MODULE-V

Binary operation on a set

Let G be a non-empty set. Then $G \times G = \{(a,b) : a \in G, b \in G\}$ if $f : G \times G \to G$ then f is said to be a binary operation on the set G.

The image of the ordered pair (a,b) under the function f is denoted by $af b$. Often use symbols $+, \times, \cdot, \circ$ etc. to denote binary operation on G, a set.

Thus '$+$' will be a binary operation on G iff

$a+b \in G \ \forall \ a, b \in G$

& $a+b$ is unique.

Similarly '$*$' will be a binary operation on G iff

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

& $a * b$ is unique.

Ex:→

Addition is binary operation on set N of Natural numbers. The sum of two natural numbers is also a natural number.

i.e. $a+b \in N \quad \forall \quad a, b \in N$

Therefore N is closed with respect to addition.

But subtraction is not a binary operation on N.

We have $4-7 = -3 \notin N$

whereas $4 \in N, \quad 7 \in N$

Thus N is not closed w.r.t. subtraction

But subtraction is a binary operation on the set of integers I,

We have $a-b \in I \quad \forall \quad a, b \in I$.

ALGEBRAIC STRUCTURE/SYSTEM

A non-empty set G equipped with one or more binary operations is called an algebraic structure.

$(N, +)$, $(I, +)$, $(I, -)$, $(R, +, \cdot)$ are all algebraic structure.

Semi-group :→

An algebraic structure $(G, *)$ is called a semi-group if the binary operation $*$ is associative on G.

i.e. if $(a*b)*c = a*(b*c)$ $\forall\ a, b \in G$

$(N, \cdot)$, $(I, +)$ & $(R, +)$ are semi-groups.

Group :→

Let G be a non-empty set equipped with a binary operation denoted by $\cdot$ i.e. $a \cdot b$ or more conveniently ab represents the element of G obtained by applying the said binary operation between the elements a & b of G taken in that order.

1. Closure property i.e. $ab \in G$ $\forall\ a, b \in G$.
2. Associativity $(ab)c = a(bc)$ $\forall\ a, b, c \in G$.
3. Existance of Identity:

$\exists$ an element $e \in G$ s.t. $ea = a = ae$ $\forall\ a \in G$. The element e is called the identity.

4. Existance of Inverse:

Each element of G possesses inverse. In other words $a \in G \Rightarrow \exists$ an element $b \in G$ s.t. $ba = e = ab$. The element b is then called the inverse of a & we write $b = a^{-1}$. Thus a^{-1} is an element of G s.t.

$$a^{-1}a = e = aa^{-1}.$$

Abelian group ... Commutative group

A group is said to be abelian or commutative if in addition to the above four postulates the following postulate is also satisfied.

5. Commutativity $ab = ba \quad \forall a, b \in G$.

Note :-

(1) Let $(A, *)$ be an algebraic structure where $*$ is a binary operation on A. An element e in A is said to be left identity if $\forall x \in A$,

$$e * x = x$$

& right identity if $\forall x \in A$

$$x * e = x.$$

(2) Suppose e_1 is a left identity & e_2 is a right identity of an algebraic system $(A, *)$.

Since e_1 is a left identity $e_1 * e_2 = e_2$.

Since e_2 is a right identity $e_1 * e_2 = e_1$

Thus we have $e_1 = e_2$.

$\therefore$ with respect to a binary operation there is at most one identity.

(3) The set Q of all rational numbers is not a group with respect to multiplication.

The rational number $0 \in Q$ but $\exists$ no rational number $a \in Q$ s.t. $0 \cdot a = 1$.
We know that $0a = 0 \; \forall \; a \in Q$.
Thus the rational number 0 doesn't possess multiplicative inverse.

Ex :→ Show that the set of all positive rational numbers forms an abelian group under the composition defined by

$$a * b = (ab)/2.$$

Sol^n :→ Let Q_+ denote the set of all +ve rational numbers.

We define an operation $*$ on Q_+ as

$$a * b = (ab)/2 \quad \forall \; a, b \in Q_+$$

To show that $(Q, *)$ is a group.

closure property :→

Since for every $a, b \in Q_+$

$(ab)/2 \; * \in Q_+$.

