Groups

Definition and examples

A Group $\langle G, * \rangle$ is an algebraic system in which the binary operation $*$ on G satisfies three conditions

(1) **Associativity**

For all $x, y, z \in G$,

$$x * (y * z) = (x * y) * z$$

(2) **Identity**

$\exists$ an elt $e \in G$ s.t for any $x \in G$,

$$x * e = e * x = x$$

(3) **Inverse**

$\forall\ x \in G$, $\exists$ an elt $x^{-1} \in G$ s.t

$$x^{-1} * x = x * x^{-1} = e.$$

Note:

1) A group $(G, *)$ in which the operation $*$ is commutative is called **abelian group** (or) **commutative gp.**

2) Cancellation property is hold in every gp.

(Since the existence of the inverse elt of every elt)

$$\left.\begin{aligned} a * b = a * c &\Rightarrow b = c \\ b * a = c * a &\Rightarrow b = c \end{aligned}\right\} \forall\ a, b, c \in G$$

3) S.T a gp cannot have any elt which is idempotent except the identity.

Proof:- Let $a \in G$ be an idempotent elt of G

i.e., $a * a = a$

Now $e = a * a^{-1} = a^{-1} * a$

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

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

$$= e * a$$

$$e = a$$

Hence the identity is the only idempotent elt of G.

Permutation

Any one-to-one mapping of a set S onto S is called a permutation of S.

Order of a Groups |G|

The order of a group $\langle G, * \rangle$ denoted by |G|, is the number of elts of G. which is finite.

Examples

① Let $\mathbb{I}$ (or) $\mathbb{Z}$ be set of integers. $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$

The algebraic system $\langle \mathbb{Z}, + \rangle$ is an abelian grp.

② $\langle \mathbb{R}, + \rangle$ and $\langle \mathbb{R} - \{0\}, \times \}$ are abelian groups where $\mathbb{R}$ is the set of all real numbers

③ $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Q} - \{0\}, \times \rangle$ are abelian groups where $\mathbb{Q}$ is the set of all rational numbers.

④ $\langle Z_m, \oplus \rangle$ (or) $\langle Z_m, +_m \rangle$ and

$\langle Z_m, \otimes \rangle$ (or) $\langle Z_m, \times_m \rangle$ are abelian groups.

where $Z_m = \{[0], [1], \ldots, [m]\}$

$\oplus$ or $+_m$ = addition modulo 'm'

$\otimes$ or $\times_m$ = multiplication modulo 'm'.

Examples of Groups

1. If M_2 is the set of 2×2 non-singular matrices over $\mathbb{R}$ via $M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{R} \text{ \& } ad-bc \neq 0 \right\}$.

P.T M_2 is a gp under the operation of usual matrix multiplication.

Soln:-

If $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

clearly $AB = \begin{bmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_1+d_1c_2 & c_1b_2+d_1d_2 \end{bmatrix} \in M_2$

closure is true.

$\because$ we can prove Associative

Now $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity elt $\in M_2$

$A^{-1} = \frac{1}{|A|} \text{adj } A$ exists $\in M_2$

$\therefore \langle M_2, \times \rangle$ is a gp.

But $AB \neq BA$ So is not commutative. (or abelian.)

2. If $*$ is defined on Q^+ s.t $a*b = \frac{ab}{3}$ for $a,b \in Q^+$, Show that $\{Q^+, *\}$ is an abelian gp.

Soln:-

(i) $a,b \in Q^+$, $\frac{ab}{3} \in Q^+$ closure.

(2) $(a*b)*c = \frac{ab}{3} * c = \frac{ab}{3} \cdot \frac{c}{3} = \frac{abc}{9}$

$a*(b*c) = a * \frac{bc}{3} = \frac{a}{3} \cdot \frac{bc}{3} = \frac{abc}{9}$

$\therefore$ associative.

