# 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 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.

So, there is an interesting connection between groups and vector spaces, but the similarities and connections do not stop there. We turn to examine **group homomorphisms**, and their similarities to linear transformations.

# 3 Group Homomorphisms and Isomorphisms

**Definition 3:** A **group homomorphism** is a function $f : G \to H$ from a group $\langle G, \cdot \rangle$ to a group $\langle H, * \rangle$ such that $f$ preserves the group structure of $G$ and $H$. That is, $f$ must satisfy the following property:

1. $f(g \cdot h) = f(g) * f(h)$

where $g, h \in G$. From this property, it can be deduced that $f(e_G) = e_H$, where $e_G$ is the identity element of $G$ and $e_H$ is the identity element of $H$, and that $f(g^{-1}) = (f(g))^{-1}$. We leave these proofs as an exercise to the reader.

This property may look familiar, and it should. This is exactly how we define a linear transformation with respect to vector addition. In fact, we can generalize this as follows.

**Theorem 2:** Let $\langle V, K, +, \cdot \rangle$ be a vector space, and let $\langle W, L, \oplus, \odot \rangle$ be a vector space. Then, a linear transformation $T : V \to W$ is a group homomorphism from $\langle V, + \rangle$ to $\langle W, \oplus \rangle$.

*Proof.* One of the two axioms[3] of a linear transformation is that $T(u+v) = T(u) \oplus T(v)$ for all $u, v \in V$, when $T$ maps $V$ to $W$. Well, because our binary operator for our group $\langle V, + \rangle$ is $+$, and our binary operator for our group $\langle W, \oplus \rangle$ is $\oplus$, our sole property for a group homomorphism is satisfied simply by this one axiom of our linear transformation, that $T(u + v) = T(u) \oplus T(v)$ for all $u, v \in V$. ■

Thus, group homomorphisms are generalizations of linear transformations between vector spaces, just like how groups are generalizations of vector spaces. We're not done just yet, though. We now introduce the concept of a **group isomorphism**.

**Definition 4:** A **group isomorphism** is a special type of group homomorphism that is bijective. That is, a group isomorphism is a function $f : G \to H$ from a group $\langle G, \cdot \rangle$ to a group $\langle H, * \rangle$ such that there exists a function $g : H \to G$ such that $f(g(h)) = h$ and $g(f(g)) = g$ for all $h \in H$. $g$ is known as the **inverse homomorphism** of $f$. So, a group isomorphism is a group homomorphism that has an inverse homomorphism.

We can generalize this to linear transformations quite nicely as well.

**Theorem 3:** Let $\langle V, K, +, \cdot \rangle$ and $\langle W, L, \oplus, \odot \rangle$ be vector spaces. Then, a linear transformation $T : V \to W$ between vector spaces is also a group isomorphism from $\langle V, + \rangle$ to $\langle W, \oplus \rangle$ if and only if $T$ is bijective.

*Proof.* We will prove this by showing that if $T$ is bijective, then $T$ is a group isomorphism, and that if $T$ is a group isomorphism, then $T$ is bijective.

1. If $T$ is bijective, then $T$ is a group isomorphism. Let $f : V \to W$ be the function $f(v) = T(v)$ for all $v \in V$. Then, $f$ is a group homomorphism from $\langle V, + \rangle$ to $\langle W, \oplus \rangle$ by Theorem 2. Let $g : W \to V$ be the function $g(w) = T^{-1}(w)$ for all $w \in W$. We know this inverse exists because $T$ is bijective. Then, $g$ is the inverse homomorphism of $f$ because $f(g(w)) = T(T^{-1}(w)) = w$ and $g(f(g)) = T^{-1}(T(g)) = g$ for all $w \in W$. Thus, $T$ is a group isomorphism.

2. If $T$ is a group isomorphism, then $T$ is bijective. Let $f : V \to W$ be the function $f(v) = T(v)$ for all $v \in V$. Then, $f$ is a group homomorphism from $\langle V, + \rangle$ to $\langle W, \oplus \rangle$ by Theorem 2. Let $g : W \to V$ be the function $g(w) = T^{-1}(w)$ for all $w \in W$. We know that this inverse homomorphism exists because $T$ is a group isomorphism. Then, $g$ is the inverse homomorphism of $f$ because $f(g(w)) = T(T^{-1}(w)) = w$ and $g(f(g)) = T^{-1}(T(g)) = g$ for all $w \in W$. Thus, $g$ is a group

[3] In class, we present this axiom as $T(u + v) = T(u) + T(v)$, but it can really be written as $T(u + v) = T(u) \oplus T(v)$, as our binary operator for vector addition may be different in our $W$ vector space.

homomorphism from $\langle W, \oplus \rangle$ to $\langle V, + \rangle$. Because $f(g(w)) = w$ for all $w \in W$ and therefore $T(T^{-1}(w)) = w$ for all $w \in W$, we know that $T$ must be bijective[4] because it has a defined inverse for all $w \in W$.

■

[4]It suffices to say that $T$ is bijective because it has a defined inverse. The proof for this statement is elementary, and is left as an exercise for the reader in order to keep this proof short both short and on topic.