$a \in G$

#

$a * b = a + b - 1$

$4 * 5 = 8$

$a \oplus b = a + b - 1$

$(\mathbb{Z}, \oplus)$ ✓

$a \oplus e = a$

$a + e - 1 = a$

$e = 1$

$H = \{\ldots a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots\}$

$a^n = a * a * \cdots * a$ ($n$ times.)

$* \to +$: $a^n = na$

$* \to *$: $a^n = a^n$

$a \oplus 1 = a + 1 - 1$

$= a$

$x \circledast y = x^y$

$(x^2)^4 = x^8$

$= x$ //

$x * (y * 2)$ 9

$= x^{y^2}$

$(x * y) * 2$

$= (x^y) * 2$

$= (x^y)^2$

$= x^{y \cdot 2}$

$\{1, 3, \ldots\}$ $a \in G$

$U(10) = \{1, 3, 3^2, 3^3, \ldots\}$

$= \{1, 3, 9, 7, \ldots\}$

$H = \{a^n : n \in \mathbb{Z}\}$

$H \leq G$.

$\langle a, b \rangle$

**Cyclic group:** ( generated by a single element )

A group $G$ is called a cyclic group if there is an element $a \in G$ s.t

$$G = \{a^n : n \in \mathbb{Z}\}$$

denoted as: $G = \langle a \rangle$

In this case, '$a$' is called a generator of $G$.

i.e. $[x \in G = \langle a \rangle \Rightarrow x = a^{(n)} : n \in \mathbb{Z}]$

$a^n \to n \cdot a$

Eg: $G = (\mathbb{Z}, +)$ .

Then $G$ is a cyclic group generated by $1$. It can also be generated by $-1$.

# If '$a$' is a generator of $G$. then

$a^{-1}$ is also a generate of $G$.

# $Z_n := \{0, 1, 2, \cdots n-1\}$. is a cyclic group (can be) generated by: 1 and n-1.

# In $Z_8$;

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $+_8$ (n, n-1)

$= \{1^8, 1^1, 1^2, \cdots 1^7\}$.

~~Generators are not unique~~

$1^1 = 1$

$1^2 = 2$

$1^3 = 3$

$1^4 = 4$

$\vdots$

$1^7 = 7$.

$3^1 = 3$ $\quad 3^5 = 7$

$3^2 = 6$ $\quad 3^6 = 2$

$3^3 = 1$ $\quad 3^7 = 5$

$3^4 = 4$ $\quad 3^8 = 0$

$Z_8 = \{3^8, 3^3, 3^6, 3^1, 3^4, 3^7, 3^2, 3^5\}$

$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 6, \quad 2^4 = 0$

$H = \{0, 2, 4, 8\} \subseteq Z_8$

'2' is not a generator of $Z_8$.

**Observation:**

Let $G = \langle a \rangle$.

If $(k, n) = 1$; then $a^k$ will also be a generator of $G$.

In $Z_8$ : $n = 8$.

$(k, 8) = 1$

$k = 1, 3, 5, 7$

Choose $a = 1$

$a^1 \rightarrow (1)^1 = 1$

$a^3 \rightarrow (1)^3 = 3$

$a^5 \rightarrow (1)^5 = 5$

$a^7 \rightarrow (1)^7 = 7$

} generators of $Z_8$.

**Order of elements of a Cyclic group**

Let $G = \langle a \rangle$ be a finite Cyclic group. i.e $|G| = n$.

Then for all $x \in G$

$\Rightarrow x = a^n : n \in Z^+$.

$$O(a^k) = \frac{n}{(k,n)}$$

If $a^k$ is a generator; $(k,n) = 1$.

$$O(a^k) = n = |G|.$$

$\Rightarrow$ In Cyclic group; order of generator = order of $G$.

$(\!(Z_8)\!)$

$O(1) = \frac{8}{(1,8)} = 8$

$O(2) = \frac{8}{(2,8)} = \frac{8}{2} = 4$

$O(3) = \frac{8}{(3,8)} = 8$

$O(4) =$

$O(5) =$

$O(6) =$

$O(7) =$

$x^n = 1$

**Eg:** The $n^{th}$ roots of unity forms a (under multiplication) Cyclic group ie

$$G = \{1, \omega, \omega^2, \ldots\ldots \omega^{n-1}\}$$

$\because \omega^n = 1$

Take $n = 10$

$$G = \{1 = \omega^{10}, \omega, \omega^2, \ldots \omega^9\} = \langle \omega \rangle$$

$\therefore$ The generators of $G$ are:

$\omega^1, \omega^9, \omega^3, \omega^7$.

