18MAB302T-DISCRETE MATHEMATICS

UNIT-4 : GROUP THEORY AND CODING THEORY

Topics

- Binary operation on a set- Groups and axioms of groups
- Properties of groups
- Permutation group, equivalence classes with addition modulo m and multiplication modulo m
- Cyclic groups and properties
- Subgroups and necessary and sufficiency of a subset to be a subgroup
- Group homomorphism and properties
- Rings- definition and examples-Zero devisors
- Integral domain- definition , examples and properties.
- Fields – definition, examples and properties
- Coding Theory – Encoders and decoders- Hamming codes
- Hamming distance-Error detected by an encoding function
- Error correction using matrices
- Group codes-error correction in group codes-parity check matrix.
- Problems on error correction in group codes
- Procedure for decoding group codes
- Applications of sets, relations and functions in Engineering

INTRODUCTION

- INTRODUCTION
- BASIC ALGEBRA
- ALGEBRAIC SYSTEM
- PROPERTIES OF ALGEBRAIC SYSTEM

MODULE-1

SETS

- A Set is a well defined collection of objects. These objects are otherwise called members or elements of the set. The set is denoted by capital letters A, B,C…
- **Examples** : A - The set of all colors in rainbow , S – the set of even numbers
- **Notations :** Sets are represented in two ways .
- **Roster form :** All the elements are listed. Ex. A = {1,3,5,7,9}
- **Set builder form :** Defining the elements of the set by specifying their common property .
- Example: V = { x / x is vowel}
- [the elements of V are a,e,i,o,u]
- $S = \{ x / x = n^2$, n is positive integer less than 30}
- S={1,4,9,16,25}

BASIC ALGEBRA

Number system

There are common notations for the number system which are

R – the set of all Real numbers, R^+ - the set of Positive real numbers.

Z, Z^+ , Z^- - set of all Integers, Positive integers, Negative integers.

C, C^+, C^- - set of all Complex, Positive complex, Negative complex numbers.

N – set of all Natural numbers i.e $N = \{1,2,3,\ldots\ldots\}$

Q, Q^+, Q^- - set of rational, positive rational, negative rational numbers

BASIC ALGEBRA-Number system

- **Congruence modulo n**

Let n be a positive integer. If a and b are two integers and n divides a – b then we say that "a is congruent to b modulo n" and we write

$a \equiv b \pmod{n}$. The integer n is called modulus.

Example : $23 \equiv 3 \pmod{5}$; $16 \equiv 0 \pmod{4}$

- **Congruence classes modulo n**

Let a be an integer. Let [a] denote the set of all integers congruent to a (mod n)

i.e $[a] = \{ x : x \in Z, x \equiv a \bmod (n)\} = \{x : x \in Z, x = a + kn \}$ for some integer k, then [a] is said to be equivalence class, modulo n, represented by [a]. The set of all congruence classes modulo n is denoted by Z_n .

$\therefore\ Z_n = \{[0], [1], [2], \ldots [n-1]\}$

BASIC ALGEBRA-Number system

- **Addition of residue classes**

Let [a], [b] ∈ Z_n then their sum is denoted by $+_n$ and is defined as follows:

$$[a] +_n [b] = \begin{cases} [a+b] & if\ a+b < n \\ [r] & if\ a+b \geq n \end{cases}$$

where r is the least non negative remainder when a+b is divided by n. hence $0 \leq r \leq n$

Ex. [1] $+_5$ [2] = [1+2]= 3

[3] $+_5$ [4] = [2] for 3+4=7 >5, 7=1x5+2

[3] $+_5$ [2] = [0]

- **Multiplication of residue classes**

Let [a], [b] ∈ Z_n then their product is denoted by $\times_n$ and is defined as follows:

$$[a] \times_n [b] = \begin{cases} [ab] & if\ ab < n \\ [r] & if\ a\,b \geq n \end{cases}$$

where r is the least non negative integer when ab is divided by n. hence $0 \leq r \leq n$

Ex. [2] $\times_5$ [2] =[4] ; [2] $\times_5$ [4] =[3] .

$$Z_n = \{[0],[1],[2],\ldots[n-1]\}$$

Algebraic systems

- A binary operation * on a set A is defined as a function from AxA into the set A itself. .
- A non empty set A with one or more binary operations on it is called an algebraic system.

Examples.

- Set : $N = \{1,2,3 \ldots\}$ – the set of natural numbers, Operation : the usual addition '+' which is a binary operation on N, then $(N, +)$ is an algebraic system.
- Similarly, $(Q, +), (Z, .), (R, +), (C, +)$ … are algebraic systems

General properties of algebraic system

Let (S, $*$) be an algebraic system, $*$ is the binary operation on S .

- **Closure property** – For all a,b $\in$ S, $a * b \in S$
- **Associativity** - For all a, b, c $\in$ S , $(a * b) * c = a * (b * c)$,
- **Commutativity** - For all a,b $\in$ S, $a * b = b * a$
- **Identity element** – There exists an element e $\in$ S, such that

  for any a $\in$ S, $a * e = e * a = a$
- **Inverse element** – For every a $\in$ S , there exists some b $\in$ S such that

  $a * b = b * a = e$, then b is called the inverse element of a.

MODULE 2

- GROUP
- ABELIAN GROUP
- FINITE AND INFINITE GROUP
- EXAMPLES
- ORDER OF GROUP
- ORDER OF ELEMENT

GROUPS

Definition : Group

If G is a non empty set and $*$ is a binary operation on G, then the algebraic system $\{G, *\}$ is called a **group** if the following axioms are satisfied:

1) For all a,b $\in$ S, $a * b \in S$ [Closure property]

2) For all a, b, c $\in$ G, $(a * b) * c = a * (b * c)$ (Associativity)

3) There exists an element e $\in$ G such that, for any a $\in$G, $a * e = e * a = a$ (Existence of identity)

4) For every a $\in$G, there exists an element $a^{-1} \in$ G such that

$$a * a^{-1} = a^{-1} * a = e$$ (Existence of inverse)

Abelian group

The group (G, $*$) which has commutative property ,

for all a,b ∈ S, $a * b = b * a$, is called an abelian group.

- **Finite/Infinite group**

  The group (G, $*$) is said to be finite or infinite according as the underlying set is finite or infinite.

- **Order of a group**

If (G, $*$) is a finite group , then the number of elements of G is the order of the group written as O(G) or |G|

- **Order of an element**

Let (G, $*$) be a group and a ∈ G, the least positive integer m, such that $a^m = e$, the identity element of G, is called order of a and is written as O(a)=m

Examples for Groups

1) The set $(Z, +)$, of all integers under addition forms a group.

