GROUPS

Groups are ubiquitous and are a primary object of study in (abstract) algebra. Roughly speaking, they encode symmetries. As this is not an algebra course, we'll look at groups primarily as a domain in which we can practice using the structures we have seen already.

A **group** is a set G that is equipped with a binary operation $\cdot : G \times G \to G$ ("multiplication") and a special element $1 \in G$ ("identity element") that satisfies the following properties:

(i) (Associativity) For all $g, h, k \in G$, we have $(g \cdot h) \cdot k = g \cdot (h \cdot k)$.
(ii) (Identity) For all $g \in G$, we have $g \cdot 1 = g$.
(iii) (Existence of Inverses) For any $g \in G$, there exists an element $g^{-1} \in G$ such that $g \cdot g^{-1} = 1$.

Example 1. The positive real numbers $\mathbb{R}_+$ with $\cdot$ being the usual multiplication is a group, with identity element 1. The group $\mathbb{Z}$ with $\cdot = +$ with identity element 0 is a group. The set $\mathbb{Z}$ under multiplication is not a group. Invertible $n \times n$ matrices form a group.

Unlike for numbers, group "multiplication" is not necessarily commutative, like the case of 2×2 matrices. If a group's multiplication is commutative ("$a \cdot b = b \cdot a$"), we say it's an **abelian** group.

Example 2. A **permutation** of a set A is a bijection $A \to A$. Permutations of A form a group, where multiplication is defined by composition: $f \cdot g = f \circ g$. We write S_n for the group of permutations of $[n]$. The group S_n is non-abelian if $n > 2$.

Example 3. Consider a square lying in a plane. The rigid motions that we can perform on a square—so that we obtain a square after the transformation—form a group. We can do nothing, rotate the square, flip across an axis passing through the midpoint of opposing edges, flip across diagonals, ... What is the group multiplication? How many elements are in this group? What is a good way to describe its elements? (It might help to begin by labeling the vertices of the square.)

A partition coming from equivalence relations can sometimes be turned into a group.

Example 4. Consider the relation on $\mathbb{Z}$ where $x \sim y$ if $n \mid x - y$. The corresponding partition of $\mathbb{Z}$ forms a group under multiplication, often denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. What's special if n is prime?

The axioms of a group are simple, and what's nice is that they can be proven for all groups.

Proposition 5. *Any $g \in G$ has only one inverse element. There exists a unique element in G that satisfies the Identity property.*

A **group homomorphism** is a function $f : G \to H$ between two groups such that $f(g \cdot g') = f(g) \cdot f(g')$. (Note that $g \cdot g'$ takes place in G, but $f(g) \cdot f(g')$ takes place in H.)

Proposition 6. *A group homomorphism must map an identity element to an identity element.*

Question 7. *Must a group homomorphism be injective? Surjective? How can you check whether a function can be upgraded to a group homomorphism?*

Question 8. *Suppose that we have an injective group homomorphism $A \to B$. Must there exist a surjective group homomorphism $B \to A$? What about vice versa? If a group homomorphism is also a bijection, must its inverse function also be a group homomorphism?*

Question 9. *How many functions are there from $\mathbb{Z}$ to $\mathbb{Z}$? How many group homomorphisms are there? What about for some other examples of groups we've seen above?*