(3) let e be the identity elt of Q^+ under $*$

s.t $a * e = e * a = a$

$$\frac{ae}{3} = a \qquad e = 3 \in Q^+$$

$$ae = 3a \quad (\times)$$

$$(ae - 3a) = 0$$

$$\Rightarrow e = 3$$

∴ Identity elt exists

(4) let b be the inverse elt s.t

$$a * b = b * a = e = 3$$

$$\frac{ab}{3} = 3$$

$b = \frac{9}{a} \in Q^+$ is the inverse of a.

$$\therefore a * \frac{9}{a} = \frac{a \times 9}{3a} = e$$

H.W

(3) $a * b = \frac{ab}{2}$ $a, b \in Q^+$

(4) $a * b = a + b + 1$, $a, b \in \mathbb{Z}$ ✓ $(a * b) * c = (a+b+1) * c$
$= a+b+1+c+1$
$= a+b+c+2$

(5) $a * b = a + b - ab$, $a, b \in \mathbb{R}$

✓ $a * e = a$
$a + e + 1 = a$
$e = -1$

(6) Verify addition modulo and multiplication modulo

check $\langle \mathbb{Z}_6, \times_6 \rangle$ is a group?

$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$

✓ $[0] \times_6 [1] = [0]$ closure

✓ $([0] \times_6 [1]) \times_6 [3] = [0] = [0] \times_6 ([1] \times_6 [3])$

✓ $[1]$ identity

✓ a^{-1} be the inverse then $[a] \times_6 [a^{-1}] = [1]$

$[a^{-1}] = \frac{[1]}{[a]}$ is not a gp but monoid.

Examples Groups and order of Groups

1) $\langle \{e\}, * \rangle \rightarrow$ Group of order 1

2) $\langle \{e, a\}, * \rangle \rightarrow$ Group of order 2

where a be any elt s.t $a * e = e * a = a$

3) $\langle \{e, a, b\}, * \rangle \rightarrow$ Group of order 3

where $*$ is defined by

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4) $\langle \mathbb{Z}_m, +_m \rangle$ & $\langle \mathbb{Z}_m, \times_m \rangle$ are group of order m.

Permutation groups

The set of all permutations of the elements of a finite set together with a binary operation (For example, right composition) form a group. Such groups are called Permutation groups.

Cyclic groups

A group $\langle G, * \rangle$ is said to be cyclic, if there exists an element $a \in G$ s.t every elt of G can be written as some power of a, that is a^n for some integer 'n'.

Notion:- Let $\langle G, * \rangle$ be a group and $a \in G$.

Define $a^0 = e$, $a^{n+1} = a^n * a$ for $n \in \mathbb{N}$

i.e, $a^n = \underbrace{a * a * \cdots * a}_{n\text{-times}}$

also define $a^{-n} = (a^{-1})^n$ for $n \in \mathbb{N}$ where a^{-1} is the inverse elt of $a \in G$.

Result ① A cyclic group is abelian

Proof:- Let $\langle G, * \rangle$ be a cyclic group.

Let $a \in G$ be a generator of $\langle G, * \rangle$

Let $b, c \in G$. **To prove:** $b * c = c * a$

Given $b = a^m$, $c = a^n$ for some $m, n \in \mathbb{Z}$

Now

$$b * c = a^m * a^n$$

$$= \underbrace{a * a * \cdots * a}_{m \text{ times}} * \underbrace{a * a * \cdots * a}_{n \text{ times}}$$

$$= a^{m+n} = a^{n+m}$$

$$= \underbrace{a * a * \cdots * a}_{n \text{ times}} * \underbrace{a * a \cdots * a}_{m \text{ times}}$$

$$= a^n * a^m$$

$$= c * b$$

Hence $\langle G, * \rangle$ is a commutative (or) abelian group.

Result ② If 'a' is a generator of a cyclic group $\langle G, * \rangle$, then a^{-1} is also a generator of $\langle G, * \rangle$.

Proof:- Let $b \in G$. Then $b = a^m$ for some $m \in \mathbb{Z}$.

Now, $b = a^{-(-m)} = (a^{-1})^{(-m)}$ Since $(a^{-1})^n = a^{-n}$

$= (a^{-1})^{(-m)}$ for some $-m \in \mathbb{Z}$

Hence (a^{-1}) is also a generator for $\langle G, * \rangle$.

Examples for cyclic groups

(i) Let $\langle G, \times \rangle$ where $G = \{1, -1, i, -i\}$ is a gp with usual multiplication ($\times$). Now $i^0 = 1 \in G$, $i^1 = i$, $i^2 = -1$, $i^3 = -i \in G$

Hence $\langle G, \times \rangle$ is a cyclic gp with the generator 'i'.

