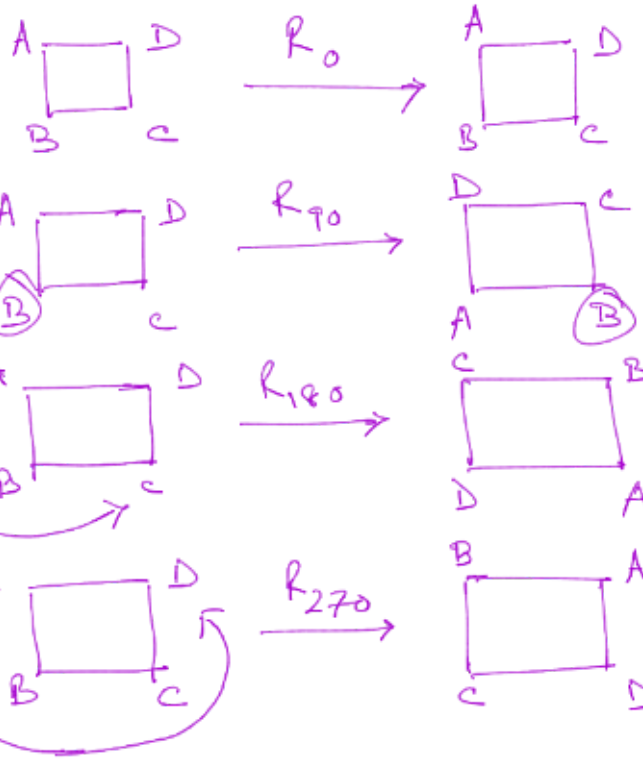
✓ Gallian

Rotation Sen Ghosh Mukhopadhay



$R_0 = R_{360}$

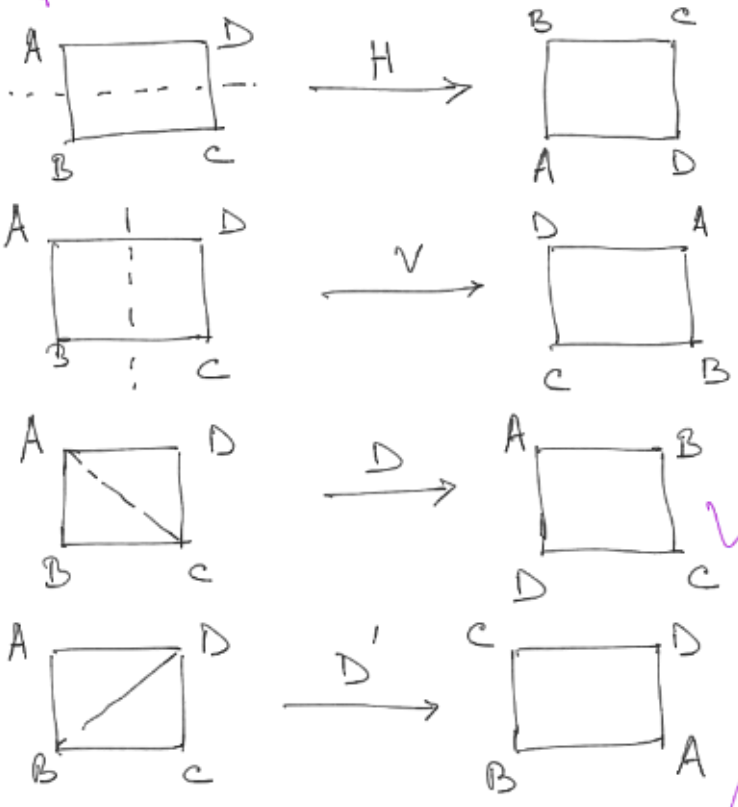
$R_{90} = R_{450}$

$(R_{-270}) = R_{n.360} + R_{90}$

(R_{-180})

(R_{-90})

