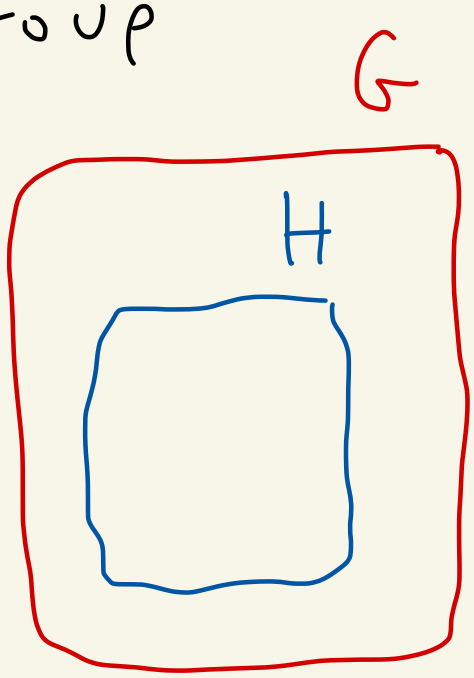
Math 4550
Topic 2 - Subgroups

Def: Let G be a group and H be a subset of G. We say that H is a subgroup of G if H itself is a group under the same operation as G.

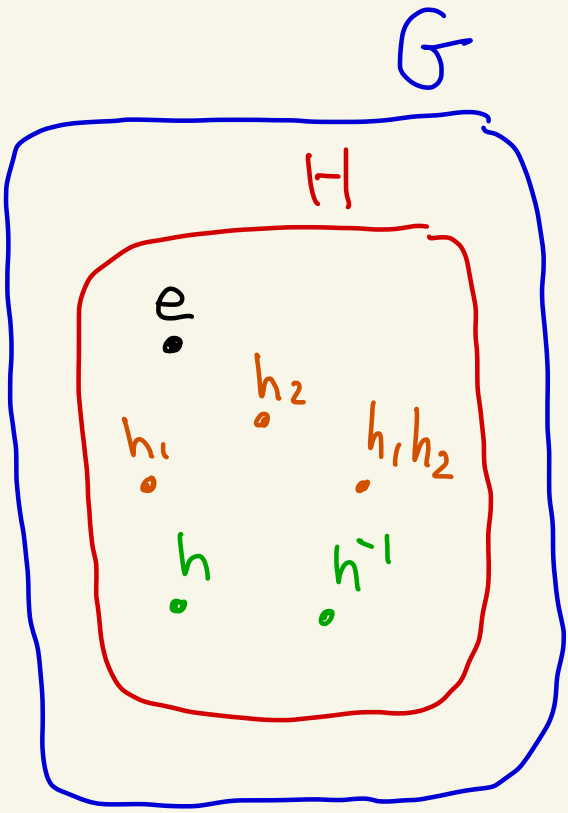


We write $H \leq G$ to mean that H is a subgroup of G.

Ex: $\mathbb{R}$ is a group under addition
$\mathbb{Z} \subseteq \mathbb{R}$ and $\mathbb{Z}$ is a group under addition
So $\mathbb{Z}$ is a subgroup of $\mathbb{R}$.
That is $\mathbb{Z} \leq \mathbb{R}$.

Theorem: Let G be a group with identity element e. Let H be a subset of G. Then, H is a subgroup of G if and only if:

1. $e \in H$
2. If $h_1, h_2 \in H$, then $h_1 h_2 \in H$ } closed under group operation
3. If $h \in H$, then $h^{-1} \in H$ } closed under inversion



Proof:

($\Rightarrow$) Suppose $H \leq G$. Then H is a group using the operation of G.

H must have an identity element e_H. Let's show that $e_H = e$, where e is the identity of G.

We have

$$e e_H = e_H = e_H e_H$$

since $e_H \in G$ and e is the identity of G

since $e_H \in H$ and e_H is the identity of H

Now e_H^{-1} exists in G.

Thus, $e e_H e_H^{-1} = e_H e_H e_H^{-1}$

So, $e = e_H$

Hence, $e \in H$.

So condition ① holds.

Condition ② holds since H is a group under the operation of G.

