) = 2n = 2^k m$$

Together these relations yield

$$2^k m = (2^k - 1)\sigma(m) \text{ .....(1)}$$

$\implies (2^{k-1})|2^k m$. But $2^k - 1 and 2^k$ are relatively prime, whence $(2^k - 1)|m$; hence $m = (2^k - 1)M$. Now, substituting this value of m into the equation (1) and cancelling $2^k - 1$ is that $\sigma(m) = 2^k M$. Because m and M are both divisors of m ($with M < m$), we have

$$2^k M = \sigma(m) \geq m + M = 2^k M$$

leading to $\sigma(m) = m + M$. The implication of this equality is that m has only two positive divisors to it , M and m itself.

It must be that m is prime and M=1 ; in other words

$$\begin{aligned}m &= (2^{k-1}M) \\ &= 2^k - 1\end{aligned}$$

Is a prime number, and hence the proof.

Remark 1.1. *Here our problem of finding even perfect number is reduced to the search for primes of the form* $2^k - 1$*, a closer look at these integers might be truthful.One thing that can be provided is that* 2^{k-1} *is a prime number, then the exponent* k *must itself be prime. More generally we have the following lemma.*

Lemma 1.1. *If* $a^k - 1$*is prime* $(a > 0, k \geq 2)$ *then a=2 and k is also prime.*

proof

$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + ... + a + 1)$
where in the present setting,

$$a^{k-1} + a^{k-2} + ... + a + 1 \geq a + 1 > 1$$

because by the hypothesis a^{k-1} is prime, the other factor must be 1; that is, a-1 = 1 so that a = 2.
If k were composite, then we could write $k = rs$ with $1 < r$ *and* $1 < s$. Thus

$$\begin{aligned} a^k - 1 &= (a^r)^s - 1 \\ &= (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + ... + a^r + 1) \end{aligned}$$

and each factor on the right is plainly greater than 1. But this violates the primality of $a^k - 1$, so that by contradiction k must be prime.

Remark 1.2. *For* $p = 2, 3, 5, 7$ *the values* $3, 7, 31, 127$ *of* $2^p - 1$ *are primes.*

so that

$$\begin{aligned} 2(2^2 - 1) &= 6 \\ 2^2(2^3 - 1) &= 28 \\ 2^4(2^5 - 1) &= 496 \\ 2^6(2^7 - 1) &= 8128 \end{aligned}$$

are all perfect numbers.Many early writers erroneously believed that $2^p - 1$ is prime for every choice of prime number p.
But we have,

$$2^{11} - 1 = 2047 = (23)(89) \text{ , not prime.}$$

But when $p = 13,\ 2^p - 1$ is prime and $2^{12}(2^{13} - 1) = 33550336$ be the fifth perfect number.
Therefore, we can say that $2^p - 1$ is prime and it is possible only when p is prime.

Theorem 1.2. *An even perfect number n ends in the digit 6 or 8 equivalently either*

$n \equiv 6(mod\ 10)$ *or* $n \equiv 8(mod\ 10)$

proof

Being an even perfect number n may be represented as $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime. According to the last lemma, the exponent k must also be prime. If $k = 2$, then $n = 6$, and the asserted result holds. We may therefore confine our assumption to case $k > 2$.
The proof falls into two parts, according as k takes the form 4m+1 or 4m+3.
If k is of the form 4m+1 then

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) \\ &= 2^{8k+1} - 2^{4m} \\ &= (2 * 16^{2m}) - 16^m \end{aligned}$$

$16^1 \equiv 6(mod\ 10)$ also
$16^t \equiv 6(mod\ 10)$ for any positive integer 't'
Therefore we get, $n = (2 * 6) - 6 \equiv 6(mod\ 10)$
Now in the case in which k= 4m+3

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 2^{8m+5} - 2^{4m+2} \\ &= (2 * 16^{2m+1}) - (4 * 16^m) \end{aligned}$$

Falling back on the fact that $16^t \equiv 6(mod\ 10)$, we see that

$$\begin{aligned} n \equiv (2 * 6) - (4 * 6) \equiv -12 \equiv 8(mod\ 10) \\ ie,\ \ n \equiv 8(mod\ 10) \end{aligned}$$

consequently, every even perfect number has a last digit equal to 6 or 8

Remark 1.3. *An even perfect number $n = 2^{k-1} * (2^k - 1)$ always ends in the digit 6 or 28. Because an integer is congruent modulo 100 to it's last two digits, it suffices to prove that, if k is of the form $4m+3$, then $n \equiv 28(mod\ 100)$.*

To see this, note that

$$\begin{aligned} 2^{k-1} &= 2^{4m+2} \\ &= (16^m)(4) \\ &\equiv (6)(4) \\ &\equiv 4(mod\ 10) \end{aligned}$$

Moreover, for $k > 2$ we have $4|2^{k-1}$, and therefore the number formed by the last two digits of 2^{k-1} is divisible by 4, and 4 divides the last two digits modulo 100, the various possibilities are

$$2^{k-1} \equiv 4, 24, 44, 64 or 84$$

But this implies that

$$2^k - 1 = 2 * 2^{k-1} \equiv 7, 47, 87, 27 \ or \ 67 (mod \ 100)$$

hence

$$n = 2^{k-1}(2^k - 1)$$
$$\equiv 4 * 7, 24 * 47, 44 * 87, 64 * 24 \ or \ 84 * 67 (mod \ 100)$$

CHAPTER 2
MERSENNE PRIME

2 Mersenne Prime

It has became traditional to call numbers of the form $M_n = 2^n - 1, n \geq 1$ Mersenne numbers after father Marin Mersenne who made an incorrect but provocative assertion concerning their primality.

definition 2.1. *Mersenne numbers that happens to be prime are said to be Mersenne primes.*

Remark 2.1. *M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and composite for all other primes $p < 257$*

Theorem 2.1. *If p and $q = 2p + 1$ are primes, then their $q|M_p$ or $q|M_p + 2$.*

proof

With reference to Fermat's theorem, we know that

$$2^{q-1} - 1 \equiv 0(modq)$$

and factorising the left hand side,that

$$(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) = (2^p - 1)(2^p + 1) \equiv 0(mod\ q)$$

$$ie,\ (2^p-1)(2^p+1) \equiv 0(mod\ q)$$
$$\implies (2^p-1)(2^p-1+2) \equiv 0(mod\ q)$$
$$\implies M_p(M_p+2) \equiv 0(mod\ q)$$

By using the theorem, "if p is a prime and $p|ab$, then $p|a$ or $p|b$ ", we cannot have both $q|M_p$ and $q|M_p+2, for\ then\ q|2$, which is impossible therefore either $q|M_p$ *or* $q|M_p+2$.

Example 2.1. *A simple application should suffice to illustrate the above theorem if* $p=23$*, then* $q=2p+1=47$ *is also a prime, so that we may consider the case of* M_{23}
The questions reduces to one of whether $47|M_{23}$ *or to put it differently, whether* $2^{23} \equiv 1(mod\ 47)$
now we have

$$2^{23} \equiv 2^3(2^5)^4 \equiv 2^3(-15)^4(mod\ 47)$$
$$(-15)^4 \equiv (225)^2 \equiv (-10)^2 \equiv 6(mod\ 47)$$

putting these two congruences together, it is seen that

$$2^{23} \equiv 2^3 * 6 \equiv 48 \equiv 1(mod\ 47)$$

hence M_{23} *is composite.*

Theorem 2.2. *If* $q=2n+1$ *is prime, then*

$$a)\ q|M_n\ ,\ provided\ that\ q \equiv 1(mod\ 8)\ or\ q \equiv 7(mod\ 8)$$
$$b)\ q|M_n+2,\ provided\ that\ q \equiv 3(mod\ 8)\ or\ q \equiv 5(mod\ 8)$$

proof

To say that $q|M_n$ is equivalent to asserting that

$$2^{(q-1)/2} = 2^n \equiv 1(mod\ q)\ .....(***)$$
$$2^n - 1 \equiv 0(mod\ q)$$

In terms of the legendre symbol, the condition (1) becomes the requirement that $(2/q) = 1$ but according to the theorem, if p is an odd prime then,

$$(2/q) = \begin{cases} 1,\ if\ p \equiv 1(mod\ 8)\ or\ p \equiv 7(mod\ 8) \\ (-1),\ if\ p \equiv 3(mod\ 8)\ or\ p \equiv 5(mod\ 8) \end{cases}$$

we get $(2/q) = 1$ when we have $q \equiv 1(mod\ 8)$ or $q \equiv 7(mod\ 8)$
the proof of (b) proceeds along similar lines.
we get $(q|m_n + 2)$ provided that $q \equiv 3(mod\ 8)$ or $q \equiv 5(mod\ 8)$

corollary 2.2.1. *If p and $q = 2p+1$ are both odd primes, with $p = 3(mod\ 4)$, then $q|M_p$*

proof

An odd prime p is either of the form $4k+1$ or $4k+2$. If $p = 4k+3$, then

$$q = 2(4k+3) + 1$$
$$= 8k + 7$$

and the above theorem yield $q|M_p$. since by the condition $q|M_n$ provided that $q \equiv 1(mod\ 8)$. In the case in which $p = 4k+1$, $q = 8k+3$ so that q does not divide M_p, since q is not congruent to $1(mod\ 8)$ or q is not congruent to $7(mod\ 8)$, hence the theorem.

Remark 2.2. *the following is a partial list of prime numbers* $p \equiv 3(mod\ 4)$ *where* $q = 2p + 1$ *is also prime:* $p = 11, 23, 83, 131, 179, 239, 251$.*In each instance,*$M_p$ *is composite.*

Exploring the matter a little further, the next tackle two results of Fermat that restricted the divisors of M_p

Theorem 2.3. *If* p *is an odd prime, then any prime divisors of* M_p *is of the form* $2k_p + 1$

proof

Let q be any prime divisors of M_p, so that $2^p \equiv 1(mod\ q)$. If 2 has order k modulo q. (ie if k is the smallest positive integer that satisfies $2^k \equiv 1(mod\ q)$),
then theorem " Let the integer a have order k modulo n. Then $a^k \equiv 1(mod\ n)$ if and only if $k|n$; in particular $k|\phi(n)$ .....$(*)$
Tells us that $k|p$. The case $k = 1$ cannot arise; for this would imply that $q|1$ (since if $k = 1$, $2^k - 1 \equiv 0(mod\ q) \implies q = 1$) an impossible situation. Therefore , because both $k|p$ and $k > 1$, the primality of p force $k = p$

In compliance with Fermat's theorem, we have $2^{q-1} \equiv 1(mod\ q)$, and again by theorem $(*)$ $k|(q-1)$ knowing that $k = p$, the net result is $p|(q-1)$. To be defined , let us put $q - 1 = pt$; then $q = pt + 1$. The proof is completed by noting that if t were an odd integer, then q would be even and a contradiction occurs. Hence , we must have $q = 2k_p + 1$. For some choice of k, which gives q the required form.

Theorem 2.4. *If* p *is an odd prime , then any prime divisor* q *of* m_p *is of the form* $q \equiv \pm 1(mod\ 8)$.

proof

Suppose that $q = 2n + 1$ is a prime divisor of m_p.
If $a = 2^{(p+1)/2}$, then

$$\begin{aligned} a^2 - 2 &= (2^{(p+1)/2})^2 - 2 \\ &= 2^{p+1} - 2 \\ &= 2^p \times 2 - 2 \\ &= 2(2^p - 1) \\ &= 2M_p \\ &\equiv 0(mod\ q) \end{aligned}$$

Raising both sides of the congruence $a^2 \equiv 2(mod\ q)$ to the n^{th} power, we get

$$a^{q-1} = a^{2n} \equiv 2^n(mod\ q)$$

Since q is an odd integer , one has $gcd(a, q) = 1$ and so $a^{q-1} \equiv 1(mod\ q)$. In conjunction, the last congruence tell us that

$$\begin{aligned} &2^n \equiv 1(mod\ q) \\ \implies\ &2^n - 1 \equiv 0(mod\ q) \\ \implies\ &q|M_n \end{aligned}$$

the theorem $(***)$ now be brought into play to reach the condition that $q \equiv \pm 1(mod\ 8)$
Therefore we get if p is an odd prime then any prime divisor q of M_p is of the form

$$q \equiv \pm 1(mod\ 8)$$

hence the theorem.

Remark 2.3. *For an illustration of how these theorems can be used, one might look at* M_{17}. *These integers of the form* $34k + 1$ *that are less than* $362 < \sqrt{M_{17}}$ *are* $35, 69, 103, 137, 171, 205, 239, 273, 307, 341$.

Because the smallest (non-trivial) divisors of M_{17} must be prime, we need only consider the primes among the foregoing 10 numbers namely, $103, 137, 239, 307$ the work can be shortened some what by noting that 307 is not congruent to $\pm 1(mod\ 8)$, and therefore we may delete 307 from our list.Now, either M_{17} is prime or one of the three remaining possibilities divide it with a little calculations we can check that M_{17} is divisible by none of $103, 137,$ *and* 239; the result M_{17} is prime.

Theorem 2.5. ***EULER:*** *If* n *is a perfect number, then any* $n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ *where the* $p_i's$ *are distinct odd primes and* $p_1 \equiv\ k_1 \equiv 1(mod\ 4)$.

proof

Let $n = \ n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ be the prime factorisation of n. Because n is perfect.We can write

$$2n = \sigma(n) = \sigma({p_1}^{k_1}) \ \times\sigma({p_2}^{k_2}) \ ..... \times\sigma({p_r}^{k_r})$$
being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$

being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$; in any event, $2n \equiv 2(mod\ 4)$. Thus , $\sigma(n) = 2n$ is divisible by 2, but not by 4. The implication is that one of the $\sigma({p_i}^{k_i})$, say $\sigma({p_i}^{k_i})$, must be an even integer (but not divisible by 4), and all the remaining $\sigma({p_i}^{k_i})$'s are odd integers.

For a given p_i , there are two cases to be considered:
$p_i \equiv 1(mod\ 4)$ and $p_i \equiv 3(mod\ 4)$. If $p_i \equiv 3 \equiv -1(mod\ 4)$, we would have,

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^{k_i}$$
$$\equiv 1 + (-1) + (-1)^2 + ... + (-1)^{k_i} (mod\ 4)$$
$$\equiv \begin{cases} 0(mod\ 4)\ if\ k_i\ is\ odd \\ 1(mod\ 4)\ if\ k_i\ is\ even \end{cases}$$

since $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$, this tells us that $p_1 \not\equiv 3(mod\ 4)$ or, to put it affirmatively, $p_1 \equiv 1(mod\ 4)$. Furthermore, the congruence $\sigma({p_i}^{k_i}) \equiv 0(mod\ 4)$ signifies that 4 divides $\sigma({p_i}^{k_i})$ which is not possible.
The conclusion : if $p_i \equiv 3(mod\ 4)$ where $i = 2, ..., r$ then it's exponent k_i must be an even integer.
Should it happen that $p_i \equiv 1(mod\ 4)$ which is certainly true for i=1,then

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^k$$
$$\equiv 1 + 1^1 + 1^2 + ... + 1^{k_i} (mod\ 4)$$
$$\equiv k_i + 1(mod\ 4)$$

The condition $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$ for as $k_1 \equiv 1(mod\ 4)$.For the other values of i, we know that $\sigma({p_i}^{k_i}) \equiv 1\ or\ 3(mod\ 4)$, and therefore $k_i \equiv 0\ or\ 2(mod\ 4)$; in any case k_i is an even integer. The crucial point is that, regardless of whether $p_i \equiv 1(mod\ 4)$ or $p_i \equiv 3(mod\ 4)$, k_i is always for $i \neq 1$. Our proof is now complete.

Remark 2.4. *In view of the preceding theorem, any odd perfect number n can be expressed as*

$$n = {p_1}^{k_1} {p_2}^{2j_2} .....{p_r}^{2j_r}$$
$$= p_1^{k_1} ({p_2}^{j_2} .....p_r^{j_r})^2$$
$$= {p_1}^{k_1} m^2$$

This leads directly to the following corollary.

corollary 2.5.1. *If n is an odd perfect number, then n is of the form $n = p^k m^2$. Where p is a prime, p does not divides m, and $p \equiv k \equiv 1(mod\ 4)$; in particular, $n = 1(mod\ 4)$*

proof

Only the last assertion is not obvious.Because $p \equiv 1(mod\ 4)$, we have $p^k \equiv 1(mod\ 4)$.Notice that m must be odd; hence $m \equiv 1$ *or* $3(mod\ 4)$, and therefore upon squaring, $m^2 \equiv 1(mod\ 4)$. It follows that

$$n = p^k m^2 \equiv 1 \times 1 \equiv 1(mod\ 4)$$

establishing our corollary.

definition 2.2. *Two numbers such as* 220 *and* 284 *are called amicable, or friendly; because they have the remarkable property that each number is " contained" within the other, in the sense that each number is equal to the sum of all the positive divisors of the other , not counting the number itself.Thus, as regards the divisors* 220

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

and for 284*,*

$$1 + 2 + 4 + 71 + 142 = 220$$

In terms of the σ function, amicable numbers m and n (or an amicable pair) are defined by the equation.

$$\sigma(m) - m = n$$
$$\sigma(n) - n = m$$

or what amounts to the same thing;

$$\sigma(m) = m + n = \sigma(n)$$

Remark 2.5. *Amicable number have been important in magic and astrology, and casting horoscope, making talismans. The Greeks believed that these numbers had a particular influence in establishing friendship between individuals.*

CHAPTER 3

FERMAT NUMBERS

3 Fermat Numbers:

definition 3.1. *A Fermat number is an integer of the form*

$$F_n = 2^{2^n} + 1,\ n \geq 0$$

If F_n is prime, it is said to be a fermat prime.

Remark 3.1. $F_0 = 3,\ F_1 = 5,\ F_2 = 17\ F_3 = 257,\ F_4 = 65537$ *and* $F_5 = 2^{2^5} + 1 = 4294967297$

Theorem 3.1. *The fermat number F_5 is divisible by* 641

proof

We begin by putting $a = 2^7$ and $b = 5$, so that

$$1 + ab = 1 + (2^7 \times 5) = 641$$

It is easily seen that

$$1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b = 2^4$$

But this implies that;

$$\begin{gathered} F_5 = 2^{2^5} + 1 = 2^{32} + 1 \\ = (2^4 \times a^4) + 1 \\ = (1 + ab - b^4)a^4 + 1 \\ (1 + ab)a^4 + (1 - a^4b^4) \\ = (1 + ab)[a^4 + (1 - ab)(1 + a^2b^2)] \end{gathered}$$

which gives $641|F_n$.

Theorem 3.2. *For fermat numbers F_n and F_m, where $m > n \geq 0$, $gcd(F_m, F_n) = 1$.*

proof

Put $d = gcd(F_m, F_n) = 1$. Because Fermat numbers are odd integers, d must be odd. If we set $x = 2^{2^n}$ *and* $k = 2^{m-n}$ *then*

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

$$= \frac{x^k - 1}{x + 1}$$

$$= x^{k-1} - x^{k-2} + ... - 1$$

hence $F_n|(F_m - 2)$.From $d|F_n$, it follows that $d|(F_m - 2)$.Now use the fact that $d|F_m$ to obtain $d|2$. But d is an odd integer, and so $d = 1$, establishing the result is claimed.

Remark 3.2. *We know that each of the Fermat numbers $F_0, F_1, F_2, ...F_N$ is divisible by a prime that does not divide any of the other F_k. Thus, there*

are at least $n+1$ distinct primes not exceeding F_n.Because there are infinitely many Fermat numbers, the number of primes is also infinite.
In 1877, the Jesuit priest T.Pepin devised the practical test(Pepin's test for determining the primality of F_n that is embodied in the following theorem.)

Theorem 3.3. *Pepin's test; For $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if*

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

proof

First let us assume that,

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Upon squaring both sides we get

$$3^{F_n-1} \equiv 1(mod\ F_n)$$

The same congruence holds for any prime p that divides F_n

$$3^{F_n-1} \equiv 1(mod\ p)$$

Now let k be the order of 3 modulo p. We know that $k|(F_n - 1)$ or in other words, that $k|2^{2^n}$ therefore k must be a power of 2.
It is not possible that $k = 2^r$ for any $r \leq 2^n - 1$
For if this were so, repeated squaring of the congruence $3^k \equiv 1(mod\ p)$ would yield

$$3^{2^{2^n-1}} \equiv 1(mod\ p)$$

or, what is the same thing,

$$3^{F_n-1} \equiv 1(mod\ p)$$

We would then arrive at $1 \equiv -1(mod\ p)$, resulting in $p = 2$, which is a contradiction. Thus the only possibility open to us is that

$$k = 2^{2^n} = F_n - 1$$

Fermat's theorem tells us that $k \leq p - 1$, which means, in turn, that $F_n = k + 1 \leq p$. Because $p|F_n$, we also have $p \leq F_n$.Together, these inequalities mean that $F_n = p$, so that F_n is prime. On the other hand, suppose that $F_n,\ n \geq 1$ is prime.
The quadratic Reciprocity Law gives

$$(3|F_n) = (F_n|3) = (2|3) = -1$$

When we use the fact that

$$F_n \equiv (-1)^{2^n} + 1 = 2(mod\ 3)$$

Applying Euler's criterion, we end up with

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Example 3.1. *Show that using Pepin's test $F_3 = 257$ is prime.*

proof

$$3^{\frac{p_3-1}{2}} = 3^{128} = 3^3(3^5)^{25}$$
$$\equiv 27(-14)^{25}$$
$$\equiv 27 \times 14^{24}(-14)$$
$$\equiv 27(17)(-14)$$
$$\equiv 27 \times 19 \equiv 513 \equiv -1(mod\ 257)$$

So that F_3 is prime.

Theorem 3.4. *Any prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, is of the form*

$$p = k \times 2^{(n+2)} + 1$$

proof

For a prime divisor p of F_n,

$$2^{2^n} \equiv -1(mod\ p)$$

Which is to say, upon squaring that

$$2^{2^{n+1}} \equiv 1(mod\ p)$$

If h is the order of 2 modulo p, this congruence tells us that $h|2^{n+1}$.We cannot have $h = 2^r$ where $1 \leq r \leq n$, for this would lead to $2^{2^n} \equiv 1(mod\ p)$ and in turn, to the contradiction that $p = 2$.This let us conclude that $h = 2^{n+1}$. Because the order of 2 modulo p divides $\phi(p) = p - 1$, we may further conclude that $2^{n+1}|p - 1$.The point is that for $n \geq 2, p \equiv 1(mod\ 8)$, and therefore, by theorem, if p is an odd number then $2|p$, the Legendre symbol $(2|P) = 1$.

Using Euler's criterion, we immediately pass to

$$2^{\frac{(p-1)}{2}} \equiv (2|p) = 1(mod\ p)$$

An appeal to theorem " let the integer a have order k modulo n, then $a^h \equiv 1(mod\ n)$ if and only if $k|n$, in particular, $k|\phi(n)$, " finishes the proof. It asserts that $h|\frac{(p-1)}{2}$, or equivalently, $2^{(n+1)}|\frac{(p-1)}{2}$.This forces $2^{n+2}|(p-1)$ and we obtain $p = k \times 2^{(n+2)} + 1$ for some integer k.

CONCLUSION

Number theory is the study of the integers and related objects.Topics studied by number theorists include the problem of determining the distribution of prime numbers within the integers and the structure and number of solutions of polynomial equations with integer co-effecients.
A branch of pure mathematics that deals with the study of natural numbers and the study deals with the set of positive whole numbers that are usually called the set of natural numbers and is partly experimental and partly theoretical.

Number theory is necessary for the study of numbers because it shows what numbers can do. It helps in providing valuable training in logical thinking and studying the relationship between different kinds of numbers. It is applied in cryptography, device authentication, websites for e-commerce, coding, and security systems.

BIBLIOGRAPHY

1. DAVID M. BURTON, ELEMENTARY NUMBER THEORY, 7th edition

2. JOSEPH H. SILVERMAN, A FRIENDLY INTRODUCTION TO NUMBER THEORY, 4th edition, Pearson

3. https://www.cuemath.com/numbers/number-theory/

NUMBERS OF SPECIAL FORMS

Project report submitted to
KANNUR UNIVERSITY
for the award of the degree
of
Bachelor of science
by
ASHIN TOM
DB20CMSR09
Under the guidance of
Ms.REMYA RAJ

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu
March 2023

CERTIFICATE

It is to certify that this project report **'NUMBERS OF SPECIAL FORMS'** is the bonafide project of **Ashin Tom** and that this project has been carried out by supervision.

Mrs.Riya Baby
Head Of The Department

Ms.Remya Raj
Supervisor

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu

DECLARATION

I Ashin Tom hereby declare that the project **'NUMBERS OF SPECIAL FORMS'** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms.Remya Raj, Department Of Mathematics,Don Bosco Arts And Science College,Angadikkadavu and has not submitted by me elsewhere for the award of my degree,diploma,title or recognition before.

ASHIN TOM
DB20CMSR09

Department Of Mathematics
Don Bosco Arts And Science College
AngadikkadavU

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude to everyone involved in this initiative.Many people have aided me in finishing this job successfully.

I'd like to express my heartfelt thanks to my supervisor Ms.Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for providing invaluable guidance, suggestions and for helping me complete my project.

I also express my sincere gratitude towards all the faculty members of the Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu.

I owe and respectfully offer my thanks to the principal and staff of Don Bosco Arts And Science College, Angadikkadavu for their constant moral support and mellifluous affection provided to me.

And i will be greatfull to all who directly or indirectly helped me to complete this project.Their guidance and support was very helpful in bringing this work to a conclusion.

CONTENTS

INTRODUCTION

Number theory(or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions.German mathematician Carl Friedrich Gauss (1777-1855) said, "Mathematics is the queen of the sciences - and number theory is the queen of mathematics.
In accordance with the research methods and objectives, we briefly divide number theory into four classes; Elementary number theory, Analytic number theory, Algebraic number theory and Geometric number theory. Here we only deals with the Elementary number theory.

Elementary number theory is also known as classical number theory.It is the basic theory for studying divisibility,congruences , diophantine equations etc, mainly by means of the four fundamental rules. It requires no long preliminary training, the content is tangible and more than any other path of mathematics, the methods of inquiry adhere to the scientific approach.

Applications of number theory:
Here are some of the most important applications of number theory. Number theory is used to find some of the important divisibility tests, whether a given integer m divides the integer n. Number theory have countless applications in mathematics as well in practical applications such as :
1) Security system like in banking securities.
2) E-commerce websites.
3) Coding theory.
4) Bar codes.
5) Making of modular designs.
6) Memory management system.
7) Authentication system.

It is also defined in hash functions, linear congruences, pseudo random numbers and fast arithmetic operations.

PRELIMINARIES

DIVISOR:

A divisor is a number that divides another number either completely or with a remainder.

GEOMETRIC PROGRESSION:

A geometric progression or a geometric sequence is the sequence , in which each term is varied by another by a common ratio. The next term of the sequence is produced when we multiply a constant(which is non-zero) to the preceding term. It is represented by:

$a, ar, ar2, ar3, ar4$ and so on.

where a is the first term and r is the common ratio.

GCD:

The greatest common divisor of two or more numbers is the greatest common factor number that divides them, exactly.
It is also called called the highest common factor (HCF).

Suppose $4, 8$ and 16 are three numbers .Then the factors of $4, 8$ and 16 are:

$4 - 1, 2, 4$
$8 - 1, 2, 4, 8$
$16 - 1, 2, 4, 8, 16$

Therefore we can conclude that 4 is the highest common factor among all three numbers.

COMPOSITE:

In mathematics composite numbers are that have more than two factors.
example:
factors of 6 are 1,2,3 and 6, which are four factors in total

PRIME:

Prime numbers are the positive integers having only two factors, 1 and the integer itself.
For example:
factors of 7 are only 1 and 7, totally two.

HYPOTHESIS:

Hypothesis is a proposition that is consistent with known data , but has been neither verified nor shown to be false.

RELATIVELY PRIME:

Two integers a and b, not both of which are zero, are said to be relatively prime whenever $gcd(a, b) = 1$.

example:
$4 - 1, 2, 4$
and $15 - 1, 3, 5$
Here $gcd(4, 15) = 1$.

Hence they are relatively prime.

CONGRUENT MODULO n:

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b(mod\ n)$ if n divides the difference $a - b$; that is provided that $a - b = kn$ for some integer k.

AMICABLE NUMBER:

Two numbers are amicable if each is equal to the sum of the proper divisors of the other (for example, 220 and 284).

PRIMALITY:

Primality:the property of being a prime number.

EULER'S CRITERION

Euler's criterion is a formula for determining whether an integer is a quadratic residue modulo a prime. Precisely,
Let p be an odd prime and a be an integer coprime to p. Then

$$a^{(p-1)/2} \equiv \begin{cases} 1\ (mod\ p)\ if\ there\ is\ an\ integer\ x\ such\ that\ a \equiv x^2\ (mod\ p), \\ -1\ (mod\ p)\ if\ there\ is\ no\ such\ integer. \end{cases}$$

Euler's criterion can be concisely reformulated using the Legendre symbol: $(a/p) = a^{(p-1)/2}\ \ (mod\ \ p)$

FERMAT'S THEOREM:

Let p be a prime and suppose that p doesn't divide a. Then $a^{p-1} \equiv 1 (mod\ p)$.

PURE MATHEMATICS:

Pure mathematics is the study of mathematical concepts independently of any application outside mathematics.

CHAPTER 1

PERFECT NUMBERS

1 Perfect Numbers

The history of the theory of numbers abounds with famous conjectues and open questions. this topic focuses on some of the intriguing congectures associated with perfect numbers.
A few of these have been satisfactorily answered, but most remain unresolved.

Example 1.1. *The pythagoreans considered it rather remarkable that the number 6 is equal to the sum of its positive* ***divisors,other than itself.***

6=1+2+3

The next number after 6 having this feature is 28; for the positive divisors of 28 are found to be 1,2,4,7,14 and 28.

28=1+2+4+7+14

And the pythagoreans called such numbers **'perfect'**.

definition 1.1. *A positive integer n is said to be perfect if n is equal to the sum of all its positive divisors,excluding n itself.*

The sum of the positive divisors of an integer n,each of them less than n, is given by $\sigma(n) - n = n$. Thus, the condition "n is perfect" amounts to asking that $\sigma(n) - n = n$ or equivalently that $\sigma(n) = 2n$

EXAMPLE

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 * 6$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 * 28$$

it was partially solved by Euclid when he proved that if the sum

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = p$$

is a prime number, then $2^{k-1}p$ is a perfect number(of necessity even). For instance, 1+2+4=7 is a prime. Hence 4*7=28 is a perfect number. Euclid's arguments makes use of the formula for the sum of a geometric progression

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = 2^{k-1}.$$

in this notation, the result reads as follows:

If 2^{k-1} is prime $(k > 1)$, then n = $2^{k-1}(2^k - 1)$ is a perfect number.

Theorem 1.1. *If $2^k - 1$ is prime $(k > 1)$, then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.*

proof

Let $2^k - 1 = p$, a prime, and consider the integer $n = 2^{k-1}p$. In as much as $gcd(2^{k-1}, p) = 1$, the multiplicativity of σ entails that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}p) \\ &= \sigma(2^{k-1})\sigma(p) \\ &= (2^{k-1})(p + 1)\end{aligned}$$

$$(2^k - 1)(2^k) = 2n$$

making n a perfect number. Now conversely assume that n is an even perfect number. we may write n as $n = 2^{k-1}m$, where m is an odd integer and $k \geq 2$. It follows from $gcd(2^{k-1}, m) = 1$ that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}m) \\ &= \sigma(2^{k-1})\sigma(m) \\ &= (2^{k-1})\sigma(m)\end{aligned}$$

whereas the requirement for a number to be perfect gives

$$\sigma(n) = 2n = 2^k m$$

Together these relations yield

$$2^k m = (2^k - 1)\sigma(m) \text{ .....(1)}$$

$\implies (2^{k-1})|2^k m$. But $2^k - 1 and 2^k$ are relatively prime, whence $(2^k - 1)|m$; hence $m = (2^k - 1)M$. Now, substituting this value of m into the equation (1) and cancelling $2^k - 1$ is that $\sigma(m) = 2^k M$. Because m and M are both divisors of m ($with M < m$), we have

$$2^k M = \sigma(m) \geq m + M = 2^k M$$

leading to $\sigma(m) = m + M$. The implication of this equality is that m has only two positive divisors to it , M and m itself.

It must be that m is prime and M=1 ; in other words

$$\begin{aligned}m &= (2^{k-1}M) \\ &= 2^k - 1\end{aligned}$$

Is a prime number, and hence the proof.

Remark 1.1. *Here our problem of finding even perfect number is reduced to the search for primes of the form* $2^k - 1$*, a closer look at these integers might be truthful.One thing that can be provided is that* 2^{k-1} *is a prime number, then the exponent* k *must itself be prime. More generally we have the following lemma.*

Lemma 1.1. *If* $a^k - 1$*is prime* $(a > 0, k \geq 2)$ *then a=2 and k is also prime.*

proof

$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + ... + a + 1)$
where in the present setting,

$$a^{k-1} + a^{k-2} + ... + a + 1 \geq a + 1 > 1$$

because by the hypothesis a^{k-1} is prime, the other factor must be 1; that is, a-1 = 1 so that a = 2.
If k were composite, then we could write $k = rs$ with $1 < r$ *and* $1 < s$. Thus

$$\begin{aligned} a^k - 1 &= (a^r)^s - 1 \\ &= (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + ... + a^r + 1) \end{aligned}$$

and each factor on the right is plainly greater than 1. But this violates the primality of $a^k - 1$, so that by contradiction k must be prime.

Remark 1.2. *For* $p = 2, 3, 5, 7$ *the values* $3, 7, 31, 127$ *of* $2^p - 1$ *are primes.*

so that

$$\begin{aligned} 2(2^2 - 1) &= 6 \\ 2^2(2^3 - 1) &= 28 \\ 2^4(2^5 - 1) &= 496 \\ 2^6(2^7 - 1) &= 8128 \end{aligned}$$

are all perfect numbers.Many early writers erroneously believed that $2^p - 1$ is prime for every choice of prime number p.
But we have,

$$2^{11} - 1 = 2047 = (23)(89) \text{ , not prime.}$$

But when $p = 13,\ 2^p - 1$ is prime and $2^{12}(2^{13} - 1) = 33550336$ be the fifth perfect number.
Therefore, we can say that $2^p - 1$ is prime and it is possible only when p is prime.

Theorem 1.2. *An even perfect number n ends in the digit 6 or 8 equivalently either*

$n \equiv 6(mod\ 10)$ *or* $n \equiv 8(mod\ 10)$

proof

Being an even perfect number n may be represented as $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime. According to the last lemma, the exponent k must also be prime. If $k = 2$, then $n = 6$, and the asserted result holds. We may therefore confine our assumption to case $k > 2$.
The proof falls into two parts, according as k takes the form 4m+1 or 4m+3.
If k is of the form 4m+1 then

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) \\ &= 2^{8k+1} - 2^{4m} \\ &= (2 * 16^{2m}) - 16^m \end{aligned}$$

$16^1 \equiv 6(mod\ 10)$ also
$16^t \equiv 6(mod\ 10)$ for any positive integer 't'
Therefore we get, $n = (2 * 6) - 6 \equiv 6(mod\ 10)$
Now in the case in which k= 4m+3

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 2^{8m+5} - 2^{4m+2} \\ &= (2 * 16^{2m+1}) - (4 * 16^m) \end{aligned}$$

Falling back on the fact that $16^t \equiv 6(mod\ 10)$, we see that

$$\begin{aligned} n \equiv (2 * 6) - (4 * 6) \equiv -12 \equiv 8(mod\ 10) \\ ie,\ \ n \equiv 8(mod\ 10) \end{aligned}$$

consequently, every even perfect number has a last digit equal to 6 or 8

Remark 1.3. *An even perfect number $n = 2^{k-1} * (2^k - 1)$ always ends in the digit 6 or 28. Because an integer is congruent modulo 100 to it's last two digits, it suffices to prove that, if k is of the form $4m+3$, then $n \equiv 28(mod\ 100)$.*

To see this, note that

$$\begin{aligned} 2^{k-1} &= 2^{4m+2} \\ &= (16^m)(4) \\ &\equiv (6)(4) \\ &\equiv 4(mod\ 10) \end{aligned}$$

Moreover, for $k > 2$ we have $4|2^{k-1}$, and therefore the number formed by the last two digits of 2^{k-1} is divisible by 4, and 4 divides the last two digits modulo 100, the various possibilities are

$$2^{k-1} \equiv 4, 24, 44, 64 or 84$$

But this implies that

$$2^k - 1 = 2 * 2^{k-1} \equiv 7, 47, 87, 27 \ or \ 67 (mod \ 100)$$

hence

$$n = 2^{k-1}(2^k - 1)$$
$$\equiv 4 * 7, 24 * 47, 44 * 87, 64 * 24 \ or \ 84 * 67 (mod \ 100)$$

CHAPTER 2
MERSENNE PRIME

2 Mersenne Prime

It has became traditional to call numbers of the form $M_n = 2^n - 1, n \geq 1$ Mersenne numbers after father Marin Mersenne who made an incorrect but provocative assertion concerning their primality.

definition 2.1. *Mersenne numbers that happens to be prime are said to be Mersenne primes.*

Remark 2.1. *M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and composite for all other primes $p < 257$*

Theorem 2.1. *If p and $q = 2p + 1$ are primes, then their $q|M_p$ or $q|M_p + 2$.*

proof

With reference to Fermat's theorem, we know that

$$2^{q-1} - 1 \equiv 0(modq)$$

and factorising the left hand side,that

$$(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) = (2^p - 1)(2^p + 1) \equiv 0(mod\ q)$$

$$ie,\ (2^p-1)(2^p+1) \equiv 0(mod\ q)$$
$$\implies (2^p-1)(2^p-1+2) \equiv 0(mod\ q)$$
$$\implies M_p(M_p+2) \equiv 0(mod\ q)$$

By using the theorem, "if p is a prime and $p|ab$, then $p|a$ or $p|b$ ", we cannot have both $q|M_p$ and $q|M_p+2, for\ then\ q|2$, which is impossible therefore either $q|M_p$ *or* $q|M_p+2$.

Example 2.1. *A simple application should suffice to illustrate the above theorem if* $p=23$*, then* $q=2p+1=47$ *is also a prime, so that we may consider the case of* M_{23}
The questions reduces to one of whether $47|M_{23}$ *or to put it differently, whether* $2^{23} \equiv 1(mod\ 47)$
now we have

$$2^{23} \equiv 2^3(2^5)^4 \equiv 2^3(-15)^4(mod\ 47)$$
$$(-15)^4 \equiv (225)^2 \equiv (-10)^2 \equiv 6(mod\ 47)$$

putting these two congruences together, it is seen that

$$2^{23} \equiv 2^3 * 6 \equiv 48 \equiv 1(mod\ 47)$$

hence M_{23} *is composite.*

Theorem 2.2. *If* $q=2n+1$ *is prime, then*

$$a)\ q|M_n\ ,\ provided\ that\ q \equiv 1(mod\ 8)\ or\ q \equiv 7(mod\ 8)$$
$$b)\ q|M_n+2,\ provided\ that\ q \equiv 3(mod\ 8)\ or\ q \equiv 5(mod\ 8)$$

proof

To say that $q|M_n$ is equivalent to asserting that

$$2^{(q-1)/2} = 2^n \equiv 1(mod\ q)\ .....(***)$$
$$2^n - 1 \equiv 0(mod\ q)$$

In terms of the legendre symbol, the condition (1) becomes the requirement that $(2/q) = 1$ but according to the theorem, if p is an odd prime then,

$$(2/q) = \begin{cases} 1,\ if\ p \equiv 1(mod\ 8)\ or\ p \equiv 7(mod\ 8) \\ (-1),\ if\ p \equiv 3(mod\ 8)\ or\ p \equiv 5(mod\ 8) \end{cases}$$

we get $(2/q) = 1$ when we have $q \equiv 1(mod\ 8)$ or $q \equiv 7(mod\ 8)$
the proof of (b) proceeds along similar lines.
we get $(q|m_n + 2)$ provided that $q \equiv 3(mod\ 8)$ or $q \equiv 5(mod\ 8)$

corollary 2.2.1. *If p and $q = 2p+1$ are both odd primes, with $p = 3(mod\ 4)$, then $q|M_p$*

proof

An odd prime p is either of the form $4k+1$ or $4k+2$. If $p = 4k+3$, then

$$q = 2(4k+3) + 1$$
$$= 8k + 7$$

and the above theorem yield $q|M_p$. since by the condition $q|M_n$ provided that $q \equiv 1(mod\ 8)$. In the case in which $p = 4k+1$, $q = 8k+3$ so that q does not divide M_p, since q is not congruent to $1(mod\ 8)$ or q is not congruent to $7(mod\ 8)$, hence the theorem.

Remark 2.2. *the following is a partial list of prime numbers* $p \equiv 3(mod\ 4)$ *where* $q = 2p + 1$ *is also prime:* $p = 11, 23, 83, 131, 179, 239, 251$.*In each instance,*$M_p$ *is composite.*

Exploring the matter a little further, the next tackle two results of Fermat that restricted the divisors of M_p

Theorem 2.3. *If* p *is an odd prime, then any prime divisors of* M_p *is of the form* $2k_p + 1$

proof

Let q be any prime divisors of M_p, so that $2^p \equiv 1(mod\ q)$. If 2 has order k modulo q. (ie if k is the smallest positive integer that satisfies $2^k \equiv 1(mod\ q)$),
then theorem " Let the integer a have order k modulo n. Then $a^k \equiv 1(mod\ n)$ if and only if $k|n$; in particular $k|\phi(n)$ .....$(*)$
Tells us that $k|p$. The case $k = 1$ cannot arise; for this would imply that $q|1$ (since if $k = 1$, $2^k - 1 \equiv 0(mod\ q) \implies q = 1$) an impossible situation. Therefore , because both $k|p$ and $k > 1$, the primality of p force $k = p$

In compliance with Fermat's theorem, we have $2^{q-1} \equiv 1(mod\ q)$, and again by theorem $(*)$ $k|(q-1)$ knowing that $k = p$, the net result is $p|(q-1)$. To be defined , let us put $q - 1 = pt$; then $q = pt + 1$. The proof is completed by noting that if t were an odd integer, then q would be even and a contradiction occurs. Hence , we must have $q = 2k_p + 1$. For some choice of k, which gives q the required form.

Theorem 2.4. *If* p *is an odd prime , then any prime divisor* q *of* m_p *is of the form* $q \equiv \pm 1(mod\ 8)$.

proof

Suppose that $q = 2n + 1$ is a prime divisor of m_p.
If $a = 2^{(p+1)/2}$, then

$$\begin{aligned} a^2 - 2 &= (2^{(p+1)/2})^2 - 2 \\ &= 2^{p+1} - 2 \\ &= 2^p \times 2 - 2 \\ &= 2(2^p - 1) \\ &= 2M_p \\ &\equiv 0(mod\ q) \end{aligned}$$

Raising both sides of the congruence $a^2 \equiv 2(mod\ q)$ to the n^{th} power, we get

$$a^{q-1} = a^{2n} \equiv 2^n(mod\ q)$$

Since q is an odd integer , one has $gcd(a, q) = 1$ and so $a^{q-1} \equiv 1(mod\ q)$. In conjunction, the last congruence tell us that

$$\begin{aligned} &2^n \equiv 1(mod\ q) \\ \implies\ &2^n - 1 \equiv 0(mod\ q) \\ \implies\ &q|M_n \end{aligned}$$

the theorem $(***)$ now be brought into play to reach the condition that $q \equiv \pm 1(mod\ 8)$
Therefore we get if p is an odd prime then any prime divisor q of M_p is of the form

$$q \equiv \pm 1(mod\ 8)$$

hence the theorem.

Remark 2.3. *For an illustration of how these theorems can be used, one might look at* M_{17}. *These integers of the form* $34k + 1$ *that are less than* $362 < \sqrt{M_{17}}$ *are* $35, 69, 103, 137, 171, 205, 239, 273, 307, 341$.

Because the smallest (non-trivial) divisors of M_{17} must be prime, we need only consider the primes among the foregoing 10 numbers namely, $103, 137, 239, 307$ the work can be shortened some what by noting that 307 is not congruent to $\pm 1(mod\ 8)$, and therefore we may delete 307 from our list.Now, either M_{17} is prime or one of the three remaining possibilities divide it with a little calculations we can check that M_{17} is divisible by none of $103, 137,$ *and* 239; the result M_{17} is prime.

Theorem 2.5. ***EULER:*** *If* n *is a perfect number, then any* $n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ *where the* $p_i's$ *are distinct odd primes and* $p_1 \equiv\ k_1 \equiv 1(mod\ 4)$.

proof

Let $n = \ n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ be the prime factorisation of n. Because n is perfect.We can write

$$2n = \sigma(n) = \sigma({p_1}^{k_1}) \ \times\sigma({p_2}^{k_2}) \ ..... \times\sigma({p_r}^{k_r})$$
being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$

being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$; in any event, $2n \equiv 2(mod\ 4)$. Thus , $\sigma(n) = 2n$ is divisible by 2, but not by 4. The implication is that one of the $\sigma({p_i}^{k_i})$, say $\sigma({p_i}^{k_i})$, must be an even integer (but not divisible by 4), and all the remaining $\sigma({p_i}^{k_i})$'s are odd integers.

For a given p_i , there are two cases to be considered:
$p_i \equiv 1(mod\ 4)$ and $p_i \equiv 3(mod\ 4)$. If $p_i \equiv 3 \equiv -1(mod\ 4)$, we would have,

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^{k_i}$$
$$\equiv 1 + (-1) + (-1)^2 + ... + (-1)^{k_i} (mod\ 4)$$
$$\equiv \begin{cases} 0(mod\ 4)\ if\ k_i\ is\ odd \\ 1(mod\ 4)\ if\ k_i\ is\ even \end{cases}$$

since $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$, this tells us that $p_1 \not\equiv 3(mod\ 4)$ or, to put it affirmatively, $p_1 \equiv 1(mod\ 4)$. Furthermore, the congruence $\sigma({p_i}^{k_i}) \equiv 0(mod\ 4)$ signifies that 4 divides $\sigma({p_i}^{k_i})$ which is not possible.
The conclusion : if $p_i \equiv 3(mod\ 4)$ where $i = 2, ..., r$ then it's exponent k_i must be an even integer.
Should it happen that $p_i \equiv 1(mod\ 4)$ which is certainly true for i=1,then

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^k$$
$$\equiv 1 + 1^1 + 1^2 + ... + 1^{k_i} (mod\ 4)$$
$$\equiv k_i + 1(mod\ 4)$$

The condition $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$ for as $k_1 \equiv 1(mod\ 4)$.For the other values of i, we know that $\sigma({p_i}^{k_i}) \equiv 1\ or\ 3(mod\ 4)$, and therefore $k_i \equiv 0\ or\ 2(mod\ 4)$; in any case k_i is an even integer. The crucial point is that, regardless of whether $p_i \equiv 1(mod\ 4)$ or $p_i \equiv 3(mod\ 4)$, k_i is always for $i \neq 1$. Our proof is now complete.

Remark 2.4. *In view of the preceding theorem, any odd perfect number n can be expressed as*

$$n = {p_1}^{k_1} {p_2}^{2j_2} .....{p_r}^{2j_r}$$
$$= p_1^{k_1} ({p_2}^{j_2} .....p_r^{j_r})^2$$
$$= {p_1}^{k_1} m^2$$

This leads directly to the following corollary.

corollary 2.5.1. *If n is an odd perfect number, then n is of the form $n = p^k m^2$. Where p is a prime, p does not divides m, and $p \equiv k \equiv 1(mod\ 4)$; in particular, $n = 1(mod\ 4)$*

proof

Only the last assertion is not obvious.Because $p \equiv 1(mod\ 4)$, we have $p^k \equiv 1(mod\ 4)$.Notice that m must be odd; hence $m \equiv 1$ *or* $3(mod\ 4)$, and therefore upon squaring, $m^2 \equiv 1(mod\ 4)$. It follows that

$$n = p^k m^2 \equiv 1 \times 1 \equiv 1(mod\ 4)$$

establishing our corollary.

definition 2.2. *Two numbers such as* 220 *and* 284 *are called amicable, or friendly; because they have the remarkable property that each number is " contained" within the other, in the sense that each number is equal to the sum of all the positive divisors of the other , not counting the number itself.Thus, as regards the divisors* 220

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

and for 284*,*

$$1 + 2 + 4 + 71 + 142 = 220$$

In terms of the σ function, amicable numbers m and n (or an amicable pair) are defined by the equation.

$$\sigma(m) - m = n$$
$$\sigma(n) - n = m$$

or what amounts to the same thing;

$$\sigma(m) = m + n = \sigma(n)$$

Remark 2.5. *Amicable number have been important in magic and astrology, and casting horoscope, making talismans. The Greeks believed that these numbers had a particular influence in establishing friendship between individuals.*

CHAPTER 3

FERMAT NUMBERS

3 Fermat Numbers:

definition 3.1. *A Fermat number is an integer of the form*

$$F_n = 2^{2^n} + 1,\ n \geq 0$$

If F_n is prime, it is said to be a fermat prime.

Remark 3.1. $F_0 = 3,\ F_1 = 5,\ F_2 = 17\ F_3 = 257,\ F_4 = 65537$ *and* $F_5 = 2^{2^5} + 1 = 4294967297$

Theorem 3.1. *The fermat number F_5 is divisible by* 641

proof

We begin by putting $a = 2^7$ and $b = 5$, so that

$$1 + ab = 1 + (2^7 \times 5) = 641$$

It is easily seen that

$$1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b = 2^4$$

But this implies that;

$$\begin{gathered} F_5 = 2^{2^5} + 1 = 2^{32} + 1 \\ = (2^4 \times a^4) + 1 \\ = (1 + ab - b^4)a^4 + 1 \\ (1 + ab)a^4 + (1 - a^4b^4) \\ = (1 + ab)[a^4 + (1 - ab)(1 + a^2b^2)] \end{gathered}$$

which gives $641|F_n$.

Theorem 3.2. *For fermat numbers F_n and F_m, where $m > n \geq 0$, $gcd(F_m, F_n) = 1$.*

proof

Put $d = gcd(F_m, F_n) = 1$. Because Fermat numbers are odd integers, d must be odd. If we set $x = 2^{2^n}$ *and* $k = 2^{m-n}$ *then*

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

$$= \frac{x^k - 1}{x + 1}$$

$$= x^{k-1} - x^{k-2} + ... - 1$$

hence $F_n|(F_m - 2)$.From $d|F_n$, it follows that $d|(F_m - 2)$.Now use the fact that $d|F_m$ to obtain $d|2$. But d is an odd integer, and so $d = 1$, establishing the result is claimed.

Remark 3.2. *We know that each of the Fermat numbers $F_0, F_1, F_2, ...F_N$ is divisible by a prime that does not divide any of the other F_k. Thus, there*

are at least $n+1$ distinct primes not exceeding F_n.Because there are infinitely many Fermat numbers, the number of primes is also infinite.
In 1877, the Jesuit priest T.Pepin devised the practical test(Pepin's test for determining the primality of F_n that is embodied in the following theorem.)

Theorem 3.3. *Pepin's test; For $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if*

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

proof

First let us assume that,

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Upon squaring both sides we get

$$3^{F_n-1} \equiv 1(mod\ F_n)$$

The same congruence holds for any prime p that divides F_n

$$3^{F_n-1} \equiv 1(mod\ p)$$

Now let k be the order of 3 modulo p. We know that $k|(F_n - 1)$ or in other words, that $k|2^{2^n}$ therefore k must be a power of 2.
It is not possible that $k = 2^r$ for any $r \leq 2^n - 1$
For if this were so, repeated squaring of the congruence $3^k \equiv 1(mod\ p)$ would yield

$$3^{2^{2^n-1}} \equiv 1(mod\ p)$$

or, what is the same thing,

$$3^{F_n-1} \equiv 1(mod\ p)$$

We would then arrive at $1 \equiv -1(mod\ p)$, resulting in $p = 2$, which is a contradiction. Thus the only possibility open to us is that

$$k = 2^{2^n} = F_n - 1$$

Fermat's theorem tells us that $k \leq p - 1$, which means, in turn, that $F_n = k + 1 \leq p$. Because $p|F_n$, we also have $p \leq F_n$.Together, these inequalities mean that $F_n = p$, so that F_n is prime. On the other hand, suppose that $F_n,\ n \geq 1$ is prime.
The quadratic Reciprocity Law gives

$$(3|F_n) = (F_n|3) = (2|3) = -1$$

When we use the fact that

$$F_n \equiv (-1)^{2^n} + 1 = 2(mod\ 3)$$

Applying Euler's criterion, we end up with

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Example 3.1. *Show that using Pepin's test $F_3 = 257$ is prime.*

proof

$$3^{\frac{p_3-1}{2}} = 3^{128} = 3^3(3^5)^{25}$$
$$\equiv 27(-14)^{25}$$
$$\equiv 27 \times 14^{24}(-14)$$
$$\equiv 27(17)(-14)$$
$$\equiv 27 \times 19 \equiv 513 \equiv -1(mod\ 257)$$

So that F_3 is prime.

Theorem 3.4. *Any prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, is of the form*

$$p = k \times 2^{(n+2)} + 1$$

proof

For a prime divisor p of F_n,

$$2^{2^n} \equiv -1(mod\ p)$$

Which is to say, upon squaring that

$$2^{2^{n+1}} \equiv 1(mod\ p)$$

If h is the order of 2 modulo p, this congruence tells us that $h|2^{n+1}$.We cannot have $h = 2^r$ where $1 \leq r \leq n$, for this would lead to $2^{2^n} \equiv 1(mod\ p)$ and in turn, to the contradiction that $p = 2$.This let us conclude that $h = 2^{n+1}$. Because the order of 2 modulo p divides $\phi(p) = p - 1$, we may further conclude that $2^{n+1}|p - 1$.The point is that for $n \geq 2, p \equiv 1(mod\ 8)$, and therefore, by theorem, if p is an odd number then $2|p$, the Legendre symbol $(2|P) = 1$.

Using Euler's criterion, we immediately pass to

$$2^{\frac{(p-1)}{2}} \equiv (2|p) = 1(mod\ p)$$

An appeal to theorem " let the integer a have order k modulo n, then $a^h \equiv 1(mod\ n)$ if and only if $k|n$, in particular, $k|\phi(n)$, " finishes the proof. It asserts that $h|\frac{(p-1)}{2}$, or equivalently, $2^{(n+1)}|\frac{(p-1)}{2}$.This forces $2^{n+2}|(p-1)$ and we obtain $p = k \times 2^{(n+2)} + 1$ for some integer k.

CONCLUSION

Number theory is the study of the integers and related objects.Topics studied by number theorists include the problem of determining the distribution of prime numbers within the integers and the structure and number of solutions of polynomial equations with integer co-effecients.
A branch of pure mathematics that deals with the study of natural numbers and the study deals with the set of positive whole numbers that are usually called the set of natural numbers and is partly experimental and partly theoretical.

Number theory is necessary for the study of numbers because it shows what numbers can do. It helps in providing valuable training in logical thinking and studying the relationship between different kinds of numbers. It is applied in cryptography, device authentication, websites for e-commerce, coding, and security systems.