Reflection :—



$H.H = R_0$

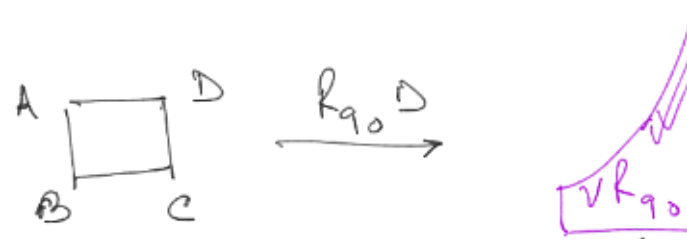
$V.V = R_0$

$D.D = R_0$

$D'.D' = R_0$

$HV = R_{180}$

$VR_{90} = D'$

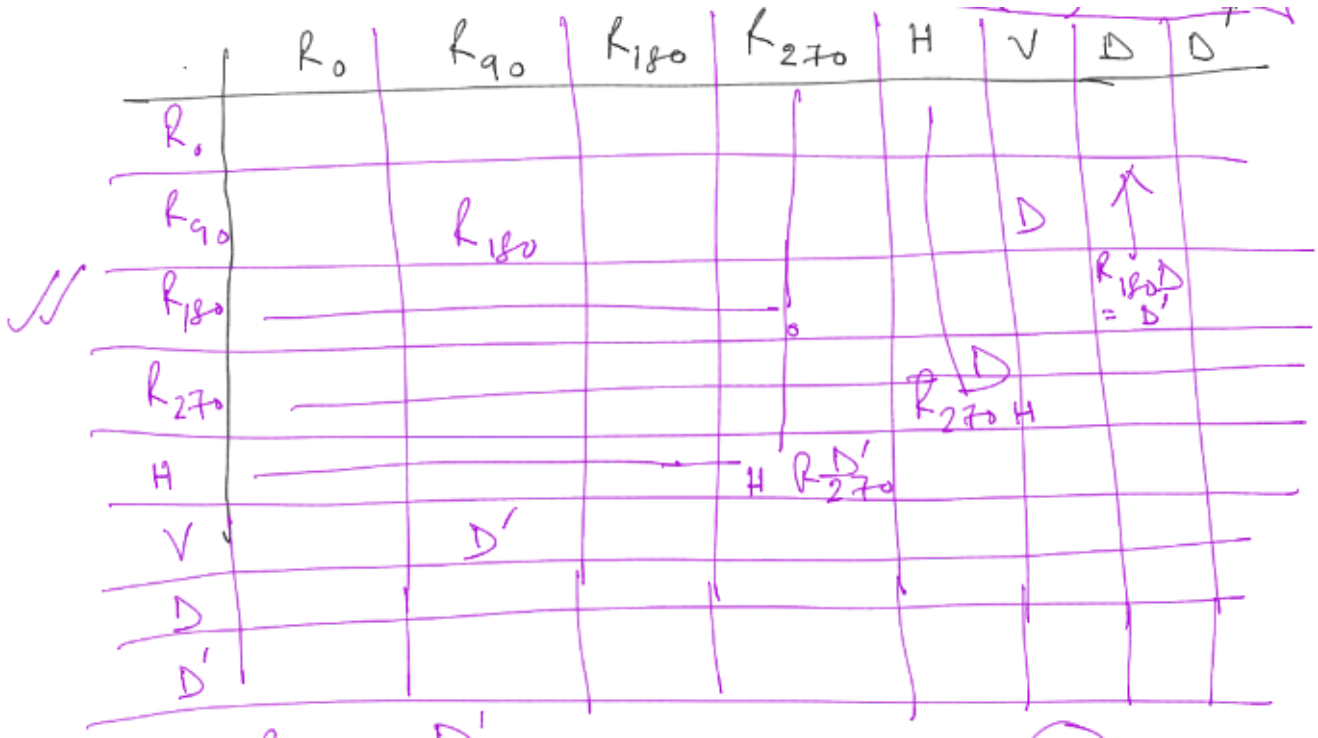


$VR_{90}(A) = V(B)$

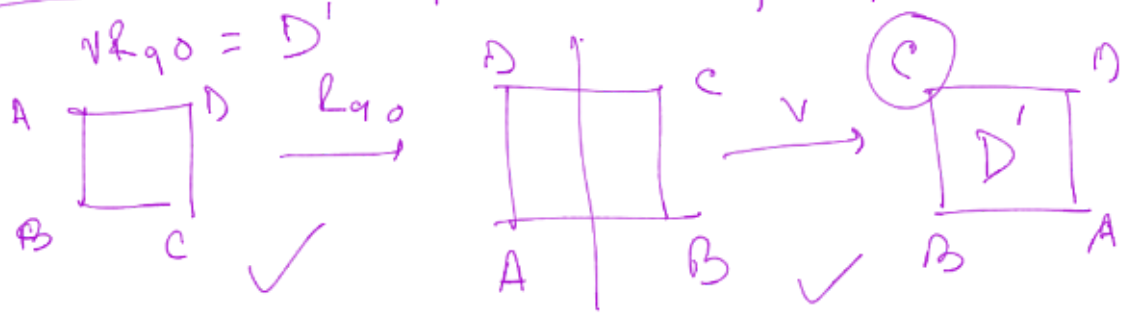
$VR_{90}(B) = V(C)$

$VR_{90}(C) = V(D) = A$

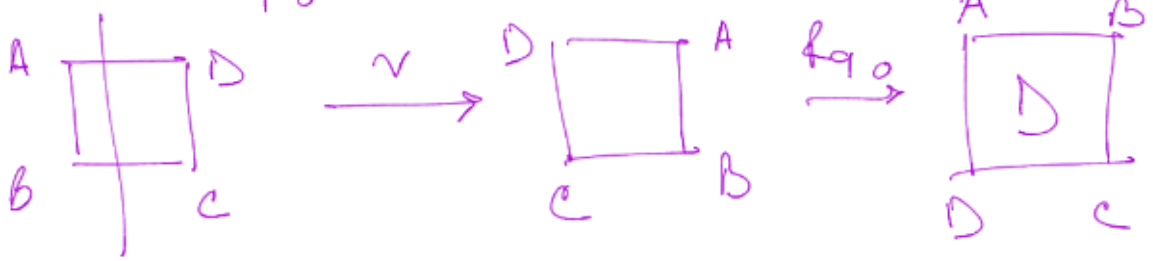
$VR_{90}(D) = C$



$VR_{90} = D'$



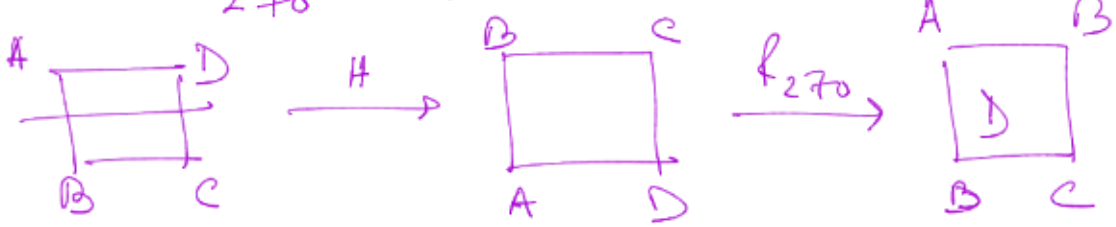
$R_{90}V = D$



$VR_{90} \neq R_{90}V$

$D' \qquad D$

$R_{270}H \neq HR_{270}$



$R_{270}H = D$

$$H \cdot R_{270^\circ} = D'$$

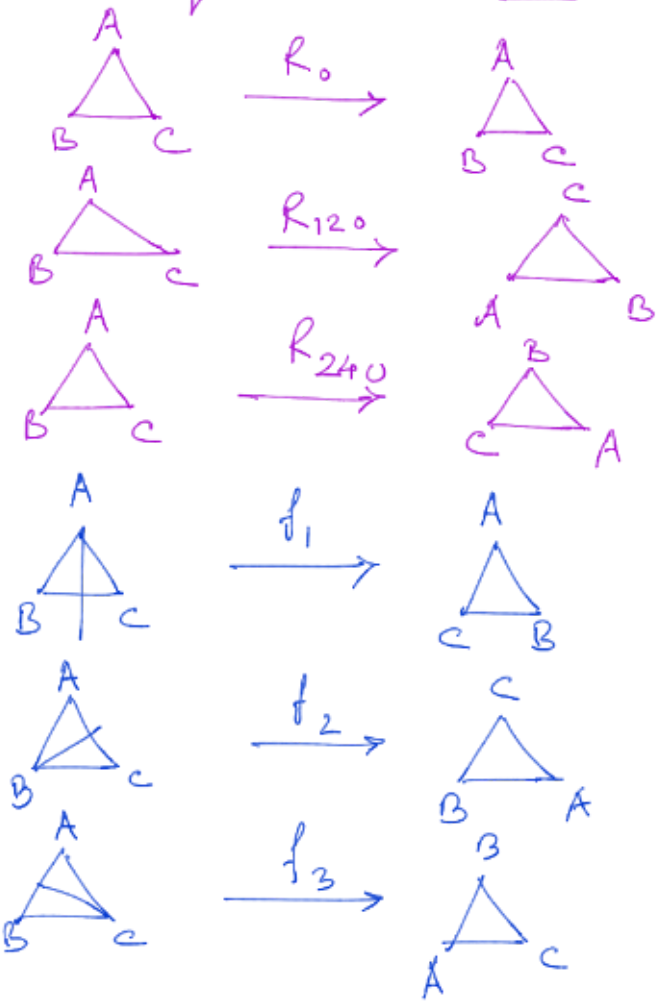
Cayley table

Def^{n}:— For any regular n-gon ($n \geq 3$), the corresponding group is called dihedral group of order $2n$. and it is denoted by D_n.

[* order of a group is the no of elements of the group]

$$D_4 = \{ R_0, R_{90}, R_{180}, R_{270}, H, V, D, D' \}$$