Now lets show ③
Let $h \in H$.
Since H is a group, there exists
$h' \in H$ where $hh' = e$.
But also in G we get $hh^{-1} = e$.
Thus, $hh' = hh^{-1}$
And, $h^{-1}hh' = h^{-1}hh^{-1}$
Thus, $eh' = eh^{-1}$
So, $h' = h^{-1}$.
Thus, $h^{-1} \in H$.
($\Leftarrow$) Suppose conditions ①, ②, ③ hold. The only condition left to show that H is a group is associativity. But thats true in G and hence is then true in H since H is a subset of G.
So $H \leq G$. ▨

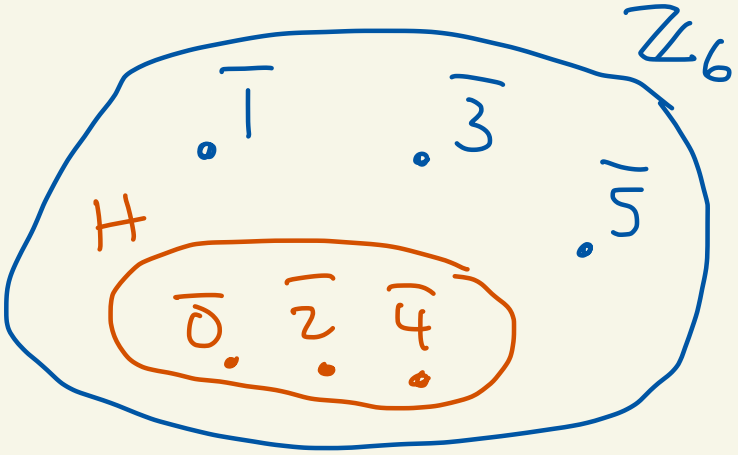
Ex: Consider the group

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Recall $\mathbb{Z}_6$ is a group under addition with identity $e = \bar{0}$.

Let's show that $H = \{\bar{0}, \bar{2}, \bar{4}\}$ is a subgroup of $\mathbb{Z}_6$.

H	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$



proof:

1. $\bar{0} \in H$
2. H is closed under $+$ by the table
3. $\bar{0}^{-1} = \bar{0} \in H$
   $\bar{2}^{-1} = \bar{4} \in H$
   $\bar{4}^{-1} = \bar{2} \in H$

Thus $H \leq G$.

Ex: Recall that

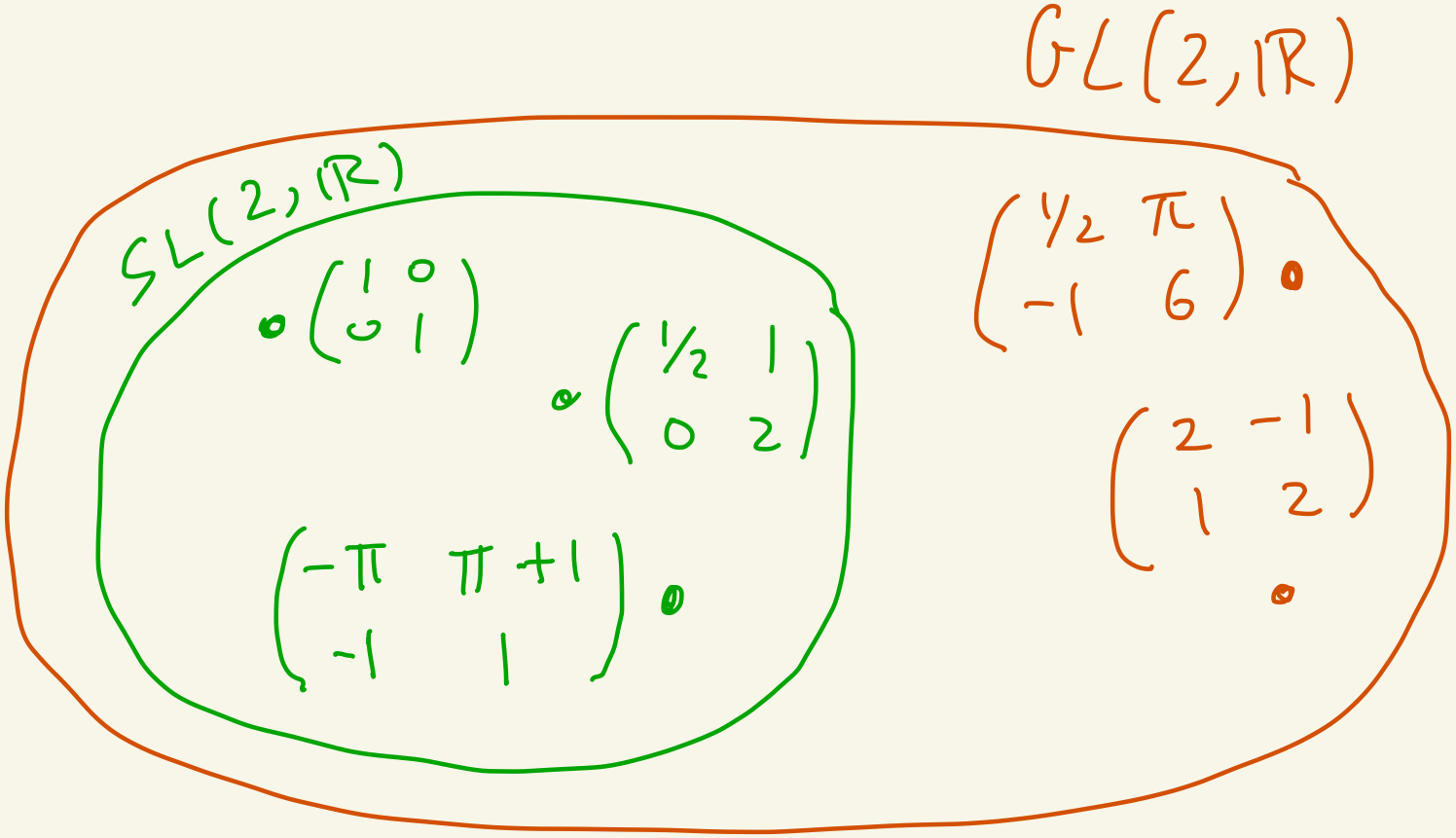
$$GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{c} a,b,c,d \in \mathbb{R} \\ ad-bc \neq 0 \end{array} \right\}$$

