Unit-4

Algebraic Systems

* Algebraic Systems :

Let n-ary operation for n = 1, 2, 3 on set X

Mapping of operations from X^n to X
When n=1, unary operation
n=2, binary operation

Any distinguished element of X such as an identity element or zero element with respect to binary operation is considered as a 0-ary operat

The binary operation are denoted by such symbol $*$, Δ, $+$, $\oplus$

Ex. $x_1, x_2 \in X$ can be represented as $x_1 * x_2$

A system consisting of a set and one or more n-ary operations on the set will be called as algebraic system. or simply algebra

Denote algebraic system by, $\langle S, f_1, f_2, \ldots \rangle$
Where S is a nonempty set and f_1, f_2 are operations on S.

The operations and relations on set S define strcture on the elements of S, an algebraic system is called an algebraic strcture

On algebraic system we can perform more than one operation also $<X, \circ>$, $<Y, *>$ similarly, systems $<X, \circ, +>$ & $<Y, *, \oplus>$ are of the same type.

$\circ$, $*$ and $+$, $\oplus$ having same degree

Ex: Let I be the set of integers consider algebraic system $<I, +, \times>$

$+$ = addition
$\times$ = Multiplication
I = set of a, b, c

① Associativity :

For any $a, b, c \in I$

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

② commutativity :

$a, b \in I$

$$a+b = b+a$$

③ Identity element :

if $0, a \in I$

$$a+0 = 0+a = a$$

Page No.:
Date: / /

④ Inverse element :

for each $a, -a \in I$

$a + (-a) = 0$ These for addition

⑤ Multiplication :

① for any $a, b, c \in I$

$(a \times b) \times c = a \times (b \times c)$ (Associativity)

② for any $a, b \in I$

$a \times b = b \times a$ (commutativity)

③ for any $a, 1 \in I$

$a \times 1 = 1 \times a = a$ (Identity element)

④ for any $a, b, c \in I$

$a \times (b + c) = (a \times b) + (a \times c)$ (Distributivity)

(5) For $a, b, c \in I$ and $a \neq 0$

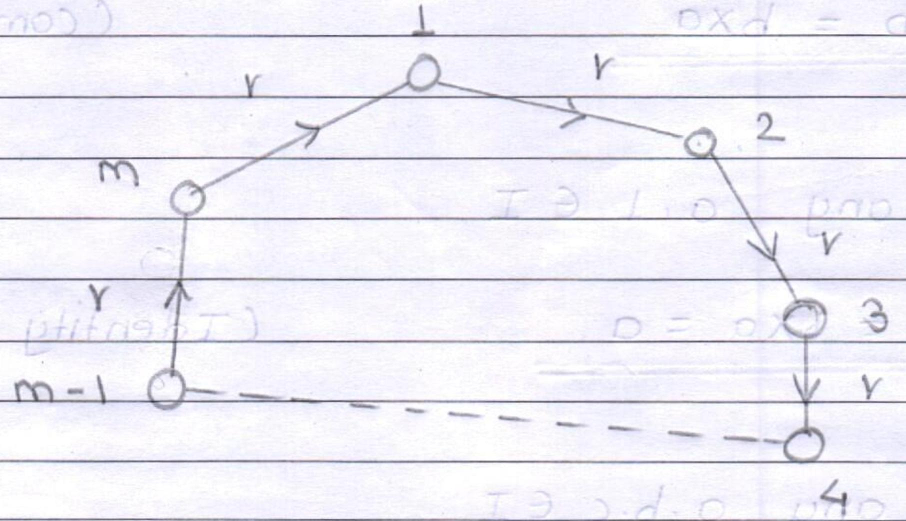
$a \times b = a \times c \Rightarrow b = c$ (cancellation property)

* Some examples of Algebric system and General properties

Ex : Let $M = \{1, 2, \ldots, m\}$ and r be the unary operation on M given by

$$r(j) = \begin{cases} j+1 & j \neq m \\ 1 & j = m \end{cases}$$

The algebra $\langle M, r\rangle$ is called clock algebra



$1 \in M$

$\forall\ 1 =$ generator of algebric system $\langle M, r\rangle$

Ex 2 : Let $X = \{a, b\}$ and S denote the set of all mappings from X to X. Let us write $S = \{f_1, f_2, f_3, f_4\}$ where