2) The set of all 2 x 2 non singular matrices over R is an abelian group under matrix addition , but not abelian with respect to matrix multiplication as $AB \neq BA$

3) The set {1,-1,i, -i } is an abelian group under multiplication of complex numbers .

Permutation group

Let A be a non empty set, then a function $f: A \to A$ is a permutation of A if f is both one to one and onto, that is f is bijective. Let S_A denotes the set of all permutations on A. Let $f: A \to A$ and $g: A \to A$ be two functions. Then their composition, denoted by $f \circ$ g , is the function $f \circ g : A \to A$ defined by

(f∘g)$(a) = g(f(a))$, the composition of function is the binary operation on S_A.

If A ={1,2,3….}, then the permutation p on A can be written as

$$p = \begin{pmatrix} 1 & 2 & \dots & n \\ p(1) & p(2) & \dots & p(n) \end{pmatrix}$$

For example $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

If A has n elements S_A has $n!$ Permutations.

Permutation group

Let $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ $and\ p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, the composition of these two permutations is defined as

$$p_1 \circ p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

MODULE 3

- PROPERTIES OF GROUPS
- PROBLEMS ON GROUPS
- PROBLEMS ON ABELIAN GROUPS

Properties of Group

1. **The identity element of the group (G, $*$) is unique.**

Proof : If possible , let e_1 and e_2 be two identities of G.

$e_1 = e_2 * e_1$ [since e_2 is the identity]

$=e_2$ [since e_1 is the identity]

i.e $e_1=e_2$, the identity element is unique

2. **The inverse of each element of (G, $*$) is unique.**

Proof : If possible , let a' and a'' be two inverses for a in G.

$a * a' = a' * a = e$

$a * a'' = a'' * a = e$

$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$

$a' = a''$ implies the inverse is unique.

Properties of Group

3.The cancellation laws are true in a group

Viz, $a * b = a * c \Rightarrow b = c$ [left cancellation law]

and $b * a = c * a \Rightarrow b = c$ [right cancellation law]

Proof :

Let $a * b = a * c$ ----(1)

Since $a \in G, a^{-1} \in G$ exists such that $a * a^{-1} = a^{-1} * a = e$

Pre multiplying (1) by a^{-1}, $a^{-1} * (a * b) = a^{-1} * (a * c)$

$$(a^{-1} * a) * b = (a^{-1} * a) * c$$

$$e * b = e * c \quad => b = c$$

Let $b * a = c * a \Rightarrow b = c$ -----------(2)

Since $a \in G, a^{-1} \in G$ exists such that $a * a^{-1} = a^{-1} * a = e$

Post multiplying (2) by a^{-1}, $(b * a) * a^{-1} = (c * a) * a^{-1}$

$$b * (a * a^{-1}) = c * (a * a^{-1})$$

$$b * e = c * e \quad => b = c$$

4. $\boldsymbol{Prove\ (a * b)^{-1} = b^{-1} * a^{-1}}$, for any a, b ∈ G.

Proof:

Consider $(a * b) * (b^{-1} * a^{-1})$

$$= a * \left(b * (b^{-1} * a^{-1})\right) \text{ [Associativity]}$$

$$= a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = e$$

$\therefore b^{-1} * a^{-1}$ is the inverse of $a * b$.

5. If a , b ∈ G, the equation $a * x = b$ has the unique solution $x = a^{-1} * b$.

6. (G, $*$) cannot have an idempotent element except the identity element.

7. If *a* has inverse b and b has inverse c , then a = c.

Problems on Groups

1. Show that the set of all non zero real numbers namely R-{0} forms an abelian group with respect to $*$ defined by $a * b = ab/2$ for all a,b ∈ R-{0}

Proof : [To prove all the four axioms]

- Closure : if a, b ∈ R-{0} then , ab/2 is also a non zero real number ∈ R-{0}
- Associativity : $a * (b * c) = a * (bc/2) = abc/4$ ---------(1)

  $(a * b) * c = ab/2 * c = abc/4$ -----------(2)

  From (1) and (2) , $a * (b * c) = (a * b) * c$
- Identity element : $a * e = a$

  $ae/2 = a \; implies \; e = 2$ is the identity element .
- Inverse element : for $a \in R - \{0\}$, $a * a^{-1} = e$

  $\frac{aa^{-1}}{2} = 2 \quad => a^{-1} = \frac{4}{a}$ is the inverse of a

Problems on Groups

2. **Prove that the set R -{1} forms an abelian group with respect to $*$ defined by**

$a * b = (a + b - ab)$, for all $a, b \in R-\{1\}$.

Proof :

- Closure : If a, b ∈ R -{1} then , $(a + b - ab)$ is also a real number ∈ R-{1}
- Associativity :

$$a * (b * c) = a * (b + c - bc) = a + b + c - bc - a(b + c - bc)$$
$$= a + b + c - ab - bc - ac + abc$$
$$(a * b) * c = (a + b - ab) * c = a + b - ab + c - (a + b - ab)c$$
$$= a + b + c - ab - bc - ac + abc$$

Hence , $a * (b * c) = (a * b) * c$.

- Identity element : $a * e = a$

$a + e - ae = a$ => $e = 0$ is the identity element .

- Inverse element : For $a \in R - \{0\}$, $a * a^{-1} = e$

$$a + a^{-1} - aa^{-1} = 0$$

$a^{-1} = \frac{a}{a-1}$ is the inverse of 'a', ($a \neq 1$).

3. Let G = { f_1, f_2, f_3, f_4} where $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$ *and* $\circ$ be the composition of functions. Prove that (G, $\circ$) is a group.

Proof :

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

- Closed : From the table it is evident that $\circ$ is closed.
- Associativity :

$$f_1 * (f_2 * f_3) = f_1 * f_4 = f_4$$

$$(f_1 * f_2) * f_3 = f_2 * f_3 = f_4$$

Hence , $f_1 * (f_2 * f_3) = (f_1 * f_2) * f_3$.

- Identity element : From the table, we can see that f_1 is the identity element.
- Inverse element : Inverse of every element is the element itself

4. Let A={1,2,3}, S_A be the set of all permutations of A, then prove that with respect to right composition of permutations $\circ$, { S_A, $\circ$ } is an abelian group.

Proof :

Let $S_A = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ where

$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$

$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $and\ p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\circ$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	P_6	p_5
p_3	p_3	p_4	p_1	p_2	P_4	p_1
p_4	p_4	p_3	p_2	p_1	p_3	p_2
p_5	p_5	p_6	p_4	p_3	p_1	p_4
p_6	p_6	p_5	p_1	p_2	p_4	p_1

- From the above table, for any two or three elements we can prove closure and associative property.

