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}

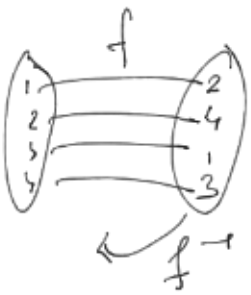
$$R_{\frac{360}{n}}^{-1} = R_{(n-1)\frac{360}{n}} = R_{-\frac{360}{n}}$$

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

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

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)