10/1/22

Group

In Group theory, classmate
(e) → Identity element

Algebric System :-
It is a set ~~with a num~~ whose element with ~~with~~ satisfy some the number of properties.

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

Abelian / Commutative Group.
$a \times b = b \times a$

Q $G = \{1, -1, i, -i\}$
Show that it is a commutative group under the binary operation multiplication.

Closure
$1 \times 1 = 1 \in G$
$(-1) \times (-1)$
1×-1

Associative
$x = 1, y = i, z = -i$
$x(yz) = 1(i(-i))$
$= 1(1)$
$= 1$
$(xy)z = (1 \cdot i)(-1)$
$= i(-1)$
$= -i^2$
$= -(-1)$
$= 1$

Identity
$e = 1 \in G$
$1 \cdot (1) = 1 ; -1 \cdot 1 = -1 ; i \cdot 1 = i$
$-i \cdot 1 = -i$

Inverse
$\exists n (1) = 1$
$1 \cdot 1 = 1$

$\exists n (-1) = -1$
$-1 \times -1 = 1$

$\exists n (i) = \cdot$

→ $(Z, +)$ is a commutative group
→
→

Q show that the operation add. modulo 10 is a group over the set $\{0, 1, 2, 3 \ldots, 9\}$
$* =$ ~~multiplication~~ ~~addition~~ modulo 10

Ans
$$a \oplus b = \begin{cases} a + b, & a+b < 10 \\ \text{LCM}(a+b) - 10, & a+b \geq 10 \end{cases}$$

Closure

$0 \oplus 9 = 9 \in G$
$8 \oplus 9 = 7 \in G$

Associative

$x = 2, y = 5, z = 9$

$(x + y) + z = (2 \oplus 5) \oplus 9$

$= 7 \oplus 9$

$= 6$

$x + (y + z) = 2 \oplus (5 \oplus 9)$

$= 2 \oplus 4$

$= 6$

Identity

0

$1 \oplus 0 = 1$

$2 \oplus 0 = 2$

$0 \in 9$

Inverse

Inv 0 = 10		
Inv 1 = 9		$1 \oplus 9 = 1$
Inv 2 = 8		$2 \oplus 8 = 1$
Inv 3 = 7		$3 \oplus 7 = 1$

Commutative

$a \oplus b = b \oplus a$

Q.1 Prove that the identity element of a group is unique.
Q.2 Prove that the inverse of an element of a group is unique

Ans Q.1 Let $(G, *)$
$(e, f) \rightarrow$ are identity element

$a e = ea = a$ — (i)
$af = fe = a$ — (ii)

$ae = af$
~~$a^{-1}(ae) = a^{-1}$~~
$\Rightarrow e = f$ (Left cancelation Law)

So, it has only one identity element.

Ans Q.2 $(G, *)$
$a \in G$

$\exists (a) = b \quad c$
$ab = ba = e$ — (i)
$ac = ca = e$ — (ii)

$ab = ac$
$\boxed{b = c}$

Sub-group

$(G, *)$

$(H, *)$ | (i) $H \subset G$
(ii) $(H, *)$ is a group.

$(R, +)$ is a group
$(Z, +)$ is a group

$Z \subset R$
Z is a subgroup of R

But, $(N, +)$ is not a subgroup of $(Z, +)$

NOTE
Let $(G, *)$ be a group and H is a subset of G $(H \subset G)$ and H is a finite set. Then $(H, *)$ is a subgroup of $(G, *)$ if H satisfies closure property on $*$.
(Important Theorem)

Ans $(H, *) \longrightarrow$ (i) $H \subset G$
(ii) $(H, *) \rightarrow$ (1) Closure
(2) Associative
(3) Identity
(4) Inverse

11/7/22

H_1 & H_2 are sub-groups of G
then $H_1 \cap H_2$ is also a subgroup of G

$G \rightarrow$ group
H_1, H_2 are subgroup of G

$H_1 \cap H_2$ is a subgroup of G

$H_1 \subset G, \quad H_2 \subset G$
$H_1 \cap H_2 \subset H_1 \subset G$
$H_1 \cap H_2 \subset G$

$H_1 \cap H_2$
$a, b \in H_1 \cap H_2 \Rightarrow a\,b \in H_1 \cap H_2$
$a \in H_1 \cap H_2 \Rightarrow a \in H_1$ & $a \in H_2$
$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ & $b \in H_2$
$a, b \in H_1 \Rightarrow a\,b \in H_1$
$a\,b \in H_2$
$a\,b \in H_1 \cap H_2$ //

