$a \in G$

#

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

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

$a * b = a + b - 1$

$4 * 5 = 8$

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

$(\mathbb{Z}, \oplus)$ ✓

$a \oplus e = a$

$a + e - 1 = a$

$e = 1$

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

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

$a \oplus 1 = a + 1 - 1 = a$ ✓

$x * y = x^y$

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

$x * (y * 2)$

$(x * y) * 2$

$(x^y) * 2$

(x^{yz})

$x * (y^2)$

x^{y^2}

$a \in G$

$U(10) = \{1, 3, 3^2, 3^3, a, a3, a3^2, a3^3\}$

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

$H \leq G$.

$\langle a, b \rangle$

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

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

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

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

i.e $[x \in G = \langle a \rangle \Rightarrow x = a^n : n \in Z]$

$a^n \to n \cdot a$

Eg: $G = (Z, +)$.

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;

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

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

~~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.

Observations

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 $a = 1$

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

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

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

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

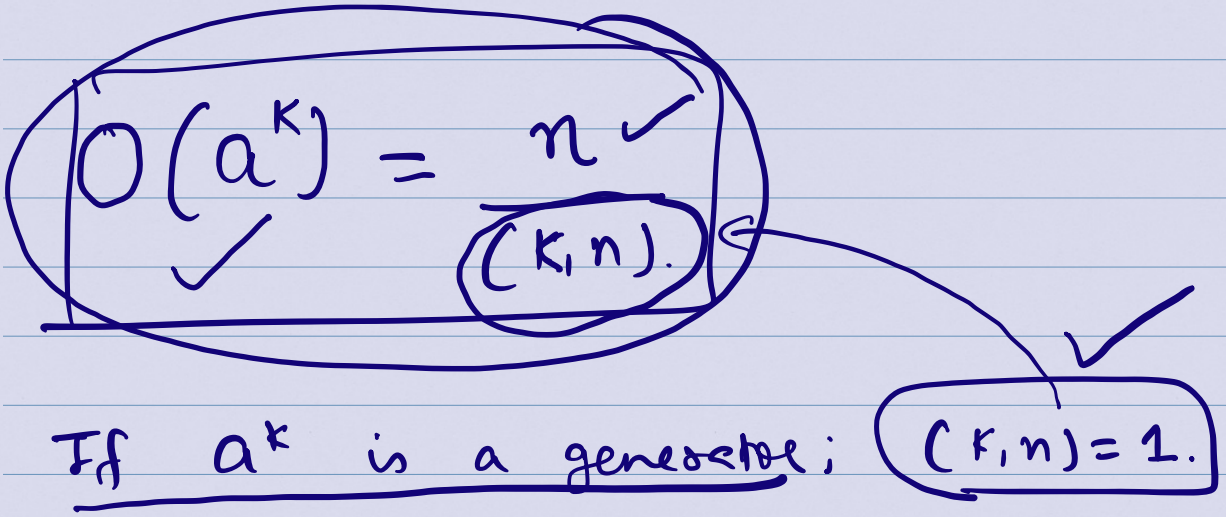
} generators of Z_8.

Order of elements of a Cyclic group

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

Then for all $x \in G$

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



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 Cyclic group ie (under multiplication)

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

$\because \omega^n = 1$

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^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.

$(i)^{-1} = ?$

$i^1 = i$

$i^2 = -1$

$i^3 = -i$

$i^4 = 1$

$\frac{1}{i} \rightarrow i^3$

$-i$

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.