is a group under matrix multiplication.

Let

$$SL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{c} a,b,c,d \in \mathbb{R} \\ ad-bc = 1 \end{array} \right\}$$

Note that $SL(2,\mathbb{R})$ is a subset of $GL(2,\mathbb{R})$



Let's show that $SL(2,\mathbb{R}) \leq GL(2,\mathbb{R})$

Proof:

① The identity of $GL(2,\mathbb{R})$ is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Since $\det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$ we have $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL(2,\mathbb{R})$

② Let $A, B \in SL(2,\mathbb{R})$.

Then $\det(A) = 1$ and $\det(B) = 1$.

So, $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$.

Thus, $AB \in SL(2,\mathbb{R})$

③ Let $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be in $SL(2,\mathbb{R})$.

Then $\det(C) = 1$.

So, $ad - bc = 1$.

We know in $GL(2,\mathbb{R})$ that

$$C^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

($ad - bc = 1$)

So, $\det(C^{-1}) = \det\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = da - (-b)(-c)$

$= ad - bc = 1$

Thus $C^{-1} \in SL(2,\mathbb{R})$.

By ①, ②, ③ we have $SL(2,\mathbb{R}) \leq GL(2,\mathbb{R})$

Note: Every group G has these subgroups:

$H = \{e\}$ ← the trivial subgroup

$H = G$ ← the improper subgroup

We will now discuss one way to create subgroups. It won't be the only way. It will be a way to create the "cyclic" subgroups. Essentially given an element $x \in G$ we will create the smallest subgroup that contains x, it will consist of all powers of x.

Lemma: Let G be a group and $x \in G$.
If $n, m \in \mathbb{Z}$, then $x^n x^m = x^{n+m}$

Proof: (Skip in class)

Note: $x^0 x^m = e x^m = x^m = x^{0+m}$ and $x^n x^0 = x^n e = x^n = x^{n+0}$.

Let $a, b > 0$.

Then,

$$x^a x^b = \underbrace{(x x \cdots x)}_{a \text{ times}} \underbrace{(x x \cdots x)}_{b \text{ times}} = x^{a+b}$$

$$x^{-a} x^b = \underbrace{(x^{-1} x^{-1} \cdots x^{-1})}_{a \text{ times}} \underbrace{(x x \cdots x)}_{b \text{ times}} = x^{-a+b}$$

$$x^a x^{-b} = \underbrace{(x x \cdots x)}_{a \text{ times}} \underbrace{(x^{-1} x^{-1} \cdots x^{-1})}_{b \text{ times}} = x^{a+(-b)}$$

$$x^{-a} x^{-b} = \underbrace{(x^{-1} x^{-1} \cdots x^{-1})}_{a \text{ times}} \underbrace{(x^{-1} x^{-1} \cdots x^{-1})}_{b \text{ times}} = x^{(-a)+(-b)}$$

Theorem: Let G be a group and $x \in G$.

