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.

1. Closure: Let $u, v \in V$. Because axiom 1 of a vector space states that $u + v \in V$ and we are using the same set V from our vector space and the same binary operator, this property holds for our group as well.

2. Associativity: Let $u, v, w \in V$. Because axiom 3 of a vector space states that $(u + v) + w = u + (v + w)$ and we are using the same set V from our vector space and the same binary operator, this property holds for our group as well.

3. Identity: Let u be an arbitrary element of V. Because axiom 4 of a vector space states that there exists a vector $0_v \in V$ such that $u + 0_v = u$ and we are using the same set V from our vector space and the same binary operator, this property holds for our group as well using the same identity element 0_v that we use for our vector space.

4. Inverse: Let u be an arbitrary element of V. Because axiom 5 of a vector space states that there exists a vector $-u \in V$ such that $u + (-u) = 0_v$ and we are using the same set V from our vector space and the same binary operator, this property holds for our group as well.

Additionally, this is also an abelian group, which requires that our group operation is commutative. We know that this is the case because axiom 2 of a vector space states that $u + v = v + u$ for all $u, v \in V$, where V is our underlying set and $+$ is our group operator. Because we have shown that each of our axioms for a group holds given a non-empty set V from a vector space and the vector addition operator $+$ from that same vector space, and that our group operation is commutative, we have proven that $\langle V, + \rangle$ is an abelian group formed from any arbitrary vector space $\langle V, K, +, \cdot \rangle$. ∎

---

[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.

3   Group Homomorphisms

4   Subgroups

5   Group actions

We have seen how vector spaces can satisfy the group axioms, so a natural area of inquiry might be to dig further into the connection between these objects. For example, instead of investigating questions about groups directly, might we instead be able to study some equivalent vector space / linear algebraic object and then leverage the tools that we have been studying this semester to answer our original question. As it turns out this is indeed possible. For the purposes of this paper (and simplicity) feel free to assume the relevant objects are finite linear groups.

To find the explicit connection we will first introduce the notion of Group Actions in the context of vector spaces. Suppose a real vector space V, and a set of n x n invertible matrices in that space. Notice that this set of transformations satisfies the group axioms under matrix multiplication. We have an identity element in I_n, by the definition of invertibility each element has an inverse, and we have shown in class that invertible matrices can be composed associatively to produce another invertible matrix. This is also known as the general linear group of V (GL(V)). A group action maps elements of a group to these transformations.

We will get to the formal definition, but first some notes for intuition. Notice how the underlying vector space is essentially unchanged after these transformations? While the coordinates of where points were mapped may be different from the original, the underlying space "looks" identical as did in the start. So these transformations acted on the space, but didn't change how it "looked". In other words, these transformations are symmetry preserving operations.

This idea is important, so I'll a give a more concrete example. Suppose a square, if you were to rotate that square by 90 degrees it would look exactly the same. Its vertices may be in different locations, but they were mapped to each other in a such a way that the structure we care about preserving (square-ness) is kept intact. Also notice that there are many different symmetries that one could exploit to perform a symmetric action. Because of the nature of a "symmetric operation", whenever one considers the set of symmetric operations on an object, there is an identity element, an inverse, and composition (the underlying structure always looks the same so composing symmetric operations will also produce the same structure, so the net result must also conform to some other symmetric operation).

Cayleys theorem tells us that every group is isomorphic to a subgroup of a symmetric group., though not a very interesting one
Proof:

The upshot is this: Groups have a deep connection to symmetry, and Group Actions map groups to symmetry groups (the set of automorphisms) of mathematical objects. When we can perform group actions on a vector space V we can often map group elements to subgroups of GL(V), allowing us to use linear algebra.