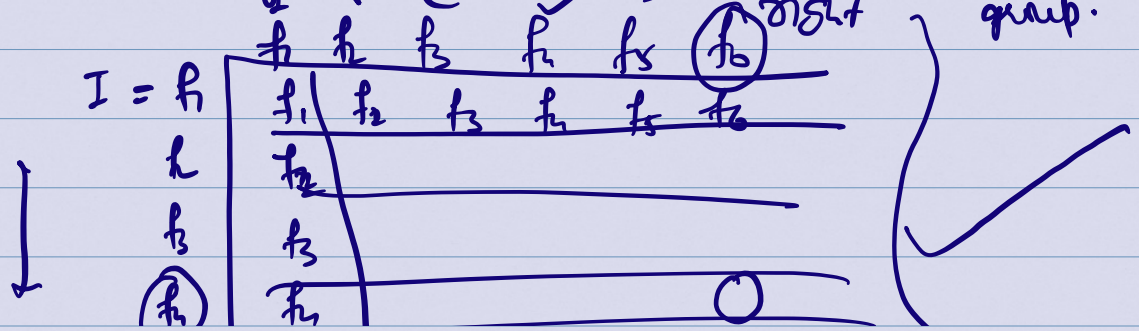
Let $|S| = 3$ (finite) i.e. $S = \{a, b, c\}$

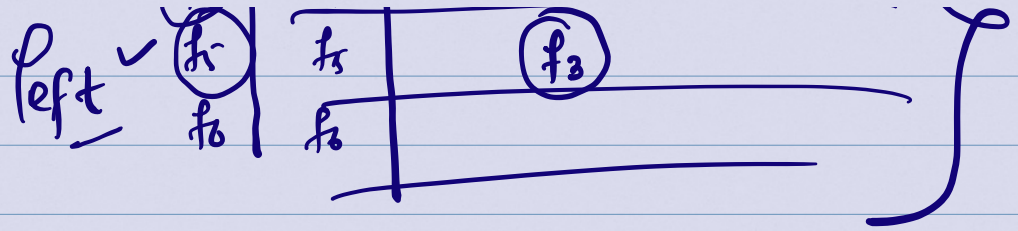
$$f_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad f_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

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

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

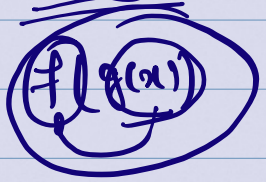
$P_3 = \{ f_1, f_2, f_3, f_4, f_5, f_6 \}$ is a group (check it), called a permutation group.