(ii) $\langle \mathbb{Z}_6, +_6 \rangle$ is a cyclic gp with $[1]$ & $[5]$ are generators.

Remark:

A cyclic gp is said to be a gp generated by 'a', or 'a' is a generator of the gp G, if $\exists\, a \in G$ s.t every elt of G can be expressed as a^n for some integer $n \in \mathbb{Z}$.

Order of the element in a group

Let $\langle G, * \rangle$ be a group and $a \in G$ with identity $e \in G$. The least positive integer 'm' for which $a^m = e$ is called the order of the elt $a \in G$ and denoted by $O(a)$.

If no such integer exists, then 'a' is of infinity order.

Example: $\langle G = \{1, -1, i, -i\}, \times \rangle$ – cyclic gp.

Then $O(1) = 0$, $O(i) = 4$, $O(-1) = 2$, $O(-i) = 3$.

Theorem Let $\langle G, * \rangle$ be a finite cyclic group generated by an elt $a \in G$. If G is of order n, that is $|G| = n$, then $a^n = e$, so that $G = \{a, a^2, a^3, \ldots, a^n = e\}$. Furthermore, n is the least positive integer for which $a^n = e$.

Proof:- I step:

Let us assume that for some +ve integer $m < n$, $a^m = e$.

Since G is a cyclic group, any elt of G can be written as a^K, for some $K \in \mathbb{I}(\mathbb{Z})$

By Euclid's algorithm,

we can write $K = mq + r$, where 'q' is some integer and $0 \le r < m$.

This means $a^K = a^{mq+r} = a^{mq} * a^r$

$$= (a^m)^q * a^r = e^q * a^r = e * a^r$$

$$a^K = a^r,$$

So that every elt can be expressed as a^r for some $0 \le r < m$,

$\Rightarrow$ G has at least 'm' distinct elts

$\Rightarrow |G| \le m < n$

$\Rightarrow \Leftarrow$ which is a contradiction.

Hence, $a^m = e$ for $m < n$ is not possible:

Hence 'n' is the least +ve integer s.t $a^n = e$:

Now to show that elts $\S$ G s.t $a, a^2, \ldots, a^n$ are all distinct, where $a^n = e$.

Suppose not, $a^i = a^j$ for $i < j \leq n$ $(a^{-j} = a^{-i}$ and $j - i < n)$

$\Rightarrow a^j * a^{-i} = e$

$\Rightarrow a^{j-i} = e \Rightarrow j - i \geq n.$

$\Rightarrow\Leftarrow$

which is a contradiction.

Subgroups and Homomorphisms

Subgroups Let $\langle G, * \rangle$ be a group and $S \subseteq G$ s.t it satisfies the following conditions

(i) $e \in S$ where e is the identity elt $\S$ $\langle G, * \rangle$.

(ii) for any $a \in S$, $a^{-1} \in S$.

(iii) For any $a, b \in S$, $a * b \in S$.

Then $\langle S, * \rangle$ is called Subgroup $\S$ $\langle G, * \rangle$.

Examples:-

① Trivial Subgroups.

$\langle \{e\}, * \rangle$ and $\langle G, * \rangle$ are trivial Subgps $\S$ $\langle G, * \rangle$.

② Proper Subgroups.

The Subgroups other than trivial subgroups are called proper Subgroups.

③ $\langle \overset{\text{even}}{E}, + \rangle$ is a Subgroup $\S$ $\langle \mathbb{Z}, + \rangle$

$\langle \overset{\text{odd}}{O}, + \rangle$ is not a Subgp $\S$ $\langle \mathbb{Z}, + \rangle$.

④ $\langle G' = \{1, -1\}, \times \rangle$ is a Subgp $\S$ $\langle G = \{1, -1, i, -i\}, \times \rangle$.

Theorem A subset $S \neq \phi$ of G is a subgroup of $\langle G, * \rangle$ if and only if for any pair of elts $a, b \in S$, $a * b^{-1} \in S$.

Proof:-

Assume that S is a subgroup, it is clear that if $a, b \in S$, then $b^{-1} \in S$ and $a * b^{-1} \in S$.

To prove the converse, let us assume that $a, b \in S$ and $a * b^{-1} \in S$ for any $a, b \in S$.

To prove S is a subgroup.