of order 8.

Equilateral triangle (D_3)



$$R_{120} = R_{\frac{360}{3}}$$

$$R_{240} = R_{2.\frac{360}{3}}$$

$$f_i^{-1} = f_i, \quad i = 1, 2, 3$$

$$f_i^2 = R_0$$

$$f_1 . f_1 = R_0$$

$$D_3 = \{ R_0, R_{120}, R_{240}, f_1, f_2, f_3 \}$$

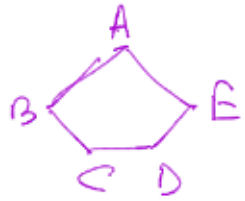
Is D_3 closed ? (H/W)

Is D_3 commutative? (#/H)

$f_1 . f_2 \neq f_2 . f_1$

$(R_{120}) \quad (R_{240})$

Regular Pentagon (D_5)



Rot $\rightarrow R_0, R_{\frac{360}{5}}, R_{2.\frac{360}{5}}, R_{3.\frac{360}{5}}, R_{4.\frac{360}{5}}$.

$R_{p.\frac{360}{5}} = R_{r.\frac{360}{5}}$, $p = 5.q + r$

$R_{33.\frac{360}{5}} = R_{3.\frac{360}{5}}$

Ref $\rightarrow f_1, f_2, f_3, f_4, f_5$.

Regular Hexagon (D_6).

Rot $\rightarrow R_0, R_{\frac{360}{6}}, \ldots, R_{5.\frac{360}{6}}$

Ref $\rightarrow f_i$, $i = 1(1)6$.

Regular n-gon.