$f_1(a) = a$ $f_1(b) = b$ $f_2(a) = a$ $f_2(b) = a$
$f_3(a) = b$ $f_3(b) = b$ $f_4(a) = b$ $f_4(b) = a$

* Homomorphism :

Let $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ be two algebraic system of the same type in the sense that both $\circ$ and $*$ are binary (n-ary) operations. A mapping $g : X \to Y$ is called a homomorphism, or simply morphism from $\langle X, \circ \rangle$ to $\langle Y, * \rangle$ if for any $x_1, x_2 \in X$

$$g(x_1 \circ x_2) = g(x_1) * g(x_2)$$

Here $\langle Y, * \rangle$ called homomorphic image of $\langle X, \circ \rangle$

* Epimorphism :

If $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ are two algebric system having mapping $g : X \to Y$ having relation onto, is called Epimorphism

* Monomorphism :

If $g : X \to Y$ is one-to-one, then g is called Monomorphism.

* **Isomorphism :**

If $g : X \rightarrow Y$ is one-to-one onto relation then g is called as Isomorphism.

* **Isomorphic :-**

If $<X, o>$ and $<Y, *>$ be two algebraic system having isomorphic mapping $g : X \rightarrow Y$ then $<X, o>$ and $<Y, *>$ called an isomorphic

* **Endomorphism :**

Let $<X, o>$ and $<Y, *>$ be two algebric system such that $Y \subseteq X$ then homomorphism from $<X, o>$ to $<Y, *>$ called an Endomorphism

* **Automorphism :**

If $<X, o>$ and $<Y, *>$ are two algebric system having mapping $g : X \rightarrow Y$ with $X = Y$ and having isomorphism (one to one onto) called automorphism

* **Congurence Relation :**

Let $<X, o>$ be an algebraic system and E be an equivalance relation on X. The E is called congurence relation on $<X, o>$

The congurence properly can be generalised to any algebric system

Now if $x_1, x_2, y_1, y_2, \in X$ with $x_1 E y_1$ and $x_2 E y_2$ since

$(x_1 \circ x_2) E (y_1 \circ y_2)$

so that,

$$[x_1 \circ x_2] = [y_1 \circ y_2]$$

If we use $*$ is binary operation

if $x_1, x_2, \in X$

then

$$[x_1] * [x_2] = [x_1 \circ x_2]$$

* Subalgebra :

If $\langle X, \circ \rangle$ is algebric system and $Y \subseteq X$ which is closed under operation $\circ$ then $\langle Y, \circ \rangle$ called subalgebra of $\langle X, \circ \rangle$

The algebric system in the subalgebra is same as the algebric system having original either it [o-ary or upto n-ary]

* Direct product :

If $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ be two algebric system of same time. Then the algebric system $\langle X \times Y, \oplus \rangle$ is called Direct product of algebra $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ provided by operation $\oplus$ by defined for any $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ as

$$\langle x_1, y_1 \rangle \oplus \langle x_2, y_2 \rangle = \langle x_1 \circ x_2 , y_1 * y_2 \rangle$$

The algebraic systems $\langle X, \circ \rangle$ and $\langle Y, * \rangle$ are called factors algebra of $\langle X \times Y \oplus \rangle$

The definition of direct direct product can be generalised on the one hand to any two algebric system of same type.

The operations in direct product we are defined in terms of corresponding operations of factor algebra

* Semigroups :

If S be a nonempty set and $\circ$ is binary operation on S, then algebric system $\langle S, \circ \rangle$ called semigroup.

If $\circ$ [composition] is associative then & $x, y, z \in S$
So

$$(x \circ y) \circ z = x \circ (y \circ z)$$

Semigroup associats on the binary relations, they are used in,
① computer architecture
② Formal language
③ Sequential machines

Semigroup have/ not have identity element.

If they have identity element then called as monoid

* Monoids :

A semigroup $\langle M, o \rangle$ with an identity element with respect to the operation o called as monoids

Algebric system $\langle M, o \rangle$ is called monoid if

$x, y, z \in M$

$(x \circ y) \circ z = x \circ (y \circ z)$ and

if $e \in M$

i.e, $e \cdot x = x \circ e = x$ called as monoids

Identity element for any binary operation if it exists it unique so, $\langle M, o, e \rangle$ also monoid can be mentioned

Question : Which is correct notation for monoids?