$\therefore$ Q_+ is closed with respect to the operation $*$.

Associativity :→

let $a, b, c \in Q_+$

Then $(a * b) * c = \left(\frac{ab}{2}\right) * c = \left(\frac{ab}{2}\right)\left(\frac{c}{2}\right)$

$= \frac{a}{2}\left(\frac{bc}{2}\right) = a * (b * c)$

Hence Associativity prop: satisfied.

Commutativity →

let $a, b \in Q_+$

Then $a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$

Existance of identity :→

The number e will be the identity element if $e \in Q_+$

& if $e * a = a = a * e \quad \forall a \in Q_+$

Now

$e * a = a$

$\Rightarrow \frac{ea}{2} = a$

$\Rightarrow \frac{ea}{2} - a = 0$

$\Rightarrow \frac{a}{2}(e-2) = 0$

$\Rightarrow e = 2$

Since $a \in Q \Rightarrow a \neq 0$

Now $2 \in Q_+$ & we have $2 * a = \frac{2a}{2}$

$= a = a * 2 \quad \forall a \in Q_+$.

$\therefore$ 2 is the identity element.

Existance of inverse

let $a \in Q_+$.

If b is inverse of a then

$b * a = e = 2$.

$\Rightarrow \frac{ba}{2} = 2 \Rightarrow b = 4/a$

Now $a \in Q_+ \Rightarrow 4/a \in Q_+$

We have $(4/a) * a = 4a/2a = 2 = a * (4/a)$

$\therefore$ $4/a$ is the inverse of a.

Thus each element of Q_+ is invertible

Hence $(Q_+, *)$ is an abelian group.

Some general properties of Groups

Theorem – 1 :→

Uniqueness of Identity.

The identity element in a group is unique.

Pf :→ Suppose e & e' are two identity elements of a group G. we have

$e \cdot e' = e$ if e' is identity

& $ee' = e'$ if e is identity

But ee' is unique element of G.

Therefore $ee' = e$ & $ee' = e'$

$\Rightarrow e = e'$

Hence the identity element is unique.

Theorem-2 :→

Uniqueness of Inverse

The inverse of each element of a group is unique.

Pf :→ let a be any element of a group G & let e be the identity element.

Suppose b & c are two inverse of a

i.e. $ba = e = ab$

& $ca = e = ac$

We have $b(ac) = be$ $[\because ac = e]$

$= b$

e is identity.

Also $(ba)c = ec = c$ $[\because ba = e]$

But in a group composition is associative.

Therefore $b(ac) = (ba)c$

Hence $b = c$.

Note:

The identity element is its own inverse. Since $ee = e$

therefore $e^{-1} = e$.

Theorem-3 :→

If the inverse of a is a^{-1}, then the inverse of a^{-1} is a

i.e. $(a^{-1})^{-1} = a$.

Pf :→ If e is the identity element, we have $a^{-1}a = e$ [By def^n of inverse]

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

[Multiplying both sides on the left by $(a^{-1})^{-1}$ which is necessarily an element of G because a^{-1} is an element of G]

$\Rightarrow \left[(a^{-1})^{-1} \cdot a^{-1}\right] a = (a^{-1})^{-1}$ [Associative prop.]

$\Rightarrow \quad e\, a = (a^{-1})^{-1}$ [inverse prop.]

$\Rightarrow \quad a = (a^{-1})^{-1}$ [Identity prop.]

Note :→ If we had used additive notation to denote the composition in G, the statement of this result would have been $-(-a) = a$.

Theorem-4 :→ Reversal Rule

Prove that $(ab)^{-1} = b^{-1}a^{-1}$.