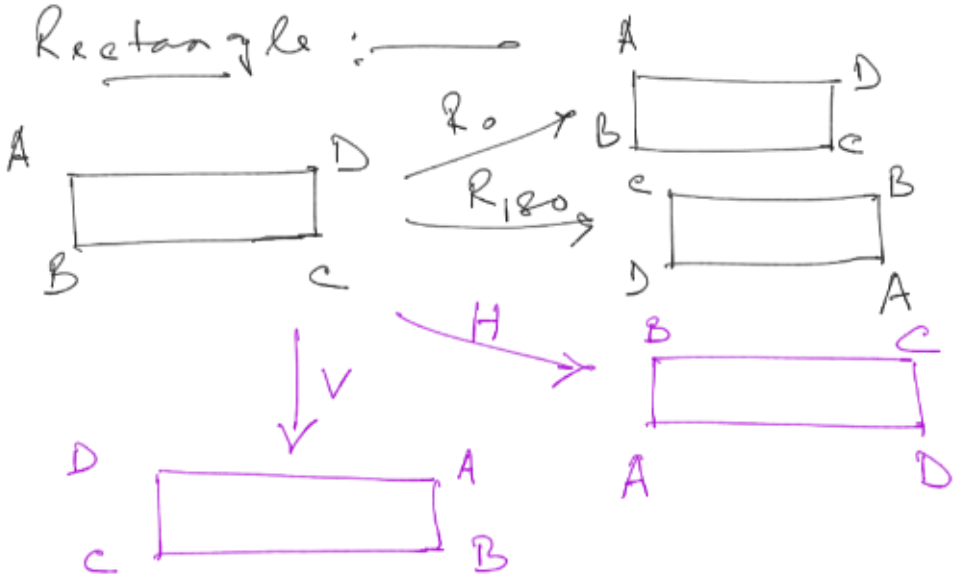
n rotations $\rightarrow R_0, R_{\frac{360}{n}}, R_{2.\frac{360}{n}}, \ldots, R_{(n-1)\frac{360}{n}}$.

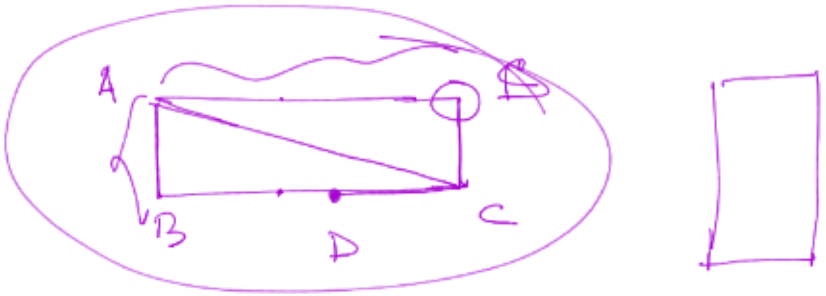
n ref :— f_i , $i = 1(1)n$.

n odd → The lines from vertices to the midpoint of the opposite side.

n even → The lines joining opposite vertices and opposite midpoints.