1. $\langle M, o \rangle$
2. $\langle M, o, e \rangle$
3. $\langle S, o \rangle$
4. None

ans : $\langle M, o \rangle$ and $\langle M, o, e \rangle$

If $\langle M, * \rangle$ is monoids and there is no gurantee that the two rows and columns are identical then

$a_i * e = a_i \neq a_j * e = a_j$

a_i = No of rows
a_j = No of columns

Ex : ① If $B(X)$ be any set from X to X with composition operation $\circ$ then

$\langle (B(X), \circ \rangle$ is monoid

② If S be nonempty set with $p(S)$ as power set then algebra
$\langle p(S), \cap \rangle$ and $\langle p(S), \cup \rangle$ are monoids with S and ϕ respectively.

Alphabet should be - not be finite or even countable

If V is nonempty set of symbols V will assume as

$V_1 = \{0, 1\}$
$V_2 = \{a, b, c \ldots z\}$
V_3, V_4 etc

An element of an alphabet is called letter, character symbol

A string is also called sequence, word or sentence depending upon its nature

A string consisting of m symbols $(m>0)$ is called a string of length m

Ex : let $V = \{a, b\}$; then string such that $m=2$
$V = \{aa, bb, ab, ba\}$

If $m=0$, i.e, empty string denoted by $\underline{\Lambda}$

The set of nonempty string denoted by ,
$V^{+} = V^{*} - \{\Lambda\}$

If $\alpha, \beta \in V^{*}$ with binary operation o then
$\alpha \cdot \beta = \alpha\beta$ called concatenation or catenation.

Ex : Let $V = \{a, b\}$ and consider strings abaab and bb.
The concatenation of these strings produces the string abaabb.

If we admit Λ (null) string in concatenation then $\Lambda a = a\Lambda = a$

$\langle V^{+}, o \rangle$ called as free semigroup.

* **Null property** -
If $\langle V^{*}, o \rangle$ is null then $\langle V^{*}, o, \Lambda \rangle$ is called monoids.

* **Cancellation** - If two strings α & β such that $\alpha, \beta \in V^{*}$ then $x \cdot \alpha_1 = \alpha$ and $x \cdot \beta_1 = \beta$ with

Page No.: Date: / /

$\alpha = \beta$ then
$$\alpha_1 . x = \beta_1 . x$$

$$\text{i.e } = \alpha_1 = \beta_1$$

* Partation of monoids :

If S be any nonempty set then partation of monoids $\Pi(S)$

If $S_1 = \{a, b\}$

$$\Pi(S_1) = \{\{\bar{a}, \bar{b}\}, \{\overline{a, b}\}\}$$

If $S_2 = \{a, b, c\}$

$$\Pi(S_2) = \{\{\bar{a}, \bar{b}, \bar{c}\}, \{\overline{a, b}, c\}, \{\bar{a}, \overline{b, c}\}, \{\overline{a, c}, \bar{b}\} \{\bar{S_2}\}\}$$

* If $P = \{P_1, P_2, ----\}$ and $Q = \{Q_1, Q_2, ---\}$ are two partotitions of a set S_1 then find $P * Q$

→ if $S = \{x_1, x_2, x_3, x_4, x_5, x_6\}$

$$P = \{\overline{x_1, x_2}, \overline{x_3, x_4, x_5}, \bar{x_6}\}$$

$$Q = \{\overline{x_1, x_2, x_3}, \overline{x_4}, \overline{x_5, x_6}\}$$

$$P * Q = \{\overline{x_1, x_2}, \overline{x_3}, \overline{x_4}, \overline{x_5}, \overline{x_6}\}$$

Take intersection of each and every element

$*$ ⇒ Associative and commutative.

⇒ if $\{\bar{S}\}$ single block identity

then $<\pi(S), *>$ or $<\pi(S), *, \{\bar{S}\}>$ is monoid

$P * P = P$ $*$ on $\pi(S)$ called product of partation.

* Sum of Partation :

Sum of Partation denoted by $\oplus$ and $\pi <\pi(S), \oplus>$ is also monoid

for any $P, Q \in \pi(S)$, a subset T of S is in $P \oplus Q$ if,

① T is the union of one or more element of P
② T is the union of one or more element of Q &
③ no subset of T satisfies ① & ② except T itself.

