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.

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

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

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

□