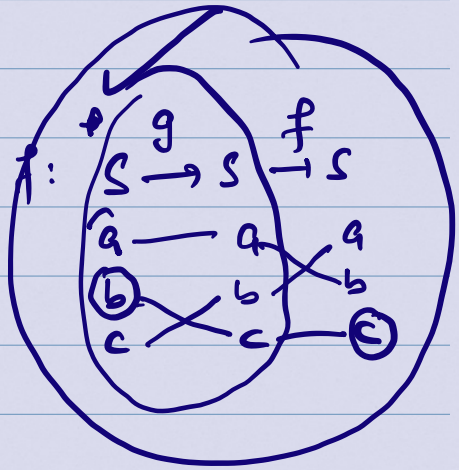
$f(x)$ $g(x)$

$f \circ g(x)$



$g \circ f(x)$

$= g(f(x))$

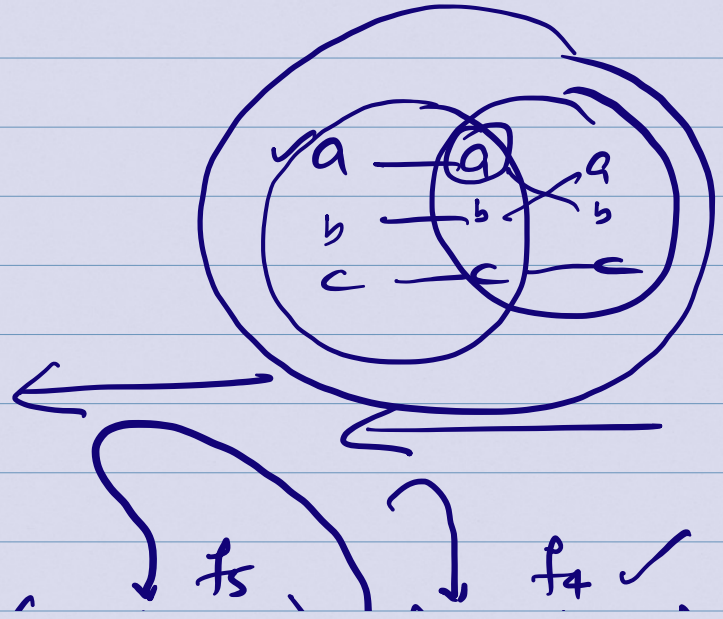


$f \circ g$

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

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

$= f(a) = b.$



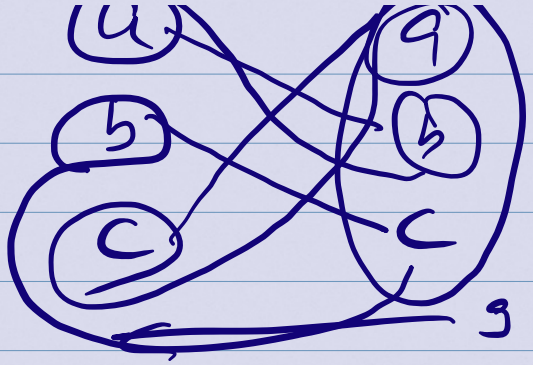
$$f_5 \cdot f_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

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

$$f_5 \cdot f_4 = f_3$$

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

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



(#) 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 ~~decompose~~ 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 S_3 is abelian! (continued)

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

$H_2 = P_3$.

$H_3 = \{f_1, f_2\}$

	f_1	f_2
f_1	f_1	f_2
f_2	f_2	f_1.

$n \swarrow$

$(f) = Iden$

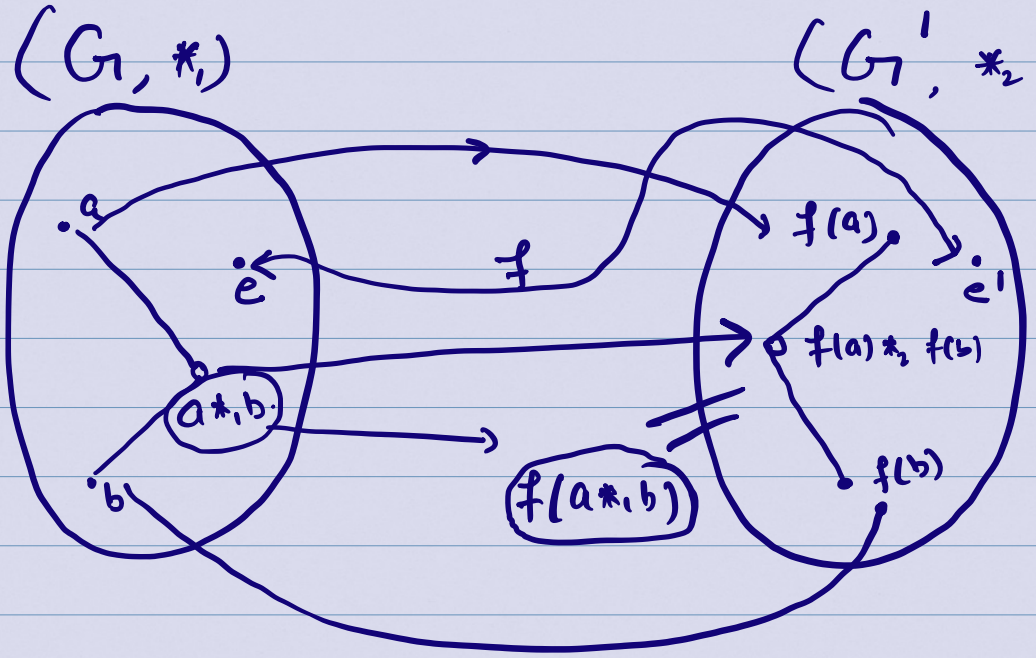
$a \in G$.

