

Group Theory

In this chapter we introduce the concept of binary operation and study few algebraic structures like, semi group, group and few of its properties.

Let A be a non empty set. A binary operation $*$ over A is a function $* : A \times A \rightarrow A$.

That is a binary operation $*$ on a non empty set A , associates each pair (a, b) of elements of A to a unique element, say $c \in A$. This is denoted by $a * b = c$.

If $*$ is a binary operation on the set A , then we say that the set A is closed under the operation $*$.

examples:

1. The set N of natural numbers is closed under addition. Whereas usual subtraction is not a binary operation on N .
2. On the set \mathbb{Q} of all rational numbers, the operation $*$ defined by $a * b = \frac{ab}{2}$, $\forall a, b \in \mathbb{Q}$ is a binary operation on \mathbb{Q} .
3. The usual matrix multiplication is a binary operation on the set of all $n \times n$ matrices over the set of real numbers.
4. Let n be a fixed positive integer, a and b be any two integers. Define $a \text{ } t_n \text{ } b = r$, where r is the least positive non negative remainder obtained when the usual sum $a + b$ is divided by n . Clearly t_n is a binary operation on $\mathbb{Z}_{\geq 0} \cup \{1, 2, \dots, n-1\}$.

Binary algebra:

A non empty set A together with a binary operation $*$ defined on it, is called a binary algebra or groupoid and it is denoted by $\langle A, * \rangle$.

example:

The set E of all even numbers, is closed under usual addition and also under usual multiplication. Thus $\langle E, + \rangle$ and $\langle E, * \rangle$ are binary algebra. Whereas, the set of all odd numbers, do not form a binary algebra under usual addition since the sum of two odd numbers is not odd.

Semi group:

A non empty set S , together with the binary operation $*$ is called a semi group if $*$ is associative in S . i.e $x, y, z \in S$, $x*(y*z) = (x*y)*z$.

Monoid

A non empty set S , together with the binary operation $*$ is called a monoid if $*$ is associative in S and if there exists a unique element e in S such that for every element x in S , $x*e = e*x = x$. e is called the identity element.

examples

1. The set \mathbb{Z} of all integers together with usual addition is a semi group. In fact it is also a monoid, with 0 as the identity element.
2. The set \mathbb{N} of all natural numbers with usual addition is a semi group. But it is not a monoid, as 0, the identity element does not belong to \mathbb{N} .

Groups

A binary algebra $\langle G, * \rangle$ is said to be a group, if the following axioms hold.

(i) Associativity:

$$\forall a, b, c \in G, a * (b * c) = (a * b) * c$$

(ii) Existence of identity:

\exists an element $e \in G$, such that $\forall a \in G$,
 $a * e = a = e * a$. The element e is called an identity element of G .

(iii) Existence of inverse

$\forall a \in G$, \exists an element $b \in G$ such that
 $a * b = e = b * a$. The element b is called an inverse of the element of a in G .

Note: A group $\langle G, * \rangle$ is a monoid in which every element has an inverse in G w.r.t the binary operation $*$.

A group $\langle G, * \rangle$ is said to be an abelian or a commutative group if the binary composition is commutative. i.e, $\forall a, b \in G, a * b = b * a$

A group $\langle G, * \rangle$ is said to be a finite group if the set G is finite, otherwise it is called an infinite group.

The number of elements in the group $\langle G, * \rangle$ is called the order of the group and it is denoted by $O(G)$.

examples:

1. $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{C}, + \rangle$ are abelian groups.
2. If \mathbb{R}^* , \mathbb{Q}^* and \mathbb{C}^* denote respectively the sets of non zero real numbers, non zero rational numbers and non zero complex numbers, then $\langle \mathbb{R}^*, \cdot \rangle$, $\langle \mathbb{Q}^*, \cdot \rangle$ and $\langle \mathbb{C}^*, \cdot \rangle$ are abelian groups.
3. The set $G = \{na \mid a \in \mathbb{Z}\}$ is an abelian group under usual addition, where n is a non-zero integer.
4. The set $\{1, \omega, \omega^2\}$ of cube roots of unity is abelian group under usual multiplication.
5. The set $G = \{1, -1, i, -i\}$ of fourth roots of unity is an abelian group under usual multiplication.
6. The set of even integers is an abelian group under usual addition.
7. The set M of all $n \times n$ non singular matrices of real numbers is a non-abelian group under usual matrix multiplication.
8. The set M of all $m \times n$ matrices over the set of real numbers is an abelian group under usual matrix addition.
9. The set G of all unimodular complex numbers is a group under usual multiplication of complex numbers.
10. The set $\{\pm 1, \pm i, \pm j, \pm k\}$ is a non-abelian group under the quaternion multiplication, defined by $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$, $ik = -j$.
The set $\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is called a quaternion group.

examples

1. Show that the set of all integers is a group under addition.

Sol Let $a, b, c \in \mathbb{Z}$ $a+b \in \mathbb{Z}$.

Hence $\langle \mathbb{Z}, + \rangle$ is closed under addition.

$$\text{(i) } \forall a, b, c \in \mathbb{Z} \quad (a+b)+c = a+(b+c)$$

Hence $\langle \mathbb{Z}, + \rangle$ is associative

$$\text{(ii) } \forall a \in \mathbb{Z}, \quad a+0 = a = 0+a$$

Hence 0 is the identity element of $\langle \mathbb{Z}, + \rangle$

$$\text{(iii) } \forall a \in \mathbb{Z}, \quad a+(-a) = 0 = (-a)+a$$

Hence $-a$ is the inverse element of a in $\langle \mathbb{Z}, + \rangle$

Therefore $\langle \mathbb{Z}, + \rangle$ is a group.

2. Show that the set of all non-zero complex numbers (\mathbb{C}^*) is a group under multiplication.

Sol i) $\forall a_1+ib_1, a_2+ib_2 \in \mathbb{C}^*, \quad (a_1+ib_1) * (a_2+ib_2)$

$$(a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1) \in \mathbb{C}^*$$

Hence $\langle \mathbb{C}^*, \cdot \rangle$ is closed under multiplication.

$$\text{(ii) } \forall (a_1+ib_1), (a_2+ib_2), (a_3+ib_3) \in \mathbb{C}^*$$

$$\begin{aligned} (a_1+ib_1) \cdot [(a_2+ib_2) \cdot (a_3+ib_3)] &= (a_1+ib_1) \cdot (a_2a_3 - b_2b_3 + i(b_2a_3 + a_2b_3)) \\ &= a_1a_2a_3 - a_1b_2b_3 - b_1b_2a_3 - b_1a_2b_3 \\ &\quad + i(a_1b_2a_3 + a_1a_2b_3 + b_1a_2a_3 - b_1b_2b_3) \\ &= ((a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)) \cdot (a_3+ib_3) \\ &= [(a_1+ib_1) \cdot (a_2+ib_2)] \cdot (a_3+ib_3) \end{aligned}$$

Hence $\langle \mathbb{C}^*, \cdot \rangle$ is associative

$$\text{(iii) } \forall a_1+ib_1 \in \mathbb{C}^*, \quad (a_1+ib_1) \cdot 1 = a_1+ib_1 = 1 \cdot (a_1+ib_1)$$

Hence 1 is the identity element of $\langle \mathbb{C}^*, \cdot \rangle$

$$\text{(iv) } \forall a_1+ib_1 \in \mathbb{C}^*, \quad (a_1+ib_1) \cdot \frac{1}{(a_1+ib_1)} = 1 = \frac{1}{(a_1+ib_1)} \cdot (a_1+ib_1)$$

Here $\frac{a_1-i b_1}{a_1^2+b_1^2} = a_1+ib_1$ is the inverse of (a_1+ib_1) in $\langle \mathbb{C}^*, \cdot \rangle$

Therefore $\langle \mathbb{C}^*, \cdot \rangle$ is a group

3 Show that $\langle N, + \rangle$ where N is the set of natural numbers is a semigroup and not a group.

(i) $\forall a, b, c \in N, (a+b)+c = a+(b+c)$.

Hence $\langle N, + \rangle$ is associative.

Therefore $\langle N, + \rangle$ is a semigroup.

(ii) $\forall a \in N, a+0=a=0+a$,

but $0 \notin N$, Hence identity element does not exist for $\langle N, + \rangle$.

Therefore $\langle N, + \rangle$ is not a group.

4 Show that $\langle Z^+, \times \rangle$ where Z^+ is the set of positive integers, is not a group.

$Z^+ = \{1, 2, 3, \dots\}$

(i) $\forall a, b, c \in Z^+, (a \times b) \times c = a \times (b \times c)$.

Hence $\langle Z^+, \times \rangle$ is associative.

(ii) $\forall a \in Z^+, a \times 1 = a = 1 \times a$

Hence 1 is the identity element of $\langle Z^+, \times \rangle$.

(iii) $\forall a \in Z^+, a \times \frac{1}{a} = 1 = \frac{1}{a} \times a$,

but $\frac{1}{a} \notin Z^+$, Hence inverse element does not exist for $\langle Z^+, \times \rangle$.

Therefore $\langle Z^+, \times \rangle$ is not a group.

5. On the set \mathbb{Q}^* of positive rational numbers the binary operation is defined by $a * b = \frac{ab}{2}$. Show that $\langle \mathbb{Q}^*, *\rangle$ is an abelian group.

Sol: (i) $\forall a, b, c \in \mathbb{Q}^*$, $(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{abc}{4} = a * \left(\frac{bc}{2}\right)$
 $= a * (b * c)$

Hence $\langle \mathbb{Q}^*, *\rangle$ is associative.

(ii) $\forall a \in \mathbb{Q}^*$, $a * 2a = a = 2 * a$

Hence 2 is the identity element of $\langle \mathbb{Q}^*, *\rangle$.

(iii) $\forall a \in \mathbb{Q}^*$, $a * \frac{4}{a} = 2 = \frac{4}{a} * a$

Hence $\frac{4}{a}$ is the inverse element of a in $\langle \mathbb{Q}^*, *\rangle$.

(iv) $\forall a, b \in \mathbb{Q}^*$, $a * b = \frac{ab}{2} = b * a$

Hence $\langle \mathbb{Q}^*, *\rangle$ is commutative.

Hence $\langle \mathbb{Q}^*, *\rangle$ is an abelian group.

6. On the set \mathbb{R} of real numbers * is defined by $a * b = a + a^2 b$, $\forall a, b \in \mathbb{R}$. Show that $\langle \mathbb{R}, *\rangle$ is not a group.

Sol: $\forall a, b, c \in \mathbb{R}$, $(a * b) * c = (a + a^2 b) * c$
 $= a + a^2 b + (a + a^2 b)^2 c$
 $= a + a^2 b + a^2 c + 2a^3 bc + a^4 b^2 c$

and $a * (b * c) = a * (b + b^2 c)$

$$= a + a^2 (b + b^2 c)$$

$$= a + a^2 b + a^2 b^2 c$$

$\therefore (a * b) * c \neq a * (b * c)$, $\langle \mathbb{R}, *\rangle$ is not associative.
Hence $\langle \mathbb{R}, *\rangle$ is not a group.

7. Verify whether $\langle \mathbb{R}, + \rangle$ with $a + b = a - b$ a group.

Sol: $\forall a, b, c \in \mathbb{R}$, $(a + b) + c = (a - b) + c = a - b - c$

$$\text{and } a + (b + c) = a + (b - c) = a - b + c$$

Since $(a + b) + c \neq a + (b + c)$, $\langle \mathbb{R}, + \rangle$ is not associative.
Hence $\langle \mathbb{R}, + \rangle$ is not a group.

Exercise

1. Show that the set of all $m \times n$ matrices over real numbers is a group under matrix addition.
2. Show that $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{R}, a \neq 0\}$ is a group under multiplication.
3. Show that the set $G = \{A, B, C, D\}$ where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ is a group under matrix multiplication.
4. Show that the set of all non zero real numbers is a group under multiplication.
5. Show that the set $G = \{2n \mid n \in \mathbb{Z}\}$ is an abelian group under addition.
6. In the set G of rational numbers $\neq 1$, define \ast by $a \ast b = a + b - ab$. Show that (G, \ast) is an abelian group.
7. Show that $\langle \mathbb{Z}, \ast \rangle$ where \mathbb{Z} is the set of integers and $a \ast b = a + b - 1$ $\forall a, b \in \mathbb{Z}$ is a group.
8. Show that the following are not groups. Give reasons.
 - i) $\langle \mathbb{Z}, \ast \rangle$ with $a \ast b = ab$.
 - ii) $\langle \mathbb{Q}^*, \ast \rangle$ with $a \ast b = a^b$, where \mathbb{Q}^* is the set of non zero rational numbers.
 - iii) $\langle \mathbb{Z}^+, + \rangle$ where \mathbb{Z}^+ is the set of positive integers.
 - iv) $\langle \mathbb{R}, \ast \rangle$ where $a \ast b = a + b + a^2 b$

Properties of a Group.

Theorem 1:

The identity element of a group is unique

Proof: Let $\langle G, * \rangle$ be a group.
If possible let e and e' be two identity elements
Since e is an identity element,

$$\text{we have } e * e = e' \text{ and } e * e' = e' \quad \text{--- (1)}$$

Again as e' is an identity element,
we have $e' * e' = e$ and $e' * e = e$ --- (2)

From (1) and (2) it follows $e = e'$
Hence the identity element in a group is unique.

Theorem 2:

The inverse of an element of a group is unique.

Proof: Let e be the identity element and
 a be an element of the group $\langle G, * \rangle$.

Let if possible b and c be two inverses of a in G .

Since b is an inverse of a , we have $a * b = e = b * a$ --- (1)

Again as c is an inverse of a , we have $a * c = e = c * a$ --- (2)

Now, $b = b * e$ [$\because e$ is the identity element]

$$\Rightarrow b = b * (a * c) \quad [\text{from (2)}]$$

$$\Rightarrow b = (b * a) * c \quad [\text{associative law}]$$

$$\Rightarrow b = e * c \quad [\text{from (1)}]$$

$$\Rightarrow b = c \quad [\because e \text{ is the identity element}]$$

Hence the inverse of an element is unique.

Theorem 3:

If a is an element of the group $\langle G, * \rangle$, then
 $(a^{-1})^{-1} = a$.

Theorem 4:

Let $\langle G, * \rangle$ be a group and $a, b \in G$, then

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

Theorem 5:

In a group $\langle G, * \rangle$ for all $a, x, y \in G$.

- (i) $a * x = a * y \Rightarrow x = y$ [left cancellation law]
- (ii) $x * a = y * a \Rightarrow x = y$ [right cancellation law].

Theorem 6:

Given two elements a and b of the group $\langle G, * \rangle$, then there exists unique solution for $a * x = b$ and $y * a = b$.

- Example .
- In the group \mathbb{R}^* of non zero real numbers the binary operation * is defined by $a*b = \frac{ab}{5}$.
 Solve $2*x*5 = 10$ in \mathbb{R}^* .