$P_1 = \{\overline{x_1, x_2}, \overline{x_3}, \overline{x_4, x_5, x_6}\}$

$Q_1 = \{\overline{x_1, x_2, x_3}, \overline{x_4}, \overline{x_5, x_6}\}$

$P_1 \oplus Q_1 = \{\overline{x_1, x_2, x_3}, \overline{x_4, x_5, x_6}\}$

$P \oplus Q = \{\overline{x_1, x_2, x_3, x_4, x_5, x_6}\}$

The sum of partation is having associative and commutative

In a monoid $\langle M, * \rangle$ the powers of any particular element, say $a \in M$, are defined as,

$$\left.\begin{aligned} a^0 &= e \\ a^1 &= a \\ a^2 &= a * a \\ a^{j+1} &= a^j * a \end{aligned}\right\} \text{ for } j \in N$$

The generalized associatives law will be

$$a^{j+k} = a^j * a^k = a^k * a^j \text{ for all } j, k \in N$$

A monoid $\langle M, *, e \rangle$ is said to be cyclic they having

$b, c \in M$ and

$b = a^m$

$c = a^n$

$$b * c = a^m * a^n = a^{m+n}$$

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

$b * c = c * b$

element a is called generator of cyclic monoid

* Homomorphism of semigroups and Monoids :

Let $<S, *>$ and $<T, \Delta>$ be any two semigroups and mapping from $g : S \rightarrow T$ such that for any two elements $a, b \in S$,

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

It is called as semigroup homomorphism.

Semigroup homomorphism is called a semigroup monomorphism, epimorphism or isomorphism depending on whether the mapping is one-to-one, onto or one-to-one onto respectively.

If we assume $<S, *>$ and $<T, \Delta>$ as algebric systems then having $a, b, c \in S$

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

$$= g(a) \Delta g(b) \Delta g(c)$$

$$\therefore g((a*b)*c) = g(a*(b*c))$$

Associative law :

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

* Identity law :

If $\langle S, * \rangle$ having identity e & $a \in S$ from $\langle S, * \rangle$ to $\langle T, \Delta \rangle$ then

$$g(a*e) = g(e*a) = g(a) \Delta g(e)$$

$$= g(e) \Delta g(a)$$

$$= g(a)$$

* Monoid homomorphism :

Let $\langle M, *, e_M \rangle$ and $\langle T, \Delta, e_T \rangle$ be any two monoids. A mapping $g : M \rightarrow T$ then for any two elements $a, b \in M$

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

$$g(e_M) = e_T$$

* Identity :

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

$$z * a = a * z = z$$

Where $\langle M, *, e_M \rangle$ and $\langle T, \Delta, e_T \rangle$ having $a \in M$

* Semigroups and Submonoids :

Submonoids :

If $< S, * >$ be semigroup and $T \subseteq S$ if the set T closed under operation $*$ then $< T, * >$ is semigroup.

similarly if $< M, *, e >$ be a monoid and $T \subseteq M$, T is closed under $*$ and $e \in T$ $< T, *, e >$ called submonoid of $< M, *, e >$

Prove $a * b = b * a$

We know, $a * a = a$

$b * b = b$

$$
\begin{aligned}
(a * a) * (b * b) &= (a * b) * (b * a) \\
&= a * (b * b) * a \\
&= a * b * a \\
&= b * a
\end{aligned}
$$

Hence,
$a * b \in S$ and $< S, * >$ is submonoid

Let $< S, * >$ and $< T, \Delta >$ be two semigroups. The direct product of $< S, * >$ and $< T, \Delta >$ is the algebraic system $\langle S \times T, \circ \rangle$ in which the operation $\circ$ on $S \times T$ is defined by

$$< s_1, t_1 > \preceq s_2, t_2 > = < s_1 * s_2 , t_1 \Delta t_2 >$$

If $\langle S, * \rangle$ and $\langle T, \Delta \rangle$ are monoids with e_S and e_T as their identity elements respectively. then their product $\langle S \times T, \circ \rangle$ is also monoid with $\langle e_S, e_T \rangle$ as identity element, because

$$\langle e_S, e_T \rangle \circ \langle s, t \rangle = \langle e_S * s, e_T \Delta t \rangle = \langle s, t \rangle$$

and

$$\langle s, t \rangle \circ \langle e_S, e_T \rangle = \langle s * e_S, t \Delta e_T \rangle = \langle s, t \rangle$$

* Groups :

Algebraic system $\langle S, * \rangle$ is called semigroup if $*$ binary operation is associative. If they have identity element e with $e \in S$ then called monoids

In addition if they satisfies inverse for each element called as group.

