UW Math Circle

Last week we talked about what a group was. Remember that we defined a group as a set of objects with an action taking two objects to another object such that there was an identity object, inverse objects and a special property called associativity.

Given a group, a subgroup of the group is some collection of the objects of the group so that all of the properties of a group are satisfied. One of the most important things to check for a subgroup is that the group action, when applied to two objects in the subgroup, gives another object in the subgroup. For example, let's consider the group of the real numbers $\mathbb{R}$ with addition. Are the integers with addition a subgroup? We can see if it is or not by checking four things:

- Are the integers a subset of the real numbers?
- Is there an identity object in the integers when the action is addition?
- Is the sum of two integers an integer?
- Are there inverses for each integer?

Since all of these check out, the integers with addition are a subgroup of the real numbers with addition!

Let's try to find more examples (or possible non-examples)!

1. Are the integers modulo 2 with addition a subgroup of the integers modulo 6 with addition?
2. Are the integers modulo 7 with addition a subgroup of the integers modulo 10 with addition?
3. Are the rational numbers with addition a subgroup of the real numbers with addition?
4. Are the integers modulo 5 with addition a subgroup of the integers modulo 10 with addition?
5. Are the integers with addition a subgroup of the nonzero real numbers with multiplication?
6. Are the permutations of two objects a subgroup of the permutations of four objects?
7. Are the nonnegative integers with addition a subgroup of the integers with addition?
8. Is 0 with addition a subgroup of the real numbers with addition?

A few weeks ago we introduced the idea of the order of an element. The order of an object of a group is the smallest number of times we apply the action of the group with the object to reach the identity object. If no combination of an element will ever reach the identity object, we say this element has infinite order. This seems confusing but consider the group of mattress flips of a square mattress:

The order of flipping the mattress across the diagonal from the upper left corner to the bottom right is 2. We flip the mattress once, interchanging the two opposite corners, and then have to flip it again to bring the mattress back to its original position.

For another example, consider the group of the integers modulo 4 with addition. The order of 1 is 4 because $1 + 1 + 1 + 1 = 0 \mod 4$. Similarly, the order of 2 is 2 because $2 + 2 = 0 \mod 4$. What is the order of 0? Try to find the order of all of the elements in the groups below. Can you find patterns in which elements have which order?

We say that a group is generated by an element if some combination of the element with itself gives every other object of the group. For example, the group of mattress flips for the mattress below

is generated by a turn of 90 degrees to the right. We say that a group has a generating set of size n if n objects in the group can be used to create any other object in the group. For example, the group of mattress flips for a square mattress

has a generating set of size 2, every mattress flip can be made out of rotating to the right by 90 degrees and flipping the mattress horizontally.

What are some generating sets for the groups below? Can you find the smallest possible generating set for each group?