Soln

$$2*x*5 = 10 \Rightarrow 2*(x*5) = 10$$

$$\Rightarrow 2*\left(\frac{5x}{5}\right) = 10$$

$$\Rightarrow 2*x = 10$$

$$\Rightarrow \frac{2x}{5} = 10$$

$$\Rightarrow x = \underline{\underline{25}}$$
 - In the set G of all rational numbers except -1 , the binary operation * defined by $a*b=a+b+ab$.
 Solve $3*4*x=0$ in \mathbb{R}^* .

Soln

$$3*4*x=0 \Rightarrow (3*4)*x=0$$

$$\Rightarrow (3+4+12)*x=0$$

$$\Rightarrow 19*x=0$$

$$\Rightarrow 19+x+19x=0$$

$$\Rightarrow 20x=-19$$

$$\Rightarrow x = \underline{\underline{-\frac{19}{20}}}$$
 - If every element of a group G is its own inverse, show that G is abelian.

Soln. By data, $\forall a \in G_1, a^{-1} = a$.

Consider $(x+y)^{-1} = y^{-1}*x^{-1}$ [By Theorem 4]

$$\Rightarrow (x+y)^{-1} = y^{-1}*x \quad [\because y^{-1}=y, x^{-1}=x]$$

$$\Rightarrow x+y = y*x \quad [\therefore x+y \in G, (x+y)^{-1}=x+y]$$

Hence G_1 is abelian.

4. If in a group $\langle G, * \rangle$, $a * a = a$ & $a \in G$, show that $a = e$ where e is the identity element.

Sol Given $(a * a) = a$

$$\Rightarrow a^{-1} * (a * a) = a^{-1} * a.$$

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

$$\Rightarrow e * a = e$$

$$\Rightarrow \underline{a = e}$$

5. Show that the groups of order 1, 2 and 3 are abelian.

i) Let G be a group of order 2.

That is G contains only one element say e .

Consider $e * e = e \cancel{= e}$

$$e * e = e * e$$

Therefore G is abelian.

ii) Let G be a group of order 2.

That is G contains two elements one of which acts as the identity element e and another element distinct from e , say a .

$$\text{Let } G = \{e, a\}.$$

The inverse of a is itself (as inverse of e is itself).

Consider $a * e = a$

$$a * e = e * a$$

Therefore G is abelian.

iii) Let G be a group of order 3 and $G = \{e, a, b\}$

(a) If $a^{-1} = a$ and $b^{-1} = b$, i.e., inverse of each element is itself. Hence G is abelian.

(b) If $a^{-1} \neq a$ and $b^{-1} \neq b$, then $a^{-1} = b$ and $b^{-1} = a$

$$\text{Consider } a * b = a * a^{-1} = e = b^{-1} * b = b * a.$$

Therefore G is abelian.

6. If $(G, *)$ is a group of even order ($a * b = ab$), then show that there exists an element $a \in G$, [where $a \neq e$] such that $a^2 = e$ [i.e., $a^{-1} = a$].

Sol: Given G is a group of even order.

Since e is its own inverse, when e is eliminated, then G will have odd number of elements. We know that each element of G has unique inverse, thus there exists an element $a (\neq e) \in G$ s.t $a^{-1} = a$.

$$\text{Now, } a = a^{-1} \Rightarrow a * a = a^{-1} * a \Rightarrow a^2 = e.$$

7 Show that a group $\langle G, * \rangle$ (s.t. $a * b = ab$) is abelian if and only if $(ab)^2 = a^2 b^2$, $\forall a, b \in G$

Sol: Let G be abelian, and we need to prove $(ab)^2 = a^2 b^2$.

$$\begin{aligned} \text{Consider } (ab)^2 &= (ab)(ab) \\ &= a(ba)b \quad (\text{associative law}) \\ &\Rightarrow a(lab)b \quad (\because G \text{ is abelian}) \\ &\Rightarrow a(a)(bb) \quad (\text{associative law}) \\ &\Rightarrow (ab)^2 = a^2 b^2 \end{aligned}$$

Conversely let $(ab)^2 = a^2 b^2$, we need to show that G is abelian.

$$\text{Consider } (ab)^2 = a^2 b^2$$

$$\begin{aligned} &\Rightarrow (ab)(ab) = (aa)(bb) \quad (\text{associative law}) \\ &\Rightarrow a(ba)b = a(ab)b \quad (\text{associative law}) \\ &\Rightarrow (ba)b = (ab)b \quad (\text{left cancellation law}) \\ &\Rightarrow (ba) = (ab) \quad (\text{right cancellation law}) \\ &\Rightarrow G \text{ is abelian.} \end{aligned}$$

Exercise

1. In the group $\langle \mathbb{Q}^+, * \rangle$, where \mathbb{Q}^+ is the set of all positive rationals and $a*b = \frac{ab}{2}$, find the solution of the equations $6*x=3$ and $y*5=7$.
2. In the set of all rational numbers except 1, define $*$ by $a*b = a+b-ab$. Solve the equations $y+3*2=-5$ and $4*y*3=7$.
3. In the set \mathbb{Z} of integers the binary operation $*$ is defined by $a*b = a+b+1$. Solve $4*3+x=2$ and $7*y*(-3)=7$.
4. If $*$ is defined by $a*b = \frac{ab}{7}$ on the set of rational numbers, find the solution of the equations $y^{-1}*2*3=4$ and $4*y*3^{-1}=2$.

Modular Systems

Addition modulo m

Let m be a fixed positive integer and a and b are any two integers, the binary composition called addition modulo m , denoted by t_m is defined as $a +_m b = \text{least non negative remainder obtained by dividing the usual sum } a+b \text{ by } m.$

Ex) under addition modulo 7, $4 +_7 6 = 3$, since the usual sum $4+6=10$ leaves 3 as remainder when divided by 7.

Similarly $4 +_4 5 = 1$, $3 +_2 7 = 0$, $2 +_5 7 = 4$.

Multiplication modulo m

Let m be a fixed positive integer and a and b are any two integers. The binary composition called multiplication modulo m , denoted by x_m is defined as $a \times_m b = \text{least non negative remainder obtained by dividing the usual product } ab \text{ by } m.$

Ex) under multiplication modulo 6, $4 \times_6 6 = 0$, since the usual product $4 \times 6 = 24$ leave 0 as remainder when divided by 6.

Similarly $4 \times_3 5 = 2$, $3 \times_4 7 = 1$, $2 \times_5 7 = 4$.

Example
Form the addition modulo 6 table for the set

$$\{0, 1, 2, 3, 4, 5\}.$$

soln

t_6	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

2. Form the table of multiplication modulo 10 of the set $\{1, 3, 7, 9\}$.

\times_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

3. Show that $\langle \mathbb{Z}_4, +_4 \rangle$, where $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ is an abelian group.

\times_{10}	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

i) Consider $3+_4(2+_4 1) = 3+_4 3 = 2$
 $(3+_4 2) +_4 1 = 1 +_4 1 = 2$
 $\therefore 3 +_4 (2 +_4 1) = (3 +_4 2) +_4 1$
Similarly with any other three elements of \mathbb{Z}_4 ,
 $(a +_4 b) +_4 c = a +_4 (b +_4 c)$.
 $\therefore \langle \mathbb{Z}_4, +_4 \rangle$ is associative.

ii) $\forall a \in \mathbb{Z}_4$, $(a +_4 0) = a = 0 +_4 a$
Hence 0 is the identity element of $\langle \mathbb{Z}_4, +_4 \rangle$.

iii) 0 is the inverse of 0 $\therefore 0 +_4 0 = 0 = 0 +_4 0$
3 is the inverse of 1 $\therefore 1 +_4 3 = 0 = 3 +_4 1$
2 is the inverse of 2 $\therefore 2 +_4 2 = 0 = 2 +_4 2$
1 is the inverse of 3 $\therefore 3 +_4 1 = 0 = 1 +_4 3$

Hence the inverse of each element exists.

iv) Since the table is symmetric about the principle diagonal, $a +_4 b = b +_4 a$, $\forall a, b \in \mathbb{Z}_4$.

Hence $\langle \mathbb{Z}_4, +_4 \rangle$ is commutative.

Therefore $\langle \mathbb{Z}_4, +_4 \rangle$ is an abelian group.

4. Show that $G = \{1, 2, 3, 4\}$ is an abelian group under multiplication modulo 5.

\times_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(i) From the table it follows that G is closed under multiplication modulo 5.

$$(ii) 3 \times_5 (4 \times_5 2) = 3 \times_5 3 = 4$$

$$(3 \times_5 4) \times_5 2 = 2 \times_5 2 = 4$$

$$\therefore 3 \times_5 (4 \times_5 2) = (3 \times_5 4) \times_5 2$$

Similarly with any other three elements of G ,
 $a \times_5 (b \times_5 c) = (a \times_5 b) \times_5 c$. $\therefore \langle G, \times_5 \rangle$ is associative.

$$(iii) \forall a \in G, a \times_5 1 = a = 1 \times_5 a$$

Hence 1 is the identity element of $\langle G, \times_5 \rangle$.

$$(iv) 1 \text{ is the inverse of } 1 \quad \therefore 1 \times_5 1 = 1 = 1 \times_5 1$$

$$3 \text{ is the inverse of } 2 \quad \therefore 2 \times_5 3 = 1 = 3 \times_5 2$$

$$2 \text{ is the inverse of } 3 \quad \therefore 3 \times_5 2 = 1 = 2 \times_5 3$$

$$4 \text{ is the inverse of } 4 \quad \therefore 4 \times_5 4 = 1 = 4 \times_5 4.$$

$$\therefore \text{inverse of each element exists in } \langle G, \times_5 \rangle.$$

(v) Since the table is symmetric about the principal diagonal $a \times_5 b = b \times_5 a \quad \forall a, b \in G$.

Hence $\langle G, \times_5 \rangle$ is commutative.

Therefore $\langle G, \times_5 \rangle$ is an abelian group.

Exercise

1. Write the addition modulo 6 table for the set $\{0, 2, 4\}$
2. Write the multiplication modulo 12 table for the set $\{1, 5, 7, 11\}$
3. Show that $\langle Z_5, +_5 \rangle$, where $Z_5 = \{0, 1, 2, 3, 4\}$ is an abelian group.
4. Show that $\langle G, \times_7 \rangle$, where $G = \{1, 2, 3, 4, 5, 6\}$ is an abelian group.
5. Show that the set $G = \{1, 2, 3\}$ is not a group under \times_4 .

Permutation and Symmetric group of order 3

A one-one, onto mapping of a finite set onto itself is called permutation and the number of elements in the set is called the degree of permutation.

Consider a set $S = \{a, b, c\}$ of three distinct elements. Let f be a one-one onto mapping from S onto itself. Then f is called a permutation.

Suppose $f(a) = b$, $f(b) = c$, $f(c) = a$. This permutation is denoted by two line notation. In this notation we write the elements of S in the first row and under each element of the first row, we put down its images under the mapping f . Thus f is denoted by $f = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$

Let $S = \{1, 2, 3\}$. There are $3!$ different ways of arranging the elements of S . Thus the total number of distinct one-one and onto functions which can be defined on S is $3! = 6$. That is the total number of distinct permutations of order 3 is 6.
All the 6 distinct permutations of order 3 for the set $S = \{1, 2, 3\}$ are as follows.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Note: The permutation $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ is same as the permutation $\begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}$ because the mapping is same in both the cases.

Equality of two permutations

Two permutations f and g of degree 3 on the set $S = \{1, 2, 3\}$ are said to be equal if ~~$f(x) = g(x)$ for all $x \in S$~~

$$f(x) = g(x) \quad \forall x \in S.$$

$f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ are equal as $f(1) = g(1) = 3, f(2) = g(2) = 1, f(3) = g(3) = 2$.

Identity permutation

The identity mapping I on the set $S = \{1, 2, 3\}$ onto itself is called the identity permutation of degree 3. i.e., $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ is the identity permutation of order 3.

Product or Composition of two permutations

Given two permutations of same order, they can be combined by means of composition of two functions. This is called the product of two permutations.

Let $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ be two permutations of degree 3. fog is the product of permutations f and g

such that $fog(1) = f(g(1)) = f(3) = 1$ Thus $fog = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$$fog(2) = f(g(2)) = f(1) = 2$$

$$fog(3) = f(g(3)) = f(2) = 3.$$

$$\text{Case 2: } f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ and } g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Also fog can be found as: $g: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{matrix} \quad f: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix} \quad \therefore fog = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Similarly gof can be found as: $f: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{matrix} \quad g: \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{matrix} \quad \therefore gof = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Observe that $fog \neq gof$.

Inverse of a permutation

Consider a permutation $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ of degree 3 on the set $S = \{1, 2, 3\}$.

Since f is a one-one onto mapping from the set S onto S , the inverse of f exists and it is

$$f^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \text{ or } = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Further f^{-1} is a permutation of degree 3.

The inverse permutation f^{-1} is written by interchanging the rows and writing in an order.

Further, $f \circ f^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$,

Also $f^{-1} \circ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$. the identity permutation

S_3 - the set of all permutations of degree 3.

Let $S = \{1, 2, 3\}$. The number of permutations of degree 3 are 6 and these are:
 $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $h = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $i = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $j = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

Thus $S_3 = \{e, f, g, h, i, j\}$

Theorem: The set S_3 of all permutations of degree 3, is a finite non-abelian group of order 6, under the product of permutations.

Symmetric group of degree 3

The group S_3 of all permutations of degree 3 is called 'the symmetric group of degree 3'.

Examples:

1. If $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ are two elements of S_3 , find fog^{-1} , gof^{-1} .

Sol: Given $f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$$f^{-1} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, g^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$fog^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$gof^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

2. If $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, in S_3 find $fogoh$ and $hogof$.

Sol: $fogoh = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{\text{Group}} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{\text{Group}} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}_{\text{Group}}$

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

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

$$hogof = \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}}_{\text{Group}} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}}_{\text{Group}} \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{\text{Group}}$$

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

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

Exercise.

1. If $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ is an element of S_3 find g^{-1} .
2. If $f = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ are in S_3 , find
 - (i) $f \circ g$ and (ii) $g \circ f$.
3. In the symmetric group of S_3 of $S = \{a, b, c\}$,
 $f^{-1} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$, $g = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$.
Find (i) $f \circ g$, (ii) $g \circ f$, (iii) $f \circ g^{-1}$.

Subgroups

A subset H of a group $\langle G, * \rangle$ is called a subgroup of G , if it is a group by itself w.r.t. the same binary operation defined in G .

Every group $\langle G, * \rangle$ will have at least two subgroups, one is the group G itself and the other is the subset $\{e\}$, where e is the identity element of G . These two subgroups of G are called trivial or improper subgroups of G . All other subgroups if it exist are called proper subgroups.

The following theorems give the necessary and sufficient conditions for a subset H of a group G to be a subgroup of G .

