The Fundamental Homomorphism Theorem

Matthew Gregoire

June 2020

Contents

Introduction

The goal of this document is to introduce the reader to the fundamental homomorphism theorem for groups, starting from basic definitions. This result is sometimes otherwise known as the first isomorphism theorem. I chose to write this document because of the difficulty I had understanding this theorem in my undegraduate algebra class. It's quite an elegant piece of mathematics, but looking back I was shocked at how poorly it was explained in my textbook.

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. To achieve our goal, we proceed at a breakneck pace most of the way through. If this is your first exposure to this material, make sure to take time to digest each result.

That being said, 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 required. The examples are clearly labeled if you don't care to read them, and unnecessary results are marked with a spade in the left margin, as shown in this sentence. The hope in marking the unnecessary parts is that, if this is used as a reference material, the reader will know exactly which results are necessary and sufficient to prove the theorem. None of the main content depends on this extra material, but the examples and marked theorems do build on each other from the beginning.

♠

1 Groups

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

Definition 1.1. Let G be a set. A **binary operation** $*$ on G is a function from $G \times G$ to G.

If in G, we have $*(a, b) = c$, we usually 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 1.2. A **group** is a set G along with a binary operation $*$ 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.

For the sake of consistency, we'll tend to use e as the identity symbol in a general group, unless stated otherwise. We'll give a few examples of groups to get a feel for their structure.

Example 1.3. 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. For similar reasons, the sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are also groups under addition.

Example 1.4. 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 $a \tilde{+} b = r$ in $\mathbb{Z}_n$. Since $0 \leq r < n$, this is also an element of $\mathbb{Z}_n$, so $\tilde{+}$ is a well-defined binary operation.

0 is again the identity, because $a + 0 = 0 + a = n \cdot 0 + a$, so $a \tilde{+} 0 = 0 \tilde{+} a = a$. 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 from this point forward. The real punchline is that this set of numbers is a group, and operating within $\mathbb{Z}_n$ should naturally feel like operating on congruence classes of integers modulo n.

In addition to to simply defining groups, we need to build up a little machinery in order to understand their structure. The next few theorems build only from the definition of a group.

Theorem 1.5. 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**, respectively.

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,

$$\left(a^{-1} * a\right) * b = \left(a^{-1} * a\right) * c.$$

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 1.6. Let G be a group with a binary operation $*$. 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 $a * a^{-1} = a^{-1} * a = e$. Also $\left(a^{-1}\right)^{-1} = a$, that is, the inverse of a^{-1} is a.

Proof. Suppose that e and e' are both elements of G that act as an identity. 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 $a * a' = a' * a = e$, then we have

$$a * a^{-1} = e = a * a'.$$

And by cancellation, $a^{-1} = a'$. 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 have other nice properties, besides being simply associative. The next few definitions solidify one of these properties, which should be fairly intuitive.

♠ **Definition 1.7.** 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 1.8.** Let G be a group with a binary operation $*$. If $*$ is commutative, then G is an **abelian group**. Otherwise, G is **nonabelian**.

Example 1.9. The familiar properties of addition show that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_n$ for any n are abelian groups.

Example 1.10. Let F be the set of all invertible functions from $\mathbb{R}$ to $\mathbb{R}$, and consider the operation of function composition defined on F. Here $i(x) = x$ serves as the identity function, and each function in F has an inverse in F by construction. Composition of invertible functions is associative as well. Finally, if $f, g \in F$, then $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$, because:

$$\begin{aligned}
\left[(f \circ g) \circ \left(g^{-1} \circ f^{-1}\right)\right](x) &= \left[f \circ \left(g \circ g^{-1}\right) \circ f^{-1}\right](x) \\
&= \left[f \circ i \circ f^{-1}\right](x) \\
&= \left[f \circ f^{-1}\right](x) \\
&= i(x),
\end{aligned}$$

which is the identity map. It can be similarly shown that $g^{-1} \circ f^{-1}$ is the left inverse of $f \circ g$ as well. Therefore the composition of invertible functions is again invertible, and F forms a group under function composition. But composition of functions is not commutative in general. Consider the invertible functions $f(x) = x + 1$ and $g(x) = x^3$. Both of these are invertible functions, but we have $(f \circ g)(x) = x^3 + 1$, while $(g \circ f)(x) = (x + 1)^3$. Therefore F is not an abelian group.