Pf :→ Suppose a & b are elements of G. & a^{-1}, b^{-1} are inverse of a & b respectively, then

$$a^{-1}a = e = a\,a^{-1}$$

& $$b^{-1}b = e = b\,b^{-1}$$

Now $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})\,a^{-1}$

[$\because$ Composition is associative]

$$= [a\,(bb^{-1})]\,a^{-1}$$

$$= [a\,e]\,a^{-1}$$

$$= a\,a^{-1}$$

$$= e$$

Also $(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)]$

$= b^{-1}[(a^{-1}a)b]$

$= b^{-1}(eb)$

$= b^{-1}b$

$= e$

Thus we have $(b^{-1}a^{-1})(ab) = (ab)(b^{-1}a^{-1})$

Thus by definition of inverse we have $(ab)^{-1} = b^{-1}a^{-1}$

If the group is commutative, then we shall have

$(ab)^{-1} = a^{-1}b^{-1}$, since $b^{-1}a^{-1} = a^{-1}b^{-1}$

Note-1:→ In additive notation the statement of this theorem will be.

$-(a+b) = (-b)+(-a)$

Theorem-5 →

Cancellation laws hold good in a group.

If a, b, c are any elements of G, then $ab = ac \Rightarrow b = c$ [Left Cancellation law]

& $ba = ca \Rightarrow b = c$ [Right cancellation law]

Pf→ $a \in G \Rightarrow \exists\ a^{-1} \in G$

such that $a^{-1}a = e = aa^{-1}$

where e is the identity element.

Now $ab = ac$

$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$

[Multiplying both sides on the left by a^{-1}]

$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$ [by Associativity]

$\Rightarrow eb = ec$

$\Rightarrow b = c$

Also $ba = ca \Rightarrow (ba)a^{-1} = (ca)a^{-1}$

$\Rightarrow b(aa^{-1}) = c(aa^{-1})$

$\Rightarrow be = ce$

$\Rightarrow b = c$

Note :→ In additive notation these results can be written as $a+b = b+c$

$\Rightarrow b = c$

& $b+a = c+a$

$\Rightarrow b = c$

Theorem-6 :→ If a, b are any two elements of a group G, then the eqn $ax = b$ & $ya = b$ have unique sol^n in G.

Pf :→ $a \in G \Rightarrow \exists\ a^{-1} \in G$ such that $a^{-1}a = e = aa^{-1}$ where e is the identity element.

$\therefore a \in G, b \in G \Rightarrow a^{-1} \in G, b \in G$

$\Rightarrow a^{-1}b \in G$ [by closure prop]

Now substituting $a^{-1}b$ for x in the left hand side of the eqn $ax = b$ we have

$$a(a^{-1}b) = (aa^{-1})b = eb = b$$

Thus $x = a^{-1}b$ is a sol^n in G of the eqn $ax = b$

To show that the sol^n is unique, let us suppose that $x = x^{-1}$ & $x_1 \neq x_2$ are two sol^n of the eqn $ax = b$.

Then $ax_1 = b$ & $ax_2 = b$.

Therefore $ax_1 = ax_2$.

By left cancellation law this gives

$$x_1 = x_2$$

Therefore the sol^n is unique.

Now to prove the eqn $ya = b$ has a unique sol^n in G.

We have $a \in G$, $b \in G$

$\Rightarrow ba^{-1} \in G$

Now $(ba^{-1})a = b(a^{-1}a) = be = b$

$\therefore y = ba^{-1}$ is a sol^n in G of the eqn $ya = b$.

Suppose y_1 & y_2 are two sol^n of this eqn. Then $y_1 a = b$ & $y_2 a = b$.

Therefore $y_1 a = y_2 a$.

By right cancellation law this gives

$y_1 = y_2$.

Therefore the sol" is unique. proved

MONOID

Let $(A, *)$ be an algebraic system where $*$ is a binary operation on A. $(A, *)$ is called monoid, if the following conditions are satisfied.

(1.) $*$ is a closed operation.

(2) $*$ is an associative operation.

(3) There is an identity.

Let $(A, *)$ be a monoid with the identity element e, & B is a subset of A. Then $(B, *)$ is said to be submonoid, if B is closed under the operation $*$ & $e \in B$.

Let $(A, *)$ & (B, o) be two monoid with e_A & e_B as their identity elements respectively. Then, their direct product $(A \times B, \square)$, is also a monoid with (e_A, e_B) as the identity element.