Theorem 1: A non empty subset H of a group $\langle G, * \rangle$ is a subgroup of G if and only if,

$$(i) a, b \in H \Rightarrow a * b \in H, (ii) a \in H \Rightarrow a^{-1} \in H.$$

Theorem 2: A non empty subset H of a group $\langle G, * \rangle$ is a subgroup of G if and only if $\forall a, b \in H, a * b^{-1} \in H$.

Examples

1. Show that the set of even integers including 0 is a subgroup of additive group of the set \mathbb{Z} of integers.

Sol. Let H be the set of even integers including 0.

Let $a, b \in H$. Thus $a=2n$ and $b=2m$ for some $n, m \in \mathbb{Z}$.

Consider, $a+b=2n+2m=2(n+m)$, which is even.

Hence $a+b \in H$.

Consider $a^{-1} = -a = -2n$, which is even.

Hence $a^{-1} \in H$

Hence H is a subgroup of \mathbb{Z} .

2. Show that the set of square roots of unity is a subgroup of the group of fourth roots of unity under multiplication.

Sol Let $H = \{1, -1\}$, the set of square roots of unity.

Let $G = \{1, -1, i, -i\}$, the set of fourth roots of unity.

Clearly $H \subseteq G$.

$$\text{Now, } 1 \in H, 1 \in H \Rightarrow 1 \cdot 1^{-1} = 1 \cdot 1 = 1 \in H$$

$$-1 \in H, -1 \in H \Rightarrow (-1) \cdot (-1)^{-1} = (-1) \cdot (-1) = 1 \in H$$

$$1 \in H, -1 \in H \Rightarrow 1 \cdot (-1)^{-1} = 1 \cdot (-1) = -1 \in H$$

$$-1 \in H, 1 \in H \Rightarrow (-1) \cdot 1^{-1} = (-1) \cdot 1 = -1 \in H$$

Thus $\forall a, b \in H, a \cdot b^{-1} \in H$.

Hence H is a subgroup of G .

3. Show that $H = \{0, 2, 4\}$ is a subgroup of the group $\langle G, +_6 \rangle$, where $G = \{0, 1, 2, 3, 4, 5\}$.

Sol $\begin{array}{c|ccc} +_6 & 0 & 2 & 4 \\ \hline 0 & 0 & 2 & 4 \\ 2 & 2 & 4 & 0 \\ 4 & 4 & 0 & 2 \end{array}$

(i) $\forall a, b \in H, a +_6 b \in H$

(ii) $0^{-1} = 0 \in H$

$2^{-1} = 4 \in H$

$4^{-1} = 2 \in H$

Hence H is a subgroup of G .

4. Show that the intersection of two subgroups of a group G is again a subgroup.

Sol Let H and K be any two subgroups of G .

(i) let $x, y \in H \cap K \Rightarrow x, y \in H$ and $x, y \in K$.
 $\Rightarrow x+y \in H$ and $x+y \in K$ [$\because H$ and K are subgroups of G].
 $\Rightarrow x+y \in H \cap K$.

(ii) let $x \in H \cap K \Rightarrow x \in H$ and $x \in K$.
 $\Rightarrow x^{-1} \in H$ and $x^{-1} \in K$ [$\because H$ and K are subgroups of G].
 $\Rightarrow x^{-1} \in H \cap K$

From (i) and (ii) $H \cap K$ is a subgroup of G .

5. Let G be a group and $a \in G$. Then the set

$N(a) = \{x \in G \mid xa = ax\}$ is a subgroup of G .
Sol. The set $N(a)$ is the set of all elements of G which commute with the fixed element a .

Let $x, y \in N(a)$, then $xa = ax$ and $ya = ay$.

Consider $ya = ay \Rightarrow y^{-1}(ya)y = y^{-1}(ay)y$

$$\Rightarrow (y^{-1}y)(ay) = (y^{-1}a)(yy^{-1})$$

$$\Rightarrow e(ay) = (y^{-1}a)e$$

$$\Rightarrow ay = y^{-1}a \quad \text{--- (1)}$$

$$\Rightarrow ay^{-1} = y^{-1}a$$

We shall show that $\forall x, y \in N(a)$, $xy^{-1} \in N(a)$

Consider $(xy^{-1})a = x(y^{-1}a)$

$$= x(ay^{-1}) \quad \text{from (1)}$$

$$= (xa)y^{-1}$$

$$= (ax)y^{-1} \quad [\because xa = ax]$$

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

$$\therefore xy^{-1} \in N(a).$$

Hence $N(a)$ is a subgroup of G .

6. Show that the union of two subgroups of a group need not be a subgroup of G .

Sol. Consider the groups $\langle \mathbb{Z}_6, +_6 \rangle$, where $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$
 Let $H = \{0, 3\}$ and $K = \{0, 2, 4\}$. Clearly H and K are subgroups of \mathbb{Z}_6 .

Consider $H \cup K = \{0, 2, 3, 4\}$.

~~Consider~~ let $3, 4 \in H \cup K$, $3 +_6 4 = 1 \notin H \cup K$.

$\therefore H \cup K$ is not closed under addition modulo 6.

Hence $H \cup K$ is not a subgroup of \mathbb{Z}_6 .

* Exercise

1. Show that $\langle \mathbb{R}^+, \times \rangle$ is a subgroup of $\langle \mathbb{R}^*, + \rangle$
2. Show that $\langle \mathbb{R}, + \rangle$ is a subgroup of $\langle \mathbb{C}, + \rangle$
3. Let G be the multiplicative group of all non singular matrices over complex numbers. Let H be the set of following matrices.
 $\pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$
Show that H is a subgroup of G .
4. Consider the group $\langle \mathbb{Z}_8, +_8 \rangle$, where $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5\}$
show that $H = \{0, 2, 4\}$ is a subgroup of \mathbb{Z}_8 .
5. Show that $H = \{1, 9\}$ is a subgroup of $\langle G, \times_{10} \rangle$,
where $G = \{1, 3, 7, 9\}$.
6. Consider the additive group $\langle \mathbb{Z}, + \rangle$ of all integers
and let $H = \{3a \mid a \in \mathbb{Z}\}$. Show that H is a subgroup of \mathbb{Z} .

Integral powers of an element of a group.

Let a be an element of a group G . Then for every integer n , by the element a^n , we mean,

(i) $a^n = a \cdot a \cdot a \dots a$, n times, if n is positive integer.

(ii) $a^{-n} = (a^n)^{-1}$, i.e., a^{-n} is the inverse of a^n .

(iii) $a^0 = e$, the identity element of G .

Note: If the group operation is denoted by $+$, then we write (i) $a + a + \dots + a$ by na instead of a^n (n is positive integer).

(ii) $\in (-na) = -na$

(iii) $0 \cdot a = 0$, the identity element of a group.

Ex In $(\mathbb{Z}_5^*, \times_5)$, where $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$$3^4 = 3 \times_5 3 \times_5 3 \times_5 3 = 1.$$

In $(\mathbb{Z}_4, +_4)$, where $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$$6(3) = 3 +_4 3 +_4 3 +_4 3 +_4 3 +_4 3 = 2,$$

here $3 \in \mathbb{Z}_4$ and 6 is the integer by which times the element 3 is composed with itself.

Order of an element

The order of an element a of a group G , is the least positive integer m such that $a^m = e$. If there exists no such integer for which $a^m = e$,

we say the element a is of infinite order.

The order of an element a is denoted by $O(a)$, read as order of a .

Note: 1. For any group, the identity element is the only element of order 1.

2. If for $a \in G$, where G is a group, $a^m = e$, for some positive integer n , then $O(a) \leq n$.

3. If $O(a) \geq n$, then $a^m \neq e$ for $0 < m < n$.

Examples

1. Find the orders of the elements of the multiplicative group $G = \{1, -1, i, -i\}$ of fourth root of unity.

Soln. Since 1 is the identity element, $O(1)=1$.

$$(-1)^2 = 1 \quad \therefore O(-1) = 2$$

$$i^4 = 1 \quad \therefore O(i) = 4$$

$$-i^4 = 1 \quad \therefore O(-i) = 4$$

2. Find the orders of the elements of the multiplicative group $G = \{1, \omega, \omega^2\}$ of cube roots of unity. [where $\omega = \frac{-1+i\sqrt{3}}{2}$]

Soln. Since 1 is the identity element $O(1)=1$.

$$\omega^3 = 1 \quad \therefore O(\omega) = 3$$

$$(\omega^2)^3 = 1 \quad \therefore O(\omega^2) = 3$$

3. Find the orders of the elements of the group.

$$G_1 = \langle \mathbb{Z}_4, +_4 \rangle$$

Soln. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

since 0 is the identity element $O(0)=1$

$$4(1) = 1+_4 1+_4 1+_4 1 = 0 \quad \therefore O(1) = 4$$

$$4(2) = 2+_4 2 = 0 \quad \therefore O(2) = 2$$

$$4(3) = 3+_4 3+_4 3 = 0 \quad \therefore O(3) = 4$$

- Note.
- In the group $\langle \mathbb{Z}, + \rangle$ of integers, every element except identity 0, is of infinite order.
 - In the multiplicative group of positive rational numbers, every element except the identity element 1, is of the infinite order.

Properties related to order of an element of a group.

1. In a group G , $O(a) = O(a^{-1})$, for every $a \in G$.
2. If a is an element of the group G , is of order n , then $a^m = e$, for any integer m , if and only if n divides m .
3. If a and x be any two elements of the group G , then $O(a) = O(xax^{-1})$.
4. In a group G , $O(ab) = O(ba)$, $\forall a, b \in G$.
5. In a group G , the order of any element a cannot exceed that of the group. That is $O(a) \leq O(G)$.
6. Let G be a group and $a \in G$. If $O(a) = n$ and $(m, n) = 1$, then $O(a^m) = n$.
7. The order of any power of an element of a group cannot exceed the order of the element.
i.e., $O(a^k) \leq O(a)$.
8. If $O(a) = n$, where a is an element of the group G and $d = (n, m)$ then $O(a^m) = \frac{n}{d}$.

Examples

1. Given an example of a group to show that $O(ab)$ need not be equal to $O(a), O(b)$.
Sol Consider the group $G = \{1, -1, i, -i\}$ of fourth roots of unity under multiplication.
 $\therefore (-1)^2 = 1 \Rightarrow O(-1) = 2$ and $\therefore (-i)^4 = 1 \Rightarrow O(-i) = 4$.
Now $(-1)(-i) = i$ and $\therefore i^4 = 1 \Rightarrow O[-1(-i)] = 4$.
But $O(-1), O(-i) = 2, 4 = 8$
Thus $O[-1(-i)] \neq O(-1). O(-i)$.

Cyclic Groups

If G is a group and $a \in G$, the subset $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is known as the cyclic subgroup of G generated by the element a . In this subgroup for every element $b \in H$, there exists an integer $m \in \mathbb{Z}$, such that $b = a^m$.

That is every element of H can be expressed as an integral power of a . For this reason, H is called the "subgroup generated by a ".

If this property of expressing every element as an integral power of a single element, say a , holds good for the whole group, then such group is called a cyclic group generated by the element a .

A group G is said to be a cyclic group generated by the element $a \in G$ if $G = \{a^n \mid n \in \mathbb{Z}\}$ and is denoted by $G = \langle a \rangle$.

Note:

1. If the binary operation for the cyclic group $G = \langle a \rangle$ is $+$, then every element of G is of the form na for some $n \in \mathbb{Z}$.
2. A cyclic group may have more than one generator.
3. A cyclic group is said to be finite cyclic group, if the group is finite, otherwise it is said to be infinite cyclic group.

examples

1. Show that the multiplicative group of fourth roots of unity is a cyclic group.

Sol $G_4 = \{1, -1, i, -i\}$

Now $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$

Therefore i is a generator of G_4 .

Thus G_4 is a cyclic group generated by the element i .

The element $-i$ is another generator of G_4 .

2. Show that the group $\langle \mathbb{Z}_5, +_5 \rangle$ is a cyclic group and every non zero element of \mathbb{Z}_5 is a generator.

Sol $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

Consider $4 \in \mathbb{Z}_5 \quad 4 = 1 \cdot 4$

$$4 +_5 4 = 3 \Rightarrow 3 = 2 \cdot 4$$

$$4 +_5 4 +_5 4 = 2 \Rightarrow 2 = 3 \cdot 4$$

$$4 +_5 4 +_5 4 +_5 4 = 1 \Rightarrow 1 = 4 \cdot 4$$

$$4 +_5 4 +_5 4 +_5 4 +_5 4 = 0 \Rightarrow 0 = 0 \cdot 4$$

Thus every element of \mathbb{Z}_5 can be expressed as some integral multiple of the element $4 \in \mathbb{Z}_5$.

Therefore \mathbb{Z}_5 is a cyclic group with 4 as a generator.

Similarly, one can verify other non zero element of \mathbb{Z}_5 is also a generator.

Note 1. $\langle \mathbb{Z}, + \rangle$ is an infinite cyclic group with 1 as a generator.

2. $\langle \mathbb{Z}_n, +_n \rangle$ is a finite cyclic group with 1 as a generator.

3. $\langle \mathbb{Q}, + \rangle$ is not a cyclic group.

[Let $\langle \mathbb{Q}, + \rangle$ be a cyclic group generated by $m \in \mathbb{Q}$.

Then $m = \frac{p}{q}$, $p, q \in \mathbb{Z}$, $q \neq 0$.

Let $\frac{1}{2q} \in \mathbb{Q} \Rightarrow \frac{1}{2q} = n \cdot m$, $n \in \mathbb{Z} \Rightarrow \frac{1}{2q} = n \cdot \frac{p}{q} \Rightarrow \frac{1}{2} = n \cdot p$.

[It is impossible as the product of two integers is not equal to a fraction. Thus $\langle \mathbb{Q}, + \rangle$ is not cyclic].

Properties of Cyclic Groups.

Theorem 1:

Every cyclic group is abelian.

Proof. Let G be a cyclic group with a as a generator.
Thus $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Let $x, y \in G$ be arbitrary.
Then there exists two integers m and n , such that
 $x = a^m$ and $y = a^n$.

Consider $x \cdot y = a^m \cdot a^n$

$$\begin{aligned} &\Rightarrow x \cdot y = a^{m+n} \\ &\Rightarrow x \cdot y = a^{n+m} \\ &\Rightarrow x \cdot y = a^n \cdot a^m \\ &\Rightarrow x \cdot y = y \cdot x \end{aligned}$$

Hence G is abelian.

Note. The converse of the above theorem is not true.
That is every abelian group is not necessarily cyclic.
Consider $G = \{v_1, v_2, v_3, v_4\}$ and the associative binary composition $*$, given by the following table.

*	v_1	v_2	v_3	v_4
v_1	v_1	v_2	v_3	v_4
v_2	v_2	v_1	v_4	v_3
v_3	v_3	v_4	v_1	v_2
v_4	v_4	v_3	v_2	v_1

(i) v_1 is the identity element,
since $v_i * v_j = v_j = v_i * v_j \forall v_i, v_j \in G$.

