DEFINITION: Let G be a group. A nonempty subset H of G is a **subgroup** of G if H is a group under the the same operation as G (i.e., $h \cdot_H h' = h \cdot_G h'$ for $h, h' \in H$). We write $H \leq G$ to indicate that H is a subgroup of G.

Any group G has two **trivial subgroups** $\{e\}$ and G.

LEMMA 1: Let H be a subset of G.

- TWO STEP TEST: If H is nonempty, H is closed under multiplication[1] and H is closed under inverses[1], then H is a subgroup of G.
- ONE STEP TEST: If H is nonempty, and for all $x, y \in H$, $xy^{-1} \in H$, then H is a subgroup of G.

LEMMA 2 (GENERAL RECIPES FOR SUBGROUPS): Let G be a group.

(1) If $H \leq G$ and $K \leq H$, then $K \leq G$.
(2) If $\{H_\alpha\}_{\alpha \in J}$ is a collection of subgroups of G, then $\bigcap_{\alpha \in J} H_\alpha \leq G$.
(3) If $f : G \to H$ is a group homomorphism, then $\mathrm{im}(G) \leq H$.
(4) If $f : G \to H$ is a group homomorphism, and $K \leq G$, then $f(K) = \{f(k) \mid k \in K\} \leq H$.
(5) If $f : G \to H$ is a group homomorphism, and $K \leq G$, then $\ker(f) \leq G$.
(6) The center $Z(G)$ is a subgroup of G.

(1) Proving subsets are subgroups:

(a) Choose a couple of parts of Lemma 2 and prove them; you can use Lemma 1.

(i) By definition, K is a group under the multiplication in H, and the multiplication in H is the same as that in G, so K is a subgroup of G.

(ii) First, note that H is nonempty since $e_G \in H_\alpha$ for all $\alpha \in J$. Moreover, given $x, y \in H$, for each α we have $x, y \in H_\alpha$ and hence $xy^{-1} \in H_\alpha$. It follows that $xy^{-1} \in H$. By the Two-Step test, H is a subgroup of G.

(iii) Since G is nonempty, then $\mathrm{image}(f)$ must also be nonemtpy; for example, it contains $f(e_G) = e_H$. If $x, y \in \mathrm{image}(f)$, then $x = f(a)$ and $y = f(b)$ for some $a, b \in G$, and hence

$$xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \mathrm{image}(f).$$

By the Two-Step Test, $\mathrm{image}(f)$ is a subgroup of H.

(iv) The restriction $g\colon K \to H$ of f to K is still a group homomorphism, and thus $f(K) = \mathrm{image} g$ is a subgroup of H.

(v) Using the One-step test, note that if $x, y \in \ker(f)$, meaning $f(x) = f(y) = e_G$, then

$$f(xy^{-1}) = f(x)f(y)^{-1} = e_G.$$

This shows that if $x, y \in \ker(f)$ then $xy^{-1} \in \ker(f)$, so $\ker(f)$ is closed for taking inverses. By the Two-Step test, $\ker(f)$ is a subgroup of G.

(vi) The center $Z(G)$ is the kernel of the permutation representation $G \to \mathrm{Perm}(G)$ for the conjugation action, so $Z(G)$ is a subgroup of G since the kernel of a homomorphism is a subgroup.

(b) Let $n \geq 3$ and consider the dihedral group D_n of symmetries of the n-gon.

(i) Is the set of all reflections in D_n a subgroup?

[1] A subset $H \subseteq G$ is *closed under multiplication* if $x, y \in H \Rightarrow xy \in H$ and *closed under inverses* if $x \in H \Rightarrow x^{-1} \in H$.

No; the composition of two reflections is not a reflection. Also, the identity is not a reflection.

(ii) Is the set of all rotations in D_n a subgroup?

Yes; the composition of two rotations is a rotation, as is the inverse of any rotation.