This is because $\forall\ a \in A$, $b \in B$.

$(e_A, e_B) \square (a, b) = (e_A * a, e_B \circ b) = (a, b)$

$(a, b) \square (e_A, e_B) = (a * e_A, b \circ e_B) = (a, b)$

Ex →

Let A be a set of people of different heights.

Let Δ be a binary operation such that $a \Delta b$ is equal to the taller one of a & b. We note that (A, Δ) is a monoid where the identity is the shortest person in A.

Cosets →

Let $(A, *)$ be an algebraic system, where $*$ is a binary operation.

Let a be an element in A.

& H be a subset of A.

The left coset of H w.r.t. a which we shall denote $a * H$, is the set of elements $\{a * x / x \in H\}$.

Similarly, the right coset of H with respect to a, denoted by $H * a$.

$= \{x * a / x \in H\}$.

Theorem →

Let $a * H$ & $b * H$ be two Cosets of H. Either $a * H$ & $b * H$ are disjoint or they are identical.

Pf ⇒ Suppose $a * H$ & $b * H$ are not disjoint,

& have f as a common element.

That is, $\exists\ h_1$ & h_2 in H such that

$f = a * h_1 = b * h_2$.

We can write $a = b * h_2 * h_1^{-1}$.

For any element x in $a * H$.

Since $x = a * h_3$ for some h_3 in H.

We have $x = b * h_2 * h_1^{-1} * h_3$

which is an element in $b * H$

because $h_2 * h_1^{-1} * h_3$ is an element in H.

In a similar way we can show that any element in $b * H$ is also an element in $a * H$.

We thus conclude that the two sets $a * H$ and $b * H$ are equal.

Order of a finite group.

If in a group G the set consists of a finite number of distinct elements then the group is called a finite group, otherwise an infinite group.

The number of elements in a finite group is called the order of the group. An infinite group is said to be of infinite order.

Lagrange's Theorem

The order of each subgroup of a finite group is a divisor of the order of the group.

Pf:→ Let G be a group of finite order n.
Let H be a subgroup of G.
& let $O(H) = m$.
Suppose $h_1, h_2 \dots h_m$ are the m members of H.

Let $a \in G$. Then Ha is a right coset of H in G & we have

$$Ha = \{h_1 a, h_2 a, \dots h_m a\}$$

Ha has m distinct members,
since $h_i a = h_j a \Rightarrow h_i = h_j$

Therefore each right coset of H in G has m distinct members.
Any two distinct right cosets H in G are disjoint i.e. they have no elements in common.

Since G is a finite group, the number of distinct right cosets of H in G will be finite say equal to k. The union of these k distinct right cosets of H in G is equal to G.

Thus if $Ha_1, Ha_2 \dots, Ha_k$ are the k distinct right cosets of H in G, then

$$G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k.$$

$\Rightarrow$ the number of elements in G
= the number of elements in Ha_1
+ " " " " " Ha_2
⋮
+ " " " " " Ha_k

[∵ two distinct right cosets are mutually disjoint]

$\Rightarrow O(G) = km \Rightarrow n = km$

$\Rightarrow k = \frac{n}{m} \Rightarrow m$ is a divisor of n.

$\Rightarrow O(H)$ is a divisor of $O(G)$.

Hence the theorem.

Note :- (1) k is the index of H in G.

We have $m = n/k$.

Thus k is a divisor of n.

Therefore, the index of every subgroup of a finite group is a divisor of the order of the group.

(2) If H is a subgroup of a finite group G, then the order of H in G = the number of distinct right (or left) cosets of H in $G = \frac{O(G)}{O(H)}$.

(3) The order of every element of a finite group is a divisor of the order of the group.

(4) If G is a finite group of order n, and $a \in G$, then $a^n = e$

CODES AND GROUP CODES

A Code is a collection of words that are to be used to represent distinct messages.

A word in a code is also called as Codeword. A block code is a code consisting of words that are of the same length.

