Introduction to Groups

Matthew Hanna

March 5, 2019

Hi all! Welcome to the 3rd installment of Matt's Math Mondays! Today, we will introduce the concept of a group and include basic proofs about them.

Let G be a collection of elements. We say that G is a group under an operation $\star$ (think of an operation of something that takes 2 elements and spits out a 3rd, addition and multiplication are examples of operations) if the following truths hold.

1. $\forall$(for all) $a, b \in$(is an element of) G, $\exists$ (there exists) $c \in G$ such that $c = a \star b$. We call this property closure. We may say that G is closed up $\star$.
2. $\forall x, y, z \in G$, it follows that $x \star (y \star z) = (x \star y) \star z$. We call this property, associativity.
3. $\exists e \in G$, which we call the identity element which satisfies the property $\forall x \in G$, $e \star x = x \star e = x$.
4. $\forall a \in G$, $\exists a^{-1} \in G$ which we call the inverse element which has the property that $a \star a^{-1} = a \star a^{-1} = e$.

Here's a basic example to help cement this idea.
Consider the set of integers under the operation of addition, which I denote as $\{\mathbb{Z}, +\}$. I claim that this is a group. To verify this, I must check the group axioms individualy.

1. $\{\mathbb{Z}, +\}$ is closed because for any two integers, their sum is also an integer.
2. $\{\mathbb{Z}, +\}$ is associative because $\forall a, b, c \in \mathbb{Z}$, we have $a + (b + c) = (a + b) + c$.
3. $\{\mathbb{Z}, +\}$ has an identity, which we call 0 because $a + 0 = 0 + a = a$, $\forall a \in \mathbb{Z}$.
4. $\{\mathbb{Z}, +\}$ has an inverse element for any element a, which we call $-a$ becauce $a + (-a) = -a + a = 0$

The following 3 proofs are meant to teach the reader on how proofs involving groups should look like.

Proposition 1: If G is a group under operation $\star$, then,
1.1: The identity of G is unique
1.2: $\forall a \in G$, a^{-1} is uniquely defined.
1.3: $(a^{-1})^{-1} = a, \forall a \in G$

Proof. **1.1**
Let $e_1, e_2 \in G$ be identity elements of G.

Then, $e_1 \star a = e_2 \star a$ by definition of an identity element.
Then, we may right multiply both sides by a^{-1}, which we know exists by definition of a group so that we may have

$$(1.1.1)\ e_1 \star a \star a^{-1} = e_2 \star a \star a^{-1}$$
$$(1.1.2)\ e_1 \star (a \star a^{-1}) = e_2 \star (a \star a^{-1}), \text{ by associativity.}$$
$$(1.1.3)\ e_1 = e_2, \text{ by inverse axiom.}$$

Therefore, the identity element of an group G is unique. In other words,

$$(1.1.4)\ \forall e_1, e_2, \ldots, e_n \in G \text{ and } \forall a \in G \text{ if}$$
$$e_1 \star a = a \star e_1 = e_2 \star a = a \star e_2 = \cdots = e_n \star a = a \star e_n = a, \text{ then } e_1 = e_2 = \cdots = e_n$$

■

Proof. **1.2**
Let $b, c \in G$ both be inverses of a. Then,

$$(1.2.1)\ b \star a = c \star a = e, \text{ where } e \text{ is the identity element.}$$
$$(1.2.2)\ b \star a \star a^{-1} = c \star a \star a^{-1} = e \star a^{-1}, \text{ right multiplying by } a^{-1}$$
$$(1.2.3)\ b \star (a \star a^{-1}) = c \star (a \star a^{-1}) = a^{-1}, \text{ by associativity.}$$
$$(1.2.4)\ b = c = a^{-1}$$

We have shown that the any element $a \in G$ has a unique inverse. In other words . . .

$$(1.2.5) \forall a \in G \text{ and } \forall a_1, a_2, \ldots, a_n \in G \text{ if}$$
$$a_1 \star a = a \star a_1 = a_2 \star a = a \star a_2 = \cdots = a_n \star a = a \star e_a = e, \text{ where } e \text{ is the identity element of } G \text{ then } a_1 = a_2 = \cdots = a_n$$

■

Proof. **1.3**
Suppose $(a^{-1})^{-1} \in G$, then

$$(1.3.1)\ (a^{-1})^{-1} \star a^{-1} = e$$
$$(1.3.2)\ (a^{-1})^{-1} \star a^{-1} \star a = e \star a, \text{ right multiplying by } a$$
$$(1.3.3)\ (a^{-1})^{-1} \star (a^{-1} \star a) = a, \text{ by associativity.}$$
$$(1.3.4)\ (a^{-1})^{-1} = a, \text{ as was desired.}$$

■