♠ Now to get more of a feel for the structure of a group, we can introduce **Cayley tables** for finite groups. The Cayley table for $\mathbb{Z}_4$ is given in Figure 1.11. The rows and columns are titled with elements of the group, and in row a and column b we put the element $a + b$. Note that the entry $a + b$ is the same as $b + a$ because $\mathbb{Z}_4$ is abelian, but this is not always the case. For a general group, the entry in row a and column b could be different from the entry in row b and column a.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Figure 1.11: Cayley table for $\mathbb{Z}_4$.

For the rest of this section, we'll develop one extended example of a nonabelian group. Consider an equilateral triangle with labeled vertices, shown in Figure 1.12. This might seem a strange thing to consider. But now

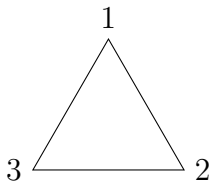

Figure 1.12

we ask ourselves: how we can transform this triangle so that it lands back on itself, potentially with the vertices rearranged? We can leave the triangle alone, which won't permute the vertices at all. We can also reflect through an axis going through one vertex, and we can rotate the triangle by 60° either clockwise or counterclockwise. This gives six possible transformations, all shown below.

From left to right and top to bottom as shown in Figure 1.13, let's give these transformations of the triangle the names e, ρ_1, ρ_2, μ_1, μ_2, and μ_3 respectively, where ρ and μ are suggesting *rotations* and *mirrorings*, respectively. The crucial step is to consider these transformations as elements of a group, where the group operation is composition of transformations. This is

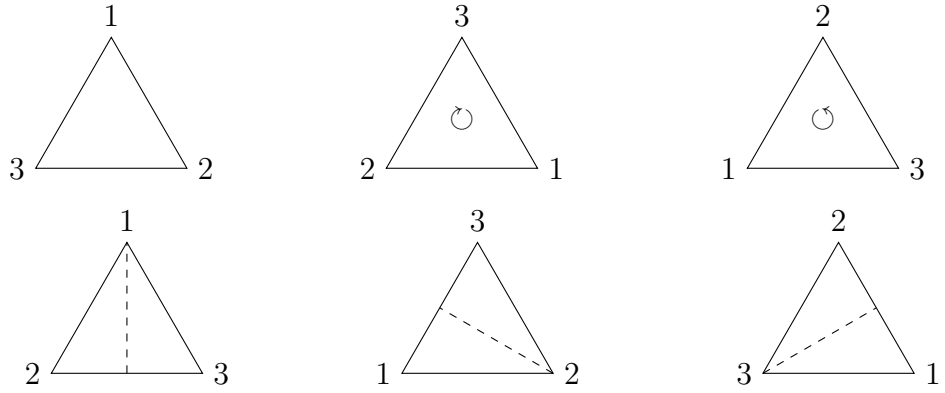

Figure 1.13: The six symmetries of an equilateral triangle.

a well-defined binary operation, because these six positions exhaust all possible orientations of the vertices. Therefore every two transformations applied in succession will result in another positioning of vertices listed above. Here e acts as the identity element. It's easy to see that the two opposite rotations are inverses of each other, and each reflection is its own inverse. Finally, each transformation can be viewed in a natural way as a bijection between $\{1, 2, 3\}$ and itself: just take the image of i as the label of the vertex that lands in position i. We know that function composition is associative, so composition of transformations is also associative. Therefore this set is a group under composition. We'll call this group D_3, the **dihedral group on 3 vertices**. In fact, symmetries of a regular n-gon will always form a group, denoted D_n.

$\circ$	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
e	e	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	e	μ_2	μ_3	μ_1
ρ_2	ρ_2	e	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	e	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	e	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	e

Figure 1.14: Cayley table for D_3.

Last but not least, the Cayley table for D_3 is shown in Figure 1.14. Notice that this group is nonabelian, as promised! This group has many interest-

ing symmetries, and will serve as our prototypical example of a nonabelian group.

2 Subgroups and Cosets

From here on out, we'll almost exclusively use multiplicative notation when discussing 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 or ambiguity.

Subgroups are a somewhat natural extension from the concept of groups. The formal definition is given below.

Definition 2.1. 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 2.2. Let $*$ be a binary operation defined on a set A, and let $B \subseteq A$. If for all $a, b \in B$, $a * b$ is also in B, then B 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 2.3. 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.