- The identity element is p_1 and the inverse of any element is the element itself.

Problems on Groups

4. Let a ≠ 0 be a fixed real number and G = $\{a^n : n \in Z\}$, Prove that G is an abelian group under multiplication .

Proof :

- Closed : if $a^{n1}, a^{n2} \in$ G then $a * b = a^{n1+n2} \in$ G as n1+n2 ∈ Z
- Associativity : For $a^{n1}, a^{n2}, a^{n3} \in$ G

$$a^{n1} * (a^{n2} * a^{n3}) = a^{n1} * a^{n2+n3} = a^{n1+n2+n3}$$

$$(a^{n1} * a^{n2}) * a^{n3} = a^{n1+n2} * a^{n3} = a^{n1+n2+n3}$$

- Identity element - $a^n * a^e = a^n$

$a^{n+e} = a^n$ implies e=0 and $a^e = a^0 = 1$ is the identity element

- Inverse element – for $a \in R$, $a^n * a^{n1} = a^0 => n + n1 = 0 => n1 = -n$

$a^{n1} = a^{-n}$ is the inverse of a^n

5. For any group (G, *) if $a^2 =$ e with a $\neq$ e, then prove that G is abelian

[Or, if every element of a group (G, *) is its own inverse, then G is abelian]

Proof:

Let $\mathrm{a}^2 = \mathrm{e}$.

$$Then\ \mathrm{a}^2 * a^{-1} = (a * a) * a^{-1} = e * a^{-1} = a^{-1}$$

$$\mathrm{a}^2 * a^{-1} = a * (a * a^{-1}) = a * e = a$$

implies $a = a^{-1}$

Then for any $a, b \in G, (a * b)^{-1} = a * b$

$$b^{-1} * a^{-1} = a * b$$

$b * a = a * b$, G is abelian.

6. Let $(G,*)$ be a group. Prove that G is abelian if and only if $(a*b)^2 = a^2 * b^2$

Proof:

Let G be abelian,

Consider $(a*b)^2 = (a*b)*(a*b)$

$= a*(b*(a*b))$ [Associativity]

$= a*((b*a)*b)$

$= a*(a*b)*b$ [commutativity]

$= (a*a)*(b*b) = a^2 * b^2$

Now , suppose $(a*b)^2 = a^2 * b^2$

$(a*b)*(a*b) = (a*a)*(b*b)$

$a*(b*(a*b)) = a*(a*(b*b))$

$b*(a*b) = a*(b*b)$

$(b*a)*b = (a*b)*b$ [Associativity]

$b*a = a*b$ ----commutative.

Thus G is abelian.

- Exercises :

1. The set $\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}$ is an abelian group under matrix multiplication.

2. The set {0,1,2,3,4} is a finite abelian group of order 5 under addition modulo 5.

3. The set {1,3,7,9} is an abelian group under multiplication modulo 10.

MODULE 4

- SUBGROUPS
- EXAMPLES FOR SUBGROUP
- CONDITIONS FOR SUBGROUP
- PROBLEMS ON SUBGROUPS

Problems on subgroups

1.The intersection of two subgroups of a group G is also a subgroup of G .

Proof:

Let $H_1\, and\; H_2$ be any two subgroups of G. $H_1 \cap H_2$ is a non-empty set, since, at least the identity element e is common to both $H_1\, and\; H_2$

Let $a \in H_1 \cap H_2, then\; a \in H_1\; and\; a \in H_2$

Let $b \in H_1 \cap H_2, then\; b \in H_1\; and\; b \in H_2$

H_1 is a subgroup of G, $a * b^{-1} \in H_1\;\; a\; and\; b\;\; \in H$

H_2 is a subgroup of G, $a * b^{-1} \in H_2\;\; a\; and\; b\;\; \in H$

$\therefore\; a * b^{-1} \in H_1 \cap H_2$ implies $H_1 \cap H_2$ is a subgroup of G.

SUBGROUPS

If $\{G, *\}$ is a group and $H \subseteq G$ is a non-empty subset of G, called **subgroup** of G , if H itself forms a group .

Theorem:

The necessary and sufficient condition for a non empty subset H of a group $\{G, *\}$ to be a subgroup is, for every $a, b \in H \Rightarrow a * b^{-1} \in H$.

2.Show that the set $\{a + bi \in C | a^2 + b^2 = 1\}$ is a subgroup f (C, •) where • is the multiplication operator.

Proof:

Let H = $\{a + bi \in C | a^2 + b^2 = 1\}$, consider two elements $x + iy, p + iq \in H$ *such that*

$x^2 + y^2 = 1, p^2 + q^2 = 1$ and the identity element of C is 1+0i

Consider $(x + iy)\ (p + iq)\hat{}(-1) = (x + iy)(p - iq) = xp + yq + i(yp - xq)$

Now $(xp + yq)^2 + (yp - xq)^2 = x^2p^2 + y^2q^2 + 2xpyq + y^2p^2 + x^2q^2 - 2ypxq$

$$= x^2(p^2 + q^2) + y^2(p^2 + q^2) = 1$$

$\therefore \quad (x + iy)(p + iq)^{-1} \in H$, H is a subgroup.

3. Let G be an abelian group with identity e, prove that all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G

Proof:

$H = \{x \mid x^2 = e\}$

$e^2 = e \therefore$ the identity element e of G $\in H$

$x^2 = e$

$x^{-1}.x^2 = x^{-1}.e \quad => \quad x = x^{-1}$

Hence, $if\ x \in H, x^{-1} \in H$ [inverse exists]

Let $x, y \in H$, since G is abelian, $xy = yx = y^{-1}x^{-1} = (xy)^{-1}$

$\therefore\ (xy)^2 = e.$ i.e $xy \in H$

Thus, if $x, y \in H, we\ have\ xy \in H$ [closed]

Thus H is a subgroup.

4. Union of two subgroups of (G,*) need not be a subgroup of (G,*).

Module 5

- Cyclic groups
- Examples
- Properties
- Problems

Cyclic group

A group (G, $*$) is said to be a **cyclic group** if there exists an element a$\in G$ such that every element of G can be expressed as some integral power of a, **a is called generator of G**.

We write G=(a)

Examples :

1. Let G={1,-1, i, -i} and G is a group under multiplication. It is cyclic with the generator i

   (i.e.) G=(i) or G=(-i)

2. Let G={1, ω, ω^2} is a cyclic group under multiplication generated by ω . ω^2 is also a generator.

3. (Z , +) is a cyclic group with generator 1. Note -1 is also a generator.