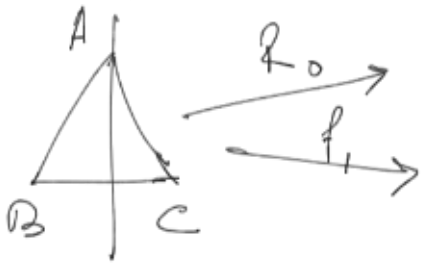
Rectangle :—





$X = \{ R_0, R_{180}, H, V \}$

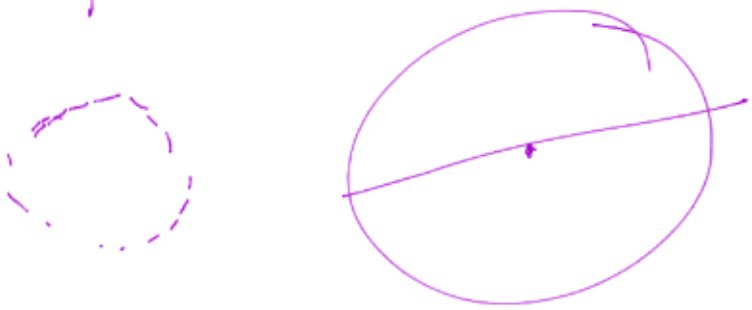
Isosceles :—

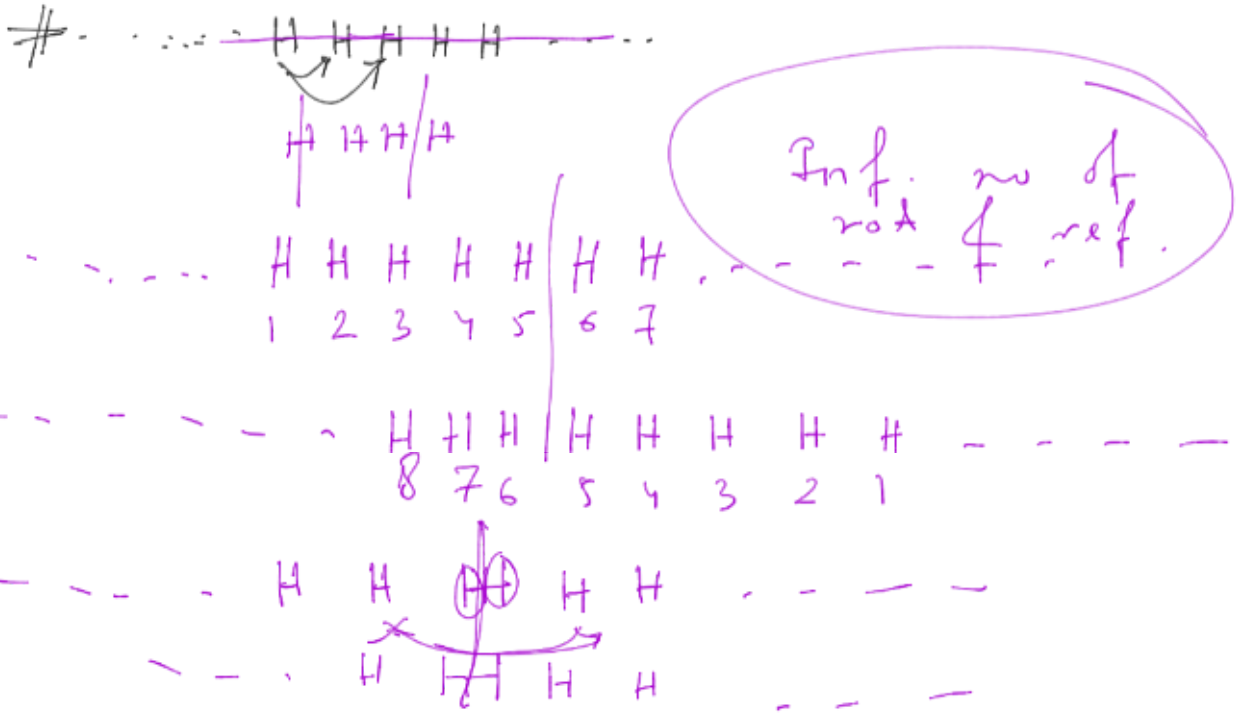


$f_1 = R_{180}$

circle :—

$\frac{360}{p}$, p rational





Dihedral group D_n ⇒ The group of symmetries of a regular n gon.

$\{R_0, R_{180}, H, V\} \longrightarrow$ Klein's 4 group.

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

$$= \{R_{90}, R_{90}^2, R_{90}^3, R_{90}^4, H, R_{90}H, R_{90}^2H, R_{90}^3H\}$$

$$= \{R_{90}, R_{90}^2, R_{90}^3, R_{90}^4 = R_0, H, R_{90}H = D', R_{90}^2H = V, R_{90}^3H = D\}$$

$R_{1\cdot\frac{360}{4}}, R_{3\cdot\frac{360}{4}}$

$$= \{\alpha, \alpha^2, \alpha^3, \alpha^4 = R_0, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$$

$$D_4 = \{\alpha, \beta : \alpha^4 = R_0 = \beta^2 ; \alpha\beta = \beta\alpha^3\}$$

$[\alpha = R_{90}, \beta = H]$

$\alpha\beta = \beta\alpha^3$??

α rot, β ref ⇒ $\alpha\beta$ is ref.

$\therefore (\alpha\beta)^{-1} = \alpha\beta$

$\Rightarrow \beta^{-1}\alpha^{-1} = \alpha\beta$

$\Rightarrow \beta\alpha^3 = \alpha\beta$

$[\beta^2 = R_0 \Rightarrow \beta^{-1} = \beta$
$\alpha^4 = R_0$
$\Rightarrow \alpha \cdot \alpha^3 = R_0$
$\Rightarrow \alpha^{-1} = \alpha^3]$

$$3 \equiv -1 \pmod 4$$
$$2 \equiv -2$$
$$5 \equiv 1$$

$\alpha^2\beta = \beta\alpha^2$, $\alpha^3\beta = \beta\alpha$

$\alpha^r\beta = \beta\alpha^{4-r}$ in case of D_4.

In D_4, what are the possibilities for α?

$\alpha^4 = R_0$, $\alpha = R_{90}, R_{270}$

$\alpha \neq R_{180}$ as $R_{180}^2 = R_0$.

If $\alpha = R_{180}$ $\alpha = R_0$, $\{\alpha, \alpha^2, \alpha^3, \alpha^4\}$ R_0, R_0, R_0, R_0

$\{\alpha, \alpha^2, \alpha^3, \alpha^4$ / $R_{180}, R_0, R_{180}, R_0\}$ R_{90}, R_{270} missing

R_{270}, $R_{270}^2 = R_{540} = R_{180}$,
$R_{270}^3 = R_{810} = R_{90}$, $R_{270}^4 = R_{1080} = R_0$
$R_{270}^3 = R_{180} \cdot R_{270} = R_{450} = R_{90}$

$$D_n = \{\alpha, \beta : \alpha^n = R_0 = \beta^2; \alpha^r \beta = \beta \alpha^{n-r}\}$$

$$(\alpha^r \beta)^{-1} = \beta^{-1} \alpha^{-r} = \beta \alpha^{n-r}$$

α r.t
β ref.

