Def'n. A subgroup of a group $(G, \circ_G)$ is a group $(H, \circ_H)$ such that H is a subset of G and $\circ_H$ is the restriction of $\circ_G$:

$$a \circ_H b = a \circ_G b,$$

$\forall\ a, b \in H$.

Ex. ① $\mathbb{Z}_{10}$ contains subgroups of order 2 & 5:

$$H_1 := \{0, 5\},\quad H_2 := \{0, 2, 4, 6, 8\}$$

Any others? $0 = \{0\}$

② S_n = permutation group on n objects

$X_n = \{1, 2, 3, \ldots, n\}$ ⟵ this is NOT the group

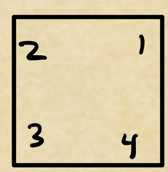
$$S_n = \{f : X_n \to X_n \mid f \text{ is a bijection}\}$$

group operation is composition

D_n = dihedral group on n vertices

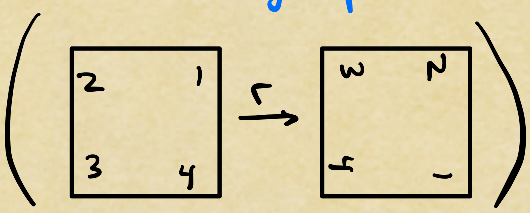
P_n = (regular) polygon with n vertices

D_n = "rigid symmetries of P_n"



$D_n \leq S_n$. Realize this by labeling vertices of P_n with integers.

↑ subgroup



$\longmapsto \left(X_4 \longrightarrow X_4 \quad \begin{matrix} 1 \longmapsto 4 & 3 \longmapsto 2 \\ 2 \longmapsto 1 & 4 \longmapsto 3 \end{matrix} \right)$

In fact $D_n \lneq S_n$ for $n \geq 4$.

3. Recall $M_n(\mathbb{R})$ forms a group under $+$.
   $GL_n(\mathbb{R}) \subseteq M_n(\mathbb{R})$ also has a group structure.
   Is it a subgroup? NO!
   The operation on $GL_n(\mathbb{R})$ is matrix mult.

Subgroup criteria

Thm A subset of a group is a subgroup if and only if the subset

1. Contains the identity element of the group;
2. is closed under the binary operation of the group; $\forall g, h \in H,\ gh \in H$
3. contains the inverse of each elements. $\forall h \in H,\ h^{-1} \in H$

Thm A subset H of a group G is a subgroup if and only if

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

(Proof)

$\S$ H is a subgroup of G.

$e \in H$ by 1 above $\Rightarrow H \neq \emptyset$

$\forall g, h \in H,\ h^{-1} \in H$ by 3 above and $gh^{-1} \in H$ by 2 above.

$\S$ H satisfies the two criteria.

We'll show that H satisfies 1, 2, & 3 from previous theorem.

① H contains the identity

$H \neq \emptyset \Rightarrow \exists\, h \in H$

By criterion ②, $hh^{-1} \in H$

$\therefore\ e \in H.$ ✓

therefore

③ H is closed under inverses.

Pick $h \in H$. Since $e, h \in H$, criterion ② gives $eh^{-1} \in H$. i.e., $h^{-1} \in H$. ✓

② H is closed under the binary operation

Pick $g, h \in H$. Then $h^{-1} \in H$ from above.

By criterion ②,

$$g(h^{-1})^{-1} \in H \Rightarrow gh \in H. \ ✓$$

By previous theorem, H is a subgroup. ∎

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

(Proof.) Let H_1, H_2 be subgroups of G.

Then $e \in H_1$ & $e \in H_2$, so $e \in H_1 \cap H_2$.

$\therefore\ H_1 \cap H_2 \neq \emptyset.$

Pick $g, h \in H_1 \cap H_2$. Then $g, h \in H_1$.

Since H_1 is a subgroup, $gh^{-1} \in H_1$.

Similarly, $gh^{-1} \in H_2$. So $gh^{-1} \in H_1 \cap H_2$.

By subgroup criteria, $H_1 \cap H_2$ is a subgroup. ∎

Defn. The subgroup $\{e\}$ of G is called the trivial subgroup. Other subgroups of G are called nontrivial. A subgroup of G which is not equal to G is called a proper subgroup.

Cyclic subgroups

Given any element $g \in G$, we denote by $\langle g \rangle$ the smallest subgroup of G which contains g.

Thm Let G be a group. For any $g \in G$,

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

Def. We call $\langle g \rangle$ the cyclic subgroup generated by g. If $G = \langle g \rangle$, we say that G is a cyclic group.