# 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.

This document is designed for a reader who has the sole objective of understanding the reasoning behind this theorem, and therefore its scope is narrow. However, we would be missing many fundamental (and beautiful) facts about the basics of group theory if we focus only on the necessary and sufficient definitions and theorems. Therefore we'll motivate these concepts with several examples, and also present some results that aren't strictly re- * quired. The examples are clearly labeled if you don't care to read them, and unnecessary results are marked with a star in the left margin, as shown in this sentence.

# 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.

**Example 2.3.** The integers $\mathbb{Z}$ under the usual addition $(+)$ form a group. The element 0 acts as the identity, and for any $a \in \mathbb{Z}$, $-a$ acts as its additive inverse. Addition is associative, so this is indeed a group.

**Example 2.4.** The integers $\mathbb{Z}_n$ of remainders modulo $n$ also form a group under addition. We'll be pedantically formal here for the sake of demonstrating the group axioms. The elements of $\mathbb{Z}_n$ are defined as the integers $x$ such that $0 \leq x < n$, and addition within $\mathbb{Z}_n$, for now given the symbol $\tilde{+}$, is defined as follows: if $a + b = nq + r$ in $\mathbb{Z}$ by the division algorithm, then $a \mathbin{\tilde{+}} b = r$. Since $0 \leq r < n$, this is also an element of $\mathbb{Z}_n$, so this is a well-defined binary operation.

0 is again the identity, because $a + 0 = 0 + a = n \cdot 0 + a$, so $a \mathbin{\tilde{+}} 0 = 0 \mathbin{\tilde{+}} a = a$. Also, the equation $a + (n - a) = (n - a) + a = n \cdot 1 + 0$ shows that $n - a$ is the inverse of $a$. Finally, to show associativity, just note that $a+(b+c) = (a+b)+c$ is true for any integers $a$, $b$, and $c$, so therefore adding any elements $a, b, c \in \mathbb{Z}_n$ must yield the same remainder.

Whew! Most of the time there's no need to be that formal. The groups $\mathbb{Z}_n$ are rather intuitive, so there's no need to get bogged down in this formalism. The real punchline is that we now have two examples of different groups, which will be useful throughout the rest of this document.

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 2.5.** 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 2.6.** Let $G$ be a group. There is a unique identity 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 $a * a^{-1} = a^{-1} * a = e$. In addition, $(a^{-1})^{-1} = a$.

*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, $a^{-1} = \tilde{a}^{-1}$. For the last property, we only need to note that $(a^{-1})^{-1}$ is (by definition) the unique element in $G$ such that $(a^{-1})^{-1} * a^{-1} = a^{-1} * (a^{-1})^{-1} = e$. By the equation $a * a^{-1} = a^{-1} * a = e$, we see that this unique element is indeed $a$.

■

Now, most operations we're familiar with aren't just associative. They have other nice properties as well. The next few definitions solidify this conceptually.

$*$ **Definition 2.7.** Let $*$ be a binary operation on a set $A$. If for all $a, b \in A$, we have $a * b = b * a$, then $*$ is a **commutative** operation.

$*$ **Definition 2.8.** Let $G$ be a group with a binary operation $*$. If $*$ is commutative, then $G$ is an **abelian group**.

**Example 2.9.** The familiar properties of integer addition show that $\mathbb{Z}$ and $\mathbb{Z}_n$ for any $n$ are abelian groups.

# 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. When we do this, it's implied that $G$ 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. And finally, since every group operation is associative, we can drop parentheses in any expression for clarity. For our purposes, these notation decisions 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 3.3.** 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. And if $H$ is a group under the operation of $G$, then this operation is a map from $H \times H$ to $H$. The third property follows from this.

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 $H$.

■

Subgroups also naturally give rise to a discussion of cosets.

**Definition 3.4.** Let $H$ be a subgroup of a group $G$, and let $a \in G$. The set $\{ah \mid h \in H\}$, denoted $aH$, is a subset of $G$. We call this the **left coset** of $H$ containing $a$. Similarly, the set $Ha = \{ha \mid h \in H\}$ is called the **right coset** of $H$ containing $a$.

The following theorems and proofs involving left cosets have symmetrical theorems and proofs involving right cosets, so for this document we'll mostly deal with left cosets. Cosets have a number of interesting properties, but proofs about properties of cosets usually aren't illuminating by themselves. Therefore, it's important to have a good intuition for some of their basic properties. We'll give a few of these properties in the following theorems.