Properties of cyclic groups

1. Every cyclic group is abelian

Proof:

Let $(G,*)$ be a cyclic group with generator a. Let $x, y \in G$ such that $x = a^m, y = a^n$

$$x * y = a^m * a^n = a^{m+n} = a^{n+m} = a^n * a^m = y * x$$

Therefore $(G,*)$ abelian.

2.Let (G, $*$) be a cyclic group generated by a , then a^{-1} is also a generator of G.

Proof:

Let (G, $*$) be a cyclic group generated by a , then $for\ x \in G\ then\ x = a^n\ for\ some\ n \in Z$

$$x = (a^{-1})^{-n}, -n \in Z$$

$\therefore\ a^{-1}$ is also a generator of G.

3. Any subgroup of a cyclic group is itself a cyclic group.

Proof :

Let (G, $*$) be a cyclic group generated by a and H be a subgroup of G.

if $a^k \in H\ then\ a^{-k} \in H$. Let m be the least positive integer such that $a^k \in H$

we have to prove that $H = (a)^m$. Let $c \in H$. $\therefore c \in G$

$$c = a^n \text{ for some } n \in Z$$

Now $n, m \in Z$, there exists integers q and r such that $n = mq + r$, $0 \leq r < m$ by division algorithm.

$$\text{Now } c = a^n = a^{mq+r} = a^{mq} * a^r$$

$$a^r = a^{-mq} * c = (a^m)^{-q} * c \in H$$

Since $c \in H, (a^m)^{-q} \in H$ and H is a subgroup. But $0 \leq r < m$ and m is the least positive integer such that $a^m \in H$. Therefore r = 0

$$\therefore c = a^{mq} = (a^m)^q$$

Hence every element of H can be written as an integer power of a^m. $\therefore H = (a^m)$ is a cyclic group.

4. The order of a cyclic group is the same as the order of its generator.

5. A finite group of order n containing an element a of order n is cyclic.

Problems

1. Find the number of generators of a cyclic group of order 5.

Let G = (a) be a cyclic group of order 5. Then G = $\{a, a^2, a^3, a^4, a^5 = e\}$.

Since (1,5) =1, (2,5) =1, (3,5) =1, (4,5) =1.

The generators are a, a^2, a^3 and a^4.

The number of generators is 4.

2. Find the number of generators of a cyclic group of order 8 .

Let G = (a) be a cyclic group of order 5. Then G=$(a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$.

Since (1,8)=1, (3,8)=1, (5,8)=1, (7,8)=1.

The generators are a, a^3, a^5 and a^7.

The number of generators is 4.

MODULE-6
GROUP HOMOMORPHISM

- DEFINITION OF HOMOMORPHISM

- EXAMPLES OF HOMOMORPHISM

- PROPERTIES OF HOMOMORPHISM

DEFINITION OF HOMOMORPHISM

- Given two groups, $(G, *)$ and $(H, \cdot)$, a **group homomorphism (morphism)** from $(G, *)$ to $(H, \cdot)$ is a function $h : G \rightarrow H$ such that for all u and v in G it holds that

$$h(u * v) = h(u) \cdot h(v) \text{ for all } u, v \in \mathrm{G}$$

- Isomorphism: A group homomorphism that is bijective; i.e., injective and surjective. Its inverse is also a group homomorphism.
- In this case, the groups G and H are called *isomorphic*; they differ only in the notation of their elements and are identical for all practical purposes
- $(G, *)$ and $(H, \cdot)$ are isomorphic – there is an isomorphism between $(G, *)$ and $(H, \cdot)$and it is denoted by $(G, *) \cong (H, \cdot)$

EXAMPLES OF HOMOMORPHISM

1. Every isomorphism is a homomorphism with Ker = {e}.

2. Let G = Z under addition and $\bar{G}$ = {1, -1} under multiplication.

   Define : $f: G \rightarrow \bar{G}$ by f(n) $=\begin{cases} 1, \text{ n is even} \\ -1, \text{ n is odd} \end{cases}$

   is a homomorphism.

PROPERTIES OF HOMOMORPHISM

If $f: G \to G'$ is a group homomorphism from $(G,*)$ to $(G',\cdot)$

(i) f(e) =e' where e and e' are the identity elements of G and G' respectively

(ii) For any aϵG, $f(a^{-1}) = [f(a)]^{-1}$.

(iii) If H is a subgroup of G, then $f(H) = \{f(h) / h \in H\}$ is a group of G.

MODULE-7
RINGS

• A **ring (R,+, ·)** is a set R on which there are defined two binary operations '+' and '·' satisfying the following axioms.

- (R1) (R,+) is an abelian group.
- (R2) (R, ·) is semigroup :The operation · has the closure, associativity and identity properties.
- (R3) The additive identity is unique and The additive inverse of any element in R is unique
- (R4) The cancellation law for addition holds. That is if a,b, c ∈ R with a+b = a+c, then b = c
- (R5) Distributive laws are true. For all a,b,c ϵ R,

  a.(b+c)=(a.b)+(a.c)

  (a+b).c=(a.c)+(b.c)

- A **commutative ring** is a ring (R,+, ·) for which ab = ba, for all a,b ∈ R. If a ring is not commutative it is called noncommutative.
- A **ring with identity e** (also called a ring with unity) is a ring R which contains an element e ∈ R (with e ≠ 0) satisfying ea = ae = a , for all a ∈ R. Generally, the unity or identity element of a ring R is denoted by 1 or 1_R.
- A ring which has finite many elements is called **finite ring**

Examples:

1. $\mathbb{Z}, \mathbb{Q}, R\ and\ \mathbb{C}$ are commutative rings with identity, with the usual operations of addition and multiplication, where $\mathbb{Z}$ (respect: $\mathbb{Q}, R\ and\ \mathbb{C}$) is the set of all integer (respect: rational, real, complex) numbers
2. Let n ≥ 1 be an integer. Then the set $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots\ldots \overline{n-1}\}$ under addition $+_n$ and multiplication $\cdot_n$ modulo n is a commutative ring with unity 1, known as the ring of integers modulo n. The multiplication modulo n is defined on $\mathbb{Z}_n$ as following: ab mod n (or a $\cdot_n$ b) is the integer r ∈ $\mathbb{Z}_n$ such that ab = qn + r in Z for some q ∈ $\mathbb{Z}$

3. Let R = $\{\bar{0}, \bar{2}, \bar{4}\} \subseteq \mathbb{Z}_6$. Then $(R, +_6, \cdot_6)$ is a commutative ring with identity $\bar{4}$.