(ii) $v_1^{-1} = v_1, v_2^{-1} = v_2, v_3^{-1} = v_3, v_4^{-1} = v_4$.
Each element is inverse of itself.

(iii) The table is symmetric.
Hence G is commutative.

Hence G is an abelian group.

This group $\langle G, * \rangle$ is known as the Klein's 4 group.

Here; $\langle v_1 \rangle = \{v_1\}, \langle v_2 \rangle = \{v_1, v_2\}, \langle v_3 \rangle = \{v_1, v_3\}, \langle v_4 \rangle = \{v_1, v_4\}$

Thus no element of G , generates the whole group G .

Hence G is not cyclic.

Theorem 2:

If a is a generator of a cyclic group G , then \bar{a} is also a generator.

Theorem 3:

If a is a generator of a cyclic group G , then $O(a) = O(G)$.

Theorem 4:

If G is a finite group of order n , containing an element of order n , then G is cyclic.

Theorem 5:

Let G be a cyclic group of order k and a be a generator. If $a^m = a^n$ ($m \neq n$), then $m \equiv n \pmod{k}$ and conversely.

Theorem 6:

Let G be a cyclic group of order d and a be a generator. The element a^k ($k < d$) is also a generator of G , if and only if $(k, d) = 1$.

Theorem 7:

Every ~~cyclic~~ subgroup of a cyclic group is cyclic.

* Let d be any positive integer. The number of positive integers less than d and prime to d , is denoted by $\phi(d)$.

Any integer n can be decomposed into product of prime factors. i.e., $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where p_1, p_2, \dots

Then $\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$ prime factors

Theorem 8:

A cyclic group of order d has $\phi(d)$ generators.

examples

1. Find the number of generators of the cyclic group of order 60.

Soln: Given $O(G) = 60$

$$\text{and } 60 = 2^2 \times 3 \times 5$$

$$\therefore \varphi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 16.$$

Thus G has 16 generators.

2. How many generators are there for the cyclic group of order 10. If a is a generator, what are the other generators?

Soln $10 = 2 \times 5 \Rightarrow \varphi(10) = 10 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 4.$

Thus there are 4 generators.

By data a is a generator. The other generators are of the form a^k , with $(k, 10) = 1$.

Hence $k=1, 3, 7, 9$. Thus the generators are a, a^3, a^7, a^9 .

Note: If the group operation is in addition form, and a is one of the generator, then other generators are of the form $k \cdot 1$ with $(k, n) = 1$, where $O(G) = n$.

3. Find the number of generators of the cyclic group

$(\mathbb{Z}_{18}, +_{18})$. Write all the generators.

Soln $O(\mathbb{Z}_{18}) = 18$ and $18 = 2 \times 3^2 \Rightarrow \varphi(18) = 18 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 6$

Thus there are 6 generators.

We know that 1 is a generator.

$$(k, 18) = 1 \Rightarrow k = 1, 5, 7, 11, 13, 17.$$

Thus the generators are 1, 5, 7, 11, 13 and 17.

Coset Decomposition of a group.

Let $\langle G, * \rangle$ be a group and H be a subgroup of G .
 For $a, b \in G$ "a is said to be congruent to b modulo H "
 or aRb , if and only if $a \cdot b^{-1} \in H$.

If a is congruent to b mod H , then we write $a \equiv b \pmod{H}$.
 The relation $a \equiv b \pmod{H}$ is an equivalence relation.
 Hence this relation gives a partition of G , into disjoint
 classes. Each member in the partition is a non-empty
 subset of G and any two distinct members of the
 partition are disjoint.

If $a \in G$, we denote the equivalent class generated by
 a by $[a]$. i.e., $[a] = \{x \in G \mid x \equiv a \pmod{H}\}$
 $= \{x \in G \mid xa^{-1} \in H\}$

Cosets of a subgroup H in a group G

Let H be a subgroup of a group $\langle G, * \rangle$ and
 a be any element of G .

The set Ha defined by $Ha = \{ha \mid h \in H\}$ is called the
 right coset of H in G w.r.t. a .

The set aH defined by $aH = \{ah \mid h \in H\}$ is called the
 left coset of H in G w.r.t. a .

Note

1. $Ha \neq \emptyset$ [$\because e \in H$ and $e \cdot a = a \in Ha$]

2. $aH \neq \emptyset$ [$\because e \in H$ and $a \cdot e = a \in aH$]
 $H \neq \emptyset$ $\therefore h \in H \Rightarrow \{h \mid h \in H\} = H$
 $\therefore aH = H$, and $Ha = H$.

Similarly $aH = H$, and $Ha = H$.
 Thus every subgroup H itself is a right coset and
 as well left coset of H in G .

3. If G is abelian, then every right coset Ha is equal
 to corresponding left coset aH .

i.e., if G is abelian $Ha = aH$. But in general $Ha \neq aH$

Results related to Cosets.

1. If H is a subgroup of a group G , then for all $a \in G$, $[a] = Ha$.
From the above theorem, we have $\forall a \in G$, $Ha = [a]$. Thus any two distinct cosets of H in G are disjoint and the union of all the right cosets of H is whole of G . In other words the collection of all distinct right cosets of H in G forms a partition of the group G . This decomposition of the group G is called the "right coset decomposition" of the group G , w.r.t. the subgroup H .
Similarly if one defines a relation called "congruence modulo H " on G by $a \equiv b \pmod{H}$ if and only if $b^{-1}a \in H$. It can be shown that $[a] = aH$ and hence the collection of all distinct left cosets of H in G form a partition of the group G . This decomposition of the group G is called the "left coset decomposition" of the group w.r.t. the subgroup H .
 2. If H is a subgroup of G , then there exists a one-to-one correspondence between any two right(left) cosets of H in G .
 3. There is one-to-one correspondence between the set of all right cosets and the set of all left cosets of a subgroup of a group.
- Index of a subgroup:
The number of distinct right(left) cosets of a subgroup H of a group G is called the index of the subgroup H in G and is denoted by $[G : H]$ and read as "the index of H in G ".

Lagrange's Theorem

If G is any finite group and H is any subgroup of G , then $O(H)$ divides $O(G)$.

Proof: Let $O(G) = n$ and $O(H) = m$.

We shall show that $m \mid n$ i.e., $n = km$, for some $k \in \mathbb{Z}$.
Since the group G is finite, there are finite number of right(left) cosets of H in G .

Let G have k distinct right(left) cosets of H and let these are $Ha_1, Ha_2, \dots, Ha_k \Rightarrow [G : H] = k$.

We know that any two right(left) cosets of H have the same number of elements.
The same number of elements.
In particular H itself is a right(left) coset of H in G .
Since $O(H) = m$, each right(left) coset of H will have m elements.

$$\text{Also } G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$$

$$\therefore O(G) = O(Ha_1) + O(Ha_2) + \dots + O(Ha_k)$$

$$\Rightarrow n = O(H) + O(H) + \dots + O(H) \quad (k \text{ times})$$

$$\Rightarrow n = m + m + \dots + m \quad (k \text{ times})$$

$$\Rightarrow n = km$$

$$\text{or } m \mid n \text{ i.e., } O(H) \mid O(G).$$

Note
1. The index of any subgroup of a finite group is a divisor of the order of the group.
[i.e., if $O(G) = n$, $[G : H] = k$ then $k \mid n$ [It follows from Lagrange's theorem]]

2. The converse of Lagrange's theorem need not be true.
i.e., If G is a finite group of order n and m is a positive integral divisor of n , then G need not have a subgroup of order m .
3. If $O(G) = n$, $O(H) = m$, $[G : H] = k$, then the number of right(left) cosets of H in G is equal to $\frac{O(G)}{O(H)}$

Consequences of Lagrange's Theorem

1. If G is a finite group and $a \in G$, then $O(a)$ divides $O(G)$.
2. If G is a finite group of order n then $\forall a \in G$, $a^n = e$, where e is the identity element of G .
3. A finite group of prime order is cyclic and hence abelian.
4. If G is a cyclic group of prime order then G has no proper subgroup.
5. Every finite group of composite order has proper subgroups.
6. Any group of order five or less than five is abelian.
7. If G is a finite cyclic group of order k , then for every divisor n of k , there exists a unique subgroup of G of order n .

Examples

1. Consider the multiplicative group $G = \{1, -1, i, -i\}$ of fourth roots of unity and $H = \{-1, 1\}$ be a subgroup of G . Write all the right cosets of H in G .
Soln Here $O(G) = 4$, $O(H) = 2$
The number of distinct right cosets of H in G is $[G : H] = \frac{O(G)}{O(H)} = \frac{4}{2} = 2$.
The right cosets are $H \cdot 1 = \{-1, 1\}$ and $H \cdot i = \{-i, i\}$

2. Find all the left cosets of $H = \{0, 4, 8\}$ in $\langle \mathbb{Z}_{12}, +_{12} \rangle$

Soln Here $O(\mathbb{Z}_{12}) = 12$ and $O(H) = 3$.

∴ number of distinct left cosets of H in $G = \frac{12}{3} = 4$.

These are

$$0 +_{12} H = \{0, 4, 8\}$$

$$1 +_{12} H = \{1, 5, 9\}$$

$$2 +_{12} H = \{2, 6, 10\}$$

$$3 +_{12} H = \{3, 7, 11\}.$$

3. List all the subgroups of the cyclic group of fourth roots of unity.

Soln $G = \{1, -1, i, -i\}$.

Here $O(G) = 4$ and i is a generator.

The divisors of 4 are 1, 2 and 4.

∴ The subgroups of G are the only subgroups generated by i , $i^2 = -1$ and $i^4 = 1$.

∴ The subgroups are

$$\langle i \rangle = \{1, -1, i, -i\}, \langle -1 \rangle = \{1, -1\}, \langle 1 \rangle = \{1\}.$$

4. List all the subgroups of a cyclic group G of order 24 and whose generator is g .

Soln Here $O(G) = 24$, $O(g) = 24$.

The divisors of 24 are 1, 2, 3, 4, 6, 8, 12 and 24.

∴ The subgroups of G are the only subgroups generated by $g, g^2, g^3, g^4, g^6, g^8, g^{12}$ and $g^{24} = e$.

5. Find all the subgroups of $\langle \mathbb{Z}_{18}, +_{18} \rangle$.

Sol: 1 is a generator of \mathbb{Z}_{18} .

The divisors of 18 are 1, 2, 3, 6, 9, 18.

∴ The generators of the subgroups are

$$1 \cdot 1 = 1, \quad 1 \cdot 2 = 2, \quad 1 \cdot 3 = 3, \quad 1 \cdot 6 = 6, \quad 1 \cdot 9 = 9, \quad 1 \cdot 18 = 0$$

Subgroups are $\langle 1 \rangle = \mathbb{Z}_{18}$

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$$

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$$

$$\langle 6 \rangle = \{0, 6, 12\}$$

$$\langle 9 \rangle = \{0, 9\}$$

$$\langle 0 \rangle = \{0\}.$$

Exercise

1. Find all the eight cosets of the subgroup $H = \{0, 3\}$ in the group $\langle \mathbb{Z}_6, +_6 \rangle$.
2. Find all the eight cosets of the subgroup $H = \{1, 3, 9\}$ in the group $\langle \mathbb{Z}_{12} - \{0\}, \times_{12} \rangle$.
3. List all the subgroups of $\langle \mathbb{Z}_9, +_9 \rangle$.
4. Find all the subgroups of $\langle \mathbb{Z}_6, +_6 \rangle$.
5. Find the number of elements in the cyclic subgroup of $\langle \mathbb{Z}_{12}, +_{12} \rangle$ generated by 3 and 8.
[Hint: If g is a generator of a cyclic group G of order n , then g^m generates a subgroup H of G of order $\frac{n}{d}$, where $d = \text{gcd}(n, m)$.]
6. Find all the left cosets of $H = \{0, 3, 6, 9\}$ in $\langle \mathbb{Z}_{12}, +_{12} \rangle$ and verify Lagrange's theorem in each case.

Homomorphism:

Let $\langle G, \cdot \rangle$ and $\langle G', * \rangle$ be two groups. A mapping $f: G \rightarrow G'$ is said to be a homomorphism if $f(g_1 \cdot g_2) = f(g_1) * f(g_2)$ for $g_1, g_2 \in G$.

That is the mapping f is said to be a homomorphism, if f maps the composition of any two elements of G into the composition of the images of the elements.

By this we say that f preserves composition.

If f is a homomorphism from the group G into G' , we say G is homomorphic to the group G' .

Isomorphism

A homomorphism f from a group G into G' is said to be isomorphism if f is a bijection.

i.e., f is both one-one and onto.

Two groups G and G' are said to be isomorphic, if there exists an isomorphism $f: G \rightarrow G'$.

This we denote it by $G \approx G'$.

Endomorphism

A homomorphism f from a group G into itself is called Endomorphism.

Automorphism

An isomorphism f from a group G onto itself is called Automorphism.

Note: The identity map $I_G: G \rightarrow G$ from the group G onto itself, defined by $I_G(g) = g$ is a homomorphism. This shows that there exists atleast one homomorphism from G into itself. Further $I_G(g) = g$ is an automorphism.

Examples

1. Let $\langle G, \cdot \rangle$ and $\langle G', * \rangle$ be two groups and e' be the identity element of G' . Define $f: G \rightarrow G'$ by $f(g) = e' \forall g \in G$. Show that f is a homomorphism.

Sol: Consider, $f(g_1, g_2) = e'$, $g_1, g_2 \in G$.

$$\text{Also, } f(g_1) * f(g_2) = e' * e' = e'$$

$$\therefore f(g_1, g_2) = f(g_1) * f(g_2).$$

Hence f is a homomorphism.

This homomorphism is called a trivial homomorphism.

2. Consider the additive group $\langle \mathbb{Z}, + \rangle$ of all integers and the group $H = \{1, -1\}$ under multiplication. Define $\varphi: \mathbb{Z} \rightarrow H$ by $\varphi(n) = \begin{cases} 1 & \text{if } n \text{ is even or zero} \\ -1 & \text{if } n \text{ is odd} \end{cases}$

Show that φ is a homomorphism.

Sol: let $m, n \in \mathbb{Z}$

Case(i) Let m and n are both even.

Then $m+n$ is even $\Rightarrow \varphi(m+n) = 1$.

Also $\varphi(m) = 1$ and $\varphi(n) = 1$.

$\therefore \varphi(m+n) = \varphi(m), \varphi(n)$.

Case(ii) Let one of m and n be even, say m be even and n be odd. Then $m+n$ is odd $\Rightarrow \varphi(m+n) = -1$,

Also $\varphi(m) = 1$ and $\varphi(n) = -1$

$\therefore \varphi(m+n) = \varphi(m), \varphi(n)$.

Case(iii) Let m and n be both odd.

Then $m+n$ is even $\Rightarrow \varphi(m+n) = 1$.

Also $\varphi(m) = -1$ and $\varphi(n) = -1$

$\therefore \varphi(m+n) = \varphi(m), \varphi(n)$.