BIBLIOGRAPHY

1. DAVID M. BURTON, ELEMENTARY NUMBER THEORY, 7th edition

2. JOSEPH H. SILVERMAN, A FRIENDLY INTRODUCTION TO NUMBER THEORY, 4th edition, Pearson

3. https://www.cuemath.com/numbers/number-theory/

NUMBERS OF SPECIAL FORMS

Project report submitted to
KANNUR UNIVERSITY
for the award of the degree
of
Bachelor of science
by
ASHNA SHAJAN
DB20CMSR12
Under the guidance of
Ms.REMYA RAJ

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu
March 2023

CERTIFICATE

It is to certify that this project report **'NUMBERS OF SPECIAL FORMS'** is the bonafide project of **Ashna Shajan** and that this project has been carried out by supervision.

Mrs.Riya Baby
Head Of The Department

Ms.Remya Raj
Supervisor

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu

DECLARATION

I Ashna Shajan hereby declare that the project **'NUMBERS OF SPECIAL FORMS'** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms.Remya Raj, Department Of Mathematics,Don Bosco Arts And Science College,Angadikkadavu and has not submitted by me elsewhere for the award of my degree,diploma,title or recognition before.

ASHNA SHAJAN
DB20CMSR12

Department Of Mathematics
Don Bosco Arts And Science College
AngadikkadavU

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude to everyone involved in this initiative.Many people have aided me in finishing this job successfully.

I'd like to express my heartfelt thanks to my supervisor Ms.Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for providing invaluable guidance, suggestions and for helping me complete my project.

I also express my sincere gratitude towards all the faculty members of the Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu.

I owe and respectfully offer my thanks to the principal and staff of Don Bosco Arts And Science College, Angadikkadavu for their constant moral support and mellifluous affection provided to me.

And i will be greatfull to all who directly or indirectly helped me to complete this project.Their guidance and support was very helpful in bringing this work to a conclusion.

CONTENTS

INTRODUCTION

Number theory(or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions.German mathematician Carl Friedrich Gauss (1777-1855) said, "Mathematics is the queen of the sciences - and number theory is the queen of mathematics.
In accordance with the research methods and objectives, we briefly divide number theory into four classes; Elementary number theory, Analytic number theory, Algebraic number theory and Geometric number theory. Here we only deals with the Elementary number theory.

Elementary number theory is also known as classical number theory.It is the basic theory for studying divisibility,congruences , diophantine equations etc, mainly by means of the four fundamental rules. It requires no long preliminary training, the content is tangible and more than any other path of mathematics, the methods of inquiry adhere to the scientific approach.

Applications of number theory:
Here are some of the most important applications of number theory. Number theory is used to find some of the important divisibility tests, whether a given integer m divides the integer n. Number theory have countless applications in mathematics as well in practical applications such as :
1) Security system like in banking securities.
2) E-commerce websites.
3) Coding theory.
4) Bar codes.
5) Making of modular designs.
6) Memory management system.
7) Authentication system.

It is also defined in hash functions, linear congruences, pseudo random numbers and fast arithmetic operations.

PRELIMINARIES

DIVISOR:

A divisor is a number that divides another number either completely or with a remainder.

GEOMETRIC PROGRESSION:

A geometric progression or a geometric sequence is the sequence , in which each term is varied by another by a common ratio. The next term of the sequence is produced when we multiply a constant(which is non-zero) to the preceding term. It is represented by:

$a, ar, ar2, ar3, ar4$ and so on.

where a is the first term and r is the common ratio.

GCD:

The greatest common divisor of two or more numbers is the greatest common factor number that divides them, exactly.
It is also called called the highest common factor (HCF).

Suppose $4, 8$ and 16 are three numbers .Then the factors of $4, 8$ and 16 are:

$4 - 1, 2, 4$
$8 - 1, 2, 4, 8$
$16 - 1, 2, 4, 8, 16$

Therefore we can conclude that 4 is the highest common factor among all three numbers.

COMPOSITE:

In mathematics composite numbers are that have more than two factors.
example:
factors of 6 are 1,2,3 and 6, which are four factors in total

PRIME:

Prime numbers are the positive integers having only two factors, 1 and the integer itself.
For example:
factors of 7 are only 1 and 7, totally two.

HYPOTHESIS:

Hypothesis is a proposition that is consistent with known data , but has been neither verified nor shown to be false.

RELATIVELY PRIME:

Two integers a and b, not both of which are zero, are said to be relatively prime whenever $gcd(a, b) = 1$.

example:
$4 - 1, 2, 4$
and $15 - 1, 3, 5$
Here $gcd(4, 15) = 1$.

Hence they are relatively prime.

CONGRUENT MODULO n:

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b(mod\ n)$ if n divides the difference $a - b$; that is provided that $a - b = kn$ for some integer k.

AMICABLE NUMBER:

Two numbers are amicable if each is equal to the sum of the proper divisors of the other (for example, 220 and 284).

PRIMALITY:

Primality:the property of being a prime number.

EULER'S CRITERION

Euler's criterion is a formula for determining whether an integer is a quadratic residue modulo a prime. Precisely,
Let p be an odd prime and a be an integer coprime to p. Then

$$a^{(p-1)/2} \equiv \begin{cases} 1\ (mod\ p)\ if\ there\ is\ an\ integer\ x\ such\ that\ a \equiv x^2\ (mod\ p), \\ -1\ (mod\ p)\ if\ there\ is\ no\ such\ integer. \end{cases}$$

Euler's criterion can be concisely reformulated using the Legendre symbol: $(a/p) = a^{(p-1)/2}\ \ (mod\ \ p)$

FERMAT'S THEOREM:

Let p be a prime and suppose that p doesn't divide a. Then $a^{p-1} \equiv 1 (mod\ p)$.

PURE MATHEMATICS:

Pure mathematics is the study of mathematical concepts independently of any application outside mathematics.

CHAPTER 1

PERFECT NUMBERS

1 Perfect Numbers

The history of the theory of numbers abounds with famous conjectues and open questions. this topic focuses on some of the intriguing congectures associated with perfect numbers.
A few of these have been satisfactorily answered, but most remain unresolved.

Example 1.1. *The pythagoreans considered it rather remarkable that the number 6 is equal to the sum of its positive* ***divisors,other than itself.***

6=1+2+3

The next number after 6 having this feature is 28; for the positive divisors of 28 are found to be 1,2,4,7,14 and 28.

28=1+2+4+7+14

And the pythagoreans called such numbers **'perfect'**.

definition 1.1. *A positive integer n is said to be perfect if n is equal to the sum of all its positive divisors,excluding n itself.*

The sum of the positive divisors of an integer n,each of them less than n, is given by $\sigma(n) - n = n$. Thus, the condition "n is perfect" amounts to asking that $\sigma(n) - n = n$ or equivalently that $\sigma(n) = 2n$

EXAMPLE

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 * 6$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 * 28$$

it was partially solved by Euclid when he proved that if the sum

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = p$$

is a prime number, then $2^{k-1}p$ is a perfect number(of necessity even). For instance, 1+2+4=7 is a prime. Hence 4*7=28 is a perfect number. Euclid's arguments makes use of the formula for the sum of a geometric progression

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = 2^{k-1}.$$

in this notation, the result reads as follows:

If 2^{k-1} is prime $(k > 1)$, then n = $2^{k-1}(2^k - 1)$ is a perfect number.

Theorem 1.1. *If $2^k - 1$ is prime $(k > 1)$, then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.*

proof

Let $2^k - 1 = p$, a prime, and consider the integer $n = 2^{k-1}p$. In as much as $gcd(2^{k-1}, p) = 1$, the multiplicativity of σ entails that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}p) \\ &= \sigma(2^{k-1})\sigma(p) \\ &= (2^{k-1})(p + 1)\end{aligned}$$

$$(2^k - 1)(2^k) = 2n$$

making n a perfect number. Now conversely assume that n is an even perfect number. we may write n as $n = 2^{k-1}m$, where m is an odd integer and $k \geq 2$. It follows from $gcd(2^{k-1}, m) = 1$ that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}m) \\ &= \sigma(2^{k-1})\sigma(m) \\ &= (2^{k-1})\sigma(m)\end{aligned}$$

whereas the requirement for a number to be perfect gives

$$\sigma(n) = 2n = 2^k m$$

Together these relations yield

$$2^k m = (2^k - 1)\sigma(m) \text{ .....(1)}$$

$\implies (2^{k-1})|2^k m$. But $2^k - 1 and 2^k$ are relatively prime, whence $(2^k - 1)|m$; hence $m = (2^k - 1)M$. Now, substituting this value of m into the equation (1) and cancelling $2^k - 1$ is that $\sigma(m) = 2^k M$. Because m and M are both divisors of m ($with M < m$), we have

$$2^k M = \sigma(m) \geq m + M = 2^k M$$

leading to $\sigma(m) = m + M$. The implication of this equality is that m has only two positive divisors to it , M and m itself.

It must be that m is prime and M=1 ; in other words

$$\begin{aligned}m &= (2^{k-1}M) \\ &= 2^k - 1\end{aligned}$$

Is a prime number, and hence the proof.

Remark 1.1. *Here our problem of finding even perfect number is reduced to the search for primes of the form* $2^k - 1$*, a closer look at these integers might be truthful.One thing that can be provided is that* 2^{k-1} *is a prime number, then the exponent* k *must itself be prime. More generally we have the following lemma.*

Lemma 1.1. *If* $a^k - 1$*is prime* $(a > 0, k \geq 2)$ *then a=2 and k is also prime.*

proof

$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + ... + a + 1)$
where in the present setting,

$$a^{k-1} + a^{k-2} + ... + a + 1 \geq a + 1 > 1$$

because by the hypothesis a^{k-1} is prime, the other factor must be 1; that is, a-1 = 1 so that a = 2.
If k were composite, then we could write $k = rs$ with $1 < r$ *and* $1 < s$. Thus

$$\begin{aligned} a^k - 1 &= (a^r)^s - 1 \\ &= (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + ... + a^r + 1) \end{aligned}$$

and each factor on the right is plainly greater than 1. But this violates the primality of $a^k - 1$, so that by contradiction k must be prime.

Remark 1.2. *For* $p = 2, 3, 5, 7$ *the values* $3, 7, 31, 127$ *of* $2^p - 1$ *are primes.*

so that

$$\begin{aligned} 2(2^2 - 1) &= 6 \\ 2^2(2^3 - 1) &= 28 \\ 2^4(2^5 - 1) &= 496 \\ 2^6(2^7 - 1) &= 8128 \end{aligned}$$

are all perfect numbers.Many early writers erroneously believed that $2^p - 1$ is prime for every choice of prime number p.
But we have,

$$2^{11} - 1 = 2047 = (23)(89) \text{ , not prime.}$$

But when $p = 13,\ 2^p - 1$ is prime and $2^{12}(2^{13} - 1) = 33550336$ be the fifth perfect number.
Therefore, we can say that $2^p - 1$ is prime and it is possible only when p is prime.

Theorem 1.2. *An even perfect number n ends in the digit 6 or 8 equivalently either*

$n \equiv 6(mod\ 10)$ *or* $n \equiv 8(mod\ 10)$

proof

Being an even perfect number n may be represented as $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime. According to the last lemma, the exponent k must also be prime. If $k = 2$, then $n = 6$, and the asserted result holds. We may therefore confine our assumption to case $k > 2$.
The proof falls into two parts, according as k takes the form 4m+1 or 4m+3.
If k is of the form 4m+1 then

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) \\ &= 2^{8k+1} - 2^{4m} \\ &= (2 * 16^{2m}) - 16^m \end{aligned}$$

$16^1 \equiv 6(mod\ 10)$ also
$16^t \equiv 6(mod\ 10)$ for any positive integer 't'
Therefore we get, $n = (2 * 6) - 6 \equiv 6(mod\ 10)$
Now in the case in which k= 4m+3

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 2^{8m+5} - 2^{4m+2} \\ &= (2 * 16^{2m+1}) - (4 * 16^m) \end{aligned}$$

Falling back on the fact that $16^t \equiv 6(mod\ 10)$, we see that

$$\begin{aligned} n \equiv (2 * 6) - (4 * 6) \equiv -12 \equiv 8(mod\ 10) \\ ie,\ \ n \equiv 8(mod\ 10) \end{aligned}$$

consequently, every even perfect number has a last digit equal to 6 or 8

Remark 1.3. *An even perfect number $n = 2^{k-1} * (2^k - 1)$ always ends in the digit 6 or 28. Because an integer is congruent modulo 100 to it's last two digits, it suffices to prove that, if k is of the form $4m+3$, then $n \equiv 28(mod\ 100)$.*

To see this, note that

$$\begin{aligned} 2^{k-1} &= 2^{4m+2} \\ &= (16^m)(4) \\ &\equiv (6)(4) \\ &\equiv 4(mod\ 10) \end{aligned}$$

Moreover, for $k > 2$ we have $4|2^{k-1}$, and therefore the number formed by the last two digits of 2^{k-1} is divisible by 4, and 4 divides the last two digits modulo 100, the various possibilities are

$$2^{k-1} \equiv 4, 24, 44, 64 or 84$$

But this implies that

$$2^k - 1 = 2 * 2^{k-1} \equiv 7, 47, 87, 27 \ or \ 67 (mod \ 100)$$

hence

$$n = 2^{k-1}(2^k - 1)$$
$$\equiv 4 * 7, 24 * 47, 44 * 87, 64 * 24 \ or \ 84 * 67 (mod \ 100)$$

CHAPTER 2
MERSENNE PRIME

2 Mersenne Prime

It has became traditional to call numbers of the form $M_n = 2^n - 1, n \geq 1$ Mersenne numbers after father Marin Mersenne who made an incorrect but provocative assertion concerning their primality.

definition 2.1. *Mersenne numbers that happens to be prime are said to be Mersenne primes.*

Remark 2.1. *M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and composite for all other primes $p < 257$*

Theorem 2.1. *If p and $q = 2p + 1$ are primes, then their $q|M_p$ or $q|M_p + 2$.*

proof

With reference to Fermat's theorem, we know that

$$2^{q-1} - 1 \equiv 0(modq)$$

and factorising the left hand side,that

$$(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) = (2^p - 1)(2^p + 1) \equiv 0(mod\ q)$$

$$ie,\ (2^p-1)(2^p+1) \equiv 0(mod\ q)$$
$$\implies (2^p-1)(2^p-1+2) \equiv 0(mod\ q)$$
$$\implies M_p(M_p+2) \equiv 0(mod\ q)$$

By using the theorem, "if p is a prime and $p|ab$, then $p|a$ or $p|b$ ", we cannot have both $q|M_p$ and $q|M_p+2, for\ then\ q|2$, which is impossible therefore either $q|M_p$ *or* $q|M_p+2$.

Example 2.1. *A simple application should suffice to illustrate the above theorem if* $p=23$*, then* $q=2p+1=47$ *is also a prime, so that we may consider the case of* M_{23}
The questions reduces to one of whether $47|M_{23}$ *or to put it differently, whether* $2^{23} \equiv 1(mod\ 47)$
now we have

$$2^{23} \equiv 2^3(2^5)^4 \equiv 2^3(-15)^4(mod\ 47)$$
$$(-15)^4 \equiv (225)^2 \equiv (-10)^2 \equiv 6(mod\ 47)$$

putting these two congruences together, it is seen that

$$2^{23} \equiv 2^3 * 6 \equiv 48 \equiv 1(mod\ 47)$$

hence M_{23} *is composite.*

Theorem 2.2. *If* $q=2n+1$ *is prime, then*

$$a)\ q|M_n\ ,\ provided\ that\ q \equiv 1(mod\ 8)\ or\ q \equiv 7(mod\ 8)$$
$$b)\ q|M_n+2,\ provided\ that\ q \equiv 3(mod\ 8)\ or\ q \equiv 5(mod\ 8)$$

proof

To say that $q|M_n$ is equivalent to asserting that

$$2^{(q-1)/2} = 2^n \equiv 1(mod\ q)\ .....(***)$$
$$2^n - 1 \equiv 0(mod\ q)$$

In terms of the legendre symbol, the condition (1) becomes the requirement that $(2/q) = 1$ but according to the theorem, if p is an odd prime then,

$$(2/q) = \begin{cases} 1,\ if\ p \equiv 1(mod\ 8)\ or\ p \equiv 7(mod\ 8) \\ (-1),\ if\ p \equiv 3(mod\ 8)\ or\ p \equiv 5(mod\ 8) \end{cases}$$

we get $(2/q) = 1$ when we have $q \equiv 1(mod\ 8)$ or $q \equiv 7(mod\ 8)$
the proof of (b) proceeds along similar lines.
we get $(q|m_n + 2)$ provided that $q \equiv 3(mod\ 8)$ or $q \equiv 5(mod\ 8)$

corollary 2.2.1. *If p and $q = 2p+1$ are both odd primes, with $p = 3(mod\ 4)$, then $q|M_p$*

proof

An odd prime p is either of the form $4k+1$ or $4k+2$. If $p = 4k+3$, then

$$q = 2(4k+3) + 1$$
$$= 8k + 7$$

and the above theorem yield $q|M_p$. since by the condition $q|M_n$ provided that $q \equiv 1(mod\ 8)$. In the case in which $p = 4k+1$, $q = 8k+3$ so that q does not divide M_p, since q is not congruent to $1(mod\ 8)$ or q is not congruent to $7(mod\ 8)$, hence the theorem.

Remark 2.2. *the following is a partial list of prime numbers* $p \equiv 3(mod\ 4)$ *where* $q = 2p + 1$ *is also prime:* $p = 11, 23, 83, 131, 179, 239, 251$.*In each instance,*$M_p$ *is composite.*

Exploring the matter a little further, the next tackle two results of Fermat that restricted the divisors of M_p

Theorem 2.3. *If* p *is an odd prime, then any prime divisors of* M_p *is of the form* $2k_p + 1$

proof

Let q be any prime divisors of M_p, so that $2^p \equiv 1(mod\ q)$. If 2 has order k modulo q. (ie if k is the smallest positive integer that satisfies $2^k \equiv 1(mod\ q)$),
then theorem " Let the integer a have order k modulo n. Then $a^k \equiv 1(mod\ n)$ if and only if $k|n$; in particular $k|\phi(n)$ .....$(*)$
Tells us that $k|p$. The case $k = 1$ cannot arise; for this would imply that $q|1$ (since if $k = 1$, $2^k - 1 \equiv 0(mod\ q) \implies q = 1$) an impossible situation. Therefore , because both $k|p$ and $k > 1$, the primality of p force $k = p$

In compliance with Fermat's theorem, we have $2^{q-1} \equiv 1(mod\ q)$, and again by theorem $(*)$ $k|(q-1)$ knowing that $k = p$, the net result is $p|(q-1)$. To be defined , let us put $q - 1 = pt$; then $q = pt + 1$. The proof is completed by noting that if t were an odd integer, then q would be even and a contradiction occurs. Hence , we must have $q = 2k_p + 1$. For some choice of k, which gives q the required form.

Theorem 2.4. *If* p *is an odd prime , then any prime divisor* q *of* m_p *is of the form* $q \equiv \pm 1(mod\ 8)$.

proof

Suppose that $q = 2n + 1$ is a prime divisor of m_p.
If $a = 2^{(p+1)/2}$, then

$$\begin{aligned} a^2 - 2 &= (2^{(p+1)/2})^2 - 2 \\ &= 2^{p+1} - 2 \\ &= 2^p \times 2 - 2 \\ &= 2(2^p - 1) \\ &= 2M_p \\ &\equiv 0(mod\ q) \end{aligned}$$

Raising both sides of the congruence $a^2 \equiv 2(mod\ q)$ to the n^{th} power, we get

$$a^{q-1} = a^{2n} \equiv 2^n(mod\ q)$$

Since q is an odd integer , one has $gcd(a, q) = 1$ and so $a^{q-1} \equiv 1(mod\ q)$. In conjunction, the last congruence tell us that

$$\begin{aligned} &2^n \equiv 1(mod\ q) \\ \implies\ &2^n - 1 \equiv 0(mod\ q) \\ \implies\ &q|M_n \end{aligned}$$

the theorem $(***)$ now be brought into play to reach the condition that $q \equiv \pm 1(mod\ 8)$
Therefore we get if p is an odd prime then any prime divisor q of M_p is of the form

$$q \equiv \pm 1(mod\ 8)$$

hence the theorem.

Remark 2.3. *For an illustration of how these theorems can be used, one might look at* M_{17}. *These integers of the form* $34k + 1$ *that are less than* $362 < \sqrt{M_{17}}$ *are* $35, 69, 103, 137, 171, 205, 239, 273, 307, 341$.

Because the smallest (non-trivial) divisors of M_{17} must be prime, we need only consider the primes among the foregoing 10 numbers namely, $103, 137, 239, 307$ the work can be shortened some what by noting that 307 is not congruent to $\pm 1(mod\ 8)$, and therefore we may delete 307 from our list.Now, either M_{17} is prime or one of the three remaining possibilities divide it with a little calculations we can check that M_{17} is divisible by none of $103, 137,$ *and* 239; the result M_{17} is prime.

Theorem 2.5. ***EULER:*** *If* n *is a perfect number, then any* $n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ *where the* $p_i's$ *are distinct odd primes and* $p_1 \equiv\ k_1 \equiv 1(mod\ 4)$.

proof

Let $n = \ n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ be the prime factorisation of n. Because n is perfect.We can write

$$2n = \sigma(n) = \sigma({p_1}^{k_1}) \ \times\sigma({p_2}^{k_2}) \ ..... \times\sigma({p_r}^{k_r})$$
being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$

being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$; in any event, $2n \equiv 2(mod\ 4)$. Thus , $\sigma(n) = 2n$ is divisible by 2, but not by 4. The implication is that one of the $\sigma({p_i}^{k_i})$, say $\sigma({p_i}^{k_i})$, must be an even integer (but not divisible by 4), and all the remaining $\sigma({p_i}^{k_i})$'s are odd integers.

For a given p_i , there are two cases to be considered:
$p_i \equiv 1(mod\ 4)$ and $p_i \equiv 3(mod\ 4)$. If $p_i \equiv 3 \equiv -1(mod\ 4)$, we would have,

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^{k_i}$$
$$\equiv 1 + (-1) + (-1)^2 + ... + (-1)^{k_i} (mod\ 4)$$
$$\equiv \begin{cases} 0(mod\ 4)\ if\ k_i\ is\ odd \\ 1(mod\ 4)\ if\ k_i\ is\ even \end{cases}$$

since $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$, this tells us that $p_1 \not\equiv 3(mod\ 4)$ or, to put it affirmatively, $p_1 \equiv 1(mod\ 4)$. Furthermore, the congruence $\sigma({p_i}^{k_i}) \equiv 0(mod\ 4)$ signifies that 4 divides $\sigma({p_i}^{k_i})$ which is not possible.
The conclusion : if $p_i \equiv 3(mod\ 4)$ where $i = 2, ..., r$ then it's exponent k_i must be an even integer.
Should it happen that $p_i \equiv 1(mod\ 4)$ which is certainly true for i=1,then

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^k$$
$$\equiv 1 + 1^1 + 1^2 + ... + 1^{k_i} (mod\ 4)$$
$$\equiv k_i + 1(mod\ 4)$$

The condition $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$ for as $k_1 \equiv 1(mod\ 4)$.For the other values of i, we know that $\sigma({p_i}^{k_i}) \equiv 1\ or\ 3(mod\ 4)$, and therefore $k_i \equiv 0\ or\ 2(mod\ 4)$; in any case k_i is an even integer. The crucial point is that, regardless of whether $p_i \equiv 1(mod\ 4)$ or $p_i \equiv 3(mod\ 4)$, k_i is always for $i \neq 1$. Our proof is now complete.

Remark 2.4. *In view of the preceding theorem, any odd perfect number n can be expressed as*

$$n = {p_1}^{k_1} {p_2}^{2j_2} .....{p_r}^{2j_r}$$
$$= p_1^{k_1} ({p_2}^{j_2} .....p_r^{j_r})^2$$
$$= {p_1}^{k_1} m^2$$

This leads directly to the following corollary.

corollary 2.5.1. *If n is an odd perfect number, then n is of the form $n = p^k m^2$. Where p is a prime, p does not divides m, and $p \equiv k \equiv 1(mod\ 4)$; in particular, $n = 1(mod\ 4)$*

proof

Only the last assertion is not obvious.Because $p \equiv 1(mod\ 4)$, we have $p^k \equiv 1(mod\ 4)$.Notice that m must be odd; hence $m \equiv 1$ *or* $3(mod\ 4)$, and therefore upon squaring, $m^2 \equiv 1(mod\ 4)$. It follows that

$$n = p^k m^2 \equiv 1 \times 1 \equiv 1(mod\ 4)$$

establishing our corollary.

definition 2.2. *Two numbers such as* 220 *and* 284 *are called amicable, or friendly; because they have the remarkable property that each number is " contained" within the other, in the sense that each number is equal to the sum of all the positive divisors of the other , not counting the number itself.Thus, as regards the divisors* 220

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

and for 284*,*

$$1 + 2 + 4 + 71 + 142 = 220$$

In terms of the σ function, amicable numbers m and n (or an amicable pair) are defined by the equation.

$$\sigma(m) - m = n$$
$$\sigma(n) - n = m$$

or what amounts to the same thing;

$$\sigma(m) = m + n = \sigma(n)$$

Remark 2.5. *Amicable number have been important in magic and astrology, and casting horoscope, making talismans. The Greeks believed that these numbers had a particular influence in establishing friendship between individuals.*

CHAPTER 3

FERMAT NUMBERS

3 Fermat Numbers:

definition 3.1. *A Fermat number is an integer of the form*

$$F_n = 2^{2^n} + 1,\ n \geq 0$$

If F_n is prime, it is said to be a fermat prime.

Remark 3.1. $F_0 = 3,\ F_1 = 5,\ F_2 = 17\ F_3 = 257,\ F_4 = 65537$ *and* $F_5 = 2^{2^5} + 1 = 4294967297$

Theorem 3.1. *The fermat number F_5 is divisible by* 641

proof

We begin by putting $a = 2^7$ and $b = 5$, so that

$$1 + ab = 1 + (2^7 \times 5) = 641$$

It is easily seen that

$$1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b = 2^4$$

But this implies that;

$$\begin{gathered} F_5 = 2^{2^5} + 1 = 2^{32} + 1 \\ = (2^4 \times a^4) + 1 \\ = (1 + ab - b^4)a^4 + 1 \\ (1 + ab)a^4 + (1 - a^4b^4) \\ = (1 + ab)[a^4 + (1 - ab)(1 + a^2b^2)] \end{gathered}$$

which gives $641|F_n$.

Theorem 3.2. *For fermat numbers F_n and F_m, where $m > n \geq 0$, $gcd(F_m, F_n) = 1$.*

proof

Put $d = gcd(F_m, F_n) = 1$. Because Fermat numbers are odd integers, d must be odd. If we set $x = 2^{2^n}$ *and* $k = 2^{m-n}$ *then*

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

$$= \frac{x^k - 1}{x + 1}$$

$$= x^{k-1} - x^{k-2} + ... - 1$$

hence $F_n|(F_m - 2)$.From $d|F_n$, it follows that $d|(F_m - 2)$.Now use the fact that $d|F_m$ to obtain $d|2$. But d is an odd integer, and so $d = 1$, establishing the result is claimed.

Remark 3.2. *We know that each of the Fermat numbers $F_0, F_1, F_2, ...F_N$ is divisible by a prime that does not divide any of the other F_k. Thus, there*

are at least $n+1$ distinct primes not exceeding F_n.Because there are infinitely many Fermat numbers, the number of primes is also infinite.
In 1877, the Jesuit priest T.Pepin devised the practical test(Pepin's test for determining the primality of F_n that is embodied in the following theorem.)

Theorem 3.3. *Pepin's test; For $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if*

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

proof

First let us assume that,

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Upon squaring both sides we get

$$3^{F_n-1} \equiv 1(mod\ F_n)$$

The same congruence holds for any prime p that divides F_n

$$3^{F_n-1} \equiv 1(mod\ p)$$

Now let k be the order of 3 modulo p. We know that $k|(F_n - 1)$ or in other words, that $k|2^{2^n}$ therefore k must be a power of 2.
It is not possible that $k = 2^r$ for any $r \leq 2^n - 1$
For if this were so, repeated squaring of the congruence $3^k \equiv 1(mod\ p)$ would yield

$$3^{2^{2^n-1}} \equiv 1(mod\ p)$$

or, what is the same thing,

$$3^{F_n-1} \equiv 1(mod\ p)$$

We would then arrive at $1 \equiv -1(mod\ p)$, resulting in $p = 2$, which is a contradiction. Thus the only possibility open to us is that

$$k = 2^{2^n} = F_n - 1$$

Fermat's theorem tells us that $k \leq p - 1$, which means, in turn, that $F_n = k + 1 \leq p$. Because $p|F_n$, we also have $p \leq F_n$.Together, these inequalities mean that $F_n = p$, so that F_n is prime. On the other hand, suppose that $F_n,\ n \geq 1$ is prime.
The quadratic Reciprocity Law gives

$$(3|F_n) = (F_n|3) = (2|3) = -1$$

When we use the fact that

$$F_n \equiv (-1)^{2^n} + 1 = 2(mod\ 3)$$

Applying Euler's criterion, we end up with

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Example 3.1. *Show that using Pepin's test $F_3 = 257$ is prime.*

proof

$$3^{\frac{p_3-1}{2}} = 3^{128} = 3^3(3^5)^{25}$$
$$\equiv 27(-14)^{25}$$
$$\equiv 27 \times 14^{24}(-14)$$
$$\equiv 27(17)(-14)$$
$$\equiv 27 \times 19 \equiv 513 \equiv -1(mod\ 257)$$

So that F_3 is prime.

Theorem 3.4. *Any prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, is of the form*

$$p = k \times 2^{(n+2)} + 1$$

proof

For a prime divisor p of F_n,

$$2^{2^n} \equiv -1(mod\ p)$$

Which is to say, upon squaring that

$$2^{2^{n+1}} \equiv 1(mod\ p)$$

If h is the order of 2 modulo p, this congruence tells us that $h|2^{n+1}$.We cannot have $h = 2^r$ where $1 \leq r \leq n$, for this would lead to $2^{2^n} \equiv 1(mod\ p)$ and in turn, to the contradiction that $p = 2$.This let us conclude that $h = 2^{n+1}$. Because the order of 2 modulo p divides $\phi(p) = p - 1$, we may further conclude that $2^{n+1}|p - 1$.The point is that for $n \geq 2, p \equiv 1(mod\ 8)$, and therefore, by theorem, if p is an odd number then $2|p$, the Legendre symbol $(2|P) = 1$.

Using Euler's criterion, we immediately pass to

$$2^{\frac{(p-1)}{2}} \equiv (2|p) = 1(mod\ p)$$

An appeal to theorem " let the integer a have order k modulo n, then $a^h \equiv 1(mod\ n)$ if and only if $k|n$, in particular, $k|\phi(n)$, " finishes the proof. It asserts that $h|\frac{(p-1)}{2}$, or equivalently, $2^{(n+1)}|\frac{(p-1)}{2}$.This forces $2^{n+2}|(p-1)$ and we obtain $p = k \times 2^{(n+2)} + 1$ for some integer k.

CONCLUSION

Number theory is the study of the integers and related objects.Topics studied by number theorists include the problem of determining the distribution of prime numbers within the integers and the structure and number of solutions of polynomial equations with integer co-effecients.
A branch of pure mathematics that deals with the study of natural numbers and the study deals with the set of positive whole numbers that are usually called the set of natural numbers and is partly experimental and partly theoretical.

Number theory is necessary for the study of numbers because it shows what numbers can do. It helps in providing valuable training in logical thinking and studying the relationship between different kinds of numbers. It is applied in cryptography, device authentication, websites for e-commerce, coding, and security systems.

BIBLIOGRAPHY

1. DAVID M. BURTON, ELEMENTARY NUMBER THEORY, 7th edition

2. JOSEPH H. SILVERMAN, A FRIENDLY INTRODUCTION TO NUMBER THEORY, 4th edition, Pearson

3. https://www.cuemath.com/numbers/number-theory/

NUMBERS OF SPECIAL FORMS

Project report submitted to
KANNUR UNIVERSITY
for the award of the degree
of
Bachelor of science
by
MUBASHIRA C P
DB20CMSR14
Under the guidance of
Ms.REMYA RAJ

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu
March 2023

CERTIFICATE

It is to certify that this project report **'NUMBERS OF SPECIAL FORMS'** is the bonafide project of **Mubashira C P** and that this project has been carried out by supervision.

Mrs.Riya Baby
Head Of The Department

Ms.Remya Raj
Supervisor

Department Of Mathematics
Don Bosco Arts And Science College
Angadikkadavu

DECLARATION

I Mubashira C P hereby declare that the project **'NUMBERS OF SPECIAL FORMS'** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms.Remya Raj, Department Of Mathematics,Don Bosco Arts And Science College,Angadikkadavu and has not submitted by me elsewhere for the award of my degree,diploma,title or recognition before.

MUBASHIRA C P
DB20CMSR14

Department Of Mathematics
Don Bosco Arts And Science College
AngadikkadavU

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude to everyone involved in this initiative.Many people have aided me in finishing this job successfully.

I'd like to express my heartfelt thanks to my supervisor Ms.Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu, for providing invaluable guidance, suggestions and for helping me complete my project.

I also express my sincere gratitude towards all the faculty members of the Department Of Mathematics, Don Bosco Arts And Science College, Angadikkadavu.

I owe and respectfully offer my thanks to the principal and staff of Don Bosco Arts And Science College, Angadikkadavu for their constant moral support and mellifluous affection provided to me.

And i will be greatfull to all who directly or indirectly helped me to complete this project.Their guidance and support was very helpful in bringing this work to a conclusion.

CONTENTS

INTRODUCTION

Number theory(or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions.German mathematician Carl Friedrich Gauss (1777-1855) said, "Mathematics is the queen of the sciences - and number theory is the queen of mathematics.
In accordance with the research methods and objectives, we briefly divide number theory into four classes; Elementary number theory, Analytic number theory, Algebraic number theory and Geometric number theory. Here we only deals with the Elementary number theory.

Elementary number theory is also known as classical number theory.It is the basic theory for studying divisibility,congruences , diophantine equations etc, mainly by means of the four fundamental rules. It requires no long preliminary training, the content is tangible and more than any other path of mathematics, the methods of inquiry adhere to the scientific approach.

Applications of number theory:
Here are some of the most important applications of number theory. Number theory is used to find some of the important divisibility tests, whether a given integer m divides the integer n. Number theory have countless applications in mathematics as well in practical applications such as :
1) Security system like in banking securities.
2) E-commerce websites.
3) Coding theory.
4) Bar codes.
5) Making of modular designs.
6) Memory management system.
7) Authentication system.

It is also defined in hash functions, linear congruences, pseudo random numbers and fast arithmetic operations.

PRELIMINARIES

DIVISOR:

A divisor is a number that divides another number either completely or with a remainder.

GEOMETRIC PROGRESSION:

A geometric progression or a geometric sequence is the sequence , in which each term is varied by another by a common ratio. The next term of the sequence is produced when we multiply a constant(which is non-zero) to the preceding term. It is represented by:

$a, ar, ar2, ar3, ar4$ and so on.

where a is the first term and r is the common ratio.

GCD:

The greatest common divisor of two or more numbers is the greatest common factor number that divides them, exactly.
It is also called called the highest common factor (HCF).

Suppose $4, 8$ and 16 are three numbers .Then the factors of $4, 8$ and 16 are:

$4 - 1, 2, 4$
$8 - 1, 2, 4, 8$
$16 - 1, 2, 4, 8, 16$

Therefore we can conclude that 4 is the highest common factor among all three numbers.

COMPOSITE:

In mathematics composite numbers are that have more than two factors.
example:
factors of 6 are 1,2,3 and 6, which are four factors in total

PRIME:

Prime numbers are the positive integers having only two factors, 1 and the integer itself.
For example:
factors of 7 are only 1 and 7, totally two.

HYPOTHESIS:

Hypothesis is a proposition that is consistent with known data , but has been neither verified nor shown to be false.

RELATIVELY PRIME:

Two integers a and b, not both of which are zero, are said to be relatively prime whenever $gcd(a, b) = 1$.

example:
$4 - 1, 2, 4$
and $15 - 1, 3, 5$
Here $gcd(4, 15) = 1$.

Hence they are relatively prime.

CONGRUENT MODULO n:

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b(mod\ n)$ if n divides the difference $a - b$; that is provided that $a - b = kn$ for some integer k.

AMICABLE NUMBER:

Two numbers are amicable if each is equal to the sum of the proper divisors of the other (for example, 220 and 284).

PRIMALITY:

Primality:the property of being a prime number.

EULER'S CRITERION

Euler's criterion is a formula for determining whether an integer is a quadratic residue modulo a prime. Precisely,
Let p be an odd prime and a be an integer coprime to p. Then

$$a^{(p-1)/2} \equiv \begin{cases} 1\ (mod\ p)\ if\ there\ is\ an\ integer\ x\ such\ that\ a \equiv x^2\ (mod\ p), \\ -1\ (mod\ p)\ if\ there\ is\ no\ such\ integer. \end{cases}$$

Euler's criterion can be concisely reformulated using the Legendre symbol: $(a/p) = a^{(p-1)/2}\ \ (mod\ \ p)$

FERMAT'S THEOREM:

Let p be a prime and suppose that p doesn't divide a. Then $a^{p-1} \equiv 1 (mod\ p)$.

PURE MATHEMATICS:

Pure mathematics is the study of mathematical concepts independently of any application outside mathematics.

CHAPTER 1

PERFECT NUMBERS

1 Perfect Numbers

The history of the theory of numbers abounds with famous conjectues and open questions. this topic focuses on some of the intriguing congectures associated with perfect numbers.
A few of these have been satisfactorily answered, but most remain unresolved.

Example 1.1. *The pythagoreans considered it rather remarkable that the number 6 is equal to the sum of its positive* ***divisors,other than itself.***

6=1+2+3

The next number after 6 having this feature is 28; for the positive divisors of 28 are found to be 1,2,4,7,14 and 28.

28=1+2+4+7+14

And the pythagoreans called such numbers **'perfect'**.

definition 1.1. *A positive integer n is said to be perfect if n is equal to the sum of all its positive divisors,excluding n itself.*

The sum of the positive divisors of an integer n,each of them less than n, is given by $\sigma(n) - n = n$. Thus, the condition "n is perfect" amounts to asking that $\sigma(n) - n = n$ or equivalently that $\sigma(n) = 2n$

EXAMPLE

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 * 6$$
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 * 28$$

it was partially solved by Euclid when he proved that if the sum

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = p$$

is a prime number, then $2^{k-1}p$ is a perfect number(of necessity even). For instance, 1+2+4=7 is a prime. Hence 4*7=28 is a perfect number. Euclid's arguments makes use of the formula for the sum of a geometric progression

$$1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} = 2^{k-1}.$$

in this notation, the result reads as follows:

If 2^{k-1} is prime $(k > 1)$, then n = $2^{k-1}(2^k - 1)$ is a perfect number.

Theorem 1.1. *If $2^k - 1$ is prime $(k > 1)$, then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.*

proof

Let $2^k - 1 = p$, a prime, and consider the integer $n = 2^{k-1}p$. In as much as $gcd(2^{k-1}, p) = 1$, the multiplicativity of σ entails that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}p) \\ &= \sigma(2^{k-1})\sigma(p) \\ &= (2^{k-1})(p + 1)\end{aligned}$$

$$(2^k - 1)(2^k) = 2n$$

making n a perfect number. Now conversely assume that n is an even perfect number. we may write n as $n = 2^{k-1}m$, where m is an odd integer and $k \geq 2$. It follows from $gcd(2^{k-1}, m) = 1$ that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}m) \\ &= \sigma(2^{k-1})\sigma(m) \\ &= (2^{k-1})\sigma(m)\end{aligned}$$

whereas the requirement for a number to be perfect gives

$$\sigma(n) = 2n = 2^k m$$

Together these relations yield

$$2^k m = (2^k - 1)\sigma(m) \text{ .....(1)}$$

$\implies (2^{k-1})|2^k m$. But $2^k - 1 and 2^k$ are relatively prime, whence $(2^k - 1)|m$; hence $m = (2^k - 1)M$. Now, substituting this value of m into the equation (1) and cancelling $2^k - 1$ is that $\sigma(m) = 2^k M$. Because m and M are both divisors of m ($with M < m$), we have

$$2^k M = \sigma(m) \geq m + M = 2^k M$$

leading to $\sigma(m) = m + M$. The implication of this equality is that m has only two positive divisors to it , M and m itself.

It must be that m is prime and M=1 ; in other words

$$\begin{aligned}m &= (2^{k-1}M) \\ &= 2^k - 1\end{aligned}$$

Is a prime number, and hence the proof.

Remark 1.1. *Here our problem of finding even perfect number is reduced to the search for primes of the form* $2^k - 1$*, a closer look at these integers might be truthful.One thing that can be provided is that* 2^{k-1} *is a prime number, then the exponent* k *must itself be prime. More generally we have the following lemma.*

Lemma 1.1. *If* $a^k - 1$*is prime* $(a > 0, k \geq 2)$ *then a=2 and k is also prime.*

proof

$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + ... + a + 1)$
where in the present setting,

$$a^{k-1} + a^{k-2} + ... + a + 1 \geq a + 1 > 1$$

because by the hypothesis a^{k-1} is prime, the other factor must be 1; that is, a-1 = 1 so that a = 2.
If k were composite, then we could write $k = rs$ with $1 < r$ *and* $1 < s$. Thus

$$\begin{aligned} a^k - 1 &= (a^r)^s - 1 \\ &= (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + ... + a^r + 1) \end{aligned}$$

and each factor on the right is plainly greater than 1. But this violates the primality of $a^k - 1$, so that by contradiction k must be prime.

Remark 1.2. *For* $p = 2, 3, 5, 7$ *the values* $3, 7, 31, 127$ *of* $2^p - 1$ *are primes.*

so that

$$\begin{aligned} 2(2^2 - 1) &= 6 \\ 2^2(2^3 - 1) &= 28 \\ 2^4(2^5 - 1) &= 496 \\ 2^6(2^7 - 1) &= 8128 \end{aligned}$$

are all perfect numbers.Many early writers erroneously believed that $2^p - 1$ is prime for every choice of prime number p.
But we have,

$$2^{11} - 1 = 2047 = (23)(89) \text{ , not prime.}$$

But when $p = 13,\ 2^p - 1$ is prime and $2^{12}(2^{13} - 1) = 33550336$ be the fifth perfect number.
Therefore, we can say that $2^p - 1$ is prime and it is possible only when p is prime.

Theorem 1.2. *An even perfect number n ends in the digit 6 or 8 equivalently either*

$n \equiv 6(mod\ 10)$ *or* $n \equiv 8(mod\ 10)$

proof

Being an even perfect number n may be represented as $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime. According to the last lemma, the exponent k must also be prime. If $k = 2$, then $n = 6$, and the asserted result holds. We may therefore confine our assumption to case $k > 2$.
The proof falls into two parts, according as k takes the form 4m+1 or 4m+3.
If k is of the form 4m+1 then

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) \\ &= 2^{8k+1} - 2^{4m} \\ &= (2 * 16^{2m}) - 16^m \end{aligned}$$

$16^1 \equiv 6(mod\ 10)$ also
$16^t \equiv 6(mod\ 10)$ for any positive integer 't'
Therefore we get, $n = (2 * 6) - 6 \equiv 6(mod\ 10)$
Now in the case in which k= 4m+3

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 2^{8m+5} - 2^{4m+2} \\ &= (2 * 16^{2m+1}) - (4 * 16^m) \end{aligned}$$

Falling back on the fact that $16^t \equiv 6(mod\ 10)$, we see that

$$\begin{aligned} n \equiv (2 * 6) - (4 * 6) \equiv -12 \equiv 8(mod\ 10) \\ ie,\ \ n \equiv 8(mod\ 10) \end{aligned}$$

consequently, every even perfect number has a last digit equal to 6 or 8

Remark 1.3. *An even perfect number $n = 2^{k-1} * (2^k - 1)$ always ends in the digit 6 or 28. Because an integer is congruent modulo 100 to it's last two digits, it suffices to prove that, if k is of the form $4m+3$, then $n \equiv 28(mod\ 100)$.*

To see this, note that

$$\begin{aligned} 2^{k-1} &= 2^{4m+2} \\ &= (16^m)(4) \\ &\equiv (6)(4) \\ &\equiv 4(mod\ 10) \end{aligned}$$

Moreover, for $k > 2$ we have $4|2^{k-1}$, and therefore the number formed by the last two digits of 2^{k-1} is divisible by 4, and 4 divides the last two digits modulo 100, the various possibilities are

$$2^{k-1} \equiv 4, 24, 44, 64 or 84$$

But this implies that

$$2^k - 1 = 2 * 2^{k-1} \equiv 7, 47, 87, 27 \ or \ 67 (mod \ 100)$$

hence

$$n = 2^{k-1}(2^k - 1)$$
$$\equiv 4 * 7, 24 * 47, 44 * 87, 64 * 24 \ or \ 84 * 67 (mod \ 100)$$

CHAPTER 2
MERSENNE PRIME

2 Mersenne Prime

It has became traditional to call numbers of the form $M_n = 2^n - 1, n \geq 1$ Mersenne numbers after father Marin Mersenne who made an incorrect but provocative assertion concerning their primality.

definition 2.1. *Mersenne numbers that happens to be prime are said to be Mersenne primes.*

Remark 2.1. *M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and composite for all other primes $p < 257$*

Theorem 2.1. *If p and $q = 2p + 1$ are primes, then their $q|M_p$ or $q|M_p + 2$.*

proof

With reference to Fermat's theorem, we know that

$$2^{q-1} - 1 \equiv 0(modq)$$

and factorising the left hand side,that

$$(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) = (2^p - 1)(2^p + 1) \equiv 0(mod\ q)$$

$$ie,\ (2^p-1)(2^p+1) \equiv 0(mod\ q)$$
$$\implies (2^p-1)(2^p-1+2) \equiv 0(mod\ q)$$
$$\implies M_p(M_p+2) \equiv 0(mod\ q)$$

By using the theorem, "if p is a prime and $p|ab$, then $p|a$ or $p|b$ ", we cannot have both $q|M_p$ and $q|M_p+2, for\ then\ q|2$, which is impossible therefore either $q|M_p$ *or* $q|M_p+2$.

Example 2.1. *A simple application should suffice to illustrate the above theorem if* $p=23$*, then* $q=2p+1=47$ *is also a prime, so that we may consider the case of* M_{23}
The questions reduces to one of whether $47|M_{23}$ *or to put it differently, whether* $2^{23} \equiv 1(mod\ 47)$
now we have

$$2^{23} \equiv 2^3(2^5)^4 \equiv 2^3(-15)^4(mod\ 47)$$
$$(-15)^4 \equiv (225)^2 \equiv (-10)^2 \equiv 6(mod\ 47)$$

putting these two congruences together, it is seen that

$$2^{23} \equiv 2^3 * 6 \equiv 48 \equiv 1(mod\ 47)$$

hence M_{23} *is composite.*

Theorem 2.2. *If* $q=2n+1$ *is prime, then*

$$a)\ q|M_n\ ,\ provided\ that\ q \equiv 1(mod\ 8)\ or\ q \equiv 7(mod\ 8)$$
$$b)\ q|M_n+2,\ provided\ that\ q \equiv 3(mod\ 8)\ or\ q \equiv 5(mod\ 8)$$

proof

To say that $q|M_n$ is equivalent to asserting that

$$2^{(q-1)/2} = 2^n \equiv 1(mod\ q)\ .....(***)$$
$$2^n - 1 \equiv 0(mod\ q)$$

In terms of the legendre symbol, the condition (1) becomes the requirement that $(2/q) = 1$ but according to the theorem, if p is an odd prime then,

$$(2/q) = \begin{cases} 1,\ if\ p \equiv 1(mod\ 8)\ or\ p \equiv 7(mod\ 8) \\ (-1),\ if\ p \equiv 3(mod\ 8)\ or\ p \equiv 5(mod\ 8) \end{cases}$$

we get $(2/q) = 1$ when we have $q \equiv 1(mod\ 8)$ or $q \equiv 7(mod\ 8)$
the proof of (b) proceeds along similar lines.
we get $(q|m_n + 2)$ provided that $q \equiv 3(mod\ 8)$ or $q \equiv 5(mod\ 8)$

corollary 2.2.1. *If p and $q = 2p+1$ are both odd primes, with $p = 3(mod\ 4)$, then $q|M_p$*

proof

An odd prime p is either of the form $4k+1$ or $4k+2$. If $p = 4k+3$, then

$$q = 2(4k+3) + 1$$
$$= 8k + 7$$

and the above theorem yield $q|M_p$. since by the condition $q|M_n$ provided that $q \equiv 1(mod\ 8)$. In the case in which $p = 4k+1$, $q = 8k+3$ so that q does not divide M_p, since q is not congruent to $1(mod\ 8)$ or q is not congruent to $7(mod\ 8)$, hence the theorem.

Remark 2.2. *the following is a partial list of prime numbers* $p \equiv 3(mod\ 4)$ *where* $q = 2p + 1$ *is also prime:* $p = 11, 23, 83, 131, 179, 239, 251$.*In each instance,*$M_p$ *is composite.*

Exploring the matter a little further, the next tackle two results of Fermat that restricted the divisors of M_p

Theorem 2.3. *If* p *is an odd prime, then any prime divisors of* M_p *is of the form* $2k_p + 1$

proof

Let q be any prime divisors of M_p, so that $2^p \equiv 1(mod\ q)$. If 2 has order k modulo q. (ie if k is the smallest positive integer that satisfies $2^k \equiv 1(mod\ q)$),
then theorem " Let the integer a have order k modulo n. Then $a^k \equiv 1(mod\ n)$ if and only if $k|n$; in particular $k|\phi(n)$ .....$(*)$
Tells us that $k|p$. The case $k = 1$ cannot arise; for this would imply that $q|1$ (since if $k = 1$, $2^k - 1 \equiv 0(mod\ q) \implies q = 1$) an impossible situation. Therefore , because both $k|p$ and $k > 1$, the primality of p force $k = p$

In compliance with Fermat's theorem, we have $2^{q-1} \equiv 1(mod\ q)$, and again by theorem $(*)$ $k|(q-1)$ knowing that $k = p$, the net result is $p|(q-1)$. To be defined , let us put $q - 1 = pt$; then $q = pt + 1$. The proof is completed by noting that if t were an odd integer, then q would be even and a contradiction occurs. Hence , we must have $q = 2k_p + 1$. For some choice of k, which gives q the required form.

Theorem 2.4. *If* p *is an odd prime , then any prime divisor* q *of* m_p *is of the form* $q \equiv \pm 1(mod\ 8)$.

proof

Suppose that $q = 2n + 1$ is a prime divisor of m_p.
If $a = 2^{(p+1)/2}$, then

$$\begin{aligned} a^2 - 2 &= (2^{(p+1)/2})^2 - 2 \\ &= 2^{p+1} - 2 \\ &= 2^p \times 2 - 2 \\ &= 2(2^p - 1) \\ &= 2M_p \\ &\equiv 0(mod\ q) \end{aligned}$$

Raising both sides of the congruence $a^2 \equiv 2(mod\ q)$ to the n^{th} power, we get

$$a^{q-1} = a^{2n} \equiv 2^n(mod\ q)$$

Since q is an odd integer , one has $gcd(a, q) = 1$ and so $a^{q-1} \equiv 1(mod\ q)$. In conjunction, the last congruence tell us that

$$\begin{aligned} &2^n \equiv 1(mod\ q) \\ \implies\ &2^n - 1 \equiv 0(mod\ q) \\ \implies\ &q|M_n \end{aligned}$$

the theorem $(***)$ now be brought into play to reach the condition that $q \equiv \pm 1(mod\ 8)$
Therefore we get if p is an odd prime then any prime divisor q of M_p is of the form

$$q \equiv \pm 1(mod\ 8)$$

hence the theorem.

Remark 2.3. *For an illustration of how these theorems can be used, one might look at* M_{17}. *These integers of the form* $34k + 1$ *that are less than* $362 < \sqrt{M_{17}}$ *are* $35, 69, 103, 137, 171, 205, 239, 273, 307, 341$.

Because the smallest (non-trivial) divisors of M_{17} must be prime, we need only consider the primes among the foregoing 10 numbers namely, $103, 137, 239, 307$ the work can be shortened some what by noting that 307 is not congruent to $\pm 1(mod\ 8)$, and therefore we may delete 307 from our list.Now, either M_{17} is prime or one of the three remaining possibilities divide it with a little calculations we can check that M_{17} is divisible by none of $103, 137,$ *and* 239; the result M_{17} is prime.

Theorem 2.5. ***EULER:*** *If* n *is a perfect number, then any* $n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ *where the* $p_i's$ *are distinct odd primes and* $p_1 \equiv\ k_1 \equiv 1(mod\ 4)$.

proof

Let $n = \ n = {p_1}^{k_1}{p_2}^{k_2}.....{p_r}^{k_r}$ be the prime factorisation of n. Because n is perfect.We can write

$$2n = \sigma(n) = \sigma({p_1}^{k_1}) \ \times\sigma({p_2}^{k_2}) \ ..... \times\sigma({p_r}^{k_r})$$
being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$

being an odd integer, either $n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$; in any event, $2n \equiv 2(mod\ 4)$. Thus , $\sigma(n) = 2n$ is divisible by 2, but not by 4. The implication is that one of the $\sigma({p_i}^{k_i})$, say $\sigma({p_i}^{k_i})$, must be an even integer (but not divisible by 4), and all the remaining $\sigma({p_i}^{k_i})$'s are odd integers.

For a given p_i , there are two cases to be considered:
$p_i \equiv 1(mod\ 4)$ and $p_i \equiv 3(mod\ 4)$. If $p_i \equiv 3 \equiv -1(mod\ 4)$, we would have,

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^{k_i}$$
$$\equiv 1 + (-1) + (-1)^2 + ... + (-1)^{k_i} (mod\ 4)$$
$$\equiv \begin{cases} 0(mod\ 4)\ if\ k_i\ is\ odd \\ 1(mod\ 4)\ if\ k_i\ is\ even \end{cases}$$

since $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$, this tells us that $p_1 \not\equiv 3(mod\ 4)$ or, to put it affirmatively, $p_1 \equiv 1(mod\ 4)$. Furthermore, the congruence $\sigma({p_i}^{k_i}) \equiv 0(mod\ 4)$ signifies that 4 divides $\sigma({p_i}^{k_i})$ which is not possible.
The conclusion : if $p_i \equiv 3(mod\ 4)$ where $i = 2, ..., r$ then it's exponent k_i must be an even integer.
Should it happen that $p_i \equiv 1(mod\ 4)$ which is certainly true for i=1,then

$$\sigma({p_i}^{k_i}) = 1 + p_i + {p_i}^2 + ... + {p_i}^k$$
$$\equiv 1 + 1^1 + 1^2 + ... + 1^{k_i} (mod\ 4)$$
$$\equiv k_i + 1(mod\ 4)$$

The condition $\sigma({p_i}^{k_i}) \equiv 2(mod\ 4)$ for as $k_1 \equiv 1(mod\ 4)$.For the other values of i, we know that $\sigma({p_i}^{k_i}) \equiv 1\ or\ 3(mod\ 4)$, and therefore $k_i \equiv 0\ or\ 2(mod\ 4)$; in any case k_i is an even integer. The crucial point is that, regardless of whether $p_i \equiv 1(mod\ 4)$ or $p_i \equiv 3(mod\ 4)$, k_i is always for $i \neq 1$. Our proof is now complete.