4. The set $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\}$ of even integers under ordinary addition and multiplication is a commutative ring without unity. More generally, if $n \geq 2$, then the set $n\mathbb{Z} = \{xn \mid x \in \mathbb{Z}\}$ under ordinary addition and multiplication is a commutative ring without unity.

5. The set $M_2(\mathbb{Z})$ of 2 x 2 matrices with integer entries is a non-commutative ring with unity.

➢ Let R be a ring with identity 1. A **non zero-element a in a ring R is called a unit** if it has a multiplicative inverse, i.e., if there exists $b \in R$ such that $ab = ba = 1$. We denote the multiplicative inverse of a by a^{-1}.

Theorem:1

Let R be a ring with identity 1.

(a) The multiplicative identity is unique.

(b) Let $a \in R$. If a has a multiplicative inverse in R, then it is unique.

Theorem:2

Let R be a ring with 1 and let R^* be the set of all multiplicative inverse elements in R. Then $(R^*, \cdot)$ is a group. It is called the group of invertible elements.

Theorem:3

Let R be a ring. Then for all $a, b, c \in R$,

(1) $a0 = 0 = 0a$.

(2) $a(-b) = -(ab) = (-a)b$.

(3) $a(b-c) = ab-ac$ and $(a-b)c = ac-bc$.

(4) $(-a)(-b) = ab$.

Theorem:4

For all positive integers m and n and for all a,b in a ring R, the following hold:

(1) $a^m a^n = a^{m+n}$.

(2) $(a^m)^n = a^{mn}$.

(3) $ma+na = (m+n)a$.

(4) $m(na) = (mn)a$.

(5) $(ma)(nb) = (mn)(ab)$

Zero Divisors:

- A non-zero element x in a ring R is called a left zero divisor if there exists a nonzero element $y \in R$ such that $xy = 0$.
- A non-zero element x in a ring R is called a right zero divisor if there exists a nonzero element $y \in R$ such that $yx = 0$.
- A non-zero element x in a ring R is called a zero divisor if it is a left and right zero divisor.

Example:

Let R be a ring with identity 1. Then $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ are zero divisors in the ring $M_{2\times 2}(R)$ of all 2×2 matrices over a ring R, (because $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$)

Lemma:

Let $\bar{x} \in \mathbb{Z}_n$. Then the following statements are equivalent:

(1) $\bar{x}$ is a zero divisor. (2) $\bar{x} \neq 0$ and $\gcd(x,n) \neq 1$.

Problems:

1. Find all zero divisors in a ring $(\mathbb{Z}_4, +_4, \cdot_4)$.

Solution: $\bar{0}$ is a non zero divisor

Since gcd(1,4) = 1 and gcd(3,4) = 1,

we have from Lemma , that $\bar{1}$ and $\bar{3}$ are non zero divisors. Since gcd(2,4) = 2 ≠ 1, , we have from Lemma , that $\bar{2}$ is a zero divisor and $\bar{2} \cdot_4 \bar{2} = 0$. Thus the zero divisor in a ring $(\mathbb{Z}_4, +_4, \cdot_4)$ is only $\bar{2}$.

2. Find all zero divisors in a ring $(\mathbb{Z}_8, +_8, \cdot_8)$

Ans: zero divisors in a ring $(\mathbb{Z}_8, +_8, \cdot_8)$ are $\{\bar{2}, \bar{4}, \bar{6}\}$

Theorems: 1. Let R be a non zero ring with identity 1. Then every unit element (element has a multiplicative inverse) a in R is a non zero divisor.

2. Let R be a non zero ring with identity 1, let R^* be the set of all unit elements in R and let R^+ be the set of zero divisor elements in R. Then $R^* \cap R^+ = \phi$.

- Let R be a ring. We say that **R satisfies the cancellation laws** for multiplication if for any a,b, c ∈ R such that a ≠ 0 and ab = ac or ba = ca, then b = c.

Example: The ring $(\mathbb{Z}_4, +_4, \cdot_4)$ does not satisfy the cancellation laws for multiplication, since $\bar{2} \cdot_4 \bar{2} = \bar{2} \cdot_4 \bar{0}$ but $\bar{2} \neq \bar{0}$.

- A ring R is without zero divisors if and only if R satisfies the cancellation laws for multiplication.

- Let R be a ring with identity which has no zero divisors. Then the only solutions of the equation $x^2 = x$ are $x = 0$ and $x = 1$.

Integral Domain

An integral domain is a commutative ring with identity which does not have zero divisors.

Theorems:

If R is an integral domain, then:

(1) R satisfies the cancellation laws for multiplication.

(2) 0 and 1 are the only idempotent elements in R.

(3) if R is a ring without zero divisors, then every subring of R is without zero divisors.

Examples:

1. The ring $(\mathbb{Z}_p, +_p, \cdot_p)$ is an integral domain, for any prime number *p*.

2. The rings $(\mathbb{Z}_6, +_6, \cdot_6)$ and $2\mathbb{Z}$ are not integral domains.

3. The rings $\mathbb{Z}, \mathbb{Q}, R \ \ and \ \mathbb{C}$ are integral domains.

Field

A field is a commutative ring with identity ($1 \neq 0$) in which every non-zero element has a multiplicative inverse.

Division Ring : A ring R with identity ($1 \neq 0$) is called a division ring or a (**skew field**) if every non-zero element has a multiplicative inverse.

Remark:

(1) If $u = a+bi$ and $v = c+di$ are complex numbers, then $u+v = (a+bi) + (c+di) = (a+c) + (b+d)i$ and $u.v = (a+bi).(c+di) = (ac-bd) + (ad+bc)i$.

(2) If $u = a+bi$, then $\bar{u} = a-bi$ and $u.\bar{u} = a^2 + b^2$

Example: (Hamilton's quaternions ring)

Let H = $\left\{\begin{bmatrix} u & \overline{-v} \\ v & \bar{u} \end{bmatrix} \mid u, v \in \mathbb{C}\right\}$ with usual addition (+) and multiplication (·) on matrices.

Then (H,+, ·) is a non-commutative division ring.

Proof. It is clear that (H,+, ·) is a subring of the ring ($M_2(\mathbb{C})$,+, ·) and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity element of the ring (H,+, ·) . The ring (H,+, ·) is non-commutative, since if A = $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and B = $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, then A.B = $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \neq$ B.A = $\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

The non-zero elements of H are invertible.