Hence φ is an homomorphism.

3. Let $M_n(\mathbb{R})$ be the group of all non-singular $n \times n$ matrices with real entries under matrix multiplication. Let \mathbb{R}^* be the multiplicative group of non-zero real numbers. If $\varphi: M_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ is defined by $\varphi(A) = |A|$, $\forall A \in M_n(\mathbb{R})$, show that φ is a homomorphism.

Sol: Consider $\varphi(AB) = |AB|$, $\forall A, B \in M_n(\mathbb{R})$

$$= |A| \cdot |B|$$

$$\varphi(AB) = \varphi(A) \cdot \varphi(B).$$

Hence φ is a homomorphism.

4. Consider the multiplicative group (\mathbb{R}^*, \cdot) of all non-zero real numbers. Define $f: \mathbb{R}^* \rightarrow \mathbb{R}^*$ by $f(x) = 2^x$, $x \in \mathbb{R}$. Verify if f is a homomorphism.

Sol: Consider $f(xy) = 2^{xy}$

$$\text{and } f(x) = 2^x, f(y) = 2^y \therefore f(x) \cdot f(y) = 2^x \cdot 2^y = 2^{x+y}$$

$$\therefore f(xy) \neq f(x) \cdot f(y)$$

Hence f is not a homomorphism.

5. Define $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}, +)$ by $f(x) = \text{greatest integer} \leq x$.

Is f a homomorphism?

Sol: By definition of f , $f(1) = 1$, $f(\frac{1}{2}) = 0$, $f(\frac{3}{2}) = 1$, ... so on
Consider $f(\frac{3}{2}) = 1$ and $f(\frac{5}{2}) = 2$

$$f\left(\frac{3}{2} + \frac{5}{2}\right) = f(4) = 4$$

$$\text{Also } f\left(\frac{3}{2}\right) + f\left(\frac{5}{2}\right) = 1 + 2 = 3$$

$$\therefore f\left(\frac{3}{2} + \frac{5}{2}\right) \neq f\left(\frac{3}{2}\right) + f\left(\frac{5}{2}\right)$$

$\therefore f$ is not a homomorphism.

Elementary properties of Homomorphism

1. Let $f: G \rightarrow G'$ be a homomorphism from the group $\langle G, \cdot \rangle$ into the group $\langle G', * \rangle$. Then
 - (i) $f(e) = e'$ where e and e' are the identity elements of the group G and G' respectively.
 - (ii) $f(a^{-1}) = [f(a)]^{-1}$, $\forall a \in G$.
2. If f is a homomorphism of a group G into G' , then the range $f(G) = \{f(g) \mid g \in G\}$ is a subgroup of G' . The set $f(G) = \{f(g) \mid g \in G\}$ is called the homomorphic image of G in G' .
3. If $f: G \rightarrow G'$ is a homomorphism of a group G into G' and H is a subgroup of G , then $f(H)$ is again a subgroup of G' .
4. If $f: G \rightarrow G$ be a homomorphism from the group G into itself and H is a cyclic subgroup of G , then $f(H)$ is again a cyclic subgroup of G .

Kernel of a Homomorphism:

Let $f: G \rightarrow G'$ be a homomorphism from the group G into G' and e' be the identity element of G' . The subset K of G defined by $K = \{a \in G \mid f(a) = e'\}$ is called the kernel of the homomorphism f and is denoted by $\ker f$.

Examples

1. If $f: \mathbb{C}^* \rightarrow \mathbb{C}^*$ is a homomorphism defined by $f(a+ib) = a - ib$ & $a+ib \in \mathbb{C}^*$, find $\ker f$.

$$\text{sol } \ker f = \{x \in \mathbb{C}^* \mid f(x) = e^i\}$$

$$= \{a+ib \mid f(a+ib) = 1\} \quad [e^i = 1]$$

$$= \{a+ib \mid a-ib = 1\}$$

$$= \{a+ib \mid a=1, b=0\}$$

$$\ker f = \{1\}$$

2. Consider the homomorphism $f: \langle \mathbb{R}^+, \cdot \rangle \rightarrow \langle \mathbb{R}, + \rangle$,

where $\langle \mathbb{R}^+, \cdot \rangle$ is the multiplicative group of all positive real numbers and $\langle \mathbb{R}, + \rangle$ is the additive group of all real numbers, defined by $f(x) = \log_{10} x$. Find $\ker f$.

$$\text{sol } \ker f = \{x \in \mathbb{R}^+ \mid f(x) = 0\}$$

$$= \{x \in \mathbb{R}^+ \mid \log_{10} x = 0\}$$

$$= \{x \in \mathbb{R}^+ \mid x = 1\}$$

$$= \{1\}$$

Results related to Isomorphism

1. If $f: G \rightarrow G'$ be an isomorphism of a group G onto a group G' and a is any element of G , then the order of $f(a)$ equals the order of a .
2. Let $f: G \rightarrow G'$ be an isomorphism. If G is abelian, then G' is also abelian.
3. Any infinite cyclic group is isomorphic to the group \mathbb{Z} of integers, under addition.
4. Any finite cyclic group of order n is isomorphic to additive group of integers modulo n .

Examples

1. Show that the additive group $\langle \mathbb{R}, + \rangle$ of all real numbers and the multiplicative group $\langle \mathbb{R}^+, \cdot \rangle$ of all positive real numbers are isomorphic.
Soln Define $f: \langle \mathbb{R}, + \rangle \rightarrow \langle \mathbb{R}^+, \cdot \rangle$ by $f(x) = e^x$, $x \in \mathbb{R}$.
Now $f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$
 $\therefore f$ is a homomorphism.
Again, $f(x) = f(y) \Rightarrow e^x = e^y$
 $\Rightarrow e^{x-y} = 1 = e^0$
 $\Rightarrow x-y=0$
 $\Rightarrow x=y$
 $\therefore f$ is one-one.
Let $y \in \mathbb{R}^+$, consider $f(\log_e y) = e^{\log_e y} = y$
 $\forall y \in \mathbb{R}^+ \exists \log_e y \in \mathbb{R}$ such that $f(\log_e y) = y$
 $\therefore f$ is onto
Hence f is a isomorphism.

2. Let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R}^* \right\}$. Show that $f: \langle G, \cdot \rangle \rightarrow \langle \mathbb{R}^*, \cdot \rangle$
defined by $f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = a$ is an isomorphism.

Sol $f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) \cdot f\left(\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right) = f\left(\begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}\right) = ab = f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) \cdot f\left(\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}\right)$

$\therefore f$ is a homomorphism.

Let $f(a) = f(b) \Rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow a = b$.

$\therefore f$ is one-one.

Let $a \in \mathbb{R}^*$, consider $f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = a$:

$\exists a \in \mathbb{R}^*$, $\exists \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in \langle G, \cdot \rangle$ such that $f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = a$.

$\therefore f$ is onto.

Hence f is an isomorphism.

Exercise!

1. Verify if the following maps are homomorphisms.
If the map is a homomorphism, find its kernel.

i) $f: \langle \mathbb{Q}, + \rangle \rightarrow \langle \mathbb{R}^*, \cdot \rangle$ defined by $f(x) = e^x$, $\forall x \in \mathbb{Q}$

ii) $f: \langle \mathbb{Z}, + \rangle \rightarrow \langle \mathbb{Z}_n, +_n \rangle$ defined by $f(a) = r$, $\forall a \in \mathbb{Z}$,
where r is the unique least non-negative remainder
when a is divided by n .

iii) $g: \langle \mathbb{C}^*, \cdot \rangle \rightarrow \langle \mathbb{C}^*, \cdot \rangle$ defined by $g(z) = |z|$, $\forall z \in \mathbb{C}^*$.

iv) $f: \langle \mathbb{R}, + \rangle \rightarrow \langle \mathbb{R}, + \rangle$ defined by $f(x) = 3x+1$, $\forall x \in \mathbb{R}$

2. Show that the following mappings are isomorphisms.

2. Show that the following mappings are isomorphisms.

i) $T: \langle G, + \rangle \rightarrow \langle G_1, + \rangle$, where $G_1 = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$,

defined by $T(a+b\sqrt{2}) = a-b\sqrt{2}$.

ii) G_1 is any group of q a fixed element of G_1 .

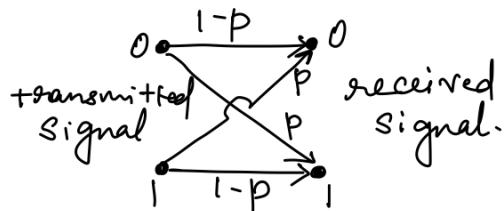
$T: G_1 \rightarrow G$ defined by $T(x) = qxq^{-1}$.

Coding Theory

In this section we introduce an area of applied mathematics called algebraic coding theory. It will be an introductory level as we seek to model the transmission of information represented by strings of the signals 0 and 1.

In digital communications, when information is transmitted in the form of strings of 0's and 1's, certain problems arise. As a result of noise in the channel, when a certain signal is transmitted a different signal may be received, thus causing the receiver to make a wrong decision. Hence we want to develop techniques to help us detect and perhaps even correct, transmission errors. However, we can only improve the chances of correct transmissions; there are no guarantees.

The model uses a binary symmetric channel. (binary - since an individual signal is represented by one of the bits 0 or 1). When a transmitter sends the signal 0 or 1 in such a channel, associated with either signal is a (constant) probability p for incorrect transmission. When that probability p is the same for both signals, the channel is called symmetric. Here, for example, we have probability p of sending 0 and having 1 received. The probability of sending signal 0 and having it received correctly is then $1-p$. All possibilities are illustrated in the following figure.



Note:

In coding theory, we assume that the transmission of any signal does not depend in any way on the transmission of prior signals. Consequently, the probability of the occurrence of all of these independent events (in their prescribed order) is given by the product of their individual probabilities.

Consider the string $c=10110$, where c is an element of the group \mathbb{Z}_2^5 , obtained from the direct product of five copies of $(\mathbb{Z}_2, +)$. When sending each bit of c through binary symmetric channel, we assume that probability of incorrect transmission is $p=0.05$, so that the probability of transmitting c with no errors is $(0.95)^5 = 0.7738$

- * What is the probability of sending $c=10110$ and receiving $r=00110$? Assume that the probability of incorrect transmission of a bit is $p=0.05$.

Sol $r=00110$ is the original message with an error in the first position. So the probability of receiving

$$r=00110 \text{ is } \left(\begin{array}{l} \text{probability} \\ \text{of incorrect} \\ \text{transmission} \\ \text{at 1st position} \end{array} \right) \times \left(\begin{array}{l} \text{probability} \\ \text{of correct} \\ \text{transmission} \\ \text{at remaining} \\ \text{positions} \end{array} \right) = 0.05 \times (0.95)^4 = 0.0407$$

- * What is the probability of sending $c=10110$ and receiving i) $r=10000$, ii) $r=00100$? Assume that the probability of incorrect transmission of a bit is $p=0.05$.

Sol i) probability of receiving $r=10000$ is $= (0.95) \times (0.95) \times (0.05) \times (0.05) \times (0.95) = 0.0021$

ii) probability of receiving $r=00100$ is $= (0.05) \times (0.95) \times (0.95) \times (0.05) \times (0.95) = 0.0021$

- * If $c=10110$ is transmitted, what is the probability that r differs from c in exactly two places?

Sol The desired probability is equal to sum of the probabilities of each error pattern with (error)(error)(no error)(no error)(no error). Each such pattern has probability $(0.05)^2 (0.95)^3$. There are ${}^5 C_2$ such patterns, so the probability of two errors in transmission is given by ${}^5 C_2 (0.05)^2 (0.95)^3 = 0.0214$

Suppose a signal $c = 10110$ is transmitted and the signal $r = 00110$ is received. Let the probability of incorrect transmission for a bit is 0.05. With the assumption of independent events, the probability of sending c and receiving r , is $(0.05)(0.95)^5 = 0.0407$.

With $e = 10000$, we can write $c + e = r$ and interpret r as the result of the sum of the original message c and the particular error pattern $e = 10000$.

Since $c, r, e \in \mathbb{Z}_2^5$ and $-1 = 1$ in \mathbb{Z}_2 , we can also write $c + r = e$ and $r + e = c$.

Theorem:

Let $c \in \mathbb{Z}_2^n$. For the transmission of c through a binary symmetric channel with probability p of incorrect transmission,

- ① the probability of receiving $r = c + e$, where e is a particular error pattern consisting of k 1's and $(n-k)$ 0's is, $p^k(1-p)^{n-k}$.
- ② the probability that k errors are made in the transmission is ${}^n C_k p^k(1-p)^{n-k}$.

Examples

1. Let C be a set of code words, where $C \subseteq \mathbb{Z}_2^7$. In each of the following, determine the third term, given any two terms [error pattern], r (received word), c (code word)], with $r = c + e$. (i) $c = 1010110$, $r = 1011111$, c (code word), (ii) $c = 1010110$, $e = 0101101$, (iii) $e = 0101111$, $r = 0000111$.

- Soln
- (i) $e = c + r = 0001001$
 - (ii) $r = c + e = 1111011$
 - (iii) $c = r + e = 0101000$.

A binary symmetric channel has probability $p=0.05$ of incorrect transmission. If the code word $c=011011101$ is transmitted, what is the probability that (a) we receive $r=011111101$? (b) we receive $r=111011100$? (c) a single error occurs? (d) a double error occurs?

Sol Given $c = 011011101$,

(a) $r = 011111101$

out of the 9 positions, there is an error in 4th position

$$\therefore P(C \text{ receiving } r) = (0.05)(0.95)^8 = 0.0332$$

(b) $r = 111011100$

out of the 9 positions, there is an error in 1st and 9th position, $\therefore P(\text{receiving } r) = (0.05)^2 (0.95)^7 = 0.0017$

(c) probability(error at ^{one position} only) = 0.0332

Out of the 9 positions, a single error can happen in ${}^9 C_1 = 9$ ways

$$\therefore \text{Probability of single error} = 9 \times 0.0332 = 0.2988$$

(d) probability(error at ^{two positions}) = 0.0017

Out of the 9 positions, a double error can happen in ${}^9 C_2 = 36$ ways

$$\therefore \text{Probability of double error} = 36 \times 0.0017 = 0.0612$$

In actuality, a binary symmetric channel is considered good when $p < 10^{-5}$. However, no matter what else we stipulate, we always want $p < 1/2$.

To improve the accuracy of transmission in a binary symmetric channel, certain types of coding schemes can be used where extra signals are provided.

For $m, n \in \mathbb{Z}^+$, let $n > m$.

Consider $\emptyset \neq W \subseteq \mathbb{Z}_2^m$. Set W consists of messages to be transmitted.

We append to each $w \in W$, $n-m$ extra signals to form the code word c , where $c \in \mathbb{Z}_2^n$.

