Definition 1. A ***group*** G consists of a set of elements (also called G) and a binary operation (usually written $\cdot$) that satisfy the following properties:

(associativity) For all elements $a, b, c \in G$, we have that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(identity) There is an element $e \in G$ (called the identity) that satisfies $e \cdot g = g \cdot e = g$ for all elements $g \in G$.

(inverses) For every element $g \in G$ there is another element $h \in G$ (known as its inverse) that satisfies $g \cdot h = h \cdot g = e$.

Example 2. The following are all groups:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (the integers, rationals, reals, and complex numbers, respectively) are all groups under addition.
- $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ (the same groups with 0 removed) are all groups under multiplication.
- $\mathbb{Z}_n$, also known as $\mathbb{Z}/n\mathbb{Z}$ (the integers modulo n) is a group under addition.
- C_n (the group of rotational symmetries of a regular n-gon) is a group under composition.
- D_n (the group of rotational and reflectional symmetries of a regular n-gon) is a group under composition.
- S_n (the permutations on the numbers 1 through n) is a group under composition of permutations.
- $GL_n(\mathbb{R})$ (the group of $n \times n$ matrices with non-zero determinant) is a group under matrix multiplication.
- $SL_n(\mathbb{R})$ (the group of $n \times n$ matrices with determinant ± 1) is a group under matrix multiplication.

(Some of these groups of more common than others. We'll be taking about $\mathbb{Z}$, $\mathbb{Z}_n$, C_n, D_n, and S_n the most in this class.)

Definition 3. A group is ***commutative*** or ***abelian*** if it satisfies the additional property:

(commutativity) For all elements $a, b \in G$, we have that $a \cdot b = b \cdot a$.

Definition 4. A ***subgroup*** of a group G is another group H whose elements are a subset of the elements of G and that has the same binary operation. This is sometimes denoted as $H < G$.

Remark 5. To find a subgroup of a given group, all we have to do is take a subset of the elements of our group that contains 1) the identity, 2) all inverses 3) the result of all multiplications.

Question 6. Which of the groups in Example 2 are abelian? Which of them are subgroups of other ones?

Proposition 7. *It's not possible for a group to have more than one identity element.*

Proposition 8. *No group element can have more than one inverse.*

Proposition 9 (Cancellation Lemma)**.** *For any group G and $a, b, c \in G$, if $a \cdot c = b \cdot c$, then $a = b$.*

Question 10 (Looking forward). What should it mean for two groups to be "the same"? Can you think of a way to make this mathematically rigorous?

If it helps, think about this: A group is a set with a binary operation on it. What does it mean for two sets to be "the same"? How can you say *this* in a way that's rigorous? What more do you need for two groups to be "the same" other than that their underlying sets are "the same"?