Let A $= \begin{bmatrix} u & \overline{-v} \\ v & \bar{u} \end{bmatrix} \in$ H with A $\neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Let B $= \begin{bmatrix} \frac{\bar{u}}{u\bar{u}+v\bar{v}} & \frac{\bar{v}}{u\bar{u}+v\bar{v}} \\ \frac{-v}{u\bar{u}+v\bar{v}} & \frac{u}{u\bar{u}+v\bar{v}} \end{bmatrix}$. Since B $\in$ H

and A.B = B.A $= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, we have A is invertible and $A^{-1} = \begin{bmatrix} \frac{\bar{u}}{u\bar{u}+v\bar{v}} & \frac{\bar{v}}{u\bar{u}+v\bar{v}} \\ \frac{-v}{u\bar{u}+v\bar{v}} & \frac{u}{u\bar{u}+v\bar{v}} \end{bmatrix}$.

Therefore, (H,+, ·) is a non-commutative division ring.

Every field is a division ring but the converse is not true in general

Example:

1. Let $H = \left\{ \begin{bmatrix} u & \overline{-v} \\ v & \bar{u} \end{bmatrix} \mid u, v \in \mathbb{C} \right\}$ with usual addition $(+)$ and multiplication $(\cdot)$

   on matrices. Then $(H,+,\cdot)$ is a non-commutative division ring (Hamilton’s

   quaternions ring) and hence it is not a field.

2. If $F = \{a+b\sqrt{3} \mid a,b \in Q\}$, then $(F,+,.)$ is a field.

Theorem: Every field is an integral domain

Proof. Let $(F, +,\cdot)$ be a field, thus $(F, +,\cdot)$ is a commutative ring with identity. Let a,b ∈ F with a ≠ 0 and a.b = 0. We will prove that b = 0. Since F is a field, it follows that a has a multiplicative inverse a^{-1} in F. Then $a^{-1}.(a.b) = a^{-1}.0 = 0$ and hence b = 0. Thus $(F, +,\cdot)$ has no zero divisors and hence $(F, +,\cdot)$ is an integral domain.

Remark: The converse of Theorem Every field is an integral domain is not true in general, for example the ring $(\mathbb{Z}, +, \cdot)$ is an integral domain but it is not a field since $2 \in \mathbb{Z}$ has no a multiplicative inverse in $\mathbb{Z}$.

Theorem: Every finite integral domain is a field.

Proof. Let R be a finite integral domain. Thus R is a commutative ring with identity. Let n be the number of distinct elements in R, say R = $\{a_1,a_2,\ldots,a_n\}$, where the a_i are the distinct elements of R. Let a be any nonzero element of R. Consider the set of products R '= $\{a.a_1,a.a_2,\ldots,a.a_n\}$. We will prove that all elements in R ' are distinct. Assume that there are i, j such that i ≠ j and $a.a_i = a.a_j$. Since R is an integral domain and a ≠ 0, we have from cancellation theorem that R satisfies the cancellation laws for multiplication and hence $a_i = a_j$ and this is a contradiction. Thus all elements in R ' are distinct. Since R' ⊆ R, we have R = R ' . Since 1 ∈ R, we have 1 ∈ R' and so 1 = $a.a_s$ for some a_s ∈ R. Since R is commutative, we have 1 = $a.a_s = a_s.a$ and hence a has a multiplicative inverse a_s in R. Therefore, R is a field.

Theroem:The ring ($\mathbb{Z}_n, +_n, \cdot_n$) is a field if and only if n is a prime number.

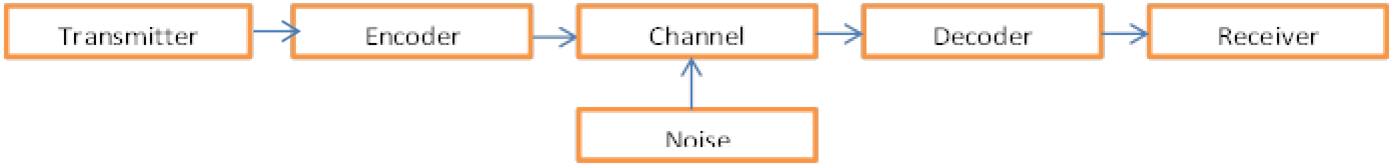
Proof. **(⇒)** Suppose that ($\mathbb{Z}_n, +_n, \cdot_n$) is a field. By Theorem Every field is an integral domain, ($\mathbb{Z}_n, +_n, \cdot_n$) is an integral domain. By Theorem (The ring ($\mathbb{Z}_p, +_p, \cdot_p$) has no zero divisor if and only if p is a prime integer number), n is a prime number.

(⇐) Suppose that n is a prime number. By Theorem (The ring ($\mathbb{Z}_p, +_p, \cdot_p$) has no zero divisor if and only if p is a prime integer number), the ring ($\mathbb{Z}_n, +_n, \cdot_n$) has no zero divisor. Since ($\mathbb{Z}_n, +_n, \cdot_n$) is a commutative ring with identity, we have ($\mathbb{Z}_n, +_n, \cdot_n$) is an integral domain. Since the ring ($\mathbb{Z}_n, +_n, \cdot_n$) is finite, we have from Theorem (Every finite integral domain is a field) that ($\mathbb{Z}_n, +_n, \cdot_n$) is a field.

CODING THEORY - ENCODERS AND DECODERS- HAMMING CODES

Encoder: **It** is a device or process which converts(transforms) data(messages) in such a way that the presence of noise in the transformed messages is detectable.

Decoder: **It** is a device or process which converts(transforms) the encoded data(message
s) into their original form that can be understood by the receiver.



Alphabet: Letters or symbols or characters . We choose binary code B= {0,1} as alphabet

Message(word): Basic unit of information which is a finite sequence of characters from a specified set or alphabet B = {0,1}

Group Code: If B ={0,1},then B^n = { $x_1, x_2, \ldots\ x_n \,/\, x_i \epsilon B$, $i = 1,2,3,\ldots n$} is a group under the binary operation of addition modulo 2, denoted by $+_2$ or $\oplus$. This group (B^n, $\oplus$) is called a group code

Cayley table for $+_2$:

$+_2$	1	0
1	0	1
0	1	0

Order of B^n is 2^n

Theorem: (B^n, $\oplus$) is a group

Proof: If $x_1, x_2, \ldots\ x_n = (x_1, x_2, \ldots\ x_n)$ and $y_1, y_2, \ldots\ y_n = (y_1, y_2, \ldots\ y_n)$ ϵ B^n, then

$x_1, x_2, \cdots\cdots x_n \quad y_1, y_2, \cdots\cdots, y_n = (x_1 +_2 y_1, x_2 +_2 y_2, \cdots\cdots, x_n +_2 y_n) \epsilon$ B^n Identity element of B^n is (0,0,0,……,0)