Definitions : A Group $\langle G, * \rangle$ is an algebraic system in which the binary operation $*$ on G satisfies 3 conditions.

① Associativity :

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

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

② Identity :

If $e, a \in G$ then

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

③ Inverse :

If , $x, x^{-1} \in G$ then

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

Group should satisfy above three properties.

* Proporties :

① Invertible :

if $a, b, c \in G$ and $a * b = b * c$

then $a = c$ $\forall$ $b \neq 0$ OR $b * a = c * b$, $a = c$

② Idempotent :

if $a \in G$ then $a * a = a$

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

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

$= e * a$

$= a$

Page No.:
Date: / /

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

The order of group $<G, *>$ denoted by $|G|$ is the no of elements of G. When G is finite.

Theorem : order of Group.

Every row and column in the composition table of group $<G, x>$ is a permutation of the element G.

Ex : ① $<\{e, a\}, *>$

$*$	e	a
e	e	a
a	a	a

② $<\{e, a, b\}, *>$

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

Ex : Let $G = \{\alpha, \beta, r, \delta\}$ and $*$ on G is given

α = identity

Now, composition table

*	α (e)	β	γ	δ
α (e)	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

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

1. $a^0 = e$
2. $a^{n+1} = a^n * a$
3. $(a^{-1})^n = a^{-n}$
4. $a^{m+n} = a^m * a^n$

e	a	b	c
e	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

Permutation Groups :

If $S = \{a, b, c\}$ be any set.
p = permutation (Groups) of set i.e., $p : S \to S$ bijective mapping.

Now consider,

$p(a) = c$
$p(b) = a$
$p(c) = b$

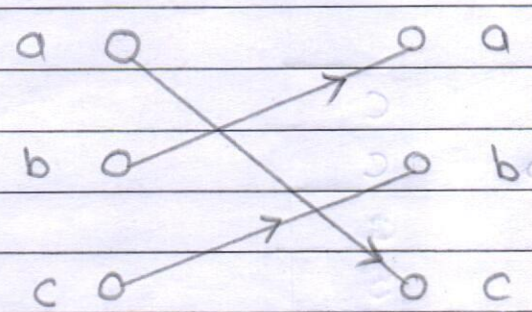
∴ Permutation :

$$p = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

According to different Notations of images

$$p = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \begin{pmatrix} a & c & b \\ c & b & a \end{pmatrix} = \begin{pmatrix} b & a & c \\ a & c & b \end{pmatrix}$$

Diagrametic representation of permutation



* Ex : $S = \{a, b\}$

No of permutation = 2 (P_1, P_2)

$$P_1 = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \qquad P_2 = \begin{pmatrix} b & a \\ a & b \end{pmatrix}$$

* Composition of permutations :

◇ denote binary operation on set representing the right composition of permutations.

If P_i and P_j are two permutations then composition will be $P_i \diamond P_j$.

As compaired to the composition of function we can use $\circ$

$$P_i \diamond P_j = P_j \circ P_i$$

composition of function is associative so the permutation is also associative.

If $S_2 = \{P_1, P_2\}$ then with $\langle S_2, \diamond \rangle$ is independent of the set of elements $\{a, b\}$

The degree of S_2 is 2

If any permutation $S_2 = \{P_1, P_2\}$ then permutation $= 2! = \underline{\underline{2}}$ degree $= \underline{\underline{2}}$

$S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ then $3! = 6$

If S_n is permutations of n elements its permutation group $\langle S_n, \diamond \rangle$ called symmetric group.

Where, permutation $= n! = 2! = 2$
degree $= n = 2$
order $= 2n = 4$

If the group P_1 and P_2 with $S_2 = \{P_1, P_2\}$ then,

◇	P_1	P_2
P_1	P_1	P_2
P_2	P_2	P_1

* Permutation of {1,2,3}

If set is $\{1,2,3\}$ then $= 3!$

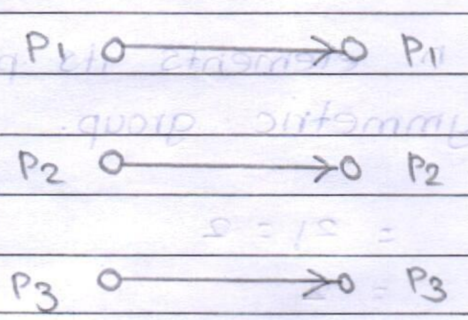
$S_3 = \{P_1, P_2, \dots P_6\}$

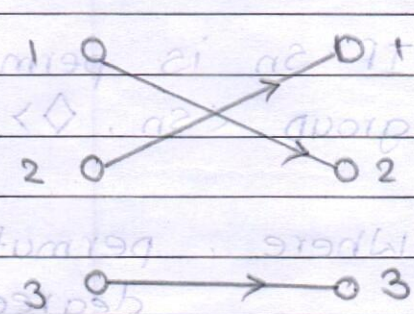
$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