Define

$$H = \{ x^k \mid k \in \mathbb{Z} \}$$

$$= \{ \ldots, x^{-3}, x^{-2}, x^{-1}, e, x, x^2, x^3, \ldots \}$$

Then $H \leq G$.

Furthermore we notate H by $\langle x \rangle$ and call $H = \langle x \rangle$ the cyclic subgroup generated by x.

Recall

x^{-2} means $(x^{-1})^2$

x^{-3} means $(x^{-1})^3$

---

proof:

① $e = x^0$ is in H.

② Let $h_1, h_2 \in H$.
Then $h_1 = x^{k_1}$ and $h_2 = x^{k_2}$ where $k_1, k_2 \in \mathbb{Z}$.
We get $h_1 h_2 = x^{k_1} x^{k_2} = x^{k_1 + k_2} \in H$.

③ Let $h \in H$.
Then $h = x^k$ where $k \in \mathbb{Z}$.
Note that $x^{-k} x^k = x^{-k+k} = x^0 = e$
Thus, $(x^k)^{-1} = x^{-k}$.
So, $h^{-1} \in H$.

By ①, ②, ③ we get that $H \leq G$.

///

Ex: Consider the group $\mathbb{R}^* = \mathbb{R} - \{0\}$.

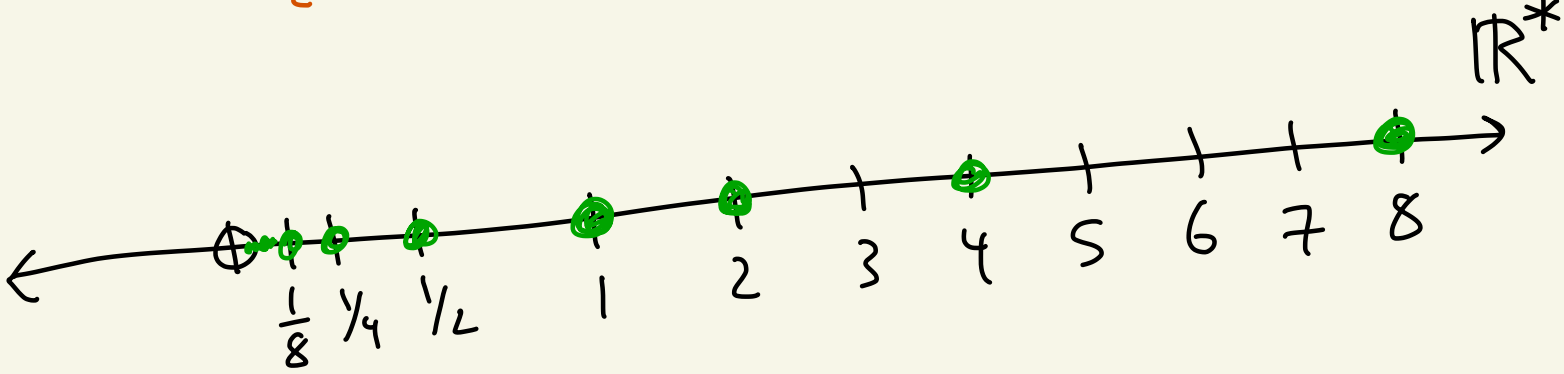
Recall that $\mathbb{R}^*$ is a group under multiplication.

Let's calculate $\langle 2 \rangle$.

We have the subgroup generated by 2 is

$$\langle 2 \rangle = \{ 2^k \mid k \in \mathbb{Z} \}$$

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



Ex: Recall that the integers $\mathbb{Z}$ are a group under addition.

