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 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.