Remark 2.4. *In view of the preceding theorem, any odd perfect number n can be expressed as*

$$n = {p_1}^{k_1} {p_2}^{2j_2} .....{p_r}^{2j_r}$$
$$= p_1^{k_1} ({p_2}^{j_2} .....p_r^{j_r})^2$$
$$= {p_1}^{k_1} m^2$$

This leads directly to the following corollary.

corollary 2.5.1. *If n is an odd perfect number, then n is of the form $n = p^k m^2$. Where p is a prime, p does not divides m, and $p \equiv k \equiv 1(mod\ 4)$; in particular, $n = 1(mod\ 4)$*

proof

Only the last assertion is not obvious.Because $p \equiv 1(mod\ 4)$, we have $p^k \equiv 1(mod\ 4)$.Notice that m must be odd; hence $m \equiv 1$ *or* $3(mod\ 4)$, and therefore upon squaring, $m^2 \equiv 1(mod\ 4)$. It follows that

$$n = p^k m^2 \equiv 1 \times 1 \equiv 1(mod\ 4)$$

establishing our corollary.

definition 2.2. *Two numbers such as* 220 *and* 284 *are called amicable, or friendly; because they have the remarkable property that each number is " contained" within the other, in the sense that each number is equal to the sum of all the positive divisors of the other , not counting the number itself.Thus, as regards the divisors* 220

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

and for 284*,*

$$1 + 2 + 4 + 71 + 142 = 220$$

In terms of the σ function, amicable numbers m and n (or an amicable pair) are defined by the equation.

$$\sigma(m) - m = n$$
$$\sigma(n) - n = m$$

or what amounts to the same thing;

$$\sigma(m) = m + n = \sigma(n)$$

Remark 2.5. *Amicable number have been important in magic and astrology, and casting horoscope, making talismans. The Greeks believed that these numbers had a particular influence in establishing friendship between individuals.*

CHAPTER 3

FERMAT NUMBERS

3 Fermat Numbers:

definition 3.1. *A Fermat number is an integer of the form*

$$F_n = 2^{2^n} + 1,\ n \geq 0$$

If F_n is prime, it is said to be a fermat prime.

Remark 3.1. $F_0 = 3,\ F_1 = 5,\ F_2 = 17\ F_3 = 257,\ F_4 = 65537$ *and* $F_5 = 2^{2^5} + 1 = 4294967297$

Theorem 3.1. *The fermat number F_5 is divisible by* 641

proof

We begin by putting $a = 2^7$ and $b = 5$, so that

$$1 + ab = 1 + (2^7 \times 5) = 641$$

It is easily seen that

$$1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b = 2^4$$

But this implies that;

$$\begin{gathered} F_5 = 2^{2^5} + 1 = 2^{32} + 1 \\ = (2^4 \times a^4) + 1 \\ = (1 + ab - b^4)a^4 + 1 \\ (1 + ab)a^4 + (1 - a^4b^4) \\ = (1 + ab)[a^4 + (1 - ab)(1 + a^2b^2)] \end{gathered}$$

which gives $641|F_n$.

Theorem 3.2. *For fermat numbers F_n and F_m, where $m > n \geq 0$, $gcd(F_m, F_n) = 1$.*

proof

Put $d = gcd(F_m, F_n) = 1$. Because Fermat numbers are odd integers, d must be odd. If we set $x = 2^{2^n}$ *and* $k = 2^{m-n}$ *then*

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

$$= \frac{x^k - 1}{x + 1}$$

$$= x^{k-1} - x^{k-2} + ... - 1$$

hence $F_n|(F_m - 2)$.From $d|F_n$, it follows that $d|(F_m - 2)$.Now use the fact that $d|F_m$ to obtain $d|2$. But d is an odd integer, and so $d = 1$, establishing the result is claimed.

Remark 3.2. *We know that each of the Fermat numbers $F_0, F_1, F_2, ...F_N$ is divisible by a prime that does not divide any of the other F_k. Thus, there*

are at least $n+1$ distinct primes not exceeding F_n.Because there are infinitely many Fermat numbers, the number of primes is also infinite.
In 1877, the Jesuit priest T.Pepin devised the practical test(Pepin's test for determining the primality of F_n that is embodied in the following theorem.)

Theorem 3.3. *Pepin's test; For $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if*

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

proof

First let us assume that,

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Upon squaring both sides we get

$$3^{F_n-1} \equiv 1(mod\ F_n)$$

The same congruence holds for any prime p that divides F_n

$$3^{F_n-1} \equiv 1(mod\ p)$$

Now let k be the order of 3 modulo p. We know that $k|(F_n - 1)$ or in other words, that $k|2^{2^n}$ therefore k must be a power of 2.
It is not possible that $k = 2^r$ for any $r \leq 2^n - 1$
For if this were so, repeated squaring of the congruence $3^k \equiv 1(mod\ p)$ would yield

$$3^{2^{2^n-1}} \equiv 1(mod\ p)$$

or, what is the same thing,

$$3^{F_n-1} \equiv 1(mod\ p)$$

We would then arrive at $1 \equiv -1(mod\ p)$, resulting in $p = 2$, which is a contradiction. Thus the only possibility open to us is that

$$k = 2^{2^n} = F_n - 1$$

Fermat's theorem tells us that $k \leq p - 1$, which means, in turn, that $F_n = k + 1 \leq p$. Because $p|F_n$, we also have $p \leq F_n$.Together, these inequalities mean that $F_n = p$, so that F_n is prime. On the other hand, suppose that $F_n,\ n \geq 1$ is prime.
The quadratic Reciprocity Law gives

$$(3|F_n) = (F_n|3) = (2|3) = -1$$

When we use the fact that

$$F_n \equiv (-1)^{2^n} + 1 = 2(mod\ 3)$$

Applying Euler's criterion, we end up with

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Example 3.1. *Show that using Pepin's test $F_3 = 257$ is prime.*

proof

$$3^{\frac{p_3-1}{2}} = 3^{128} = 3^3(3^5)^{25}$$
$$\equiv 27(-14)^{25}$$
$$\equiv 27 \times 14^{24}(-14)$$
$$\equiv 27(17)(-14)$$
$$\equiv 27 \times 19 \equiv 513 \equiv -1(mod\ 257)$$

So that F_3 is prime.

Theorem 3.4. *Any prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, is of the form*

$$p = k \times 2^{(n+2)} + 1$$

proof

For a prime divisor p of F_n,

$$2^{2^n} \equiv -1(mod\ p)$$

Which is to say, upon squaring that

$$2^{2^{n+1}} \equiv 1(mod\ p)$$

If h is the order of 2 modulo p, this congruence tells us that $h|2^{n+1}$.We cannot have $h = 2^r$ where $1 \leq r \leq n$, for this would lead to $2^{2^n} \equiv 1(mod\ p)$ and in turn, to the contradiction that $p = 2$.This let us conclude that $h = 2^{n+1}$. Because the order of 2 modulo p divides $\phi(p) = p - 1$, we may further conclude that $2^{n+1}|p - 1$.The point is that for $n \geq 2, p \equiv 1(mod\ 8)$, and therefore, by theorem, if p is an odd number then $2|p$, the Legendre symbol $(2|P) = 1$.

Using Euler's criterion, we immediately pass to

$$2^{\frac{(p-1)}{2}} \equiv (2|p) = 1(mod\ p)$$

An appeal to theorem " let the integer a have order k modulo n, then $a^h \equiv 1(mod\ n)$ if and only if $k|n$, in particular, $k|\phi(n)$, " finishes the proof. It asserts that $h|\frac{(p-1)}{2}$, or equivalently, $2^{(n+1)}|\frac{(p-1)}{2}$.This forces $2^{n+2}|(p-1)$ and we obtain $p = k \times 2^{(n+2)} + 1$ for some integer k.

CONCLUSION

Number theory is the study of the integers and related objects.Topics studied by number theorists include the problem of determining the distribution of prime numbers within the integers and the structure and number of solutions of polynomial equations with integer co-effecients.
A branch of pure mathematics that deals with the study of natural numbers and the study deals with the set of positive whole numbers that are usually called the set of natural numbers and is partly experimental and partly theoretical.

Number theory is necessary for the study of numbers because it shows what numbers can do. It helps in providing valuable training in logical thinking and studying the relationship between different kinds of numbers. It is applied in cryptography, device authentication, websites for e-commerce, coding, and security systems.

BIBLIOGRAPHY

1. DAVID M. BURTON, ELEMENTARY NUMBER THEORY, 7th edition

2. JOSEPH H. SILVERMAN, A FRIENDLY INTRODUCTION TO NUMBER THEORY, 4th edition, Pearson

3. https://www.cuemath.com/numbers/number-theory/

AN INTRODUCTION TO GRAPH THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

AKHIL RAJ P
DB20CMSR01

under the guidance of
Ms. Remya Raj

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty

March 2023

Examiner 1 **Examiner 2**

CERTIFICATE

This is to certify that **"An Introduction To Graph Theory"** is a bona fide project of **Akhil Raj P**, Register Number: **DB20CMSR01** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Ms. Remya Raj
Project Supervisor

DECLARATION

I, Akhil Raj P, hereby declare that the project: "An Introduction To Graph Theory" is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

Akhil Raj P

DB20CMSR01

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that had helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thank you for all your encouragement.

CONTENTS

INTRODUCTION

In mathematics, graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. Graph theory is a delightful playground for the exploration of proof techniques in Discrete Mathematics. The results of graph theory have applications in many areas of the computing, social and natural sciences. One of the beauties of graph theory is that it depends very little on other branches of mathematics. The subject of graph theory had its beginnings in recreational math problems but it has grown into a significant area of mathematical research, with applications in chemistry, operations research, social sciences, and computer science.

Graph Theory can model and study many real-world problems and is applied in a wide range of disciplines. In computer science, graph theory is used to model networks and communications as seen in the case of Google search, Google Maps and social media. Furthermore, graph theory is used in chemistry to model molecules and in biology to study genomes. It is even used in linguistics and social sciences. Using graph theory in Machine Learning and neural network is also one of the new trends.

The history of graph theory may be specifically traced to 1735, when the Swiss mathematician Leonhard Euler solved the Königsberg bridge problem. The Königsberg bridge problem was an old puzzle concerning the possibility of finding a path over every one of seven bridges that span a forked river flowing past an island—but without crossing any bridge twice. Euler argued that no such path exists since in Königsberg, the four land masses were connected by an odd number of bridges, it was impossible to draw the desired route. His proof involved only references to the physical arrangement of the bridges, but essentially he proved the first theorem in graph theory.

CHAPTER 1

BASIC CONCEPTS IN GRAPH THEORY

1.1 GRAPH

A graph G = (V(G),E(G)) consists of two finite sets:

i The vertex set of the graph, denoted by V(G) or V, which is a non-empty set of elements called vertices,

ii The edge set of the graph, denoted by E(G) or E, which is a possible empty set of elements called edges,

such that each edge e in E is assigned an unordered pair of vertices (u,v) called the end vertices of e.

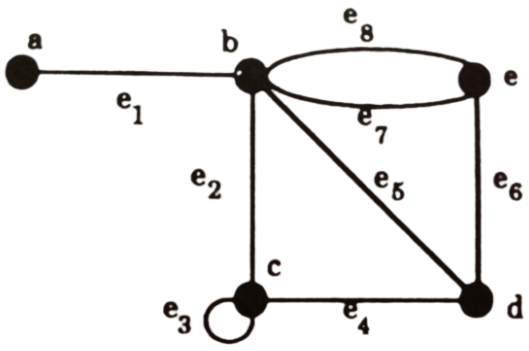
Vertices of a graph are also known as nodes or points while edges are also called links or lines.

1.1.1 EXAMPLE

Let G = (V,E) where V = $\{a, b, c, d, e\}$, E = $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$, and the ends of edges are given by:

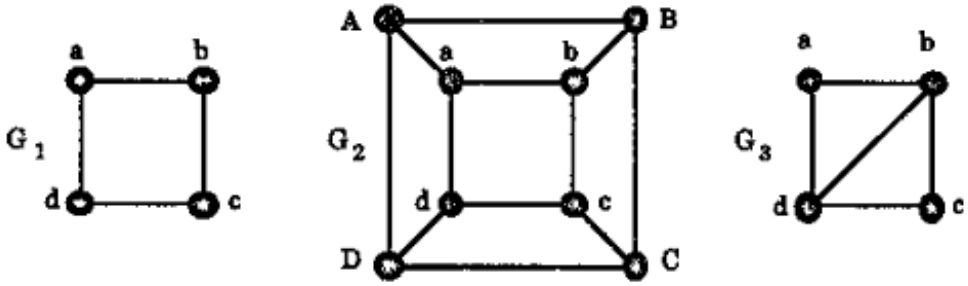
$e_1 \longleftrightarrow (a, b)$ $e_2 \longleftrightarrow (b, c)$ $e_3 \longleftrightarrow (c, c)$ $e_4 \longleftrightarrow (c, d)$ $e_5 \longleftrightarrow (b, d)$
$e_6 \longleftrightarrow (d, e)$ $e_7 \longleftrightarrow (b, e)$ $e_8 \longleftrightarrow (b, e)$.

Then, G can be represented diagrammatically as:



1.2 SUBGRAPHS

Let H be a graph with vertex set $V(H)$ and edge set $E(H)$ and similarly, let G be a graph with vertex set $V(G)$ and edge set $E(G)$. Then we say that H is a subgraph of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. In such a case, we also say that G is a supergraph of H.

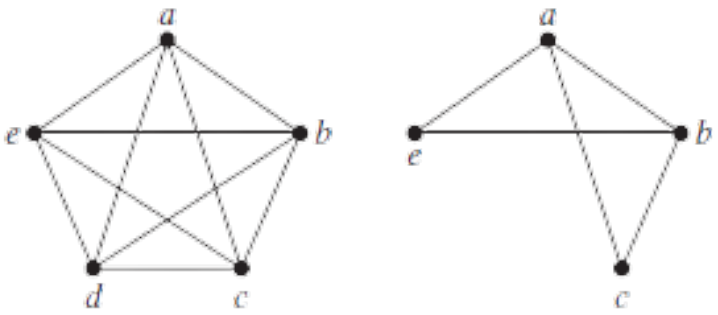


In the above example, G_1 is a subgraph of both G_2 and G_3. But, G_3 is not a subgraph of G_2.

1.2.1 PROPER SUBGRAPH

If H is a subgraph of G then we write: $H \subseteq G$. When $H \subseteq G$ but $H \neq G$, i.e., $V(H) \neq V(G)$ or $E(H) \neq E(G)$, then H is called a proper subgraph of G.

1.2.2 EXAMPLE

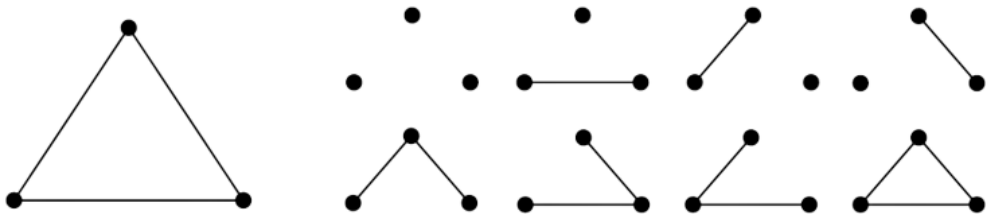


A Subgraph of K_5.

1.2.3 SPANNING SUBGRAPH

A spanning subgraph of a graph G is a subgraph H with $V(H) = V(G)$, i.e., H and G have exactly the same vertex set.

1.2.4 EXAMPLE



the graph C_3

spanning subgraphs of C_3

1.3 SOME DEFINITIONS

Definition 1.1. ***LOOP***

An edge for which two end vertices are the same is called a loop.

Definition 1.2. ***PARALLEL EDGES***

If two or more edges of G have the same end vertices, these edges are called multiple or parallel edges.

Definition 1.3. ***INCIDENT EDGE***

Any edge is said to be incident to the vertices connected by the edge.

Definition 1.4. ***ADJACENT VERTEX***

A vertex is said to be adjacent to other vertices if it has an edge connecting it to the vertices.

Definition 1.5. ***ISOLATED VERTEX***

Any vertex without any edges coming in or out of it is called an isolated vertex.

Definition 1.6. ***VERTEX DEGREES***

Let v be a vertex of a graph G. The degree $d(v)$ of v is the number of edges of G incident with v, counting each loop twice, i.e., it is the number of times v is an end vertex of an edge.

Definition 1.7. ***BIPARTITION***

Let G be a graph. If the vertex set V of G can be partitioned into two non-empty subsets X and Y in such a way that each edge of G has one end in X and one end in Y, then G is called bipartite.
The partition V is called a bipartition of G.

1.4 PATHS, CYCLES AND TREES

1.4.1 WALK

A walk in a graph G is a finite sequence:

$$W = v_0 e_1 v_1 e_2 v_2 ... v_{k-1} e_k v_k \tag{1.1}$$

whose terms are alternatively vertices and edges such that, for $1 \leq i \leq k$, the edge e_i has ends v_{i-1} and v_i. Thus, each edge e_i is immediately preceded and succeeded by the two vertices with which it is incident.

The walk W in (2.1) is a $v_0 - v_k$ walk, or, a walk from v_0 to v_k. The vertex v_0 is called the ***origin*** of the walk while v_k is called the ***terminus*** of W. (v_0 and v_k need not be distinct.)
The vertices v_1, v_2,...,v_{k-1}, in a walk W are called its ***internal vertices***. The integer k, the number of edges in the walk, is called the ***length*** of W.

1.4.2 TRIVIAL WALK

A trivial walk is a walk containing no edges.
Thus, for any vertex v of a graph G,

$$W = v$$

gives a trivial walk. It has length 0.

1.4.3 CLOSED AND OPEN WALK

For two given vertices u and v of a graph G, a $u - v$ walk is said to be ***closed*** or ***open*** depending on whether $u = v$ or $u \neq v$.

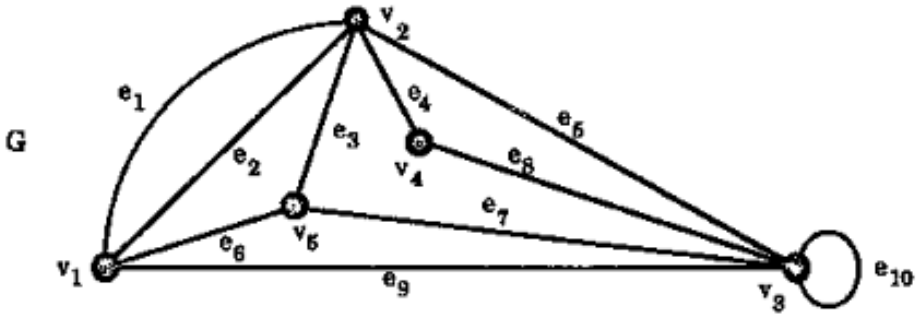
1.4.4 TRAIL

If the edges $e_1, e_2, ..., e_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k v_k$ are distinct, W is called a ***trail***.

1.4.5 PATH

If the vertices $v_0, v_1, ..., v_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k\, v_k$ are distinct then W is called a ***path***.
A path with n vertices is sometimes denoted by P_n and it has length $n - 1$.

1.4.6 EXAMPLE



Let the above graph G be such that the walks W_1, W_2, W_3, W_4 be defined as:

- $W_1 = v_1\, e_1\, v_2\, e_5\, v_3\, e_{10}\, v_3\, e_5\, v_2\, e_3\, v_5$
- $W_2 = v_1\, e_1\, v_2\, e_1\, v_1\, e_1\, v_2$
- $W_3 = v_1\, v_5\, v_2\, v_4\, v_3\, v_1$
- $W_4 = v_2\, v_4\, v_3\, v_5\, v_1$

Here, the length of:

1. $W_1 = 5$
2. $W_2 = 3$
3. $W_3 = 5$
4. $W_4 = 4$.

Then,

1. W_1, W_2 and W_4 are open walks while W_3 is a closed walk.
2. W_3, W_4 are trails but W_1 and W_2 aren't.
3. W_4 is a path but W_1, W_2 and W_3 aren't.

Theorem 1.4.1. *Given any two vertices u and v of a graph G, every $u-v$ walk contains a $u-v$ path,*
i.e., given any walk,

$$W = u\, e_1\, v_1 ... v_{k-1}\, e_k\, v$$

then, after some deletion of vertices and edges if necessary, we can find a sub-sequence P of W which is a $u-v$ path.

Proof. If $u = v$, i.e.,if W is closed, then the trivial path $P = u$ will do.

Now suppose $u \neq v$,i.e.,W is open and let the vertices of W be given, in order, by:

$$u = u_0, u_1, u_2, ..., u_{k-1}, u_k = v.$$

If none of the vertices of G occurs in W more than once, then W is already a $u-v$ path and so we are finished by taking $P = W$.

So now suppose that there are vertices of G that occur in W twice or more. Then there are distinct i, j with $i < j$, say, such that $u_i = u_j$. If the terms $u_i, u_{i+1}, ..., u_{j-1}$ (and the preceding edges) are deleted from W then we obtain a $u-v$ walk W_1 having fewer vertices than W. If there is no repetition of vertices in W_1, then W_1 is a $u-v$ path and setting $P = W_1$ finishes the proof.
If this is not the case, then we repeat the above deletion procedure until finally arriving at a $u-v$ walk that is a path, as required. □

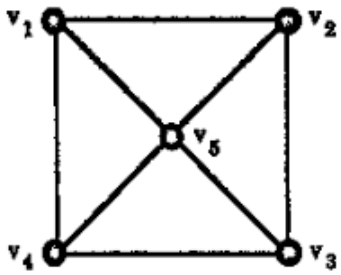
1.4.7 CYCLE

A non-trivial closed trail in a graph G is called a cycle if its origin and internal vertices are distinct i.e.,
A cycle in a graph is a non-empty trail in which only the first and last vertices are equal.

A cycle of length k is called a $k-cycle$. A $k-cycle$ is called odd or even depending on whether k is odd or even.

A $3-cycle$ is often called a triangle. An $n-cycle$, i.e., a cycle with n vertices, will sometimes be denoted by C_n.

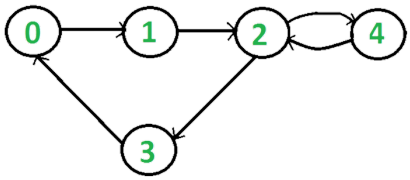
EXAMPLE 1:



In the above example,

1. C = $v_1\, v_2\, v_3\, v_4\, v_1$ is a 4-cycle.
2. $T = v_1\, v_2\, v_5\, v_3\, v_4\, v_5\, v_1$ in a non-trivial closed trail which is not a cycle since v_5 occurs twice as an internal vertex.
3. C_1 = $v_1\, v_2\, v_5\, v_1$ is a triangle.

EXAMPLE 2:

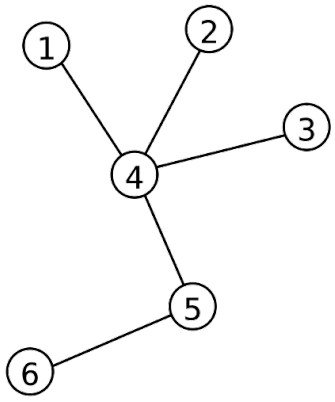


Here, $0 \to 1 \to 2 \to 3 \to 0$ is a 4-cycle but $0 \to 1 \to 2 \to 4 \to 2 \to 3 \to 0$ is not a cycle since the vertex 2, an internal vertex, occurs twice.

1.4.8 TREES

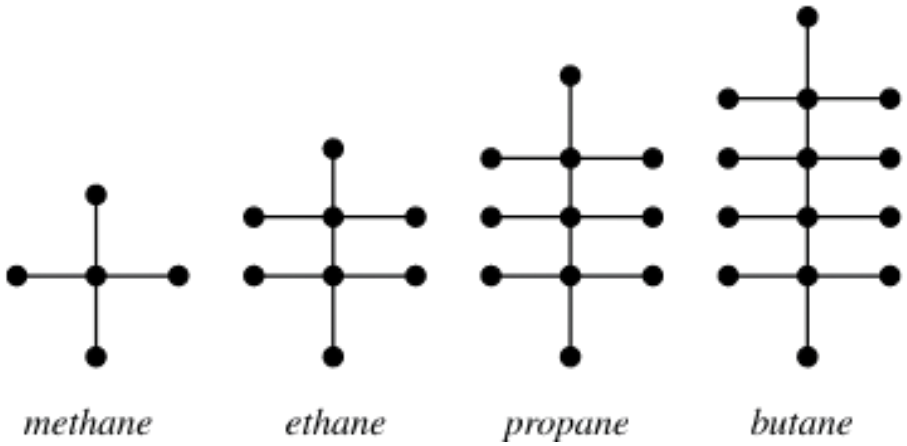
A graph G is called ***acyclic*** if it contains no cycles.
A graph G is called a ***tree*** if it is a connected acyclic graph, i.e., A tree is an undirected graph in which any two vertices are connected by exactly one path.

EXAMPLE 1:



The above graph is an undirected connected acyclic graph and thus, a tree.

EXAMPLE 2:



The above example shows the representation of the first four hydrocarbons as trees.

CHAPTER 2

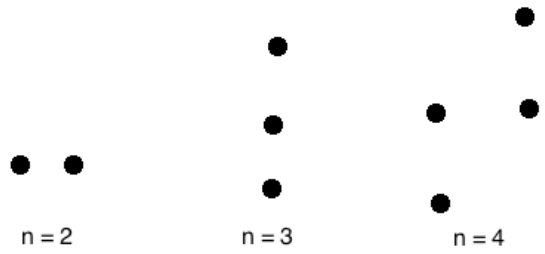
TYPES AND PROPERTIES OF GRAPHS

2.1 TYPES OF GRAPHS

Definition 2.1. ***NULL GRAPH***

A null graph is a graph in which there are no edges between its vertices. A null graph is also called empty graph.

EXAMPLE:



In all the above graphs, there are no edges between the vertices.

Definition 2.2. ***TRIVIAL GRAPH***

A trivial graph is the graph which has only one vertex.

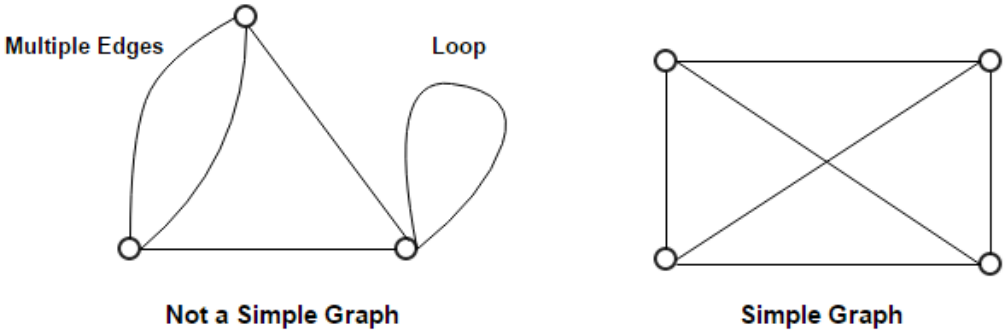
EXAMPLE:

In the above graph, there is only one vertex 'v' without any edge. Therefore, it is a trivial graph.

Definition 2.3. ***SIMPLE GRAPH***

A simple graph is the undirected graph with no parallel edges and no loops. A simple graph which has n vertices, the degree of every vertex is at most $n-1$.

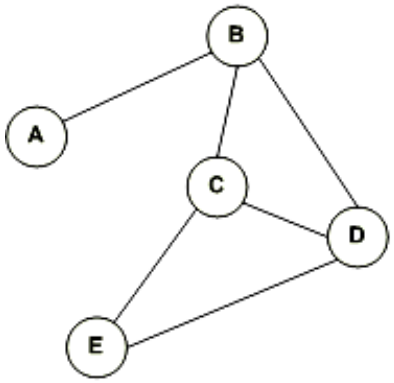
EXAMPLE:



Definition 2.4. ***UNDIRECTED GRAPH***

An undirected graph is a graph whose edges are not directed. The relations between pairs of vertices in an undirected graph are symmetric, so that each edge has no directional character. They only represent whether or not a relationship exists between two vertices. Thus, all the edges in an undirected graph are bidirectional.

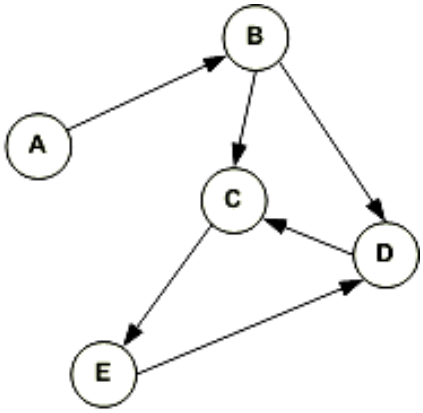
EXAMPLE:



Definition 2.5. ***DIRECTED GRAPH***

A directed graph is a graph in which the edges are directed by arrows.
Directed graphs are also known as digraphs.

EXAMPLE:

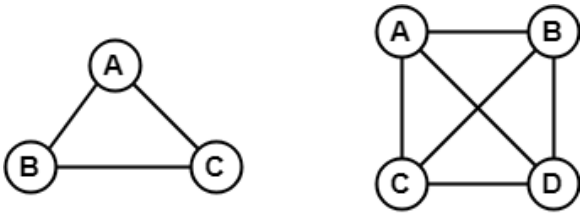


In the above graph, each edge is directed by the arrow. A directed edge has an arrow from A to B means A is related to B but B is not related to A.

Definition 2.6. ***COMPLETE GRAPH***

A graph in which every pair of vertices is joined by exactly one edge is called complete graph. It contains all possible edges.
A complete graph with n vertices contains exactly $\binom{n}{2}$ *edges.*

EXAMPLE:

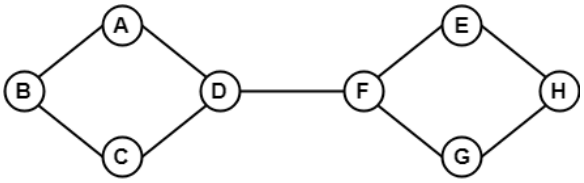


In the above example, since each vertex in the graph is connected with all the remaining vertices through exactly one edge, both are complete graphs.

Definition 2.7. ***CONNECTED GRAPH***

A connected graph is a graph in which we can visit from any one vertex to any other vertex. In a connected graph, at least one edge or path exists between every pair of vertices.

EXAMPLE:

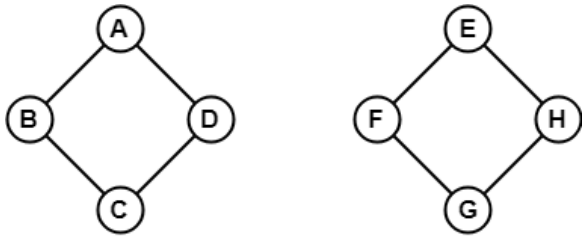


In the above example, we can traverse from any one vertex to any other vertex. It means there exists at least one path between every pair of vertices therefore, it a connected graph.

Definition 2.8. ***DISCONNECTED GRAPH***

A disconnected graph is a graph in which any path does not exist between every pair of vertices.

EXAMPLE:

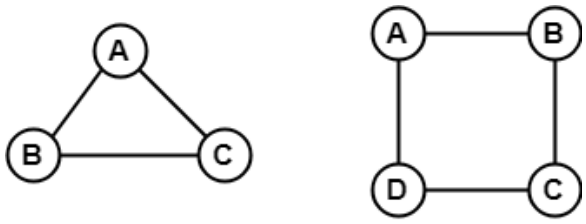


The above graph consists of two independent components which are disconnected. Since it is not possible to visit from the vertices of one component to the vertices of other components, it is a disconnected graph.

Definition 2.9. ***REGULAR GRAPH***

A regular graph is a graph in which degree of all the vertices is same.
If the degree of all the vertices is k*, then it is called* $k - regulargraph$*.*

EXAMPLE:



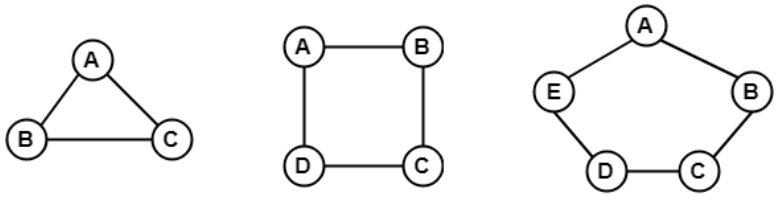
In the above example, all the vertices have degree 2*. Therefore they are called* $2 - Regulargraph$*.*

Definition 2.10. ***CYCLIC GRAPH***

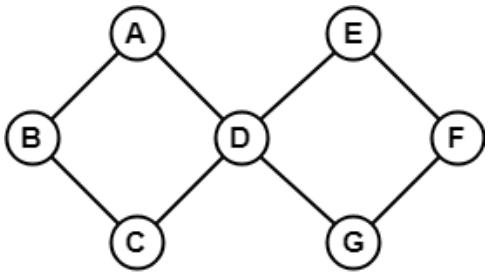
A graph with n vertices (where $n >= 3$) and n edges forming a cycle of n with all its edges is known as cycle graph.
In the cycle graph, degree of each vertex is 2.

A graph containing at least one cycle in it is known as a cyclic graph.

EXAMPLE:



In the above example, all the vertices have degree 2. Therefore they all are cyclic graphs.

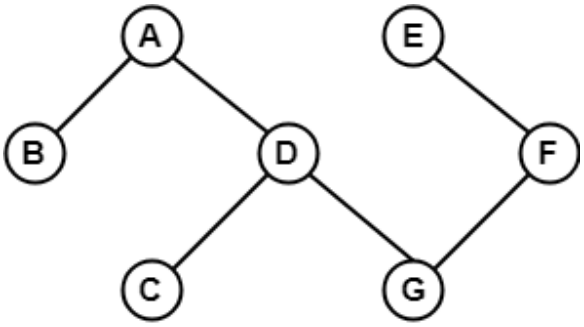


The above graph contains two cycles in it and therefore it is a cyclic graph.

Definition 2.11. ***ACYCLIC GRAPH***

A graph which does not contain any cycle in it is called as an acyclic graph.

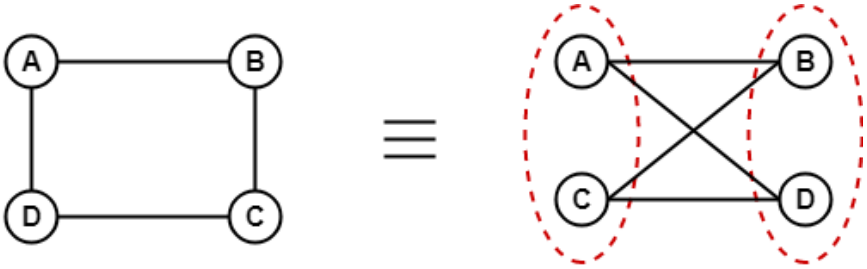
EXAMPLE:



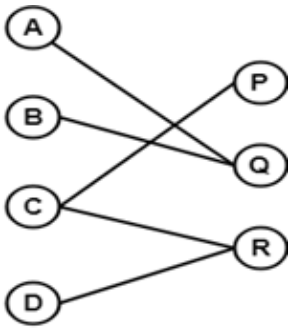
Definition 2.12. ***BIPARTITE GRAPH***

A bipartite graph is a graph in which the vertex set can be partitioned into two sets such that edges only go between sets, not within them.
A graph $G(V, E)$ is called bipartite graph if its vertex-set $V(G)$ can be decomposed into two non-empty disjoint subsets $V_1(G)$ and $V_2(G)$ in such a way that each edge $e \in E(G)$ has its one last joint in $V_1(G)$ and other last point in $V_2(G)$.
The partition $V = V1 \cup V2$ is known as bipartition of G.

EXAMPLE 1:



EXAMPLE 2:

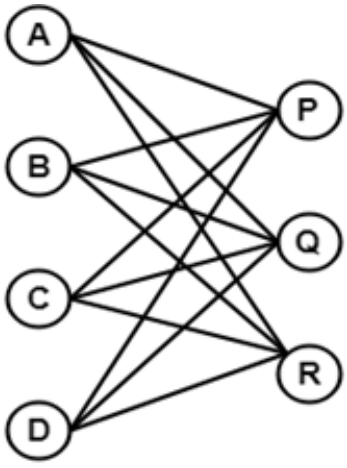


Definition 2.13. ***COMPLETE BIPARTITE GRAPH***

A complete bipartite graph is a bipartite graph in which each vertex in the first set is joined to each vertex in the second set by exactly one edge.
A complete bipartite graph is a bipartite graph which is complete.

$$Complete\,Bipartite\,Graph = Bipartite\,Graph + Complete\,Graph \quad (2.1)$$

EXAMPLE:

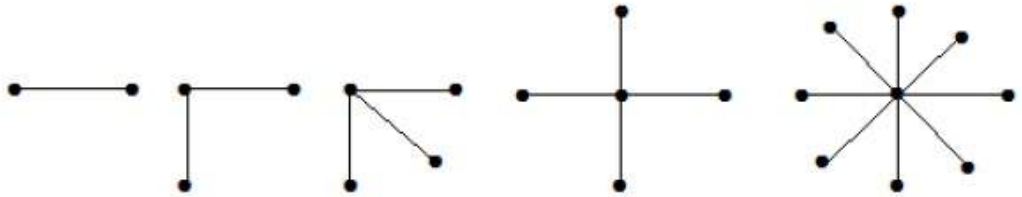


The above graph is known as $K_{4,3}$

Definition 2.14. ***STAR GRAPH***

A star graph is a complete bipartite graph in which $n-1$ vertices have degree 1 and a single vertex has degree $(n-1)$. This exactly looks like a star where $(n-1)$ vertices are connected to a single central vertex.
A star graph with n vertices is denoted by S_n.

EXAMPLE:

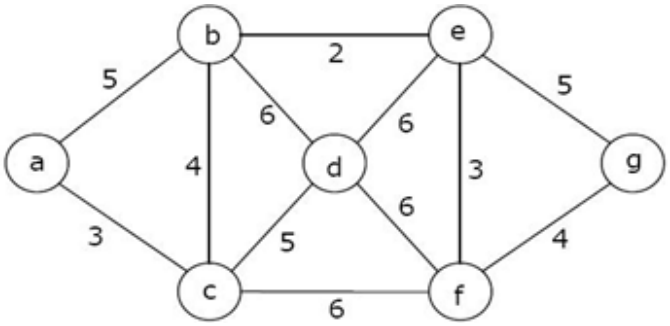


In the above example, out of n vertices, all the $(n-1)$ vertices are connected to a single vertex. Hence, it is a star graph.

Definition 2.15. ***WEIGHTED GRAPH***

A weighted graph is a graph whose edges have been labeled with some weights or numbers.
The length of a path in a weighted graph is the sum of the weights of all the edges in the path.

EXAMPLE:



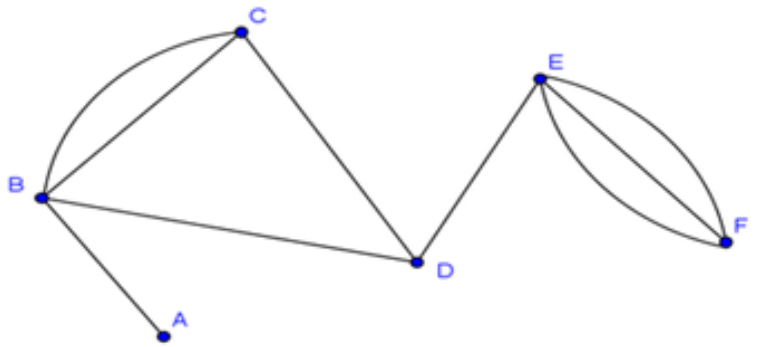
In the above graph, if the path chosen is $a \to b \to c \to d \to e \to g$ *then the length of the path is :*

$$5 + 4 + 5 + 6 + 5 = 25.$$

Definition 2.16. ***MULTI GRAPH***

A graph in which there are multiple edges between any pair of vertices or there are edges from a vertex to itself (loop) is called a multi - graph.

EXAMPLE:

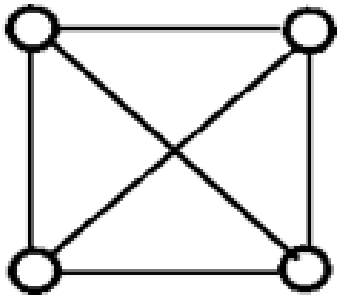


In the above graph, vertex-set B *and* C *are connected with two edges. Similarly, vertex sets* E *and* F *are connected with* 3 *edges. Therefore, it is a multi graph.*

Definition 2.17. ***PLANAR GRAPH***

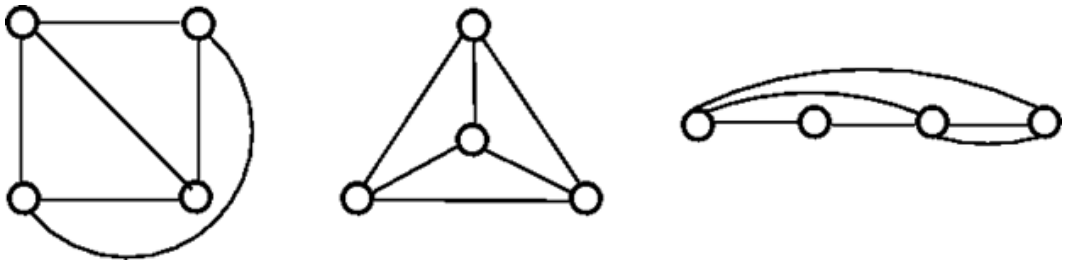
A planar graph is a graph that we can draw in a plane in such a way that no two edges of it cross each other except at a vertex to which they are incident,
i.e., A planar graph is a graph that can be embedded in the plane such that its edges intersect only at their endpoints.

EXAMPLE:



The above graph may not seem to be planar because it has edges crossing each other. But we can redraw the above graph.

The three plane drawings of the above graph are:



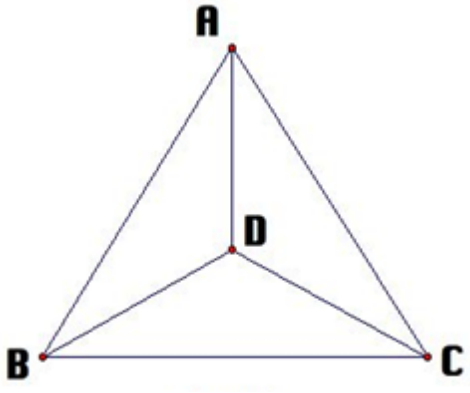
The above three graphs do not consist of two edges crossing each other and therefore, all the above graphs are planar.

2.2 PROPERTIES OF GRAPHS

2.2.1 DISTANCE BETWEEN TWO VERTICES

Distance is basically the number of edges in a shortest path between vertex X and vertex Y. If there are many paths connecting two vertices, then the shortest path is considered as the distance between the two vertices.
Distance between any two vertices X and Y is denoted by $d(X, Y)$.

EXAMPLE:



Suppose, we want to find the distance between vertex B and D. Then, first of all, we have to find the shortest path between vertex B and D.
There are many paths from vertex B to vertex D:

- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Here, length = 3
- B $\rightarrow$ D. Length = 1 (Shortest Path)
- B $\rightarrow$ A $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Length = 3

Hence, the minimum distance between vertex B and vertex D is 1.

2.2.2 ECCENTRICITY OF A VERTEX

Eccentricity of a vertex is the maximum distance between a vertex to all other vertices. It is denoted by $e(V)$.
For a disconnected graph, all vertices are defined to have infinite eccentricity.

2.2.3 RADIUS OF CONNECTED GRAPHS

The radius of a connected graph is the minimum eccentricity from all the vertices. In other words, the minimum among all the distances between a vertex to all other vertices is called as the radius of the graph.
It is denoted by $r(G)$.

2.2.4 DIAMETER OF A GRAPH

Diameter of a graph is the maximum eccentricity from all the vertices. In other words, the maximum among all the distances between a vertex to all other vertices is considered as the diameter of the graph G.
It is denoted by $d(G)$.

2.2.5 CENTRAL POINT

If the eccentricity of the graph is equal to its radius, then it is known as central point of the graph,

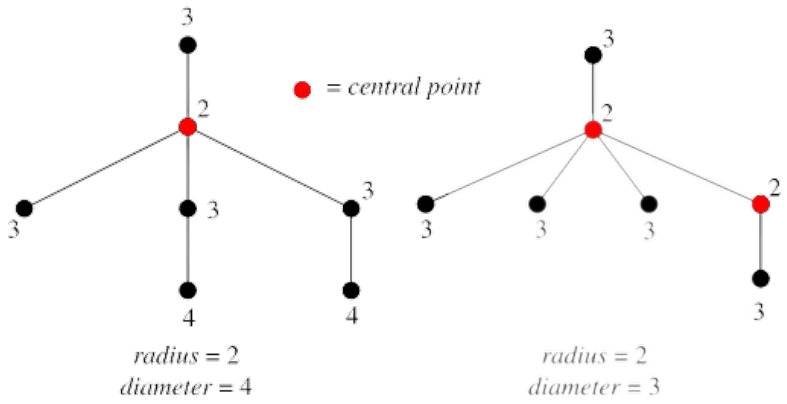
Or,

If $r(V) = e(V)$, then V is the central point of the graph G.

2.2.6 CENTRE OF A GRAPH

The set of all the central point of the graph is known as centre of the graph.

2.2.7 EXAMPLE



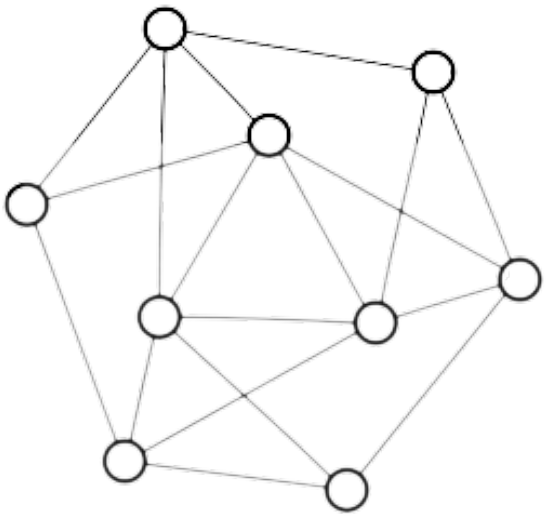
2.2.8 CIRCUMFERENCE OF A GRAPH

The total number of edges in the longest cycle of graph G is known as the circumference of G.

2.2.9 GIRTH

The total number of edges in the shortest cycle of graph G is known as girth.
It is denoted by $g(G)$.

2.2.10 EXAMPLE



For the above graph,

- Order $= 9$.
- Size (number of edges) $= 18$.
- Radius $= 2$.
- Circumference $= 9$.
- Girth $= 3$.

CHAPTER 3

THE FIRST THEOREM OF GRAPH THEORY

3.1 THE FIRST THEOREM

Theorem 3.1.1. *For any graph G with e edges and n vertices: $v_1, v_2, ..., v_n$,*

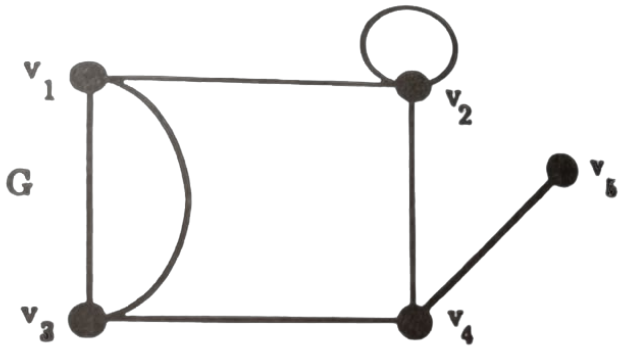
$$\sum_{i=1}^{n} d(v_i) = 2e \tag{3.1}$$

ie, In a graph G, the sum of the degrees of the vertices is equal to twice the number of edges.

Proof.

Each edge, since it has two end vertices, contributes precisely 2 to the sum of the degrees, i.e, when the degrees of the vertices are summed, each edge is counted twice.
□

3.1.1 EXAMPLE



In the above graph, we have,

1. $d(v_1) = 3$
2. $d(v_2) = 4$
3. $d(v_3) = 3$
4. $d(v_4) = 3$
5. $d(v_5) = 1$
6. Number of edges, $e = 7$.

Then,

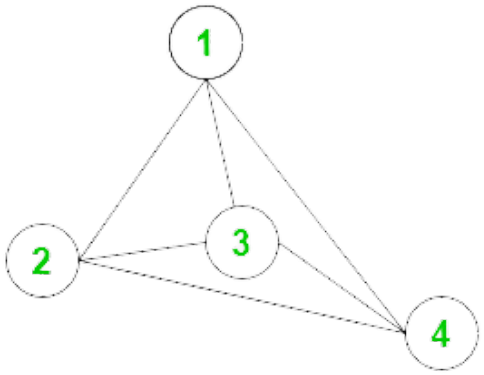
$$d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) = 14 = 2 \times e \tag{3.2}$$

i.e.,

$$\sum_{i=1}^{5} d(v_i) = 2 \times 7 = 14 \tag{3.3}$$

Remark 1. *A vertex of a graph is called odd or even depending on whether its degree is odd or even.*

EXAMPLE:



Here, the vertex degrees are:

1. $d(1) = 3$
2. $d(2) = 3$
3. $d(3) = 3$
4. $d(4) = 3$

Hence, all the vertices here are called odd vertices.

Corollary 3.1.1.1. *In a graph G, there is an even number of odd vertices.*

Proof. Let W be the set of odd vertices of G and let U be the set of even vertices of G.
Then, for each $u \in U$, $d(u)$ is even.
Also,

$$\sum_{u \in U} d(u),$$

being a sum of even numbers, is even.

However, by the previous theorem where V is the vertex set of G and e is the number of its edges,

$$\sum_{u \in U} d(u) + \sum_{w \in W} d(w) = \sum_{v \in V} d(v) = 2e. \tag{3.4}$$

Thus,

$$\sum_{w \in W} d(w) = 2e - \sum_{u \in U} d(u), \tag{3.5}$$

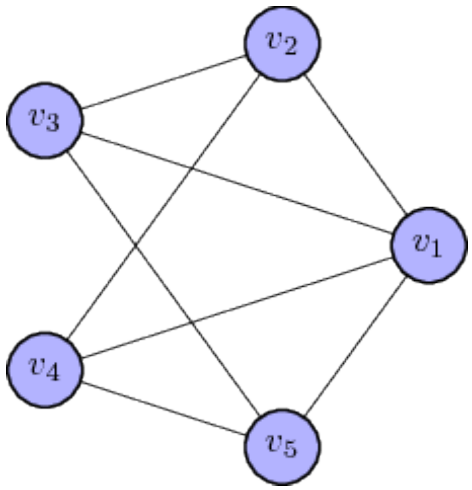
is even (being the difference of two even numbers).

As all the terms in:

$$\sum_{w \in W} d(w),$$

are odd and their sum is even, there must be an even number of them (because the sum of an odd number of odd numbers is odd).
□

EXAMPLE:

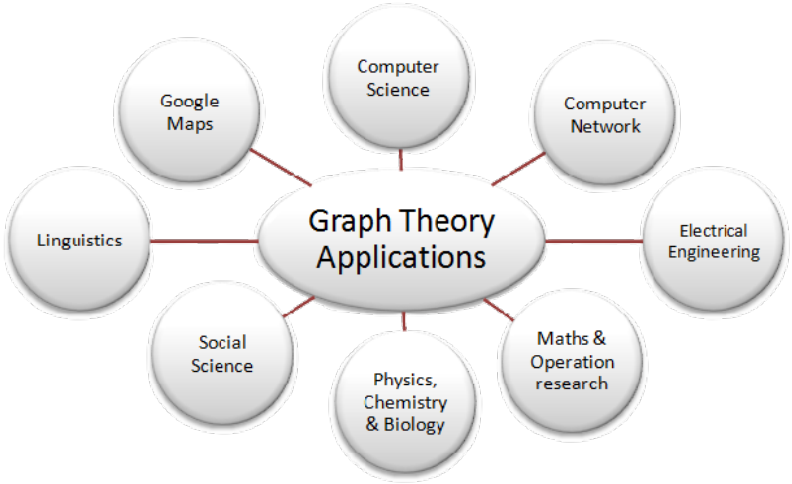


In the above graph, $d(v_1) = 4$, $d(v_2) = 3$, $d(v_3) = 3$, $d(v_4) = 3$ and $d(v_5) = 3$. Hence, out of the 5 vertices, v_2, v_3, v_4 and v_5 have odd degrees, i.e., there is an even number (4) of odd vertices.

CHAPTER 4

APPLICATIONS OF GRAPH THEORY

Graph Theory is used in vast area of science and technologies.



1. **COMPUTER SCIENCE**
   In computer science, graph theory is used for the study of algorithms like:

   - **Dijkstra's Algorithm** : Dijkstra's algorithm allows us to find the shortest path between any two vertices of a graph. This algorithm helps in finding the shortest paths between nodes in a graph, which may represent, for example, road networks.

- **Prim's Algorithm** : Prim's Algorithm is a greedy algorithm that is used to find the subset of edges that includes every vertex of the graph such that the sum of the weights of the edges can be minimized for a weighted undirected graph.
- **Kruskal's Algorithm**: Kruskal's Algorithm is used to discover the shortest path between two points in a connected weighted graph.

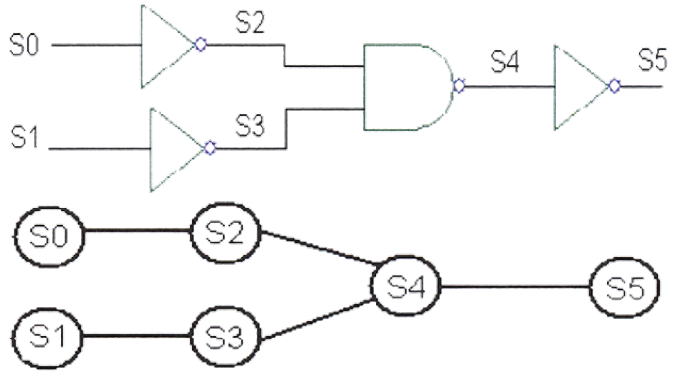
Moreover, graphs are used:

- To define the flow of computation.
- To represent networks of communication.
- To represent data organization.
- To find shortest path in road or a network.
- In Google Maps, various locations are represented as vertices or nodes and the roads are represented as edges and graph theory is used to find the shortest path between two nodes.

2. **ELECTRICAL ENGINEERING**

In Electrical Engineering, graph theory is used in designing of circuit connections. These circuit connections are named as topologies. Some topologies are series, bridge, star and parallel topologies.

EXAMPLE:



3. **LINGUISTICS**

- In linguistics, graphs are mostly used for parsing of a language tree and grammar of a language tree.
- Semantics networks are used within lexical semantics, especially as applied to computers, modeling word meaning is easier when a given word is understood in terms of related words.
- Methods in phonology (e.g. theory of optimality, which uses lattice graphs) and morphology (e.g. morphology of finite - state, using finite-state transducers) are common in the analysis of language as a graph.

