Subgroup criteria

Recall: A subgroup is an especially strong set of symmetries.

Thm ① A subset of a group is a subgroup iff

① it contains the identity element;

② it's closed under the binary operation;

③ it contains the inverse of each of its elements.

(Proof.) Exercise. ◼

Thm ② A subset H of a group G is a subgroup iff

① H is nonempty;

② $\forall\, g, h \in H,\ gh^{-1} \in H.$

(Proof.) First, suppose $H \leq G$ is a subgroup.

$e \in H \Rightarrow H \neq \emptyset.$

$\forall g, h \in H$, $h^{-1} \in H$, since H is a group.

$\therefore\ gh^{-1} \in H$, b/c H is closed under $\circ$.

Conversely, suppose $H \subseteq G$ is nonempty subset s.t., $\forall\, g, h \in H$, $gh^{-1} \in H$.

by the assumed property

$H \neq \emptyset \Rightarrow \exists\, g \in H \Rightarrow gg^{-1} \in H \Rightarrow e \in H$ ① ✓

$\forall\, h \in H$, $e \cdot h^{-1} \in H$, by the property. ③ ✓

So $h^{-1} \in H$.

$\forall g, h \in H$, $h^{-1} \in H$, so $g(h^{-1})^{-1} \in H$

$\therefore gh \in H$. (2) ✓

So H is a subgroup. ∎

<u>Corollary</u>. The intersection of two subgroups of a group is again a subgroup.

(Proof.) Exercise. ∎

<u>Cyclic subgroups</u>

<u>Definitions & properties</u>

Given any element $g \in G$ in a group, we denote by $\langle g \rangle$ the smallest subgroup of G which contains g. This is called the subgroup generated by g.

<u>Ex</u> (1). Let's compute $\langle n \rangle \leq (\mathbb{Z}, +)$.

$n \in \langle n \rangle$. $\quad n + n = 2n \to 2n \in \langle n \rangle$

$kn + n = (k+1)n \to (k+1)n \in \langle n \rangle$

Closure under inverses $\Rightarrow -n \in \langle n \rangle$

$\rightsquigarrow -kn \in \langle n \rangle$, $\forall k \geq 1$.

Identity: $0 \in \langle n \rangle$.

So $\underbrace{n\mathbb{Z} := \{\dots, -2n, -n, 0, n, 2n, \dots\} \subseteq \langle n \rangle}_{\text{i.e., any subgroup containing } n \text{ must contain } n\mathbb{Z}.}$

Check: $n\mathbb{Z} \neq \emptyset$ ✓

given $kn, mn \in n\mathbb{Z}$,

this is gh^{-1} written additively

$$\underbrace{(kn) - (mn)} = (k-m)n \in n\mathbb{Z} \checkmark$$

By Thm ②, $n\mathbb{Z} \leq \mathbb{Z}$ is a subgroup.

So $n\mathbb{Z} = \langle n \rangle$.

Ex ② Consider $(\mathbb{R}^*, \times)$, where $\mathbb{R}^* = \mathbb{R} - \{0\}$.

Let's compute $\langle a \rangle$.

$1 \in \langle a \rangle$ by identity

$a^{-1} \in \langle a \rangle$ by inverses

$a \cdot a = a^2 \in \langle a \rangle$, and in fact $a^k \in \langle a \rangle$, $\forall k \in \mathbb{Z}$.

So $\{a^k \mid k \in \mathbb{Z}\} \subseteq \langle a \rangle$.

Check: LHS is a subgroup of $(\mathbb{R}^*, \times)$.

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

Thm ③ Let G be a group, $g \in G$. Then

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

(Proof.) Exercise. ☒

We call $\langle g \rangle$ the cyclic subgroup generated by G. If $\exists\, g \in G$ s.t. $G = \langle g \rangle$, then we call G a cyclic group and call g a generator for G.

Ex $(\mathbb{Z},+)$ is cyclic b/c $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

$(\mathbb{R}^*, \times)$ is not cyclic (it's too big)

The order of an element $g \in G$ is $|g| := |\langle g \rangle|$.

i.e., $|g| = n$ if $g^n = e$

& $|g| = \infty$ if no such n exists.

Thm 4 Every cyclic group is abelian.

(Proof.) Exercise. ☒

Subgroups of cyclic groups

Thm 5 Every subgroup of a cyclic group is cyclic.

(Proof.) Let $G = \langle g \rangle$ be a cyclic group, $H \leq G$ a subgroup. If $H = \{e\}$, then $H = \langle e \rangle$ and we're done.

So $\exists\, h \in H$ s.t. $h \neq e$. Then $\langle h \rangle \subseteq H$.

Moreover, $h = g^n$ for some $n \neq 0$. Since $h^{-1} \in H$, we may assume WLOG that $n \geq 1$.

Let $m \leq n$ be the smallest positive integer s.t. $g^m \in H$.

We claim $H = \langle g^m \rangle$.

To see this, choose $a \in H$. We will show that

$a = (g^m)^q$, for some $q \in \mathbb{Z}$, so that $a \in \langle g^m \rangle$.

B/c $a \in G$, $a = g^k$, for some $k \in \mathbb{Z}$.

By division algorithm,

$$k = mq + r, \quad 0 \le r < m.$$

So $g^k = g^{mq+r} = (g^m)^q g^r$. $\left(\rightarrow g^r = (g^m)^{-q} g^k\right)$

Now $g^m \in H \Rightarrow (g^m)^{-q} \in H$. Also, $a = g^k \in H$.

So $g^r = (g^m)^{-q} g^k \in H$. Since m is smallest pos. integer w/ this property, $r = 0$. So in fact $k = mq$.

So $a = g^{mq} = (g^m)^q \in \langle g^m \rangle$.

$\therefore H \subseteq \langle g^m \rangle$. $\therefore H = \langle g^m \rangle$. ◩

<u>Rmk</u> ① Converse of this theorem is false: S_3.

② We can use this theorem to identify all subgroups of $\mathbb{Z}$.