$[\alpha^n = R_0 = R_{360}$
$-r = 360 - r]$

$$D_{10} = \{R_0, R_{36}, R_{72}, \ldots, R_{9.36}, f_1, f_2, \ldots$$
$$= \{R_{36}, R_{36}^2, \ldots, R_{36}^9, R_0, f_7, R_{36} f_7, R_{36}^2 f_7, \ldots, R_{36}^9 f_7, f_{10}\}$$

$$R_{36}^{\cancel{4}} f_7 = R_{36}^9 f_7$$

$\Rightarrow$ [illegible]

$$\Rightarrow R_{36}^{-4} R_{36}^{4} f_7 = R_{36}^{-4} R_{36}^{9} f_7$$

$$\Rightarrow R_{36}^{-4+4} f_7 = R_{36}^{-4+9} f_7$$

$$\Rightarrow R_0 f_7 = R_{36}^{5} f_7$$

$$\Rightarrow R_0 f_7 f_7 = R_{36}^{5} f_7 f_7$$

$$\Rightarrow R_0 R_0 = R_{36}^{5} R_0$$

$$\Rightarrow R_0 = R_{36}^{5}$$

Conclusion :- $R_{36}^{p} f_7 \neq R_{36}^{q} f_7$

where $p \neq q$.

$$D_{10} = \{ R_{36}, f_7 : R_{36}^{10} = R_0 = f_7^2 ; R_{36}^{r} f_7 = f_7 R_{36}^{10-r} \}$$

$$\left(R_{36}^{r} f_7\right)^{-1} = f_7^{-1} R_{36}^{-r}$$

$$\Rightarrow R_{36}^{r} f_7 = f_7 R_{36}^{n-r}$$

Rot :- $R_0, R_{1.\frac{360}{10}}, R_{2.\frac{360}{10}}, R_{3.\frac{360}{10}}, f_7 R_{\frac{360}{10}}, \ldots, f_7 R_{9.\frac{360}{10}} \}$

we can choose,

$\lambda = R_{m.\frac{360}{10}}$, where $\gcd(m, 10) = 1$.

$m \in U(10)$

$$\left(R_{2.\frac{360}{10}}\right)^5 = R_0 \qquad = \{1, 3, 7, 9\}$$

$$\left(R_{\frac{360}{5}}\right)^5 = R_0$$

$$R_{4.\frac{360}{10}} = R_{2.\frac{360}{5}}$$

$$\left(R_{2.\frac{360}{5}}\right)^5 = R_0$$

$$R_{5.\frac{360}{10}} = \left(R_{\frac{360}{2}}\right)^2 = R_0$$

$$\left(R_{7.\frac{360}{10}}\right)^{10} = R_0$$

In case of D_n, we choose,

$$\alpha = R_{\frac{360}{n}}, R_{m.\frac{360}{n}} \text{ where } \gcd(m,n) = 1.$$

No of possibilities of m is $\phi(n)$.

D_{12}, $\alpha = R_{\frac{360}{12}}, R_{5.\frac{360}{12}}, R_{7.\frac{360}{12}}, R_{11.\frac{360}{12}}$

In D_n, why reflection followed by rotation is a reflection?

Why reflection followed by reflection is a rotation ?

$\Rightarrow D_n = \{ \alpha, \beta : \alpha^n = R_0 = \beta^2 ;$

$= \{ \underbrace{\alpha, \alpha^2, \ldots, \alpha^{n-1}}_{\text{Rot}}, \underbrace{\beta, \alpha\beta, \ldots \alpha^{n-1}\beta}_{\text{Ref}} \} \alpha^r \beta = \beta \alpha^{n-r} \}$

Take arbitrary reflection $\alpha^p \beta$, rotation α^q

$\alpha^q \cdot (\alpha^p \beta) = \alpha^{q+p} \cdot \beta$ (ref)

$= (\alpha^q \alpha^p) \beta$

$(\alpha^p \beta) \alpha^q = (\beta \alpha^{n-p}) \alpha^q$

$= \beta \cdot \alpha^{n-p+q}$ (ref)

$\alpha^p (\beta \alpha^q) = \alpha^p \cdot (\alpha^{n-q} \beta)$

$= (\alpha^p \alpha^{n-q}) \beta$ [Assoc]