Let $a, b \in S$.

ie; To prove $e \in S$, $a * b \in S$ and $a^{-1} \in S$.

Since, $a * b^{-1} \in S \Rightarrow a * b^{-1} = a * a^{-1} = e$

Take $b = a$ $\Rightarrow a * b^{-1} = e \in S$

$\Rightarrow b^{-1} = a^{-1}$

Now, $a \in S$ & $e \in S \Rightarrow e * a^{-1} \in S \Rightarrow a^{-1} \in S$.

Now $b \in S$, $e \in S \Rightarrow e * b^{-1} \in S \Rightarrow b^{-1} \in S$.

Now $a \in S$ and $b^{-1} \in S$

$\Rightarrow a * (b^{-1})^{-1} \in S \Rightarrow a * b \in S$

Hence $\langle S, * \rangle$ is a subgp of $\langle G, * \rangle$.

Group Homomorphism

Definition. Let $\langle G, * \rangle$ and $\langle H, \Delta \rangle$ be two groups. A mapping $g : G \to H$ is called a gp homomorphism from $\langle G, * \rangle$ to $\langle H, \Delta \rangle$, If for any $a, b \in G$,

(i) $g(a * b) = g(a) \Delta g(b)$

(ii) $g(e_G) = e_H$

(iii) $g(a^{-1}) = [g(a)]^{-1}$.

Definitions A group homomorphism 'g' is called a

(a) group monomorphism, If 'g' is 1-1.

(b) gp epimorphism, if 'g' is onto and

(c) gp isomorphism, if 'g' is both 1-1 & onto.

Isomorphic groups: $\cong$

If there is a gp isomorphism from a gp $\langle G, * \rangle$ to a groups $\langle H, \Delta \rangle$, then $\langle G, * \rangle$ is isomorphic to $\langle H, \Delta \rangle$.

ie; $\langle G, * \rangle \cong \langle H, \Delta \rangle$.

Endomorphism

A group homomorphism from a groups $\langle G, * \rangle$ to $\langle G, * \rangle$ is called an endomorphism.

Automorphism

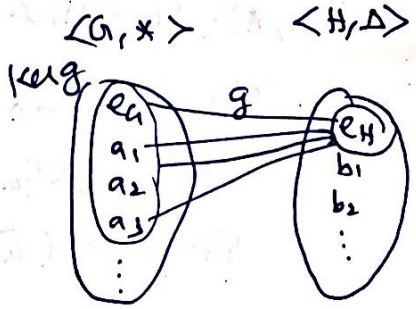
A group isomorphism from a gp $\langle G, * \rangle$ to a same group $\langle G, * \rangle$ is called an automorphism.

Kernel of a Homomorphism

Let 'g' be a gp homomorphism from $\langle G, * \rangle$ to $\langle H, \Delta \rangle$. The set of elements of G which are mapped into e_H (the identity of H) is called the kernel of the homomorphism 'g' and denoted by Ker(g).

i.e. $\text{Ker}(g) = \{ a \in G : g(a) = e_H \}$

Note: $\text{Ker}(g) \subseteq \langle G, * \rangle$.



Example Let $g: \langle \mathbb{Z}, + \rangle \longrightarrow \langle \mathbb{Z}, + \rangle$ defined by

$$g(a) = a \quad \forall\ a \in \mathbb{Z}$$

↳ identity fn.

Then * 'g' is a gp homo.

* 'g' is a gp mono, gp epi, gp isomorphism, endo & automorphism.

Now, $\ker(g) = \{ a \in \mathbb{Z} : g(a) = 0 \} = \{0\}$

↳ $\langle \{0\}, + \rangle$ is a subgp of $\langle \mathbb{Z}, + \rangle$.

Theorem The kernal of a homomorphism g from a group $\langle G, * \rangle$ to $\langle H, \Delta \rangle$ is a subgroup of $\langle G, * \rangle$.

Proof:- e_G, e_H are identity elts of G & H respectively.

(1) To prove: $e_G \in \langle \ker(g), * \rangle$

Since $g(e_G) = e_H \Rightarrow e_G \in \ker(g)$.

(2) To prove: For $a \in \ker g$, $a^{-1} \in \ker g$.