4. **PHYSICS AND CHEMISTRY**

- In physics and chemistry, graph theory is used to study molecules.
- The 3D structure of complicated simulated atomic structures can be studied quantitatively by gathering statistics on graph-theoretic properties related to the topology of the atoms.
- Statistical physics also uses graphs. In this field graphs can represent local connections between interacting parts of a system, as well as the dynamics of a physical process on such systems.
- Graphs are also used to express the micro-scale channels of porous media, in which the vertices represent the pores and the edges represent the smaller channels connecting the pores.
- Graph is also helpful in constructing the molecular structure as well as lattice of the molecule. It also helps us to show the bond relation in between atoms and molecules, also help in comparing structure of one molecule to other.

5. **COMPUTER NETWORK**

- In computer network, the relationships among interconnected computers within the network, follow the principles of graph theory.
- Graph theory is widely used in modeling and routing in networks.
- Graph theory is also used in network security.

6. **SOCIAL SCIENCES**

- Graph theory is also used in sociology. For example, to explore rumor spreading, or to measure actors' prestige notably through the use of social network analysis software.
- Acquaintanceship and friendship graphs describe whether people know each other or not.
- In influence graphs model, certain people can influence the behavior of others.
- In collaboration graphs model to check whether two people work together in a particular way, such as acting in a movie together.

7. **BIOLOGY**

- Nodes in biological networks represent bio-molecules such as genes, proteins or metabolites, and edges connecting these nodes indicate functional, physical or chemical interactions between the corresponding bio-molecules.
- Graph theory is used in transcriptional regulation networks.
- It is also used in Metabolic networks.
- In PPI (Protein - Protein interaction) networks graph theory is also useful.
- Characterizing drug - drug target relationships.

8. **MATHEMATICS**

In mathematics, operational research is the important field. Graph theory provides many useful applications in operational research like:

- Minimum cost path.
- A scheduling problem.

9. **MISCELLANEOUS**

Graphs are used to represent the routes between the cities. With the help of tree that is a type of graph, we can create hierarchical ordered information such as family tree.

CONCLUSION

Graph theory has delivered important scientific discoveries, such as improved understanding of breakdown of electricity distribution systems or the propagation of infections in social networks, till date.

Graph theory also provides a remarkably simple way to characterize the complexity of ecological networks. Indices such as connectance, degree distribution or network topology serve as basic measurements to describe their structure. Such indices facilitate comparison between different systems and revealing commonalities and variations. Nowadays, the relatively important number of network studies leads to a myriads of ways to sample, analyze and interpret them.

Graph theory is an exceptionally rich area for programmers and designers. Graphs can be used to solve some very complex problems, such as least cost routing, mapping, program analysis, and so on. Network devices, such as routers and switches, use graphs to calculate optimal routing for traffic.

Graph theory is rapidly moving into the mainstream of mathematics mainly because of its applications in diverse fields which include biochemistry (genomics), electrical engineering (communications networks and coding theory), computer science (algorithms and computations) and operations research (scheduling).

Hence, studying graphs through a framework provides answers to many arrangement, networking, optimization, matching and operational problems. Graphs can be used to model many types of relations and processes in physical, biological, social and information systems, and has a wide range of useful applications.

BIBLIOGRAPHY

1. J. Clark and D. A. Holton, ***A First Look at Graph Theory***, World Scientific Publishing, 1991, 1-31, 47-51.

2. Wilson, J Robin, ***An Introduction To Graph Theory***, Addison Wesley Longman Ltd, 4th ed, 1972.

3. Javapoint, *Types of Graphs*, ***<https://www.javatpoint.com/graph-theory-types-of-graphs>***

4. Javapoint, *Tree and Forest*, ***<https://www.javatpoint.com/graph-theory-tree-and-forest>***

5. Javapoint, *Basic Properties of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-basic-properties>***

6. Programiz, *Dijkstra's Algorithm*, ***<https://www.programiz.com/dsa/dijkstra-algorithm>***

7. Javapoint, *Applications of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-applications>***

8. Britannica, *Graph Theory*, ***<https://www.britannica.com/topic/graph-theory>***

AN INTRODUCTION TO GRAPH THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

LAKSHMI DILEEP
DB20CMSR13

under the guidance of
Ms. Remya Raj

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty

March 2023

Examiner 1 **Examiner 2**

CERTIFICATE

This is to certify that **"An Introduction To Graph Theory"** is a bona fide project of **Lakshmi Dileep**, Register Number: **DB20CMSR13** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Ms. Remya Raj
Project Supervisor

DECLARATION

I, Lakshmi Dileep, hereby declare that the project: "An Introduction To Graph Theory" is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

Lakshmi Dileep

DB20CMSR13

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that had helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thank you for all your encouragement.

CONTENTS

INTRODUCTION

In mathematics, graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. Graph theory is a delightful playground for the exploration of proof techniques in Discrete Mathematics. The results of graph theory have applications in many areas of the computing, social and natural sciences. One of the beauties of graph theory is that it depends very little on other branches of mathematics. The subject of graph theory had its beginnings in recreational math problems but it has grown into a significant area of mathematical research, with applications in chemistry, operations research, social sciences, and computer science.

Graph Theory can model and study many real-world problems and is applied in a wide range of disciplines. In computer science, graph theory is used to model networks and communications as seen in the case of Google search, Google Maps and social media. Furthermore, graph theory is used in chemistry to model molecules and in biology to study genomes. It is even used in linguistics and social sciences. Using graph theory in Machine Learning and neural network is also one of the new trends.

The history of graph theory may be specifically traced to 1735, when the Swiss mathematician Leonhard Euler solved the Königsberg bridge problem. The Königsberg bridge problem was an old puzzle concerning the possibility of finding a path over every one of seven bridges that span a forked river flowing past an island—but without crossing any bridge twice. Euler argued that no such path exists since in Königsberg, the four land masses were connected by an odd number of bridges, it was impossible to draw the desired route. His proof involved only references to the physical arrangement of the bridges, but essentially he proved the first theorem in graph theory.

CHAPTER 1

BASIC CONCEPTS IN GRAPH THEORY

1.1 GRAPH

A graph G = (V(G),E(G)) consists of two finite sets:

i The vertex set of the graph, denoted by V(G) or V, which is a non-empty set of elements called vertices,

ii The edge set of the graph, denoted by E(G) or E, which is a possible empty set of elements called edges,

such that each edge e in E is assigned an unordered pair of vertices (u,v) called the end vertices of e.

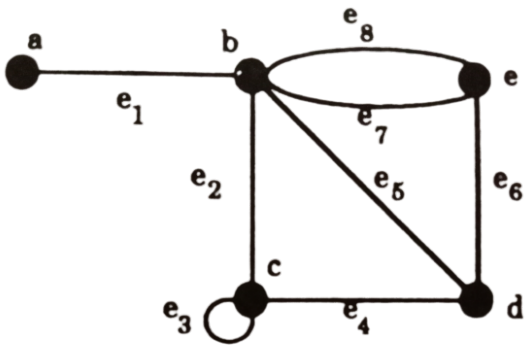
Vertices of a graph are also known as nodes or points while edges are also called links or lines.

1.1.1 EXAMPLE

Let G = (V,E) where V = $\{a, b, c, d, e\}$, E = $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$, and the ends of edges are given by:

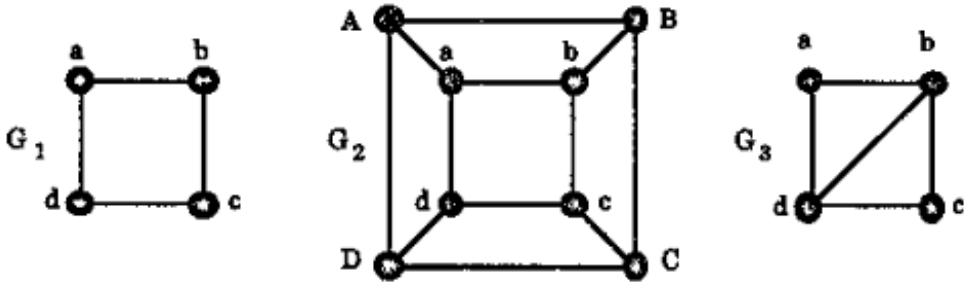
$e_1 \longleftrightarrow (a, b)$ $e_2 \longleftrightarrow (b, c)$ $e_3 \longleftrightarrow (c, c)$ $e_4 \longleftrightarrow (c, d)$ $e_5 \longleftrightarrow (b, d)$
$e_6 \longleftrightarrow (d, e)$ $e_7 \longleftrightarrow (b, e)$ $e_8 \longleftrightarrow (b, e)$.

Then, G can be represented diagrammatically as:



1.2 SUBGRAPHS

Let H be a graph with vertex set $V(H)$ and edge set $E(H)$ and similarly, let G be a graph with vertex set $V(G)$ and edge set $E(G)$. Then we say that H is a subgraph of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. In such a case, we also say that G is a supergraph of H.

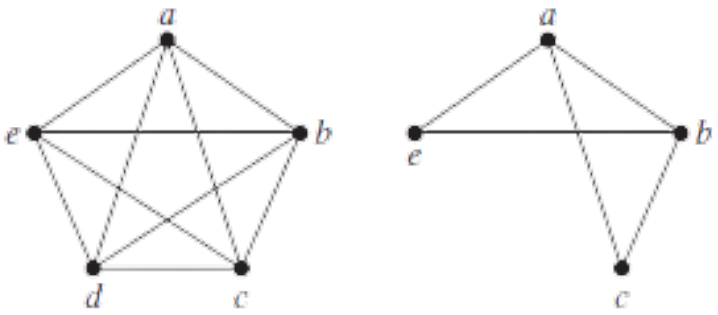


In the above example, G_1 is a subgraph of both G_2 and G_3. But, G_3 is not a subgraph of G_2.

1.2.1 PROPER SUBGRAPH

If H is a subgraph of G then we write: $H \subseteq G$. When $H \subseteq G$ but $H \neq G$, i.e., $V(H) \neq V(G)$ or $E(H) \neq E(G)$, then H is called a proper subgraph of G.

1.2.2 EXAMPLE

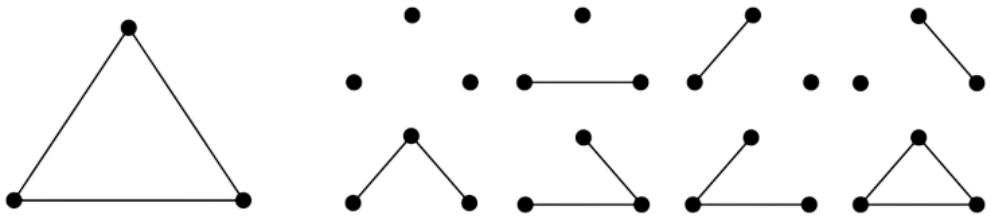


A Subgraph of K_5.

1.2.3 SPANNING SUBGRAPH

A spanning subgraph of a graph G is a subgraph H with $V(H) = V(G)$, i.e., H and G have exactly the same vertex set.

1.2.4 EXAMPLE



the graph C_3

spanning subgraphs of C_3

1.3 SOME DEFINITIONS

Definition 1.1. ***LOOP***

An edge for which two end vertices are the same is called a loop.

Definition 1.2. ***PARALLEL EDGES***

If two or more edges of G have the same end vertices, these edges are called multiple or parallel edges.

Definition 1.3. ***INCIDENT EDGE***

Any edge is said to be incident to the vertices connected by the edge.

Definition 1.4. ***ADJACENT VERTEX***

A vertex is said to be adjacent to other vertices if it has an edge connecting it to the vertices.

Definition 1.5. ***ISOLATED VERTEX***

Any vertex without any edges coming in or out of it is called an isolated vertex.

Definition 1.6. ***VERTEX DEGREES***

Let v be a vertex of a graph G. The degree $d(v)$ of v is the number of edges of G incident with v, counting each loop twice, i.e., it is the number of times v is an end vertex of an edge.

Definition 1.7. ***BIPARTITION***

Let G be a graph. If the vertex set V of G can be partitioned into two non-empty subsets X and Y in such a way that each edge of G has one end in X and one end in Y, then G is called bipartite.
The partition V is called a bipartition of G.

1.4 PATHS, CYCLES AND TREES

1.4.1 WALK

A walk in a graph G is a finite sequence:

$$W = v_0 e_1 v_1 e_2 v_2 ... v_{k-1} e_k v_k \tag{1.1}$$

whose terms are alternatively vertices and edges such that, for $1 \leq i \leq k$, the edge e_i has ends v_{i-1} and v_i. Thus, each edge e_i is immediately preceded and succeeded by the two vertices with which it is incident.

The walk W in (2.1) is a $v_0 - v_k$ walk, or, a walk from v_0 to v_k. The vertex v_0 is called the ***origin*** of the walk while v_k is called the ***terminus*** of W. (v_0 and v_k need not be distinct.)
The vertices v_1, v_2,...,v_{k-1}, in a walk W are called its ***internal vertices***. The integer k, the number of edges in the walk, is called the ***length*** of W.

1.4.2 TRIVIAL WALK

A trivial walk is a walk containing no edges.
Thus, for any vertex v of a graph G,

$$W = v$$

gives a trivial walk. It has length 0.

1.4.3 CLOSED AND OPEN WALK

For two given vertices u and v of a graph G, a $u - v$ walk is said to be ***closed*** or ***open*** depending on whether $u = v$ or $u \neq v$.

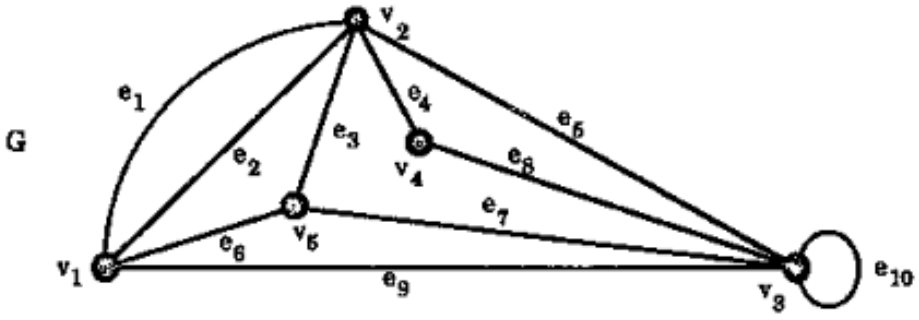
1.4.4 TRAIL

If the edges $e_1, e_2, ..., e_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k v_k$ are distinct, W is called a ***trail***.

1.4.5 PATH

If the vertices $v_0, v_1, ..., v_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k\, v_k$ are distinct then W is called a ***path***.
A path with n vertices is sometimes denoted by P_n and it has length $n - 1$.

1.4.6 EXAMPLE



Let the above graph G be such that the walks W_1, W_2, W_3, W_4 be defined as:

- $W_1 = v_1\, e_1\, v_2\, e_5\, v_3\, e_{10}\, v_3\, e_5\, v_2\, e_3\, v_5$
- $W_2 = v_1\, e_1\, v_2\, e_1\, v_1\, e_1\, v_2$
- $W_3 = v_1\, v_5\, v_2\, v_4\, v_3\, v_1$
- $W_4 = v_2\, v_4\, v_3\, v_5\, v_1$

Here, the length of:

1. $W_1 = 5$
2. $W_2 = 3$
3. $W_3 = 5$
4. $W_4 = 4$.

Then,

1. W_1, W_2 and W_4 are open walks while W_3 is a closed walk.
2. W_3, W_4 are trails but W_1 and W_2 aren't.
3. W_4 is a path but W_1, W_2 and W_3 aren't.

Theorem 1.4.1. *Given any two vertices u and v of a graph G, every $u-v$ walk contains a $u-v$ path,*
i.e., given any walk,

$$W = u\, e_1\, v_1 ... v_{k-1}\, e_k\, v$$

then, after some deletion of vertices and edges if necessary, we can find a sub-sequence P of W which is a $u-v$ path.

Proof. If $u = v$, i.e.,if W is closed, then the trivial path $P = u$ will do.

Now suppose $u \neq v$,i.e.,W is open and let the vertices of W be given, in order, by:

$$u = u_0, u_1, u_2, ..., u_{k-1}, u_k = v.$$

If none of the vertices of G occurs in W more than once, then W is already a $u-v$ path and so we are finished by taking $P = W$.

So now suppose that there are vertices of G that occur in W twice or more. Then there are distinct i, j with $i < j$, say, such that $u_i = u_j$. If the terms $u_i, u_{i+1}, ..., u_{j-1}$ (and the preceding edges) are deleted from W then we obtain a $u-v$ walk W_1 having fewer vertices than W. If there is no repetition of vertices in W_1, then W_1 is a $u-v$ path and setting $P = W_1$ finishes the proof.
If this is not the case, then we repeat the above deletion procedure until finally arriving at a $u-v$ walk that is a path, as required. □

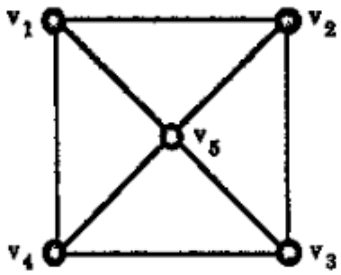
1.4.7 CYCLE

A non-trivial closed trail in a graph G is called a cycle if its origin and internal vertices are distinct i.e.,
A cycle in a graph is a non-empty trail in which only the first and last vertices are equal.

A cycle of length k is called a $k-cycle$. A $k-cycle$ is called odd or even depending on whether k is odd or even.

A $3-cycle$ is often called a triangle. An $n-cycle$, i.e., a cycle with n vertices, will sometimes be denoted by C_n.

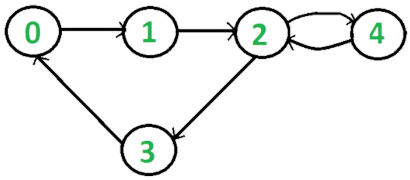
EXAMPLE 1:



In the above example,

1. C = $v_1\, v_2\, v_3\, v_4\, v_1$ is a 4-cycle.
2. $T = v_1\, v_2\, v_5\, v_3\, v_4\, v_5\, v_1$ in a non-trivial closed trail which is not a cycle since v_5 occurs twice as an internal vertex.
3. C_1 = $v_1\, v_2\, v_5\, v_1$ is a triangle.

EXAMPLE 2:

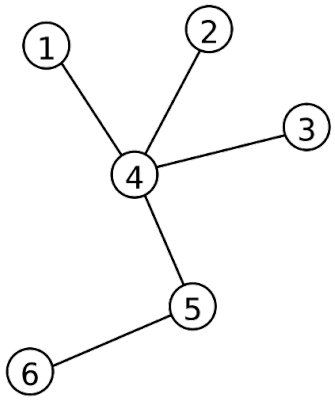


Here, $0 \to 1 \to 2 \to 3 \to 0$ is a 4-cycle but $0 \to 1 \to 2 \to 4 \to 2 \to 3 \to 0$ is not a cycle since the vertex 2, an internal vertex, occurs twice.

1.4.8 TREES

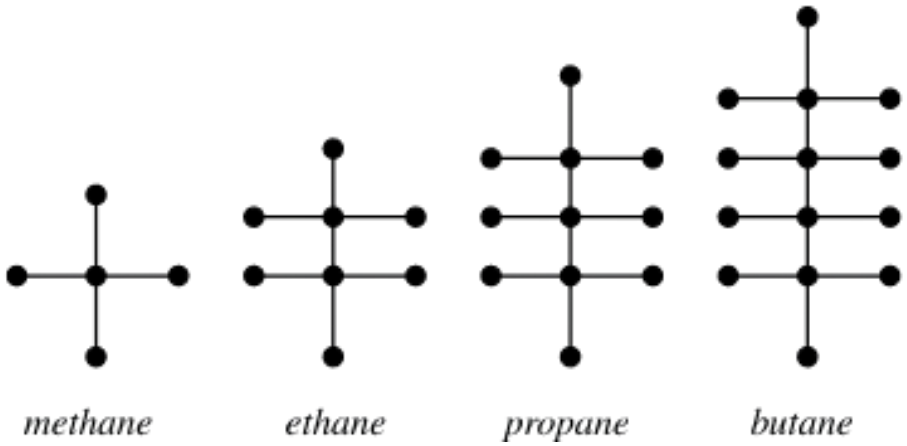
A graph G is called ***acyclic*** if it contains no cycles.
A graph G is called a ***tree*** if it is a connected acyclic graph, i.e., A tree is an undirected graph in which any two vertices are connected by exactly one path.

EXAMPLE 1:



The above graph is an undirected connected acyclic graph and thus, a tree.

EXAMPLE 2:



The above example shows the representation of the first four hydrocarbons as trees.

CHAPTER 2

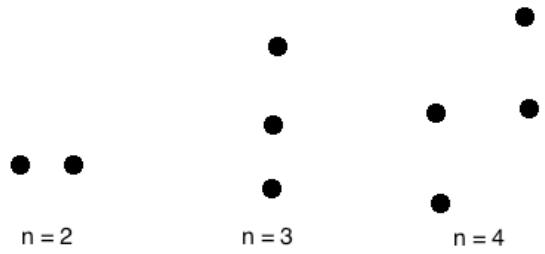
TYPES AND PROPERTIES OF GRAPHS

2.1 TYPES OF GRAPHS

Definition 2.1. ***NULL GRAPH***

A null graph is a graph in which there are no edges between its vertices. A null graph is also called empty graph.

EXAMPLE:



In all the above graphs, there are no edges between the vertices.

Definition 2.2. ***TRIVIAL GRAPH***

A trivial graph is the graph which has only one vertex.

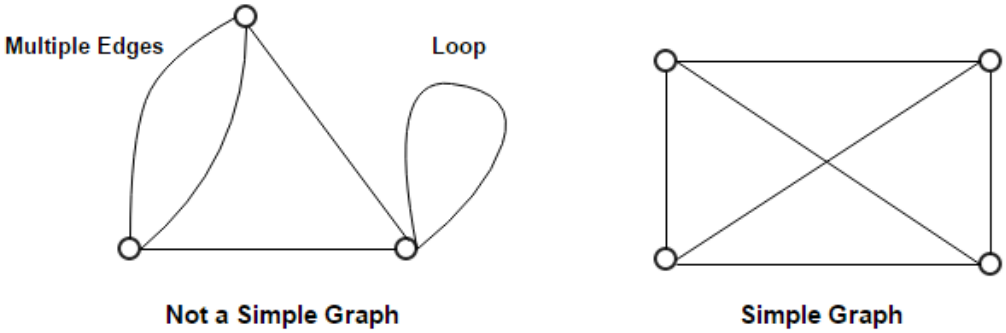
EXAMPLE:

In the above graph, there is only one vertex 'v' without any edge. Therefore, it is a trivial graph.

Definition 2.3. ***SIMPLE GRAPH***

A simple graph is the undirected graph with no parallel edges and no loops. A simple graph which has n vertices, the degree of every vertex is at most $n-1$.

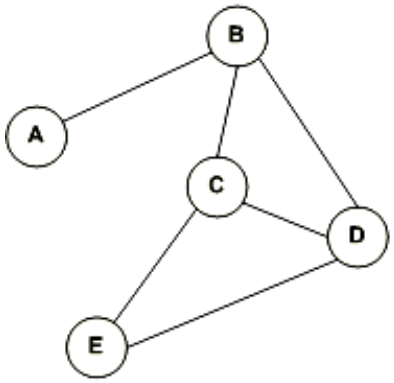
EXAMPLE:



Definition 2.4. ***UNDIRECTED GRAPH***

An undirected graph is a graph whose edges are not directed. The relations between pairs of vertices in an undirected graph are symmetric, so that each edge has no directional character. They only represent whether or not a relationship exists between two vertices. Thus, all the edges in an undirected graph are bidirectional.

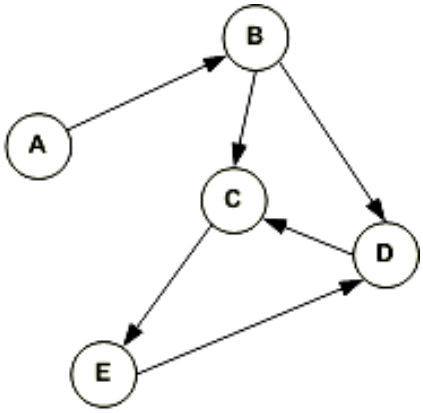
EXAMPLE:



Definition 2.5. ***DIRECTED GRAPH***

A directed graph is a graph in which the edges are directed by arrows.
Directed graphs are also known as digraphs.

EXAMPLE:

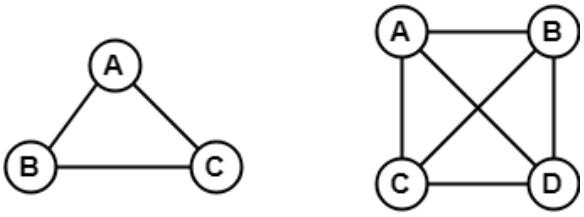


In the above graph, each edge is directed by the arrow. A directed edge has an arrow from A to B means A is related to B but B is not related to A.

Definition 2.6. ***COMPLETE GRAPH***

A graph in which every pair of vertices is joined by exactly one edge is called complete graph. It contains all possible edges.
A complete graph with n vertices contains exactly $\binom{n}{2}$ *edges.*

EXAMPLE:

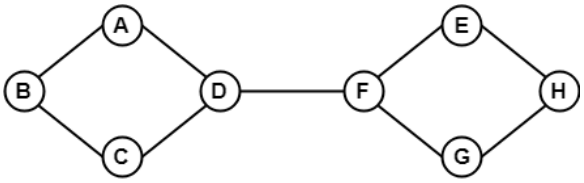


In the above example, since each vertex in the graph is connected with all the remaining vertices through exactly one edge, both are complete graphs.

Definition 2.7. ***CONNECTED GRAPH***

A connected graph is a graph in which we can visit from any one vertex to any other vertex. In a connected graph, at least one edge or path exists between every pair of vertices.

EXAMPLE:

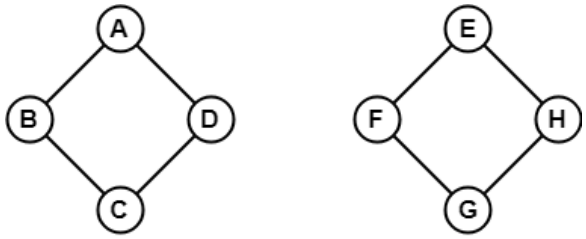


In the above example, we can traverse from any one vertex to any other vertex. It means there exists at least one path between every pair of vertices therefore, it a connected graph.

Definition 2.8. ***DISCONNECTED GRAPH***

A disconnected graph is a graph in which any path does not exist between every pair of vertices.

EXAMPLE:

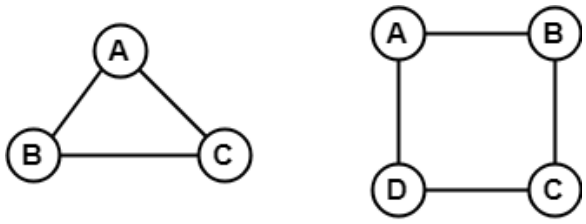


The above graph consists of two independent components which are disconnected. Since it is not possible to visit from the vertices of one component to the vertices of other components, it is a disconnected graph.

Definition 2.9. ***REGULAR GRAPH***

A regular graph is a graph in which degree of all the vertices is same.
If the degree of all the vertices is k*, then it is called* $k - regulargraph$*.*

EXAMPLE:



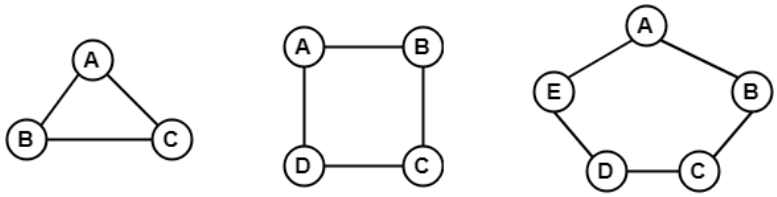
In the above example, all the vertices have degree 2*. Therefore they are called* $2 - Regulargraph$*.*

Definition 2.10. ***CYCLIC GRAPH***

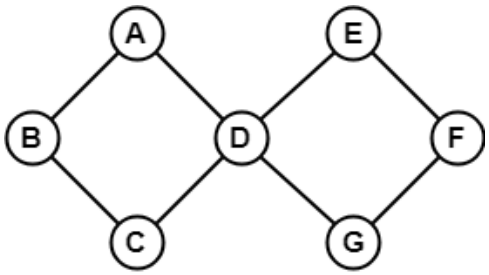
A graph with n vertices (where $n >= 3$) and n edges forming a cycle of n with all its edges is known as cycle graph.
In the cycle graph, degree of each vertex is 2.

A graph containing at least one cycle in it is known as a cyclic graph.

EXAMPLE:



In the above example, all the vertices have degree 2. Therefore they all are cyclic graphs.

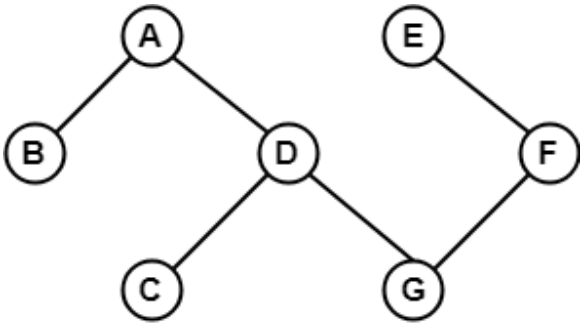


The above graph contains two cycles in it and therefore it is a cyclic graph.

Definition 2.11. ***ACYCLIC GRAPH***

A graph which does not contain any cycle in it is called as an acyclic graph.

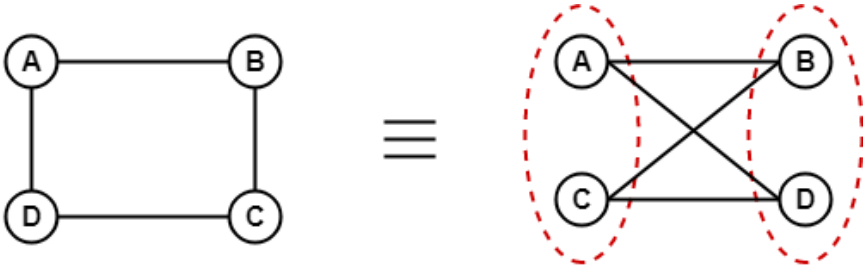
EXAMPLE:



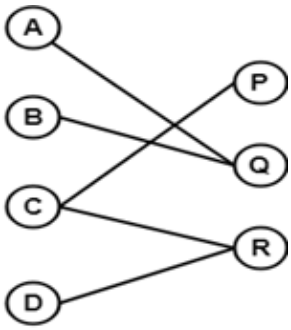
Definition 2.12. ***BIPARTITE GRAPH***

A bipartite graph is a graph in which the vertex set can be partitioned into two sets such that edges only go between sets, not within them.
A graph $G(V, E)$ is called bipartite graph if its vertex-set $V(G)$ can be decomposed into two non-empty disjoint subsets $V_1(G)$ and $V_2(G)$ in such a way that each edge $e \in E(G)$ has its one last joint in $V_1(G)$ and other last point in $V_2(G)$.
The partition $V = V1 \cup V2$ is known as bipartition of G.

EXAMPLE 1:



EXAMPLE 2:

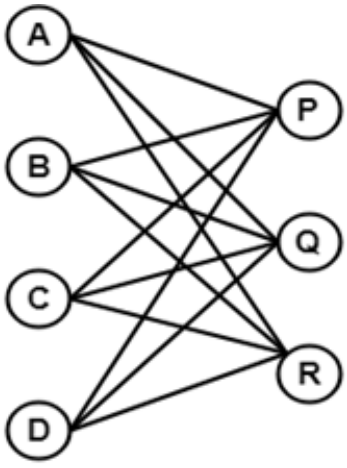


Definition 2.13. ***COMPLETE BIPARTITE GRAPH***

A complete bipartite graph is a bipartite graph in which each vertex in the first set is joined to each vertex in the second set by exactly one edge.
A complete bipartite graph is a bipartite graph which is complete.

$$Complete\,Bipartite\,Graph = Bipartite\,Graph + Complete\,Graph \quad (2.1)$$

EXAMPLE:

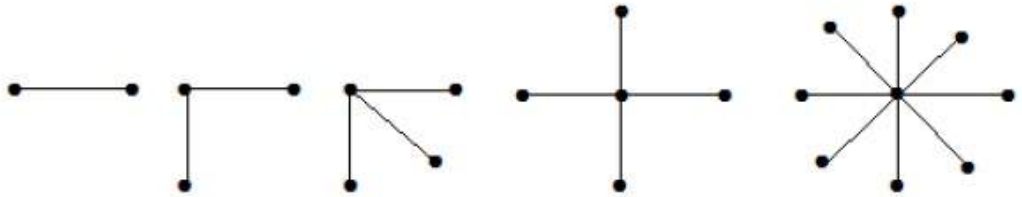


The above graph is known as $K_{4,3}$

Definition 2.14. ***STAR GRAPH***

A star graph is a complete bipartite graph in which $n-1$ vertices have degree 1 and a single vertex has degree $(n-1)$. This exactly looks like a star where $(n-1)$ vertices are connected to a single central vertex.
A star graph with n vertices is denoted by S_n.

EXAMPLE:

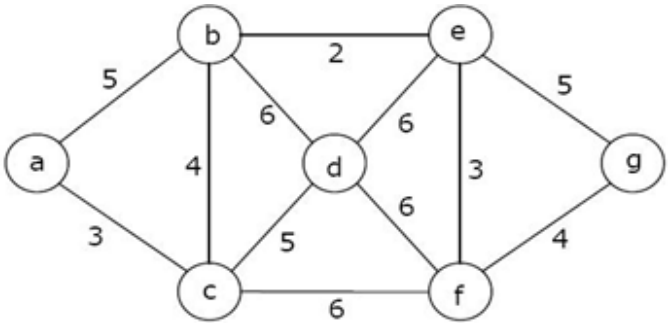


In the above example, out of n vertices, all the $(n-1)$ vertices are connected to a single vertex. Hence, it is a star graph.

Definition 2.15. ***WEIGHTED GRAPH***

A weighted graph is a graph whose edges have been labeled with some weights or numbers.
The length of a path in a weighted graph is the sum of the weights of all the edges in the path.

EXAMPLE:



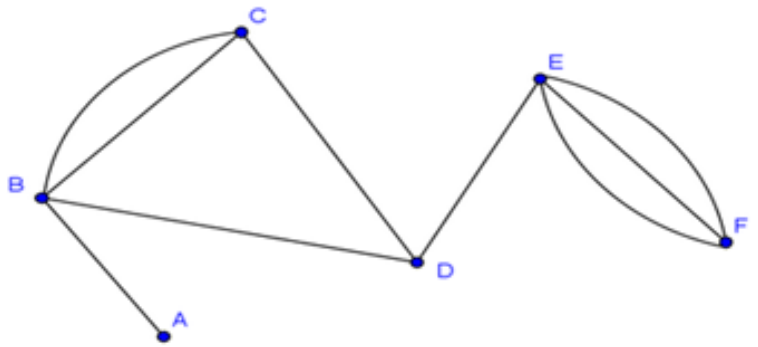
In the above graph, if the path chosen is $a \to b \to c \to d \to e \to g$ *then the length of the path is :*

$$5 + 4 + 5 + 6 + 5 = 25.$$

Definition 2.16. ***MULTI GRAPH***

A graph in which there are multiple edges between any pair of vertices or there are edges from a vertex to itself (loop) is called a multi - graph.

EXAMPLE:

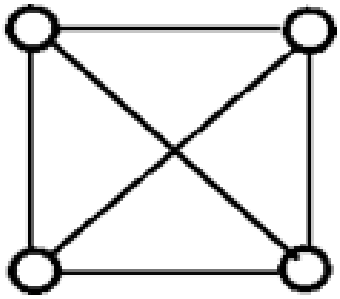


In the above graph, vertex-set B *and* C *are connected with two edges. Similarly, vertex sets* E *and* F *are connected with* 3 *edges. Therefore, it is a multi graph.*

Definition 2.17. ***PLANAR GRAPH***

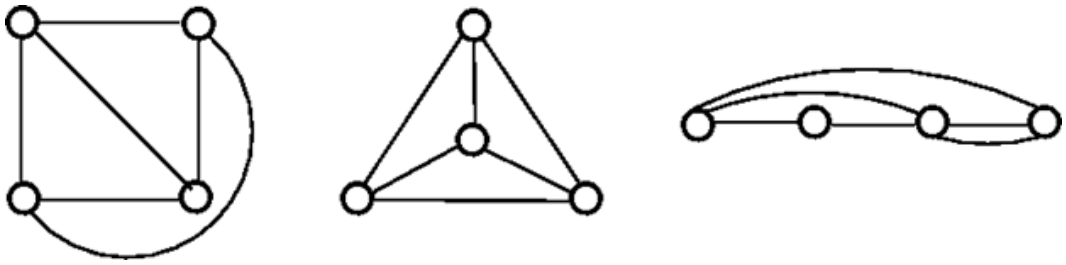
A planar graph is a graph that we can draw in a plane in such a way that no two edges of it cross each other except at a vertex to which they are incident,
i.e., A planar graph is a graph that can be embedded in the plane such that its edges intersect only at their endpoints.

EXAMPLE:



The above graph may not seem to be planar because it has edges crossing each other. But we can redraw the above graph.

The three plane drawings of the above graph are:



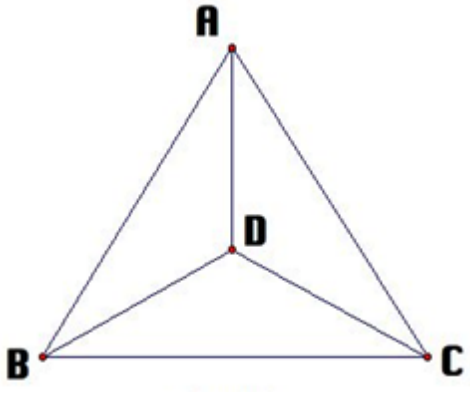
The above three graphs do not consist of two edges crossing each other and therefore, all the above graphs are planar.

2.2 PROPERTIES OF GRAPHS

2.2.1 DISTANCE BETWEEN TWO VERTICES

Distance is basically the number of edges in a shortest path between vertex X and vertex Y. If there are many paths connecting two vertices, then the shortest path is considered as the distance between the two vertices.
Distance between any two vertices X and Y is denoted by $d(X, Y)$.

EXAMPLE:



Suppose, we want to find the distance between vertex B and D. Then, first of all, we have to find the shortest path between vertex B and D.
There are many paths from vertex B to vertex D:

- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Here, length = 3
- B $\rightarrow$ D. Length = 1 (Shortest Path)
- B $\rightarrow$ A $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Length = 3

Hence, the minimum distance between vertex B and vertex D is 1.

2.2.2 ECCENTRICITY OF A VERTEX

Eccentricity of a vertex is the maximum distance between a vertex to all other vertices. It is denoted by $e(V)$.
For a disconnected graph, all vertices are defined to have infinite eccentricity.

2.2.3 RADIUS OF CONNECTED GRAPHS

The radius of a connected graph is the minimum eccentricity from all the vertices. In other words, the minimum among all the distances between a vertex to all other vertices is called as the radius of the graph.
It is denoted by $r(G)$.

2.2.4 DIAMETER OF A GRAPH

Diameter of a graph is the maximum eccentricity from all the vertices. In other words, the maximum among all the distances between a vertex to all other vertices is considered as the diameter of the graph G.
It is denoted by $d(G)$.

2.2.5 CENTRAL POINT

If the eccentricity of the graph is equal to its radius, then it is known as central point of the graph,

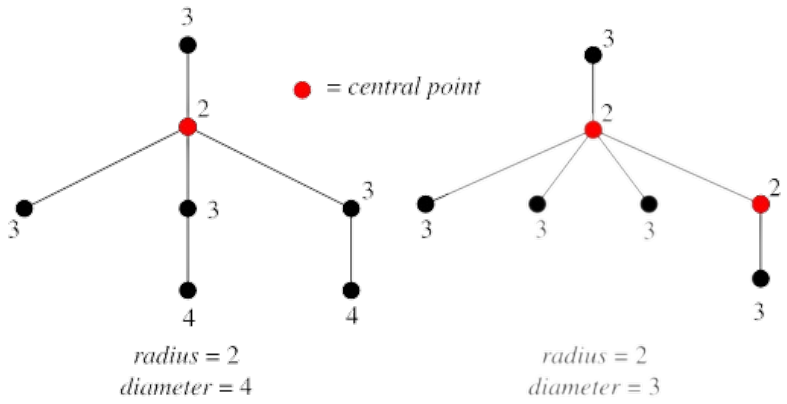
Or,

If $r(V) = e(V)$, then V is the central point of the graph G.

2.2.6 CENTRE OF A GRAPH

The set of all the central point of the graph is known as centre of the graph.

2.2.7 EXAMPLE



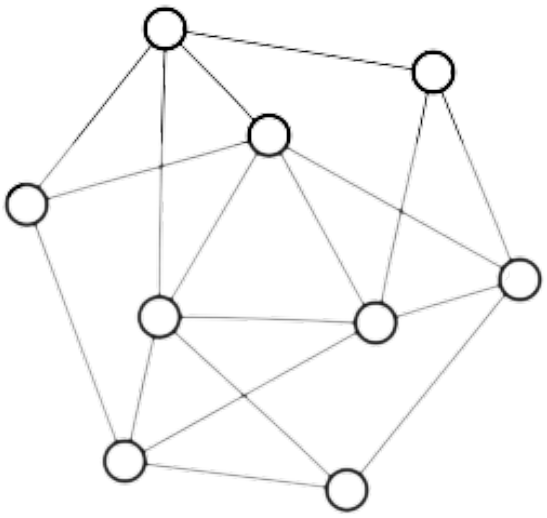
2.2.8 CIRCUMFERENCE OF A GRAPH

The total number of edges in the longest cycle of graph G is known as the circumference of G.

2.2.9 GIRTH

The total number of edges in the shortest cycle of graph G is known as girth.
It is denoted by $g(G)$.

2.2.10 EXAMPLE



For the above graph,

- Order $= 9$.
- Size (number of edges) $= 18$.
- Radius $= 2$.
- Circumference $= 9$.
- Girth $= 3$.

CHAPTER 3

THE FIRST THEOREM OF GRAPH THEORY

3.1 THE FIRST THEOREM

Theorem 3.1.1. *For any graph G with e edges and n vertices: $v_1, v_2, ..., v_n$,*

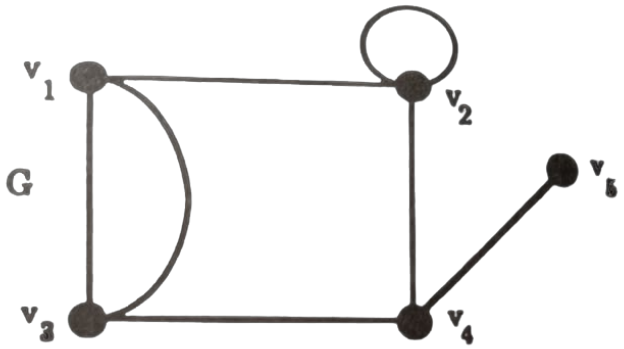
$$\sum_{i=1}^{n} d(v_i) = 2e \tag{3.1}$$

ie, In a graph G, the sum of the degrees of the vertices is equal to twice the number of edges.

Proof.

Each edge, since it has two end vertices, contributes precisely 2 to the sum of the degrees, i.e, when the degrees of the vertices are summed, each edge is counted twice.
□

3.1.1 EXAMPLE



In the above graph, we have,

1. $d(v_1) = 3$
2. $d(v_2) = 4$
3. $d(v_3) = 3$
4. $d(v_4) = 3$
5. $d(v_5) = 1$
6. Number of edges, $e = 7$.

Then,

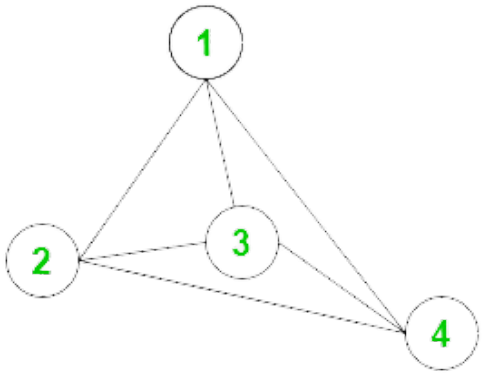
$$d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) = 14 = 2 \times e \tag{3.2}$$

i.e.,

$$\sum_{i=1}^{5} d(v_i) = 2 \times 7 = 14 \tag{3.3}$$

Remark 1. *A vertex of a graph is called odd or even depending on whether its degree is odd or even.*

EXAMPLE:



Here, the vertex degrees are:

1. $d(1) = 3$
2. $d(2) = 3$
3. $d(3) = 3$
4. $d(4) = 3$

Hence, all the vertices here are called odd vertices.

Corollary 3.1.1.1. *In a graph G, there is an even number of odd vertices.*

Proof. Let W be the set of odd vertices of G and let U be the set of even vertices of G.
Then, for each $u \in U$, $d(u)$ is even.
Also,

$$\sum_{u \in U} d(u),$$

being a sum of even numbers, is even.

However, by the previous theorem where V is the vertex set of G and e is the number of its edges,

$$\sum_{u \in U} d(u) + \sum_{w \in W} d(w) = \sum_{v \in V} d(v) = 2e. \tag{3.4}$$

Thus,

$$\sum_{w \in W} d(w) = 2e - \sum_{u \in U} d(u), \tag{3.5}$$

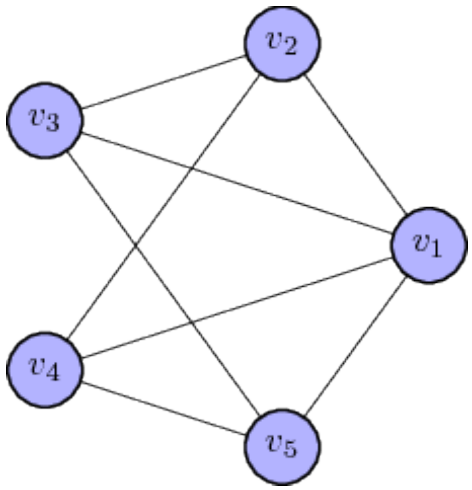
is even (being the difference of two even numbers).

As all the terms in:

$$\sum_{w \in W} d(w),$$

are odd and their sum is even, there must be an even number of them (because the sum of an odd number of odd numbers is odd).
□

EXAMPLE:

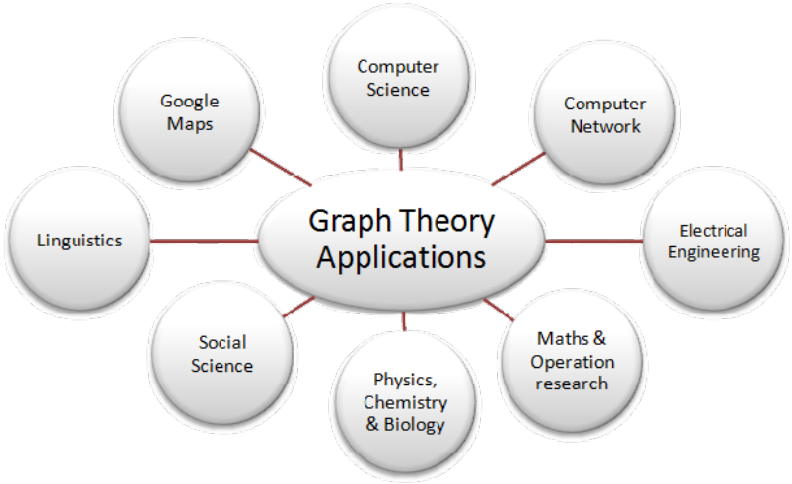


In the above graph, $d(v_1) = 4$, $d(v_2) = 3$, $d(v_3) = 3$, $d(v_4) = 3$ and $d(v_5) = 3$. Hence, out of the 5 vertices, v_2, v_3, v_4 and v_5 have odd degrees, i.e., there is an even number (4) of odd vertices.

CHAPTER 4

APPLICATIONS OF GRAPH THEORY

Graph Theory is used in vast area of science and technologies.



1. **COMPUTER SCIENCE**
   In computer science, graph theory is used for the study of algorithms like:

   - **Dijkstra's Algorithm** : Dijkstra's algorithm allows us to find the shortest path between any two vertices of a graph. This algorithm helps in finding the shortest paths between nodes in a graph, which may represent, for example, road networks.

- **Prim's Algorithm** : Prim's Algorithm is a greedy algorithm that is used to find the subset of edges that includes every vertex of the graph such that the sum of the weights of the edges can be minimized for a weighted undirected graph.
- **Kruskal's Algorithm**: Kruskal's Algorithm is used to discover the shortest path between two points in a connected weighted graph.

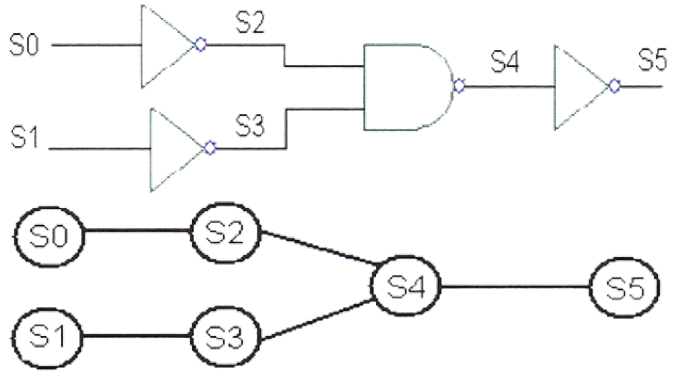
Moreover, graphs are used:

- To define the flow of computation.
- To represent networks of communication.
- To represent data organization.
- To find shortest path in road or a network.
- In Google Maps, various locations are represented as vertices or nodes and the roads are represented as edges and graph theory is used to find the shortest path between two nodes.

2. **ELECTRICAL ENGINEERING**

In Electrical Engineering, graph theory is used in designing of circuit connections. These circuit connections are named as topologies. Some topologies are series, bridge, star and parallel topologies.

EXAMPLE:



3. **LINGUISTICS**

- In linguistics, graphs are mostly used for parsing of a language tree and grammar of a language tree.
- Semantics networks are used within lexical semantics, especially as applied to computers, modeling word meaning is easier when a given word is understood in terms of related words.
- Methods in phonology (e.g. theory of optimality, which uses lattice graphs) and morphology (e.g. morphology of finite - state, using finite-state transducers) are common in the analysis of language as a graph.

4. **PHYSICS AND CHEMISTRY**

- In physics and chemistry, graph theory is used to study molecules.
- The 3D structure of complicated simulated atomic structures can be studied quantitatively by gathering statistics on graph-theoretic properties related to the topology of the atoms.
- Statistical physics also uses graphs. In this field graphs can represent local connections between interacting parts of a system, as well as the dynamics of a physical process on such systems.
- Graphs are also used to express the micro-scale channels of porous media, in which the vertices represent the pores and the edges represent the smaller channels connecting the pores.
- Graph is also helpful in constructing the molecular structure as well as lattice of the molecule. It also helps us to show the bond relation in between atoms and molecules, also help in comparing structure of one molecule to other.

5. **COMPUTER NETWORK**

- In computer network, the relationships among interconnected computers within the network, follow the principles of graph theory.
- Graph theory is widely used in modeling and routing in networks.
- Graph theory is also used in network security.

6. **SOCIAL SCIENCES**

- Graph theory is also used in sociology. For example, to explore rumor spreading, or to measure actors' prestige notably through the use of social network analysis software.
- Acquaintanceship and friendship graphs describe whether people know each other or not.
- In influence graphs model, certain people can influence the behavior of others.
- In collaboration graphs model to check whether two people work together in a particular way, such as acting in a movie together.

7. **BIOLOGY**

- Nodes in biological networks represent bio-molecules such as genes, proteins or metabolites, and edges connecting these nodes indicate functional, physical or chemical interactions between the corresponding bio-molecules.
- Graph theory is used in transcriptional regulation networks.
- It is also used in Metabolic networks.
- In PPI (Protein - Protein interaction) networks graph theory is also useful.
- Characterizing drug - drug target relationships.

8. **MATHEMATICS**

In mathematics, operational research is the important field. Graph theory provides many useful applications in operational research like:

- Minimum cost path.
- A scheduling problem.

9. **MISCELLANEOUS**

Graphs are used to represent the routes between the cities. With the help of tree that is a type of graph, we can create hierarchical ordered information such as family tree.

CONCLUSION

Graph theory has delivered important scientific discoveries, such as improved understanding of breakdown of electricity distribution systems or the propagation of infections in social networks, till date.

Graph theory also provides a remarkably simple way to characterize the complexity of ecological networks. Indices such as connectance, degree distribution or network topology serve as basic measurements to describe their structure. Such indices facilitate comparison between different systems and revealing commonalities and variations. Nowadays, the relatively important number of network studies leads to a myriads of ways to sample, analyze and interpret them.

Graph theory is an exceptionally rich area for programmers and designers. Graphs can be used to solve some very complex problems, such as least cost routing, mapping, program analysis, and so on. Network devices, such as routers and switches, use graphs to calculate optimal routing for traffic.

Graph theory is rapidly moving into the mainstream of mathematics mainly because of its applications in diverse fields which include biochemistry (genomics), electrical engineering (communications networks and coding theory), computer science (algorithms and computations) and operations research (scheduling).

Hence, studying graphs through a framework provides answers to many arrangement, networking, optimization, matching and operational problems. Graphs can be used to model many types of relations and processes in physical, biological, social and information systems, and has a wide range of useful applications.

BIBLIOGRAPHY

1. J. Clark and D. A. Holton, ***A First Look at Graph Theory***, World Scientific Publishing, 1991, 1-31, 47-51.

2. Wilson, J Robin, ***An Introduction To Graph Theory***, Addison Wesley Longman Ltd, 4th ed, 1972.

3. Javapoint, *Types of Graphs*, ***<https://www.javatpoint.com/graph-theory-types-of-graphs>***

4. Javapoint, *Tree and Forest*, ***<https://www.javatpoint.com/graph-theory-tree-and-forest>***

5. Javapoint, *Basic Properties of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-basic-properties>***

6. Programiz, *Dijkstra's Algorithm*, ***<https://www.programiz.com/dsa/dijkstra-algorithm>***

7. Javapoint, *Applications of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-applications>***

8. Britannica, *Graph Theory*, ***<https://www.britannica.com/topic/graph-theory>***

AN INTRODUCTION TO GRAPH THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

SANIKA TOM
DB20CMSR15

under the guidance of
Ms. Remya Raj

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty

March 2023

Examiner 1 **Examiner 2**

CERTIFICATE

This is to certify that **"An Introduction To Graph Theory"** is a bona fide project of **Sanika Tom**, Register Number: **DB20CMSR15** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Ms. Remya Raj
Project Supervisor

DECLARATION

I,Sanika Tom, hereby declare that the project: "An Introduction To Graph Theory" is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

Sanika Tom

DB20CMSR15

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that had helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thank you for all your encouragement.

CONTENTS

INTRODUCTION

In mathematics, graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. Graph theory is a delightful playground for the exploration of proof techniques in Discrete Mathematics. The results of graph theory have applications in many areas of the computing, social and natural sciences. One of the beauties of graph theory is that it depends very little on other branches of mathematics. The subject of graph theory had its beginnings in recreational math problems but it has grown into a significant area of mathematical research, with applications in chemistry, operations research, social sciences, and computer science.

