The Fundamental Homomorphism Theorem

Matthew Gregoire

May 2020

Contents

1 Introduction

While taking an undergraduate abstract algebra class, the most confusing topic for me was the fundamental homomorphism theorem for groups, otherwise known as the first isomorphism theorem. This result is quite elegant, but looking back I'm shocked at how poorly it was explained in my textbook. This is meant to be a document to build straight up to this theorem from basic definitions.

2 Groups

First, here are the basic preliminaries we need to start talking about groups.

Definition 2.1. Let G be a set. A **binary operation** on G is a function $* : G \times G \to G$.

If in G, we have $*(a, b) = c$, we often write $a * b = c$. In fact, we can often drop the operation symbol and write this as $ab = c$, if no confusion will result. For now, we'll continue explicitly writing the operation for clarity.

Definition 2.2. A **group** is a set G with a binary operation $* : G \times G \to G$ that satisfies the following properties:

- There exists an element $e \in G$ such that, for all $a \in G$, $a * e = e * a = a$. Here e is referred to as the **identity element** for $*$.
- For all $a \in G$, there exists an $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. We call a^{-1} the **inverse** of a.
- For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$. In this case, we say $*$ is an **associative** operation.

In order to tackle the fundamental homomorphism theorem, we need to first build up a litte machinery in order to understand groups. The next few theorems build only from the definition of a group.

Theorem 2.1. Let G be a group with a binary operation $*$. Then for all $a, b, c \in G$, $a * b = a * c$ implies that $b = c$, and $b * a = c * a$ also implies $b = c$. These are called the **left and right cancellation laws**.

Proof. Suppose that $a * b = a * c$. We know there exists $a^{-1} \in G$, so therefore:

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

By the associative property:

$$(a^{-1} * a) * b = (a^{-1} * a) * c$$

By definition of a^{-1}:

$$e * b = e * c$$

And finally, by definition of e, we have $b = c$. Similarly, if $b * a = c * a$, then $(b * a) * a^{-1} = (c * a) * a^{-1}$. Therefore $b * (a * a^{-1}) = c * (a * a^{-1})$, and $b * e = c * e$, or $b = c$.

□

Theorem 2.2. Let G be a group. There is a unique element $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. Similarly, for $a \in G$, there is a unique element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Proof. Suppose that e and e' are both elements of G with the given property. Then we have $e = e * e'$, using e' as the identity. But we also have $e * e' = e'$, using e as the identity. Therefore $e = e'$.

Now let $a \in G$. If $a * a^{-1} = a^{-1} * a = e$, and also $a * \tilde{a}^{-1} = \tilde{a}^{-1} * a = e$, then we have:

$$a * a^{-1} = e = a * \tilde{a}^{-1}$$

And by cancellation, $a^{-1} = \tilde{a}^{-1}$.

□

3 Subgroups and Cosets

From here on out, we'll use multiplicative notation exclusively when discusing group operations. Also, constantly specifying the name of a group's operation can get tedious, so by abuse of notation, we can feel free to refer to a group G by itself, and assume that it has an associated operation that satisfies the group axioms. Since it's still convenient to give this operation a name, we might as well call it multiplication in most cases. For our purposes, this shouldn't cause any confusion.

Subgroups are still a somewhat intuitive topic. The formal definition is below.

Definition 3.1. Let G be a group, and let $H \subseteq G$. If under the binary operation of G, H forms a group, we call H a **subgroup** of G.

An important and related concept is closure under a specified binary operation.

Definition 3.2. Let $*$ be a binary operation of a set G, and let $H \subseteq G$. If for all $a, b \in H$, $a * b$ is also in H, then H is **closed under**, or **has closure under**, the operation $*$.

In order for H to be a subgroup of G, H needs to satisfy the group axioms. This makes the next theorem feel somewhat tautological, but it provides a methodical way to check if a given subset H is indeed a subgroup of G.

Theorem 3.1. Let G be a group, and let $H \subseteq G$. Then H is a subgroup of G if and only if:

- $e \in H$
- For all $a \in H$, $a^{-1} \in H$. (**Closure under inverses**)
- For all $a, b \in H$, $ab \in H$. (**Closure under multiplication**)

Proof. Suppose H is a subgroup of G. Then the group axioms hold within H, so clearly the first two properties hold. The third property follows from how we define a binary operation on H as a map from $H \times H$ to H.

Conversely, suppose that the above properties hold for a subset H of G. Since we are guaranteed an identity element, and an inverse for every element, we only need to check the associative property. Let $a, b, c \in H$. Then applying the group axioms in G, we have $a(bc) = (ab)c$. But this can also be viewed as an equation in H, so multiplication is associative within H. □