(c) Let $n \in \mathbb{Z}_{\geq 1}$, and define $\mathrm{SL}_n(\mathbb{R})$ to be the set of $n \times n$ real matrices with determinant 1. Show[2] that $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$. ($\mathrm{SL}_n(\mathbb{R})$ is called the **special linear group**.)

Recall that $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism, and the identity of $\mathbb{R}^\times$ is 1. Thus, this follows from part (5) of Lemma 2.

(d) Let $n \in \mathbb{Z}_{\geq 1}$. Recall from linear algebra that an $n \times n$ matrix Q is *orthogonal* if $Q^T Q = I$, where ^{T} denotes transpose and I denotes the identity matrix. Define $\mathrm{O}_n(\mathbb{R})$ to be the set of $n \times n$ real orthogonal matrices. Show that $\mathrm{O}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$. ($\mathrm{O}_n(\mathbb{R})$ is called the **orthogonal group**.)

We use the two-step test. Let $A, B \in O_n$, so $A^T A = I$ and $B^T B = I$. Since A is square, note that $AA^T = I$ as well. Then $(AB)^T(AB) = B^T A^T AB = B^T B = I$, so $AB \in O_n$. Also, $(A^{-1})^T = (A^T)^{-1}$, so $(A^{-1})^T A^{-1} = (A^T)^{-1} A^{-1} = (AA^T)^{-1} = I^{-1} = I$, so $A^{-1} \in O_n$. Thus, O_n is a group.

(e) Define $\mathrm{SO}_n(\mathbb{R})$ to be the set of $n \times n$ real orthogonal matrices that have determinant 1. Show that $\mathrm{SO}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$. ($\mathrm{SO}_n(\mathbb{R})$ is called the **special orthogonal group**.)

By definition, $SO_n = SL_n \cap O_n$, so by part 2 of Lemma 2, this is a subgroup.

(2) Prove or disprove: The union of two subgroups of a group is a subgroup.

(3) Prove Lemma 1.

[2] Hint: This becomes very quick with a proper use of Lemma 2.

DEFINITION: Let G be a group, and $S \subseteq G$ be a subset. The **subgroup of G generated by S** is the intersection of all subgroups of G that contain S:

$$\langle S \rangle := \bigcap_{\substack{H \leq G \\ S \subseteq H}} H$$

PROPOSITION: Let G be a group, and $S \subseteq G$ be a subset. Then

$$\langle S \rangle = \{x_1^{j_1} \cdots x_m^{j_m} \mid x_i \in S,\ j_i \in \mathbb{Z}\}.$$

(4) Explain why $\bigcap_{\substack{H \leq G \\ S \subseteq H}} H$ is a subgroup of G, and why it is the *unique smallest* subgroup of G that contains S.

It follows from the Lemma that this is a subgroup. Call this group K. If H is a subgroup of G containing S, then K is the intersection of H with some other set, by definition of K, so $K \subseteq H$. This means that K is the unique smallest subgroup containing S.

(5) PROOF OF THE PROPOSITION: Let $K = \{x_1^{j_1} \cdots x_m^{j_m} \mid x_i \in S,\ j_i \in \mathbb{Z}\}$ as in the Proposition.

(a) What concrete things do you need to show about K, S, and subgroups $H \leq G$ to prove this equality?

(b) Complete the proof.

CAYLEY'S THEOREM: Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.

(6) Prove[3] Cayley's Theorem.

Let G act on G by left multiplication. This action induces a permutation representation $\rho : G \to \mathrm{Perm}(G)$. We claim that ρ is injective. Indeed, if $\rho(g)$ is the identity permutation, then $gh = g \cdot h = h$ for all $h \in H$, whence $g = e$. If G has n elements, we can label them 1 through n, and identify $\mathrm{Perm}(G)$ with S_n; so we have an injective homomorphism ρ from G to S_n. Let H be the image of ρ; we have an injective homomorphismρ' from G to H, and by definition of image, this is also surjective. Thus ρ' is an isomorphism so $G \cong H$. This is the isomorphism we seek.

[3] Hint: Let G act on G by left multiplication.