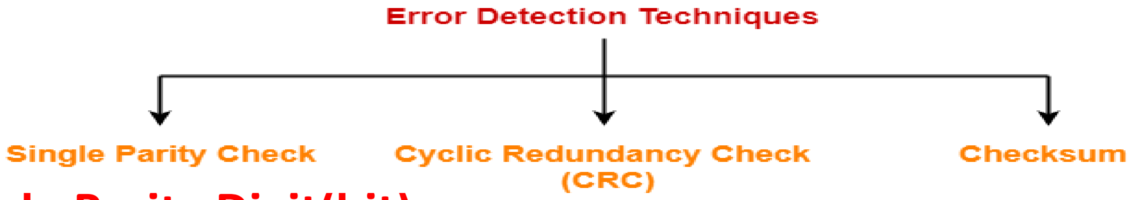
Inverse of $x_1, x_2, \ldots\ x_n$ is itself

Hence (B^n, $\oplus$) is a group and it is also abelian

Encoding Function:

- Let n, m be integers such that n>m. An one – to – one function $e: B^m \to B^n$ (each word in B^m is assigned different code words in B^n) is called an (m,n) encoding function or code.
- If $b \in B^m$ is the original word , then e(b) is the code word or encoded word representing b.
- The additional 0's and 1's in e(b) (as n>m) will provide the means to detect or correct errors in the transmission channel
- Each code word x = e(b) is received as the word x_t in B^n.

Block codes – The message is divided into fixed-sized blocks of bits, to which redundant bits are added for error detection or correction.



Single Parity Check: Parity Digit(bit):

- One extra bit (digit) called as **parity digit** is sent along with the original data bits.
- Parity digit helps to check if any error occurred in the data during the transmission.

Hamming Code(developed by R.W. Hamming for error correction)

- The codes obtained by introducing additional digits called parity digits to the digits in the original message are called Hamming Codes
    - **Hamming Codes = Original data + parity bit**
- block code that is capable of detecting up to two simultaneous bit errors and correcting single-bit errors.

Error detection using single parity check involves the following steps:-

At sender side,

- Total number of 1's in the data unit to be transmitted is counted.
- The total number of 1's in the data unit is made even in case of even parity.
- The total number of 1's in the data unit is made odd in case of odd parity.
- This is done by adding an extra bit called as **parity bit**.

The newly formed code word (Original data + parity bit) is transmitted to the receiver

Error detection using single parity check involves the following steps:-

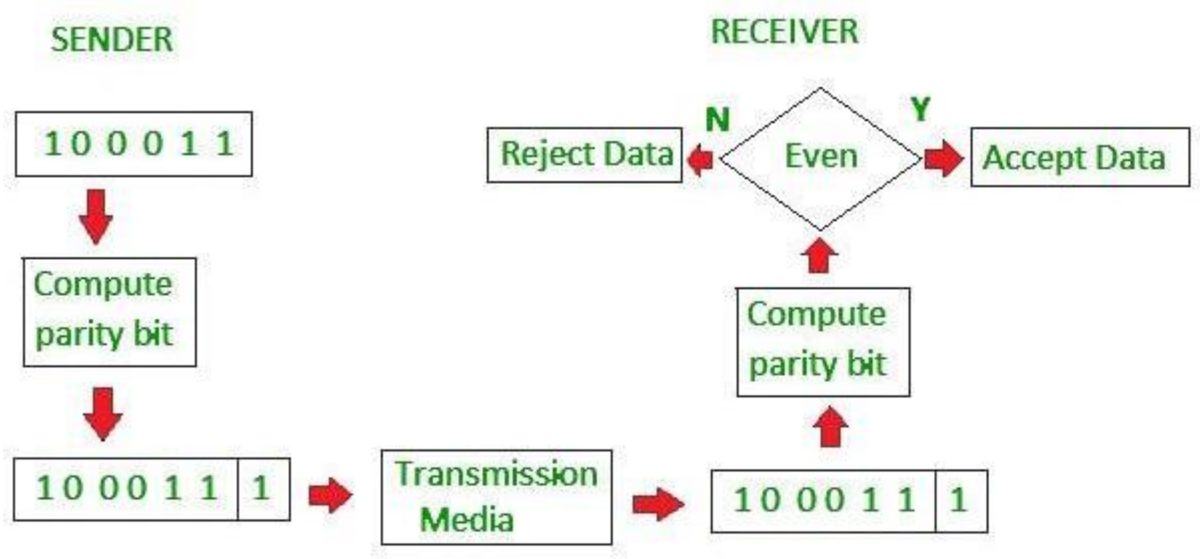
At receiver side,

- Receiver receives the transmitted code word.
- The total number of 1's in the received code word is counted.

Then, following cases are possible:-

- If total number of 1's is even and even parity is used, then receiver assumes that no error occurred.
- If total number of 1's is even and odd parity is used, then receiver assumes that error occurred.
- If total number of 1's is odd and odd parity is used, then receiver assumes that no error occurred.
- If total number of 1's is odd and even parity is used, then receiver assumes that error occurred

Parity Check Example:-



Parity Checking

Traditionally 7 bits represent a normal ASCII character, with the parity bit being added as the 8th bit. In this scenario, data is to be sent between devices using an even parity. Below is a sample of data at both the sender and receivers end:

Character	Sender	Parity Bit	Receiver	Parity	
"E"	1000101	1	10001011	Even	
"A"	1000001	0	10000010	Even	
"C"	1000011	1	11100111	Even	
"q"	1110001	0	11100000	Odd	**Error!**

Issues:

- Errors will not be detected if there are an even number of bit swaps, which maintains the agreed parity (even or odd)
- Adding an extra bit to every byte will have a significant increase on the amount of data being transmitted