$H = \langle a \rangle$

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 two groups under $*_1$ and $*_2$ resp. Then a map

$$f: (G, *_1) \longrightarrow (G', *_2)$$

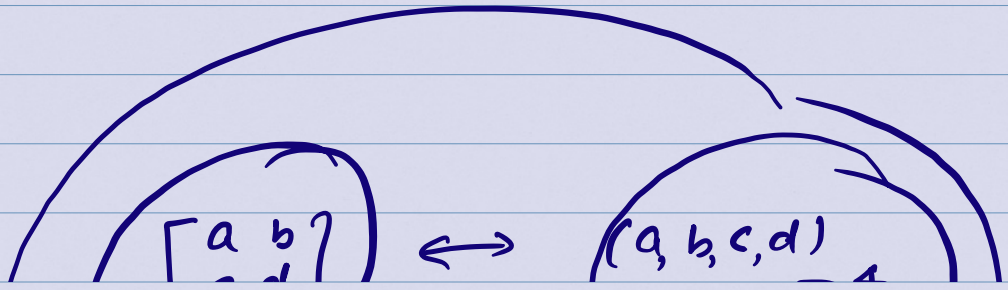
is called homomorphism if

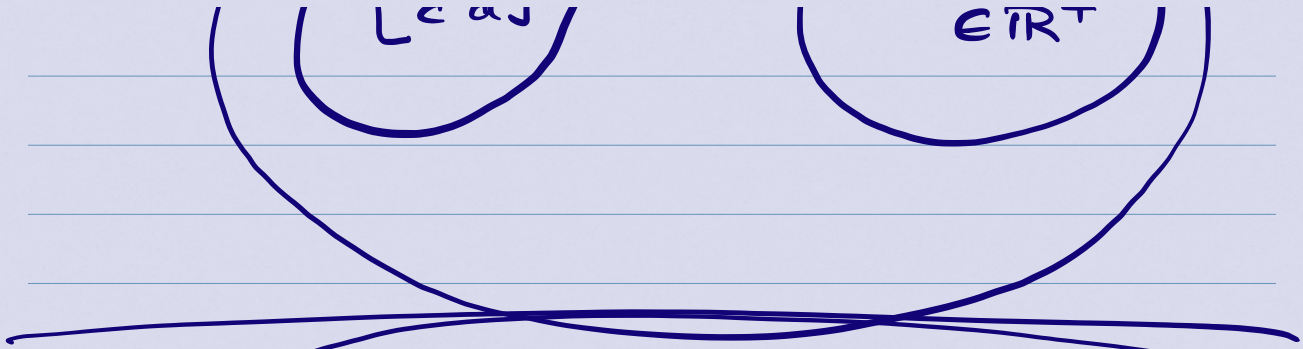
$$f(a *_1 b) = f(a) *_2 f(b)$$

Isomorphism: Homomorphism + [(1-1) + (onto)]

f^{-1} exists.

$G \cong G'$





Two Imp prop of homomorphisms

Let $f: G \longrightarrow G'$; f is homomorphism

Then (i) $f(e) = e'$; where e is the identity of G.

e' is the identity of G'.

How?