This process is called encoding and is represented by the function $E: W \rightarrow \mathbb{Z}_2^n$. Then $E(w) = c$ and $E(W) = C \subseteq \mathbb{Z}_2^n$.

Since the function E simply appends extra bits to the (distinct) messages the encoding process is one-to-one.

Upon transmission, c is received as $T(c)$, where $T(c) \in \mathbb{Z}_2^n$. T is not a function because $T(c)$ may be different at different transmission times (or the noise in the channel changes with time).

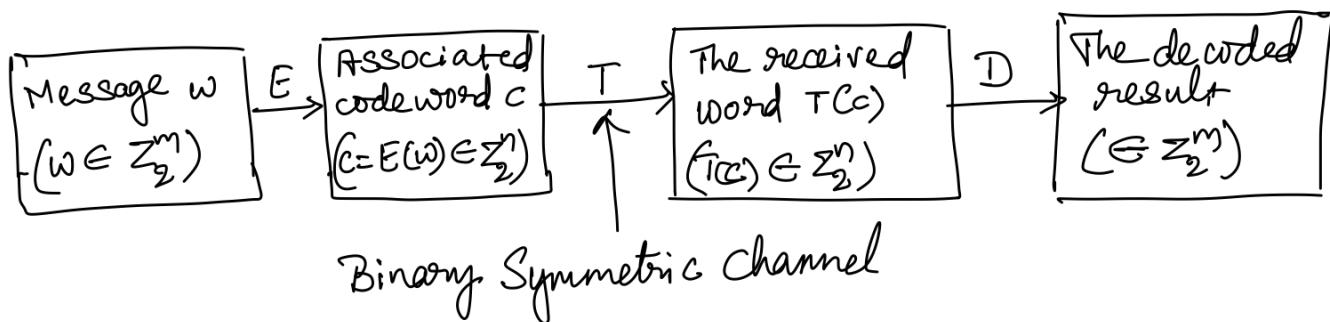
Upon receiving $T(c)$, we want to apply a decoding function $D: \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ to remove the extra signal and, we hope, obtain the original message w .

Ideally $D \circ E$ should be the identity function on W , with $D: C \rightarrow W$. Since this cannot be expected, we seek functions E and D such that there is a high probability of correctly decoding the received word $T(c)$ and recapturing the original message w .

In addition, we want the ratio $\frac{m}{n}$ to be as large as possible so that an excessive number of signals are not appended to w in getting the code word $c = E(w)$. This ratio $\frac{m}{n}$ measures the efficiency of our scheme and is called the rate of the code.

Finally, the functions E and D should be more theoretical results; they must be practical in the sense that they can be implemented electronically.

In such a scheme, the functions E and D are called the encoding and decoding functions, respectively, of an (n, m) block code.



Parity-check code

Consider the $(m+1, m)$ block code for $m=8$.

Let $\mathcal{W} = \mathbb{Z}_2^8$. For any $w = w_1 w_2 \dots w_8 \in \mathcal{W}$, define

$$E: \mathbb{Z}_2^8 \rightarrow \mathbb{Z}_2^9 \text{ by } E(w) = w_1 w_2 \dots w_8 w_9,$$

where $w_9 = \sum_{i=1}^8 w_i$, with the addition performed modulo 2.

$$\text{e.g. } E(11001101) = 110011011, E(00110011) = 001100110$$

For all $w \in \mathbb{Z}_2^8$, $E(w)$ contains an even number of 1's.

So for $w = 11010110$ and $E(w) = 110101101$, if we receive

$T(c) = T(E(w))$ as 100101101, from the odd number of 1's in $T(c)$ we know that a mistake has occurred in transmission. Hence we are able to detect single errors in transmission.

The probability of sending the code word 110101101 and making at most one error in transmission is

$$\underbrace{(1-p)^9}_{\substack{\text{all bits transmitted} \\ \text{correctly}}} + \underbrace{{}^9 C_1 p(1-p)^8}_{\substack{\text{an error is detected} \\ \text{at one position.}}}$$

$$\text{For } p=0.001, \text{ the probability is } (0.999)^9 + {}^9 C_1 (0.001)(0.999)^8 \\ = 0.999964$$

If we detect an error and we are able to relay a signal back to the transmitter to repeat the transmission of the code word, and continue this process until the received word has an even number of 1's, then the probability of sending the code word 110101101 and receiving the correct transmission is approximately 0.999964.

If an even ~~positive~~ number of ~~errors~~ ones occur in transmission, $T(c)$ is accepted as the correct word and we interpret its first eight components as the original message.

This scheme is called the $(m+1, m)$ parity-check code (even parity-check code as we are looking for even number of ones to occur) and is appropriate only when multiple errors are not likely to occur.

If we send the message 1010110 through the channel, we have probability $(0.999)^8 = 0.992028$ of correct transmission.

By using this parity-check code, we increase our chances of getting the correct message to approximately 0.999964.

However (i) an extra signal is sent (perhaps additional transmission are required)

(ii) the rate of code has decreased from 1 to $\frac{8}{9}$.

Note :

1. If we are looking for an even number of ones to occur in $T(c)$, then its called even parity check code.
2. If we are looking for an odd number of ones to occur in $T(c)$, then its called odd parity check code.

example
 Suppose 160 bits are sent, in successive strings of length 8. Find the probability of receiving the correct message (i) without any coding scheme, (ii) with the parity-check method. Assume $p = 0.001$

$$(i) \text{ with the parity-check method. Assume } p = 0.001$$

$$\text{Sol}^n P(\text{receiving correct message}) = (0.999)^{160} = 0.852076.$$

$$(ii) P(\text{receiving correct message})$$

$$= (0.99964)^{20} = 0.999280$$

* Suppose the message $w = 110101$ is sent. Find the probability of receiving the correct message (i) without any coding scheme; (ii) with the parity-check method. Assume $p = 0.05$.

$$(i) \text{ Probability (receiving correct code without any coding method)} = (0.95)^6 = 0.7351$$

(ii) In the parity-check method, we append a bit to the code word, such that the new code has even number of 1's.

$$\therefore \text{the new code } c = 1101010$$

$$-\text{Probability (receiving correct code with parity-check method)} = (0.95)^7 + 2, (0.05)(0.95)^6 = 0.9556$$

* For the given codes, apply (i) the even parity check and (ii) the odd parity check and hence write the transmitted code.

$$(a) w = 1011, (b) w = 1010, (c) 101101, (d) 110111$$

code word	even parity	odd parity
(a) 1011	10111	10110
(b) 1010	10100	10101
(c) 101101	1011010	1011011
(d) 110111	1101111	1101110

* For the code 101101, apply the odd parity check.
 If the following codes are received, determine whether the received codes are correct or not and whether the error is detected or not.

$$\textcircled{i} r = 1011011, \textcircled{ii} r = 1111011, \textcircled{iii} r = 1001111$$

^{soln} original code (w)	transmitted code after odd parity (c)	received code (r ₂)	error in received code Yes/No	If there is error, is error detected Yes/No
\textcircled{i} 101101	1011011	1011011	No	—
\textcircled{ii} 101101	1011011	1\underline{1}11011	Yes	Yes
\textcircled{iii} 101101	1011011	10\underline{0}1111	Yes	No (as there are odd number of ones in both c and r ₂)

* For the code 110111 apply the even parity check.

If the following codes are received, determine whether the received codes are correct or not and whether the error is detected or not.

$$\textcircled{i} r = 1101111, \textcircled{ii} r = 1100111, \textcircled{iii} r = 1001011$$

^{soln} original code (w)	transmitted code after odd parity (c)	received code (r ₂)	error in received code Yes/No	If there is error, is error detected Yes/No
\textcircled{i} 110111	1101111	1101111	No	—
\textcircled{ii} 110111	1101111	110\underline{0}111	Yes	Yes
\textcircled{iii} 110111	1101111	1\underline{0}01011	Yes	No (as there are even number of ones in both c and r ₂)

Triple repetition code:

The $(3m, m)$ triple repetition code is one where we can both detect and correct single errors in transmission.

With $m=8$ and $W = \mathbb{Z}_2^8$, we define $E: \mathbb{Z}_2^8 \rightarrow \mathbb{Z}_2^{24}$ by $E(w_1, w_2, \dots, w_8) = w_1 w_2 \dots w_8 w_1 w_2 \dots w_8 w_1 w_2 \dots w_8$.

⇒ If $w = 10110111$, then $c = E(w) = 1011011101101110110111$

The decoding function $D: \mathbb{Z}_2^{24} \rightarrow \mathbb{Z}_2^8$ is carried out by the majority rule.

⇒ If $T(c) = 10100111001101110110110$, then we have errors occurring in positions 4, 9 and 24.

We decode $T(c)$ by examining the first, ninth and seventeenth positions to see what signal appears more times.

Here it is 1 (which occurs twice), so we decode the first entry in the decoded message as 1.

Continuing with the entries in the second, tenth and eighteenth positions, the result for the second entry of the decoded message is 0 (which occurs all three times).

3rd, 11th and 19th positions are 1, 1, 1, so decoded message is 1

4th, 12th and 20th positions are 0, 1, 1, so decoded message is 1

5th, 13th and 21st positions are 0, 0, 0, so decoded message is 0

6th, 14th and 22nd positions are 1, 1, 1, so decoded message is 1

7th, 15th and 23rd positions are 1, 1, 1, so decoded message is 1

8th, 16th and 24th positions are 1, 1, 0, so decoded message is 1

So the decoded message is 10110111

Although we have more than one transmission error here, it is acceptable, as the two errors occur after eight or sixteen spaces after the first, i.e., the two incorrect transmissions occur for the same bit of the original message.

With $p=0.001$, the probability of correctly decoding a single bit is (by majority rule can make at most 1 error out of 3 positions) $(0.999)^3 + 3 \cdot (0.001)(0.999)^2 = 0.999997$.

So the probability of receiving and correctly decoding the eight-bit message is $(0.999997)^8 = 0.999976$. Here we transmit 24 signals for this message, so the rate is now $\frac{8}{24} = \frac{1}{3}$

- i) The triple repetition code increases the accuracy and ability to detect and correct single errors (from 0.999964 to 0.999976)
- ii) The rate of code has decreased from $\frac{8}{9}$ to $\frac{1}{3}$.
- iii) But we do not waste time with retransmission.

Examples

1. Let $E: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^9$ be the encoding function for the triple repetition code.

(a) triple repetition code.
 (b) If $D: \mathbb{Z}_2^9 \rightarrow \mathbb{Z}_2^3$ is the corresponding decoding function,
 apply D to decode the received words (i) 111101100,

(ii) 010011111.

(c) Find three different received words r for which

$$D(r) = 000.$$

(d) For each $w \in \mathbb{Z}_2^3$, what is $|D^{-1}(w)|$?

$$(a) r_1 = 111101100$$

1st, 4th and 7th positions have 1, 1, 1 \therefore decoded message is 1

2nd, 5th and 8th positions have 1, 0, 0 \therefore decoded message is 0

3rd, 6th and 9th positions have 1, 1, 0 \therefore decoded message is 1

\therefore the final decoded word is 101

$$r_2 = 010011111$$

1st, 4th and 7th positions have 0, 0, 1 \therefore decoded message is 0

2nd, 5th and 8th positions have 1, 1, 1 \therefore decoded message is 1

3rd, 6th and 9th positions have 0, 1, 1 \therefore decoded message is 1

\therefore the final decoded word is 011

$$(b) D(r) = 000$$

\therefore in the 1st, 4th and 7th positions, 0 should be majority.

2nd, 5th and 8th positions, 0 should be majority.

3rd, 6th and 9th positions, 0 should be majority.

\therefore the possible received messages are

$$000000000, 100000000, 010000000$$

$$(c) D: \mathbb{Z}_2^9 \rightarrow \mathbb{Z}_2^3 \quad |\mathbb{Z}_2^9| = 512, \quad |\mathbb{Z}_2^3| = 8$$

$$\therefore \forall w \in \mathbb{Z}_2^3 \quad |D^{-1}(w)| = \frac{|\mathbb{Z}_2^9|}{|\mathbb{Z}_2^3|} = 64.$$

* The $(5m, m)$ five-times repetition code has encoding function $E: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^{5m}$, where $E(w) = wwww$. Decoding with $\mathbb{Z}_2^{5m} \rightarrow \mathbb{Z}_2^m$ is accomplished by the majority rule (here we are able to correct single and double errors made in transmission).

(a) With $p=0.05$, what is the probability for the transmission and correct decoding of the signal 0 ?

(b) Answer part (a) for the message 110 in place of the signal 0 .

(c) For $m=2$, decode the received word $r = 0111001001$.

(d) If $m=2$, find three received words r where $D(r)=00$.

(e) For $m=2$ and $D: \mathbb{Z}_2^{10} \rightarrow \mathbb{Z}_2^2$, what is $|D^{-1}(w)|$ for each $w \in \mathbb{Z}_2^2$?

Sol (a) Here $w=0$, $\therefore E: \mathbb{Z}_2^1 \rightarrow \mathbb{Z}_2^5$, $\therefore T(w) = 00000$ then $D: \mathbb{Z}_2^5 \rightarrow \mathbb{Z}_2^1$

With $p=0.05$, the probability of correctly decoding a single bit is (by majority rule can make at most 2 error out of 5 positions)

$$(0.95)^5 + {}^5C_1(0.05)(0.95)^4 + {}^5C_2(0.05)^2(0.95)^3 = 0.998842$$

So the probability of receiving and correctly decoding the one-bit message is $(0.998842)^1 = 0.998842$.

(b) Here $w=110$, $E: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^{15}$, $\therefore T(w) = 110110110$ then $D: \mathbb{Z}_2^{15} \rightarrow \mathbb{Z}_2^3$

With $p=0.05$, the probability of correctly decoding a single bit is (by majority rule can make at most 2 error out of 5 positions)

$$(0.95)^5 + {}^5C_1(0.05)(0.95)^4 + {}^5C_2(0.05)^2(0.95)^3 = 0.998842$$

So the probability of receiving and correctly decoding the three-bit message is $(0.998842)^3 = 0.996530$

c) with $m=2$, received word $r = 0111001001$.

The 1st, 3rd, 5th, 7th and 9th positions have 0, 1, 0, 1, 0
by majority rule the correct message is 0

The 2nd, 4th, 6th, 8th and 10th positions have 1, 1, 0, 0, 1
by majority rule the correct message is 1

The decoded message is 01.

d) $m=2$, and $D(r)=00$, the received word r is

0000000000, 0000000011, 1100000000

e) $m=2$, $D: \mathbb{Z}_2^{10} \rightarrow \mathbb{Z}_2^2$

for each $w \in \mathbb{Z}_2^2$, $|D^{-1}(w)| = \frac{|\mathbb{Z}_2^{10}|}{|\mathbb{Z}_2^2|} = 256$.

Error-detecting and error-correcting capabilities of a coding scheme.