Graph Theory can model and study many real-world problems and is applied in a wide range of disciplines. In computer science, graph theory is used to model networks and communications as seen in the case of Google search, Google Maps and social media. Furthermore, graph theory is used in chemistry to model molecules and in biology to study genomes. It is even used in linguistics and social sciences. Using graph theory in Machine Learning and neural network is also one of the new trends.

The history of graph theory may be specifically traced to 1735, when the Swiss mathematician Leonhard Euler solved the Königsberg bridge problem. The Königsberg bridge problem was an old puzzle concerning the possibility of finding a path over every one of seven bridges that span a forked river flowing past an island—but without crossing any bridge twice. Euler argued that no such path exists since in Königsberg, the four land masses were connected by an odd number of bridges, it was impossible to draw the desired route. His proof involved only references to the physical arrangement of the bridges, but essentially he proved the first theorem in graph theory.

CHAPTER 1

BASIC CONCEPTS IN GRAPH THEORY

1.1 GRAPH

A graph G = (V(G),E(G)) consists of two finite sets:

i The vertex set of the graph, denoted by V(G) or V, which is a non-empty set of elements called vertices,

ii The edge set of the graph, denoted by E(G) or E, which is a possible empty set of elements called edges,

such that each edge e in E is assigned an unordered pair of vertices (u,v) called the end vertices of e.

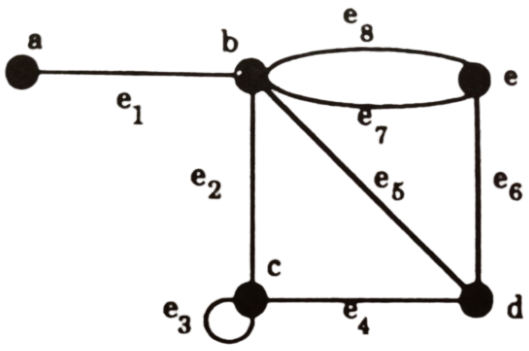
Vertices of a graph are also known as nodes or points while edges are also called links or lines.

1.1.1 EXAMPLE

Let G = (V,E) where V = $\{a, b, c, d, e\}$, E = $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$, and the ends of edges are given by:

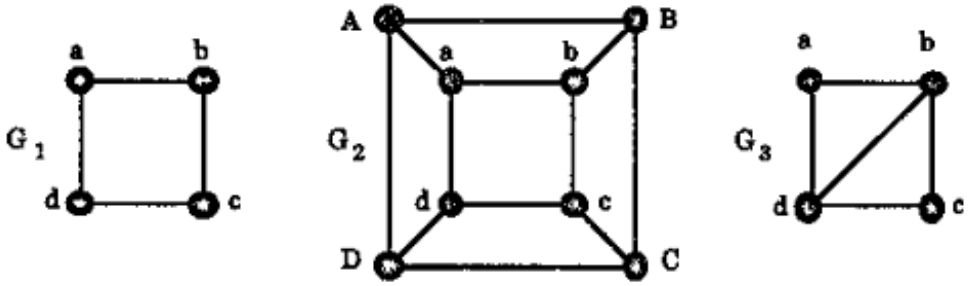
$e_1 \longleftrightarrow (a, b)$ $e_2 \longleftrightarrow (b, c)$ $e_3 \longleftrightarrow (c, c)$ $e_4 \longleftrightarrow (c, d)$ $e_5 \longleftrightarrow (b, d)$
$e_6 \longleftrightarrow (d, e)$ $e_7 \longleftrightarrow (b, e)$ $e_8 \longleftrightarrow (b, e)$.

Then, G can be represented diagrammatically as:



1.2 SUBGRAPHS

Let H be a graph with vertex set $V(H)$ and edge set $E(H)$ and similarly, let G be a graph with vertex set $V(G)$ and edge set $E(G)$. Then we say that H is a subgraph of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. In such a case, we also say that G is a supergraph of H.

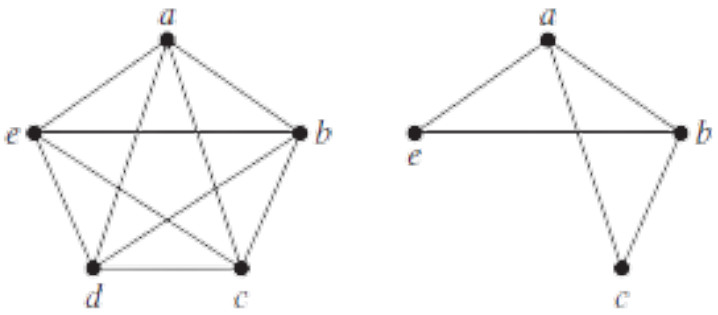


In the above example, G_1 is a subgraph of both G_2 and G_3. But, G_3 is not a subgraph of G_2.

1.2.1 PROPER SUBGRAPH

If H is a subgraph of G then we write: $H \subseteq G$. When $H \subseteq G$ but $H \neq G$, i.e., $V(H) \neq V(G)$ or $E(H) \neq E(G)$, then H is called a proper subgraph of G.

1.2.2 EXAMPLE

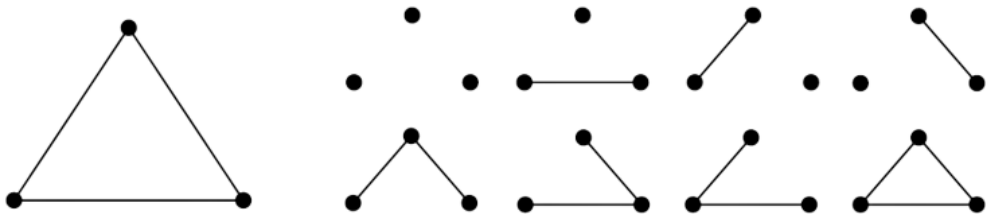


A Subgraph of K_5.

1.2.3 SPANNING SUBGRAPH

A spanning subgraph of a graph G is a subgraph H with $V(H) = V(G)$, i.e., H and G have exactly the same vertex set.

1.2.4 EXAMPLE



the graph C_3

spanning subgraphs of C_3

1.3 SOME DEFINITIONS

Definition 1.1. ***LOOP***

An edge for which two end vertices are the same is called a loop.

Definition 1.2. ***PARALLEL EDGES***

If two or more edges of G have the same end vertices, these edges are called multiple or parallel edges.

Definition 1.3. ***INCIDENT EDGE***

Any edge is said to be incident to the vertices connected by the edge.

Definition 1.4. ***ADJACENT VERTEX***

A vertex is said to be adjacent to other vertices if it has an edge connecting it to the vertices.

Definition 1.5. ***ISOLATED VERTEX***

Any vertex without any edges coming in or out of it is called an isolated vertex.

Definition 1.6. ***VERTEX DEGREES***

Let v be a vertex of a graph G. The degree $d(v)$ of v is the number of edges of G incident with v, counting each loop twice, i.e., it is the number of times v is an end vertex of an edge.

Definition 1.7. ***BIPARTITION***

Let G be a graph. If the vertex set V of G can be partitioned into two non-empty subsets X and Y in such a way that each edge of G has one end in X and one end in Y, then G is called bipartite.
The partition V is called a bipartition of G.

1.4 PATHS, CYCLES AND TREES

1.4.1 WALK

A walk in a graph G is a finite sequence:

$$W = v_0 e_1 v_1 e_2 v_2 ... v_{k-1} e_k v_k \tag{1.1}$$

whose terms are alternatively vertices and edges such that, for $1 \leq i \leq k$, the edge e_i has ends v_{i-1} and v_i. Thus, each edge e_i is immediately preceded and succeeded by the two vertices with which it is incident.

The walk W in (2.1) is a $v_0 - v_k$ walk, or, a walk from v_0 to v_k. The vertex v_0 is called the ***origin*** of the walk while v_k is called the ***terminus*** of W. (v_0 and v_k need not be distinct.)
The vertices v_1, v_2,...,v_{k-1}, in a walk W are called its ***internal vertices***. The integer k, the number of edges in the walk, is called the ***length*** of W.

1.4.2 TRIVIAL WALK

A trivial walk is a walk containing no edges.
Thus, for any vertex v of a graph G,

$$W = v$$

gives a trivial walk. It has length 0.

1.4.3 CLOSED AND OPEN WALK

For two given vertices u and v of a graph G, a $u - v$ walk is said to be ***closed*** or ***open*** depending on whether $u = v$ or $u \neq v$.

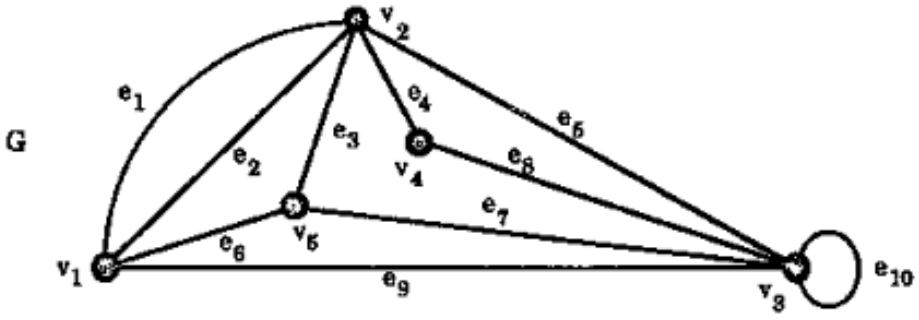
1.4.4 TRAIL

If the edges $e_1, e_2, ..., e_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k v_k$ are distinct, W is called a ***trail***.

1.4.5 PATH

If the vertices $v_0, v_1, ..., v_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k\, v_k$ are distinct then W is called a ***path***.
A path with n vertices is sometimes denoted by P_n and it has length $n - 1$.

1.4.6 EXAMPLE



Let the above graph G be such that the walks W_1, W_2, W_3, W_4 be defined as:

- $W_1 = v_1\, e_1\, v_2\, e_5\, v_3\, e_{10}\, v_3\, e_5\, v_2\, e_3\, v_5$
- $W_2 = v_1\, e_1\, v_2\, e_1\, v_1\, e_1\, v_2$
- $W_3 = v_1\, v_5\, v_2\, v_4\, v_3\, v_1$
- $W_4 = v_2\, v_4\, v_3\, v_5\, v_1$

Here, the length of:

1. $W_1 = 5$
2. $W_2 = 3$
3. $W_3 = 5$
4. $W_4 = 4$.

Then,

1. W_1, W_2 and W_4 are open walks while W_3 is a closed walk.
2. W_3, W_4 are trails but W_1 and W_2 aren't.
3. W_4 is a path but W_1, W_2 and W_3 aren't.

Theorem 1.4.1. *Given any two vertices u and v of a graph G, every $u-v$ walk contains a $u-v$ path,*
i.e., given any walk,

$$W = u\, e_1\, v_1 ... v_{k-1}\, e_k\, v$$

then, after some deletion of vertices and edges if necessary, we can find a sub-sequence P of W which is a $u-v$ path.

Proof. If $u = v$, i.e.,if W is closed, then the trivial path $P = u$ will do.

Now suppose $u \neq v$,i.e.,W is open and let the vertices of W be given, in order, by:

$$u = u_0, u_1, u_2, ..., u_{k-1}, u_k = v.$$

If none of the vertices of G occurs in W more than once, then W is already a $u-v$ path and so we are finished by taking $P = W$.

So now suppose that there are vertices of G that occur in W twice or more. Then there are distinct i, j with $i < j$, say, such that $u_i = u_j$. If the terms $u_i, u_{i+1}, ..., u_{j-1}$ (and the preceding edges) are deleted from W then we obtain a $u-v$ walk W_1 having fewer vertices than W. If there is no repetition of vertices in W_1, then W_1 is a $u-v$ path and setting $P = W_1$ finishes the proof.
If this is not the case, then we repeat the above deletion procedure until finally arriving at a $u-v$ walk that is a path, as required. □

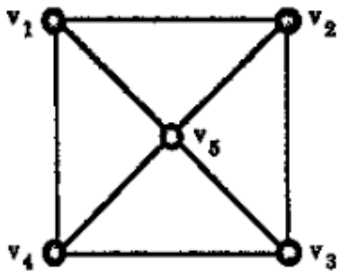
1.4.7 CYCLE

A non-trivial closed trail in a graph G is called a cycle if its origin and internal vertices are distinct i.e.,
A cycle in a graph is a non-empty trail in which only the first and last vertices are equal.

A cycle of length k is called a $k-cycle$. A $k-cycle$ is called odd or even depending on whether k is odd or even.

A $3-cycle$ is often called a triangle. An $n-cycle$, i.e., a cycle with n vertices, will sometimes be denoted by C_n.

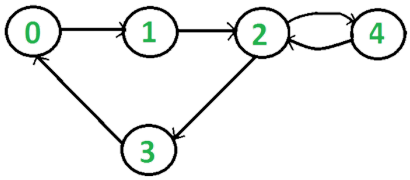
EXAMPLE 1:



In the above example,

1. C = $v_1\, v_2\, v_3\, v_4\, v_1$ is a 4-cycle.
2. $T = v_1\, v_2\, v_5\, v_3\, v_4\, v_5\, v_1$ in a non-trivial closed trail which is not a cycle since v_5 occurs twice as an internal vertex.
3. C_1 = $v_1\, v_2\, v_5\, v_1$ is a triangle.

EXAMPLE 2:

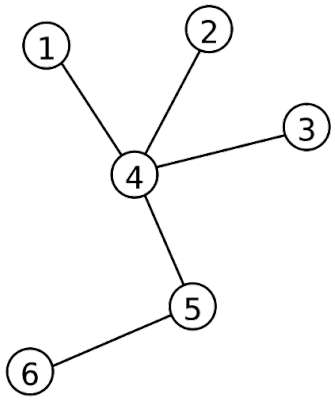


Here, $0 \to 1 \to 2 \to 3 \to 0$ is a 4-cycle but $0 \to 1 \to 2 \to 4 \to 2 \to 3 \to 0$ is not a cycle since the vertex 2, an internal vertex, occurs twice.

1.4.8 TREES

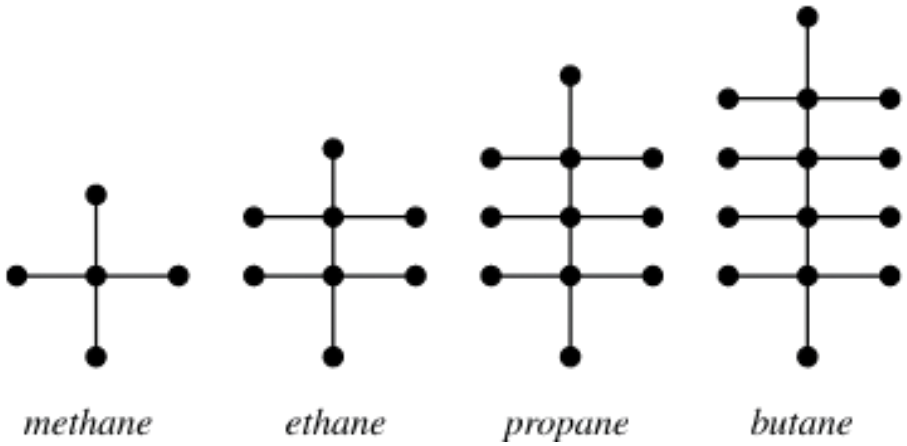
A graph G is called ***acyclic*** if it contains no cycles.
A graph G is called a ***tree*** if it is a connected acyclic graph, i.e., A tree is an undirected graph in which any two vertices are connected by exactly one path.

EXAMPLE 1:



The above graph is an undirected connected acyclic graph and thus, a tree.

EXAMPLE 2:



The above example shows the representation of the first four hydrocarbons as trees.

CHAPTER 2

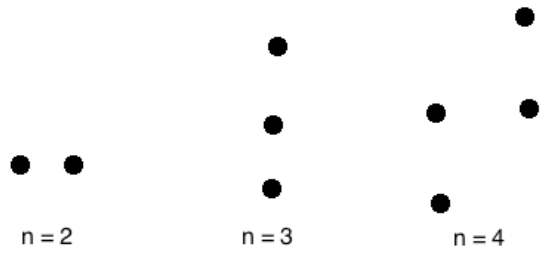
TYPES AND PROPERTIES OF GRAPHS

2.1 TYPES OF GRAPHS

Definition 2.1. ***NULL GRAPH***

A null graph is a graph in which there are no edges between its vertices. A null graph is also called empty graph.

EXAMPLE:



In all the above graphs, there are no edges between the vertices.

Definition 2.2. ***TRIVIAL GRAPH***

A trivial graph is the graph which has only one vertex.

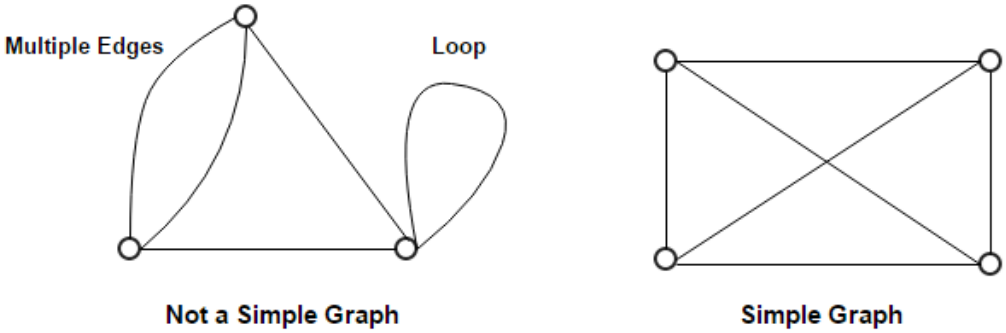
EXAMPLE:

In the above graph, there is only one vertex 'v' without any edge. Therefore, it is a trivial graph.

Definition 2.3. ***SIMPLE GRAPH***

A simple graph is the undirected graph with no parallel edges and no loops. A simple graph which has n vertices, the degree of every vertex is at most $n-1$.

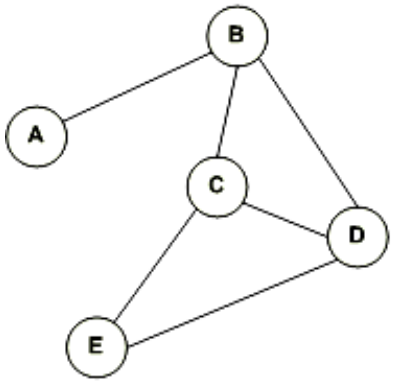
EXAMPLE:



Definition 2.4. ***UNDIRECTED GRAPH***

An undirected graph is a graph whose edges are not directed. The relations between pairs of vertices in an undirected graph are symmetric, so that each edge has no directional character. They only represent whether or not a relationship exists between two vertices. Thus, all the edges in an undirected graph are bidirectional.

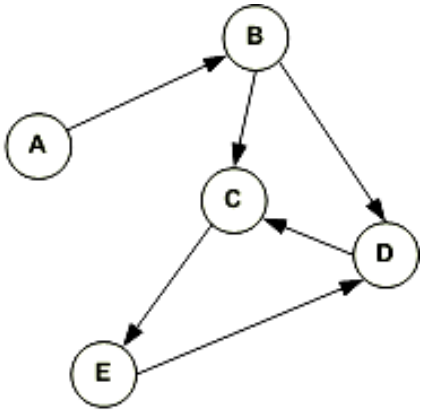
EXAMPLE:



Definition 2.5. ***DIRECTED GRAPH***

A directed graph is a graph in which the edges are directed by arrows.
Directed graphs are also known as digraphs.

EXAMPLE:

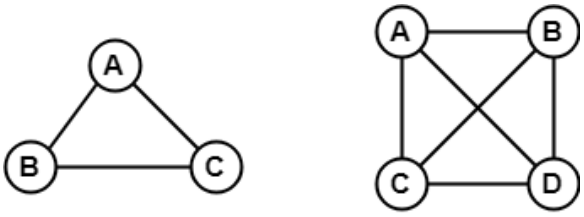


In the above graph, each edge is directed by the arrow. A directed edge has an arrow from A to B means A is related to B but B is not related to A.

Definition 2.6. ***COMPLETE GRAPH***

A graph in which every pair of vertices is joined by exactly one edge is called complete graph. It contains all possible edges.
A complete graph with n vertices contains exactly $\binom{n}{2}$ *edges.*

EXAMPLE:

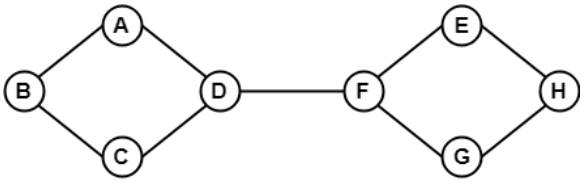


In the above example, since each vertex in the graph is connected with all the remaining vertices through exactly one edge, both are complete graphs.

Definition 2.7. ***CONNECTED GRAPH***

A connected graph is a graph in which we can visit from any one vertex to any other vertex. In a connected graph, at least one edge or path exists between every pair of vertices.

EXAMPLE:

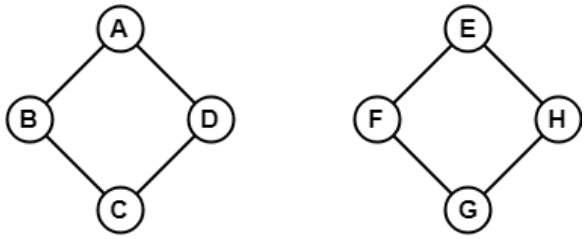


In the above example, we can traverse from any one vertex to any other vertex. It means there exists at least one path between every pair of vertices therefore, it a connected graph.

Definition 2.8. ***DISCONNECTED GRAPH***

A disconnected graph is a graph in which any path does not exist between every pair of vertices.

EXAMPLE:

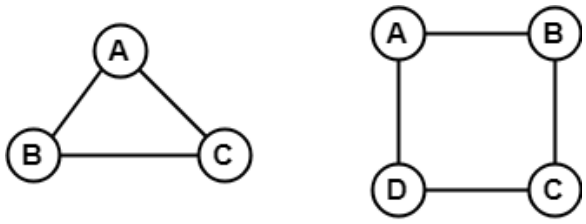


The above graph consists of two independent components which are disconnected. Since it is not possible to visit from the vertices of one component to the vertices of other components, it is a disconnected graph.

Definition 2.9. ***REGULAR GRAPH***

A regular graph is a graph in which degree of all the vertices is same.
If the degree of all the vertices is k*, then it is called* $k - regulargraph$*.*

EXAMPLE:



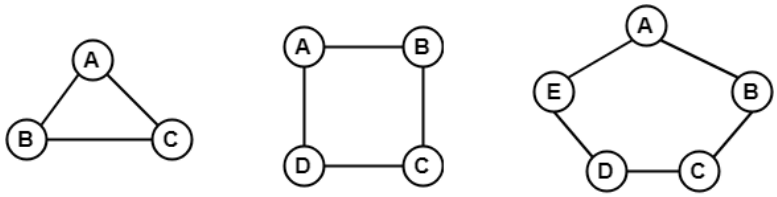
In the above example, all the vertices have degree 2*. Therefore they are called* $2 - Regulargraph$*.*

Definition 2.10. ***CYCLIC GRAPH***

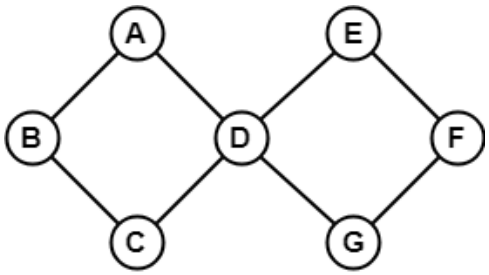
A graph with n vertices (where $n >= 3$) and n edges forming a cycle of n with all its edges is known as cycle graph.
In the cycle graph, degree of each vertex is 2.

A graph containing at least one cycle in it is known as a cyclic graph.

EXAMPLE:



In the above example, all the vertices have degree 2. Therefore they all are cyclic graphs.

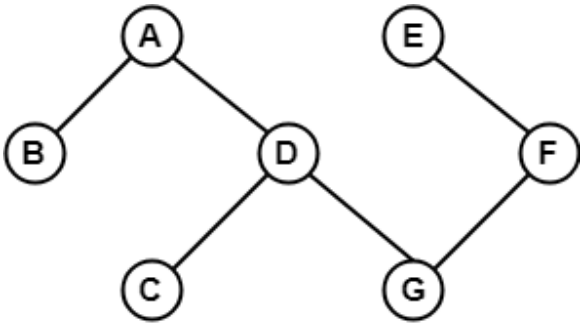


The above graph contains two cycles in it and therefore it is a cyclic graph.

Definition 2.11. ***ACYCLIC GRAPH***

A graph which does not contain any cycle in it is called as an acyclic graph.

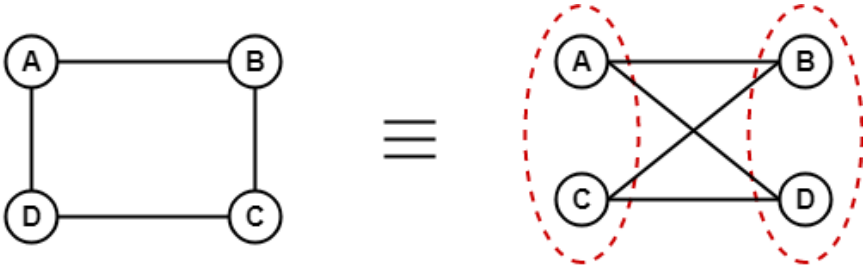
EXAMPLE:



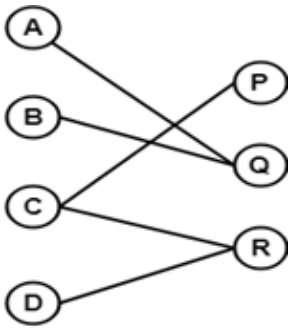
Definition 2.12. ***BIPARTITE GRAPH***

A bipartite graph is a graph in which the vertex set can be partitioned into two sets such that edges only go between sets, not within them.
A graph $G(V, E)$ is called bipartite graph if its vertex-set $V(G)$ can be decomposed into two non-empty disjoint subsets $V_1(G)$ and $V_2(G)$ in such a way that each edge $e \in E(G)$ has its one last joint in $V_1(G)$ and other last point in $V_2(G)$.
The partition $V = V1 \cup V2$ is known as bipartition of G.

EXAMPLE 1:



EXAMPLE 2:

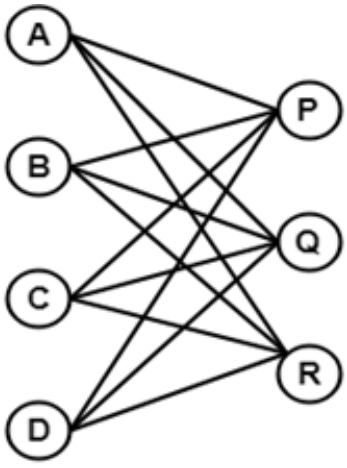


Definition 2.13. ***COMPLETE BIPARTITE GRAPH***

A complete bipartite graph is a bipartite graph in which each vertex in the first set is joined to each vertex in the second set by exactly one edge.
A complete bipartite graph is a bipartite graph which is complete.

$$Complete\,Bipartite\,Graph = Bipartite\,Graph + Complete\,Graph \quad (2.1)$$

EXAMPLE:

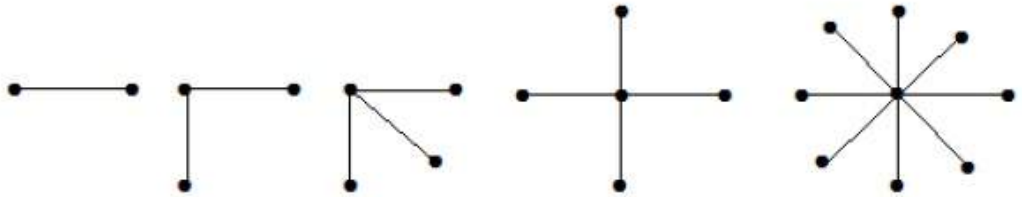


The above graph is known as $K_{4,3}$

Definition 2.14. ***STAR GRAPH***

A star graph is a complete bipartite graph in which $n-1$ vertices have degree 1 and a single vertex has degree $(n-1)$. This exactly looks like a star where $(n-1)$ vertices are connected to a single central vertex.
A star graph with n vertices is denoted by S_n.

EXAMPLE:

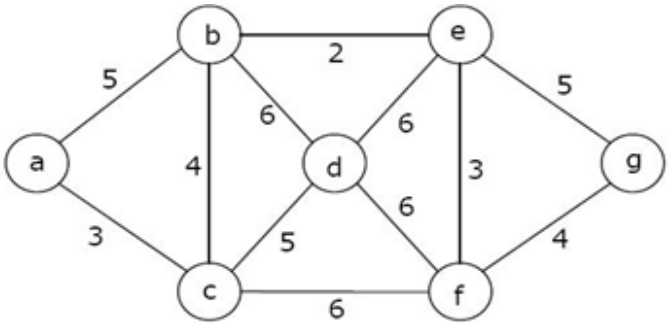


In the above example, out of n vertices, all the $(n-1)$ vertices are connected to a single vertex. Hence, it is a star graph.

Definition 2.15. ***WEIGHTED GRAPH***

A weighted graph is a graph whose edges have been labeled with some weights or numbers.
The length of a path in a weighted graph is the sum of the weights of all the edges in the path.

EXAMPLE:



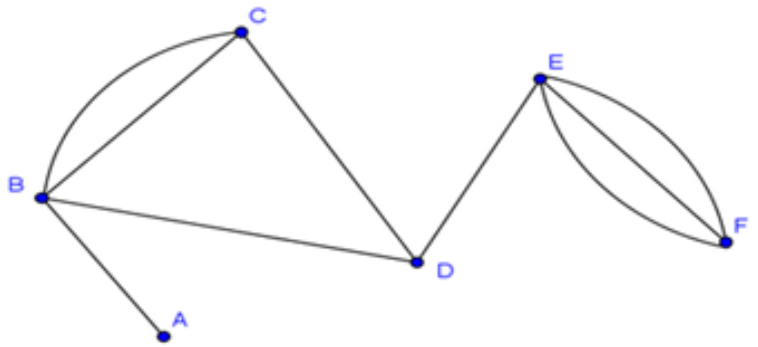
In the above graph, if the path chosen is $a \to b \to c \to d \to e \to g$ *then the length of the path is :*

$$5 + 4 + 5 + 6 + 5 = 25.$$

Definition 2.16. ***MULTI GRAPH***

A graph in which there are multiple edges between any pair of vertices or there are edges from a vertex to itself (loop) is called a multi - graph.

EXAMPLE:

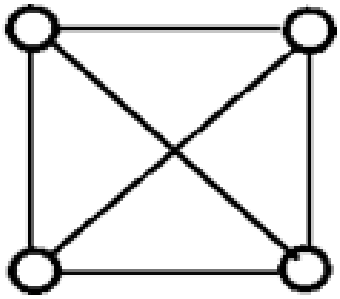


In the above graph, vertex-set B *and* C *are connected with two edges. Similarly, vertex sets* E *and* F *are connected with* 3 *edges. Therefore, it is a multi graph.*

Definition 2.17. ***PLANAR GRAPH***

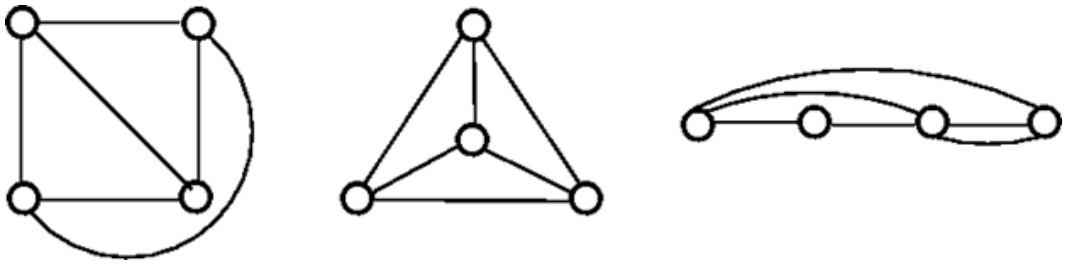
A planar graph is a graph that we can draw in a plane in such a way that no two edges of it cross each other except at a vertex to which they are incident,
i.e., A planar graph is a graph that can be embedded in the plane such that its edges intersect only at their endpoints.

EXAMPLE:



The above graph may not seem to be planar because it has edges crossing each other. But we can redraw the above graph.

The three plane drawings of the above graph are:



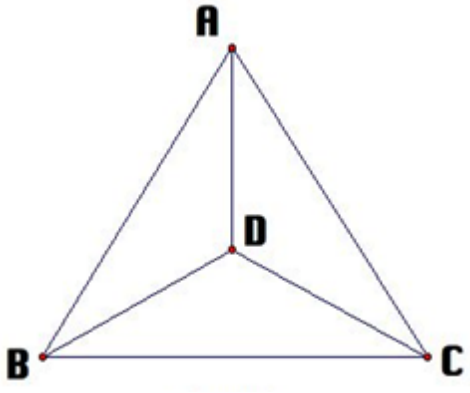
The above three graphs do not consist of two edges crossing each other and therefore, all the above graphs are planar.

2.2 PROPERTIES OF GRAPHS

2.2.1 DISTANCE BETWEEN TWO VERTICES

Distance is basically the number of edges in a shortest path between vertex X and vertex Y. If there are many paths connecting two vertices, then the shortest path is considered as the distance between the two vertices.
Distance between any two vertices X and Y is denoted by $d(X, Y)$.

EXAMPLE:



Suppose, we want to find the distance between vertex B and D. Then, first of all, we have to find the shortest path between vertex B and D.
There are many paths from vertex B to vertex D:

- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Here, length = 3
- B $\rightarrow$ D. Length = 1 (Shortest Path)
- B $\rightarrow$ A $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Length = 3

Hence, the minimum distance between vertex B and vertex D is 1.

2.2.2 ECCENTRICITY OF A VERTEX

Eccentricity of a vertex is the maximum distance between a vertex to all other vertices. It is denoted by $e(V)$.
For a disconnected graph, all vertices are defined to have infinite eccentricity.

2.2.3 RADIUS OF CONNECTED GRAPHS

The radius of a connected graph is the minimum eccentricity from all the vertices. In other words, the minimum among all the distances between a vertex to all other vertices is called as the radius of the graph.
It is denoted by $r(G)$.

2.2.4 DIAMETER OF A GRAPH

Diameter of a graph is the maximum eccentricity from all the vertices. In other words, the maximum among all the distances between a vertex to all other vertices is considered as the diameter of the graph G.
It is denoted by $d(G)$.

2.2.5 CENTRAL POINT

If the eccentricity of the graph is equal to its radius, then it is known as central point of the graph,

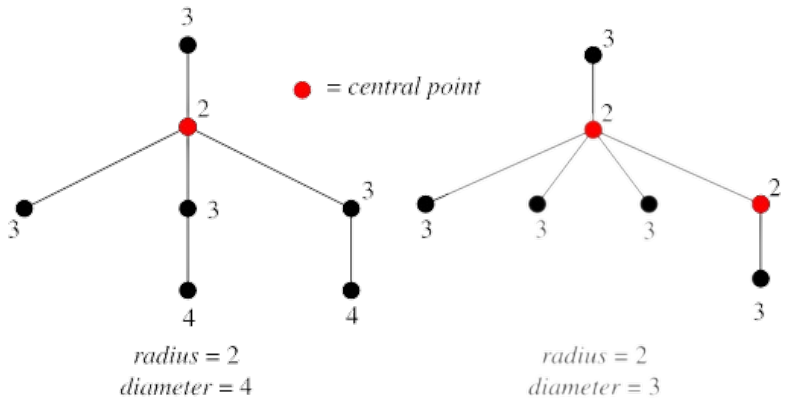
Or,

If $r(V) = e(V)$, then V is the central point of the graph G.

2.2.6 CENTRE OF A GRAPH

The set of all the central point of the graph is known as centre of the graph.

2.2.7 EXAMPLE



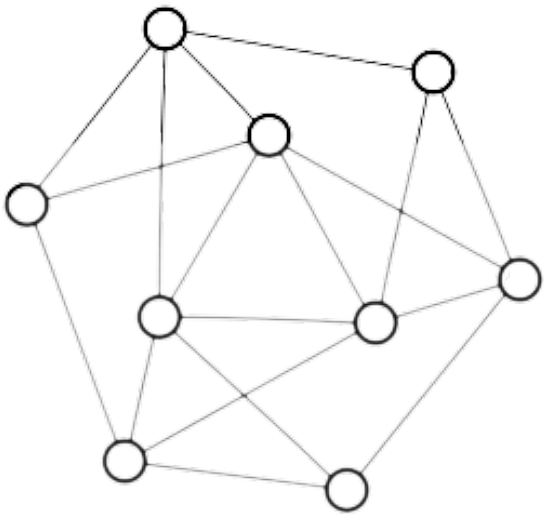
2.2.8 CIRCUMFERENCE OF A GRAPH

The total number of edges in the longest cycle of graph G is known as the circumference of G.

2.2.9 GIRTH

The total number of edges in the shortest cycle of graph G is known as girth.
It is denoted by $g(G)$.

2.2.10 EXAMPLE



For the above graph,

- Order $= 9$.
- Size (number of edges) $= 18$.
- Radius $= 2$.
- Circumference $= 9$.
- Girth $= 3$.

CHAPTER 3

THE FIRST THEOREM OF GRAPH THEORY

3.1 THE FIRST THEOREM

Theorem 3.1.1. *For any graph G with e edges and n vertices: $v_1, v_2, ..., v_n$,*

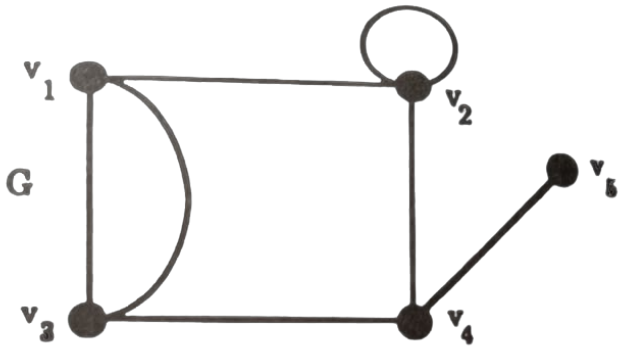
$$\sum_{i=1}^{n} d(v_i) = 2e \tag{3.1}$$

ie, In a graph G, the sum of the degrees of the vertices is equal to twice the number of edges.

Proof.

Each edge, since it has two end vertices, contributes precisely 2 to the sum of the degrees, i.e, when the degrees of the vertices are summed, each edge is counted twice.
□

3.1.1 EXAMPLE



In the above graph, we have,

1. $d(v_1) = 3$
2. $d(v_2) = 4$
3. $d(v_3) = 3$
4. $d(v_4) = 3$
5. $d(v_5) = 1$
6. Number of edges, $e = 7$.

Then,

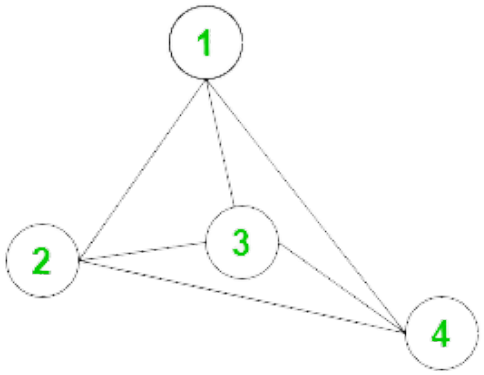
$$d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) = 14 = 2 \times e \tag{3.2}$$

i.e.,

$$\sum_{i=1}^{5} d(v_i) = 2 \times 7 = 14 \tag{3.3}$$

Remark 1. *A vertex of a graph is called odd or even depending on whether its degree is odd or even.*

EXAMPLE:



Here, the vertex degrees are:

1. $d(1) = 3$
2. $d(2) = 3$
3. $d(3) = 3$
4. $d(4) = 3$

Hence, all the vertices here are called odd vertices.

Corollary 3.1.1.1. *In a graph G, there is an even number of odd vertices.*

Proof. Let W be the set of odd vertices of G and let U be the set of even vertices of G.
Then, for each $u \in U$, $d(u)$ is even.
Also,

$$\sum_{u \in U} d(u),$$

being a sum of even numbers, is even.

However, by the previous theorem where V is the vertex set of G and e is the number of its edges,

$$\sum_{u \in U} d(u) + \sum_{w \in W} d(w) = \sum_{v \in V} d(v) = 2e. \tag{3.4}$$

Thus,

$$\sum_{w \in W} d(w) = 2e - \sum_{u \in U} d(u), \tag{3.5}$$

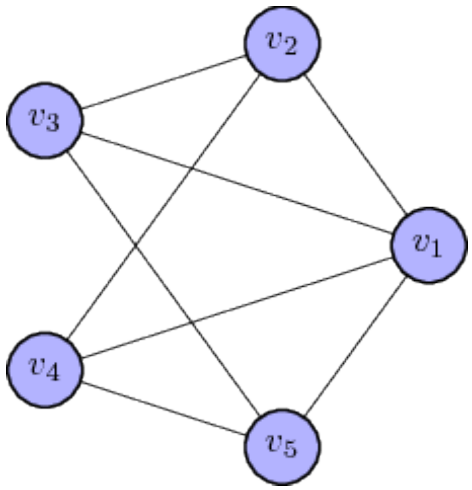
is even (being the difference of two even numbers).

As all the terms in:

$$\sum_{w \in W} d(w),$$

are odd and their sum is even, there must be an even number of them (because the sum of an odd number of odd numbers is odd).
□

EXAMPLE:

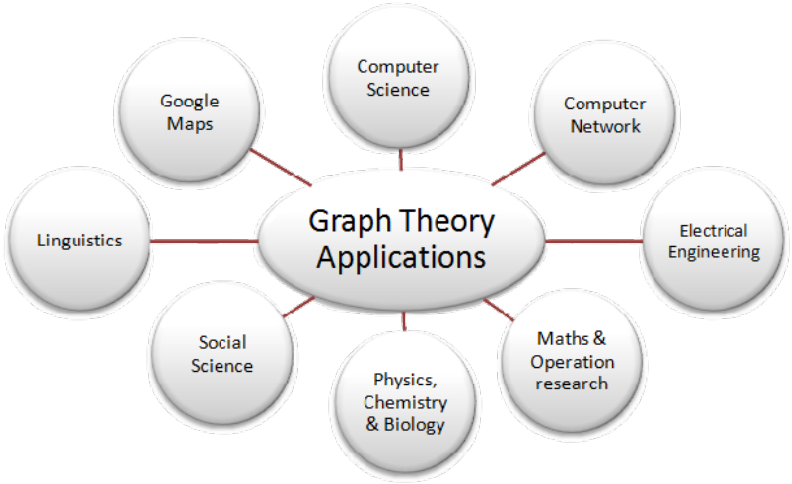


In the above graph, $d(v_1) = 4$, $d(v_2) = 3$, $d(v_3) = 3$, $d(v_4) = 3$ and $d(v_5) = 3$. Hence, out of the 5 vertices, v_2, v_3, v_4 and v_5 have odd degrees, i.e., there is an even number (4) of odd vertices.

CHAPTER 4

APPLICATIONS OF GRAPH THEORY

Graph Theory is used in vast area of science and technologies.



1. **COMPUTER SCIENCE**
   In computer science, graph theory is used for the study of algorithms like:

   - **Dijkstra's Algorithm** : Dijkstra's algorithm allows us to find the shortest path between any two vertices of a graph. This algorithm helps in finding the shortest paths between nodes in a graph, which may represent, for example, road networks.

- **Prim's Algorithm** : Prim's Algorithm is a greedy algorithm that is used to find the subset of edges that includes every vertex of the graph such that the sum of the weights of the edges can be minimized for a weighted undirected graph.
- **Kruskal's Algorithm**: Kruskal's Algorithm is used to discover the shortest path between two points in a connected weighted graph.

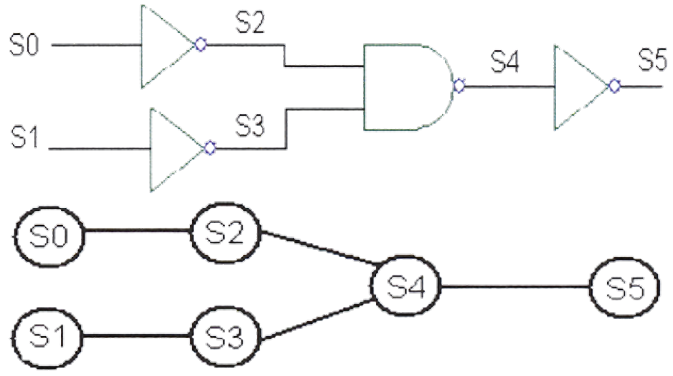
Moreover, graphs are used:

- To define the flow of computation.
- To represent networks of communication.
- To represent data organization.
- To find shortest path in road or a network.
- In Google Maps, various locations are represented as vertices or nodes and the roads are represented as edges and graph theory is used to find the shortest path between two nodes.

2. **ELECTRICAL ENGINEERING**

In Electrical Engineering, graph theory is used in designing of circuit connections. These circuit connections are named as topologies. Some topologies are series, bridge, star and parallel topologies.

EXAMPLE:



3. **LINGUISTICS**

- In linguistics, graphs are mostly used for parsing of a language tree and grammar of a language tree.
- Semantics networks are used within lexical semantics, especially as applied to computers, modeling word meaning is easier when a given word is understood in terms of related words.
- Methods in phonology (e.g. theory of optimality, which uses lattice graphs) and morphology (e.g. morphology of finite - state, using finite-state transducers) are common in the analysis of language as a graph.

4. **PHYSICS AND CHEMISTRY**

- In physics and chemistry, graph theory is used to study molecules.
- The 3D structure of complicated simulated atomic structures can be studied quantitatively by gathering statistics on graph-theoretic properties related to the topology of the atoms.
- Statistical physics also uses graphs. In this field graphs can represent local connections between interacting parts of a system, as well as the dynamics of a physical process on such systems.
- Graphs are also used to express the micro-scale channels of porous media, in which the vertices represent the pores and the edges represent the smaller channels connecting the pores.
- Graph is also helpful in constructing the molecular structure as well as lattice of the molecule. It also helps us to show the bond relation in between atoms and molecules, also help in comparing structure of one molecule to other.

5. **COMPUTER NETWORK**

- In computer network, the relationships among interconnected computers within the network, follow the principles of graph theory.
- Graph theory is widely used in modeling and routing in networks.
- Graph theory is also used in network security.

6. **SOCIAL SCIENCES**

- Graph theory is also used in sociology. For example, to explore rumor spreading, or to measure actors' prestige notably through the use of social network analysis software.
- Acquaintanceship and friendship graphs describe whether people know each other or not.
- In influence graphs model, certain people can influence the behavior of others.
- In collaboration graphs model to check whether two people work together in a particular way, such as acting in a movie together.

7. **BIOLOGY**

- Nodes in biological networks represent bio-molecules such as genes, proteins or metabolites, and edges connecting these nodes indicate functional, physical or chemical interactions between the corresponding bio-molecules.
- Graph theory is used in transcriptional regulation networks.
- It is also used in Metabolic networks.
- In PPI (Protein - Protein interaction) networks graph theory is also useful.
- Characterizing drug - drug target relationships.

8. **MATHEMATICS**

In mathematics, operational research is the important field. Graph theory provides many useful applications in operational research like:

- Minimum cost path.
- A scheduling problem.

9. **MISCELLANEOUS**

Graphs are used to represent the routes between the cities. With the help of tree that is a type of graph, we can create hierarchical ordered information such as family tree.

CONCLUSION

Graph theory has delivered important scientific discoveries, such as improved understanding of breakdown of electricity distribution systems or the propagation of infections in social networks, till date.

Graph theory also provides a remarkably simple way to characterize the complexity of ecological networks. Indices such as connectance, degree distribution or network topology serve as basic measurements to describe their structure. Such indices facilitate comparison between different systems and revealing commonalities and variations. Nowadays, the relatively important number of network studies leads to a myriads of ways to sample, analyze and interpret them.

Graph theory is an exceptionally rich area for programmers and designers. Graphs can be used to solve some very complex problems, such as least cost routing, mapping, program analysis, and so on. Network devices, such as routers and switches, use graphs to calculate optimal routing for traffic.

Graph theory is rapidly moving into the mainstream of mathematics mainly because of its applications in diverse fields which include biochemistry (genomics), electrical engineering (communications networks and coding theory), computer science (algorithms and computations) and operations research (scheduling).

Hence, studying graphs through a framework provides answers to many arrangement, networking, optimization, matching and operational problems. Graphs can be used to model many types of relations and processes in physical, biological, social and information systems, and has a wide range of useful applications.

BIBLIOGRAPHY

1. J. Clark and D. A. Holton, ***A First Look at Graph Theory***, World Scientific Publishing, 1991, 1-31, 47-51.

2. Wilson, J Robin, ***An Introduction To Graph Theory***, Addison Wesley Longman Ltd, 4th ed, 1972.

3. Javapoint, *Types of Graphs*, ***<https://www.javatpoint.com/graph-theory-types-of-graphs>***

4. Javapoint, *Tree and Forest*, ***<https://www.javatpoint.com/graph-theory-tree-and-forest>***

5. Javapoint, *Basic Properties of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-basic-properties>***

6. Programiz, *Dijkstra's Algorithm*, ***<https://www.programiz.com/dsa/dijkstra-algorithm>***

7. Javapoint, *Applications of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-applications>***

8. Britannica, *Graph Theory*, ***<https://www.britannica.com/topic/graph-theory>***

AN INTRODUCTION TO GRAPH THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

SOJANA P P
DB20CMSR16

under the guidance of
Ms. Remya Raj

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty

March 2023

Examiner 1 **Examiner 2**

CERTIFICATE

This is to certify that **"An Introduction To Graph Theory"** is a bona fide project of **Sojana P P**, Register Number: **DB20CMSR16** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head Of Department

Ms. Remya Raj
Project Supervisor

DECLARATION

I, Sojana P P, hereby declare that the project: "An Introduction To Graph Theory" is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

Sojana P P

DB20CMSR16

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout the course of the successful accomplishment of this project.

First, I wish to express my sincere gratitude to my supervisor, Ms. Remya Raj, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that had helped me tremendously at all times in my research and writing of this project. Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thank you for all your encouragement.

CONTENTS

INTRODUCTION

In mathematics, graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. Graph theory is a delightful playground for the exploration of proof techniques in Discrete Mathematics. The results of graph theory have applications in many areas of the computing, social and natural sciences. One of the beauties of graph theory is that it depends very little on other branches of mathematics. The subject of graph theory had its beginnings in recreational math problems but it has grown into a significant area of mathematical research, with applications in chemistry, operations research, social sciences, and computer science.

Graph Theory can model and study many real-world problems and is applied in a wide range of disciplines. In computer science, graph theory is used to model networks and communications as seen in the case of Google search, Google Maps and social media. Furthermore, graph theory is used in chemistry to model molecules and in biology to study genomes. It is even used in linguistics and social sciences. Using graph theory in Machine Learning and neural network is also one of the new trends.

The history of graph theory may be specifically traced to 1735, when the Swiss mathematician Leonhard Euler solved the Königsberg bridge problem. The Königsberg bridge problem was an old puzzle concerning the possibility of finding a path over every one of seven bridges that span a forked river flowing past an island—but without crossing any bridge twice. Euler argued that no such path exists since in Königsberg, the four land masses were connected by an odd number of bridges, it was impossible to draw the desired route. His proof involved only references to the physical arrangement of the bridges, but essentially he proved the first theorem in graph theory.

CHAPTER 1

BASIC CONCEPTS IN GRAPH THEORY

1.1 GRAPH

A graph G = (V(G),E(G)) consists of two finite sets:

i The vertex set of the graph, denoted by V(G) or V, which is a non-empty set of elements called vertices,

ii The edge set of the graph, denoted by E(G) or E, which is a possible empty set of elements called edges,

such that each edge e in E is assigned an unordered pair of vertices (u,v) called the end vertices of e.

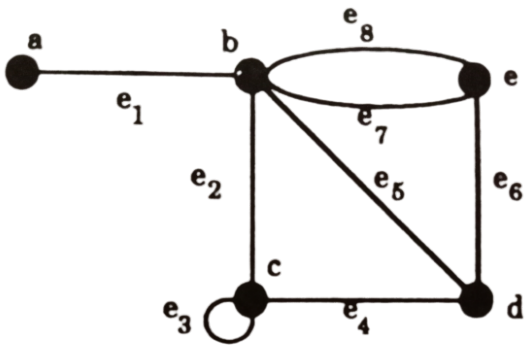
Vertices of a graph are also known as nodes or points while edges are also called links or lines.

1.1.1 EXAMPLE

Let G = (V,E) where V = $\{a, b, c, d, e\}$, E = $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$, and the ends of edges are given by:

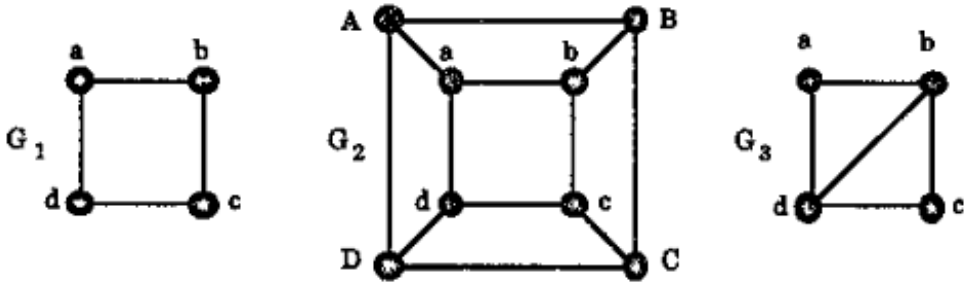
$e_1 \longleftrightarrow (a, b)$ $e_2 \longleftrightarrow (b, c)$ $e_3 \longleftrightarrow (c, c)$ $e_4 \longleftrightarrow (c, d)$ $e_5 \longleftrightarrow (b, d)$
$e_6 \longleftrightarrow (d, e)$ $e_7 \longleftrightarrow (b, e)$ $e_8 \longleftrightarrow (b, e)$.

Then, G can be represented diagrammatically as:



1.2 SUBGRAPHS

Let H be a graph with vertex set $V(H)$ and edge set $E(H)$ and similarly, let G be a graph with vertex set $V(G)$ and edge set $E(G)$. Then we say that H is a subgraph of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. In such a case, we also say that G is a supergraph of H.

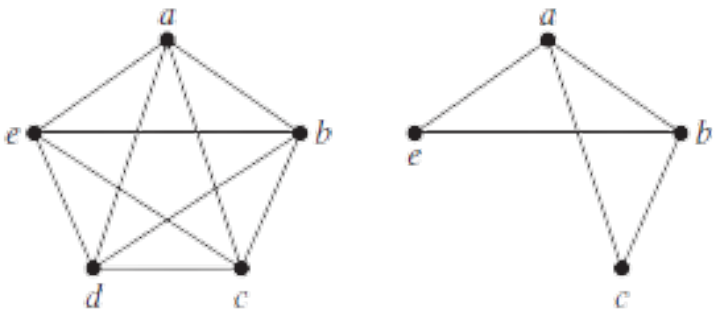


In the above example, G_1 is a subgraph of both G_2 and G_3. But, G_3 is not a subgraph of G_2.

1.2.1 PROPER SUBGRAPH

If H is a subgraph of G then we write: $H \subseteq G$. When $H \subseteq G$ but $H \neq G$, i.e., $V(H) \neq V(G)$ or $E(H) \neq E(G)$, then H is called a proper subgraph of G.