$(\omega^3)^4 = \omega^{12} = \omega^{10} \cdot \omega^2 = 1 \cdot \omega^2$

---

$xy = yx$

$x = a^m$

$y = a^k$

$xy = a^{m+k} = a^{k+m} = yx$

# Every Cyclic group is an abelian group.

$a^m$ $a^n$

A B

$a^1, a^2, a^3, a^4$

$a^1 \cdot a^3 = a^4$

$a * a * a * a$

$1+3$ $3+1$

$a^4 : a^4$ $a^3 a^1$

AC = CA

But Converse is not true

Think

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

$1^2 = 1$

$5^2 = 1$

$7^2 = 1$

$11^2 = 1$

not cyclic

\# under multiplication

Prove that $\{1, -1, i, -i\} : i^2 = -1$;
is a cyclic group. Find generators also.

$(i)^{-1}$

$i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

$\frac{1}{i} \rightarrow i$

$-i$

\# Every subgroup of a cyclic group is cyclic.

# Permutation Group

A map 'f' from S to S (S is any set) is called a permutation if f is 1–1 and onto.

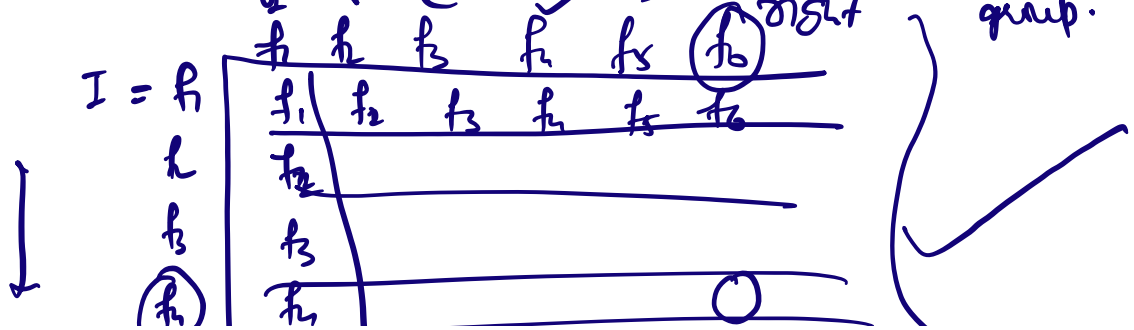
Let $|S| = 3$ (finite) i.e. $S = \{a, b, c\}$

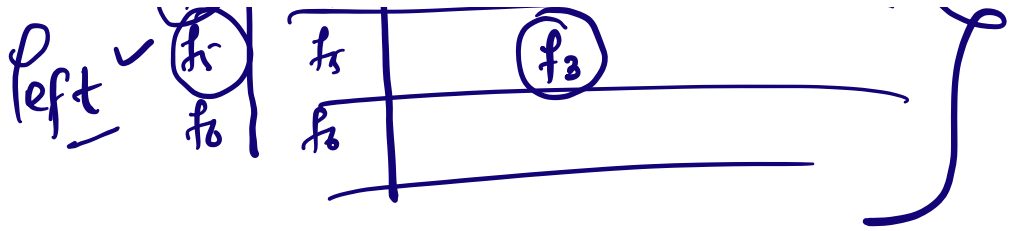
$$f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad f_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

$$f_3 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \quad f_4 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

$$f_5 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \quad f_6 = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

$P_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$ is a group (check it), called a permutation group.