$$e *_1 e = e$$

$$\Rightarrow f(e *_1 e) = f(e)$$

$$\Rightarrow f(e) *_2 f(e) = f(e).$$

$$\Rightarrow (f(e))^{-1} *_2 [f(e) *_2 f(e)] = (f(e))^{-1} *_2 f(e)$$

$$\Rightarrow e' *_2 f(e) = e'$$

$$\Rightarrow \boxed{f(e) = e'}$$

(ii) $(f(a))^{-1} = f(a^{-1})$

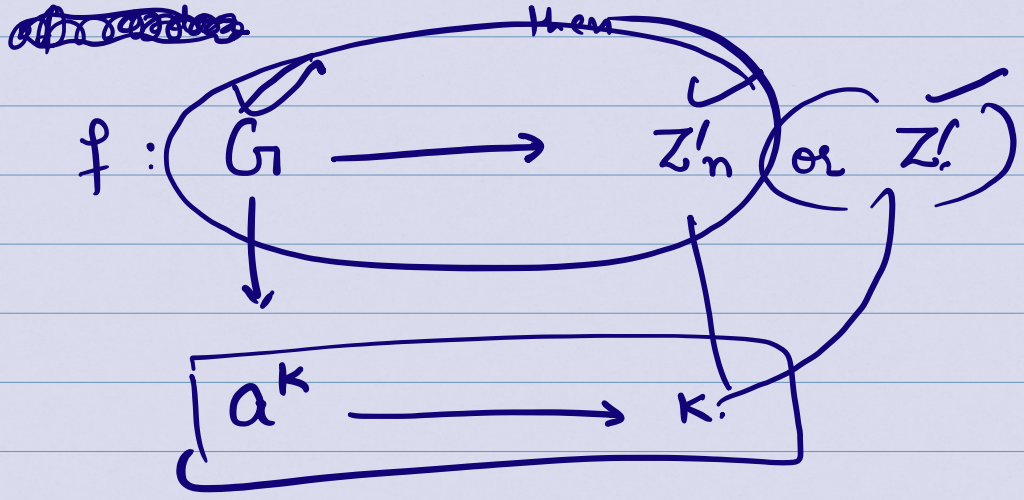
$$a *_1 a^{-1} = e = a^{-1} *_1 a$$

$$\Rightarrow f(a) *_2 f(a^{-1}) = e' = f(a^{-1}) *_2 f(a)$$

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

(#) Any finite Cyclic group of order n is isomorphic to Z'_n; and any infinite Cyclic group is isomorphic to Z'.

→ If 'a' is a generator of a cyclic group G.



Claim is; f is isomorphism.

$a^{k_1}, a^{k_2} \in G.$

$$f(a^{k_1} \odot a^{k_2}) = f(a^{k_1+k_2}) = k_1 + k_2 = 1$$

$$f(a^{k_1}) \oplus f(a^{k_2})$$

$G \cong Z_n$ or $G \cong Z_\infty$. Conclusion

$U(10) = \{1, 3, 7, 9\}$ → Cyclic

$U(5) = \{1, 2, 3, 4\}$ → Cyclic

$U(10) = \langle 3 \rangle = \{3^1, 3^2, 3^3, 3^4\}$

$3^4 = 1$

$\{1, 2, 3, 4\} = Z_4$

$U(10) \cong Z_4$.

$U(5) \cong Z_4$

$U(10) \cong U(5)$

$U(12) = \{1, 5, 7, 11\}$ → Not Cyclic

$U(12) \ncong U(10)$

$5^2 = 1$

$7^2 = 1$

$11^2 = 1$

$\forall\, x \in U(12)$

$x^2 = 1$

Claim

$\phi : U(10) \longrightarrow U(12)$; Isomorphism

$\phi(9) = \phi(3 \cdot 3) = \phi(3)\phi(3)$

$= (\phi(3))^2$

$= 1$

$\phi(1) = \phi(1 \cdot 1) = (\phi(1))^2 = 1$

$\phi(9) = \phi(1)$

but $9 \neq 1$.

Contradiction as ϕ is not 1-1

Hence $U(12) \ncong U(10)$

(a, b, c, d)

Cayley's Theorem

Every group is isomorphic to a group of permutations.

$\exists$ $f: G \longrightarrow \bar{G}$ (isomorphism)

G → any group

$\bar{G}$ → group of permutations

[$a \in G$ (fixed) and define

$f_a : G \to G : f_a(x) = ax \quad \forall x \in G$

$\Rightarrow f_a$ is a permutation on G.]

$f: G \to \bar{G}$

by

$a \longrightarrow f_a$.

OR

$f(a) = f_a$

$a \in G$

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

$G = \{ag_1, ag_2, ag_3\}$

Eg: Let $G = U(12) = \{1, 5, 7, 11\}$

$$f_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix} \qquad f_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}$$

$$f_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix} \qquad f_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix}$$

$$f: U(12) \longrightarrow P = \{f_1, f_5, f_7, f_{11}\}$$

$1 \longrightarrow f_1$

$5 \longrightarrow f_5$

$7 \longrightarrow f_7$

$11 \longrightarrow f_{11}$

Cosets and Lagrange's Theorem

Let G be a group and H be a subgroup of G.

