Thm: Every subgroup of a cyclic group is cyclic.

Cyclic group: $a \in G$ s.t. $G = \langle a \rangle = \{a^0, a, a^2, a^3, a^{-1}, a^{-2}, a^{-3}, \dots\}$ | $a^0 = e$

Pick a subgroup $H \subset G$. Claim is H is also cyclic.

$G = \{g^0\, g^1\, \boxed{g^2}\, g^3\, g^4\, g^{?}\, g^n\}$

e H

$\{\boxed{g^0}\, g^1\, g^2\, \boxed{g^3}\, g^4\, \boxed{g^5}\, g^6\, \boxed{g^7}$

$m = 3$

g^m

Claim: Let m be the minimum power of g s.t. $g^m \in H$.

pick an arbitrary elt. $\boxed{g^n \in H}$ $n > m$.

Division: Given two pos. integers $n > m$.

write $\boxed{n = q \cdot m + r}$ where $\boxed{0 \leq r < m}$

e.g. $\left.\begin{array}{l} n = 7 \\ m = 2 \end{array}\right\}$ $7 = 3 \cdot 2 + 1$

$\uparrow$ q $\uparrow$ r

$$g^n = g^{q \cdot m + r}$$

$$= \underbrace{(g^m)^q}\, g^r \rightarrow g^r = \overbrace{\underbrace{(g^m)^{-q}}_{\in H}\, \underbrace{g^n}_{\in H}}^{\in H}$$

$\because r = 0$

$$\boxed{g^n = (g^m)^q}$$

$g^m \in H$ by choice.

$\rightarrow (g^m)^{-q} \in H$

$g^n \in H$ by choice.

$\rightarrow \boxed{g^r \in H}$

By the div. alg: $0 \leq r < m$

$\therefore r = 0$.

$\therefore n = q \cdot m + 0$

$\boxed{n = q \cdot m}$

∴ arbitrary elt $g^n \in H$ can be written $g^n = (g^m)^q$.

$$\boxed{H \subseteq \langle g^m \rangle}$$

We want to prove: $\boxed{H = \langle g^m \rangle}$

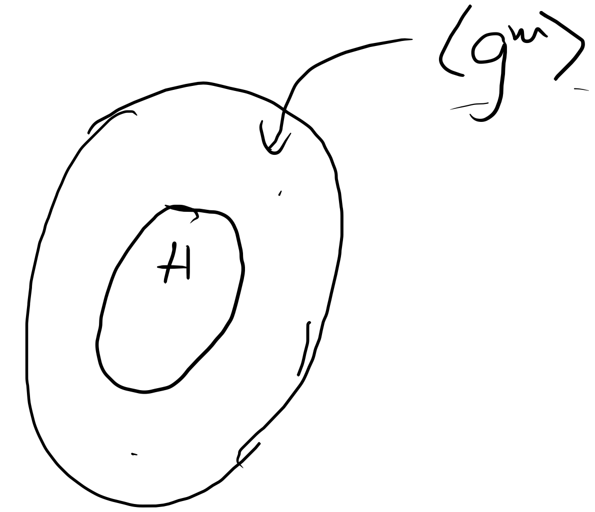
Need to show $\langle g^m \rangle \subseteq H$.

It's true because $g^m \in H$ by choice.

∴ every power of $g^m \in H$ by closure.

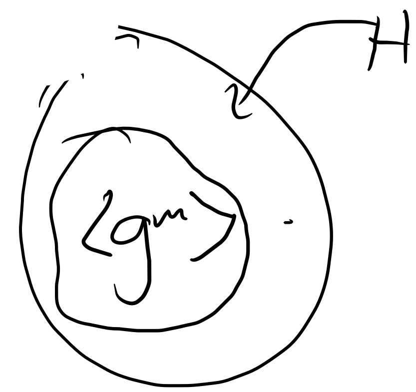
$$\therefore \boxed{\langle g^m \rangle \subseteq H}$$

$$\therefore \boxed{\langle g^m \rangle = H}$$



To show two sets A & B are equal

$A = B \longleftrightarrow$ $A \subseteq B$, $B \subseteq A$.