Cosets and Lagrange's Theorem

Cosets
Let G be any group & H is a subgroup of G

$H = \{h_1, h_2, h_3 \dots h_m\}$

$\forall a \in G$, aH → Left coset
Ha → Right coset

$aH = \{ah_1, ah_2, ah_3, ah_4 \dots ah_m\}$

$Ha = \{h_1a, h_2a, h_3a, h_4a \dots h_ma\}$

order $(H) = k$ then order $(aH) = k$

Theorem
Let G be any group, H is a subgroup of G. Let a & b are any 2 element of G then, aH & bH are 2 cosets of H & G. Either $aH = bH$ or, $aH \cap bH = \phi$

Contradiction to proof it
⇒ Let us assume that aH & bH have some common elements.
Let
$H = \{h_1, h_2, h_3 \dots, h_m\}$
$aH = \{ah_1, ah_2, ah_3, \dots ah_m\}$
$bH = \{bh_1, bh_2, bh_3, \dots bh_m\}$

Let $ah_1 = bh_2$
$\Rightarrow a = bh_2h_1^{-1}$ — (1)

Let $x \in aH$

$\Rightarrow x = ah_3 \quad (h_3 \in H)$

$\Rightarrow x = bh_2h_1^{-1}h_3$ —— (from eq ①)

$h_1 \in H$

$h_1^{-1} \in H$

$\Rightarrow x = b\,h_2h_1^{-1}h_3$

So, $h_2h_1^{-1}h_3 = h_4 \in H$

$x = bh_4$

$bh_4 \in bH$

$x \in bH$

$\forall x \in aH \Rightarrow x \in bH$

$\boxed{aH \subset bH}$ —— ①

$x \in bH$

$x = bh_3$

$x = ah_1h_2^{-1}h_3$

$x = ah_i \in aH$

$\forall x \in bH \Rightarrow x \in aH$

$\boxed{bH \subset aH}$ —— ②

from ① & ②

$aH = bH$

Lagrange's Theorem

The order of any ~~finite group~~ subgroup divides the order of any finite group.

$O(G) = H$ is a subgroup of G

$O(H) \mid O(G)$ $\quad O \Rightarrow$ order

$O(G) = n$

$G = \{g_1, g_2, g_3, \ldots, g_n\}$

$O(H) = m$

$H = \{h_1, h_2, \ldots, h_m\}$

Left coset of H in G

$g_1H, g_2H, g_3H, g_4H, \ldots g_nH$

Let the number of distinct coset be k

G
$H \subset G$
$a \in H \subset G$
$aH = H$

$D = \{g_1H, g_2H, \ldots, g_nH\}$

$O(H) = m$

$O(mH) = m$

$O(D) = O(g_1H) + O(g_2H) + \cdots + O(g_nH)$

$g_1H \cup g_2H \cup g_3H \cup \cdots g_nH = G$

$O(G) = O(g_1H) + O(g_2H) \cdots + O(g_nH)$

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

$n = mk$

$n = mk$

$m \mid n$

$O(H) \mid O(G)$

12/01/22

Normal Sub-group → (NSG)

G be any group

N is a subgroup of G

$\forall g \in G \quad gng^{-1} \in N \quad n \in N$

Theorem (1)

Let G be any group

N is a sub group of G

N is a N. subgroup of G iff

$xNx^{-1} = N \quad \forall x \in G$

Proof

$N = \{n_1, n_2, \ldots, n_k\}$

$xNx^{-1} = \{xn_1x^{-1}, xn_2x^{-1}, xn_3x^{-1}, \ldots\}$

(1) Let N is a N. subgroup of G

$xNx^{-1} = N$

$xNx^{-1} \subset N \;\&\; N \subset xNx^{-1}$ $\quad x \in G,\ xnx^{-1} \in N$

$y \in xNx^{-1}$

$\Rightarrow y = xnx^{-1} \quad n \in N$

N is NSG of G

$\Rightarrow xnx^{-1} \in N$

$\Rightarrow y \in N$

$\boxed{xNx^{-1} \subset N}$

$x^{-1}n(x^{-1})^{-1}$

$x(x^{-1}nx)$

$xx^{-1}nx$

$(nx)x^{-1} \in xNx^{-1}$

$n \in xNx^{-1}$

$\boxed{N \subset xnx^{-1}}$

Theorem (2)

Let G be any group

N is a normal sub-group of G

N is a NSG iff $xH = Hx$

Proof

N is a NSG of G

$xN = Nx$

N is a NSG iff $xNx^{-1} = N$

$xNx^{-1} = N$

$(xNx^{-1})x = Nx$

$xNx^{-1}x = Nx$

$xNe = Nx$ $\quad (e$ = Identity$)$

$xNe = Nx$

$xN = Nx$

Let, $Nx = xN$

N is a NSG of G

$xN = Nx$

$xNx^{-1} = (Nx)x^{-1}$

$xNx^{-1} = Nxx^{-1}$

$xNx^{-1} = Ne$

$xNx^{-1} = N$

N is a NSG of G.