$= \alpha^{p+n-q} \beta$

$\beta \cdot \alpha^{n-p+q} = \beta \cdot \alpha^{-p+q}$

$= \alpha^{n-(-p+q)} \beta$

$= \alpha^{n+p-q} \beta$

D_{12}, $p = 3$, $q = 7$

$\alpha^{p+n-q} \beta = \alpha^8 \beta = \beta \alpha^4$

$= \beta \alpha^{q-p}$

$\alpha^r \beta = \beta \alpha^{n-r} = \beta \alpha^{-r}$

Take two arbitrary ref. $\alpha^p\beta$, $\alpha^q\beta$

$$(\alpha^p\beta)(\alpha^q\beta) = \alpha^p(\beta\alpha^q)\beta$$

$$= \alpha^p \alpha^{n-q} \beta\beta$$

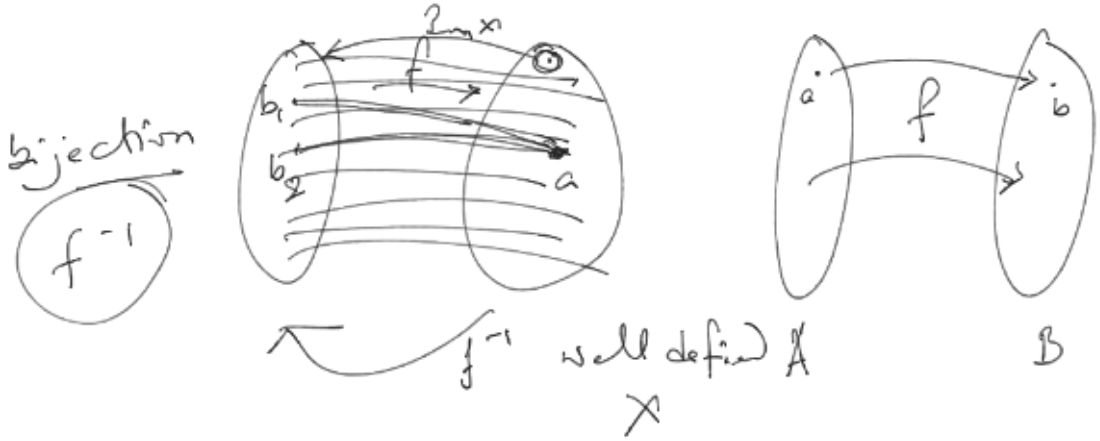
$$= \alpha^{n+p-q}\beta^2$$

$$= \alpha^{n+p-q}(\underline{\gamma o A})$$

Binary operation

$S \times S \longrightarrow S$

$(a, b) \longrightarrow a * b \in S.$



Def^n :— Let S be any nonempty set. A binary operation on S is a function that assigns each ordered pair of elements of S to an elements of S.

'$*$' on a set S will be a binary operator if

i) Exactly one element is assigned to each possible ordered pair of elements of S. ($a * b = c$, $\forall a, b$)

ii) for each ordered pair of elements of S, the element assigned to it belongs to S.

 # Def :— A binary operation of a set S is a function $S \times S$ to S. For each $(a, b) \in S \times S$, we have $a \circ b$ in S. ['$\circ$' is the binary operator]

/ a) S is closed under '$\circ$'.

b) $(S, \circ)$ is closed.

Ex:— i) $(\mathbb{R}, +)$ is closed.

'+' is a binary operator on $\mathbb{R}$.

ii) $(\mathbb{R}^*, +)$ $\quad \mathbb{R}^* \equiv \mathbb{R} - \{0\}$.

$-n + n = 0 \notin \mathbb{R}^*$.

'+' is not binary on $\mathbb{R}^*$.

iii) $M(\mathbb{R})$, the set of all real matrices.

Usual matrix addition is not binary as $A + B$ is not defined when A and B has different orders.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{pmatrix}$$

Induced operation :—

$(G, *)$ $\quad H \subseteq G$.

Let $*$ be a binary operation on G $\left[* : G \times G \to G\right]$ and H be a subset of G.

H is closed under $*$ if $a * b \in H$, $\forall\, a, b \in H$.

In this case, the binary operation on H (by restricting $*$ on H) is the induced operation on H.

Ex:— i) $(\mathbb{R}, +)$. $\quad \mathbb{Z} \subset \mathbb{R}$.

$(\mathbb{Z}, +)$ is closed. '+' is induced on $\mathbb{Z}$.

a) $(\mathbb{R}, +)$ $\quad \mathbb{R}^* \subset \mathbb{R}$

2) $(\mathbb{R}^*, +)$ is not closed. '+' is not induced on $\mathbb{R}^*$.

3) $H \subseteq \mathbb{Z}^+$, $H = \{ n^2 : n \in \mathbb{Z}^+ \}$

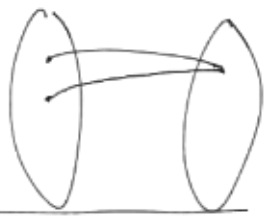
$(H, +)$ is not closed.

$(H, \cdot)$ is closed.

$a, b \in S$, $a_1, b_1 \in S$

$(a, b) \to a \circ b$ (unique)

$(a_1, b_1) \to a_1 \circ b_1$ (unique)



A = Math 2nd year $= \{ a_1, a_2, \ldots, a_{50} \}$

$(A, *)$ age of students are diff.

$a_1 * a_2 = c$, c is the youngest but older than both a_1 and a_2.

$*$ is Not binary.

Take a_i and a_j, the oldest and second oldest.

$a_i * a_j$ is not defined.

Ex:—

1) $\mathbb{Z}^+$. Define a binary operator $*$ on $\mathbb{Z}^+$ by

$a * b =$ smaller of a & b or the common value if $a = b$.

$7 * 23 = 7$, $11 * 11 = 11$.

2) $(\mathbb{Z}^+, *')$ by $a *' b = a$

$7 *' 23 = 7$, $23 *' 7 = 23$.

3) $(\mathbb{Z}^+, *'')$, by $a *'' b = (a * b) + 2$

[$*$ is defined in $\mathbb{Z}^+$]

$7 *'' 23 = (7 * 23) + 2 = 7 + 2 = 9$.

Commutative :—

Ex 1, 3 are commutative.

Ex 2 is not "

Associative :—

Ex 2 → $a *' (b *' c) = a *' b = a$

$(a *' b) *' c = a *' c = a$.

Ex 1 associative

Ex 3 :— $(2 *'' 5) *'' 9 = 4 *'' 9 = 6$

$2 *'' (5 *'' 9) = 2 *'' 7 = 4$

Not Associative.

Def" :— 1) A binary operation $*$ on S is commutative iff $a * b = b * a$, $\forall a, b \in S$.

2) A binary operation $*$ on S is associative iff $a * (b * c) = (a * b) * c$. $\forall a, b, c \in S$.

