Proposition: (one-step subgroup test)

Let G be a group with operation "$\cdot$". Let $H \subseteq G$ be nonempty. Then H is a subgroup of G if and only if $x \cdot y^{-1} \in H$ $\forall\ x, y \in H$.

proof: $\Rightarrow$) Suppose H is a subgroup. Then if $y \in H$, $y^{-1} \in H$ and if $x, z \in H$, $x \cdot z \in H$. Setting $z = y^{-1}$, $x \cdot y^{-1} \in H$.

$\Leftarrow$ Use the subgroup test.

Since $x \cdot y^{-1} \in H$ $\forall$ $x, y \in H$,

setting $y = x$ gives us

that $e = x \cdot x^{-1} \in H$.

Since $e \in H$, $y^{-1} = e \cdot y^{-1} \in H$.

But $y^{-1} \in H \Rightarrow$

$$\underbrace{x \cdot (y^{-1})^{-1}}_{x \cdot y} \in H$$

Then $\forall$ $x, y \in H$, we have

$x \cdot y \in H$ and $y^{-1} \in H$.

Therefore, H is a subgroup by the subgroup test.

$\square$

Proposition: (intersection of subgroups)

Let G be a group with operation "$\cdot$". Let I be an index set (of any cardinality, but not empty).

$\forall\ \alpha \in I$, let H_α be a subgroup of G. Then

$$H = \bigcap_{\alpha \in I} H_\alpha \leq G.$$

proof: Observe H is nonempty since $e \in H_\alpha\ \forall\ \alpha \in I$, so

$$e \in H = \bigcap_{\alpha \in I} H_\alpha.$$

Let's use the one-step subgroup test: take $x, y \in H$.

Since $H_\alpha \leq G \ \forall \alpha \in I$,

we know $x \cdot y^{-1} \in H_\alpha$.

Therefore, $x \cdot y^{-1} \in \bigcap_{\alpha \in I} H_\alpha = H$.

So by the one-step subgroup test, H is a subgroup. $\square$

Note: (unions) Suppose $H, K \leq G$.

Then $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Notation: (subgroup generated by subset)

Let G be a group and let S be a nonempty subset of G. We define the subgroup generated by S to be

$$\boxed{\bigcap_{\substack{S \subseteq H \\ H \leq G}} H}$$

(intersect all subgroups of G that contain S)

Since $S \subseteq G$, this intersection is over a nonempty collection.

Notation for the subgroup generated by S is $\langle S \rangle$.

You can check that $\langle S \rangle$ is the smallest subgroup of G containing S.

Proposition: (subgroup generated by an element)

Let G be a group with operation "$\cdot$". Let $x \in G$.

Then

$$\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$$

where

$$x^n = \underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}$$

if $n \in \mathbb{N}$,

$x^0 = e$ by convention, and

$$x^{-n} = (x^n)^{-1}.$$

proof: We must show that $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup first:

Since $x^0 = e \in \{x^n \mid n \in \mathbb{Z}\}$, our set is nonempty.

To see this is a subgroup, use the 1-step subgroup test. Let $n, m \in \mathbb{Z}$.

Without loss of generality, suppose $n \geq m$.

Cases: 1) $m > 0$. Then

$$x^n \cdot x^m = x^{n+m}$$

2) Either $m=0$ or $n=0$.

Then $x^n \cdot x^m = x^n \quad (m=0)$

or $x^n \cdot x^m = x^m \quad (n=0)$

3) $n < 0$. Then

$$x^n \cdot x^m = (x^{-n})^{-1} \cdot (x^{-m})^{-1}.$$

But also, $(x^{n+m})^{-1} = x^{-(n+m)}$,

so

$$x^{-n-m} = x^{-n} \cdot x^{-m}$$

implies that

$$x^{-n-m} \cdot \left(x^{n} \cdot x^{m}\right)$$

$$= x^{-n-m}\left(x^{m} \cdot x^{n}\right)$$

$$= x^{-n}\, x^{-m}\left(x^{m} \cdot x^{n}\right)$$

$$= x^{-n}\left(\underbrace{x^{-m} x^{m}}_{e}\right) x^{n}$$

$$= x^{-n} \cdot x^{n}$$

$$= e$$

$$\Rightarrow \quad x^n \cdot x^m = \left(x^{-n-m}\right)^{-1} = x^{n+m}$$

4) $n>0$, $m<0$

Then

$$x^n \cdot x^m = x^{n+m-m} \cdot x^m$$

$$= \left(x^{n+m} \cdot x^{-m}\right) \cdot x^m$$

(n>m, m<0, so n+m>0, -m>0)

$$= x^{n+m}\left(\underbrace{x^{-m} \cdot x^{m}}_{e}\right)$$

$$= x^{n+m}$$

Therefore, $\{x^n \mid n \in \mathbb{Z}\} \leq G$.

Since $\langle x \rangle$ is the smallest subgroup of G containing x,

$$\langle x \rangle \subseteq \{x^n \mid n \in \mathbb{Z}\}.$$

But $e \in \langle x \rangle$ and

$$x^n \in \langle x \rangle \quad \forall\, n \in \mathbb{N}$$

since $\langle x \rangle$ is a subgroup.

Then $x^{-n} = (x^n)^{-1} \in \langle x \rangle$

$$\forall\, n \in \mathbb{N} \Rightarrow \{x^n \mid n \in \mathbb{Z}\} \subseteq \langle x \rangle.$$

We have containment both ways, so

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}. \quad \square$$

Definition: (cyclic group, generators)

A group G is said to be **cyclic** if $\exists\ x \in G$ with $G = \langle x \rangle$. If $y \in G$ and $\langle y \rangle = G$, we say that y is a **generator** of G.

Example 4: $(\mathbb{Z}, \mathbb{Z}_n)$

Consider $(\mathbb{Z}, +)$.

Then $\mathbb{Z} = \langle 1 \rangle$ since if

$n \in \mathbb{N}$, $n = \underbrace{1+1+1+\dots+1}_{n \text{ times}}$.

Furthermore, if $n \in \mathbb{N}$,

$\mathbb{Z}_n = \langle [1] \rangle$, by

the same argument.

Up to isomorphism, these are the only cyclic groups!

Definition: (order of an element, notation)

Let G be a group, $x \in G$.

We define the **order** of x to be $|\langle x \rangle|$.

Notation: $o(x)$ for the order of x.

Proposition: (characterization of order)

If G is a group and $x \in G$, then $o(x)$ is the smallest $n \in \mathbb{N}$ such that $x^n = e$.

proof: If $n \in \mathbb{N}$ is the smallest natural number with $x^n = e$, then $x^{n+1} = x^n \cdot x = e \cdot x = x$. Similarly, for any positive power of x,

$$x^m = x^{[m]_n}.$$

Observe also that $(n \geq 2)$

$$e = x^n = x^{n-1} \cdot x$$

$$\Rightarrow \quad x^{n-1} = x^{-1}$$ by uniqueness of the inverse.

Therefore,

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

$$\Rightarrow \quad o(x) = n.$$

Other direction next time!