Since $a \in \ker g \Rightarrow g(a) = e_H$

Now, $g(a^{-1}) = [g(a)]^{-1} = (e_H)^{-1} = e_H$

$\Rightarrow g(a^{-1}) = e_H \Rightarrow a^{-1} \in \ker g$.

(3) To prove: For $a, b \in \ker g$, $a * b \in \ker g$.

Since, $a, b \in \ker g \Rightarrow g(a) = e_H$ & $g(b) = e_H$.

Now $g(a * b) = g(a) \Delta g(b) = e_H \Delta e_H = e_H$

$\Rightarrow a * b \in \ker g$

$\therefore$ $\ker g$ is a subgp of $\langle G, * \rangle$. P.T.O.

Cosets and Lagrange's Theorem

Cosets Let $\langle H, * \rangle$ be a subgroup of $\langle G, * \rangle$. For any $a \in G$, the set aH defined by

$$aH = \{ a * h \mid h \in H \}$$ is called the left coset of H in G determined by the elt $a \in G$. The elt a is called the representative elt of the left coset aH.

Example

① Let $\langle G = \mathbb{Z}_4, +_4 \rangle$ be a gp s.t and $\langle H = \{[0], [2]\}, * \rangle$ is a subgp of $\langle \mathbb{Z}_4, +_4 \rangle$.

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Then the distinct left cosets are

$\{[1], [3]\}$ and $\{[0], [2]\}$.

Now $aH = \{ a * h \; ; h \in H \}$ where $a \in G$.

If $a = [0]$, then

$$[0]H = \{ [0] +_4 [0], [0] +_4 [2] \}$$

$$[0]H = \{ [0], [2] \} = H.$$

If $a = [1]$, then $[1]H = \{ [1] +_4 [0], [1] +_4 [2] \}$

$$= \{ [1], [3] \}$$

If $a = [2]$, then $[2]H = \{ [2] +_4 [0], [2] +_4 [2] \} = \{ [2], [0] \}$

$$= [0]H = H.$$

If $a = [3]$, then $[3]H = \{ [3] +_4 [0], [3] +_4 [2] \} = \{ [3], [1] \}$

$$= [1]H.$$

② Ex Find the left cosets. Consider $(\mathbb{Z}_{12}, \oplus)$. Ad $H = \{0, 4, 8\}$ is a subgroup.

Lagrange's Theorem

The order of a subgroup of a finite group divides the order of the group.

Proof:- Let $\langle G, * \rangle$ be a finite group of order 'n'.

That is $|G| = n$,

and let $\langle H, * \rangle$ be a subgp of $\langle G, * \rangle$ and $|H| = m \leq n$.

To prove: 'm' divides 'n'. ie, n/m = an integer.

Property: Every left coset of H in G determined by any elt of G must have the same number of elt as the number of elts in H.

Hence, every left coset of H in G has exactly 'm' elements, and the left cosets partition the gp G. (Union of all the left cosets of H is G)

$\Rightarrow$ The number of left cosets of H in G must to n/m, and it is an integer.

$\therefore n = rm$

$\Rightarrow$ 'm' divides 'n'.

$\Rightarrow$ The order of a subgp of a finite gp divides the order of the group.

Corollary: ①

The order of any elt of a finite gp is a divisor of the order of the group.

Proof: Let $|G| = n$. Let $a \in G$, $a^m = e$ $o(a) = m$

order of a is the same as the order of the cyclic subgp $\langle a \rangle$. cyclic $\langle a \rangle$ is a subgp.

Proof:- ② $\langle G, * \rangle$ is a finite group of order 'n', then $a^n = e$ for any elt $a \in G$.

③ Every group of prime order is cyclic.

Let $|G| = p$ (prime)

Let $a \in G$ & $a \neq e$. $o(a)$ divides p.

$\therefore o(a)$ is 1 or p.

$\because a \neq e \therefore o(a) = p$ $G = \langle a \rangle$. Here G is cyclic.

Normal Subgroup:-

A Subgroup $\langle H, * \rangle$ of $\langle G, * \rangle$ is called a normal subgroup if for any $a \in G$, $aH = Ha$ (ie, the left & right coset of H in G generated by a are the same) or if $a^{-1} * h * a \in H$ for all $a \in G$, $h \in H$.

Example:-

Let $\langle \mathbb{Z}, + \rangle$ be the gp of integers and m be any the integer.