$g^m = (g)^m$

$\langle a \rangle = \{a^0, a^{\pm1}, a^{\pm2}, \dots\}$

Center of a Group

$$C(G) = \{a \in G : \boxed{ax = xa}\ \forall x \in G\}$$

Claim $C(G)$ is a subgroup of G.

1. Identity: Does $ex = xe \ \forall x \in G$?

$$x = x \ \checkmark$$

2.) Assoc.: If $a, b, c \in C$

Does $(ab)c \overset{?}{=} a(bc)$? $\checkmark$ $\rightarrow$ Yes.

3) Closure: If $a \in C$ & $b \in C$, Is $ab \in C$?

If $ab \in C \rightarrow ab \cdot x = x \cdot ab \ \forall x \in G$.

$= a \cdot xb$ RHS

$= x \cdot ab$ LHS

LHS = RHS $\checkmark$

4.) Inverses:

If $a \in C \rightarrow$ Is a^{-1} in C?

Does $\boxed{a^{-1}x \overset{?}{=} xa^{-1}}$ $\forall x \in G$ if $a \in C$?

$$\boxed{ax = xa \ \forall x \in C}$$

Side Calc^n:

$a^{-1}x = xa^{-1}$

$\cancel{a}a^{-1}x = a \cdot xa^{-1}$

$\boxed{x = axa^{-1}}$

$\cancel{a^{-1}x = a^{-1}axa^{-1}}$

$\cancel{\boxed{a^{-1}x = xa^{-1}}}$

$\boxed{a^{-1}x = xa^{-1}}$

$x = axa^{-1}$

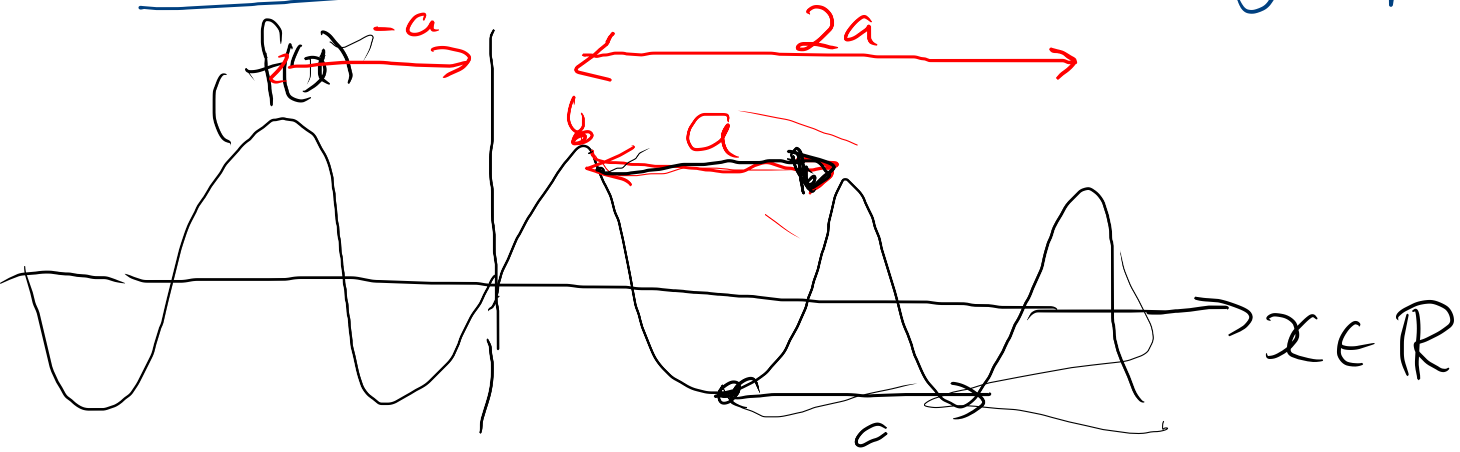
$\boxed{xa = ax}$

$xa = ax$

$x = axa^{-1}$

$a^{-1}x = xa^{-1}$

③ Periods of a function on a group is a subgroup.



$f: \mathbb{R} \to \mathbb{R}$ $\quad \{\mathbb{R}, +\} \to \{\mathbb{R}, +\}$.