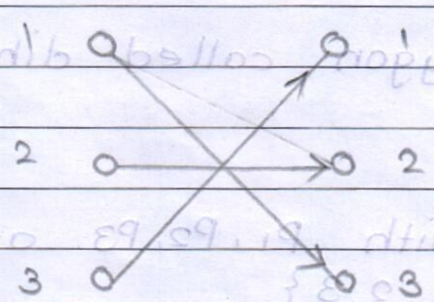
$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

P_1: $\quad$ P_2:

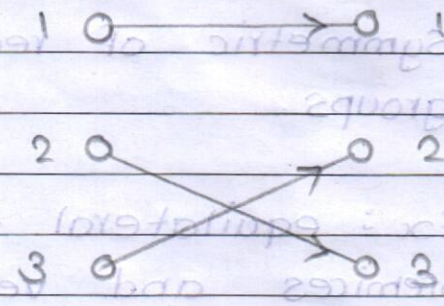




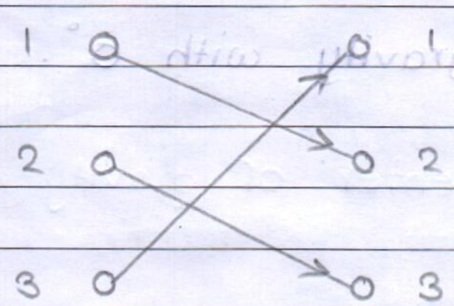
P_3 :



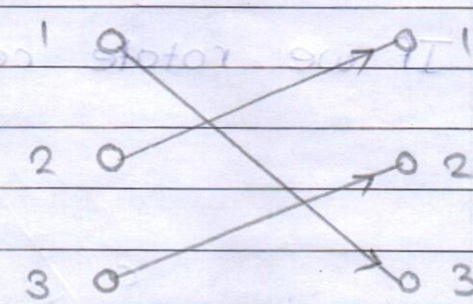
P_4 :



P_5 :



P_6 :



Now $P_3 \diamond P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \diamond \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

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

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

$$= P_4$$

$$\underline{P_3 \diamond P_5 = P_4}$$

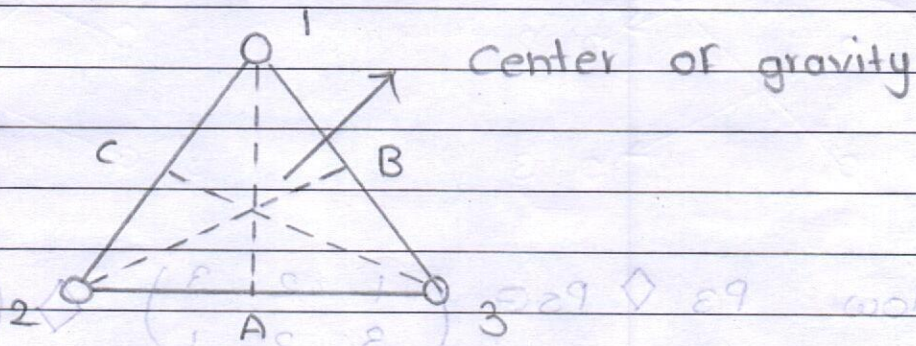
* Dihedral group :

Symmetric of regular polygon called dihedral groups.

Ex : equilateral trangle with P_1, P_2, P_3 as premices and vertices $\{1, 2, 3\}$

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

If we rotate centre of gravity with 0°.