Then the set of multiples of 'm' forms a subgp which may denote by $\langle H_m, + \rangle$.

ie, $H_m = \{ mk : k \in \mathbb{N} \}$

Since $\langle \mathbb{Z}, + \rangle$ is abelian, $\langle H_m, + \rangle$ is a normal subgp.

Theorem Let $\langle G, * \rangle$ and $\langle H, \Delta \rangle$ be groups and $g: G \to H$ be a homomorphism. Then the kernel of g is a normal subgp.

Proof:- WKT $\langle \ker g, * \rangle$ is a subgroup of $\langle G, * \rangle$

$$K = \ker g = \{ a \mid a \in G \text{ and } g(a) = e_H \}.$$

Let $a \in G$ and $k \in K \Rightarrow g(k) = e_H$.

To prove $a^{-1} * k * a \in K$ ie, $g(a^{-1} * k * a) = e_H$

For $g(a^{-1} * k * a) = g(a^{-1}) \Delta g(k * a)$

$= (g(a))^{-1} \Delta (g(k) \Delta g(a))$

$= (g(a))^{-1} \Delta (e_H \Delta g(a))$

$= (g(a))^{-1} \Delta g(a)$

$= e_H$

$\therefore$ $\ker g$ is a normal subgp of $\langle G, * \rangle$.

Quotient Group (Factor group)

Let N be a normal subgroup of G. Then the group $\frac{G}{N}$ is called the Quotient gp of G modulo N.

Theorem (Fundamental theorem of homomorphism gp)

Let $f : \langle G, * \rangle \longrightarrow \langle H, \Delta \rangle$ be an epimorphism. Let K be the kernel of f. Then $\frac{G}{K} \cong H$.

Proof:- Define $\phi : \frac{G}{K} \longrightarrow H$ by $\phi(Ka) = f(a)$.

(i) ϕ is well defined.

Let $Kb = Ka$. Then $b \in Ka$

Hence $b = ka$ where $k \in K$

Now $f(b) = f(ka) = f(k) f(a) = e_H f(a) = f(a)$

$\therefore \phi(Kb) = f(b) = f(a) = \phi(Ka)$.

(ii) ϕ is 1-1.

For $\phi(Ka) = \phi(Kb) \Rightarrow f(a) = f(b)$

$\Rightarrow f(a) f(b)^{-1} = e_H$

$\Rightarrow f(ab^{-1}) = e_H$

$\Rightarrow ab^{-1} \in K$

$\Rightarrow a \in Kb \Rightarrow Ka = Kb$.

(iii) ϕ is onto. Let $h \in H$. Since f is onto, $\exists\, a \in G$ s.t $f(a) = h$. $\therefore \phi(Ka) = f(a) = h$.

(iv) ϕ is homo

$\phi(KaKb) = \phi(Kab) = f(ab) = f(a) f(b)$

$= \phi(Ka)\, \phi(Kb)$.

$\therefore G/K \cong H$.

Coding Theory

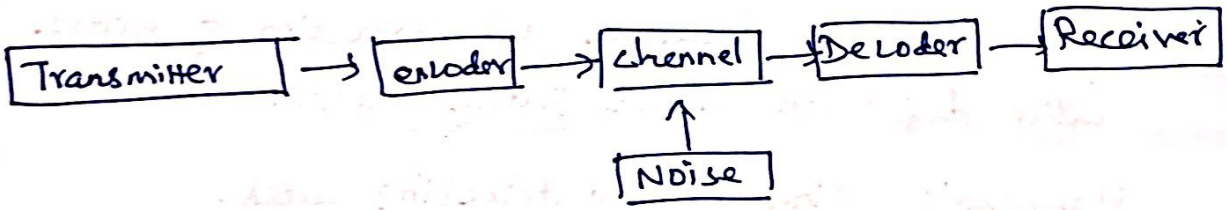
Encoders and Decoders

An encoder is a device which transforms the incoming messages in such a way that the presence of noise in the transformed messages is detectable.

A decoder is a device which transforms the encoded message into their original form that can be understood by the receiver.

By using a suitable encoder and decoder, it may be possible to detect the distortions in the messages due to noise in the channel and to correct them.