ASCII(AMERICAN STANDARD CODE INFORMATION INTERCHANGE

ASCII Code: Character to Binary

0	0011 0000	O	0100 1111	m	0110 1101
1	0011 0001	P	0101 0000	n	0110 1110
2	0011 0010	Q	0101 0001	o	0110 1111
3	0011 0011	R	0101 0010	p	0111 0000
4	0011 0100	S	0101 0011	q	0111 0001
5	0011 0101	T	0101 0100	r	0111 0010
6	0011 0110	U	0101 0101	s	0111 0011
7	0011 0111	V	0101 0110	t	0111 0100
8	0011 1000	W	0101 0111	u	0111 0101
9	0011 1001	X	0101 1000	v	0111 0110
A	0100 0001	Y	0101 1001	w	0111 0111
B	0100 0010	Z	0101 1010	x	0111 1000
C	0100 0011	a	0110 0001	y	0111 1001
D	0100 0100	b	0110 0010	z	0111 1010
E	0100 0101	c	0110 0011	.	0010 1110
F	0100 0110	d	0110 0100	,	0010 0111
G	0100 0111	e	0110 0101	:	0011 1010
H	0100 1000	f	0110 0110	;	0011 1011
I	0100 1001	g	0110 0111	?	0011 1111
J	0100 1010	h	0110 1000	!	0010 0001
K	0100 1011	i	0110 1001	'	0010 1100
L	0100 1100	j	0110 1010	"	0010 0010
M	0100 1101	k	0110 1011	(	0010 1000
N	0100 1110	l	0110 1100	)	0010 1001
				space	0010 0000

Hamming Codes:

- If the original message is a binary string of length m, the Hamming encoded message is string of length n (n>m).
- m digits represent the information part of the message and the remaining (n-m) digits are for the detection and correction of errors in the message received.
- In Hamming's single error detecting code of length n, the first (n-1) digits contain the information part of the message and the last digit is made either 0 or 1.

Even Parity Check:-

- The extra digit introduced in the last position of the encoded word of length n, gives an even number of 1's

Odd Parity Check:-

- The extra digit introduced in the last position of the encoded word of length n, gives an odd number of 1's

Weight of the Binary string:-

- The number of 1's in the binary string $x \in B^2$. It is denoted by $|x|$.

Hamming Distance:-

- If $x_1, x_2, \ldots\ldots x_n = (x_1, x_2, \ldots\ldots x_n)$ and $y_1, y_2, \ldots\ldots y_n = (y_1, y_2, \ldots\ldots y_n) \epsilon B^n$, the number of positions in the strings for which $x_i \neq y_i$ *is called the Hamming Distance between x and y. It is denoted by H(x,y)*
- $H(x,y)$ = *weight of* $x \quad y = \sum_{i=1}^{n} (xi +_2 y_i)$

Example of Hamming Distance:-

If x= 11010 and y = 10101,then H(x,y) $=|x \quad y| = |01111| = 4$

- The minimum distance of a code (a set of encoded words) is the minimum of the Hamming distances between all pairs of encoded words in the code.
- For example: If x = 10110, y = 11110 and z = 10011, then H(x,y) = 1, H(y,z) = 3, H(z,x) = 2 and so the minimum distance between these code words is 1.

Theorem:1. A code(an(m,n)encoding function)can detect at the most k errors if and only if the minimum distance between any two code words is at least (k+1)

Example:

- Let x= 000 and y = 111 be the encoded words (two values of

- $H(x,y) = |\sum_{i=1}^{3} (x_i +_2 y_i)| = 3$
- In x = 000, one error occurs, the received word could be 100 or 001 or 010.
- In y = 111, one error occurs, the received word could be 011 or 101 or 110
- The two sets of received words {100 , 001 , 010}and {011 , 101 , 110} are distinct
- Hence, if any of the above six words is received due to one error, it is easily found out which encoded word has get altered and in which digit position the error has occurred and hence, the error is corrected.
- If two error occur during transmission,

  the word 000 would have been received as 110 or 011 or 101

  the word 111 would have been received as 100 or 001 or 100

- If an error in single digit is corrected in any of received word 110 or 011 or 101, the corrected word would be 111, which is not the transmitted word.
- Similarly, If an error in single digit is corrected in any of received word 100 or 001 or 100, the corrected word would be 000, which is not the transmitted word.

Theorem:2. A code can correct a set of at most k errors iff the minimum distance between any two code words is at least (2k+1) Example:

- Let x= 000 and y = 111 be the encoded words (two values of encoding function)

- $H(x,y) = |\sum_{i=1}^{3}(xi +_2 y_i)| = 3$
- In x = 000, during transmission zero or one error occurs, the received word could be 000 or 100 or 001 or 010.
- In y = 111, during transmission zero one error occurs, the received word could be 111 or 011 or 101 or 110
- The two sets of received words {000,100 , 001 , 010}and {111,011 , 101 , 110} are distinct
- So whatever words received, the single or no error can be easily detected and corrected.

Basic Notions of Error Correction using Matrices:- Generator Matrix:

- Let $e: B^m \rightarrow B^n$ be the encoding function with m<n, m,n $\in z^+$ and B = {0,1}. Consider the m x n matrix G over B. This matrix G is called the generator matrix for the code
- It is of the form $[I_m|A]$, I_m is the m x m unit matrix and A is an m x (n-m) matrix to be chosen suitably.
- If w is a message in B^m, then e(w) = wG and the code (the set of code words) $C = e(B^m) \subseteq B^n$, where w is a (1 x m) vector
- If w is a message in B^2,
- Assume $G = \begin{bmatrix} 1 & 0 & 11 & 0 \\ 0 & 1 & 01 & 1 \end{bmatrix}$

- $B^2 = \{00,01,10,11\}$
- Code words corresponding to above message are
- $e(00) = \begin{bmatrix} 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 00 & 0 \end{bmatrix}$
- $e(10) = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 11 & 0 \end{bmatrix}$
- $e(01) = \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 01 & 1 \end{bmatrix}$
- $e(11) = \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 10 & 1 \end{bmatrix}$
- Clearly $C = e(B^2) \subseteq B^5$

Problems:

1. Given the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ corresponding to the encoding function $e: B^3 \rightarrow B^6$,find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message. Are all the words decoded uniquely?

(i) 110101 (ii) 001111 (iii) 110001 (iv) 111111

Solution: If we assume the G = $[I_3|A]$, I_3 is the 3 x 3 unit matrix, then

$$H = [A^T|\ I_3] = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Compute the syndrome of each of the received word by using H$\cdot$ $[r]^{T}$

(i) H$\cdot$ $[r]^{T}$= H$\cdot$ $[e(w)]^{T}$= $\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, Received word is the transmitted word itself and the original message is 110

(ii) H$\cdot$ $[r]^{T}$ = H$\cdot$ $[e(w)]^{T}$= $\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$, Received word is the fifth column of H, the element in the fifth position of r is changed, Therefore, the decoded word is 001101 and the original message is 001.

(iii) $H\cdot[r]^T = H\cdot[e(w)]^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, Received word is the fourth column of H, the element in the fourth position of r is changed, Therefore, the decoded word is 110101 and the original message is 110

(iv) $H\cdot[r]^T = H\cdot[e(w)]^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$, Received word is not identical with any column of H, the received word cannot be decoded uniquely.