Group

Def^n :— A Group is an ordered pair $(G, *)$, where G is a nonempty set and $*$ is a binary operation on G s.t. the following properties hold —

i) **Associative prop :—**

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

ii) **Existence of identity :—**

$\exists\ e \in G$, s.t for any $a \in G$,

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

iii) **Existence of inverse :—**

for each $a \in G$, $\exists\ b \in G$ s.t.

$$a * b = b * a = e.$$

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

Abelian Group :—

If $*$ is commutative, then $(G, *)$ is an abelian / commutative group.

i.e. $a * b = b * a$, $\forall\ a, b \in G$.

Ex :—

1) $(D_n, \circ)$ is a group.

R_0 is the id element.

$f_i^{-1} = f_i$, f_i ref.

$R_p^{-1} = R_{-p}$

R_p^{-1} R_{-p}

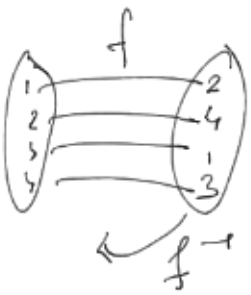
$$R_{\frac{360}{n}}^{-1} = R_{(n-1)\frac{360}{n}} = R_{-\frac{360}{n}}$$

$$R_{r\cdot\frac{360}{n}} = R_{(n-r)\frac{360}{n}} = R_{-r\cdot\frac{360}{n}}.$$

$$n - r \equiv -r \pmod{n}$$

2) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

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



S_n

D_4 $\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$ R_{90}

$\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}$ D

3) $(\mathbb{R}^n, +, \cdot)$ $(\mathbb{R}^n, +)$ abelian group.

$(V, +, \cdot)$ is a vector space.

$(V, +)$ is abelian group.

(c) $(\alpha) + (\beta)$ (1) $\alpha = \alpha$

$\mathbb{R}$ $\mathbb{R}^n$ $\mathbb{R}^n$ $\mathbb{R}$ $\mathbb{R}^n$

$\alpha + \beta = \beta + \alpha$

$\alpha + \theta = \alpha$

$\alpha + (-\alpha) = \theta$

$\alpha, \beta \in \mathbb{R}^n$

θ null vector in $\mathbb{R}^n$

$\theta = (0, 0, \ldots, 0)$

4) $(\mathbb{R}, +)$

$(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ form a group.

5) $(\mathbb{R}, \cdot)$ is not a group. $(\mathbb{Z}, \cdot)$ is not a group.

$(\mathbb{R}^*, \cdot)$ is a group.

6) $(\mathbb{Z}^*, \cdot)$ is not a group.

only $1, -1$ has inverse.

$2^{-1} = \frac{1}{2} \notin \mathbb{Z}^*$.

7) $(\mathbb{Z}, -)$ is not associative.

8) $(m\mathbb{Z}, +)$ is a group.

$(3\mathbb{Z}, +)$ ...

9) $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

$(\mathbb{Z}_n, +)$ $\quad \bar{2} \to \bar{0}$

$\bar{p} + \overline{(n-p)} = \bar{0}$

$\mathbb{Z}_{12}$, $\quad \bar{7} + \bar{5} = \bar{0}$

10) $(\mathbb{Z}_n, \cdot)$ is not a group.

$\bar{0}$ has no inverse.

11) $(\mathbb{Z}_n^*, \cdot)$ $\quad \mathbb{Z}_n^* = \{\bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

$\mathbb{Z}_8^* \to \bar{2} \cdot \bar{4} = \bar{0}$

$(\mathbb{Z}_7^*, \cdot)$ is a group.

$(\mathbb{Z}_p^*, \cdot)$, p prime, is a group.

$\bar{a} \in \mathbb{Z}_n^*$ has an inverse iff

$\text{g.c.d.}(\bar{a}, \bar{n}) = \bar{1}$

$\mathbb{Z}_{12}^* \to \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\} = U(12)$.

$\Rightarrow (U(12), \cdot)$ a group ??

·	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$1^{-1} = 1$

$5^{-1} = 5$

$7^{-1} = 7$

$11^{-1} = 11$

Group

$U(12) = \{ \bar{1}, \bar{5}, \bar{7}, \overline{11} \}$

$A = \{ R_0, R_{180}, H, V \}$ } equivalent (Isomorphic)

$U(n) = \{ x \in \mathbb{N} : x < n ; \gcd(x, n) = 1 \}$

$|U(n)| = \phi(n)$

order of $U(n)$

If n is prime, let $n = p$.

$U(p) = \{ \bar{1}, \bar{2}, \ldots, \overline{p-1} \}$

$= \mathbb{Z}_p^*$

12) $G = \{ e, a, b, c \}$ s.t.

$a^2 = b^2 = c^2 = e$.

$(G, \cdot)$ is an abelian group. It is called Klein's 4 group. (K-4 group)

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

$a \cdot b \neq e$ [Uniqueness of inverse]

as $a \cdot a = e$

$a \cdot b = a \Rightarrow b = e$ [Left cancellation law]

$a \cdot b = b \Rightarrow a = e$ [Right cancellation

$a \cdot b = a \Rightarrow a = e$ [Right cancellation law]

$\therefore \quad a \cdot b = e.$

K - 4
U(12)
Group of Sym. for rectangle
$= \{ R_0, R_{180}, H, V \}$

} Equivalent (Isomorphic)