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.

Additionally, another special type of group we will see is an **abelian group**.

Definition 2: An **abelian group** is a group $\langle V, \cdot \rangle$ such that for all $u, v \in V$, $u \cdot v = v \cdot u$. This means that our group operation is commutative, and the order in which we add elements does not matter.

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 the following axioms, where $u, v, w \in V$ and $c, d \in \mathbb{R}$:

1. $u + v \in V$
2. $u + v = v + u$
3. $(u + v) + w = u + (v + w)$
4. there exists a vector $0_v \in V$ such that $u + 0_v = u$
5. there exists a vector $-u \in V$ such that $u + (-u) = 0_v$
6. $cu \in V$
7. $c(u + v) = cu + cv$
8. $(c + d)u = cu + du$
9. $c(du) = (cd)u$
10. $1 \cdot u = u$

This is absolutely a correct definition, but we can introduce some additional notation as well as generalize $\mathbb{R}$. We will say that a vector space is a tuple $\langle V, K, +, \cdot \rangle$, where V is a non-empty set, K is a field[2], $+$ is our vector addition operator, and $\cdot$ is our scalar multiplication operator, and all of the previous axioms hold.

As we have seen, a group is a set of elements closed under a binary operation, which seems like a less restrictive version of a vector space, especially after having established this notation. It turns out that this is indeed the case, and that given our vector field $\langle V, K, +, \cdot \rangle$, we can always define an abelian group as simply $\langle V, + \rangle$.

Theorem 1: Let $\langle V, K, +, \cdot \rangle$ be a vector space. Then, $\langle V, + \rangle$ is an abelian group.

Proof. In order to prove this theorem, we will verify all of the axioms of a group given that V is a non-empty set of a vector space, and $+$ is the vector addition operator from that same vector space. ■

3 Group Homomorphisms

4 Subgroups

[2] A **field** refers to a set on which addition, multiplication, subtraction, etc. are defined as we know them to work for the real numbers. This is not incredibly important here, but it is relevant to note that the field K is not necessarily the real numbers.