The model of a typical data communication system with noise is given as follows



Group code

Definition If $B=\{0,1\}$ then $B^n=\{x_1,x_2,\dots x_n \mid x_i \in B, i=1,2,\dots n\}$ is a group under the binary operation of addition modulo 2, denoted by $\oplus$. This group is $(B^n,\oplus)$ called a group code.

Let us prove $(B^n,\oplus)$ is a group.

If $x_1,x_2,\dots x_n \equiv (x_1,x_2,\dots x_n) \in$
$y_1,y_2,\dots y_n \equiv (y_1,y_2,\dots y_n) \in B^n$, then

$$x_1,x_2,\dots x_n \oplus y_1,y_2,\dots y_n = (x_1\oplus y_1,\ x_2\oplus y_2,\dots x_n\oplus y_n) \in B^n.$$

Since $x_i \oplus_2 y_i = 1$ or 0, as

$$0 \oplus_2 0 = 0, \quad 0 \oplus_2 1 = 1, \quad 1 \oplus_2 0 = 1 \text{ & } 1 \oplus_2 1 = 0$$

clearly $(0,0,\ldots 0)$ is the identity elt of B^n. Also the inverse of $x_1, x_2, \ldots x_n$ is itself.

Hence $(B^n, \oplus_2)$ is a group - it is abelian.

Hamming codes

Hamming codes obtained by introducing additional digits called parity digits to the digits in the original message are called Hamming codes.

In a message, that is 'n' digits; m digits $(m < n)$ are used to represent the information part of the message, and the remaining $k = n-m$ digits are used for detection and correction of errors. The latter digits are called parity checks.

Hamming's single-error detecting codes:

The information contents of the message is contained in the first 'n-1' digits of a code and the last digit position is made either 0 or 1. So as to make the entire message contain an even number of 1's. Such an encoding procedure is called an even parity check. Alternatively an odd parity check can be used by making the entire message contain an odd number of 1's.

Example: The messages are 00, 01, 10, 11.

If a single even-parity digit is added, then the message are encoded as 000, 011, 101, 110.

If a single odd-parity digit is added, then the message are encoded as 001, 010, 100, 111.

Note:- Hamming developed an error-correcting method, based on these parity checks, that enabled the detection & the positions of erroneous (or) redundant digits.

Definitions

1. The number of 1's in the binary string $x \in B^n$ is called the weight of x and is denoted by $|x|$.

2. If x and y represent the binary strings $x_1, x_2, \cdots x_n$ and $y_1, y_2 \cdots y_n$ the number of positions in the strings for which $x_i \neq y_i$ is called the Hamming distance between x and y and denoted by $H(x,y)$.

Obviously $H(x,y)$ = weight of $x \oplus y$

$$= \sum_{i=1}^{n} (x_i \oplus_2 y_i)$$

For example, if $x = 11010$, $y = 10101$ then

$$H(x,y) = |x \oplus y| = |01111| = 4.$$

3. The minimum distance of a code (a set of encoded words) is the minimum of the Hamming distances b/w all pairs of encoded words in that code.

For eg, if $x = 10110$, $y = 11110$ & $z = 10011$, then $H(x,y) = 1$, $H(y,z) = 3$ & $H(z,x) = 2$ and so the minimum distance b/w these code words $= 1$.

Theorem 1. A code can detect at the most k errors if and only if the minimum distance between any two code words is at least (k+1).

2. A code can correct a set of at the most k errors if and only if the minimum distance between any two code words is at least (2k+1).

Group codes

An (m,n) encoding function is one-to-one function $e: B^m \to B^n$ (where $m<n$). If $b \in B^m$ then $e(b)$ is called the code word representing b.

Parity check code

A function $e: B^m \to B^{m+1}$ defined by

$$e(b_1, b_2, \ldots, b_m) = b_1 b_2 \ldots b_m b_{m+1}$$

where $b_{m+1} = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd} \end{cases}$

is an encoding function. This function is called parity (m, m+1) check code.

Example:- The code word representing 101 under (3,4) parity check is $B^3 \to B^4$

$e(101) = 1010$ (Since $|101|$ is even).

$e(100) = 1001$ (Since $|100|$ is odd).

Problems

① Show that the (2,5) encoding function defined by $e(00) = 00000$, $e(01) = 01110$, $e(10) = 10101$ $e(11) = 11011$ is a group code.