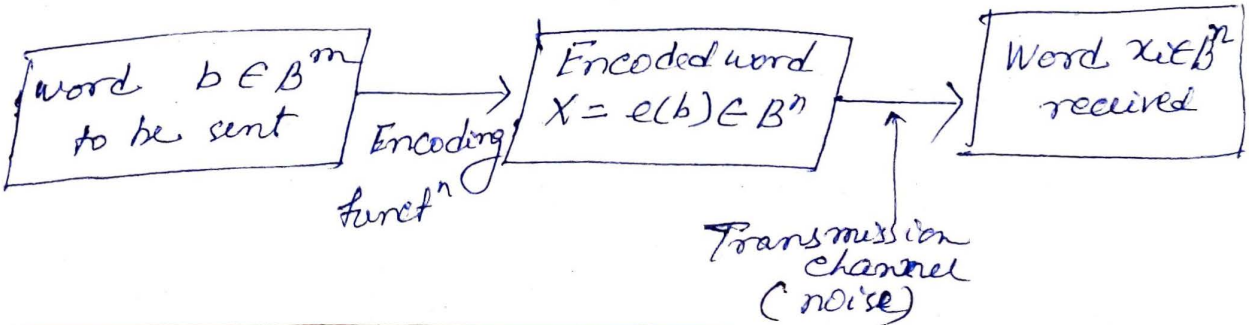
One of the criteria for choosing a block code to represent a set of messages is its ability to correct errors.

Suppose a codeword is transmitted from its origin to its destination. In the course of transmission, interferences such as noises might cause some of the 1s in the codeword to be received as 0s, & some of the 0s to be received as 1s. Consequently, the received word might no longer be the transmitted one, and it is our desire to recover the transmitted word if at all possible. This is what we mean by error correction.

Let $B = \{0, 1\}$

We define $B^m = B \times B \times \cdots \times B$ (m factors)

A sequence of letters from an alphabet is often referred to as a word.



Parity check code →

The following encoding funct^n $e: B^m \to B^{m+1}$ is called the parity $(m, m+1)$ check code.

Suppose $b = b_1 b_2 b_3 \cdots b_m \in B^m$

We define the encoding funct^n $e(b)$ as

$$e(b) = b_1 b_2 b_3 \cdots b_m b_{m+1}$$

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

[$|b|$ represents weight of b]

It may be observed that b_{m+1} is zero iff the number of 1's in b is an even number. Thus, every code word $e(b)$ has even weight.

Ex → Let us assume $m = 3$, then

$e(000) = 0000$ $\quad |(000)| = 0$ even

$e(001) = 0011$ $\quad |(001)| = 1$ odd

$e(010) = 0101$ $\quad |(010)| = 1$ odd

$e(011) = 0110$ $\quad |(011)| = 2$ even

$e(100) = 1001$

$e(101) = 1010$

$e(110) = 1100$

$e(111) = 1111$

Code words.

let $b = 111$ then $x = e(b) = 1111$.
If transmission channel transmits x as $x_i = 1101$ then $w(x_i) = 3$, and we can say that an odd number of errors (at least one) has occured.

Ex :→ Consider $(3,4)$ parity check code. For each of the received words determine whether an error will be detected ?

(a) 0010

(b) 1001

Sol^n :→ (a) 0010 – Yes, since weight = 1, which is odd

(b) 1001 – no, since weight = 2, which is even..

[Note :→ If the received word has even weight, then we can't guarantee that the code word was correctly transmitted, as this encoding function can't detect an even number of errors]

Ex :→ Consider $(2,6)$ encoding funct^n e.

$e(00) = 000000$ $\quad$ $e(10) = 101010$

$e(01) = 011110$ $\quad$ $e(11) = 111000$

(a) Find the minimum distance of e.

(b) How many errors will e detect ?

Sol^n →

(a) $d(e(00), e(01))$

$= |(000000) \oplus (011110)| = |(011110)| = 4$

$d(e(01), e(10))$

$= |(011110) \oplus (101010)|$

$= |(110100)| = 3$

$d\ |e(10), e(11)| = |(101010) \oplus (111000)|$

$= |(010010)| = 2$

Similarly finding all, we found that the minimum distance is 2.