Theorem (3)

G is any group
N is a NSG of G
Then, N is a NSG iff $NxNy = Nxy$

Proof

N is NSG of G
$NxNy = Nxy$

L.H.S
$(Nx)(Ny)$
$= N(xN)y$
$= N(Nx)y$ $(Nx = xN)$
$= NN\,xy$
$= N^2xy$
$= Nxy$

Let, $NxNy = Nxy$
$\Rightarrow$ N is a NSG of G
$\Rightarrow NxNx^{-1} = Nxx^{-1}$
$\Rightarrow NxNx^{-1} = Ne$
$\Rightarrow NxNx^{-1} = N$
$\Rightarrow n_1xn_2x^{-1} \in N$
$\Rightarrow n_1^{-1}(n_1xn_2x^{-1}) \in n_1^{-1}N$
$\Rightarrow n_1^{-1}n_1xn_2x^{-1} \in n_1^{-1}N$
$\Rightarrow exn_2x^{-1} \in n_1^{-1}N$
$\Rightarrow xn_2x^{-1} \in n_1^{-1}N$
$\Rightarrow xn_2x^{-1} \in N$

N is a NSG of G.

Theorem (4)

Every subgroup of abelian group is normal SG

G $\rightarrow$ abelian group
N $\rightarrow$ SG of G
N is a NSG of G

$n \in N$, $xnx^{-1} \in N$
$xnx^{-1} = x(nx^{-1})$
$= x(x^{-1}n)$
$= (xx^{-1})n$ (Asso.)
$= en$

Theorem (5)

G is any grp.
N_1, N_2 are 2 NSG of G
$N_1 \cap N_2$ is also a NSG of G.

Proof $N_1 \cap N_2$ is also a SG of G

$\forall n \in N_1 \cap N_2, x \in G$
$xnx^{-1} \in N_1 \cap N_2$
$n \in N_1 \cap N_2$
$n \in N_1$ & $n \in N_2$
$xnx^{-1} \in N_1$, $xnx^{-1} \in N_2$

$\boxed{xnx^{-1} \in N_1 \cap N_2}$

We have to prove it
1. $N_1 \cap N_2$ is a SG of G
2. $N_1 \cap N_2$ satisfy Normal property

Theorem 6

Let G be any grp
H is a SG of G
N is a NSG of G

$H \cap N$ is a NSG of H

Proof To prove :-
1. $H \cap N$ is a SG of H
2. $H \cap N$ satisfies Normal property

$H \cap N$ is a SG of G
$H \cap N$ is itself a group
$H \cap N \subset H$
$\boxed{H \cap N \text{ is a SG of } H}$

$\forall \alpha \in H \cap N$, $h \in H$
$h \alpha h^{-1} \in H \cap N$

$h \alpha \in H$ & $\alpha \in N$
$h \alpha h^{-1} \in N$
$h \in H, h^{-1} \in H, \alpha \in H$
$h \alpha h^{-1} \in H$
$\boxed{h \alpha h^{-1} \in H \cap N}$

Homomorphism

$(G, *)$ $(G', \cdot)$

$\phi \; G \to G'$
$\phi(a * b) = \phi(a) \cdot \phi(b)$

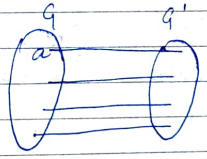
(11) $\forall \alpha \in H \cap N$, $h \in H$
$h \alpha h^{-1} \in H \cap N$
$\alpha \in H$ & $\alpha \in N$.
$h \alpha h^{-1} \in N$ (By normal property)

$h \in H, h^{-1} \in H, \alpha \in H$
$h \alpha h^{-1} \in H$
$h \alpha h^{-1} \in H \cap H$

Homomorphism

Let $(G, *)$ $(G', \cdot)$

$\phi : G \to G'$
$\phi(a * b) = \phi(a) \; \phi(b)$



Ex Let $(G, \cdot)$ & $(G', +)$ be two groups over respective operations

$\phi G \to G'$
$\forall x \in G \Rightarrow \phi(x) = 1$
$\phi(x \cdot y) = \phi(x) + \phi(y)$

$\phi(x) = \log x \qquad \phi(y) = \log y$

$\phi(x \cdot y) = \log(xy)$

$= \log x + \log y$

$= \phi(x) + \phi(y)$

Isomorphism:

(Q) $\phi : G \to G'$

e is the identity element of G

e' " " " " G'

S.t.