Period a satisfies $f(x) = f(x+a)\ \forall x \in \mathbb{R}$

$$\boxed{P = \{0, \pm a, \pm 2a, \pm 3a\} = a\mathbb{Z}}$$

If $a = 1$ $\quad \mathbb{Z}$

<u>Th^m</u>: Let G be a group & $f: G \to G$.

A period is any elt $a \in G$ s.t.

$$\boxed{f(a \circ x) = f(x) \ \forall x \in G.}$$

The set of all periods is a subgroup of G.
$= P$

<u>Pf</u>: 1. <u>Identity</u>: ✓

Is $e \in P$?

Does $f(e \circ x) = f(x)\ \forall x \in G$.

$f(x) = f(x)\ \forall x \in G$ ✓

2. <u>Assoc.</u> ✓

By inheritance.

③ Closure: If $a \in P$, $b \in P$, is $ab \in P$?

Does $f(x) = f(abx)$ if $f(x) = f(ax)$, $f(x) = f(bx)$ $\forall x \in G$?

$$f(a \circ \underbrace{\ }_{G}) = f(\underbrace{\ }) \qquad a \in P$$

- we have $x \in G$.
- $\therefore$ $bx \in G$ by closure.

$$f(a \circ \underbrace{bx}) = f(\underbrace{b}_{P}\underbrace{x}_{G}) = f(x). \quad \forall x \in G.$$

$\therefore$ $\boxed{f(abx) = f(x) \quad \forall x \in G}$ ✓.

④ Inverse: If $a \in P$ is $a^{-1} \in P$?

$$f(\underbrace{a^{-1}}_{G}\underbrace{x}_{G}) = f(a \circ \underbrace{a^{-1}x}_{\text{"}ex\text{"}}) = f(x).$$

$$\boxed{f(\underbrace{z}_{G}) = f(\underbrace{a}_{P} \circ z)}$$

Or: If $\boxed{f(ax) = f(x)}$ ($a \in P$)

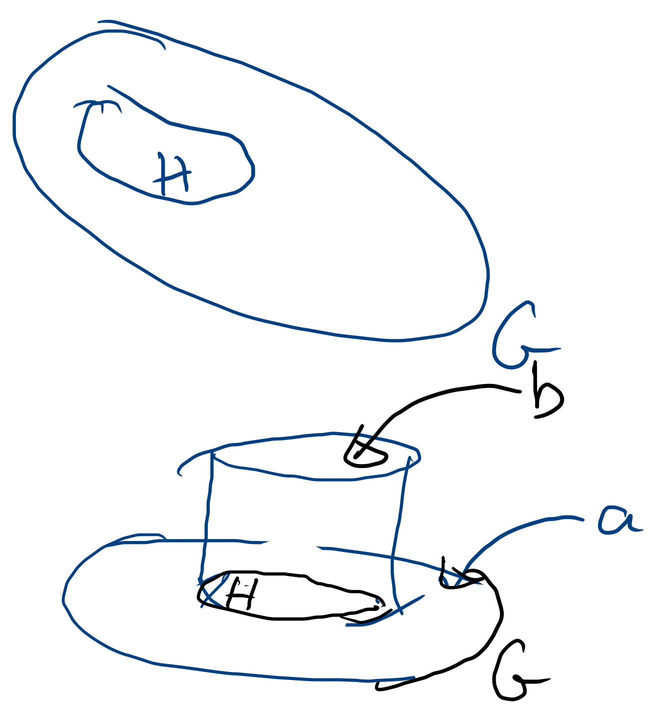
Is $\boxed{f(a^{-1}x) = f(x)}$?