**Theorem 3.5.** Let $H$ be a subgroup of $G$, and let $a, b \in G$. The following are equivalent:

- $a \in bH$
- $aH = bH$
- $b^{-1}a \in H$

*Proof.* We'll prove these implications in order. First, suppose $a \in bH$. So $a = bh_1$ for some $h \in H$. Let $ah \in aH$. Then $ah = (bh_1)h = b(h_1h)$. Because $H$ is a subgroup, $h_1h \in H$, so $b(h_1h) \in bH$, meaning that $ah \in bH$, or $aH \subseteq bH$. Now let $bh \in bH$. Note that $b = ah_1^{-1}$. Therefore $bh = (ah_1^{-1})h = a(h_1^{-1}h)$. Again, because $H$ is a subgroup, $h_1^{-1}h \in H$, so $bh \in aH$, and $bH \subseteq aH$. Therefore $aH = bH$.

Now suppose that $aH = bH$. If $ah_1 \in aH$, then there exists an $h_2 \in H$ such that $ah_1 = bh_2$. Multiplying on the left by $b^{-1}$ and on the right by $h_1^{-1}$, we see that $b^{-1}a = h_2h_1^{-1}$. Because $H$ is a subgroup, we therefore have $b^{-1}a \in H$.

Finally, suppose that $b^{-1}a \in H$. So there exists an $h \in H$ such that $b^{-1}a = h$. Multiplying on the left by $b$, this implies that $a = bh \in bH$, proving the theorem.

■

Again, the proof of the above theorem isn't terribly important. The important thing to realize is that, in a loose sense, the equivalent statements above can be "multiplied by $b$" to get one of the other forms.

**Theorem 3.6.** Let $H$ be a subgroup of a group $G$. Then the set of all left cosets of $H$ partition $G$.

*Proof.* Since $H$ is a subgroup of $G$, we must have $e \in H$, so $H$ is nonempty. Therefore no left coset of $H$ is empty by construction. Let $a \in G$. Since $e \in H$, we have $ae = a \in aH$, so each element is in at least one coset. Suppose $a \in bH$ and $a \in cH$ for $b, c \in G$. By the above theorem, we therefore have $aH = bH$ and $aH = cH$. Set equality is an equivalence relation, so therefore $bH = cH$. This shows that every element of $G$ is in exactly one left coset of $H$.

■

# 4 Normal Subgroups

Normal subgroups may be the first concept introduced here that seems a little unmotivated. As it turns out, normal subgroups are incredibly relevant to homomorphisms. If you feel like you're missing the forest for the trees, understanding the *statement* of a theorem is more important than understanding its proof, because we'll be building on these concepts from here on out. Feel free to skip a confusing proof and come back to it later.

**Definition 4.1.** Let $H$ be a subgroup of $G$. We call $H$ a **normal** subgroup of $G$ if

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} = H$$

for all $g \in G$.

As it turns out, it doesn't matter much what we take as the definition of a normal subgroup, as the next theorem shows. Textbooks often take any one of the following equivalent characterizations of normal subgroups as the definition.

**Theorem 4.2.** Let $H$ be a subgroup of $G$. The following are equivalent:

- For all $g \in G$, $gHg^{-1} = H$.
- For all $g \in G$ and $h \in H$, $ghg^{-1} \in H$.
- For all $g \in G$, $gH = Hg$.

*Proof.* First, assume that $gHg^{-1} = H$. then clearly if $gh_1g^{-1} \in gHg^{-1}$, then there exists an $h_2 \in H$ such that $gh_1g^{-1} = h_2$, so the first implication holds.

Now, assume that the second listed property holds. Let $gh \in gH$. We know that there exists an $h' \in H$ such that $ghg^{-1} = h'$. Therefore $gh = h'g \in Hg$, so $gH \subseteq Hg$. Similarly, let $hg \in Hg$. Applying the assumption with the element $g^{-1} \in G$, we know that there exists an $h' \in H$ such that $g^{-1}h\left(g^{-1}\right)^{-1} = g^{-1}hg = h'$. Therefore $hg = h'g \in Hg$, so $Hg \subseteq gH$. This means that $gH = Hg$.

Finally, let $g \in G$, and assume that $gH = Hg$. Therefore:

$$\begin{aligned} \{gh \,|\, h \in H\} &= \{hg \,|\, h \in H\} \\ \{ghg^{-1} \,|\, h \in H\} &= \{hgg^{-1} \,|\, h \in H\} \\ \{ghg^{-1} \,|\, h \in H\} &= \{h \,|\, h \in H\} \\ gHg^{-1} &= H \end{aligned}$$

So our theorem is proven. We can feel free to use these alternate definitions interchangeably.

■

# 5 Homomorphisms

Now that we have a good understanding of ways to classify group structures, we'd like to have some way to relate the structure of one group to the structure of another. Homomorphisms are exactly the tool we need.

**Definition 5.1.** Let $G$ and $G'$ be groups. A **homomorphism** between $G$ and $G'$ is a function $\phi : G \to G'$ such that

$$\phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in G$.