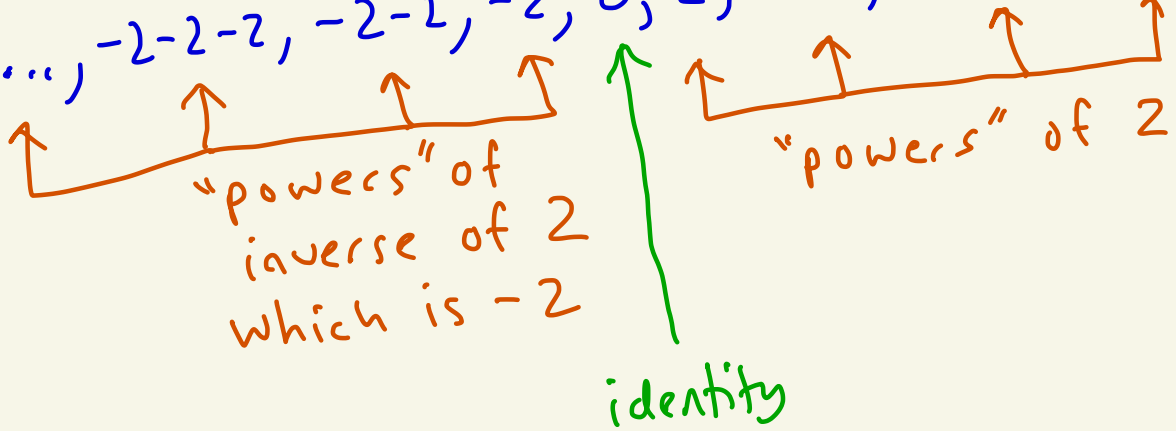
So in this case in the abstract theorem, for example, a^3 means $\underbrace{a+a+a}_{\text{3rd "power" of } a \text{ in } \mathbb{Z}}$.

Let $x = 2$.

Let's calculate $\langle 2 \rangle$ in $\mathbb{Z}$.

We get

$$\langle 2 \rangle = \{\ldots, -2-2-2, -2-2, -2, 0, 2, 2+2, 2+2+2, \ldots\}$$



So, subgroup generated by 2 is

$$\langle 2 \rangle = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$

$$= \{2n \mid n \in \mathbb{Z}\}$$

is the set of multiples of 2.

Ex: In general for $\mathbb{Z}$ one gets

$$\langle n \rangle = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$$

This cyclic subgroup has a special name, it is denoted by $n\mathbb{Z}$.

For example,

$$3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$7\mathbb{Z} = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$$

$$-3\mathbb{Z} = \{\ldots, 6, 3, 0, -3, -6, \ldots\}$$

the same

$$0\mathbb{Z} = \{0\}$$

Def: Let G be a group and $x \in G$.
If there exists a positive integer m where $x^m = e$, then the order of x is defined to be the smallest positive integer k where $x^k = e$.
If no such m exists then x has infinite order.

Ex: Consider $U_6 = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$
Where $\zeta = e^{\frac{2\pi}{6}i} = e^{\frac{\pi}{3}i}$ and $\zeta^6 = 1$.
Let $x = \zeta^2$.
We have:
ζ^2 ← 1st power of $x = \zeta^2$
$(\zeta^2)^2 = \zeta^4$ ← 2nd power of $x = \zeta^2$
$(\zeta^2)^3 = \zeta^6 = 1$ ← 3rd power of $x = \zeta^2$

The smallest positive power of $x = \zeta^2$ that gives the identity 1 is 3.
Thus, ζ^2 has order 3 in U_6.

Ex: In $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

let $x = \bar{2}$.

We have

$\bar{2}$ ← 1st "power" of $\bar{2}$

$\bar{2}+\bar{2} = \bar{4}$ ← 2nd "power" of $\bar{2}$

$\bar{2}+\bar{2}+\bar{2} = \bar{6}$ ← 3rd "power" of $\bar{2}$

$\bar{2}+\bar{2}+\bar{2}+\bar{2} = \bar{8} = \bar{0}$ ← 4th power of $\bar{2}$

The smallest positive power of $\bar{2}$ that gives the identity $\bar{0}$ is 4.

Thus, $\bar{2}$ has order 4 in $\mathbb{Z}_8$.

Ex: Consider the group $\mathbb{R}^* = \mathbb{R} - \{0\}$.

Recall $\mathbb{R}^*$ is a group under multiplication with $e = 1$.

Let $x = 2$.

Then,

$x = 2$

$x^2 = 2^2 = 4$

$x^3 = 2^3 = 8$

$x^4 = 2^4 = 16$

⋮ ⋮ ⋮

} there is no positive power of 2 that gives the identity element 1. Thus, 2 has infinite order in $\mathbb{R}^*$.

Theorem: (Division Algorithm)

Let $m, n \in \mathbb{Z}$ with $m > 0$.

Then there exist unique integers q and r where

$$n = qm + r \quad \text{and} \quad 0 \leq r < m$$

Proof: See my 3450 or 4460 notes. ▨

Ex: $n = 38$, $m = 4$

$$\begin{array}{r|l} & 9 \leftarrow q \\ \hline 4 & 38 \\ & -36 \\ \hline & 2 \leftarrow r \end{array}$$

Thus, $38 = 9 \cdot 4 + 2$

$n = q \cdot m + r$, $0 \leq r < m$

Ex: $n = 36$, $m = 4$

$$\begin{array}{r|l} & 9 \leftarrow q \\ \hline 4 & 36 \\ & -36 \\ \hline & 0 \leftarrow r \end{array}$$

Thus, $36 = 9 \cdot 4 + 0$

$n = q \cdot m + r$, $0 \leq r < m$

$r = 0$ means m divides n

Theorem: Let G be a group and $x \in G$.