Soln:- Denote $e(00)$, $e(01)$, $e(10)$, $e(11)$ by x^0, x^1, x^2, x^3.

The set of these code words is closed under $+_2$ as can be seen from the table

$+_2$	x^0	x^1	x^2	x^3
x^0	x^0	x^1	x^2	x^3
x^1	x^1	x^0	x^3	x^2
x^2	x^2	x^3	x^0	x^1
x^3	x^3	x^2	x^1	x^0

As x^0 is identity & Inverse of any elt is itself, the code words form a subgp of B^5.

$\therefore$ e is a group code.

Decoding function

An (n,m) decoding function d associated with an encoding function $e: B^m \longrightarrow B^n$ $(n>m)$ is an onto function $d: B^n \longrightarrow B^m$ s.t

$doe = I_{B^m}$ where I is the identity function on B^m.

Using matrix

Note:- 1. When $m, n \in \mathbb{Z}^+$ and $m < n$, the encoding fn $e: B^m \to B^n$ is given by a $m \times n$ matrix G over B. This matrix G is called the generator matrix for the code and is of the form $[I_m | A]$ where I_m is the $m \times m$ unit matrix and A is an $m \times (n-m)$ matrix to be chosen suitably. And If w is a message $\in B^m$, $e(w) = wG$.

2. Parity check matrix was assumed as an $(n-m) \times m$ matrix $H = [A^T | I_{n-m}]$

Problem ① Find the code words generated by the encoding function $e: B^2 \to B^5$ with respect to the parity check matrix $H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Determine the (2,5) group code function.

$m = 2 \quad n = 5$

Soln:- Given $H = \left[\begin{array}{cc|ccc} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right] = [A^T | I_{n-m}]$

$(n-m) \times m$ i.e. 3×2; 3×3

Hence the generator matrix G is given by

$$G = [I_m | A] = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Now $B^2 = \{[0\,0]\ [0\,1]\ [1\,0]\ [1\,1]\}$ & $e(w) = wG$

$$e(00) = (00)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0\,0\,0\,0\,0)$$

$$e(01) = (01)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0\,1\,0\,1\,1)$$

$$e(10) = (10)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1\,0\,0\,1\,1)$$

$$e(11) = (11)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (1\,1\,0\,0\,0)$$

These are code words generated by H.

(2) Let $m=2$, $n=5$ and $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Determine the group code $e_H : B^2 \to B^5$.

Soln:-

$$B^2 = \{(00)\ (01)\ (10)\ (11)\}$$

$$H = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right] = [A^T \mid I_3]$$

$$\therefore G = \left[\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{array}\right] = [I_m \mid A]$$

$e(w) = wG$

$e(00) = (00)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (0\ 0\ 0\ 0\ 0)$

$e(10) = (10)G = (0\ 1\ 0\ 1\ 1)$

$e(01) = (01)G = (1\ 0\ 1\ 1\ 0)$

$e(11) = (11)G = (1\ 1\ 1\ 0\ 1)$

(3) Determine the group code $(3,6)$ using the parity check matrix $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ $e: B^3 \to B^6$

$m=3$, $n=6$

H.W

Soln:-

$$H = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

$$B^3 = \{(000)\ (001)\ (010)\ (100)\ (011)\ (101)\ (110)\ (111)\}$$

$$G = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

$e(w) = wG$

$e(000) = wG = (000000)$

$e(001) = wG = (001111)$

④ $e: B^3 \to B^6$, $H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Hw

Example:-

1. d be the $(4,3)$ decoding function. Determine $d(y)$ for the word $y \in B^4$. (a) $y = 0110$ (b) $y = 1011$.

Soln:-

$e: B^m \to B^{m+1}$, $e(b^m) = b^{m+1}$

$d: B^{m+1} \to B^m$

✓ $e: B^3 \to B^4$

✓ M_2.

✓ $d: B^4 \to B^3$

By defn $d(b) = b_1 b_2 b_3$ where $b = b_1 b_2 b_3 b_4$

So $d(y) = d(0110)$ where $y = 0110 \in B^4$

$\therefore d(y) = 011$.

Hw $d(1011) = 101$.

⑤ Example 5.7 in J. Veerarajan Page No 304

⑥ Part B, Pblm 29, 30, 31, 32. (Exercise).