(i) $\phi(e) = e'$

(ii) $\forall a \in G \Rightarrow \phi(a^{-1}) = (\phi(a))^{-1}$

→ (i) $ae = a$

$\Rightarrow \phi(ae) = \phi(a)$

$\Rightarrow \phi(a)\phi(e) = \phi(a)$ ($\because \phi$ is a homo mor.)

$\Rightarrow \phi(a)\phi(e) = \phi(a)e'$ ($\phi(a)e' = \phi(a)$)

$\Rightarrow \phi(e) = e'$

(ii) $e' = \phi(e)$

$\Rightarrow e' = \phi(a \cdot a^{-1})$ ($\because a \cdot a^{-1} = e$)

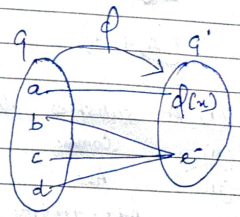
$\Rightarrow e' = \phi(a)\phi(a^{-1})$ ($\because \phi$ is a homo mor.)

$\Rightarrow$ Inv. of $\phi(a)$ is $\phi(a^{-1})$

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

Kernel of a homomorphism

$\phi : G \to G'$



If we take these elements as a set (K_ϕ)

$x \in K_\phi \Rightarrow \phi(x) = e'$

If ϕ is a homomorphism from $G \to G'$

K is a NSG of G.

(i) K is a SG of G

(ii) K satisfies Normal Property

i.e. $gKg^{-1} \in K$

(a) $K \subset G$, closure:

$\forall a, b \in K \Rightarrow ab \in K$

$a \in K \Rightarrow \phi(a) = e'$

$b \in K \Rightarrow \phi(b) = e'$

$\phi(ab) = \phi(a)\phi(b)$ (ϕ is a mono. mor.)

$= e'e'$

$= e'$

$\Rightarrow ab \in K$

(iii) $\phi(gKg^{-1}) = \phi(g)\phi(K)\phi(g^{-1}) = \phi(g)e'\phi(g^{-1})$

$= \phi(g)\phi(g^{-1}) = \phi(gg^{-1})$ (mono no.)

$= \phi(e)$

$\phi(gKg^{-1}) = e'$

$gKg^{-1} \in K$

Ring:

$(A, +, \cdot)$

(I) A satisfies closes +
(II) Comm.
(III) Ass.
(IV) Add. Identity
(V) Add. Inv.
(VI) Closer *
(VII) Associative *
(VIII) $a(b+c) = ab+ac$

Q $(Z, +, \cdot)$ Ring $(R, +, \cdot)$ Ring $(N, +, \cdot)$ Doesn't satisfy is Identity & Inverse not satisfied.

Commutative Ring / Ring with unit element

$(R, +, \cdot)$
$a, b \in R \Rightarrow ab = ba$ } Commutative Ring.

$(R, +, \cdot)$
$\forall x \in R \Rightarrow xe = x$
(multiplicative ring) } Ring with unit elements.

Zero Divisors of a Ring

Let $(A, +, \cdot)$ be a Ring ~~divisors~~
$x \neq 0 \in A$ & $y \in A$, $y \neq 0$, then y is 0 divisor of x if $xy = 0$ or $yx = 0$.

Q) $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $y = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

$x \neq 0$ $y \neq 0$

$$xy = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

Field

$(A, +, \cdot)$

+	U, Comm., Ass., Iden., Inv.
*	
+, *	Distributive

Date 15/01/22
Page

Integral Domain

Suppose $(A, +, .)$ is a ring. This ring is called integral domain if it satisfies:

i) $ab = ba$ (commutative prop. for mul.)

ii) $1 \in A$ such that $x \cdot 1 = 1 \cdot x = x$ (Iden. mul.)

iii) A has no zero divisor.

OR)

A commutative ring with unit element is called an integral domain if it has no zero divisor.