Define a set $aH = \{ah : h \in H\}$;

Here $a \in G$.

We call aH, a left coset of H in G.

Similarly $Ha = \{ha : h \in H\}$ is a right coset of H in G.

Eg: $G = \mathbb{Z}_9$; $H = \{0, 3, 6\}$

The list all the left cosets of H in G.

$0 + H = H$ ✓

$1 + H = \{1, 4, 7\}$

$2 + H = \{2, 5, 8\}$

$3 + H = \{3, 6, 0\} = H$ ✓

$4 + H = \{4, 7, 1\} = 1 + H$

$5 + H = 2 + H$

$6 + H = H$ ✓

$7 + H = 1 + H$

$8 + H = 2 + H$

In total, H, $1+H$, $2+H$ are three distinct cosets of H in G.

Note that cosets are not subgroups in

general.

Some properties of Cosets.

(i) $aH = H$ iff $a \in H$.

(ii) either $aH = bH$ or $aH \cap bH = \phi$. In particular

(iii) $|aH| = |bH| \quad \forall\ a, b \in G$. $(|aH| = |H|)$

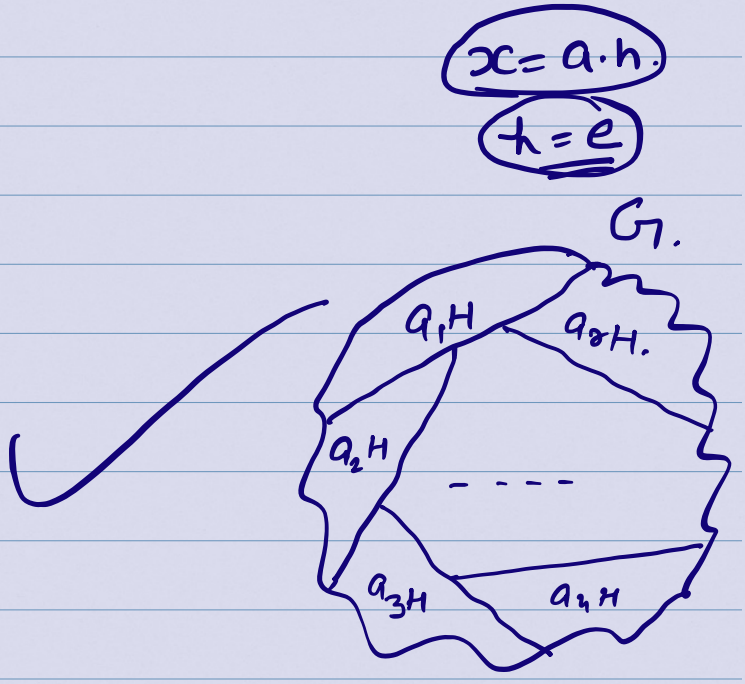
(iv) aH is a subgroup of $G \Leftrightarrow a \in H$. $(aH = H)$

(v) $a \in aH$.

@ $x \in aH$.

$x = a \cdot h$.

$h = e$



Lagrange's Theorem

If G is a finite group and H is a subgroup of G:, then $O(H)$ divides $O(G)$.

Moreover the no of distinct left (right) cosets of H in G is $\frac{O(G)}{O(H)}$

Pf:- Let $a_1H, a_2H, \ldots a_rH$ denote all the distinct left cosets of H in G.

$\left[\because\ a \in G: \quad aH = a_iH \text{ for } i=1,\ldots r.\right]$

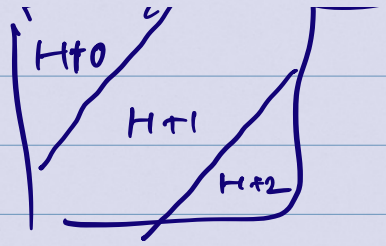
Also $a \in aH$.