1.2.2 EXAMPLE

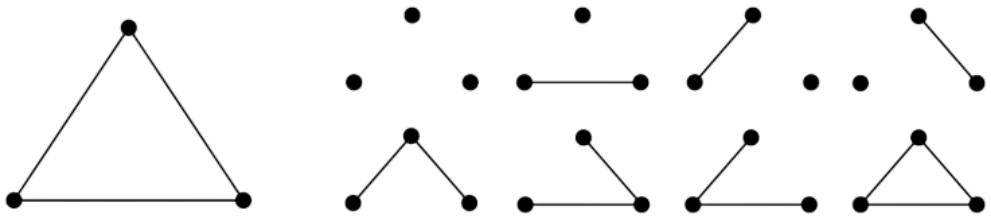


A Subgraph of K_5.

1.2.3 SPANNING SUBGRAPH

A spanning subgraph of a graph G is a subgraph H with $V(H) = V(G)$, i.e., H and G have exactly the same vertex set.

1.2.4 EXAMPLE



the graph C_3

spanning subgraphs of C_3

1.3 SOME DEFINITIONS

Definition 1.1. ***LOOP***

An edge for which two end vertices are the same is called a loop.

Definition 1.2. ***PARALLEL EDGES***

If two or more edges of G have the same end vertices, these edges are called multiple or parallel edges.

Definition 1.3. ***INCIDENT EDGE***

Any edge is said to be incident to the vertices connected by the edge.

Definition 1.4. ***ADJACENT VERTEX***

A vertex is said to be adjacent to other vertices if it has an edge connecting it to the vertices.

Definition 1.5. ***ISOLATED VERTEX***

Any vertex without any edges coming in or out of it is called an isolated vertex.

Definition 1.6. ***VERTEX DEGREES***

Let v be a vertex of a graph G. The degree $d(v)$ of v is the number of edges of G incident with v, counting each loop twice, i.e., it is the number of times v is an end vertex of an edge.

Definition 1.7. ***BIPARTITION***

Let G be a graph. If the vertex set V of G can be partitioned into two non-empty subsets X and Y in such a way that each edge of G has one end in X and one end in Y, then G is called bipartite.
The partition V is called a bipartition of G.

1.4 PATHS, CYCLES AND TREES

1.4.1 WALK

A walk in a graph G is a finite sequence:

$$W = v_0 e_1 v_1 e_2 v_2 ... v_{k-1} e_k v_k \tag{1.1}$$

whose terms are alternatively vertices and edges such that, for $1 \leq i \leq k$, the edge e_i has ends v_{i-1} and v_i. Thus, each edge e_i is immediately preceded and succeeded by the two vertices with which it is incident.

The walk W in (2.1) is a $v_0 - v_k$ walk, or, a walk from v_0 to v_k. The vertex v_0 is called the ***origin*** of the walk while v_k is called the ***terminus*** of W. (v_0 and v_k need not be distinct.)
The vertices v_1, v_2,...,v_{k-1}, in a walk W are called its ***internal vertices***. The integer k, the number of edges in the walk, is called the ***length*** of W.

1.4.2 TRIVIAL WALK

A trivial walk is a walk containing no edges.
Thus, for any vertex v of a graph G,

$$W = v$$

gives a trivial walk. It has length 0.

1.4.3 CLOSED AND OPEN WALK

For two given vertices u and v of a graph G, a $u - v$ walk is said to be ***closed*** or ***open*** depending on whether $u = v$ or $u \neq v$.

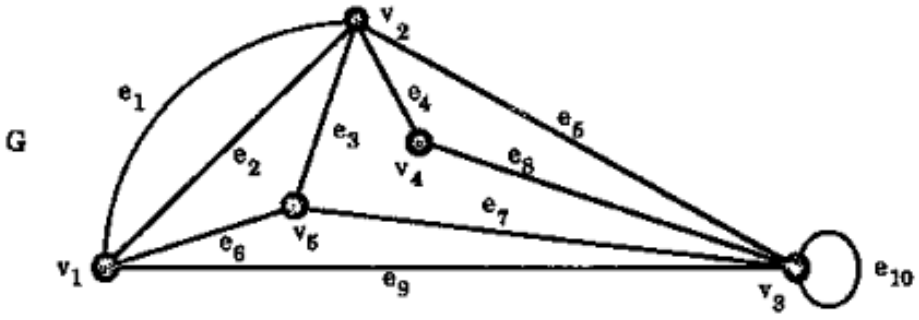
1.4.4 TRAIL

If the edges $e_1, e_2, ..., e_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k v_k$ are distinct, W is called a ***trail***.

1.4.5 PATH

If the vertices $v_0, v_1, ..., v_k$ of the walk $W = v_0\, e_1\, v_1\, e_2\, v_2 ... e_k\, v_k$ are distinct then W is called a ***path***.
A path with n vertices is sometimes denoted by P_n and it has length $n - 1$.

1.4.6 EXAMPLE



Let the above graph G be such that the walks W_1, W_2, W_3, W_4 be defined as:

- $W_1 = v_1\, e_1\, v_2\, e_5\, v_3\, e_{10}\, v_3\, e_5\, v_2\, e_3\, v_5$
- $W_2 = v_1\, e_1\, v_2\, e_1\, v_1\, e_1\, v_2$
- $W_3 = v_1\, v_5\, v_2\, v_4\, v_3\, v_1$
- $W_4 = v_2\, v_4\, v_3\, v_5\, v_1$

Here, the length of:

1. $W_1 = 5$
2. $W_2 = 3$
3. $W_3 = 5$
4. $W_4 = 4$.

Then,

1. W_1, W_2 and W_4 are open walks while W_3 is a closed walk.
2. W_3, W_4 are trails but W_1 and W_2 aren't.
3. W_4 is a path but W_1, W_2 and W_3 aren't.

Theorem 1.4.1. *Given any two vertices u and v of a graph G, every $u-v$ walk contains a $u-v$ path,*
i.e., given any walk,

$$W = u\, e_1\, v_1 ... v_{k-1}\, e_k\, v$$

then, after some deletion of vertices and edges if necessary, we can find a sub-sequence P of W which is a $u-v$ path.

Proof. If $u = v$, i.e.,if W is closed, then the trivial path $P = u$ will do.

Now suppose $u \neq v$,i.e.,W is open and let the vertices of W be given, in order, by:

$$u = u_0, u_1, u_2, ..., u_{k-1}, u_k = v.$$

If none of the vertices of G occurs in W more than once, then W is already a $u-v$ path and so we are finished by taking $P = W$.

So now suppose that there are vertices of G that occur in W twice or more. Then there are distinct i, j with $i < j$, say, such that $u_i = u_j$. If the terms $u_i, u_{i+1}, ..., u_{j-1}$ (and the preceding edges) are deleted from W then we obtain a $u-v$ walk W_1 having fewer vertices than W. If there is no repetition of vertices in W_1, then W_1 is a $u-v$ path and setting $P = W_1$ finishes the proof.
If this is not the case, then we repeat the above deletion procedure until finally arriving at a $u-v$ walk that is a path, as required. □

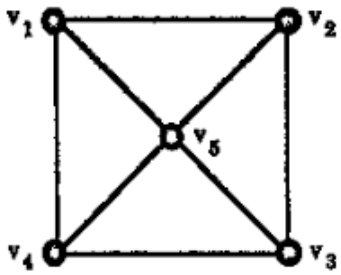
1.4.7 CYCLE

A non-trivial closed trail in a graph G is called a cycle if its origin and internal vertices are distinct i.e.,
A cycle in a graph is a non-empty trail in which only the first and last vertices are equal.

A cycle of length k is called a $k-cycle$. A $k-cycle$ is called odd or even depending on whether k is odd or even.

A $3-cycle$ is often called a triangle. An $n-cycle$, i.e., a cycle with n vertices, will sometimes be denoted by C_n.

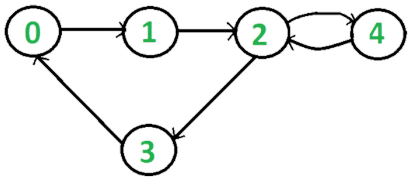
EXAMPLE 1:



In the above example,

1. C = $v_1\, v_2\, v_3\, v_4\, v_1$ is a 4-cycle.
2. $T = v_1\, v_2\, v_5\, v_3\, v_4\, v_5\, v_1$ in a non-trivial closed trail which is not a cycle since v_5 occurs twice as an internal vertex.
3. C_1 = $v_1\, v_2\, v_5\, v_1$ is a triangle.

EXAMPLE 2:

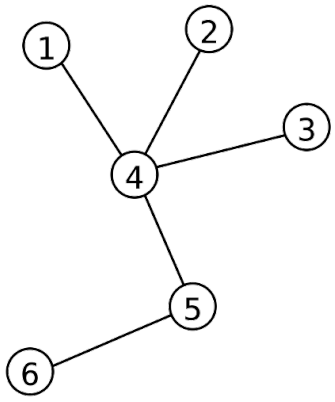


Here, $0 \to 1 \to 2 \to 3 \to 0$ is a 4-cycle but $0 \to 1 \to 2 \to 4 \to 2 \to 3 \to 0$ is not a cycle since the vertex 2, an internal vertex, occurs twice.

1.4.8 TREES

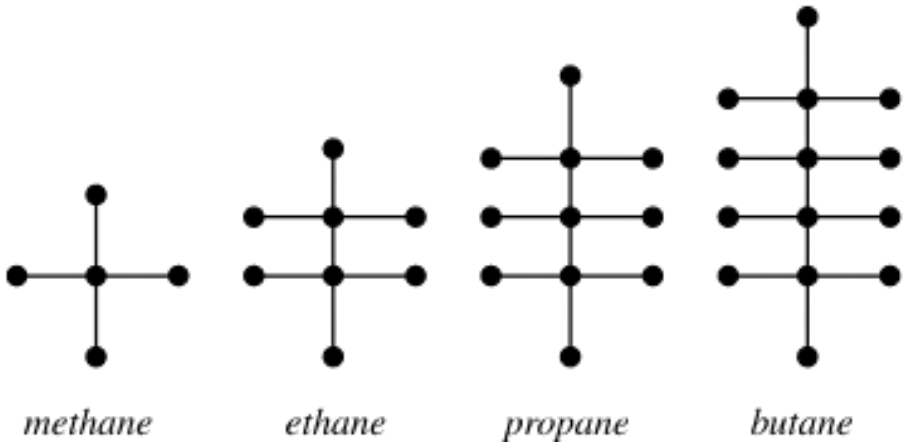
A graph G is called ***acyclic*** if it contains no cycles.
A graph G is called a ***tree*** if it is a connected acyclic graph, i.e., A tree is an undirected graph in which any two vertices are connected by exactly one path.

EXAMPLE 1:



The above graph is an undirected connected acyclic graph and thus, a tree.

EXAMPLE 2:



The above example shows the representation of the first four hydrocarbons as trees.

CHAPTER 2

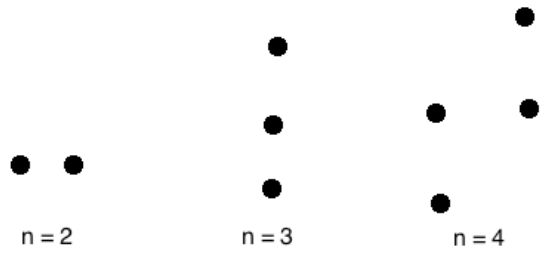
TYPES AND PROPERTIES OF GRAPHS

2.1 TYPES OF GRAPHS

Definition 2.1. ***NULL GRAPH***

A null graph is a graph in which there are no edges between its vertices. A null graph is also called empty graph.

EXAMPLE:



In all the above graphs, there are no edges between the vertices.

Definition 2.2. ***TRIVIAL GRAPH***

A trivial graph is the graph which has only one vertex.

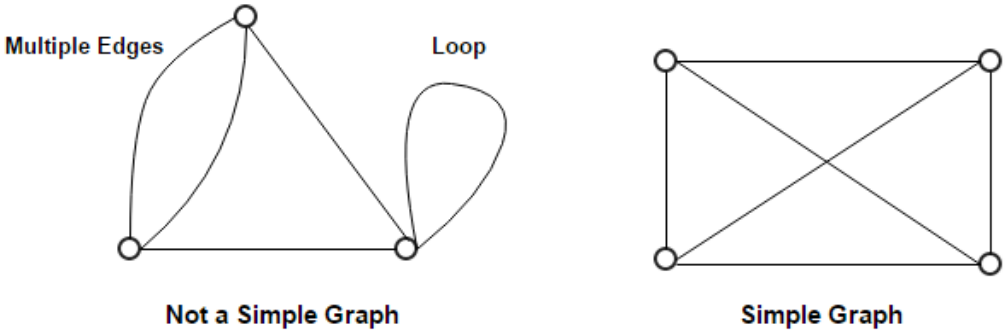
EXAMPLE:

In the above graph, there is only one vertex 'v' without any edge. Therefore, it is a trivial graph.

Definition 2.3. ***SIMPLE GRAPH***

A simple graph is the undirected graph with no parallel edges and no loops. A simple graph which has n vertices, the degree of every vertex is at most $n-1$.

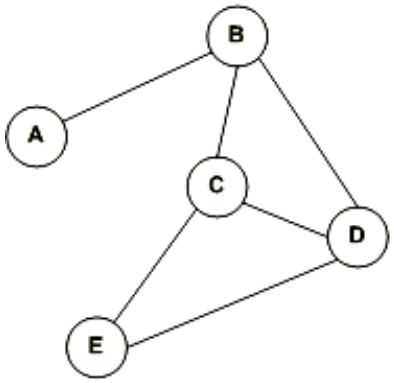
EXAMPLE:



Definition 2.4. ***UNDIRECTED GRAPH***

An undirected graph is a graph whose edges are not directed. The relations between pairs of vertices in an undirected graph are symmetric, so that each edge has no directional character. They only represent whether or not a relationship exists between two vertices. Thus, all the edges in an undirected graph are bidirectional.

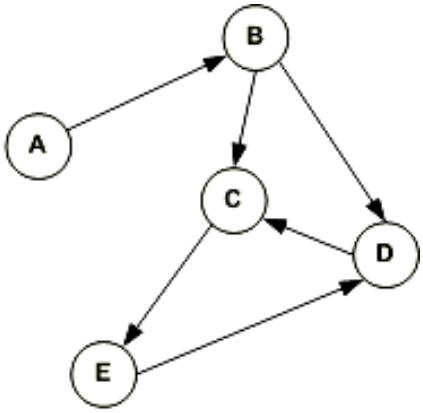
EXAMPLE:



Definition 2.5. ***DIRECTED GRAPH***

A directed graph is a graph in which the edges are directed by arrows.
Directed graphs are also known as digraphs.

EXAMPLE:

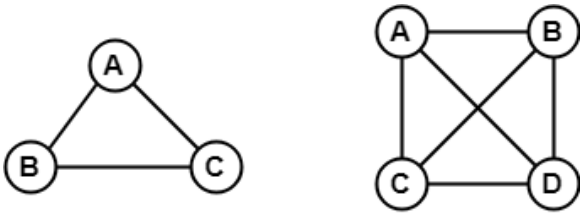


In the above graph, each edge is directed by the arrow. A directed edge has an arrow from A to B means A is related to B but B is not related to A.

Definition 2.6. ***COMPLETE GRAPH***

A graph in which every pair of vertices is joined by exactly one edge is called complete graph. It contains all possible edges.
A complete graph with n vertices contains exactly $\binom{n}{2}$ *edges.*

EXAMPLE:

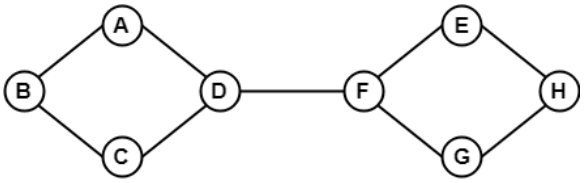


In the above example, since each vertex in the graph is connected with all the remaining vertices through exactly one edge, both are complete graphs.

Definition 2.7. ***CONNECTED GRAPH***

A connected graph is a graph in which we can visit from any one vertex to any other vertex. In a connected graph, at least one edge or path exists between every pair of vertices.

EXAMPLE:

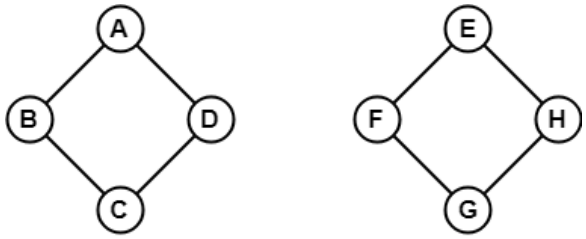


In the above example, we can traverse from any one vertex to any other vertex. It means there exists at least one path between every pair of vertices therefore, it a connected graph.

Definition 2.8. ***DISCONNECTED GRAPH***

A disconnected graph is a graph in which any path does not exist between every pair of vertices.

EXAMPLE:

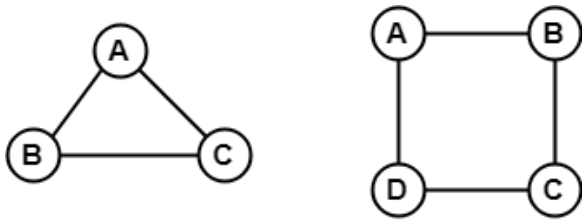


The above graph consists of two independent components which are disconnected. Since it is not possible to visit from the vertices of one component to the vertices of other components, it is a disconnected graph.

Definition 2.9. ***REGULAR GRAPH***

A regular graph is a graph in which degree of all the vertices is same.
If the degree of all the vertices is k*, then it is called* $k - regulargraph$*.*

EXAMPLE:



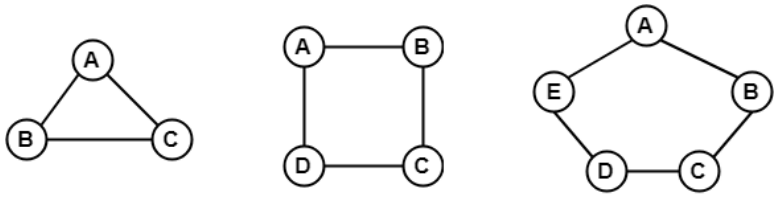
In the above example, all the vertices have degree 2*. Therefore they are called* $2 - Regulargraph$*.*

Definition 2.10. ***CYCLIC GRAPH***

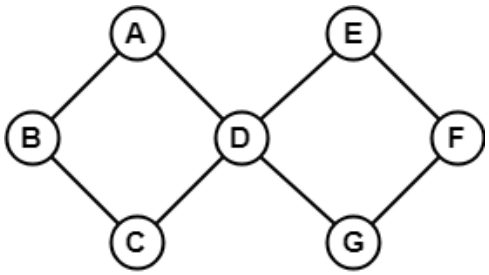
A graph with n vertices (where $n >= 3$) and n edges forming a cycle of n with all its edges is known as cycle graph.
In the cycle graph, degree of each vertex is 2.

A graph containing at least one cycle in it is known as a cyclic graph.

EXAMPLE:



In the above example, all the vertices have degree 2. Therefore they all are cyclic graphs.

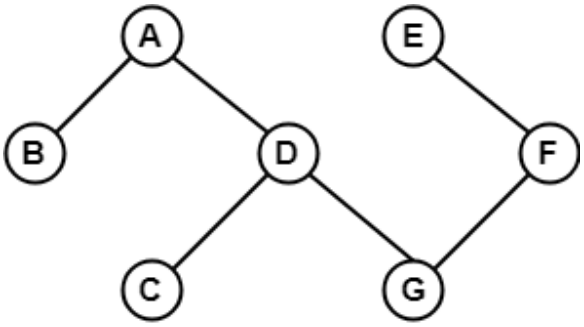


The above graph contains two cycles in it and therefore it is a cyclic graph.

Definition 2.11. ***ACYCLIC GRAPH***

A graph which does not contain any cycle in it is called as an acyclic graph.

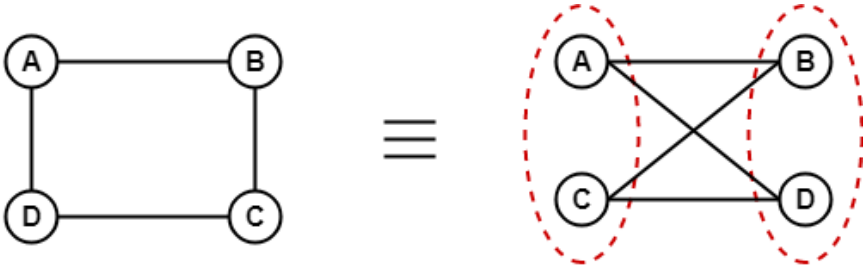
EXAMPLE:



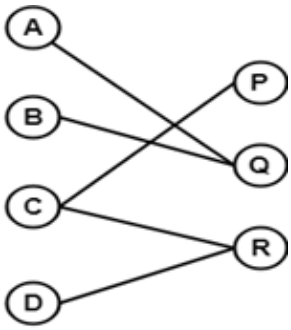
Definition 2.12. ***BIPARTITE GRAPH***

A bipartite graph is a graph in which the vertex set can be partitioned into two sets such that edges only go between sets, not within them.
A graph $G(V, E)$ is called bipartite graph if its vertex-set $V(G)$ can be decomposed into two non-empty disjoint subsets $V_1(G)$ and $V_2(G)$ in such a way that each edge $e \in E(G)$ has its one last joint in $V_1(G)$ and other last point in $V_2(G)$.
The partition $V = V1 \cup V2$ is known as bipartition of G.

EXAMPLE 1:



EXAMPLE 2:

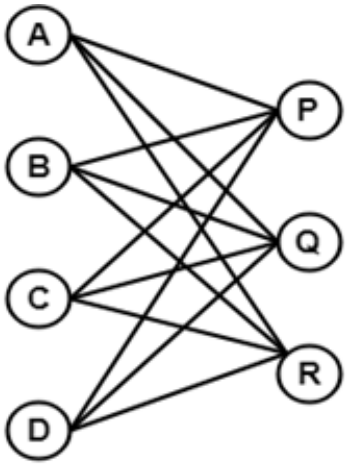


Definition 2.13. ***COMPLETE BIPARTITE GRAPH***

A complete bipartite graph is a bipartite graph in which each vertex in the first set is joined to each vertex in the second set by exactly one edge.
A complete bipartite graph is a bipartite graph which is complete.

$$Complete\,Bipartite\,Graph = Bipartite\,Graph + Complete\,Graph \quad (2.1)$$

EXAMPLE:

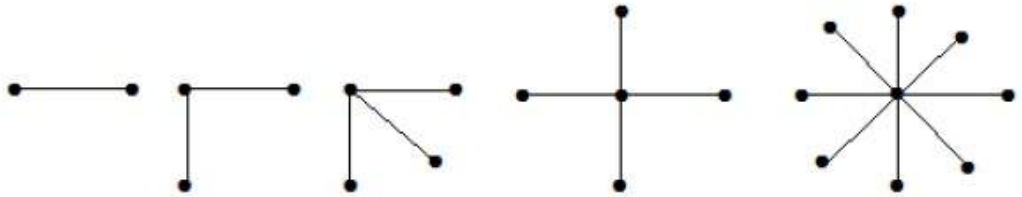


The above graph is known as $K_{4,3}$

Definition 2.14. ***STAR GRAPH***

A star graph is a complete bipartite graph in which $n-1$ vertices have degree 1 and a single vertex has degree $(n-1)$. This exactly looks like a star where $(n-1)$ vertices are connected to a single central vertex.
A star graph with n vertices is denoted by S_n.

EXAMPLE:

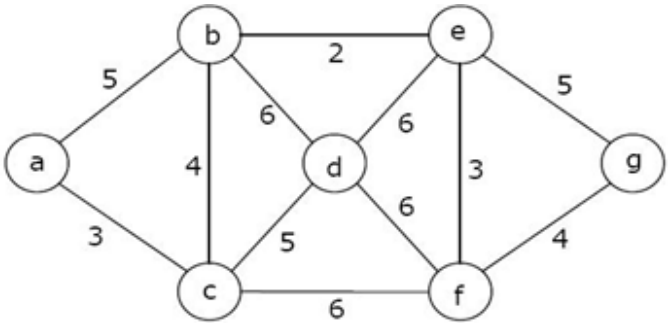


In the above example, out of n vertices, all the $(n-1)$ vertices are connected to a single vertex. Hence, it is a star graph.

Definition 2.15. ***WEIGHTED GRAPH***

A weighted graph is a graph whose edges have been labeled with some weights or numbers.
The length of a path in a weighted graph is the sum of the weights of all the edges in the path.

EXAMPLE:



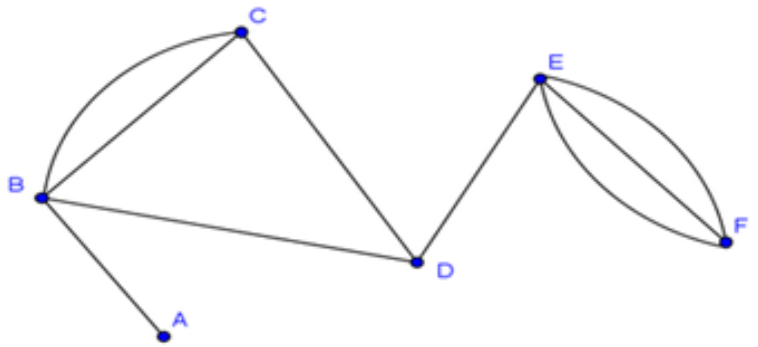
In the above graph, if the path chosen is $a \to b \to c \to d \to e \to g$ *then the length of the path is :*

$$5 + 4 + 5 + 6 + 5 = 25.$$

Definition 2.16. ***MULTI GRAPH***

A graph in which there are multiple edges between any pair of vertices or there are edges from a vertex to itself (loop) is called a multi - graph.

EXAMPLE:

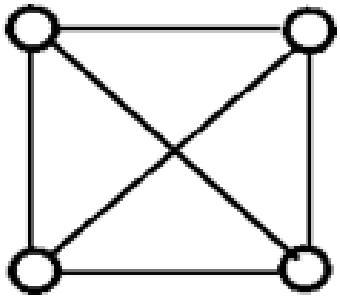


In the above graph, vertex-set B *and* C *are connected with two edges. Similarly, vertex sets* E *and* F *are connected with* 3 *edges. Therefore, it is a multi graph.*

Definition 2.17. ***PLANAR GRAPH***

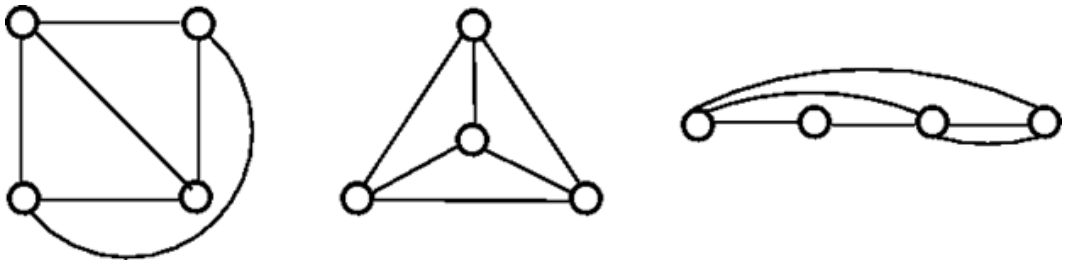
A planar graph is a graph that we can draw in a plane in such a way that no two edges of it cross each other except at a vertex to which they are incident,
i.e., A planar graph is a graph that can be embedded in the plane such that its edges intersect only at their endpoints.

EXAMPLE:



The above graph may not seem to be planar because it has edges crossing each other. But we can redraw the above graph.

The three plane drawings of the above graph are:



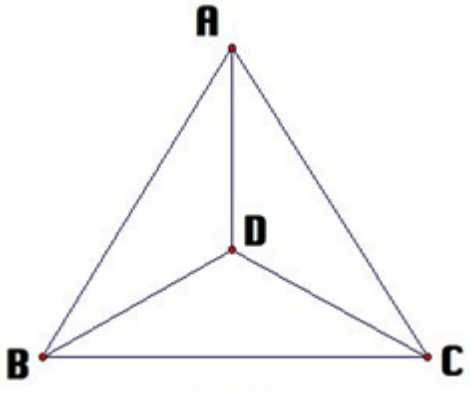
The above three graphs do not consist of two edges crossing each other and therefore, all the above graphs are planar.

2.2 PROPERTIES OF GRAPHS

2.2.1 DISTANCE BETWEEN TWO VERTICES

Distance is basically the number of edges in a shortest path between vertex X and vertex Y. If there are many paths connecting two vertices, then the shortest path is considered as the distance between the two vertices.
Distance between any two vertices X and Y is denoted by $d(X, Y)$.

EXAMPLE:



Suppose, we want to find the distance between vertex B and D. Then, first of all, we have to find the shortest path between vertex B and D.
There are many paths from vertex B to vertex D:

- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Here, length = 3
- B $\rightarrow$ D. Length = 1 (Shortest Path)
- B $\rightarrow$ A $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ D. Length = 2
- B $\rightarrow$ C $\rightarrow$ A $\rightarrow$ D. Length = 3

Hence, the minimum distance between vertex B and vertex D is 1.

2.2.2 ECCENTRICITY OF A VERTEX

Eccentricity of a vertex is the maximum distance between a vertex to all other vertices. It is denoted by $e(V)$.
For a disconnected graph, all vertices are defined to have infinite eccentricity.

2.2.3 RADIUS OF CONNECTED GRAPHS

The radius of a connected graph is the minimum eccentricity from all the vertices. In other words, the minimum among all the distances between a vertex to all other vertices is called as the radius of the graph.
It is denoted by $r(G)$.

2.2.4 DIAMETER OF A GRAPH

Diameter of a graph is the maximum eccentricity from all the vertices. In other words, the maximum among all the distances between a vertex to all other vertices is considered as the diameter of the graph G.
It is denoted by $d(G)$.

2.2.5 CENTRAL POINT

If the eccentricity of the graph is equal to its radius, then it is known as central point of the graph,

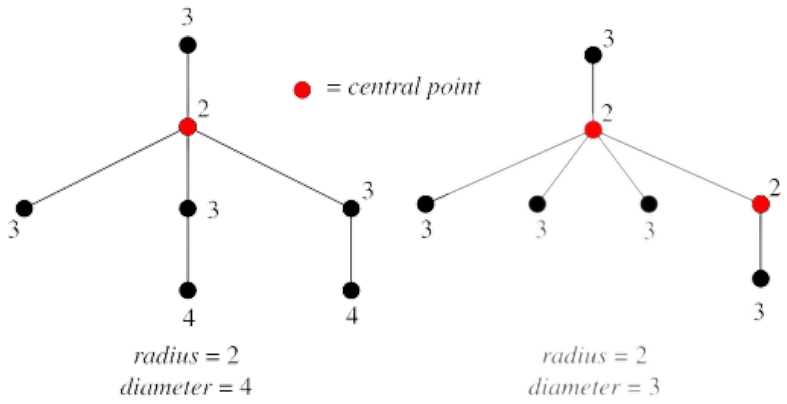
Or,

If $r(V) = e(V)$, then V is the central point of the graph G.

2.2.6 CENTRE OF A GRAPH

The set of all the central point of the graph is known as centre of the graph.

2.2.7 EXAMPLE



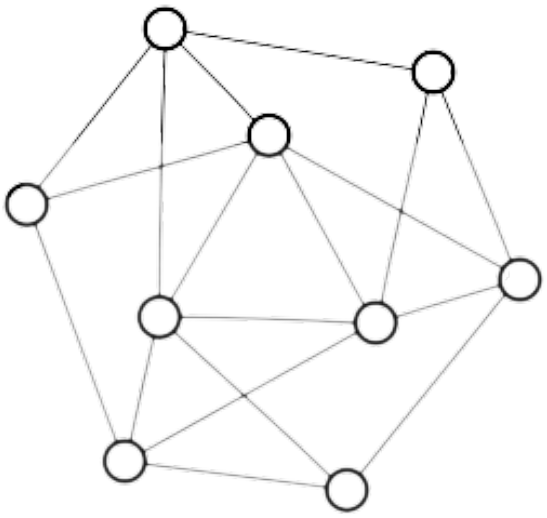
2.2.8 CIRCUMFERENCE OF A GRAPH

The total number of edges in the longest cycle of graph G is known as the circumference of G.

2.2.9 GIRTH

The total number of edges in the shortest cycle of graph G is known as girth.
It is denoted by $g(G)$.

2.2.10 EXAMPLE



For the above graph,

- Order $= 9$.
- Size (number of edges) $= 18$.
- Radius $= 2$.
- Circumference $= 9$.
- Girth $= 3$.

CHAPTER 3

THE FIRST THEOREM OF GRAPH THEORY

3.1 THE FIRST THEOREM

Theorem 3.1.1. *For any graph G with e edges and n vertices: $v_1, v_2, ..., v_n$,*

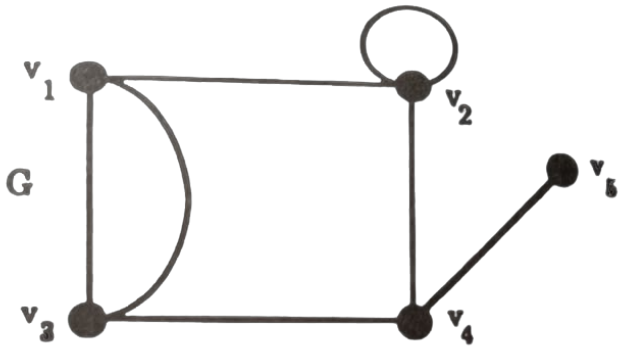
$$\sum_{i=1}^{n} d(v_i) = 2e \tag{3.1}$$

ie, In a graph G, the sum of the degrees of the vertices is equal to twice the number of edges.

Proof.

Each edge, since it has two end vertices, contributes precisely 2 to the sum of the degrees, i.e, when the degrees of the vertices are summed, each edge is counted twice.
□

3.1.1 EXAMPLE



In the above graph, we have,

1. $d(v_1) = 3$
2. $d(v_2) = 4$
3. $d(v_3) = 3$
4. $d(v_4) = 3$
5. $d(v_5) = 1$
6. Number of edges, $e = 7$.

Then,

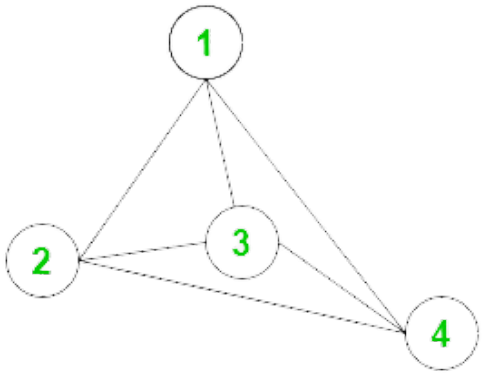
$$d(v_1) + d(v_2) + d(v_3) + d(v_4) + d(v_5) = 14 = 2 \times e \tag{3.2}$$

i.e.,

$$\sum_{i=1}^{5} d(v_i) = 2 \times 7 = 14 \tag{3.3}$$

Remark 1. *A vertex of a graph is called odd or even depending on whether its degree is odd or even.*

EXAMPLE:



Here, the vertex degrees are:

1. $d(1) = 3$
2. $d(2) = 3$
3. $d(3) = 3$
4. $d(4) = 3$

Hence, all the vertices here are called odd vertices.

Corollary 3.1.1.1. *In a graph G, there is an even number of odd vertices.*

Proof. Let W be the set of odd vertices of G and let U be the set of even vertices of G.
Then, for each $u \in U$, $d(u)$ is even.
Also,

$$\sum_{u \in U} d(u),$$

being a sum of even numbers, is even.

However, by the previous theorem where V is the vertex set of G and e is the number of its edges,

$$\sum_{u \in U} d(u) + \sum_{w \in W} d(w) = \sum_{v \in V} d(v) = 2e. \tag{3.4}$$

Thus,

$$\sum_{w \in W} d(w) = 2e - \sum_{u \in U} d(u), \tag{3.5}$$

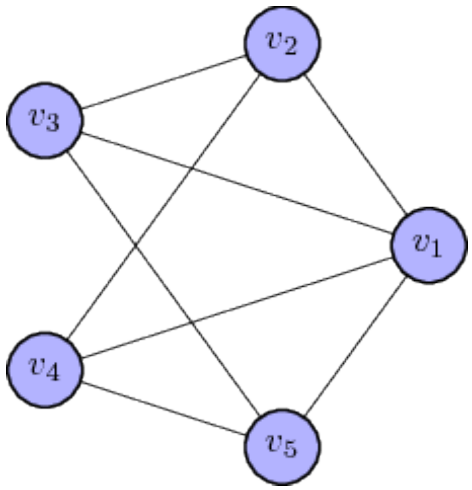
is even (being the difference of two even numbers).

As all the terms in:

$$\sum_{w \in W} d(w),$$

are odd and their sum is even, there must be an even number of them (because the sum of an odd number of odd numbers is odd).
□

EXAMPLE:

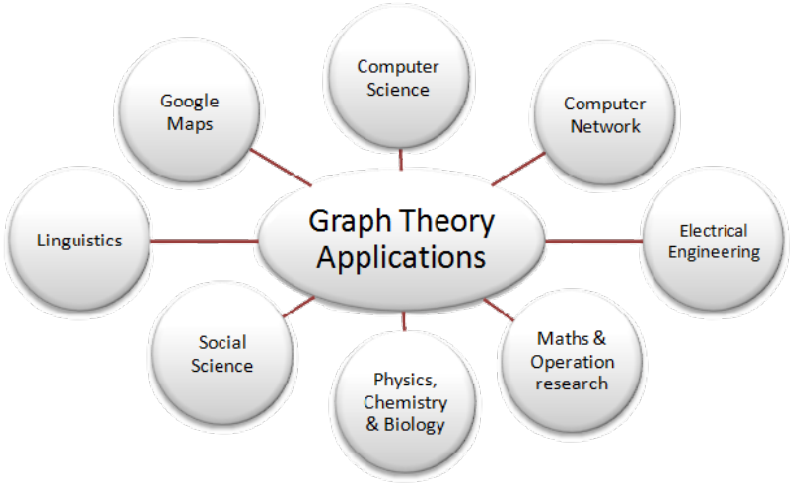


In the above graph, $d(v_1) = 4$, $d(v_2) = 3$, $d(v_3) = 3$, $d(v_4) = 3$ and $d(v_5) = 3$. Hence, out of the 5 vertices, v_2, v_3, v_4 and v_5 have odd degrees, i.e., there is an even number (4) of odd vertices.

CHAPTER 4

APPLICATIONS OF GRAPH THEORY

Graph Theory is used in vast area of science and technologies.



1. **COMPUTER SCIENCE**
   In computer science, graph theory is used for the study of algorithms like:

   - **Dijkstra's Algorithm** : Dijkstra's algorithm allows us to find the shortest path between any two vertices of a graph. This algorithm helps in finding the shortest paths between nodes in a graph, which may represent, for example, road networks.

- **Prim's Algorithm** : Prim's Algorithm is a greedy algorithm that is used to find the subset of edges that includes every vertex of the graph such that the sum of the weights of the edges can be minimized for a weighted undirected graph.
- **Kruskal's Algorithm**: Kruskal's Algorithm is used to discover the shortest path between two points in a connected weighted graph.

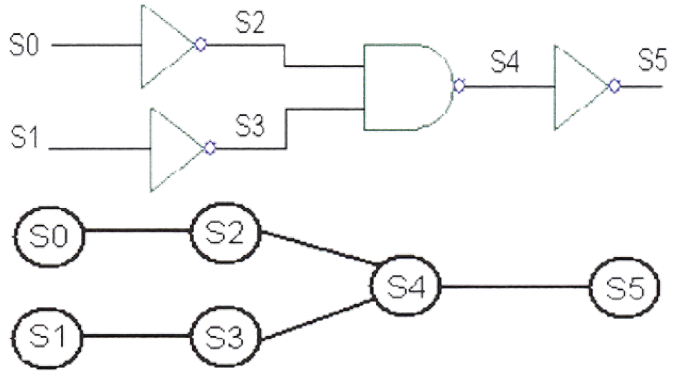
Moreover, graphs are used:

- To define the flow of computation.
- To represent networks of communication.
- To represent data organization.
- To find shortest path in road or a network.
- In Google Maps, various locations are represented as vertices or nodes and the roads are represented as edges and graph theory is used to find the shortest path between two nodes.

2. **ELECTRICAL ENGINEERING**

In Electrical Engineering, graph theory is used in designing of circuit connections. These circuit connections are named as topologies. Some topologies are series, bridge, star and parallel topologies.

EXAMPLE:



3. **LINGUISTICS**

- In linguistics, graphs are mostly used for parsing of a language tree and grammar of a language tree.
- Semantics networks are used within lexical semantics, especially as applied to computers, modeling word meaning is easier when a given word is understood in terms of related words.
- Methods in phonology (e.g. theory of optimality, which uses lattice graphs) and morphology (e.g. morphology of finite - state, using finite-state transducers) are common in the analysis of language as a graph.

4. **PHYSICS AND CHEMISTRY**

- In physics and chemistry, graph theory is used to study molecules.
- The 3D structure of complicated simulated atomic structures can be studied quantitatively by gathering statistics on graph-theoretic properties related to the topology of the atoms.
- Statistical physics also uses graphs. In this field graphs can represent local connections between interacting parts of a system, as well as the dynamics of a physical process on such systems.
- Graphs are also used to express the micro-scale channels of porous media, in which the vertices represent the pores and the edges represent the smaller channels connecting the pores.
- Graph is also helpful in constructing the molecular structure as well as lattice of the molecule. It also helps us to show the bond relation in between atoms and molecules, also help in comparing structure of one molecule to other.

5. **COMPUTER NETWORK**

- In computer network, the relationships among interconnected computers within the network, follow the principles of graph theory.
- Graph theory is widely used in modeling and routing in networks.
- Graph theory is also used in network security.

6. **SOCIAL SCIENCES**

- Graph theory is also used in sociology. For example, to explore rumor spreading, or to measure actors' prestige notably through the use of social network analysis software.
- Acquaintanceship and friendship graphs describe whether people know each other or not.
- In influence graphs model, certain people can influence the behavior of others.
- In collaboration graphs model to check whether two people work together in a particular way, such as acting in a movie together.

7. **BIOLOGY**

- Nodes in biological networks represent bio-molecules such as genes, proteins or metabolites, and edges connecting these nodes indicate functional, physical or chemical interactions between the corresponding bio-molecules.
- Graph theory is used in transcriptional regulation networks.
- It is also used in Metabolic networks.
- In PPI (Protein - Protein interaction) networks graph theory is also useful.
- Characterizing drug - drug target relationships.

8. **MATHEMATICS**

In mathematics, operational research is the important field. Graph theory provides many useful applications in operational research like:

- Minimum cost path.
- A scheduling problem.

9. **MISCELLANEOUS**

Graphs are used to represent the routes between the cities. With the help of tree that is a type of graph, we can create hierarchical ordered information such as family tree.

CONCLUSION

Graph theory has delivered important scientific discoveries, such as improved understanding of breakdown of electricity distribution systems or the propagation of infections in social networks, till date.

Graph theory also provides a remarkably simple way to characterize the complexity of ecological networks. Indices such as connectance, degree distribution or network topology serve as basic measurements to describe their structure. Such indices facilitate comparison between different systems and revealing commonalities and variations. Nowadays, the relatively important number of network studies leads to a myriads of ways to sample, analyze and interpret them.

Graph theory is an exceptionally rich area for programmers and designers. Graphs can be used to solve some very complex problems, such as least cost routing, mapping, program analysis, and so on. Network devices, such as routers and switches, use graphs to calculate optimal routing for traffic.

Graph theory is rapidly moving into the mainstream of mathematics mainly because of its applications in diverse fields which include biochemistry (genomics), electrical engineering (communications networks and coding theory), computer science (algorithms and computations) and operations research (scheduling).

Hence, studying graphs through a framework provides answers to many arrangement, networking, optimization, matching and operational problems. Graphs can be used to model many types of relations and processes in physical, biological, social and information systems, and has a wide range of useful applications.

BIBLIOGRAPHY

1. J. Clark and D. A. Holton, ***A First Look at Graph Theory***, World Scientific Publishing, 1991, 1-31, 47-51.

2. Wilson, J Robin, ***An Introduction To Graph Theory***, Addison Wesley Longman Ltd, 4th ed, 1972.

3. Javapoint, *Types of Graphs*, ***<https://www.javatpoint.com/graph-theory-types-of-graphs>***

4. Javapoint, *Tree and Forest*, ***<https://www.javatpoint.com/graph-theory-tree-and-forest>***

5. Javapoint, *Basic Properties of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-basic-properties>***

6. Programiz, *Dijkstra's Algorithm*, ***<https://www.programiz.com/dsa/dijkstra-algorithm>***

7. Javapoint, *Applications of Graph Theory*, ***<https://www.javatpoint.com/graph-theory-applications>***

8. Britannica, *Graph Theory*, ***<https://www.britannica.com/topic/graph-theory>***

CODING THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

ARYA FRANCIS
DB20CMSR11

under the guidance of
Ms. Ajeena Joseph

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty
March 2023

Examiners:

1.

2.

CERTIFICATE

This is to certify that **"Coding Theory"** is a bona fide project of **ARYA FRANCIS DB20CMSR11** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head of department

Ms. Ajeena Joseph
Project Supervisor

DECLARATION

I, **ARYA FRANCIS**, hearby declare that the project **"Coding Theory"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Ms. Ajeena Joseph**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

ARYA FRANCIS
DB20CMSR11

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organisation for supporting me throughout the course of the successful accomplishment of this project.

First I wish to express my sincere gratitude to my supervisor, Ms. Ajeena Joseph, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project.Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

CONTENTS

INTRODUCTION

Coding theory is the study of the properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines—such as information theory, electrical engineering, mathematics, linguistics, and computer science— for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data.

Coding theory, sometimes called algebraic coding theory, deals with the design of error-correcting codes for the reliable transmission of information across noisy channels. It makes use of classical and modern algebraic techniques involving finite fields, group theory, and polynomial algebra. It has connections with other areas of discrete mathematics, especially number theory and the theory of experimental designs.

The history of coding theory is in 1948, Claude Shannon published "A Mathematical Theory of Communication", an article in two parts in the July and October issues of the Bell System Technical Journal. This work focuses on the problem of how best to encode the information a sender wants to transmit. In this fundamental work he used tools in probability theory, developed by Norbert Wiener, which were in their nascent stages of being applied to communication theory at that time. Shannon developed information entropy as a measure for the uncertainty in a message while essentially inventing the field of information theory.The binary Golay

code was developed in 1949. It is an error-correcting code capable of correcting up to three errors in each 24-bit word, and detecting a fourth.

In first chapter 'Introduction to Coding Theory' we discussed about some basic concept of Coding Theory. It includes Basic Assumption where some fundamental definition and assumptions are stated, Information Rate, The Effect of Error Correction and Detection, Weight and Distance, Maximum Likelihood Decoding, Reliability of MLD, Error Detection and Correction. In the second chapter 'Linear Code' we discuss about linear codes and its properties and also some theorems. Linear Code is an important concept in Coding Theory. Second chapter includes Independence, Basis and Dimension, Matrices, Finding Bases for C, Generating Matrices, Parity Check Matrices, Equivalent Code, Distance of Linear Codes, Cosets, MLD of Linear Code.

PRELIMINARY

Binary Number

A binary number is a number expressed in the basis-2 numerical system or binary number system, a method of which uses only two symbols: typically "0" and "1".

Binary Addition

Binary addition is the sum of two or more binary numbers. Binary addition rules is,
0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

Probability

Probability is the likelihood that an event will occur and is calculated by dividing the number of favourable outcomes by the total number of possible outcomes.

Linear Combination

Let V be a vector space and S is non empty subset of V. A vector x in V is said to be a linear combination of elements of S if there exist a finite number of elements y_1,y_2,.....,y_n in S and scalars α_1,α_2,.....,α_n in F such that x=$\alpha_1 y_1$+$\alpha_2 y_2$+.....+$\alpha_n y_n$

Span

Let S be a non-empty subset of a vector space V, the set of all linear combination of S is called Span of S. It is denoted by [S] or Span(S).

Subspace

A subset W of a vector space V over a field F is called a subspace of V if W is a vector space over F under the operation of addition and scalar multiplication defined on V.

Subset

A set A is a subset of another set B if all element of the set A are element of the set B.

Linearly Independent and Dependent

Let S=$\{u_1,u_2,.....,u_n\}$ be a subset of a vector space V, $\alpha_1,\alpha_2,.....,\alpha_n$ be scalars and $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n$ be a linear combination of S.

The set S=$\{u_1,u_2,.....,u_n\}$ is said to be Linearly Independent if $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n=0 \Rightarrow \alpha_1=\alpha_2,.....=\alpha_n= 0$ (The only solution).

If there exist a non-trivial solution for $\alpha_1,\alpha_2,.....,\alpha_n$, That is atleast one α_i is not zero. Then the set is called Linearly Dependent.

Dimension

Let β be a basis of a vector space V if the number of vectors in β is n then the vector space V is called n-dimensional vector space and written as dim(V)=n.

Elementary Row Operation

The operation that are performed on rows of a matrix.

Rank

The number 'r' with the following two properties is called the Rank of the matrix.

1. There is atleast one non-zero minor of order r.
2. Every minor of order (r+1) is zero or vanish.

Cosets

Coset is subset of mathematical group consisting of all the products obtained by multiplying fixed element of group by each of elements of given subgroup, either on right or on left. Cosets are basic tool in study of groups

CHAPTER 1

INTRODUCTION TO CODING THEORY

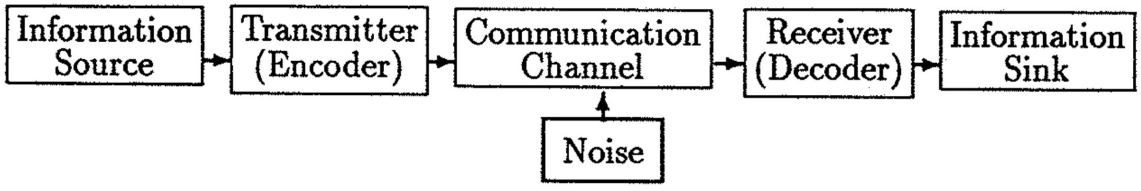
1.1 Coding Theory

Coding theory is the study of methods for efficient and accurate transfer of information from one place to another.

Definition 1.1. ***Channel***
The physical medium through which the information is transmitted is called a channel.

Definition 1.2. ***Noise***
Undesirable disturbance which may cause the information received to differ from what was transmitted is called noise.

Coding theory deals with the problem of dealing and correcting transmission error caused by noise on the channel.Rough idea of a general information transmission system.



The most important part of diagram is noise because without it there would be no need for coding theory.

1.2 Basic Assumption

We state some fundamental definitions and assumptions which will be applied in the coding theory.

Definition 1.3. ***Digits***
The information to be sent is transmitted by a sequence of 0's and 1's which is called digits.

Definition 1.4. ***Word***
Word is a sequence of digits.

Definition 1.5. ***Length of Word***
The length of a word is the number of digits in the word.

Definition 1.6. ***Binary Code***
A binary code is the set of words.
Eg: C= {00,01,10,11}

Definition 1.7. ***Block Code***
A block code is code having all its words of the same length.

Definition 1.8. ***Codewords***
The words that belong to a given code is called codewords. We denote the number of codewords in a code c by $|c|$.

A word is transmitted by sending its digits one after other across a binary channel. Each digit is transmitted mechanically, electrically, magnetically or by one of two types of easily differentiated pulses.

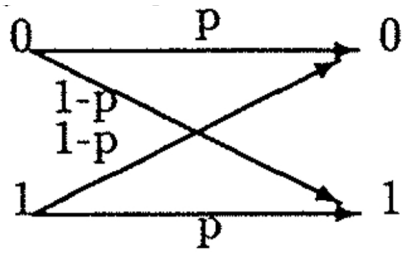
The codeword of length n is received as a word of length n. There is no difficulty in identifying the beginning of the first word transmitted. For example if we are using codeword of length 3 and receive

011011001, then the word received are in order 011,011,001.

Noise is scattered randomly as opposed to being in clumps is called bursts. That is the probability of any one digit being affected in transmission is same as that of any other digit and is not influenced by errors made in neighbouring digits.

A binary channel is symmetric, if 0 and 1 are transmitted with equal accuracy. The reliability of Binary Symmetric Channel(BSC) is a real number p , $0 \leq p \leq 1$, where p is the probability that the digit sent is the digit received.

If p is the probability that the digit received is the digit sent and 1-p is the probability that the digit received is not the digit sent. Then the following diagram shows how BSC operates.



Remarks

- The total number of words of length n is 2^n.
- If p=1 is the perfect channel then there is no chance of a digit being altered in transmission. If all Channel is perfect. then there is no need of coding theory. But no channel is perfect.
- Any channel with $0 \leq p \leq \frac{1}{2}$ can be converted into a channel with $\frac{1}{2} \leq p \leq 1$. We are using BSC with probability $\frac{1}{2} < p < 1$.
- Actually a channel p=0 is uninteresting because we can change by converting 0's into1 and 1's into 0. This will not help in the development coding theory.

1.3 Information Rate

The addition of digits to codeword may be improve error correction. $\frac{1}{n}\ log_2|\mathrm{c}|$ is the information rate of a code is the number that is designs measure the proportion of each codeword.The information rate ranges between 0 and 1.

1.4 The Effects Of Error Correction And Detection

To demonstrate the dramatic effect that the addition of a parity-check digit to a code can have in recognizing when error occur, we consider the following codes.
Suppose that all 2^{11} words of length 11 are codewords; then no error is detected.
Let the reliability of the channel be p = 1-10^{-8}.
Suppose that digits are transmitted at the rate of 10^7 digits per second.
The probability that the word is transmitted incorrectly is approximately $11p^{10}$(1-p), is about $\frac{11}{10^8}$.

$$\frac{11}{10^8}\ .\ \frac{10^7}{11} = 0.1 \text{ words per second}$$

are transmitted incorrectly without being detected. That is one wrong word every 10 seconds, 6 a minute, 360 an hour, or 8640 a day!

Now suppose that a parity-check digit is added to each codeword, so the number of 1's in each of the 2048 codewords is even. Then any single error is always detected, so at least 2 errors must occur if a word is to be transmitted incorrectly without our knowledge. The probability of at least 2 error occurring is 1-p^{12}-$12P^{11}$(1-p) which is approximated by $\binom{12}{2}p^{10}$(1-p)^2.

$$\text{p=1-}10^{-8} \rightarrow \frac{66}{10^{16}}$$

Now approximately

$$\frac{66}{10^{16}}\frac{10^7}{12} = 5.5\times 10^{-9}$$

words per second are transmitted incorrectly without being detected. That is about one error every 2000 days!

So if we are willing to reduce the information rate by lengthening the code from 11 to 12 we are very likely to know when errors occur. To decide where these errors have actually occurred, we may need to request the retransmission of the message. Physically this means that either transmission must be held up until confirmation is received or messages must be stored temporarily until retransmission is requested; both alternatives may be very costly in time or in storage space.

Therefore, at the expense of further increase in wordlength, it may well be worth incorporating error- correction capabilities into the code. Introducing such capabilities may also make encoding and decoding more difficult, but will help to avoid the hidden costs in time or space mentioned above.