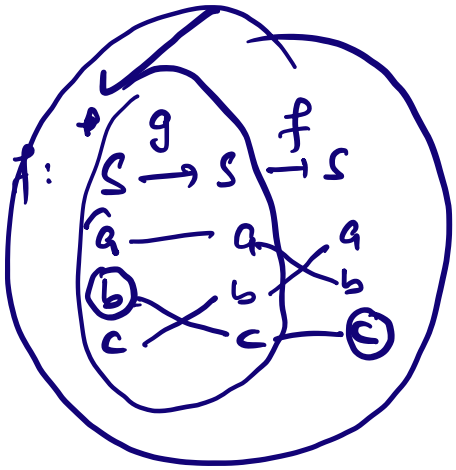



$f(x)$ $g(x)$

$f \circ g(x)$


$g \circ f(x)$

$= g(f(x))$

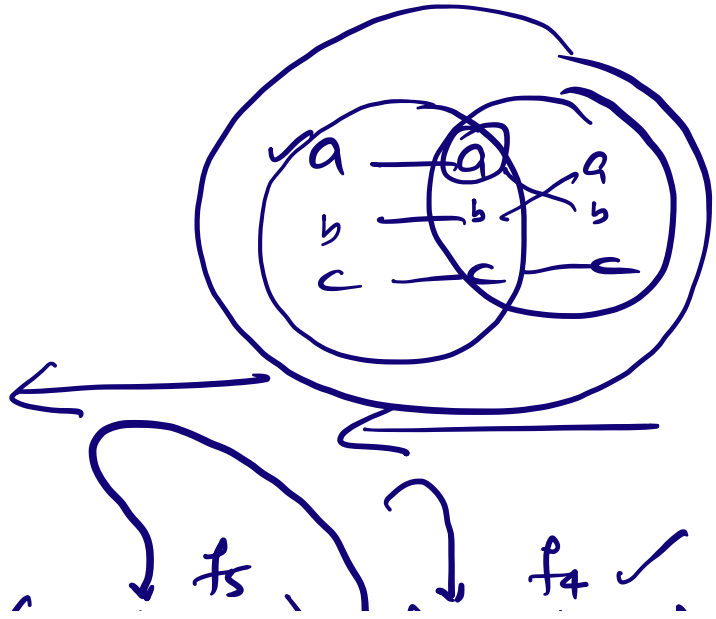



$f \circ g$

$$\begin{pmatrix} a \to b \\ b \to c \\ c \to a \end{pmatrix}$$

$(f \circ g)(a) = f(g(a))$

$= f(a) = b.$



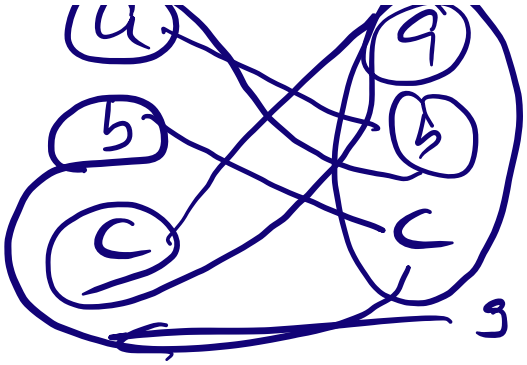
$$f_5 \cdot f_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

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

$$f_5 \cdot f_4 = f_3$$

$$f = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \quad f^{-1} = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}^{-1} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$




(#) A group is a permutation group if its elements are permutations.
∴ $P_3$ is a permutation group.

Therefore any subgroup of $P_3$ is also a permutation group.

# Check $P_3$ is a group. (Try ~~decomposition~~ composition table)

# Find Identity element in $P_3$.

# Inverse of all elements of $P_3$.

# The order of all elements of $P_3$.

# Find all possible subgroups of $P_3$.

# Check if $P_3$ is Abelian? (ans No)

# Check if $H_3$ is abelian! (Yes)

$H_1 = \{\text{identity}\}$

$H_2 = P_3$.

$H_3 = \{f_1, f_2\}$

| | $f_1$ | $f_2$ |
|---|---|---|
| $f_1$ | $f_1$ | $f_2$ |
| $f_2$ | $f_2$ | $f_1$ |

$n$

$(f) = \text{Identity}$

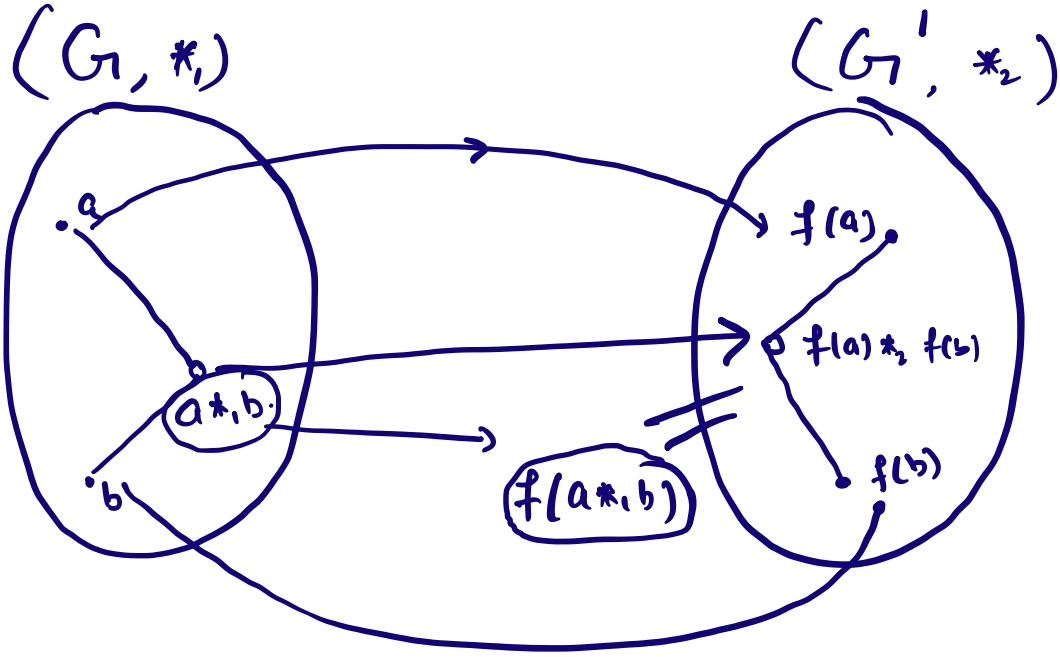
$a \in G$.

$H = \langle a \rangle$

**Observation:**

A subgroup of a non-abelian group can be an abelian group

## Homomorphism



$$f(a *_1 b) = f(a) *_2 f(b)$$

Let $G$ and $G'$ be