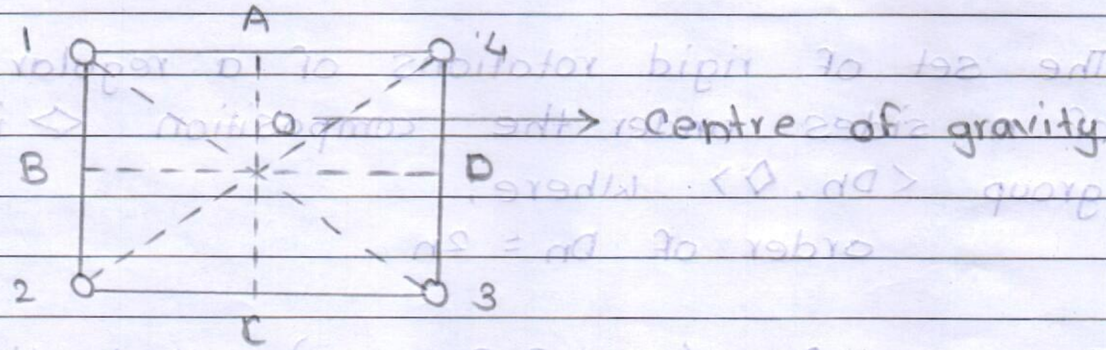
If we rotate it with 120° clock wise and counterclockwise then one of the result will be P_1, P_5, P_6

$$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

clockwise Anticlockwise

◇	P_1	P_5	P_6
P_1	P_1	P_5	P_6
P_5	P_5	P_6	P_1
P_6	P_6	P_1	P_5

In case of square,
$\langle D_4, \Diamond \rangle$ is dihedral group.



order = 8 = degree × 2

permutation group of degree = 4

order = clockwise and anticlockwise rotations of square of gravity.

clockwise rotations :

$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ $\quad r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ $\quad r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

counterclockwise operations :

$r_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ $\quad r_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$r_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ $\quad r_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$

If any polygon contain n sides
order = $2n$

The set of rigid rotations of a regular polygon of n sides under the composition $\diamond$ is a group $\langle D_n, \diamond \rangle$ where,
order of $D_n = 2n$

The group $D_n = (n = 1, 2, 3, ----)$ called dihedral group.

* Cyclic Group / Abelian:

A Group $\langle G, * \rangle$ is a said to be cyclic if there exist an element $a \in G$, such that every element of G can be written as same power of a. i.e., a^n for some integer n

if $p, q \in G$

$p = a^r \qquad q = a^s$ for some $r, s \in I$

$p * q = a^r * a^s$

$= a^{r+s}$

$= a^{s+r}$

$= q \times p$

$p * q = q * p$

* **Subgroups and Homomorphism :**

① Subgroups :

If $<G, *>$ be any group and $S \subseteq G$ be satisfies

① $e \in S$ and e is identity of $<G, *>$

② $a \in S$, $a^{-1} \in S$

③ for $a, b \in S$, $a * b \in S$

Then $<S, *>$ called subgroup of $<G, *>$

② Group Homomorphism :

If $<G, *>$ and $<H, \Delta>$ be two groups a mapping $g : G \to H$ is called group homomorphism from $<G, *>$ to $<H, \Delta>$ for any $a, b \in G$

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

$$g(e_G) = e_H$$

for any $a \in G$

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

for any $a \in G$, $a^{-1} \in G$

$$g(a * a^{-1}) = g(e_G) = e_H$$

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

$$g(a^{-1} * a) = g(e_G) = e_H$$

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

Before group called as group homomorphism it should be

1. Monomorphism — One to one
2. Epimorphism — onto
3. Isomorphism — one to one onto
4. Endomorphism — a group $\langle G, * \rangle$ to $\langle G, * \rangle$ is called endomorphism

While an isomorphism of $\langle G, * \rangle$ to $\langle G, * \rangle$ called automorphism.

* kernal :

If g be group homomorphism form $\langle G, * \rangle$ to $\langle H, \Delta \rangle$ the set of elements of G which are mapping into e_H the identity of it, is called kernel of homomorphism g and denoted by $ker(g)$

Theorem : Every finite group of n is isomorphic to a permutation group of degree 'n'.

Let $\langle G, * \rangle$ be any group of order 'n'

Let abc any element $a \in G$ then permutation of a
$a = P_a$

$P_a(c) = c * a$ for $c \in G$

Now
$P_e \diamond P_a = P_a \diamond P_e = P_a$ for any $a \in G$

$P_a^{-1} \diamond P_a = P_e$

for $a, b \in G$
$P_a \diamond P_b = P_{a*b}$

From above we prove that

$F(a*b) = f(a) \diamond f(b)$

* Group codes :

Group codes contain two things :
① Error Detection
② Error correction

Many system today contain telephone & communin line are corrupted by presence of noise.