(a) If x has finite order n, then

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$$

and $x^{k_1} \neq x^{k_2}$ if $0 \leq k_1 < k_2 \leq n-1$.

So, $n = |\langle x \rangle|$.

(b) If x has infinite order then

$$\langle x \rangle = \{\ldots, x^{-3}, x^{-2}, x^{-1}, e, x, x^2, x^3, \ldots\}$$

and $x^{k_1} \neq x^{k_2}$ if $k_1 \neq k_2$.

---

proof:

(a) Let x have finite order n.

Let $S = \{e, x, x^2, \ldots, x^{n-1}\}$

We will show that $S = \langle x \rangle$.

clearly $S \subseteq \langle x \rangle$

Let's show that $\langle x \rangle \subseteq S$.

Let $x^m \in \langle x \rangle$ where $m \in \mathbb{Z}$.

By the division algorithm $m = qn + r$ where $0 \leq r < n$.

Then $x^m = x^{qn+r} = (x^n)^q x^r = e^q x^r = x^r \in S$

(x has order n)

Thus $S \subseteq \langle x \rangle$.

So, $S = \langle x \rangle$.

Now suppose $x^{k_1} = x^{k_2}$ with $0 \leq k_1 < k_2 \leq n-1$

Then $x^{k_2 - k_1} = e$ with $0 < k_2 - k_1 < n$.

This contradicts the fact that x has order n.

(b) Suppose x has infinite order.

If $x^{k_1} = x^{k_2}$ with say $k_1 > k_2$

then $x^{k_1 - k_2} = e$ with $k_1 - k_2 > 0$

which contradicts x having infinite order.

Ex: Consider $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

Let's find all cyclic subgroups of $\mathbb{Z}_6$.

$\langle \bar{0} \rangle = \{\bar{0}\}$

$\langle \bar{1} \rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{0}\} = \mathbb{Z}_6$

$\bar{1}+\bar{1}$ $\quad$ $\bar{1}+\bar{1}+\bar{1}$ $\cdots$

$\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{0}\}$

$\bar{2}+\bar{2}$ $\quad$ $\bar{2}+\bar{2}+\bar{2}$

$\langle \bar{3} \rangle = \{\bar{3}, \bar{0}\}$

$\langle \bar{4} \rangle = \{\bar{4}, \bar{2}, \bar{0}\}$

$\langle \bar{5} \rangle = \{\bar{5}, \bar{4}, \bar{3}, \bar{2}, \bar{1}, \bar{0}\} = \mathbb{Z}_6$

Answer:

$\{\bar{0}\} \longleftarrow \langle \bar{0} \rangle$

$\{\bar{0}, \bar{3}\} \longleftarrow \langle \bar{3} \rangle$

$\{\bar{0}, \bar{2}, \bar{4}\} \longleftarrow \langle \bar{2} \rangle = \langle \bar{4} \rangle$

$\mathbb{Z}_6 \longleftarrow \langle \bar{1} \rangle = \langle \bar{5} \rangle$

Def: Let G be a group.
We say that G is **cyclic**
if there exists $x \in G$ where $G = \langle x \rangle$.
If this is the case then we call
x a **generator** of G.

Ex: $\mathbb{Z}_6 = \langle \bar{1} \rangle$ is cyclic

In general, $\mathbb{Z}_n = \langle \bar{1} \rangle$ is cyclic

---

Ex: $U_n = \langle \zeta \rangle$ where $\zeta = e^{\frac{2\pi}{n} i}$ is cyclic

---

Ex: $\mathbb{Z}$ is cyclic since

$\mathbb{Z} = \langle 1 \rangle = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Theorem: If G is a cyclic group, then G is abelian.

---

proof:

Suppose G is cyclic.

Then there exists $x \in G$ where $G = \langle x \rangle$.

Let $a, b \in G$.

Then $a = x^k$ and $b = x^l$ where $k, l \in \mathbb{Z}$.

So,

$$ab = x^k x^l = x^{k+l} = x^{l+k} = x^l x^k = ba$$

Thus G is abelian.

$\square$