$\Rightarrow$ for $x \in G$:

$x \in \bigcup_{i}^{r} a_iH.$

Q.E.D.

$$G \subseteq \bigcup_{i=1}^{r} a_i H.$$



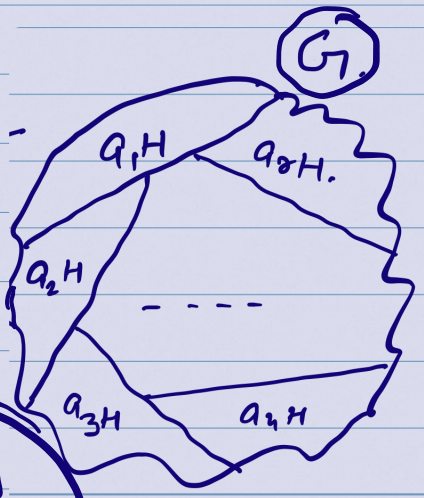
But $\bigcup_{i=1}^{r} a_i H \subseteq G$. $\left[\because a_i H \subseteq G \ \forall i\right]$ $\leq$

$$\Rightarrow \boxed{G = a_1 H \cup a_2 H \cup \dots \cup a_r H.}$$

we have:

(i) $|aH| = |bH| = |H| \quad \forall a, b \in G.$

(ii) $aH \cap bH = \phi$ if $aH \neq bH.$



$$|G| = |a_1 H| + |a_2 H| + \dots |a_r H|$$

$$= r \cdot |H|$$

$\{1, 2, 3\}$

$\{1, 2, 9\}$

$$n(A \cup B) = n(A) + n(B) - n(A \cap B)$$

$\Rightarrow$ $|H| \mid |G|$ and $r = \frac{|G|}{|H|}$

r : No of left cosets.

Corollary

Cor 1.)

$O(G) = |G|$

$O(a) \mid O(G) \quad \forall \; a \in G.$

Think of $H = \langle a \rangle$ Then $O(H) = O(a)$.

$a \in G$.

$a^2 \in G$.

$\{a, a^2, a^3, \ldots\} = \langle a \rangle = H$

$a^n = e$

Cor 2)

Every group of prime order is cyclic.

$O(G) = p$.

any $a \in G$.

but $\forall\, a \in G$, $O(a) \neq 1$ otherwise].

$O(a) = 1$ or p. $\mid p \mid$

$\exists\ a \in G$: $O(a) = p$.

Construct $H = \langle a \rangle$. then $O(H) = p$.

$H \subseteq G$.

$O(H) = p$.

Cyclic

$H = G$.

Cyclic

Cor 3) $a^{|G|} = e$

$|a| \mid |G| \Rightarrow |G| = K \cdot |a|$

$a^{|G|} = a^{K \cdot |a|} = (a^{|a|})^K = e^K = e$.

Normal Subgroup

A subgroup H of G is called a normal subgroup of G iff $aH = Ha$ $\forall\ a \in G$.

[Condition: for $g \in G$; $h \in H$ $\Rightarrow ghg^{-1} \in H$]

(H) $x, y \in H$ $\Rightarrow xy^{-1} \in H$

$H \leq G$

Don't be Confused with:

(1) $ah = ha \quad \forall h \in H; \forall a \in G.$

(2) and $aH = Ha \quad \forall a \in G.$

$x \in aH = (Ha)$: for some $h_2 \in H$.

$x = ah_1 = h_2 a$

$ah_1 = h_2 a$

$H = \{a, b, c\}$

$a_1H = \{a_1a, a_1b, a_1c\}$

$Ha_1 = \{aa_1, ba_1, ca_1\}$

(1,43)

Eg:

$S_3 = \{1, (12), (13), (23), (123), (132)\}$

$A_3 = \{1, (123), (132)\}$

$A_3 \leq S_3$.