(b) A code will detect k or fewer errors iff its minimum distance is at least $(k+1)$.

Since here the minimum distance is 2, So we have

$$2 \geq k+1$$

$$\Rightarrow \quad k \leq 1$$

So, the code will detect one or fewer errors.

Ex → Show that (2,5) encoding funct^n $e: B^3 \to B^7$ defined by

$e(00) = 00000$ $\quad e(10) = 10101$

$e(01) = 01110$ $\quad e(11) = 11011$

is a group.

Sol'n To prove it is a group code, we have to examine the following steps

(a) For closure

$(00000) \oplus (01110) = 01110 \in B^5$

$(00000) \oplus (10101) = 10101 \in B^5$

$(01110) \oplus (10101) = 11011 \in B^5$

$(01110) \oplus (11011) = 10101 \in B^5$

$(10101) \oplus (11011) = 01110 \in B^5$

By checking in this way we found that if $x, y \in B^5$

then $x \oplus y \in B^5$

(b) For Associativity

$((00000) \oplus (01110)) \oplus (10101)$

$= (00000) \oplus ((01110) \oplus (10101))$

will holds true.

(c) Identity element :

Since $(00000) \in B^5$, hence check for identity is satisfied.

(d) Existance of Inverse :

$(01110) \oplus (01110) = (00000)$

Hence element is inverse of itself.

Hence, it is a group code as all four properties of group holds true.

Note :-

(1) Suppose $e: B^m \to B^n$, is an (m,n) encoding funct^n. We define an onto funct^n $d: B^n \to B^m$ such that if $d(x_i) = b' \in B^m$ and the transmission channel has no noise, then $b' = b$.

This onto funct^n d is known as (n,m) decoding funct^n associated with the encoding funct^n e.

Here $x = e(b)$ is the encoded word & x_i is the received word.

The decoding funct^n d should be an onto funct^n because every received word can be decoded to give a transmitted word.

(2) Let us again consider the parity check code which was defined earlier. The corresponding decoding funct^n $d: B^{m+1} \to B^m$ can be defined as follows :

If $z = z_1 z_2 \cdots z_m z_{m+1}$

then $d(z) = z_1 z_2 \cdots z_m$

It may be observed that, if

$b = b_1 b_2 \cdots b_m \in B^m$

then $(d \circ e)(b) = d(e(b)) = b$

For example if $m = 4$,

Then $d(10100) = 1010$

& $d(11111) = 1111$.

(3) Let $x_1, x_2 \cdots x_N$ denote the codewords in $\mathcal{C}$.

We shall compute the conditional probability $P(x_i | y)$ for $i = 1, 2 \cdots N$ where $P(x_i | y)$ is the probability that x_i was the transmitted word given that y was the received word. If $P(x_k | y)$ is the largest of all conditional probabilities computed, we shall conclude that x_k was the transmitted word.

Such criterion for determining the transmitted word is known as the maximum-likelihood decoding criterion.

$d(x_i, y)$ for $i = 1, 2 \cdots N$

conclude that x_k was the transmitted word if $d(x_k, y)$ is the smallest among all distances computed.

This is known as minimum-distance decoding criterion.

If we assume that the occurrence of errors in the position are independent and the probability of the occurrence of the error is p then

$$P(x_i | y) = (1-p)^{n-t} \cdot p^t$$

where t is the distance between x_i & y.

For $p < \frac{1}{2}$, the smaller $d(x_i/y)$ is, the larger $P(x_i/y)$ will be.
Therefore the minimum-distance decoding criterion is equivalent to the maximum likelihood decoding criterion.

A code of distance $2t+1$ can correct t or fewer transmission errors when the minimum distance decoding criterion is followed.

Suppose a codeword x was transmitted and the word y was received.
If no more than t errors have occurred in the course of transmission, we have

$$d(x,y) \leq t$$

let x_1 be another codeword.
Since $d(x, x_1) \geq 2t+1$
and $d(x, x_1) \leq d(x,y) + d(y, x_1)$
we have

$$d(y, x_1) \geq t+1$$

Therefore, the minimum-distance decoding criterion will indeed select x as the transmitted word.