One simple scheme to introduce error-correction is to form a repetition code where each codeword is transmitted three times in succession. Then if at most one error is made per 33 digit codeword, at least two of the three transmission will be correct. Then the information rate is $\frac{1}{3}$. So we add only 4 extra digit to each 11 digit codeword. This produce a code with information rate $\frac{11}{15}$.

So it is our task to design codes with reasonable information rates, low encoding and decoding costs and some error-correcting or error-detecting capabilities that make the need for retransmission unlikely.

1.5 Weight And Distance

Let v be a word of length n. The Hamming weight or simply weight of v is the number of times the digit 1 occur in v . We denote weight of v as wt(v).

Example 1.5.1. *wt(110101)= 4*

Let v and w be words of length n. Then the Hamming Distance or simply distance between v and w is the number of positions in which v and w disagree. We denote distance between v and w as d(v,w).

Eg: d(01011,00111)=2

Note

The distance between v and w is same as the weight of error pattern. That is

$$d(v, w) = wt(v+w).$$

Example 1.5.2. *d(v, w) =d(11010,01101)=4*
wt(v+w) = wt(11010=01101) = wt(10111) = 4

The probability formula of error pattern u=v+w ,

$$\phi_p(v,w) = p^{n-wt(u)}(1-p)^{wt(u)}$$

1.6 Maximum Likelihood Decoding

Two basic problems of coding,

1. Encoding : We have to determine a code to use for sending our messages.
    - First we select a positive integer k, the length of each binary word corresponding to a message k, k must be chosen so that $|M| \leq |k^k| = 2^k$.
    - Next we decide how many digit we need to add to each word of length k to ensure that as many errors can be corrected or detected as we require.
    - To transmit a particular message then transmitter finds the word of length k assigned to that of message,then transmits the codeword of length n corresponding to that word of length k.

2. Decoding: A word w in $k^n$is received. Now we proceed MLD, for decoding which word v in c was sent.

   (a) Complete Maximum Likelihood Decoding: If there is one and only one word v in c close to w than any other word in c, we decode w as v. if there are several words in c closest to w, then we select arbitrary one of them and conclude that it was the codeword sent.

   (b) Incomplete MLD: if there is a unique word v in c closest to w, then we decode w as v. but if there are several words in c, at the same distance from w, then we request a retransmission. In some cases if the received word w is too far away from any word in the code, we ask for a retransmission.

1.7 Reliability Of MLD

The probability that if v is sent over a BSC of probability p then IMLD correctly concludes that v was sent. θ_p(C,v) is the sum of all the probabilities θ_p(v,w) as w ranges over L(v). That is,

$$\theta_p(\text{C,v})=\sum_{w\in L(v)} \theta_p(v,w)$$

where L(v) all word which are close to v. The higher the probability is, the more correctly the word can be decoded.

1.8 Error Detection and correction

Error Detecting Code

If v in C sent and w in k^n is received, then u=v+w is the error pattern. Any word u in k^n can occur as an error pattern, and we wish to know which error patterns C will detect.
We say that code C detects the error pattern u if and only if v+u is not a codeword, for every v in C. In other words, u is detected if for any transmitted codeword v, the decoder upon receiving v+u can recognize that it is not a codeword and hence that some error has

occurred.

Example 1.8.1. *Let C={001, 101, 110} for the error pattern u=010. We calculate v+010 for all v in C.*

$$001+010=011,\ 101+010=111,\ 110+010=100$$

None of the three words 011, 111 or 100 is in C, so C detects the error pattern 010. On the other hand, for the error pattern u= 100,

$$001+100=101,\ 101+100=001,\ 110+100=010$$

Since at least one of these sums is in C, C does not detect the error pattern 100.

Error Correcting Code

If a word v in a code C is transmitted over BSC and w is the received resulting in the error pattern u=v+w. Then code C corrects the error pattern u, if for all v in C, v+u is closer to v than to any other word in C. Also, a code is said to be a t error correcting code if it corrects all error patterns of weight at most t and does not correct at least one error pattern of weight t+1.

Example 1.8.2. *Let C={000,111}*

- *Take the error pattern u=010. For v=000*

  $$d(000,v+u)=d(000,010)=1 \text{ and}$$
  $$d(111,v+u)=d(111,010)=2$$

  And for v=111,

  $$d(000,v+u)=d(000,101)=2$$
  $$d(111,v+u)=d(111,101)=1$$

  Thus C corrects the error pattern 010.

- *Now take the error pattern u=110. For v=000*

d(000,v+u)=d(000,110)=2 and
d(111,v+u)=d(111,110)=1

Since v+u is not closer to v=000 than to 111. C does not correct the error pattern 110.

CHAPTER 2

LINEAR CODE

2.1 Linear code

A code C is called a linear code if v+w is a word in C whenever v and w are in C. That is, a linear code is a code which is closed under addition of words.

Example 2.1.1. *C = {000, 111} is a linear code, since all four of the sums.*

000+000=000
000+111=111
111+000=111
111+111=000

are in C. But C_1 = {000, 001, 101} is not a linear code, since 001 and 101 are in C_1 but 001+101 is not in C_1.

2.2 Two Important Subspace

The vector w is said to be a linear combination of vectors $v_1, v_2, \ldots\ldots v_K$, if there are scalars $a_1, a_2, \ldots\ldots a_k$ as such that,

$$w=a_1v_1+a_2v_2+\ldots\ldots+a_kv_k$$

The set of all linear combinations of the vectors in a given set $S=\{v_1,v_2,\ldots\ldots v_k\}$ is called the linear span of S, and is denoted by <S>.

If S is empty, we define <S>= {0}.
In linear algebra it is shown that for any subset S of a vector space V, the linear span <S> is a subspace of V, called the subspace spanned or generated by S.

Theorem 2.2.1. *For any subset S of K^n, the code C=<S> generated by S consists precisely of the following words the zero word, all words in S, and all sums of two or more words in S.*

Example 2.2.1. *Let S = {0100, 0011, 1100}. Then the code C =<S> generated by S consists of*

0000, 0100, 0100+0011=0111, 0100+0011+1100=1011,
1100, 0011,0100+1100=1000, 0011+1100=1111;

that is, C=<S>={0000,0100,0011,1100,0111,1000,111,1011}.

2.3 Independence, Basis, Dimension

The main objective is to find an efficient way to describe a linear code without having to list all the codewords.
A set S={v_1,v_2,.....v_k} of vectors is linearly dependent if these are scalars a_1, a_2,.....a_k not all zero such that,

$$a_1v_1+a_2v_2+.....+a_kv_k=0$$

Otherwise the set S is linearly independent.
The test for linear independence, then, is to form the vector equation using arbitrary scalars. All the scalars a_1, a_2,.....a_k to be 0, then the set S is linearly independent. If at least one a_i can be chosen to be non-zero then S is linearly independent.
Any set of vectors containing the zero vectors is linearly dependent.
A nonempty subset B, of vectors from a vector space V is a basis for V if both:

1. B spans V (that is, <B>=V)
2. B is linearly independent set.

Note
Any Linearly independent set B is automatically a basis for <B>. Also since any linearly independent set S of vectors that contains a nonzero word always contains a largest independent subset B, we can extract from S a basis B for <S>. If S={0} then we say that the basis of S is the empty set $\emptyset$.

Theorem 2.3.1. *A linear code of dimension k contains precisely 2^k codewords.*

Theorem 2.3.2. *Let C=<S> be the linear code generated by a subset S of k^n. Then (dimension of C)+(dimension of $C^{\perp}$)=n*

Theorem 2.3.3. *A linear code of dimension k has precisely* $\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$ *different bases.*

Example 2.3.1. *The linear code k^4 and hence* $\frac{1}{4!}\prod_{i=0}^{3}(2^4 - 2^i)$= $\frac{1}{4!}$ *(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)= 840 different bases. Any linear code contained in k^n, for n≥4 which has dimension 4 also has 840 different bases.*

2.4 Matrices

An m×n matrix is a rectangular array of scalars with m rows and n columns. If A is an m × n matrix and B is an n×p matrix, then the product AB is the m×p matrix which has for its (i,j)th entry.

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

There are two types of elementary row operations which may be performed on a matrix over K. They are:

1. interchanging two rows
2. replacing a row by itself plus another row

Two matrices are row equivalent if one can be obtained from the other by a sequence of elementary row operators.
A1 in a matrix M (over K) is called a leading 1 if there are no 1s to its left in the same row, and a column of M is called a leading column if it contains a leading 1. M is in Row Echelon Form (REF) if the zero rows of M (if any) are all at the bottom, and each leading 1 is to the right of the leading 1s in the rows above.
If further, each leading column contains exactly one 1, M is in Reduced Row Echelon Form (RREF).

Example 2.4.1. *Find the REF for the matrix M below using elementary row operation.*

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

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 1 to row 2, row 3 and row 4)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 2 to row 3)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 4)*

So the REF of matrix M is

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

Example 2.4.2. *Find the RREF for the matrix M below using elementary row operation.*

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

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$ *(add row 1 to row 2 and to row 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(interchange row 2 and 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 1)*

So the RREF of matrix M is

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

2.5 Bases for C=<S> and $C^{\perp}$

We develop algorithms for finding bases for a linear code and its dual.
Let S be a nonempty subset of K^n. The first two algorithms provide a basis for C=<S>, the linear code generated by S.

Algorithm 2.5.1. *Form the matrix A whose rows are the words in S. Use elementary row operations to find a REF of A. Then the nonzero*

rows of the REF form a basis for C =<S>.
The algorithm works because the rows of A generate C and elementary row operations simply interchange words or replace one word (row) with another in C giving a new set of codewords which still generates C. Clearly the nonzero rows of a matrix in REF are linearly independent.

Example 2.5.1. *We find a basis for the linear code C=<S> for S = {11101, 10110, 01011, 11010}*

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

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&1&0&1&1\\0&0&1&1&1\end{bmatrix}$$ *(add row 1 to row 2 and to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&1&0&1&1\end{bmatrix}$$ *(interchange row 3 to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&0&0&0&0\end{bmatrix}$$ *(add row 2 to row 4)*

The last matrix is a REF of A. By Algorithm 2.5.1. {11101, 01011, 00111} is a basis for C=<S> . Another REF of A is

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

So {11101, 01100, 00111} is also a basis for C=<S >. Note that Algorithm 2.5.1 does not produce a unique basis for <S>, nor are the words in the basis necessarily in the given set S.

Algorithm 2.5.2. *Form the matrix A whose rows are the words in S. Use elementary row operations to place A in RREF. Let G be the k×n matrix consisting of all the nonzero rows of the RREF. Let X be the k×(n-k) matrix obtained from G by deleting the leading columns of G. Form an n×(n-k) matrix H as follows:*

1. *In the rows of H corresponding to the leading columns of G, place, in order,the rows of X.*
2. *In the remaining n-k rows of H, place, in order, the rows of the (n-k)×(n-k) identity matrix I.*

Then the columns of H form a basis for $C^{\perp}$

2.6 Generating Matrices and Encoding

The rank of a matrix over K is the number of nonzero rows in any REF of the matrix. The dimension k of the code C is the dimension of C, as a subspace of K^n. If C also has length n and distance d, then we refer to C as an (n, k, d) linear code.
If C is a linear code of length n and dimension k, then any matrix whose rows form a basis for C is called a generator matrix for C.
Note
A generator matrix for C must have k rows and n columns and it must have rank k.

Theorem 2.6.1. *A matrix G is a generator matrix for some linear code C if and only if the rows of G are linearly independent, that is, if and only if the rank of G is equal to the number of rows of G.*

Theorem 2.6.2. *If G is a generator matrix for a linear code C, then any matrix row equivalent to G is also a generator matrix for C. In particular, any linear code has a generator matrix in RREF.*

Example 2.6.1. *We find a generator matrix for the code C={0000,1110,0111,1001}. Using Algorithm 2.5.1,*

$$A=\begin{bmatrix}0&0&0&0\\1&1&1&0\\0&1&1&1\\1&0&0&1\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&0&0&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&1&1&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

so $G=\begin{bmatrix}1&1&1&0\\0&1&1&1\end{bmatrix}$ *is a generator matrix for C. By Algorithm 2.5.2, since the RREF of A is* $\begin{bmatrix}1&0&0&1\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$, $G_1=\begin{bmatrix}1&0&0&1\\0&1&1&1\end{bmatrix}$ *is also a generator matrix for C.*

2.7 Parity Check Matrices

A matrix H is called a parity-check matrix for a linear code C if the columns of H form a basis for the dual code C. If C has length n and dimension k, then, since the sum of the dimensions of C and $C^{\perp}$ is in any parity-check matrix for C must have n rows, n-k columns and rank n - k.

Theorem 2.7.1. *A matrix H is a parity-check matrix for some linear code C if and only if the columns of H are linearly independent*

Theorem 2.7.2. *If H is a parity-check matrix for a linear code C of length n, then C consists precisely of all words v in* K^n *such that vH=0.*

Theorem 2.7.3. *Matrices G and H are generating and parity-check matrices, respectively, for some linear code C if and only if*

1. *the rows of G are linearly independent,*
2. *the columns of H are linearly independent,*
3. *the number of rows of G plus the number of columns of H equals the number of columns of G which equals the number of rows of H,*

4. GH=0

Theorem 2.7.4. *H is a parity-check matrix of C if and only if H^T is a generator matrix for $C^{\perp}$*

Example 2.7.1. *We find a parity check matrix for the code C={0000,1110,0111,1001} of Example 2.6.1. There we found that*

$$G_1 = \begin{bmatrix} 10 & 01 \\ 01 & 11 \end{bmatrix} = \begin{bmatrix} I & X \end{bmatrix}$$

is a generator matrix for C which is in RREF. By Algorithm 2.5.2, we connect H

$$H = \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

is a parity check matrix for C. Note that vH= 00 for all words v in C.

2.8 Distance of Linear Code

The distance of a linear code is the minimum weight of any nonzero codeword. The distance of a linear code can also be determined from a parity-check matrix for the code.

Theorem 2.8.1. *Let H be a parity-check matrix for a linear code C. Then C has distance d if and only if any set of d-1 rows of H is linearly independent, and at least one set of d rows of linearly dependent.*

Example 2.8.1. *Let C be the linear code with parity-check matrix*

$$H = \begin{bmatrix} 110 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

By inspection it is seen that no two rows of H sum to 000, so any two rows of H are linearly independent. But rows 1, 3, and 4, for instance sum to 000, and hence are linearly dependent. Therefore d-1=2, so the distance of C is d = 3.

2.9 Cosets

If C is a linear code of length n, and if u is any word of length n, we define the coset of C determined by u to be the set of all words of the form v+u as v ranges over all the words in C. We denote this coset by C+u. Thus,

$$C + u = \{v+u \mid v \in C\}.$$

Example 2.9.1. *Let C={000, 111}, and let u= 101. Then,*

$$C+101=\{000+ 101, 111+101\} = \{101,010\}.$$

Note that also

$$C+111= \{000+111, 111+111\}=\{111,000\} = C$$

and

$$C+010= \{000 +010, 111+010)\}=\{010, 101\}= C+101.$$

Theorem 2.9.1. *Let C be a linear code of length n. Let u and v be words of length of n.*

1. *If u is in the coset C + v, then C + u = C + v; that is, each word in a coset determines that coset.*
2. *The word u is in the coset C + u.*
3. *If u + v is in C, then u and v are in the same coset.*
4. *If u + v is not in C, then u and v are in different cosets.*
5. *Every word in K^n is contained in one and only one coset of C; that is, either C + u = C + v, or C + u and C + v have no words in common.*
6. *|C + u|= |C|; that is, the number of words in a coset of C is equal to the number of words in the code C.*
7. *If C has dimension k, then there are exactly 2^{n-k} different cosets of C, and each coset contains exactly 2^k words.*

8. *The code C itself is one of its cosets.*

Example 2.9.2. *We list the cosets of the code*

$$C = \{0000, 1011, 0101, 1110\}$$

- *C itself is a coset.(Theorem 2.10.1 (8))*
- *Every word in C will determine the coset C by (tTheorem 2.10.1 (1) and (5)), so we pick a word u in K^4 not in C. For later use in decoding, it will help to pick u of smallest weight possible. So let's take u = 1000. Then we get the coset,*

$$C + 1000 = \{1000, 0011, 1101, 0110\}.$$

- *Now pick another word, of small weight, in K but not in C or C+1000, say 0100. Form another coset,*

$$C + 0100 = \{0100, 1111, 0001, 1010\}.$$

- *Repeating the process with 0010 yields the coset*

$$C + 0010 = \{0010, 1001, 0111, 1100\}$$

- *The code C has dimension k = 2. Then,*

$$2^{n-k} = 2^{4-2} = 2^2 = 4$$

We have listed 4 cosets with $2^k = 2^n = 4$ words.and every word in K^4 is accounted for appearing in exactly one coset.

- *Also observe that 0001 + 1010= 1011 is in C, thus 0001 and 1010 are in the same coset, namely C+0100 (see (3)). On the other hand, 0100 + 0010= 0110 is not in C, and 0100 and 0010 are in different cosets (see (4)).*

2.10 MLD for Linear Code

Let C be a linear code. Assume the codeword v in C is transmitted and the word w is received, resulting in the error pattern u = v + w. Then w + u = v is in C, so the error pattern u and the received word w are in the same coset of C by (3) of Theorem 2.10.1.

Since error patterns of small weight are the most likely to occur, here is how MLD works for a linear code C. Upon receiving the word w, we choose a word u of least weight in the coset C + w (which must contain w) and conclude that v = w + u was the word sent.

Example 2.10.1. *Let C={0000, 1011, 0101, 1110}. The cosets of C (Example 2.10.2) are*

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100

Suppose w= 1101 is received.

$$C + w = C + 1101 = \{1101, 0110, 1000, 0011\}$$

The coset C + w= C+ 1101 containing w is the second one listed.
The word of least weight in this coset is u= 1000, which we choose as the error pattern.
We conclude that,

$$v = w + u = 1101 + 1000 = 0101$$

0101was the most likely codeword sent.

Now suppose w=1111 is received.

$$C + w = C + 1111 = \{1111, 0100, 1010, 0001\}$$

In the coset C+w containing 1111 there are two words of smallest weight, 0100 and 0001. Since we are doing CMLD, we arbitrarily select one of these, say u= 0100, for the error pattern, and conclude that v = w + u= 1111 + 0100 = 1011 was a most likely codeword sent.

Theorem 2.10.1. *Let C be a linear code of length n. Let H be a parity-check matrix for C. Let w and u be words in* K^n.

1. *wH = 0 if and only if w is a codeword in C.*
2. *wH = uH if and only if w and u lie in the same coset of C.*
3. *If u is the error pattern in a received word w, then uH is the sum of the rows of H that correspond to the positions in which errors occurred in transmission.*

CONCLUSION

Our aim was to take a note on coding theory by its breath of coverage. Coding theory is the study of properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines such as information theory, electrical engineering, mathematics, linguistics and computer science-for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data. This project work helps us to know more about coding theory.

I have much pleasure in conveying my heart full thanks to my teachers and colleagues.

BIBLIOGRAPHY

1. D.G.Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger and J.R. Wall,***CODING THEORY The Essentials***, Marcel Dekkar, Inc., 1991.

2. Richard W Hamming, ***Coding and Information Theory***, Prentice-Hall, Inc., 1986.

3. Steven Roman, ***Coding and Information Theory***, Springer Science and Business Media, 1992.

4. Wikipedia, Coding Theory, ***<https://en.wikipedia.org › wiki › Coding-theory>***

5. Wikipedia, Linear Code, ***<https://en.wikipedia.org › wiki › Linear-code>***

CODING THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

HRIDHU P
DB20CMSR04

under the guidance of
Ms. Ajeena Joseph

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty
March 2023

Examiners:

1.

2.

CERTIFICATE

This is to certify that **"Coding Theory"** is a bona fide project of **Hridhu P DB20CMSR04** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head of department

Ms. Ajeena Joseph
Project Supervisor

DECLARATION

I, **Hridhu P**, hearby declare that the project **"Coding Theory"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Ms. Ajeena Joseph**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

Hridhu P
DB20CMSRO4

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organisation for supporting me throughout the course of the successful accomplishment of this project.

First I wish to express my sincere gratitude to my supervisor, Ms. Ajeena Joseph, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project.Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

CONTENTS

INTRODUCTION

Coding theory is the study of the properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines—such as information theory, electrical engineering, mathematics, linguistics, and computer science— for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data.

Coding theory, sometimes called algebraic coding theory, deals with the design of error-correcting codes for the reliable transmission of information across noisy channels. It makes use of classical and modern algebraic techniques involving finite fields, group theory, and polynomial algebra. It has connections with other areas of discrete mathematics, especially number theory and the theory of experimental designs.

The history of coding theory is in 1948, Claude Shannon published "A Mathematical Theory of Communication", an article in two parts in the July and October issues of the Bell System Technical Journal. This work focuses on the problem of how best to encode the information a sender wants to transmit. In this fundamental work he used tools in probability theory, developed by Norbert Wiener, which were in their nascent stages of being applied to communication theory at that time. Shannon developed information entropy as a measure for the uncertainty in a message while essentially inventing the field of information theory.The binary Golay

code was developed in 1949. It is an error-correcting code capable of correcting up to three errors in each 24-bit word, and detecting a fourth.

In first chapter 'Introduction to Coding Theory' we discussed about some basic concept of Coding Theory. It includes Basic Assumption where some fundamental definition and assumptions are stated, Information Rate, The Effect of Error Correction and Detection, Weight and Distance, Maximum Likelihood Decoding, Reliability of MLD, Error Detection and Correction. In the second chapter 'Linear Code' we discuss about linear codes and its properties and also some theorems. Linear Code is an important concept in Coding Theory. Second chapter includes Independence, Basis and Dimension, Matrices, Finding Bases for C, Generating Matrices, Parity Check Matrices, Equivalent Code, Distance of Linear Codes, Cosets, MLD of Linear Code.

PRELIMINARY

Binary Number

A binary number is a number expressed in the basis-2 numerical system or binary number system, a method of which uses only two symbols: typically "0" and "1".

Binary Addition

Binary addition is the sum of two or more binary numbers. Binary addition rules is,
0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

Probability

Probability is the likelihood that an event will occur and is calculated by dividing the number of favourable outcomes by the total number of possible outcomes.

Linear Combination

Let V be a vector space and S is non empty subset of V. A vector x in V is said to be a linear combination of elements of S if there exist a finite number of elements y_1,y_2,.....,y_n in S and scalars α_1,α_2,.....,α_n in F such that x=$\alpha_1 y_1$+$\alpha_2 y_2$+.....+$\alpha_n y_n$

Span

Let S be a non-empty subset of a vector space V, the set of all linear combination of S is called Span of S. It is denoted by [S] or Span(S).

Subspace

A subset W of a vector space V over a field F is called a subspace of V if W is a vector space over F under the operation of addition and scalar multiplication defined on V.

Subset

A set A is a subset of another set B if all element of the set A are element of the set B.

Linearly Independent and Dependent

Let S=$\{u_1,u_2,.....,u_n\}$ be a subset of a vector space V, $\alpha_1,\alpha_2,.....,\alpha_n$ be scalars and $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n$ be a linear combination of S.

The set S=$\{u_1,u_2,.....,u_n\}$ is said to be Linearly Independent if $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n=0 \Rightarrow \alpha_1=\alpha_2,.....=\alpha_n= 0$ (The only solution).

If there exist a non-trivial solution for $\alpha_1,\alpha_2,.....,\alpha_n$, That is atleast one α_i is not zero. Then the set is called Linearly Dependent.

Dimension

Let β be a basis of a vector space V if the number of vectors in β is n then the vector space V is called n-dimensional vector space and written as dim(V)=n.

Elementary Row Operation

The operation that are performed on rows of a matrix.

Rank

The number 'r' with the following two properties is called the Rank of the matrix.

1. There is atleast one non-zero minor of order r.
2. Every minor of order (r+1) is zero or vanish.

Cosets

Coset is subset of mathematical group consisting of all the products obtained by multiplying fixed element of group by each of elements of given subgroup, either on right or on left. Cosets are basic tool in study of groups

CHAPTER 1

INTRODUCTION TO CODING THEORY

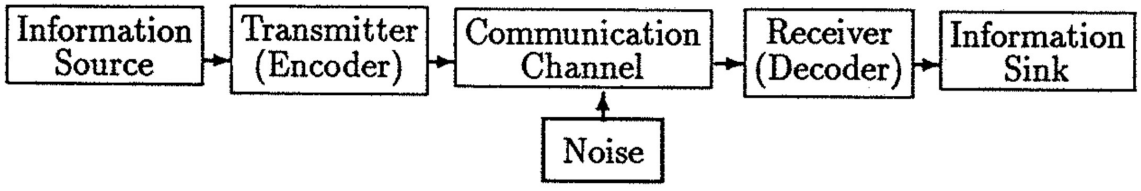
1.1 Coding Theory

Coding theory is the study of methods for efficient and accurate transfer of information from one place to another.

Definition 1.1. ***Channel***
The physical medium through which the information is transmitted is called a channel.

Definition 1.2. ***Noise***
Undesirable disturbance which may cause the information received to differ from what was transmitted is called noise.

Coding theory deals with the problem of dealing and correcting transmission error caused by noise on the channel.Rough idea of a general information transmission system.



The most important part of diagram is noise because without it there would be no need for coding theory.

1.2 Basic Assumption

We state some fundamental definitions and assumptions which will be applied in the coding theory.

Definition 1.3. ***Digits***
The information to be sent is transmitted by a sequence of 0's and 1's which is called digits.

Definition 1.4. ***Word***
Word is a sequence of digits.

Definition 1.5. ***Length of Word***
The length of a word is the number of digits in the word.

Definition 1.6. ***Binary Code***
A binary code is the set of words.
Eg: C= {00,01,10,11}

Definition 1.7. ***Block Code***
A block code is code having all its words of the same length.

Definition 1.8. ***Codewords***
The words that belong to a given code is called codewords. We denote the number of codewords in a code c by $|c|$.

A word is transmitted by sending its digits one after other across a binary channel. Each digit is transmitted mechanically, electrically, magnetically or by one of two types of easily differentiated pulses.

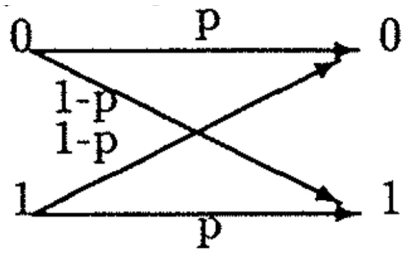
The codeword of length n is received as a word of length n. There is no difficulty in identifying the beginning of the first word transmitted. For example if we are using codeword of length 3 and receive

011011001, then the word received are in order 011,011,001.

Noise is scattered randomly as opposed to being in clumps is called bursts. That is the probability of any one digit being affected in transmission is same as that of any other digit and is not influenced by errors made in neighbouring digits.

A binary channel is symmetric, if 0 and 1 are transmitted with equal accuracy. The reliability of Binary Symmetric Channel(BSC) is a real number p , $0 \leq p \leq 1$, where p is the probability that the digit sent is the digit received.

If p is the probability that the digit received is the digit sent and 1-p is the probability that the digit received is not the digit sent. Then the following diagram shows how BSC operates.



Remarks

- The total number of words of length n is 2^n.
- If p=1 is the perfect channel then there is no chance of a digit being altered in transmission. If all Channel is perfect. then there is no need of coding theory. But no channel is perfect.
- Any channel with $0 \leq p \leq \frac{1}{2}$ can be converted into a channel with $\frac{1}{2} \leq p \leq 1$. We are using BSC with probability $\frac{1}{2} < p < 1$.
- Actually a channel p=0 is uninteresting because we can change by converting 0's into1 and 1's into 0. This will not help in the development coding theory.

1.3 Information Rate

The addition of digits to codeword may be improve error correction. $\frac{1}{n}\ log_2|\mathrm{c}|$ is the information rate of a code is the number that is designs measure the proportion of each codeword.The information rate ranges between 0 and 1.

1.4 The Effects Of Error Correction And Detection

To demonstrate the dramatic effect that the addition of a parity-check digit to a code can have in recognizing when error occur, we consider the following codes.
Suppose that all 2^{11} words of length 11 are codewords; then no error is detected.
Let the reliability of the channel be p = 1-10^{-8}.
Suppose that digits are transmitted at the rate of 10^7 digits per second.
The probability that the word is transmitted incorrectly is approximately $11p^{10}$(1-p), is about $\frac{11}{10^8}$.

$$\frac{11}{10^8}\ .\ \frac{10^7}{11} = 0.1 \text{ words per second}$$

are transmitted incorrectly without being detected. That is one wrong word every 10 seconds, 6 a minute, 360 an hour, or 8640 a day!

Now suppose that a parity-check digit is added to each codeword, so the number of 1's in each of the 2048 codewords is even. Then any single error is always detected, so at least 2 errors must occur if a word is to be transmitted incorrectly without our knowledge. The probability of at least 2 error occurring is 1-p^{12}-$12P^{11}$(1-p) which is approximated by $\binom{12}{2}p^{10}$(1-p)^2.

$$\text{p=1-}10^{-8} \rightarrow \frac{66}{10^{16}}$$

Now approximately

$$\frac{66}{10^{16}}\frac{10^7}{12} = 5.5\times 10^{-9}$$

words per second are transmitted incorrectly without being detected. That is about one error every 2000 days!

So if we are willing to reduce the information rate by lengthening the code from 11 to 12 we are very likely to know when errors occur. To decide where these errors have actually occurred, we may need to request the retransmission of the message. Physically this means that either transmission must be held up until confirmation is received or messages must be stored temporarily until retransmission is requested; both alternatives may be very costly in time or in storage space.

Therefore, at the expense of further increase in wordlength, it may well be worth incorporating error- correction capabilities into the code. Introducing such capabilities may also make encoding and decoding more difficult, but will help to avoid the hidden costs in time or space mentioned above.

One simple scheme to introduce error-correction is to form a repetition code where each codeword is transmitted three times in succession. Then if at most one error is made per 33 digit codeword, at least two of the three transmission will be correct. Then the information rate is $\frac{1}{3}$. So we add only 4 extra digit to each 11 digit codeword. This produce a code with information rate $\frac{11}{15}$.

So it is our task to design codes with reasonable information rates, low encoding and decoding costs and some error-correcting or error-detecting capabilities that make the need for retransmission unlikely.

1.5 Weight And Distance

Let v be a word of length n. The Hamming weight or simply weight of v is the number of times the digit 1 occur in v . We denote weight of v as wt(v).

Example 1.5.1. *wt(110101)= 4*

Let v and w be words of length n. Then the Hamming Distance or simply distance between v and w is the number of positions in which v and w disagree. We denote distance between v and w as d(v,w).

Eg: d(01011,00111)=2

Note

The distance between v and w is same as the weight of error pattern. That is

$$d(v, w) = wt(v+w).$$

Example 1.5.2. *d(v, w) =d(11010,01101)=4*
wt(v+w) = wt(11010=01101) = wt(10111) = 4

The probability formula of error pattern u=v+w ,

$$\phi_p(v,w) = p^{n-wt(u)}(1-p)^{wt(u)}$$

1.6 Maximum Likelihood Decoding

Two basic problems of coding,

1. Encoding : We have to determine a code to use for sending our messages.
    - First we select a positive integer k, the length of each binary word corresponding to a message k, k must be chosen so that $|M| \leq |k^k| = 2^k$.
    - Next we decide how many digit we need to add to each word of length k to ensure that as many errors can be corrected or detected as we require.
    - To transmit a particular message then transmitter finds the word of length k assigned to that of message,then transmits the codeword of length n corresponding to that word of length k.

2. Decoding: A word w in $k^n$is received. Now we proceed MLD, for decoding which word v in c was sent.

   (a) Complete Maximum Likelihood Decoding: If there is one and only one word v in c close to w than any other word in c, we decode w as v. if there are several words in c closest to w, then we select arbitrary one of them and conclude that it was the codeword sent.

   (b) Incomplete MLD: if there is a unique word v in c closest to w, then we decode w as v. but if there are several words in c, at the same distance from w, then we request a retransmission. In some cases if the received word w is too far away from any word in the code, we ask for a retransmission.

1.7 Reliability Of MLD

The probability that if v is sent over a BSC of probability p then IMLD correctly concludes that v was sent. θ_p(C,v) is the sum of all the probabilities θ_p(v,w) as w ranges over L(v). That is,

$$\theta_p(\text{C,v})=\sum_{w\in L(v)} \theta_p(v,w)$$

where L(v) all word which are close to v. The higher the probability is, the more correctly the word can be decoded.

1.8 Error Detection and correction

Error Detecting Code

If v in C sent and w in k^n is received, then u=v+w is the error pattern. Any word u in k^n can occur as an error pattern, and we wish to know which error patterns C will detect.
We say that code C detects the error pattern u if and only if v+u is not a codeword, for every v in C. In other words, u is detected if for any transmitted codeword v, the decoder upon receiving v+u can recognize that it is not a codeword and hence that some error has

occurred.

Example 1.8.1. *Let C={001, 101, 110} for the error pattern u=010. We calculate v+010 for all v in C.*

$$001+010=011,\ 101+010=111,\ 110+010=100$$

None of the three words 011, 111 or 100 is in C, so C detects the error pattern 010. On the other hand, for the error pattern u= 100,

$$001+100=101,\ 101+100=001,\ 110+100=010$$

Since at least one of these sums is in C, C does not detect the error pattern 100.

Error Correcting Code

If a word v in a code C is transmitted over BSC and w is the received resulting in the error pattern u=v+w. Then code C corrects the error pattern u, if for all v in C, v+u is closer to v than to any other word in C. Also, a code is said to be a t error correcting code if it corrects all error patterns of weight at most t and does not correct at least one error pattern of weight t+1.

Example 1.8.2. *Let C={000,111}*

- *Take the error pattern u=010. For v=000*

  $$d(000,v+u)=d(000,010)=1 \text{ and}$$
  $$d(111,v+u)=d(111,010)=2$$

  And for v=111,

  $$d(000,v+u)=d(000,101)=2$$
  $$d(111,v+u)=d(111,101)=1$$

  Thus C corrects the error pattern 010.

- *Now take the error pattern u=110. For v=000*

d(000,v+u)=d(000,110)=2 and
d(111,v+u)=d(111,110)=1

Since v+u is not closer to v=000 than to 111. C does not correct the error pattern 110.

CHAPTER 2

LINEAR CODE

2.1 Linear code

A code C is called a linear code if v+w is a word in C whenever v and w are in C. That is, a linear code is a code which is closed under addition of words.

Example 2.1.1. *C = {000, 111} is a linear code, since all four of the sums.*

000+000=000
000+111=111
111+000=111
111+111=000

are in C. But C_1 = {000, 001, 101} is not a linear code, since 001 and 101 are in C_1 but 001+101 is not in C_1.

2.2 Two Important Subspace

The vector w is said to be a linear combination of vectors $v_1, v_2, \ldots\ldots v_K$, if there are scalars $a_1, a_2, \ldots\ldots a_k$ as such that,

$$w=a_1v_1+a_2v_2+\ldots\ldots+a_kv_k$$

The set of all linear combinations of the vectors in a given set $S=\{v_1,v_2,\ldots\ldots v_k\}$ is called the linear span of S, and is denoted by <S>.

If S is empty, we define <S>= {0}.
In linear algebra it is shown that for any subset S of a vector space V, the linear span <S> is a subspace of V, called the subspace spanned or generated by S.

Theorem 2.2.1. *For any subset S of K^n, the code C=<S> generated by S consists precisely of the following words the zero word, all words in S, and all sums of two or more words in S.*

Example 2.2.1. *Let S = {0100, 0011, 1100}. Then the code C =<S> generated by S consists of*

0000, 0100, 0100+0011=0111, 0100+0011+1100=1011,
1100, 0011,0100+1100=1000, 0011+1100=1111;

that is, C=<S>={0000,0100,0011,1100,0111,1000,111,1011}.

2.3 Independence, Basis, Dimension

The main objective is to find an efficient way to describe a linear code without having to list all the codewords.
A set S={v_1,v_2,.....v_k} of vectors is linearly dependent if these are scalars a_1, a_2,.....a_k not all zero such that,

$$a_1v_1+a_2v_2+.....+a_kv_k=0$$

Otherwise the set S is linearly independent.
The test for linear independence, then, is to form the vector equation using arbitrary scalars. All the scalars a_1, a_2,.....a_k to be 0, then the set S is linearly independent. If at least one a_i can be chosen to be non-zero then S is linearly independent.
Any set of vectors containing the zero vectors is linearly dependent.
A nonempty subset B, of vectors from a vector space V is a basis for V if both:

1. B spans V (that is, <B>=V)
2. B is linearly independent set.

Note
Any Linearly independent set B is automatically a basis for <B>. Also since any linearly independent set S of vectors that contains a nonzero word always contains a largest independent subset B, we can extract from S a basis B for <S>. If S={0} then we say that the basis of S is the empty set $\emptyset$.

Theorem 2.3.1. *A linear code of dimension k contains precisely 2^k codewords.*

Theorem 2.3.2. *Let C=<S> be the linear code generated by a subset S of k^n. Then (dimension of C)+(dimension of $C^{\perp}$)=n*

Theorem 2.3.3. *A linear code of dimension k has precisely* $\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$ *different bases.*

Example 2.3.1. *The linear code k^4 and hence* $\frac{1}{4!}\prod_{i=0}^{3}(2^4 - 2^i)$= $\frac{1}{4!}$ *(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)= 840 different bases. Any linear code contained in k^n, for n≥4 which has dimension 4 also has 840 different bases.*

2.4 Matrices

An m×n matrix is a rectangular array of scalars with m rows and n columns. If A is an m × n matrix and B is an n×p matrix, then the product AB is the m×p matrix which has for its (i,j)th entry.

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

There are two types of elementary row operations which may be performed on a matrix over K. They are:

1. interchanging two rows
2. replacing a row by itself plus another row

Two matrices are row equivalent if one can be obtained from the other by a sequence of elementary row operators.
A1 in a matrix M (over K) is called a leading 1 if there are no 1s to its left in the same row, and a column of M is called a leading column if it contains a leading 1. M is in Row Echelon Form (REF) if the zero rows of M (if any) are all at the bottom, and each leading 1 is to the right of the leading 1s in the rows above.
If further, each leading column contains exactly one 1, M is in Reduced Row Echelon Form (RREF).

Example 2.4.1. *Find the REF for the matrix M below using elementary row operation.*

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

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 1 to row 2, row 3 and row 4)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 2 to row 3)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 4)*

So the REF of matrix M is

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

Example 2.4.2. *Find the RREF for the matrix M below using elementary row operation.*

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

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$ *(add row 1 to row 2 and to row 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(interchange row 2 and 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 1)*

So the RREF of matrix M is

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

2.5 Bases for C=<S> and $C^{\perp}$

We develop algorithms for finding bases for a linear code and its dual.
Let S be a nonempty subset of K^n. The first two algorithms provide a basis for C=<S>, the linear code generated by S.

Algorithm 2.5.1. *Form the matrix A whose rows are the words in S. Use elementary row operations to find a REF of A. Then the nonzero*

rows of the REF form a basis for C =<S>.
The algorithm works because the rows of A generate C and elementary row operations simply interchange words or replace one word (row) with another in C giving a new set of codewords which still generates C. Clearly the nonzero rows of a matrix in REF are linearly independent.

Example 2.5.1. *We find a basis for the linear code C=<S> for S = {11101, 10110, 01011, 11010}*

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

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&1&0&1&1\\0&0&1&1&1\end{bmatrix}$$ *(add row 1 to row 2 and to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&1&0&1&1\end{bmatrix}$$ *(interchange row 3 to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&0&0&0&0\end{bmatrix}$$ *(add row 2 to row 4)*

The last matrix is a REF of A. By Algorithm 2.5.1. {11101, 01011, 00111} is a basis for C=<S> . Another REF of A is

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

So {11101, 01100, 00111} is also a basis for C=<S >. Note that Algorithm 2.5.1 does not produce a unique basis for <S>, nor are the words in the basis necessarily in the given set S.

Algorithm 2.5.2. *Form the matrix A whose rows are the words in S. Use elementary row operations to place A in RREF. Let G be the k×n matrix consisting of all the nonzero rows of the RREF. Let X be the k×(n-k) matrix obtained from G by deleting the leading columns of G. Form an n×(n-k) matrix H as follows:*

1. *In the rows of H corresponding to the leading columns of G, place, in order,the rows of X.*
2. *In the remaining n-k rows of H, place, in order, the rows of the (n-k)×(n-k) identity matrix I.*

Then the columns of H form a basis for $C^{\perp}$

2.6 Generating Matrices and Encoding

The rank of a matrix over K is the number of nonzero rows in any REF of the matrix. The dimension k of the code C is the dimension of C, as a subspace of K^n. If C also has length n and distance d, then we refer to C as an (n, k, d) linear code.
If C is a linear code of length n and dimension k, then any matrix whose rows form a basis for C is called a generator matrix for C.
Note
A generator matrix for C must have k rows and n columns and it must have rank k.

Theorem 2.6.1. *A matrix G is a generator matrix for some linear code C if and only if the rows of G are linearly independent, that is, if and only if the rank of G is equal to the number of rows of G.*

Theorem 2.6.2. *If G is a generator matrix for a linear code C, then any matrix row equivalent to G is also a generator matrix for C. In particular, any linear code has a generator matrix in RREF.*

Example 2.6.1. *We find a generator matrix for the code C={0000,1110,0111,1001}. Using Algorithm 2.5.1,*

$$A=\begin{bmatrix}0&0&0&0\\1&1&1&0\\0&1&1&1\\1&0&0&1\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&0&0&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&1&1&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

so $G=\begin{bmatrix}1&1&1&0\\0&1&1&1\end{bmatrix}$ *is a generator matrix for C. By Algorithm 2.5.2, since the RREF of A is* $\begin{bmatrix}1&0&0&1\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$, $G_1=\begin{bmatrix}1&0&0&1\\0&1&1&1\end{bmatrix}$ *is also a generator matrix for C.*

2.7 Parity Check Matrices

A matrix H is called a parity-check matrix for a linear code C if the columns of H form a basis for the dual code C. If C has length n and dimension k, then, since the sum of the dimensions of C and $C^{\perp}$ is in any parity-check matrix for C must have n rows, n-k columns and rank n - k.

Theorem 2.7.1. *A matrix H is a parity-check matrix for some linear code C if and only if the columns of H are linearly independent*

Theorem 2.7.2. *If H is a parity-check matrix for a linear code C of length n, then C consists precisely of all words v in* K^n *such that vH=0.*

Theorem 2.7.3. *Matrices G and H are generating and parity-check matrices, respectively, for some linear code C if and only if*

1. *the rows of G are linearly independent,*
2. *the columns of H are linearly independent,*
3. *the number of rows of G plus the number of columns of H equals the number of columns of G which equals the number of rows of H,*

4. GH=0

Theorem 2.7.4. *H is a parity-check matrix of C if and only if H^T is a generator matrix for $C^{\perp}$*

Example 2.7.1. *We find a parity check matrix for the code C={0000,1110,0111,1001} of Example 2.6.1. There we found that*

$$G_1 = \begin{bmatrix} 10 & 01 \\ 01 & 11 \end{bmatrix} = \begin{bmatrix} I & X \end{bmatrix}$$

is a generator matrix for C which is in RREF. By Algorithm 2.5.2, we connect H

$$H = \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

is a parity check matrix for C. Note that vH= 00 for all words v in C.

2.8 Distance of Linear Code

The distance of a linear code is the minimum weight of any nonzero codeword. The distance of a linear code can also be determined from a parity-check matrix for the code.

Theorem 2.8.1. *Let H be a parity-check matrix for a linear code C. Then C has distance d if and only if any set of d-1 rows of H is linearly independent, and at least one set of d rows of linearly dependent.*

Example 2.8.1. *Let C be the linear code with parity-check matrix*

$$H = \begin{bmatrix} 110 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

By inspection it is seen that no two rows of H sum to 000, so any two rows of H are linearly independent. But rows 1, 3, and 4, for instance sum to 000, and hence are linearly dependent. Therefore d-1=2, so the distance of C is d = 3.

2.9 Cosets

If C is a linear code of length n, and if u is any word of length n, we define the coset of C determined by u to be the set of all words of the form v+u as v ranges over all the words in C. We denote this coset by C+u. Thus,

$$C + u = \{v+u \mid v \in C\}.$$

Example 2.9.1. *Let C={000, 111}, and let u= 101. Then,*

$$C+101=\{000+ 101, 111+101\} = \{101,010\}.$$

Note that also

$$C+111= \{000+111, 111+111\}=\{111,000\} = C$$

and

$$C+010= \{000 +010, 111+010)\}=\{010, 101\}= C+101.$$

Theorem 2.9.1. *Let C be a linear code of length n. Let u and v be words of length of n.*

1. *If u is in the coset C + v, then C + u = C + v; that is, each word in a coset determines that coset.*
2. *The word u is in the coset C + u.*
3. *If u + v is in C, then u and v are in the same coset.*
4. *If u + v is not in C, then u and v are in different cosets.*
5. *Every word in K^n is contained in one and only one coset of C; that is, either C + u = C + v, or C + u and C + v have no words in common.*
6. *|C + u|= |C|; that is, the number of words in a coset of C is equal to the number of words in the code C.*
7. *If C has dimension k, then there are exactly 2^{n-k} different cosets of C, and each coset contains exactly 2^k words.*

8. *The code C itself is one of its cosets.*

Example 2.9.2. *We list the cosets of the code*

$$C = \{0000, 1011, 0101, 1110\}$$

- *C itself is a coset.(Theorem 2.10.1 (8))*
- *Every word in C will determine the coset C by (tTheorem 2.10.1 (1) and (5)), so we pick a word u in K^4 not in C. For later use in decoding, it will help to pick u of smallest weight possible. So let's take u = 1000. Then we get the coset,*

$$C + 1000 = \{1000, 0011, 1101, 0110\}.$$

- *Now pick another word, of small weight, in K but not in C or C+1000, say 0100. Form another coset,*

$$C + 0100 = \{0100, 1111, 0001, 1010\}.$$

- *Repeating the process with 0010 yields the coset*

$$C + 0010 = \{0010, 1001, 0111, 1100\}$$

- *The code C has dimension k = 2. Then,*

$$2^{n-k} = 2^{4-2} = 2^2 = 4$$

We have listed 4 cosets with $2^k = 2^n = 4$ words.and every word in K^4 is accounted for appearing in exactly one coset.

- *Also observe that 0001 + 1010= 1011 is in C, thus 0001 and 1010 are in the same coset, namely C+0100 (see (3)). On the other hand, 0100 + 0010= 0110 is not in C, and 0100 and 0010 are in different cosets (see (4)).*

2.10 MLD for Linear Code

Let C be a linear code. Assume the codeword v in C is transmitted and the word w is received, resulting in the error pattern u = v + w. Then w + u = v is in C, so the error pattern u and the received word w are in the same coset of C by (3) of Theorem 2.10.1.

Since error patterns of small weight are the most likely to occur, here is how MLD works for a linear code C. Upon receiving the word w, we choose a word u of least weight in the coset C + w (which must contain w) and conclude that v = w + u was the word sent.

Example 2.10.1. *Let C={0000, 1011, 0101, 1110}. The cosets of C (Example 2.10.2) are*

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100

Suppose w= 1101 is received.

$$C + w = C + 1101 = \{1101, 0110, 1000, 0011\}$$

The coset C + w= C+ 1101 containing w is the second one listed.
The word of least weight in this coset is u= 1000, which we choose as the error pattern.
We conclude that,

$$v = w + u = 1101 + 1000 = 0101$$

0101was the most likely codeword sent.

Now suppose w=1111 is received.

$$C + w = C + 1111 = \{1111, 0100, 1010, 0001\}$$

In the coset C+w containing 1111 there are two words of smallest weight, 0100 and 0001. Since we are doing CMLD, we arbitrarily select one of these, say u= 0100, for the error pattern, and conclude that v = w + u= 1111 + 0100 = 1011 was a most likely codeword sent.

Theorem 2.10.1. *Let C be a linear code of length n. Let H be a parity-check matrix for C. Let w and u be words in* K^n.

1. *wH = 0 if and only if w is a codeword in C.*
2. *wH = uH if and only if w and u lie in the same coset of C.*
3. *If u is the error pattern in a received word w, then uH is the sum of the rows of H that correspond to the positions in which errors occurred in transmission.*

CONCLUSION

Our aim was to take a note on coding theory by its breath of coverage. Coding theory is the study of properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines such as information theory, electrical engineering, mathematics, linguistics and computer science-for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data. This project work helps us to know more about coding theory.

I have much pleasure in conveying my heart full thanks to my teachers and colleagues.

BIBLIOGRAPHY

1. D.G.Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger and J.R. Wall,***CODING THEORY The Essentials***, Marcel Dekkar, Inc., 1991.

2. Richard W Hamming, ***Coding and Information Theory***, Prentice-Hall, Inc., 1986.

3. Steven Roman, ***Coding and Information Theory***, Springer Science and Business Media, 1992.

4. Wikipedia, Coding Theory, ***<https://en.wikipedia.org › wiki › Coding-theory>***

5. Wikipedia, Linear Code, ***<https://en.wikipedia.org › wiki › Linear-code>***

CODING THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

SOURAG A
DB20CMSR02

under the guidance of
Ms. Ajeena Joseph

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty
March 2023

Examiners:

1.

2.

CERTIFICATE

This is to certify that **"Coding Theory"** is a bona fide project of **SOURAG A DB20CMSR02** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head of department

Ms. Ajeena Joseph
Project Supervisor

DECLARATION

I, **SOURAG A**, hearby declare that the project **"Coding Theory"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Ms. Ajeena Joseph**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

SOURAG A
DB20CMSR02

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organisation for supporting me throughout the course of the successful accomplishment of this project.

First I wish to express my sincere gratitude to my supervisor, Ms. Ajeena Joseph, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project.Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

CONTENTS

INTRODUCTION

Coding theory is the study of the properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines—such as information theory, electrical engineering, mathematics, linguistics, and computer science— for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data.

Coding theory, sometimes called algebraic coding theory, deals with the design of error-correcting codes for the reliable transmission of information across noisy channels. It makes use of classical and modern algebraic techniques involving finite fields, group theory, and polynomial algebra. It has connections with other areas of discrete mathematics, especially number theory and the theory of experimental designs.

The history of coding theory is in 1948, Claude Shannon published "A Mathematical Theory of Communication", an article in two parts in the July and October issues of the Bell System Technical Journal. This work focuses on the problem of how best to encode the information a sender wants to transmit. In this fundamental work he used tools in probability theory, developed by Norbert Wiener, which were in their nascent stages of being applied to communication theory at that time. Shannon developed information entropy as a measure for the uncertainty in a message while essentially inventing the field of information theory.The binary Golay

code was developed in 1949. It is an error-correcting code capable of correcting up to three errors in each 24-bit word, and detecting a fourth.

In first chapter 'Introduction to Coding Theory' we discussed about some basic concept of Coding Theory. It includes Basic Assumption where some fundamental definition and assumptions are stated, Information Rate, The Effect of Error Correction and Detection, Weight and Distance, Maximum Likelihood Decoding, Reliability of MLD, Error Detection and Correction. In the second chapter 'Linear Code' we discuss about linear codes and its properties and also some theorems. Linear Code is an important concept in Coding Theory. Second chapter includes Independence, Basis and Dimension, Matrices, Finding Bases for C, Generating Matrices, Parity Check Matrices, Equivalent Code, Distance of Linear Codes, Cosets, MLD of Linear Code.

PRELIMINARY

Binary Number

A binary number is a number expressed in the basis-2 numerical system or binary number system, a method of which uses only two symbols: typically "0" and "1".

Binary Addition

Binary addition is the sum of two or more binary numbers. Binary addition rules is,
0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

Probability

Probability is the likelihood that an event will occur and is calculated by dividing the number of favourable outcomes by the total number of possible outcomes.

Linear Combination

Let V be a vector space and S is non empty subset of V. A vector x in V is said to be a linear combination of elements of S if there exist a finite number of elements y_1,y_2,.....,y_n in S and scalars α_1,α_2,.....,α_n in F such that x=$\alpha_1 y_1$+$\alpha_2 y_2$+.....+$\alpha_n y_n$

Span

Let S be a non-empty subset of a vector space V, the set of all linear combination of S is called Span of S. It is denoted by [S] or Span(S).

Subspace

A subset W of a vector space V over a field F is called a subspace of V if W is a vector space over F under the operation of addition and scalar multiplication defined on V.

Subset

A set A is a subset of another set B if all element of the set A are element of the set B.

Linearly Independent and Dependent

Let S=$\{u_1,u_2,.....,u_n\}$ be a subset of a vector space V, $\alpha_1,\alpha_2,.....,\alpha_n$ be scalars and $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n$ be a linear combination of S.

The set S=$\{u_1,u_2,.....,u_n\}$ is said to be Linearly Independent if $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n=0 \Rightarrow \alpha_1=\alpha_2,.....=\alpha_n= 0$ (The only solution).

If there exist a non-trivial solution for $\alpha_1,\alpha_2,.....,\alpha_n$, That is atleast one α_i is not zero. Then the set is called Linearly Dependent.

Dimension

Let β be a basis of a vector space V if the number of vectors in β is n then the vector space V is called n-dimensional vector space and written as dim(V)=n.

Elementary Row Operation

The operation that are performed on rows of a matrix.

Rank

The number 'r' with the following two properties is called the Rank of the matrix.

1. There is atleast one non-zero minor of order r.
2. Every minor of order (r+1) is zero or vanish.

Cosets

Coset is subset of mathematical group consisting of all the products obtained by multiplying fixed element of group by each of elements of given subgroup, either on right or on left. Cosets are basic tool in study of groups

CHAPTER 1

INTRODUCTION TO CODING THEORY

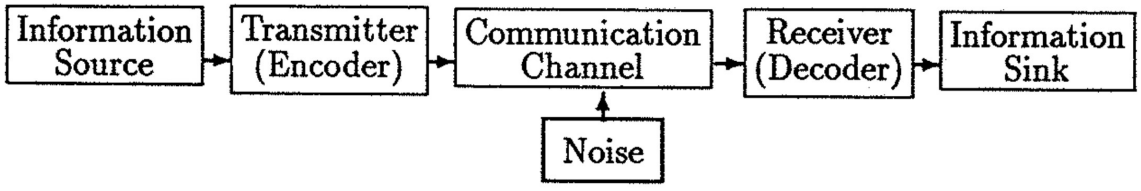
1.1 Coding Theory

Coding theory is the study of methods for efficient and accurate transfer of information from one place to another.

Definition 1.1. ***Channel***
The physical medium through which the information is transmitted is called a channel.

Definition 1.2. ***Noise***
Undesirable disturbance which may cause the information received to differ from what was transmitted is called noise.

Coding theory deals with the problem of dealing and correcting transmission error caused by noise on the channel.Rough idea of a general information transmission system.



The most important part of diagram is noise because without it there would be no need for coding theory.

1.2 Basic Assumption

We state some fundamental definitions and assumptions which will be applied in the coding theory.

Definition 1.3. ***Digits***
The information to be sent is transmitted by a sequence of 0's and 1's which is called digits.

Definition 1.4. ***Word***
Word is a sequence of digits.

Definition 1.5. ***Length of Word***
The length of a word is the number of digits in the word.

Definition 1.6. ***Binary Code***
A binary code is the set of words.
Eg: C= {00,01,10,11}

Definition 1.7. ***Block Code***
A block code is code having all its words of the same length.