Q. $(z, +, .)$ → Ring
- ↳ comm. prop. for mult.
- ↳ multiplicative identity prop.
- ↳ has no zero divisor.

$\therefore (z, +, .)$ is an integral domain.

Imp

Thm 1:

Every field is an Integral Domain.

Ex: $(D, +, .)$ is a field. → + 5 prop.
→ * 5 "
→ Distributive

Date .....
Page .....

Let $a, b \in D$.

$$ab = 0 \quad \text{---(1)}$$

(i) Suppose, $a \neq 0$ & $ab = 0$.

$a \in D \Rightarrow a^{-1}$ exists & $a^{-1} \neq 0$.

$$ab = 0$$

$$\Rightarrow a^{-1}(ab) = a^{-1}0$$

$$\Rightarrow (a^{-1}a)b = a^{-1}0$$

$$\Rightarrow 1b = a^{-1}0 \qquad (\because aa^{-1} = I)$$

$$\Rightarrow b = 0 \qquad \text{(Identity prop.)}.$$

(ii) ——, $b \neq 0$ & $ab = 0$

$b \in D$, $\Rightarrow b^{-1}$ exists & $b^{-1} \neq 0$

$$ab = 0$$

$$\Rightarrow (ab)b^{-1} = 0b^{-1}$$

$$\Rightarrow a(bb^{-1}) = 0b^{-1}$$

$$\Rightarrow a1 = 0b^{-1}$$

$$a = 0$$

i.e. $ab = 0$ for any one of (a or b) must be 0 out.

$\therefore$ D has no zero divisor.

$\Rightarrow$ D is an integral domain.

Imp Thm 2:

Every finite integral domain is a field.

Let D is a Finite integral domain.

Show that: D is a field.

Suppose: $D = \{x_1, x_2, \dots, x_n\}$.

Let x is any element of D.

$$xD = \{xx_1, xx_2, \dots, xx_n\} \in D$$

(closer prop)

If possible, let $xx_i = xx_j$

$$\Rightarrow x(x_i - x_j) = 0$$

either $x = 0$ or $x_i - x_j = 0$

$\because$ D has no zero divisor

$\therefore$ Product of two non-zero elements $\neq 0$.

$$\therefore x_i = x_j$$

Let $xx_i = x$ ($\because$ every element of xD = any 1 ele of D).

$\Rightarrow x_i$ is identity element.

$$x_i = 1$$

Since, $x_i = 1$

so, out of $xx_1, xx_2, \dots, xx_n$ one element must be 1.

Let $xx_j = 1$

$$\Rightarrow x_j = x^{-1}$$

so, $\forall x \in D \Rightarrow x^{-1} \in D$

where $xx^{-1} = x^{-1}x = 1$

Hence, D is a field.

Date .....
Page .....

Q- Let $(R, +, \cdot)$ be a Ring / Field
$a, b \in R$.

(i) $a0 = 0 \cdot a = 0$

(ii) $a(-b) = (-a)b = -ab$

→ (i) We know that, since R is a ring it must satisfy identity & prop.

$\therefore$ ~~$a + 0 = 0$~~ $a + 0 = a$ (Ident add.)

$\Rightarrow (a+0) \cdot a = a \cdot 0$ (mult. Ident).

$\Rightarrow a \cdot 0 + 0 \cdot 0 = a \cdot 0$ (Dist.)

$\Rightarrow a \cdot 0 + 0 = a \cdot 0$

$\Rightarrow a \cdot 0 = a \cdot 0$

$x + 0 = x$ (Add. Iden.)

P.T. $x = 0$

$\Rightarrow 0 + 0 = 0$

$\Rightarrow a(0+0) = a \cdot 0$ (closer.)

$\Rightarrow a \cdot 0 + a \cdot 0 = a \cdot 0$ (Dist.).

$\Rightarrow \underline{a \cdot 0} + a \cdot 0 = \underline{a \cdot 0} + 0$ (Identity)

$\Rightarrow a \cdot 0 = 0$ —(i) (L.C. law)

$x + 0 = x$

$\Rightarrow 0 + 0 = 0$ ($x = 0$)

$\Rightarrow (0+0)a = 0 \cdot a$ (closer)

$\Rightarrow 0a + 0a = 0a$ (Dist.)

$\Rightarrow \underline{0a} + 0a = \underline{0a} + 0$ (Add. ident).

$\Rightarrow 0a = 0$ —(ii) (L.C. law).

from (i) & (ii):

$a \cdot 0 = 0 \cdot a = 0$

Date .....
Page .....