Consider a code $C \subseteq \mathbb{Z}_2^4$, where $c_1 = 0111$, $c_2 = 1111 \in C$. Both the transmitter and the receiver know the elements of C . So if the transmitter sends c_1 , but the person receiving the code word receives $T(c_1)$ as 1111, makes whatever decision (a wrong one) c_2 implies. Consequently, although only one transmission error was made, the result could be unpleasant.

Unfortunately we have two code words that are almost the same. They are rather close to each other, for they differ in only one component.

weight of an element, distance between two elements.

For any element $\mathbf{x} = x_1 x_2 \dots x_n \in \mathbb{Z}_2^n$, where $n \in \mathbb{Z}^+$, the weight of \mathbf{x} , denoted by $wt(\mathbf{x})$, is the number

of components x_i of \mathbf{x} , for $1 \leq i \leq n$, where $x_i = 1$. If $y \in \mathbb{Z}_2^n$, the distance between \mathbf{x} and y , denoted as $d(\mathbf{x}, y)$, is the number of components where $x_i \neq y_i$, for $1 \leq i \leq n$.

$$\therefore \text{For } \mathbf{x}, y \in \mathbb{Z}_2^n, d(\mathbf{x}, y) = \sum_{i=1}^n d(x_i, y_i),$$

$$\text{where for each } 1 \leq i \leq n, d(x_i, y_i) = \begin{cases} 0, & \text{if } x_i = y_i \\ 1, & \text{if } x_i \neq y_i \end{cases}$$

example

* For $n=5$, let $\mathbf{x} = 01001$ and $y = 11101$. Find $wt(\mathbf{x})$, $wt(y)$, $d(\mathbf{x}, y)$, $wt(\mathbf{x} + y)$.

$$\text{So } wt(\mathbf{x}) = 2, \quad wt(y) = 4, \quad d(\mathbf{x}, y) = 2.$$

$$\mathbf{x} + y = 10100, \quad \therefore wt(\mathbf{x} + y) = 2.$$

Lemma: For all $x, y \in \mathbb{Z}_2^n$, $\text{wt}(x+y) \leq \text{wt}(x) + \text{wt}(y)$.

Proof: We prove this lemma by examining, for each $1 \leq i \leq n$, the components $x_i, y_i, x_i + y_i$ of $x, y, x+y$ respectively. Only one situation would cause this inequality to be false: if $x_i + y_i = 1$ while $x_i = 0$ and $y_i = 0$, for some $1 \leq i \leq n$. But this will never occur because $x_i + y_i = 1$ implies that exactly one of x_i and y_i is 1.

Example
Verify $\text{wt}(x+y) \leq \text{wt}(x) + \text{wt}(y)$, for $x = 01001$, $y = 11101$

Sol^m Given $x=01001$, $y=11101$, $\therefore x+y=10100$

$$wt(x) = 2, \quad wt(y) = 4, \quad wt(x+y) = 2$$

and $9 < 2+4$ is true.

$$\text{ie } \text{wt}(x+y) < \text{wt}(x) + \text{wt}(y)$$

Theorem: The distance function d defined on $\Sigma_2^n \times \Sigma_2^n$ satisfies

the following for all $x, y, z \in \Sigma^*$.

(a) $d(x, y) \geq 0$, (b) $d(x, y) = 0$ iff $x = y$, (c) $d(x, y) = d(y, x)$,

$$\textcircled{d} \quad d(x, z) \leq d(x, y) + d(y, z)$$

Proof: (a) $d(x, y) = \sum_{i=1}^n d(x_i, y_i) = 0$ if $x_i = y_i \forall 1 \leq i \leq n$.
 $\quad\quad\quad > 1$ if there is at least one $x_i \neq y_i$.

$\therefore d(x, y) \geq 0$

b) Let $d(x, y) = 0 \Rightarrow \sum_{i=1}^n d(x_i, y_i) = 0 \Rightarrow x_i = y_i \text{ for } 1 \leq i \leq n, \text{ i.e. } x = y$

Let $x = y$, then $x_i = y_i \forall 1 \leq i \leq n \Rightarrow \sum_{i=1}^n d(x_i, y_i) = 0 \Rightarrow d(x, y) = 0$

$$\textcircled{2} \text{ let } d(x, y) = \sum_{i=1}^n d(x_i, y_i) = \sum_{i=1}^n d(y_i, x_i) = d(y, x)$$

$$\text{(d) In } \mathbb{Z}_2^n \quad y + y = 0 \quad \therefore d(x, z) = \text{wt}(x + z) = \text{wt}(x + y + y + z) \\ \leq \text{wt}(x + y) + \text{wt}(y + z) \quad (\text{by lemma}) \\ \equiv d(x, y) + d(y + z)$$

Hamming metric

When a function satisfies the four properties

- (a) $d(x, y) \geq 0$,
- (b) $d(x, y) = 0$ iff $x = y$,
- (c) $d(x, y) = d(y, x)$,
- (d) $d(x, z) \leq d(x, y) + d(y, z)$, then it is called a distance function or metric, and we call (\mathbb{Z}_2^n, d) a metric space. Hence d (as given above) is often referred to as the Hamming metric.

Sphere of radius k

For $n, k \in \mathbb{Z}^+$ and $x \in \mathbb{Z}_2^n$, the sphere of radius k centered at x is defined as $S(x, k) = \{y \in \mathbb{Z}_2^n \mid d(x, y) \leq k\}$.

example For $n=3$ and $x=110 \in \mathbb{Z}_2^3$, find $S(x, 1)$ and $S(x, 2)$.

* For $n=3$ and $x=110 \in \mathbb{Z}_2^3$, find $S(x, 1)$ and $S(x, 2)$.

Sol) $S(x, 1) = \{y \in \mathbb{Z}_2^3 \mid d(x, y) \leq 1\} = \{110, 010, 100, 111\}$

$S(x, 2) = \{y \in \mathbb{Z}_2^3 \mid d(x, y) \leq 2\} = \{110, 010, 100, 111, 000, 101, 011\}$.

Theorem 1 Let $E: W \rightarrow C$ be an encoding function with the set of messages $W \subseteq \mathbb{Z}_2^m$ and the set of code words $E(W) = C \subseteq \mathbb{Z}_2^n$ where $m < n$. For $k \in \mathbb{Z}^+$, we can detect transmission errors of weight $\leq k$ if and only if the minimum distance between code words is at least $k+1$.

Theorem 2 Let $E: W \rightarrow C$ be an encoding function with the set of messages $W \subseteq \mathbb{Z}_2^m$ and the set of code words $E(W) = C \subseteq \mathbb{Z}_2^n$ where $m < n$, and $k \in \mathbb{Z}^+$ then we can construct a decoding function $D: \mathbb{Z}_2^n \rightarrow W$ that corrects all transmission errors of weight $\leq k$ if and only if the minimum distance between code words is at least $2k+1$.

example

* With $W = \mathbb{Z}_2^6$, let $E: W \rightarrow \mathbb{Z}_2^6$ be given by

$$E(00) = \underset{r_1}{000000}, E(10) = \underset{r_2}{101010}, E(01) = \underset{r_3}{010101}, E(11) = \underset{r_4}{111111}$$

$$d(r_1, r_2) = 3, d(r_1, r_3) = 3, d(r_1, r_4) = 6, d(r_2, r_3) = 6, d(r_2, r_4) = 3, d(r_3, r_4) = 3$$

The minimum distance between the code words is 3.

by Theorem 1, $k+1=3 \Rightarrow k=2$, by Theorem 2, $2k+1=3 \Rightarrow k=1$.
So, we can detect double errors and correct single errors.

$$\text{with } S(000000, 1) = \{x \in \mathbb{Z}_2^6 \mid d(000000, x) \leq 1\}$$

$$= \{000000, 100000, 010000, 001000, 000100, 000010, 000001\}$$

the decoding function $D: \mathbb{Z}_2^6 \rightarrow W$ gives $D(x) = 00 \quad \forall x \in S(000000, 1)$
[By majority rule at (1st, 3rd, 5th) positions and (2nd, 4th, 6th) positions].

$$\text{with } S(010101, 1) = \{x \in \mathbb{Z}_2^6 \mid d(010101, x) \leq 1\}$$

$$= \{010101, 110101, 000101, 011101, 010001, 010111, 010100\}$$

and here $D(x) = 01 \quad \forall x \in S(010101, 1)$. [by majority rule]
We observe that the definition of D accounts for

$$7 + 7 = 14 \quad [7 \text{ from } S(000000, 1) \text{ & } 7 \text{ from } S(010101, 1)]$$

of the elements of \mathbb{Z}_2^6 . Similarly $S(101010) \cap S(111111)$ contributes 14 more elements of \mathbb{Z}_2^6 to the definition of D.

Since $|\mathbb{Z}_2^6| = 64$, there remains 36 ($64 - 28$) other elements to account for.

We define $D(x) = 00$ for any other message for these 36 other elements and have a decoding function that will correct single errors.

With regard to detection, if $c = 010101$ and $T(c) = r_2 = 111101$, we can detect this double error because r_2 is not a code word.

But if $T(c) = r_1 = 111111$, a triple error has occurred, so we think that $c = 111111$ and incorrectly decode r_1 as 11, instead of as the correct message 01.

* With $W = \Sigma_2^2$, let $E: W \rightarrow \Sigma_2^6$ be given by
 $E(00) = 000000$, $E(10) = 101010$, $E(01) = 010101$, $E(11) = 111111$
List the elements in $S(101010, 1)$ and $S(111111, 1)$.

Soln $S(101010, 1) = \{x \in \Sigma_2^6 \mid d(101010, x) \leq 1\}$
 $= \{101010, 001010, 111010, 100010, 101110, 101000, 101011\}$

$S(111111, 1) = \{x \in \Sigma_2^6 \mid d(111111, x) \leq 1\}$
 $= \{111111, 011111, 101111, 110111, 111011, 111101, 111110\}$

* With $W = \Sigma_2^2$, let $E: W \rightarrow \Sigma_2^6$ be given by
 $E(00) = 000000$, $E(10) = 101010$, $E(01) = 010101$, $E(11) = 111111$

Decode each of the following received word

(a) 110101, (b) 101011, (c) 001111, (d) 110000.

Soln (a) 110101 majority at 1st, 3rd & 5th position is 0
majority at 2nd, 4th & 6th position is 1

\therefore the decoded word is 01.

(b) 101011 majority at 1st, 3rd & 5th position is 1
majority at 2nd, 4th & 6th position is 0

\therefore the decoded word is 10

(c) 001111 majority at 1st, 3rd & 5th position is 1
majority at 2nd, 4th & 6th position is 1

\therefore the decoded word is 11.

(d) 110000 majority at 1st, 3rd & 5th position is 0
majority at 2nd, 4th & 6th position is 0

\therefore the decoded word is 00

- * (a) If $x \in \mathbb{Z}_2^{10}$, determine $|S(x,1)|$, $|S(x,2)|$, $|S(x,3)|$.
 (b) For $n, k \in \mathbb{Z}^+$, with $1 \leq k \leq n$, if $x \in \mathbb{Z}_2^n$, what is $|S(x,k)|$?

Solⁿ $S(x,1) = \{y \in \mathbb{Z}_2^{10} \mid d(x,y) \leq 1\}$
 $= \{y \in \mathbb{Z}_2^{10} \mid d(x,y) = 0 \text{ or } d(x,y) = 1\}$

for $d(x,y)=0$, y should be same as x , there is only one such possibility
 for $d(x,y)=1$, y should differ from x , at only one position, and
 there are ${}^{10}C_1 = 10$ such possibilities.

$$\therefore |S(x,1)| = 1 + 10 = 11$$

$$S(x,2) = \{y \in \mathbb{Z}_2^{10} \mid d(x,y) \leq 2\} = \{y \in \mathbb{Z}_2^{10} \mid d(x,y) = 0 \text{ or } d(x,y) = 1 \text{ or } d(x,y) = 2\}$$

for $d(x,y)=0$, there is only one possibility.

for $d(x,y)=1$, there are 10 possibilities.

for $d(x,y)=2$, y should differ from x , at only two positions,
 and there are ${}^{10}C_2 = 45$ possibilities

$$\therefore |S(x,2)| = 1 + 10 + 45 = 56$$

$$\text{Similarly } |S(x,3)| = 1 + {}^{10}C_1 + {}^{10}C_2 + {}^{10}C_3 = 176$$

(b) with $1 \leq k \leq n$, for $x \in \mathbb{Z}_2^n$,

$$|S(x,k)| = 1 + {}^nC_1 + {}^nC_2 + \dots + {}^nC_k = \sum_{i=0}^k {}^nC_k$$

* Let $E: \mathbb{Z}_2^5 \rightarrow \mathbb{Z}_2^{25}$ be an encoding function where the minimum distance between code words is 9. What is the largest value of k such that we can detect errors of weight $\leq k$? If we wish to correct errors of weight $\leq n$, what is the maximum value of n ?

Solⁿ We can use Theorem 1 to find k . $\therefore k+1=9 \Rightarrow k=8$

We can use Theorem 2 to find n . $\therefore 2n+1=9 \Rightarrow n=4$

* For each of the following encoding functions, find the minimum distance between the code words. Discuss the error-detecting and error-correcting capabilities of each code.

$$\textcircled{a}: E: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^5$$

$$00 \rightarrow 00001, 01 \rightarrow 01010, 10 \rightarrow 10100, 11 \rightarrow 11111$$

$$\textcircled{b} E: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^{10}$$

$$00 \rightarrow 0000000000 \quad 01 \rightarrow 0000011111 \\ 10 \rightarrow 1111100000 \quad 11 \rightarrow 1111111111$$

$$\textcircled{c} E: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^6$$

$$000 \rightarrow 000111 \quad 001 \rightarrow 001001 \quad 010 \rightarrow 010010 \quad 011 \rightarrow 011100 \\ 100 \rightarrow 100100 \quad 101 \rightarrow 101010 \quad 110 \rightarrow 110001 \quad 111 \rightarrow 111000$$

$$\textcircled{d} E: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^8$$

$$000 \rightarrow 00011111 \quad 001 \rightarrow 00111010 \\ 010 \rightarrow 01010101 \quad 011 \rightarrow 01110000 \\ 100 \rightarrow 10001101 \quad 101 \rightarrow 10101000 \\ 110 \rightarrow 11000100 \quad 111 \rightarrow 11100011$$

Soln

$$\textcircled{a} d(00001, 01010) = 3, d(00001, 10100) = 3, d(00001, 11111) = 4 \\ d(01010, 10100) = 4, d(01010, 11111) = 3, d(10100, 11111) = 3$$

∴ minimum distance between code words is 3.

Applying Theorem 1 $k+1=3 \Rightarrow k=2$

∴ the code can detect all errors of weight ≤ 2 .

Apply Theorem 2 $2k+1=3 \Rightarrow k=1$

∴ the code can correct all errors of weight ≤ 1

- ⑥ Let the code words be denoted as follows:
 $r_1 = 0000000000$, $r_2 = 0000011111$, $r_3 = 111110000000$, $r_4 = 1111111111$
 $d(r_1, r_2) = 5$, $d(r_1, r_3) = 5$, $d(r_1, r_4) = 10$, $d(r_2, r_3) = 10$, $d(r_2, r_4) = 5$,
 $d(r_3, r_4) = 5$

∴ minimum distance between code words is 5.

