A Swift Introduction to Group Theory

Cade McManus, Michael Moorman

December 2022

1 What is Group Theory?

In order to connect the ideas of group theory to the real world, we must first understand what a group is in relation to linear algebra. A group is a set of elements that are closed under a binary operation, similarly to how vector spaces are closed under addition and scalar multiplication, but with the generalization that groups need not be composed of only vectors, but any set of elements.

Definition 1: A **group** is a set S with a binary[1] operation $\cdot$ such that the following axioms hold:

1. Closure: For all $a, b \in S$, $a \cdot b \in S$.
2. Associativity: For all $a, b, c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Identity: There exists a unique element $e \in S$ such that for all $a \in S$, $a \cdot e = e \cdot a = a$.
4. Inverse: For all $a \in S$, there exists a unique element $a^{-1} \in S$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Formally, the set S is known as the **underlying set** of the group, and the binary operation $\cdot$ is known as the **group operation**. Frequently, a group G is denoted by $G = \langle S, \cdot \rangle$. Additionally, abuses of notation are common, such that G referring to a group can be used to refer to the group itself or the underlying set, such that a statement like '$a \in G$' is meant to convey that a is an element in the underlying set of the group G.

Example: This may seem confusing, but let's make it more concrete with an example: the real numbers together with the operation of addition as we know it. This group would be written $G = \langle \mathbb{R}, + \rangle$. Let's verify our axioms to truly grasp what they mean through this example:

1. Closure: Let $x, y \in \mathbb{R}$. Because the sum of any two real numbers is defined as a real number, it must be the case that $x + y \in \mathbb{R}$.
2. Associativity: Let $x, y, z \in \mathbb{R}$. Because addition of real numbers does not depend on the way in which terms are associated, it is the case that $(x+y)+z = x+y+z$ and that $x+(y+z) = x+y+z$. Thus, $(x + y) + z = x + (y + z)$.
3. Identity: Let $e = 0$. $0 \in \mathbb{R}$, and the addition of 0 to any $x \in \mathbb{R}$ is equal to x itself. Thus, for all $x \in \mathbb{R}$, $e + x = x + e = x$.
4. Inverse: For all $x \in \mathbb{R}$, allow x^{-1}, the inverse of x, to be equal to $-x$, the negation of x. Thus, $-x + x = 0$ via simple addition, and $e = 0$. Therefore, for any choice of $x \in \mathbb{R}$, there exists an inverse element x^{-1} in $\mathbb{R}$ such that $x + x^{-1} = e$, the identity element.

That's all! We have proven that the real numbers, along with the operation of addition as we know it, form a group! Now that we're a bit more comfortable with what a group is, what does it have to do with linear algebra? Or even anything else at all?

[1] **Binary** refers to the number of elements that the operation requires to be defined, specifically 2. Consider the binary operation of multiplication. The expression $5*$ does not make sense without a second input, making multiplication of real numbers a binary operation.

2 Vector Spaces and their Connections to Groups

In class, we defined a vector space as a non-empty set V on which two operations, scalar multiplication and vector addition, are defined subject to ten different axioms, of which the principles of closure, associativity, identity, and inverse are included for vector addition. For scalar multiplication, these properties are not all explicitly included, simply because scalar multiplication is a binary operation, but only involves a single vector, rather than two, as its other input is a scalar, so the ideas of associativity in this case and other similar properties don't have proper analogs.

This definition ought to sound familiar. Just like groups, vector spaces are defined as the combination of a set and operations! Groups, however, are only defined by one operation which you are free to choose. So, in a sense, s

3 Group Homomorphisms

4 Subgroups