The important thing to realize here is that the multiplication on the left-hand side is happening within $G$, and the multiplication on the right-hand side is happening within $G'$. If we explicitly write these group operations as $*$ and $\star$, respectively, the homomorphism property above can be written as

$$\phi(a * b) = \phi(a) \star \phi(b).$$

The next theorems will show a few ways in which the structure of $G$ is mapped onto the structure of $G'$ under a homomorphism.

**Theorem 5.2.** Let $G$ and $G'$ be groups, and let $\phi : G \to G'$ be a homomorphism. Then the following hold:

- If $e$ and $e'$ are the respective identities for $G$ and $G'$, then $\phi(e) = e'$.
- For all $a \in G$, $\phi(a^{-1}) = \phi(a)^{-1}$.
- If $H$ is a subgroup of $G$, then $\phi(H)$ is a subgroup of $G'$.
- If $H'$ is a subgroup of $G'$, then $\phi^{-1}(H')$ is a subgroup of $G$.

*Proof.* Let $a \in G$. By our group axioms and application of the homomorphism property, we have:

$$e'\phi(a) = \phi(a) = \phi(ea) = \phi(e)\phi(a)$$

Therefore by cancellation, $e' = \phi(e)$.

For the second property, note that $\phi(a)^{-1}$ is the unique element of $G'$ such that $\phi(a)^{-1}\phi(a) = \phi(a)\phi(a)^{-1} = e'$. But we also have the following:

$$e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$$

$$e' = \phi(e) = \phi(a^{-1}a) = \phi(a^{-1})\phi(a)$$

Therefore we have $\phi(a)^{-1} = \phi(a^{-1})$.

Now let $H$ be a subgroup of $G$. First, we know $e \in H$, so therefore $e' = \phi(e) \in \phi(H)$. Let $h', g' \in \phi(H)$, so there exists $h, g \in H$ such that $\phi(h) = h'$ and $\phi(g) = g'$. Because $H$ is a subgroup, $h^{-1} \in H$, and therefore $\phi(h^{-1}) = \phi(h)^{-1} = h'^{-1} \in \phi(H)$, so $H$ is closed under inverses. And because $\phi$ is a homomorphism:

$$h'g' = \phi(h)\phi(g) = \phi(hg)$$

But $H$ is a subgroup of $G$, so $hg \in H$, which implies that $h'g' \in \phi(H)$. Therefore $\phi(H)$ is a subgroup of $G'$.

Finally, let $H'$ be a subgroup of $G'$. We need to show that $\phi^{-1}(H')$ is a subgroup of $G$. Since $H'$ is a subgroup, $e' \in H'$, and because $\phi(e) = e'$, we have $e \in \phi^{-1}(H')$. Let $a, b \in \phi^{-1}(H')$. Therefore $\phi(a), \phi(b) \in H'$. Because $H'$ is a subgroup, $\phi(a)^{-1} = \phi(a^{-1}) \in H'$, meaning that $a^{-1} \in \phi^{-1}(H')$, so $\phi^{-1}(H')$ is closed under inverses. We also know that $\phi(a)\phi(b) = \phi(ab) \in H'$. Therefore $ab \in \phi^{-1}(H')$, so $\phi^{-1}(H')$ is closed under multiplication, and is therefore a subgroup of $G$.

■

Great! So we can see that homomorphisms (loosely speaking) take identities to identities, inverses to inverses, and subgroups to subgroups. There's in fact a stricter kind of structure-preserving map between groups, described in the definition below.

**Definition 5.3.** Let $G$ and $G'$ be groups. We say a map $\phi : G \to G'$ is a **group isomorphism** if it is a homomorphism, and is a bijection.

If we can find an isomorphism between two groups, then their structures are actually completely identical. The only difference between them is the names of the elements. For now, note that an isomorphism must be injective, but this need not be the case for homomorphisms. In particular, more than one element of $G$ may be mapped to the identity of $G'$. This concept is important enough that it warrants a definition.

**Definition 5.4.** Let $\phi : G \to G'$ be a group homomorphism. The set

$$\{g \in G \mid \phi(g) = e'\}$$

is called the **kernel** of $\phi$, denoted $\ker \phi$.

**Theorem 5.5.** If $\phi : G \to G'$ is a group homomorphism, then $\ker \phi$ is a normal subgroup of $G$.

*Proof.* Clearly $e \in \ker \phi$, because $\phi(e) = e'$. If $a, b \in \ker \phi$, then

$$\phi(a^{-1}) = \phi(a)^{-1} = e'^{-1} = e',$$

so $a^{-1}$ is also in $\ker \phi$. Also, by the homomorphism property,

$$\phi(ab) = \phi(a)\phi(b) = e'e' = e',$$

so $\ker \phi$ is a subgroup of $G$. To show that it's normal, let $g \in G$ and $k \in \ker \phi$. Then we have

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e'\phi(g)^{-1} = e',$$

So $gkg^{-1}$ is in $\ker \phi$ as well.

■