(ii) $x + (-x) = 0$ — (i) (Add. inv.)

$\Rightarrow b + (-b) = 0$ ($x = b$)

$\Rightarrow a(b + (-b)) = a \cdot 0$ (closer)

$\Rightarrow ab + a(-b) = a \cdot 0$ (Dist.)

$\Rightarrow ab + a(-b) = 0$ ($\because a \cdot 0 = 0$)

$\Rightarrow ab$ is additive inv. of $a(-b)$

$\Rightarrow a(-b) = -ab$ — (ii)

putting $x = a$ in eq (1).

$\Rightarrow a + (-a) = 0$ (Add. inv.)

$\Rightarrow (a + (-a))b = 0b$ (closer)

$\Rightarrow ab + (-a)b = 0b$ (Dist.)

$\Rightarrow ab + (-a)b = 0$ ($0 \cdot a = 0$).

$\Rightarrow ab$ is add. inv of $(-a)b$.

$\Rightarrow (-a)b = -ab$ — (iii)

from (ii) & (iii):

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

XTRA Class

Date
Page

Codes & Group Codes

— Word is a sequence of letters

— Code is a collection of words used to represent diff. messages.

— Any word in a code is called a codeword.

— Block code is a code consisting of equal length words.

— Binary alphabet : Generally in a code only these are used i.e. 0 & 1.

Binary Operation ($\oplus$).

$x = 101100$

$y = 101001$

$x \oplus y = 000101$

x	y	$x \oplus y$
1	1	0
1	0	1
0	1	1
0	0	0

$A = \{x, y, z, \ldots\}$ — all the binary seq^n of length n.

$(A, \oplus)$ is a grp if :

(i) $x \oplus y \in A$ closer

(ii) $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ Ass.

(iii) $x \oplus e = x$ $(e = 00000)$. Iden.

(iv) $x \oplus (-x) = 0$ Inv.

— Weight of a word (w) : no. of 1 present in the word.

$x = 10101$ wt = 3

$y = 01111$ wt = 4.

→ Distance ($d(x,y)$):

$$d(x,y) = \overset{\text{weight.}}{w}(x \oplus y)$$

$$= w(11010)$$

$$= 3.$$

In words: Distance b/w x & y is no. of pos^s where x & y differs.

Properties:

(i) $d(x,y) = d(y,x)$

(ii) $d(x,y) \leq d(x,z) + d(z,y)$.

(ii) LHS: $d(x,y) = w(x \oplus y)$

$= w(x \oplus 0 \oplus y)$

$= w(x \oplus z \oplus z \oplus y)$

$\leq w(x \oplus z) + w(z \oplus y)$

$\leq d(x,z) + d(z,y)$

Date .....
Page .....

Distance of a blockcode:

Let G be any blockcode. The distance of G is the min^{m} distance b/w any pair distinct code words of G.

Max^{m} likelihood decoding criterion

Let $x_1, x_2, x_3 --, x_n$ denotes the code words in a blockcode G & y is the received word.

Let us find out $P(x_i|y)$ $i=1,2,---,n$ where $P(x_i|y)$ is the probab. that x_i is the transmitted word under the condn that y is the received word.

$$P(x_i|y) = \frac{P(x_i \cap y)}{P(y)}$$

If $P(x_k|y)$ is the largest conditional probab. among $P(x_1|y), P(x_2|y) --- P(x_n|y)$ then we conclude that x_k was the received word.

Date .....
Page .....

Minm distance decoding criterion

Similarly, if $d(x_k, y)$ is minm then x_k is considered as the transmitted word. This criterion is called of minm d— d— er—.

NOTE: When minm distance decoding criterion is followed then a code of distance $2t+1$ can correct t or fewer transmission errors.

Pf:

Let x is a codeword which is transmitted & y is the receiving word of the error is $\leq t$. So

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

Let x_1 be another codeword

But, $d(x, x_1) \geq 2t+1$ ($\because$ Given).

Now,

$$d(x, x_1) \leq d(x, y) + d(y, x_1)$$

$$\Rightarrow 2t+1 \leq t + d(y, x_1)$$

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

Since, the minm dist. occurs in case of x, so x is the transmitted word.

Date .....
Page .....

Group code :

We know that $(A, \oplus)$ is a group. $(G, \oplus)$ is called a group code if $(G, \oplus)$ is a subgrp of $(A, \oplus)$ where A is a set of all binary sequences of length n.