(12) → $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

(12) (123) = = (13)(12)

(123) (12) = (13) (23)

$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$ (f) $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ (g) $= \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$

(12) (123)

= (132) (12)

(12) A_3 = A_3 (12)

$(12)\{1,h,h\} = \{1,h,h\}(12)$

$\{(12), (12)h, (12)h\}$

$\therefore \{(12), h(12), h(12)\}$

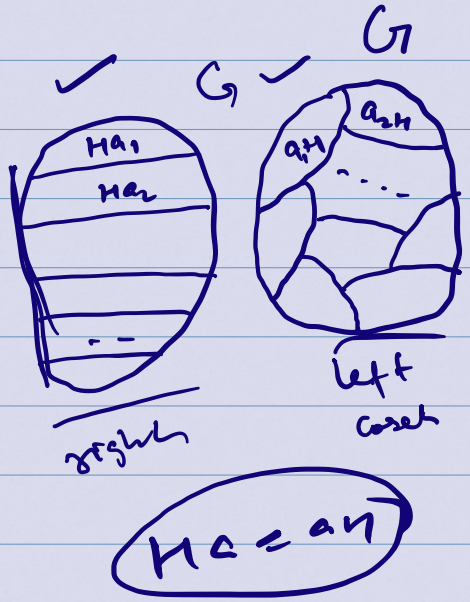
A_3 is a normal subgroup of S_3.

hgg^{-1}

$Ha = aH \ \forall a \in G$, $H \subseteq G$.

$h \in H, g \in G \Rightarrow ghg^{-1} \in H$

\# Every subgroup of an abelian group is normal.



$$\frac{G}{H} =$$

Let G be a group and H be a normal subgroup of G. Then define

$$\frac{G}{H} = \{ aH : a \in G \}$$

is a group under the operation defined as:

$$(aH)(bH) = a(Hb)H$$
$$= a(bH)H \quad (H \text{ is normal})$$

$= (ab)(HH)$

$= (ab)H$ ✓

!! $(aH), (bH) \ \forall \ G/H.$

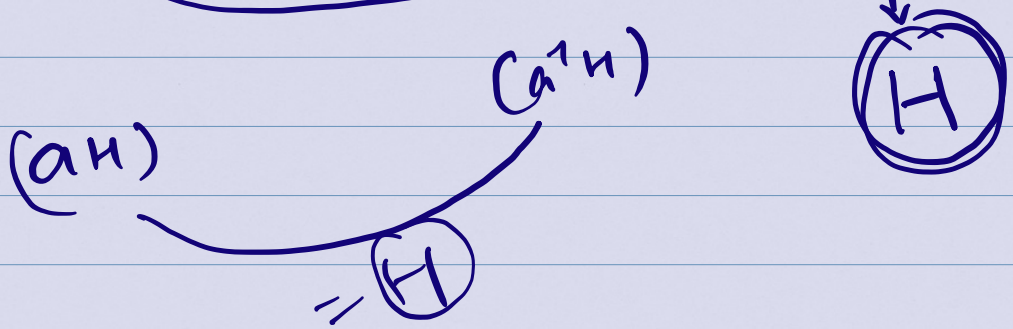
$(aH)(bH) = (ab)H \in \frac{G}{H}$

$a \in G$, $b \in G$ $\Rightarrow ab \in G.$

$H = eH : e \in G.$

$(aH)(eH) = (ae)H = aH$

$\frac{G}{H}$



Called a quotient group.

\# $G = \mathbb{Z}$ (abelian) ; $H = 4\mathbb{Z} = \{0, 4, 8, \dots\}$ (normal)

$$\frac{G}{H} = \{0+H, 1+H, 2+H, 3+H\}$$

$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

where $\bar{a} = a + H$.

$\frac{G}{4} \leftarrow \mathbb{Z}_4$

$$\mathbb{Z}_4 = \frac{\mathbb{Z}'}{4\mathbb{Z}'}$$

aH

$aH = H \Leftrightarrow a \in H$.

$$O\left(\frac{G}{H}\right) = \frac{O(G)}{O(H)} \quad \text{if } G \text{ is finite.}$$

$X \longrightarrow Y$