① Error correcting :

strcture in the design of error-correcting codes is important.

First it faciliates finding the properties of a code; seoond, it makes the hardware realization of such code protical.

The first part of this section is concerned with a simple communication model and the basic notations of error correction.

The second part of the section deals with design of codes.

* communication model :

A communication process may take place in a varity of ways.

E.g. ① Telephone call
② sending a message by a telegram or a letter
③ using sign language.

Information is transformed from sender to receive
Ex: Water to electricity, music to speech etc.

An ideal communication system can be represented by at least three essential parts, namely
① Transmitter, sender or source
② channel or storage medium
③ Receiver

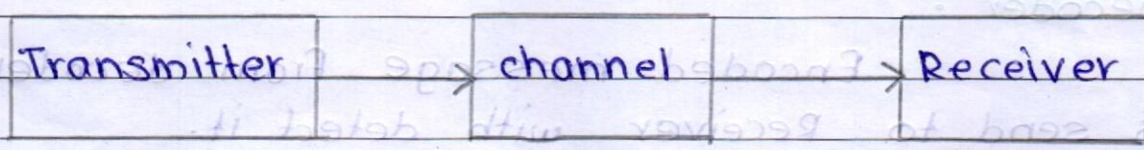


fig: General model of data communication system

Disturbance in communication is called noise.

Ex: wind, passing car, other voice etc.

A device that can be used to improve the efficie-ncy of the communication channel is encoder. which transforms incoming messages.

To improve the system we add encoder and decoder to the communication model.

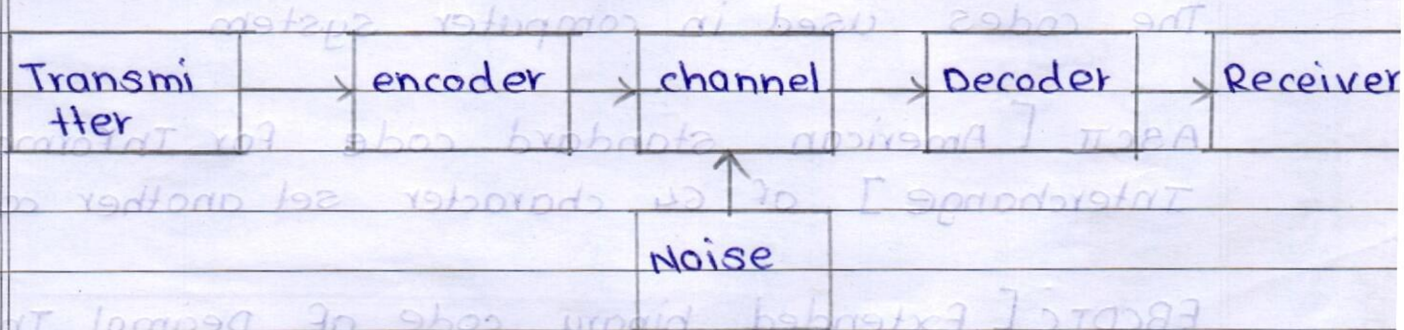


fig: General strcture of typical data communication system with noise.

Encoder :
IF the original message is with presence of noise then they transfor message to receiver with encoded form.

Decoder :
Encoded message from decoder is send to Receiver with detect it.

Any elements of the alphabet called symbol, letter or character.

A finite sequence of characters of alphabet called message or word.
Length of word $l(x)$ for x word
No of symbols in word.

The encoding or encipherring process or decoding or deciphering process takes place in one to one manner (mapping)

The codes used in computer system

ASCII [American standard code for Information Interchange] of 64 character set another code.

EBCDIC [Extended binary code of Decimal Inter-change code].

Binary channel - In many communication restricted binary valued alphabet to 0 and 1 called binary channel.

Let represent Alphabet {A, B, ... H} 8 alphabet by 3 binary codes digit. It is necessary to send 0 and 1 in particular manner.

Symbol	original code
A	000
B	001
C	010
D	011
E	100
F	101
G	110
H	111

Lucky Page No.:
Date : / /

		22/12	24/12	28/12
1	Satyajit	Jadhav	A	P
2	Komal	Abirekar	P	P
3	Adityi	Dongare	P	A
4	Umesa	Mulhalli	P	A
5	Rant	A	P	A
6	Ajay	Jadhav A	P	P
7	Deraj	~~Rucha~~	P	P
	Rucha		P	P