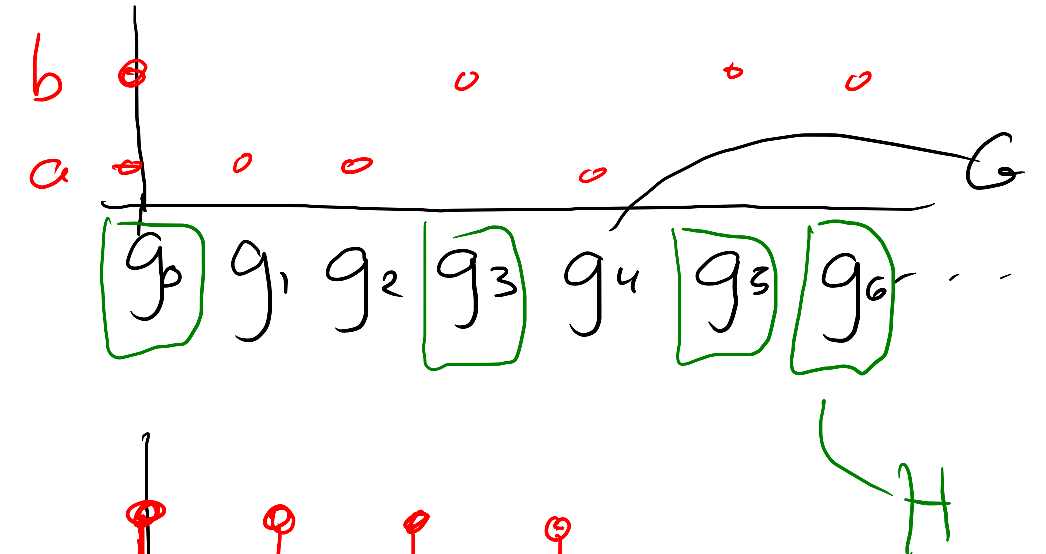
$$\boxed{f(a^{-1}x) = f(x) \quad \forall x \in G} \quad \text{if } \boxed{f(ax) = f(x)}$$

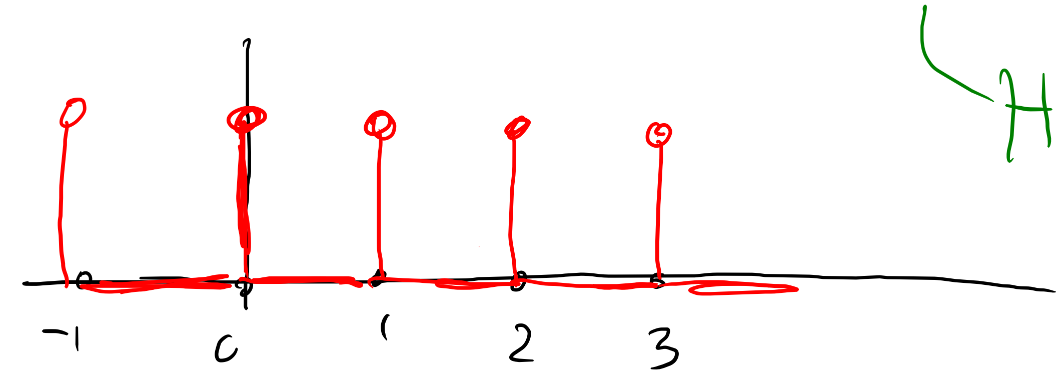
Shown: every periodic set of a function on a Group is a subgroup.

Converse True: Is every subgroup a periodic set of some function?

True.

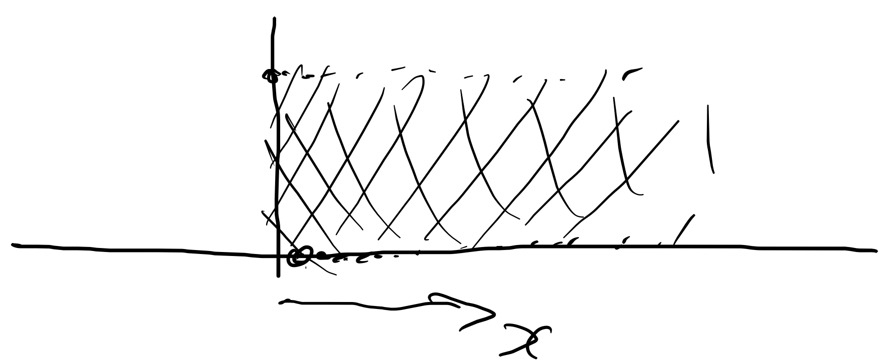






$H = \mathbb{Z}$

$$f(x) = b, \quad x \in H$$
$$f(x) = a, \quad x \notin H$$



$H = \mathbb{Q}$

$H \subset \mathbb{R}$