Applying Theorem 1 $k+1=5 \Rightarrow k=4$

∴ the code can detect all errors of weight ≤ 4 .

Apply Theorem 2 $2k+1=5 \Rightarrow k=2$

∴ the code can correct all errors of weight ≤ 2

- ⑦ Let the code words be denoted as follows:

- $r_1 = 000111$, $r_2 = 001001$, $r_3 = 010010$, $r_4 = 011100$,
 $r_5 = 100100$, $r_6 = 101010$, $r_7 = 110001$, $r_8 = 111000$

	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8
r_1	*	3	3	4	3	4	4	6
r_2	3	*	4	3	4	3	3	3
r_3	3	4	*	3	4	3	3	3
r_4	4	3	3	*	3	4	4	2
r_5	3	4	4	3	*	3	3	3
r_6	4	3	3	4	3	*	4	2
r_7	4	3	3	4	3	4	*	2
r_8	6	3	3	2	3	2	2	*

∴ minimum distance between code words is 2.

Applying Theorem 1 $k+1=2 \Rightarrow k=1$

the code can detect all errors of weight ≤ 1

Apply Theorem 2 $2k+1=2 \Rightarrow k=\frac{1}{2}$

the code can correct all errors of weight $\leq \frac{1}{2}$
 i.e. the code cannot correct any error

In this section the encoding and decoding functions are given by matrices over \mathbb{Z}_2 . One of these matrices will help us to locate the nearest code word for a given received word. This will be especially helpful as the set C of code words grows larger.

Let $G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ be a 3×6 matrix over \mathbb{Z}_2 .

The first 3 columns of G_1 form the 3×3 identity matrix. Letting A denote the matrix formed from the last three columns of G_1 , we write $G_1 = [I_3 | A]$ to denote its structure. The (partitioned) matrix G_1 is called a generator matrix.

G_1 is used to define an encoding function $E: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^6$ as follows:

For $w \in \mathbb{Z}_2^3$, $E(w) = wG_1$ is the element in \mathbb{Z}_2^6 obtained by multiplying w , considered as a three-dimensional row vector, by the matrix G_1 on its right. [in the calculations here we have $1+1=0$]

[Even if the set W of messages is not all of \mathbb{Z}_2^3 , we will assume that all of \mathbb{Z}_2^3 is encoded and that the transmitter and receiver will both know the real messages of importance and their corresponding code words.]

$$E[110] = (110)G_1 = [110] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [110101],$$

$$E[010] = (010)G_1 = [010] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [010011]$$

Note that $E[110]$ is obtained by adding first two rows of G_1 , whereas $E[010]$ is simply the second row of G_1 .

So for $w = \{000, 100, 010, 001, 110, 101, 011, 111\}$ the codewords are $C = \{000000, 100110, 010011, 001101, 110101, 101011, 011110, 111000\}$ and one can recapture the corresponding message $\in \mathbb{Z}_2^6$ by simply dropping the last three components of the codeword. In addition the minimum distance between code words is 3, so we can detect errors of weight ≤ 2 and correct single errors.

For any $w = w_1 w_2 w_3 \in \mathbb{Z}_2^3$, $E(w) = w_1 w_2 w_3 w_4 w_5 w_6 \in \mathbb{Z}_2^6$.

Since $E(w) = [w_1 w_2 w_3] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} = [w_1 w_2 w_3 (w_1 + w_3)(w_1 + w_2)(w_2 + w_3)]$

$\Rightarrow w_4 = w_1 + w_3$, $w_5 = w_1 + w_2$, $w_6 = w_2 + w_3$ and these equations are called the parity-check equations.

Since $w_i \in \mathbb{Z}_2$, for each $1 \leq i \leq 6$, $w_i = -w_i$.

So the above equations can be written as

$$\left. \begin{array}{l} w_1 + w_3 - w_4 = 0 \\ w_1 + w_2 - w_5 = 0 \\ w_2 + w_3 - w_6 = 0 \end{array} \right\} \quad \begin{array}{l} w_1 + 0 + w_3 + w_4 + 0 + 0 = 0 \\ w_1 + w_2 + 0 + 0 + w_5 + 0 = 0 \\ 0 + w_2 + w_3 + 0 + 0 + w_6 = 0 \end{array}$$

Hence $\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Or $H(E(w))^{tr} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, where $(E(w))^{tr}$ denotes the transpose of $E(w)$.

Consequently, if $r = r_1 r_2 \dots r_6 \in \mathbb{Z}_2^6$, we can identify r as a code word if and only if $H \cdot r^{tr} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Writing $H = [B | I_3]$, we notice that if the rows and columns of B are interchanged, then we get A . Hence $B = A^{tr}$

Since the minimum distance between the code words of this example is 3, we should be able to develop a decoding function that corrects single errors.

Suppose we receive $r = 110110$

We want to find the code word c that is the nearest neighbour of r .

If there is a long list of code words against which to check r , we would be better off to first examine

$H \cdot r^+$, which is called the syndrome of r .

Here

$$H \cdot r^+ = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$\therefore r$ is not a code word.

(is the second column of H)

We want to at least detect an error

We know the code words are

$$C = \{000000, 100110, 010011, 001101, 110101, 101011, 011110, 111000\}$$

$$\begin{matrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \end{matrix}$$

The received word is $r = 110110$

$$d(c_1, r) = 4, d(c_2, r) = 1, d(c_3, r) = 3, d(c_4, r) = 5, d(c_5, r) = 2, d(c_6, r) = 4, \\ d(c_7, r) = 2, d(c_8, r) = 3$$

$\therefore d(100110, r) = 1$ is the minimum.

Writing $r = c + e = 100110 + 010000$, we find that the transmission error occurs in the second component of r .

Changing the second component of r , we get c ; the message w comprises of first three components of c .

Let $r = c + e$, where c is a code word and e is an error pattern of weight 1.

Suppose that 1 is in the i^{th} component of e , where $1 \leq i \leq 6$.

$$\text{Then } H \cdot r^{+r} = H \cdot (c + e)^{+r} = H \cdot (c^{+r} + e^{+r}) = H \cdot c^{+r} + H \cdot e^{+r}$$

With c a code word, it follows that $H \cdot c^{+r} = 0$,

so $H \cdot r^{+r} = H \cdot e^{+r} = i^{\text{th}}$ column of matrix H .

Thus c and r differ only in the i^{th} component, and we can determine c by simply changing the i^{th} component of r .

Correct multiple errors

Suppose we receive $r = 000111$.

$$\text{Then } H \cdot r^{+r} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \text{ which is not a column of } H.$$

Yet $H \cdot r^{+r}$ can be obtained as the sum of two columns of H . If $H \cdot r^{+r}$ came from the first and sixth columns of H , correcting these components in r results in the code word 100110.

If we sum the third and fifth columns of H to get this syndrome, upon changing the third and fifth component of r we get a second code word, 001101.

So we cannot expect H to correct multiple errors.

[This is no surprise, since the minimum distance between code words is 3 $\Rightarrow 2k+1=3 \Rightarrow k=1$, the code can correct errors of at most 1]

Parity-check matrix and Generator matrix

For $m, n \in \mathbb{Z}^+$ with $m < n$, the encoding function $E: \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ is given by an $m \times n$ matrix G over \mathbb{Z}_2 . The matrix G is called the generator matrix for the code and has the form $[I_m | A]$, where A is an $m \times (n-m)$ matrix.

Here, $E(w) = wG$ for each message $w \in \mathbb{Z}_2^m$,

$$A = E(\mathbb{Z}_2^m) \subset \mathbb{Z}_2^n.$$

and the code $C = E(\mathbb{Z}_2^m) \subset \mathbb{Z}_2^n$. The associated parity-check matrix H is an $(n-m) \times n$ matrix of the form $[A^T | I_{n-m}]$.

This matrix can also be used to define the encoding function E , because if $w = w_1 w_2 \dots w_m \in \mathbb{Z}_2^m$, then $E(w) = w_1 w_2 \dots w_m w_{m+1} \dots w_n$, where $w_{m+1} \dots w_n$ can be determined from the set of $n-m$ (parity-check) equations that arise from $H \cdot (E(w))^T = 0$, the column vector of $n-m$ 0's.

This unique parity-check matrix H also provides a decoding scheme that corrects single errors in transmission if:

① H does not contain a column of 0's.

[If the i^{th} column of H had all 0's and $H \cdot r^T = 0$ for a received word r , we couldn't decide whether r was a code word or a received word whose i^{th} component was incorrectly transmitted. We do not want to compare r with all code words when C is large.]

② No two columns of H are the same.

[If the i^{th} and j^{th} columns of H are the same and $H \cdot r^T$ equals this repeated column, then how would we decide which component of r to change?]

When H satisfies the above two conditions, we get the following decoding algorithm.

For any $r \in \mathbb{Z}_2^n$, if $T(c) = r$, then:

1. With $H \cdot r^{+r} = 0$, we feel that the transmission was correct and that r is the code word that was transmitted. The decoded message then consists of the first m components of r .
2. With $H \cdot r^{+r}$ equal to the i^{th} column of H , we feel that there has been a single error in transmission and change the i^{th} component of r in order to get the code word c . Here the first m components of c yield the original message.
3. If neither case 1 nor case 2 occurs, we feel that there has been more than one transmission error and we cannot provide a reliable way to decode in this situation.

Note: If we start with a parity-check matrix $H = [B | I_{n-m}]$ and use it, as described above, to define the function E , then we obtain the same set of code words that is generated by the unique associated generator matrix $G = [I_m | B^{+r}]$.

examples
for
① Use the parity-check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$

to decode the following received words.

- ① $\begin{array}{c} 111101 \\ R_1 \end{array}$, ② $\begin{array}{c} 110101 \\ R_2 \end{array}$, ③ $\begin{array}{c} 001111 \\ R_3 \end{array}$, ④ $\begin{array}{c} 100100 \\ R_4 \end{array}$
- ⑤ $\begin{array}{c} 110001 \\ R_5 \end{array}$, ⑥ $\begin{array}{c} 111111 \\ R_6 \end{array}$, ⑦ $\begin{array}{c} 111100 \\ R_7 \end{array}$, ⑧ $\begin{array}{c} 010100 \\ R_8 \end{array}$.

② Are all the results in part ① uniquely determined?

SOL Consider $H \cdot R_1^{tr}$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad \therefore H \cdot R_1^{tr} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

Similarly we can obtain all other decoded words.

③ The decoded words are

- ① 101 , ② 000 , ③ 010 , ④ 010 , ⑤ 100 , ⑥ 111 , ⑦ 100 , ⑧ 111
- 3rd column no error 5th column single error 5th column single error 6th column single error sum of 1st 4th column sum of 1st 4th column 2 errors 2 errors 2 errors 2 errors

received word	correction at position	decoded word	considering 1st 3 bits of decoded word
① 111101	3rd	110101	110
② 110101	nil	110101	110
③ 001111	5th	001101	001
④ 100100	5th	100110	100
⑤ 110001	4th	110101	110
⑥ 111111	1st & 6th	011110 (there are other possibilities)	011
⑦ 111100	4th	111000	111
⑧ 010100	1st & 6th	110101 (there are other possibilities)	110

② No, not all results are uniquely determined
⑨ & ⑩ received words have other possibilities.

* The encoding function $E: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^5$ is given by the generator matrix $G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.

(a) Determine all code words. What can we say about the error-detection capability of this code? What about its error-correction capability?

(b) Find the associated parity-check matrix H .

(c) Use H to decode each of the following received

words. (i) 11011, (ii) 10101, (iii) 11010
 (iv) 00111, (v) 11101, (vi) 00110.

$$\text{Soln. } w = \{00, 10, 01, 11\}$$

$$\text{ex } c = wG = \begin{bmatrix} 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = 00000$$

$$\therefore C = \left\{ \underset{c_1}{00000}, \underset{c_2}{10110}, \underset{c_3}{01011}, \underset{c_4}{11101} \right\}$$

$d(c_1, c_2) = 3, d(c_1, c_3) = 3, d(c_1, c_4) = 4, d(c_2, c_3) = 4, d(c_2, c_4) = 3, d(c_3, c_4) = 3$.
 The minimum distance between code words is 3.

The code can detect all errors of weight ≤ 2 ($\because k+1=3 \Rightarrow k=2$) and correct all single ($\because 2k+1=3 \Rightarrow k=1$) errors.

(b) Here $E: \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^5 \quad \therefore m=2, n=5 \quad G = [I_2 | A]$

$$\therefore H = [A^{tr} | I_3] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{where } A = \begin{bmatrix} 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

(c) Given (i) 11011, (ii) 10101, (iii) 11010, (iv) 00111, (v) 11101, (vi) 00110
 using $H \cdot R^{tr}$ - decoded words are 110, 011, 111, 111, 000, 110
 errors happening at 1st, 2nd, (1st & 5th), (1st & 5th), nil, 1st positions
 decoded words after correction are
 01011, 11101, 01011, 10110, 11101, 10110
 Considering the first 2 bits, the decoded words are
 01, 11, 01, 10, 11, 10

* Define the encoding function $E: \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^6$ by means of the parity-check matrix

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(a) Determine all code words.

(b) Does this code correct all single errors in transmission?

Sol'

Given

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

If $r = r_1 r_2 r_3 r_4 r_5 r_6 \in \mathbb{Z}_2^6$, r is identified as a code word iff

$$H \cdot r^{+r} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \text{ i.e. } \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ r_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\Rightarrow r_1 + 0 + r_3 + r_4 + 0 + 0 = 0 \Rightarrow r_4 = r_1 + r_3$$

$$r_1 + r_2 + 0 + 0 + r_5 + 0 = 0 \Rightarrow r_5 = r_1 + r_2$$

$$r_1 + 0 + r_3 + 0 + 0 + r_6 = 0 \Rightarrow r_6 = r_1 + r_3$$

with $r_1 r_2 r_3$ as $r_4 r_5 r_6$ is the code word is

r_1	r_2	r_3	r_4	r_5	r_6	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8
0	0	0	0	0	0	000000	-	4	2	3	4	3	5
1	0	0	1	1	1	100111	1	-	4	3	2	3	3
0	1	0	0	1	0	010010	2	4	-	4	3	3	5
0	0	1	1	0	1	001101	3	2	4	-	5	4	3
1	1	0	1	0	1	110101	3	3	5	-	3	4	2
1	0	1	0	1	0	101010	4	2	4	3	-	5	3
0	1	1	1	1	1	011111	3	3	3	4	5	-	4
1	1	1	0	0	0	111000	5	3	3	2	3	4	-

since the minimum distance between code words is 2
 $\Rightarrow 2k+1=2 \Rightarrow k=\frac{1}{2}$, so this code cannot correct single errors in transmission.