Definition 1.8. ***Codewords***
The words that belong to a given code is called codewords. We denote the number of codewords in a code c by $|c|$.

A word is transmitted by sending its digits one after other across a binary channel. Each digit is transmitted mechanically, electrically, magnetically or by one of two types of easily differentiated pulses.

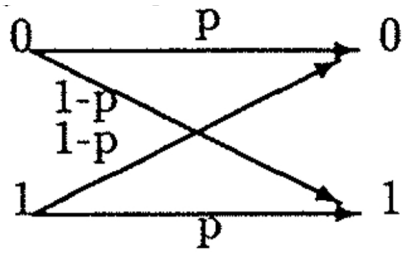
The codeword of length n is received as a word of length n. There is no difficulty in identifying the beginning of the first word transmitted. For example if we are using codeword of length 3 and receive

011011001, then the word received are in order 011,011,001.

Noise is scattered randomly as opposed to being in clumps is called bursts. That is the probability of any one digit being affected in transmission is same as that of any other digit and is not influenced by errors made in neighbouring digits.

A binary channel is symmetric, if 0 and 1 are transmitted with equal accuracy. The reliability of Binary Symmetric Channel(BSC) is a real number p , $0 \leq p \leq 1$, where p is the probability that the digit sent is the digit received.

If p is the probability that the digit received is the digit sent and 1-p is the probability that the digit received is not the digit sent. Then the following diagram shows how BSC operates.



Remarks

- The total number of words of length n is 2^n.
- If p=1 is the perfect channel then there is no chance of a digit being altered in transmission. If all Channel is perfect. then there is no need of coding theory. But no channel is perfect.
- Any channel with $0 \leq p \leq \frac{1}{2}$ can be converted into a channel with $\frac{1}{2} \leq p \leq 1$. We are using BSC with probability $\frac{1}{2} < p < 1$.
- Actually a channel p=0 is uninteresting because we can change by converting 0's into1 and 1's into 0. This will not help in the development coding theory.

1.3 Information Rate

The addition of digits to codeword may be improve error correction. $\frac{1}{n}\ log_2|\mathrm{c}|$ is the information rate of a code is the number that is designs measure the proportion of each codeword.The information rate ranges between 0 and 1.

1.4 The Effects Of Error Correction And Detection

To demonstrate the dramatic effect that the addition of a parity-check digit to a code can have in recognizing when error occur, we consider the following codes.
Suppose that all 2^{11} words of length 11 are codewords; then no error is detected.
Let the reliability of the channel be p = 1-10^{-8}.
Suppose that digits are transmitted at the rate of 10^7 digits per second.
The probability that the word is transmitted incorrectly is approximately $11p^{10}$(1-p), is about $\frac{11}{10^8}$.

$$\frac{11}{10^8}\ .\ \frac{10^7}{11} = 0.1 \text{ words per second}$$

are transmitted incorrectly without being detected. That is one wrong word every 10 seconds, 6 a minute, 360 an hour, or 8640 a day!

Now suppose that a parity-check digit is added to each codeword, so the number of 1's in each of the 2048 codewords is even. Then any single error is always detected, so at least 2 errors must occur if a word is to be transmitted incorrectly without our knowledge. The probability of at least 2 error occurring is 1-p^{12}-$12P^{11}$(1-p) which is approximated by $\binom{12}{2}p^{10}$(1-p)^2.

$$\text{p=1-}10^{-8} \rightarrow \frac{66}{10^{16}}$$

Now approximately

$$\frac{66}{10^{16}}\frac{10^7}{12} = 5.5\times 10^{-9}$$

words per second are transmitted incorrectly without being detected. That is about one error every 2000 days!

So if we are willing to reduce the information rate by lengthening the code from 11 to 12 we are very likely to know when errors occur. To decide where these errors have actually occurred, we may need to request the retransmission of the message. Physically this means that either transmission must be held up until confirmation is received or messages must be stored temporarily until retransmission is requested; both alternatives may be very costly in time or in storage space.

Therefore, at the expense of further increase in wordlength, it may well be worth incorporating error- correction capabilities into the code. Introducing such capabilities may also make encoding and decoding more difficult, but will help to avoid the hidden costs in time or space mentioned above.

One simple scheme to introduce error-correction is to form a repetition code where each codeword is transmitted three times in succession. Then if at most one error is made per 33 digit codeword, at least two of the three transmission will be correct. Then the information rate is $\frac{1}{3}$. So we add only 4 extra digit to each 11 digit codeword. This produce a code with information rate $\frac{11}{15}$.

So it is our task to design codes with reasonable information rates, low encoding and decoding costs and some error-correcting or error-detecting capabilities that make the need for retransmission unlikely.

1.5 Weight And Distance

Let v be a word of length n. The Hamming weight or simply weight of v is the number of times the digit 1 occur in v . We denote weight of v as wt(v).

Example 1.5.1. *wt(110101)= 4*

Let v and w be words of length n. Then the Hamming Distance or simply distance between v and w is the number of positions in which v and w disagree. We denote distance between v and w as d(v,w).

Eg: d(01011,00111)=2

Note

The distance between v and w is same as the weight of error pattern. That is

$$d(v, w) = wt(v+w).$$

Example 1.5.2. *d(v, w) =d(11010,01101)=4*
wt(v+w) = wt(11010=01101) = wt(10111) = 4

The probability formula of error pattern u=v+w ,

$$\phi_p(v,w) = p^{n-wt(u)}(1-p)^{wt(u)}$$

1.6 Maximum Likelihood Decoding

Two basic problems of coding,

1. Encoding : We have to determine a code to use for sending our messages.
    - First we select a positive integer k, the length of each binary word corresponding to a message k, k must be chosen so that $|M| \leq |k^k| = 2^k$.
    - Next we decide how many digit we need to add to each word of length k to ensure that as many errors can be corrected or detected as we require.
    - To transmit a particular message then transmitter finds the word of length k assigned to that of message,then transmits the codeword of length n corresponding to that word of length k.

2. Decoding: A word w in $k^n$is received. Now we proceed MLD, for decoding which word v in c was sent.

   (a) Complete Maximum Likelihood Decoding: If there is one and only one word v in c close to w than any other word in c, we decode w as v. if there are several words in c closest to w, then we select arbitrary one of them and conclude that it was the codeword sent.

   (b) Incomplete MLD: if there is a unique word v in c closest to w, then we decode w as v. but if there are several words in c, at the same distance from w, then we request a retransmission. In some cases if the received word w is too far away from any word in the code, we ask for a retransmission.

1.7 Reliability Of MLD

The probability that if v is sent over a BSC of probability p then IMLD correctly concludes that v was sent. θ_p(C,v) is the sum of all the probabilities θ_p(v,w) as w ranges over L(v). That is,

$$\theta_p(\text{C,v})=\sum_{w\in L(v)} \theta_p(v,w)$$

where L(v) all word which are close to v. The higher the probability is, the more correctly the word can be decoded.

1.8 Error Detection and correction

Error Detecting Code

If v in C sent and w in k^n is received, then u=v+w is the error pattern. Any word u in k^n can occur as an error pattern, and we wish to know which error patterns C will detect.
We say that code C detects the error pattern u if and only if v+u is not a codeword, for every v in C. In other words, u is detected if for any transmitted codeword v, the decoder upon receiving v+u can recognize that it is not a codeword and hence that some error has

occurred.

Example 1.8.1. *Let C={001, 101, 110} for the error pattern u=010. We calculate v+010 for all v in C.*

$$001+010=011,\ 101+010=111,\ 110+010=100$$

None of the three words 011, 111 or 100 is in C, so C detects the error pattern 010. On the other hand, for the error pattern u= 100,

$$001+100=101,\ 101+100=001,\ 110+100=010$$

Since at least one of these sums is in C, C does not detect the error pattern 100.

Error Correcting Code

If a word v in a code C is transmitted over BSC and w is the received resulting in the error pattern u=v+w. Then code C corrects the error pattern u, if for all v in C, v+u is closer to v than to any other word in C. Also, a code is said to be a t error correcting code if it corrects all error patterns of weight at most t and does not correct at least one error pattern of weight t+1.

Example 1.8.2. *Let C={000,111}*

- *Take the error pattern u=010. For v=000*

  $$d(000,v+u)=d(000,010)=1 \text{ and}$$
  $$d(111,v+u)=d(111,010)=2$$

  And for v=111,

  $$d(000,v+u)=d(000,101)=2$$
  $$d(111,v+u)=d(111,101)=1$$

  Thus C corrects the error pattern 010.

- *Now take the error pattern u=110. For v=000*

d(000,v+u)=d(000,110)=2 and
d(111,v+u)=d(111,110)=1

Since v+u is not closer to v=000 than to 111. C does not correct the error pattern 110.

CHAPTER 2

LINEAR CODE

2.1 Linear code

A code C is called a linear code if v+w is a word in C whenever v and w are in C. That is, a linear code is a code which is closed under addition of words.

Example 2.1.1. *C = {000, 111} is a linear code, since all four of the sums.*

000+000=000
000+111=111
111+000=111
111+111=000

are in C. But C_1 = {000, 001, 101} is not a linear code, since 001 and 101 are in C_1 but 001+101 is not in C_1.

2.2 Two Important Subspace

The vector w is said to be a linear combination of vectors $v_1, v_2, \ldots\ldots v_K$, if there are scalars $a_1, a_2, \ldots\ldots a_k$ as such that,

$$w=a_1v_1+a_2v_2+\ldots\ldots+a_kv_k$$

The set of all linear combinations of the vectors in a given set $S=\{v_1,v_2,\ldots\ldots v_k\}$ is called the linear span of S, and is denoted by <S>.

If S is empty, we define <S>= {0}.
In linear algebra it is shown that for any subset S of a vector space V, the linear span <S> is a subspace of V, called the subspace spanned or generated by S.

Theorem 2.2.1. *For any subset S of K^n, the code C=<S> generated by S consists precisely of the following words the zero word, all words in S, and all sums of two or more words in S.*

Example 2.2.1. *Let S = {0100, 0011, 1100}. Then the code C =<S> generated by S consists of*

0000, 0100, 0100+0011=0111, 0100+0011+1100=1011,
1100, 0011,0100+1100=1000, 0011+1100=1111;

that is, C=<S>={0000,0100,0011,1100,0111,1000,111,1011}.

2.3 Independence, Basis, Dimension

The main objective is to find an efficient way to describe a linear code without having to list all the codewords.
A set S={v_1,v_2,.....v_k} of vectors is linearly dependent if these are scalars a_1, a_2,.....a_k not all zero such that,

$$a_1v_1+a_2v_2+.....+a_kv_k=0$$

Otherwise the set S is linearly independent.
The test for linear independence, then, is to form the vector equation using arbitrary scalars. All the scalars a_1, a_2,.....a_k to be 0, then the set S is linearly independent. If at least one a_i can be chosen to be non-zero then S is linearly independent.
Any set of vectors containing the zero vectors is linearly dependent.
A nonempty subset B, of vectors from a vector space V is a basis for V if both:

1. B spans V (that is, <B>=V)
2. B is linearly independent set.

Note
Any Linearly independent set B is automatically a basis for <B>. Also since any linearly independent set S of vectors that contains a nonzero word always contains a largest independent subset B, we can extract from S a basis B for <S>. If S={0} then we say that the basis of S is the empty set $\emptyset$.

Theorem 2.3.1. *A linear code of dimension k contains precisely 2^k codewords.*

Theorem 2.3.2. *Let C=<S> be the linear code generated by a subset S of k^n. Then (dimension of C)+(dimension of $C^{\perp}$)=n*

Theorem 2.3.3. *A linear code of dimension k has precisely* $\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$ *different bases.*

Example 2.3.1. *The linear code k^4 and hence* $\frac{1}{4!}\prod_{i=0}^{3}(2^4 - 2^i)$= $\frac{1}{4!}$ *(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)= 840 different bases. Any linear code contained in k^n, for n≥4 which has dimension 4 also has 840 different bases.*

2.4 Matrices

An m×n matrix is a rectangular array of scalars with m rows and n columns. If A is an m × n matrix and B is an n×p matrix, then the product AB is the m×p matrix which has for its (i,j)th entry.

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

There are two types of elementary row operations which may be performed on a matrix over K. They are:

1. interchanging two rows
2. replacing a row by itself plus another row

Two matrices are row equivalent if one can be obtained from the other by a sequence of elementary row operators.
A1 in a matrix M (over K) is called a leading 1 if there are no 1s to its left in the same row, and a column of M is called a leading column if it contains a leading 1. M is in Row Echelon Form (REF) if the zero rows of M (if any) are all at the bottom, and each leading 1 is to the right of the leading 1s in the rows above.
If further, each leading column contains exactly one 1, M is in Reduced Row Echelon Form (RREF).

Example 2.4.1. *Find the REF for the matrix M below using elementary row operation.*

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

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 1 to row 2, row 3 and row 4)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 2 to row 3)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 4)*

So the REF of matrix M is

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

Example 2.4.2. *Find the RREF for the matrix M below using elementary row operation.*

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

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$ *(add row 1 to row 2 and to row 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(interchange row 2 and 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 1)*

So the RREF of matrix M is

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

2.5 Bases for C=<S> and $C^{\perp}$

We develop algorithms for finding bases for a linear code and its dual.
Let S be a nonempty subset of K^n. The first two algorithms provide a basis for C=<S>, the linear code generated by S.

Algorithm 2.5.1. *Form the matrix A whose rows are the words in S. Use elementary row operations to find a REF of A. Then the nonzero*

rows of the REF form a basis for C =<S>.
The algorithm works because the rows of A generate C and elementary row operations simply interchange words or replace one word (row) with another in C giving a new set of codewords which still generates C. Clearly the nonzero rows of a matrix in REF are linearly independent.

Example 2.5.1. *We find a basis for the linear code C=<S> for S = {11101, 10110, 01011, 11010}*

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

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&1&0&1&1\\0&0&1&1&1\end{bmatrix}$$ *(add row 1 to row 2 and to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&1&0&1&1\end{bmatrix}$$ *(interchange row 3 to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&0&0&0&0\end{bmatrix}$$ *(add row 2 to row 4)*

The last matrix is a REF of A. By Algorithm 2.5.1. {11101, 01011, 00111} is a basis for C=<S> . Another REF of A is

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

So {11101, 01100, 00111} is also a basis for C=<S >. Note that Algorithm 2.5.1 does not produce a unique basis for <S>, nor are the words in the basis necessarily in the given set S.

Algorithm 2.5.2. *Form the matrix A whose rows are the words in S. Use elementary row operations to place A in RREF. Let G be the k×n matrix consisting of all the nonzero rows of the RREF. Let X be the k×(n-k) matrix obtained from G by deleting the leading columns of G. Form an n×(n-k) matrix H as follows:*

1. *In the rows of H corresponding to the leading columns of G, place, in order,the rows of X.*
2. *In the remaining n-k rows of H, place, in order, the rows of the (n-k)×(n-k) identity matrix I.*

Then the columns of H form a basis for $C^{\perp}$

2.6 Generating Matrices and Encoding

The rank of a matrix over K is the number of nonzero rows in any REF of the matrix. The dimension k of the code C is the dimension of C, as a subspace of K^n. If C also has length n and distance d, then we refer to C as an (n, k, d) linear code.
If C is a linear code of length n and dimension k, then any matrix whose rows form a basis for C is called a generator matrix for C.
Note
A generator matrix for C must have k rows and n columns and it must have rank k.

Theorem 2.6.1. *A matrix G is a generator matrix for some linear code C if and only if the rows of G are linearly independent, that is, if and only if the rank of G is equal to the number of rows of G.*

Theorem 2.6.2. *If G is a generator matrix for a linear code C, then any matrix row equivalent to G is also a generator matrix for C. In particular, any linear code has a generator matrix in RREF.*

Example 2.6.1. *We find a generator matrix for the code C={0000,1110,0111,1001}. Using Algorithm 2.5.1,*

$$A=\begin{bmatrix}0&0&0&0\\1&1&1&0\\0&1&1&1\\1&0&0&1\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&0&0&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&1&1&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

so $G=\begin{bmatrix}1&1&1&0\\0&1&1&1\end{bmatrix}$ *is a generator matrix for C. By Algorithm 2.5.2, since the RREF of A is* $\begin{bmatrix}1&0&0&1\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$, $G_1=\begin{bmatrix}1&0&0&1\\0&1&1&1\end{bmatrix}$ *is also a generator matrix for C.*

2.7 Parity Check Matrices

A matrix H is called a parity-check matrix for a linear code C if the columns of H form a basis for the dual code C. If C has length n and dimension k, then, since the sum of the dimensions of C and $C^{\perp}$ is in any parity-check matrix for C must have n rows, n-k columns and rank n - k.

Theorem 2.7.1. *A matrix H is a parity-check matrix for some linear code C if and only if the columns of H are linearly independent*

Theorem 2.7.2. *If H is a parity-check matrix for a linear code C of length n, then C consists precisely of all words v in* K^n *such that vH=0.*

Theorem 2.7.3. *Matrices G and H are generating and parity-check matrices, respectively, for some linear code C if and only if*

1. *the rows of G are linearly independent,*
2. *the columns of H are linearly independent,*
3. *the number of rows of G plus the number of columns of H equals the number of columns of G which equals the number of rows of H,*

4. GH=0

Theorem 2.7.4. *H is a parity-check matrix of C if and only if H^T is a generator matrix for $C^{\perp}$*

Example 2.7.1. *We find a parity check matrix for the code C={0000,1110,0111,1001} of Example 2.6.1. There we found that*

$$G_1 = \begin{bmatrix} 10 & 01 \\ 01 & 11 \end{bmatrix} = \begin{bmatrix} I & X \end{bmatrix}$$

is a generator matrix for C which is in RREF. By Algorithm 2.5.2, we connect H

$$H = \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

is a parity check matrix for C. Note that vH= 00 for all words v in C.

2.8 Distance of Linear Code

The distance of a linear code is the minimum weight of any nonzero codeword. The distance of a linear code can also be determined from a parity-check matrix for the code.

Theorem 2.8.1. *Let H be a parity-check matrix for a linear code C. Then C has distance d if and only if any set of d-1 rows of H is linearly independent, and at least one set of d rows of linearly dependent.*

Example 2.8.1. *Let C be the linear code with parity-check matrix*

$$H = \begin{bmatrix} 110 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

By inspection it is seen that no two rows of H sum to 000, so any two rows of H are linearly independent. But rows 1, 3, and 4, for instance sum to 000, and hence are linearly dependent. Therefore d-1=2, so the distance of C is d = 3.

2.9 Cosets

If C is a linear code of length n, and if u is any word of length n, we define the coset of C determined by u to be the set of all words of the form v+u as v ranges over all the words in C. We denote this coset by C+u. Thus,

$$C + u = \{v+u \mid v \in C\}.$$

Example 2.9.1. *Let C={000, 111}, and let u= 101. Then,*

$$C+101=\{000+ 101, 111+101\} = \{101,010\}.$$

Note that also

$$C+111= \{000+111, 111+111\}=\{111,000\} = C$$

and

$$C+010= \{000 +010, 111+010)\}=\{010, 101\}= C+101.$$

Theorem 2.9.1. *Let C be a linear code of length n. Let u and v be words of length of n.*

1. *If u is in the coset C + v, then C + u = C + v; that is, each word in a coset determines that coset.*
2. *The word u is in the coset C + u.*
3. *If u + v is in C, then u and v are in the same coset.*
4. *If u + v is not in C, then u and v are in different cosets.*
5. *Every word in K^n is contained in one and only one coset of C; that is, either C + u = C + v, or C + u and C + v have no words in common.*
6. *|C + u|= |C|; that is, the number of words in a coset of C is equal to the number of words in the code C.*
7. *If C has dimension k, then there are exactly 2^{n-k} different cosets of C, and each coset contains exactly 2^k words.*

8. *The code C itself is one of its cosets.*

Example 2.9.2. *We list the cosets of the code*

$$C = \{0000, 1011, 0101, 1110\}$$

- *C itself is a coset.(Theorem 2.10.1 (8))*
- *Every word in C will determine the coset C by (tTheorem 2.10.1 (1) and (5)), so we pick a word u in K^4 not in C. For later use in decoding, it will help to pick u of smallest weight possible. So let's take u = 1000. Then we get the coset,*

$$C + 1000 = \{1000, 0011, 1101, 0110\}.$$

- *Now pick another word, of small weight, in K but not in C or C+1000, say 0100. Form another coset,*

$$C + 0100 = \{0100, 1111, 0001, 1010\}.$$

- *Repeating the process with 0010 yields the coset*

$$C + 0010 = \{0010, 1001, 0111, 1100\}$$

- *The code C has dimension k = 2. Then,*

$$2^{n-k} = 2^{4-2} = 2^2 = 4$$

We have listed 4 cosets with $2^k = 2^n = 4$ words.and every word in K^4 is accounted for appearing in exactly one coset.

- *Also observe that 0001 + 1010= 1011 is in C, thus 0001 and 1010 are in the same coset, namely C+0100 (see (3)). On the other hand, 0100 + 0010= 0110 is not in C, and 0100 and 0010 are in different cosets (see (4)).*

2.10 MLD for Linear Code

Let C be a linear code. Assume the codeword v in C is transmitted and the word w is received, resulting in the error pattern u = v + w. Then w + u = v is in C, so the error pattern u and the received word w are in the same coset of C by (3) of Theorem 2.10.1.

Since error patterns of small weight are the most likely to occur, here is how MLD works for a linear code C. Upon receiving the word w, we choose a word u of least weight in the coset C + w (which must contain w) and conclude that v = w + u was the word sent.

Example 2.10.1. *Let C={0000, 1011, 0101, 1110}. The cosets of C (Example 2.10.2) are*

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100

Suppose w= 1101 is received.

$$C + w = C + 1101 = \{1101, 0110, 1000, 0011\}$$

The coset C + w= C+ 1101 containing w is the second one listed.
The word of least weight in this coset is u= 1000, which we choose as the error pattern.
We conclude that,

$$v = w + u = 1101 + 1000 = 0101$$

0101was the most likely codeword sent.

Now suppose w=1111 is received.

$$C + w = C + 1111 = \{1111, 0100, 1010, 0001\}$$

In the coset C+w containing 1111 there are two words of smallest weight, 0100 and 0001. Since we are doing CMLD, we arbitrarily select one of these, say u= 0100, for the error pattern, and conclude that v = w + u= 1111 + 0100 = 1011 was a most likely codeword sent.

Theorem 2.10.1. *Let C be a linear code of length n. Let H be a parity-check matrix for C. Let w and u be words in* K^n.

1. *wH = 0 if and only if w is a codeword in C.*
2. *wH = uH if and only if w and u lie in the same coset of C.*
3. *If u is the error pattern in a received word w, then uH is the sum of the rows of H that correspond to the positions in which errors occurred in transmission.*

CONCLUSION

Our aim was to take a note on coding theory by its breath of coverage. Coding theory is the study of properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines such as information theory, electrical engineering, mathematics, linguistics and computer science-for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data. This project work helps us to know more about coding theory.

I have much pleasure in conveying my heart full thanks to my teachers and colleagues.

BIBLIOGRAPHY

1. D.G.Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger and J.R. Wall,***CODING THEORY The Essentials***, Marcel Dekkar, Inc., 1991.

2. Richard W Hamming, ***Coding and Information Theory***, Prentice-Hall, Inc., 1986.

3. Steven Roman, ***Coding and Information Theory***, Springer Science and Business Media, 1992.

4. Wikipedia, Coding Theory, ***<https://en.wikipedia.org › wiki › Coding-theory>***

5. Wikipedia, Linear Code, ***<https://en.wikipedia.org › wiki › Linear-code>***

CODING THEORY

Project report submitted to
KANNUR UNIVERSITY

for the award of the degree of
BACHELOR OF SCIENCE

by

SWATHI P
DB20CMSR08

under the guidance of
Ms. Ajeena Joseph

Department Of Mathematics
Don Bosco Arts And Science College
Angadikadavu, Iritty
March 2023

Examiners:

1.

2.

CERTIFICATE

This is to certify that **"Coding Theory"** is a bona fide project of **SWATHI P DB20CMSR08** and that this project has been carried out under my supervision.

Mrs. Riya Baby
Head of department

Ms. Ajeena Joseph
Project Supervisor

DECLARATION

I, **SWATHI P**, hearby declare that the project **"Coding Theory"** is an original record of studies and bona fide project carried out by me during the period of 2020-2023 under the guidance of **Ms. Ajeena Joseph**, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, Iritty, and that this project has not been submitted by me elsewhere for the award of my degree, diploma, title or recognition, before.

SWATHI P
DB20CMSR08

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to several individuals and organisation for supporting me throughout the course of the successful accomplishment of this project.

First I wish to express my sincere gratitude to my supervisor, Ms. Ajeena Joseph, Department Of Mathematics, Don Bosco Arts And Science College, Angadikadavu, for her enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this project.Without her support and guidance, this project would've seemed an ordeal. I could not have imagined having a better supervisor in my study.

I also wish to express my sincere thanks to all the faculty members of the Department Of Mathematics at Don Bosco Arts And Science College, Angadikkadavu, for their consistent support and assistance.

Thank you to everyone at Don Bosco Arts And Science College Angadikkadavu, including our Principal, Dr. Francis Karackat, management, teaching and non-teaching staff. It was great sharing premises with all of you during last three years.

I'd also like to thank my friends and parents for their support and encouragement as I worked on this assignment.

I shall always remain indebted to God, the almighty, who has granted countless blessing, knowledge, and opportunity to the writer, so that I have been finally able to accomplish this project.

Once again, thanks for all your encouragement.

CONTENTS

INTRODUCTION

Coding theory is the study of the properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines—such as information theory, electrical engineering, mathematics, linguistics, and computer science— for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data.

Coding theory, sometimes called algebraic coding theory, deals with the design of error-correcting codes for the reliable transmission of information across noisy channels. It makes use of classical and modern algebraic techniques involving finite fields, group theory, and polynomial algebra. It has connections with other areas of discrete mathematics, especially number theory and the theory of experimental designs.

The history of coding theory is in 1948, Claude Shannon published "A Mathematical Theory of Communication", an article in two parts in the July and October issues of the Bell System Technical Journal. This work focuses on the problem of how best to encode the information a sender wants to transmit. In this fundamental work he used tools in probability theory, developed by Norbert Wiener, which were in their nascent stages of being applied to communication theory at that time. Shannon developed information entropy as a measure for the uncertainty in a message while essentially inventing the field of information theory.The binary Golay

code was developed in 1949. It is an error-correcting code capable of correcting up to three errors in each 24-bit word, and detecting a fourth.

In first chapter 'Introduction to Coding Theory' we discussed about some basic concept of Coding Theory. It includes Basic Assumption where some fundamental definition and assumptions are stated, Information Rate, The Effect of Error Correction and Detection, Weight and Distance, Maximum Likelihood Decoding, Reliability of MLD, Error Detection and Correction. In the second chapter 'Linear Code' we discuss about linear codes and its properties and also some theorems. Linear Code is an important concept in Coding Theory. Second chapter includes Independence, Basis and Dimension, Matrices, Finding Bases for C, Generating Matrices, Parity Check Matrices, Equivalent Code, Distance of Linear Codes, Cosets, MLD of Linear Code.

PRELIMINARY

Binary Number

A binary number is a number expressed in the basis-2 numerical system or binary number system, a method of which uses only two symbols: typically "0" and "1".

Binary Addition

Binary addition is the sum of two or more binary numbers. Binary addition rules is,
0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

Probability

Probability is the likelihood that an event will occur and is calculated by dividing the number of favourable outcomes by the total number of possible outcomes.

Linear Combination

Let V be a vector space and S is non empty subset of V. A vector x in V is said to be a linear combination of elements of S if there exist a finite number of elements y_1,y_2,.....,y_n in S and scalars α_1,α_2,.....,α_n in F such that x=$\alpha_1 y_1$+$\alpha_2 y_2$+.....+$\alpha_n y_n$

Span

Let S be a non-empty subset of a vector space V, the set of all linear combination of S is called Span of S. It is denoted by [S] or Span(S).

Subspace

A subset W of a vector space V over a field F is called a subspace of V if W is a vector space over F under the operation of addition and scalar multiplication defined on V.

Subset

A set A is a subset of another set B if all element of the set A are element of the set B.

Linearly Independent and Dependent

Let S=$\{u_1,u_2,.....,u_n\}$ be a subset of a vector space V, $\alpha_1,\alpha_2,.....,\alpha_n$ be scalars and $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n$ be a linear combination of S.

The set S=$\{u_1,u_2,.....,u_n\}$ is said to be Linearly Independent if $\alpha_1u_1+\alpha_2u_2+.....+\alpha_nu_n=0 \Rightarrow \alpha_1=\alpha_2,.....=\alpha_n= 0$ (The only solution).

If there exist a non-trivial solution for $\alpha_1,\alpha_2,.....,\alpha_n$, That is atleast one α_i is not zero. Then the set is called Linearly Dependent.

Dimension

Let β be a basis of a vector space V if the number of vectors in β is n then the vector space V is called n-dimensional vector space and written as dim(V)=n.

Elementary Row Operation

The operation that are performed on rows of a matrix.

Rank

The number 'r' with the following two properties is called the Rank of the matrix.

1. There is atleast one non-zero minor of order r.
2. Every minor of order (r+1) is zero or vanish.

Cosets

Coset is subset of mathematical group consisting of all the products obtained by multiplying fixed element of group by each of elements of given subgroup, either on right or on left. Cosets are basic tool in study of groups

CHAPTER 1

INTRODUCTION TO CODING THEORY

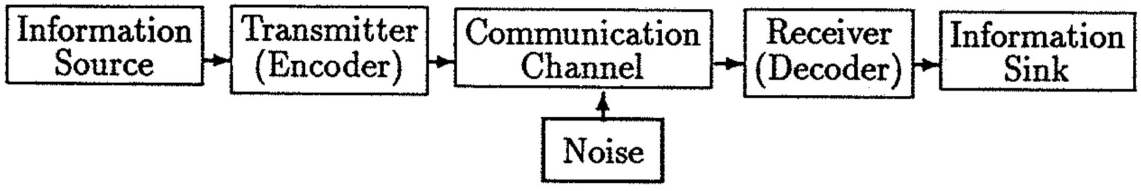
1.1 Coding Theory

Coding theory is the study of methods for efficient and accurate transfer of information from one place to another.

Definition 1.1. ***Channel***
The physical medium through which the information is transmitted is called a channel.

Definition 1.2. ***Noise***
Undesirable disturbance which may cause the information received to differ from what was transmitted is called noise.

Coding theory deals with the problem of dealing and correcting transmission error caused by noise on the channel.Rough idea of a general information transmission system.



The most important part of diagram is noise because without it there would be no need for coding theory.

1.2 Basic Assumption

We state some fundamental definitions and assumptions which will be applied in the coding theory.

Definition 1.3. ***Digits***
The information to be sent is transmitted by a sequence of 0's and 1's which is called digits.

Definition 1.4. ***Word***
Word is a sequence of digits.

Definition 1.5. ***Length of Word***
The length of a word is the number of digits in the word.

Definition 1.6. ***Binary Code***
A binary code is the set of words.
Eg: C= {00,01,10,11}

Definition 1.7. ***Block Code***
A block code is code having all its words of the same length.

Definition 1.8. ***Codewords***
The words that belong to a given code is called codewords. We denote the number of codewords in a code c by $|c|$.

A word is transmitted by sending its digits one after other across a binary channel. Each digit is transmitted mechanically, electrically, magnetically or by one of two types of easily differentiated pulses.

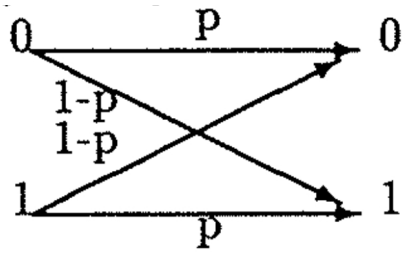
The codeword of length n is received as a word of length n. There is no difficulty in identifying the beginning of the first word transmitted. For example if we are using codeword of length 3 and receive

011011001, then the word received are in order 011,011,001.

Noise is scattered randomly as opposed to being in clumps is called bursts. That is the probability of any one digit being affected in transmission is same as that of any other digit and is not influenced by errors made in neighbouring digits.

A binary channel is symmetric, if 0 and 1 are transmitted with equal accuracy. The reliability of Binary Symmetric Channel(BSC) is a real number p , $0 \leq p \leq 1$, where p is the probability that the digit sent is the digit received.

If p is the probability that the digit received is the digit sent and 1-p is the probability that the digit received is not the digit sent. Then the following diagram shows how BSC operates.



Remarks

- The total number of words of length n is 2^n.
- If p=1 is the perfect channel then there is no chance of a digit being altered in transmission. If all Channel is perfect. then there is no need of coding theory. But no channel is perfect.
- Any channel with $0 \leq p \leq \frac{1}{2}$ can be converted into a channel with $\frac{1}{2} \leq p \leq 1$. We are using BSC with probability $\frac{1}{2} < p < 1$.
- Actually a channel p=0 is uninteresting because we can change by converting 0's into1 and 1's into 0. This will not help in the development coding theory.

1.3 Information Rate

The addition of digits to codeword may be improve error correction. $\frac{1}{n}\ log_2|\mathrm{c}|$ is the information rate of a code is the number that is designs measure the proportion of each codeword.The information rate ranges between 0 and 1.

1.4 The Effects Of Error Correction And Detection

To demonstrate the dramatic effect that the addition of a parity-check digit to a code can have in recognizing when error occur, we consider the following codes.
Suppose that all 2^{11} words of length 11 are codewords; then no error is detected.
Let the reliability of the channel be p = 1-10^{-8}.
Suppose that digits are transmitted at the rate of 10^7 digits per second.
The probability that the word is transmitted incorrectly is approximately $11p^{10}$(1-p), is about $\frac{11}{10^8}$.

$$\frac{11}{10^8}\ .\ \frac{10^7}{11} = 0.1 \text{ words per second}$$

are transmitted incorrectly without being detected. That is one wrong word every 10 seconds, 6 a minute, 360 an hour, or 8640 a day!

Now suppose that a parity-check digit is added to each codeword, so the number of 1's in each of the 2048 codewords is even. Then any single error is always detected, so at least 2 errors must occur if a word is to be transmitted incorrectly without our knowledge. The probability of at least 2 error occurring is 1-p^{12}-$12P^{11}$(1-p) which is approximated by $\binom{12}{2}p^{10}$(1-p)^2.

$$\text{p=1-}10^{-8} \rightarrow \frac{66}{10^{16}}$$

Now approximately

$$\frac{66}{10^{16}}\frac{10^7}{12} = 5.5\times 10^{-9}$$

words per second are transmitted incorrectly without being detected. That is about one error every 2000 days!

So if we are willing to reduce the information rate by lengthening the code from 11 to 12 we are very likely to know when errors occur. To decide where these errors have actually occurred, we may need to request the retransmission of the message. Physically this means that either transmission must be held up until confirmation is received or messages must be stored temporarily until retransmission is requested; both alternatives may be very costly in time or in storage space.

Therefore, at the expense of further increase in wordlength, it may well be worth incorporating error- correction capabilities into the code. Introducing such capabilities may also make encoding and decoding more difficult, but will help to avoid the hidden costs in time or space mentioned above.

One simple scheme to introduce error-correction is to form a repetition code where each codeword is transmitted three times in succession. Then if at most one error is made per 33 digit codeword, at least two of the three transmission will be correct. Then the information rate is $\frac{1}{3}$. So we add only 4 extra digit to each 11 digit codeword. This produce a code with information rate $\frac{11}{15}$.

So it is our task to design codes with reasonable information rates, low encoding and decoding costs and some error-correcting or error-detecting capabilities that make the need for retransmission unlikely.

1.5 Weight And Distance

Let v be a word of length n. The Hamming weight or simply weight of v is the number of times the digit 1 occur in v . We denote weight of v as wt(v).

Example 1.5.1. *wt(110101)= 4*

Let v and w be words of length n. Then the Hamming Distance or simply distance between v and w is the number of positions in which v and w disagree. We denote distance between v and w as d(v,w).

Eg: d(01011,00111)=2

Note

The distance between v and w is same as the weight of error pattern. That is

$$d(v, w) = wt(v+w).$$

Example 1.5.2. *d(v, w) =d(11010,01101)=4*
wt(v+w) = wt(11010=01101) = wt(10111) = 4

The probability formula of error pattern u=v+w ,

$$\phi_p(v,w) = p^{n-wt(u)}(1-p)^{wt(u)}$$

1.6 Maximum Likelihood Decoding

Two basic problems of coding,

1. Encoding : We have to determine a code to use for sending our messages.
    - First we select a positive integer k, the length of each binary word corresponding to a message k, k must be chosen so that $|M| \leq |k^k| = 2^k$.
    - Next we decide how many digit we need to add to each word of length k to ensure that as many errors can be corrected or detected as we require.
    - To transmit a particular message then transmitter finds the word of length k assigned to that of message,then transmits the codeword of length n corresponding to that word of length k.

2. Decoding: A word w in $k^n$is received. Now we proceed MLD, for decoding which word v in c was sent.

   (a) Complete Maximum Likelihood Decoding: If there is one and only one word v in c close to w than any other word in c, we decode w as v. if there are several words in c closest to w, then we select arbitrary one of them and conclude that it was the codeword sent.

   (b) Incomplete MLD: if there is a unique word v in c closest to w, then we decode w as v. but if there are several words in c, at the same distance from w, then we request a retransmission. In some cases if the received word w is too far away from any word in the code, we ask for a retransmission.

1.7 Reliability Of MLD

The probability that if v is sent over a BSC of probability p then IMLD correctly concludes that v was sent. θ_p(C,v) is the sum of all the probabilities θ_p(v,w) as w ranges over L(v). That is,

$$\theta_p(\text{C,v})=\sum_{w\in L(v)} \theta_p(v,w)$$

where L(v) all word which are close to v. The higher the probability is, the more correctly the word can be decoded.

1.8 Error Detection and correction

Error Detecting Code

If v in C sent and w in k^n is received, then u=v+w is the error pattern. Any word u in k^n can occur as an error pattern, and we wish to know which error patterns C will detect.
We say that code C detects the error pattern u if and only if v+u is not a codeword, for every v in C. In other words, u is detected if for any transmitted codeword v, the decoder upon receiving v+u can recognize that it is not a codeword and hence that some error has

occurred.

Example 1.8.1. *Let C={001, 101, 110} for the error pattern u=010. We calculate v+010 for all v in C.*

$$001+010=011,\ 101+010=111,\ 110+010=100$$

None of the three words 011, 111 or 100 is in C, so C detects the error pattern 010. On the other hand, for the error pattern u= 100,

$$001+100=101,\ 101+100=001,\ 110+100=010$$

Since at least one of these sums is in C, C does not detect the error pattern 100.

Error Correcting Code

If a word v in a code C is transmitted over BSC and w is the received resulting in the error pattern u=v+w. Then code C corrects the error pattern u, if for all v in C, v+u is closer to v than to any other word in C. Also, a code is said to be a t error correcting code if it corrects all error patterns of weight at most t and does not correct at least one error pattern of weight t+1.

Example 1.8.2. *Let C={000,111}*

- *Take the error pattern u=010. For v=000*

  $$d(000,v+u)=d(000,010)=1 \text{ and}$$
  $$d(111,v+u)=d(111,010)=2$$

  And for v=111,

  $$d(000,v+u)=d(000,101)=2$$
  $$d(111,v+u)=d(111,101)=1$$

  Thus C corrects the error pattern 010.

- *Now take the error pattern u=110. For v=000*

d(000,v+u)=d(000,110)=2 and
d(111,v+u)=d(111,110)=1

Since v+u is not closer to v=000 than to 111. C does not correct the error pattern 110.

CHAPTER 2

LINEAR CODE

2.1 Linear code

A code C is called a linear code if v+w is a word in C whenever v and w are in C. That is, a linear code is a code which is closed under addition of words.

Example 2.1.1. *C = {000, 111} is a linear code, since all four of the sums.*

000+000=000
000+111=111
111+000=111
111+111=000

are in C. But C_1 = {000, 001, 101} is not a linear code, since 001 and 101 are in C_1 but 001+101 is not in C_1.

2.2 Two Important Subspace

The vector w is said to be a linear combination of vectors $v_1, v_2, \ldots\ldots v_K$, if there are scalars $a_1, a_2, \ldots\ldots a_k$ as such that,

$$w=a_1v_1+a_2v_2+\ldots\ldots+a_kv_k$$

The set of all linear combinations of the vectors in a given set $S=\{v_1,v_2,\ldots\ldots v_k\}$ is called the linear span of S, and is denoted by <S>.

If S is empty, we define <S>= {0}.
In linear algebra it is shown that for any subset S of a vector space V, the linear span <S> is a subspace of V, called the subspace spanned or generated by S.

Theorem 2.2.1. *For any subset S of K^n, the code C=<S> generated by S consists precisely of the following words the zero word, all words in S, and all sums of two or more words in S.*

Example 2.2.1. *Let S = {0100, 0011, 1100}. Then the code C =<S> generated by S consists of*

0000, 0100, 0100+0011=0111, 0100+0011+1100=1011,
1100, 0011,0100+1100=1000, 0011+1100=1111;

that is, C=<S>={0000,0100,0011,1100,0111,1000,111,1011}.

2.3 Independence, Basis, Dimension

The main objective is to find an efficient way to describe a linear code without having to list all the codewords.
A set S={v_1,v_2,.....v_k} of vectors is linearly dependent if these are scalars a_1, a_2,.....a_k not all zero such that,

$$a_1v_1+a_2v_2+.....+a_kv_k=0$$

Otherwise the set S is linearly independent.
The test for linear independence, then, is to form the vector equation using arbitrary scalars. All the scalars a_1, a_2,.....a_k to be 0, then the set S is linearly independent. If at least one a_i can be chosen to be non-zero then S is linearly independent.
Any set of vectors containing the zero vectors is linearly dependent.
A nonempty subset B, of vectors from a vector space V is a basis for V if both:

1. B spans V (that is, <B>=V)
2. B is linearly independent set.

Note
Any Linearly independent set B is automatically a basis for <B>. Also since any linearly independent set S of vectors that contains a nonzero word always contains a largest independent subset B, we can extract from S a basis B for <S>. If S={0} then we say that the basis of S is the empty set $\emptyset$.

Theorem 2.3.1. *A linear code of dimension k contains precisely 2^k codewords.*

Theorem 2.3.2. *Let C=<S> be the linear code generated by a subset S of k^n. Then (dimension of C)+(dimension of $C^{\perp}$)=n*

Theorem 2.3.3. *A linear code of dimension k has precisely* $\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$ *different bases.*

Example 2.3.1. *The linear code k^4 and hence* $\frac{1}{4!}\prod_{i=0}^{3}(2^4 - 2^i)$= $\frac{1}{4!}$ *(2^4-1)(2^4-2)(2^4-2^2)(2^4-2^3)= 840 different bases. Any linear code contained in k^n, for n≥4 which has dimension 4 also has 840 different bases.*

2.4 Matrices

An m×n matrix is a rectangular array of scalars with m rows and n columns. If A is an m × n matrix and B is an n×p matrix, then the product AB is the m×p matrix which has for its (i,j)th entry.

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

There are two types of elementary row operations which may be performed on a matrix over K. They are:

1. interchanging two rows
2. replacing a row by itself plus another row

Two matrices are row equivalent if one can be obtained from the other by a sequence of elementary row operators.
A1 in a matrix M (over K) is called a leading 1 if there are no 1s to its left in the same row, and a column of M is called a leading column if it contains a leading 1. M is in Row Echelon Form (REF) if the zero rows of M (if any) are all at the bottom, and each leading 1 is to the right of the leading 1s in the rows above.
If further, each leading column contains exactly one 1, M is in Reduced Row Echelon Form (RREF).

Example 2.4.1. *Find the REF for the matrix M below using elementary row operation.*

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

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 1 to row 2, row 3 and row 4)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$ *(add row 2 to row 3)*

$$\Rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 4)*

So the REF of matrix M is

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

Example 2.4.2. *Find the RREF for the matrix M below using elementary row operation.*

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

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$ *(add row 1 to row 2 and to row 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(interchange row 2 and 3)*

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ *(add row 3 to row 1)*

So the RREF of matrix M is

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

2.5 Bases for C=<S> and $C^{\perp}$

We develop algorithms for finding bases for a linear code and its dual.
Let S be a nonempty subset of K^n. The first two algorithms provide a basis for C=<S>, the linear code generated by S.

Algorithm 2.5.1. *Form the matrix A whose rows are the words in S. Use elementary row operations to find a REF of A. Then the nonzero*

rows of the REF form a basis for C =<S>.
The algorithm works because the rows of A generate C and elementary row operations simply interchange words or replace one word (row) with another in C giving a new set of codewords which still generates C. Clearly the nonzero rows of a matrix in REF are linearly independent.

Example 2.5.1. *We find a basis for the linear code C=<S> for S = {11101, 10110, 01011, 11010}*

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

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&1&0&1&1\\0&0&1&1&1\end{bmatrix}$$ *(add row 1 to row 2 and to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&1&0&1&1\end{bmatrix}$$ *(interchange row 3 to row 4)*

$$\to\begin{bmatrix}1&1&1&0&1\\0&1&0&1&1\\0&0&1&1&1\\0&0&0&0&0\end{bmatrix}$$ *(add row 2 to row 4)*

The last matrix is a REF of A. By Algorithm 2.5.1. {11101, 01011, 00111} is a basis for C=<S> . Another REF of A is

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

So {11101, 01100, 00111} is also a basis for C=<S >. Note that Algorithm 2.5.1 does not produce a unique basis for <S>, nor are the words in the basis necessarily in the given set S.

Algorithm 2.5.2. *Form the matrix A whose rows are the words in S. Use elementary row operations to place A in RREF. Let G be the k×n matrix consisting of all the nonzero rows of the RREF. Let X be the k×(n-k) matrix obtained from G by deleting the leading columns of G. Form an n×(n-k) matrix H as follows:*

1. *In the rows of H corresponding to the leading columns of G, place, in order,the rows of X.*
2. *In the remaining n-k rows of H, place, in order, the rows of the (n-k)×(n-k) identity matrix I.*

Then the columns of H form a basis for $C^{\perp}$

2.6 Generating Matrices and Encoding

The rank of a matrix over K is the number of nonzero rows in any REF of the matrix. The dimension k of the code C is the dimension of C, as a subspace of K^n. If C also has length n and distance d, then we refer to C as an (n, k, d) linear code.
If C is a linear code of length n and dimension k, then any matrix whose rows form a basis for C is called a generator matrix for C.
Note
A generator matrix for C must have k rows and n columns and it must have rank k.

Theorem 2.6.1. *A matrix G is a generator matrix for some linear code C if and only if the rows of G are linearly independent, that is, if and only if the rank of G is equal to the number of rows of G.*

Theorem 2.6.2. *If G is a generator matrix for a linear code C, then any matrix row equivalent to G is also a generator matrix for C. In particular, any linear code has a generator matrix in RREF.*

Example 2.6.1. *We find a generator matrix for the code C={0000,1110,0111,1001}. Using Algorithm 2.5.1,*

$$A=\begin{bmatrix}0&0&0&0\\1&1&1&0\\0&1&1&1\\1&0&0&1\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\1&0&0&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&1&1&1\\0&0&0&0\end{bmatrix}\rightarrow\begin{bmatrix}1&1&1&0\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

so $G=\begin{bmatrix}1&1&1&0\\0&1&1&1\end{bmatrix}$ *is a generator matrix for C. By Algorithm 2.5.2, since the RREF of A is* $\begin{bmatrix}1&0&0&1\\0&1&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$, $G_1=\begin{bmatrix}1&0&0&1\\0&1&1&1\end{bmatrix}$ *is also a generator matrix for C.*

2.7 Parity Check Matrices

A matrix H is called a parity-check matrix for a linear code C if the columns of H form a basis for the dual code C. If C has length n and dimension k, then, since the sum of the dimensions of C and $C^{\perp}$ is in any parity-check matrix for C must have n rows, n-k columns and rank n - k.

Theorem 2.7.1. *A matrix H is a parity-check matrix for some linear code C if and only if the columns of H are linearly independent*

Theorem 2.7.2. *If H is a parity-check matrix for a linear code C of length n, then C consists precisely of all words v in* K^n *such that vH=0.*

Theorem 2.7.3. *Matrices G and H are generating and parity-check matrices, respectively, for some linear code C if and only if*

1. *the rows of G are linearly independent,*
2. *the columns of H are linearly independent,*
3. *the number of rows of G plus the number of columns of H equals the number of columns of G which equals the number of rows of H,*

4. GH=0

Theorem 2.7.4. *H is a parity-check matrix of C if and only if H^T is a generator matrix for $C^{\perp}$*

Example 2.7.1. *We find a parity check matrix for the code C={0000,1110,0111,1001} of Example 2.6.1. There we found that*

$$G_1 = \begin{bmatrix} 10 & 01 \\ 01 & 11 \end{bmatrix} = \begin{bmatrix} I & X \end{bmatrix}$$

is a generator matrix for C which is in RREF. By Algorithm 2.5.2, we connect H

$$H = \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} 01 \\ 11 \\ 10 \\ 01 \end{bmatrix}$$

is a parity check matrix for C. Note that vH= 00 for all words v in C.

2.8 Distance of Linear Code

The distance of a linear code is the minimum weight of any nonzero codeword. The distance of a linear code can also be determined from a parity-check matrix for the code.

Theorem 2.8.1. *Let H be a parity-check matrix for a linear code C. Then C has distance d if and only if any set of d-1 rows of H is linearly independent, and at least one set of d rows of linearly dependent.*

Example 2.8.1. *Let C be the linear code with parity-check matrix*

$$H = \begin{bmatrix} 110 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

By inspection it is seen that no two rows of H sum to 000, so any two rows of H are linearly independent. But rows 1, 3, and 4, for instance sum to 000, and hence are linearly dependent. Therefore d-1=2, so the distance of C is d = 3.

2.9 Cosets

If C is a linear code of length n, and if u is any word of length n, we define the coset of C determined by u to be the set of all words of the form v+u as v ranges over all the words in C. We denote this coset by C+u. Thus,

$$C + u = \{v+u \mid v \in C\}.$$

Example 2.9.1. *Let C={000, 111}, and let u= 101. Then,*

$$C+101=\{000+ 101, 111+101\} = \{101,010\}.$$

Note that also

$$C+111= \{000+111, 111+111\}=\{111,000\} = C$$

and

$$C+010= \{000 +010, 111+010)\}=\{010, 101\}= C+101.$$

Theorem 2.9.1. *Let C be a linear code of length n. Let u and v be words of length of n.*

1. *If u is in the coset C + v, then C + u = C + v; that is, each word in a coset determines that coset.*
2. *The word u is in the coset C + u.*
3. *If u + v is in C, then u and v are in the same coset.*
4. *If u + v is not in C, then u and v are in different cosets.*
5. *Every word in K^n is contained in one and only one coset of C; that is, either C + u = C + v, or C + u and C + v have no words in common.*
6. *|C + u|= |C|; that is, the number of words in a coset of C is equal to the number of words in the code C.*
7. *If C has dimension k, then there are exactly 2^{n-k} different cosets of C, and each coset contains exactly 2^k words.*

8. *The code C itself is one of its cosets.*

Example 2.9.2. *We list the cosets of the code*

$$C = \{0000, 1011, 0101, 1110\}$$

- *C itself is a coset.(Theorem 2.10.1 (8))*
- *Every word in C will determine the coset C by (tTheorem 2.10.1 (1) and (5)), so we pick a word u in K^4 not in C. For later use in decoding, it will help to pick u of smallest weight possible. So let's take u = 1000. Then we get the coset,*

$$C + 1000 = \{1000, 0011, 1101, 0110\}.$$

- *Now pick another word, of small weight, in K but not in C or C+1000, say 0100. Form another coset,*

$$C + 0100 = \{0100, 1111, 0001, 1010\}.$$

- *Repeating the process with 0010 yields the coset*

$$C + 0010 = \{0010, 1001, 0111, 1100\}$$

- *The code C has dimension k = 2. Then,*

$$2^{n-k} = 2^{4-2} = 2^2 = 4$$

We have listed 4 cosets with $2^k = 2^n = 4$ words.and every word in K^4 is accounted for appearing in exactly one coset.

- *Also observe that 0001 + 1010= 1011 is in C, thus 0001 and 1010 are in the same coset, namely C+0100 (see (3)). On the other hand, 0100 + 0010= 0110 is not in C, and 0100 and 0010 are in different cosets (see (4)).*

2.10 MLD for Linear Code

Let C be a linear code. Assume the codeword v in C is transmitted and the word w is received, resulting in the error pattern u = v + w. Then w + u = v is in C, so the error pattern u and the received word w are in the same coset of C by (3) of Theorem 2.10.1.

Since error patterns of small weight are the most likely to occur, here is how MLD works for a linear code C. Upon receiving the word w, we choose a word u of least weight in the coset C + w (which must contain w) and conclude that v = w + u was the word sent.

Example 2.10.1. *Let C={0000, 1011, 0101, 1110}. The cosets of C (Example 2.10.2) are*

0000	1000	0100	0010
1011	0011	1111	1001
0101	1101	0001	0111
1110	0110	1010	1100

Suppose w= 1101 is received.

$$C + w = C + 1101 = \{1101, 0110, 1000, 0011\}$$

The coset C + w= C+ 1101 containing w is the second one listed.
The word of least weight in this coset is u= 1000, which we choose as the error pattern.
We conclude that,

$$v = w + u = 1101 + 1000 = 0101$$

0101was the most likely codeword sent.

Now suppose w=1111 is received.

$$C + w = C + 1111 = \{1111, 0100, 1010, 0001\}$$

In the coset C+w containing 1111 there are two words of smallest weight, 0100 and 0001. Since we are doing CMLD, we arbitrarily select one of these, say u= 0100, for the error pattern, and conclude that v = w + u= 1111 + 0100 = 1011 was a most likely codeword sent.

Theorem 2.10.1. *Let C be a linear code of length n. Let H be a parity-check matrix for C. Let w and u be words in* K^n.

1. *wH = 0 if and only if w is a codeword in C.*
2. *wH = uH if and only if w and u lie in the same coset of C.*
3. *If u is the error pattern in a received word w, then uH is the sum of the rows of H that correspond to the positions in which errors occurred in transmission.*

CONCLUSION

Our aim was to take a note on coding theory by its breath of coverage. Coding theory is the study of properties of codes and their respective fitness for specific applications. Codes are used for data compression, cryptography, error detection and correction, data transmission and data storage. Codes are studied by various scientific disciplines such as information theory, electrical engineering, mathematics, linguistics and computer science-for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of redundancy and the correction or detection of errors in the transmitted data. This project work helps us to know more about coding theory.

I have much pleasure in conveying my heart full thanks to my teachers and colleagues.

BIBLIOGRAPHY

1. D.G.Hoffman, D.A. Leonard, C.C. Lindner, K.T. Phelps, C.A. Rodger and J.R. Wall,***CODING THEORY The Essentials***, Marcel Dekkar, Inc., 1991.

2. Richard W Hamming, ***Coding and Information Theory***, Prentice-Hall, Inc., 1986.

3. Steven Roman, ***Coding and Information Theory***, Springer Science and Business Media, 1992.

4. Wikipedia, Coding Theory, ***<https://en.wikipedia.org › wiki › Coding-theory>***

5. Wikipedia, Linear Code, ***<https://en.wikipedia.org › wiki › Linear-code>***