■

Example 2.4. If G is any group, the set $\{e\}$ containing only the identity, with binary operation $e * e = e$, is always a subgroup of G that quickly satisfies the requirements of Theorem 2.3. This is sometimes called the **trivial subgroup** of G. Moreover, G is also a subgroup of itself, the **improper subgroup** of G.

Example 2.5. Take the set $\{\dots, -8, -4, 0, 4, 8, \dots\} \subseteq \mathbb{Z}$ consisting of all multiples of 4, with the operation of addition. This is denoted $4\mathbb{Z}$. We can see $0 \in 4\mathbb{Z}$, and acts as the identity. Also, if $n = 4k$ for $k \in \mathbb{Z}$, then $-n = -(4k) = 4(-k) \in 4\mathbb{Z}$. Finally, $4a + 4b = 4(a + b) \in 4\mathbb{Z}$ for any $4a, 4b \in 4\mathbb{Z}$. Therefore $4\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition. The same method can show that $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ for any $n \geq 1$.

Example 2.6. Take within D_3 the subset $\{e, \rho_1, \rho_2\}$ of the rotations and the identity (a trivial rotation). By examining the Cayley table in Figure 1.14, we see that this set is closed under composition and inverses, and is thus a subgroup of D_3. By a similar argument, the subset $\{e, \mu_1\}$ is also a subgroup of D_3.

Subgroups also naturally give rise to discussion of cosets.

Definition 2.7. 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.

Example 2.8. Take the group $\mathbb{Z}$ and its subgroup $4\mathbb{Z}$. Here, note that we'll write cosets in additive notation, because these groups are written in additive

notation. The cosets are given below.

$$\begin{aligned} 0 + 4\mathbb{Z} &= \{\dots, -8, -4, 0, 4, 8, \dots\} \\ 1 + 4\mathbb{Z} &= \{\dots, -7, -3, 1, 5, 9, \dots\} \\ 2 + 4\mathbb{Z} &= \{\dots, -6, -2, 2, 6, 10, \dots\} \\ 3 + 4\mathbb{Z} &= \{\dots, -5, -1, 3, 5, 11, \dots\} \end{aligned}$$

We'll prove soon the intuitive fact that these cosets do indeed partition $\mathbb{Z}$. We could also take the coset of any other integer. For example, $-6 + 4\mathbb{Z} = \{\dots, -14, -10, -6, -2, 2, 6, 10, \dots\} = 2 + 4\mathbb{Z}$. This shows that the choices of representatives for cosets is not unique.

Example 2.9. Consider D_3 and its subgroup $H = \{e, \mu_1\}$. The left cosets of H are as follows.

$$\begin{aligned} eH &= \{e, \mu_1\} \\ \rho_1 H &= \{\rho_1, \mu_2\} \\ \rho_2 H &= \{\rho_2, \mu_3\} \end{aligned}$$

We can also verify (using the Cayley table in Figure 1.14) that these left cosets are unique. That is, $\mu_2 H = \rho_1 H$, and $\mu_3 H = \rho_2 H$. We will prove that this is true in general in Theorem 2.10.

The following theorems and proofs involving left cosets have symmetrical theorems and proofs involving right cosets. For this document we'll mostly deal with left cosets, but this is only done for simplicity. Right cosets have corresponding properties. Cosets have a number of interesting properties, but the next few proofs aren't illuminating by themselves. Therefore it's far more important to have a good intuition for some of their basic properties than to remember all the mechanics of the proofs.

Theorem 2.10. 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 mechanics of the proof above aren'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. Internalizing this result will help in all of our work from here on out. Also, from this we immediately have the following.

Corollary 2.11. Let $h \in H$. Then $hH = H$.

Proof. First, we immediately see that $eH = \{eh \,|\, h \in H\} = H$. Therefore, taking $a = h$ and $b = e$ in the preceding theorem, we're given the first bulleted property. Therefore the second property holds, and $hH = eH = H$.

■

Theorem 2.12. 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.

■

At this point, we'll take a slight detour to prove Lagrange's Theorem. While not strictly necessary to understand the Fundamental Homomorphism Theorem, the result is so elegant that we would be remiss to leave it out.

♠ **Theorem 2.13.** If H is a subgroup of G, then every left coset of H has the same cardinality as H itself.

Proof. Let aH be a coset of H. We'll find a bijection between H and aH, namely, the map defined by $f(x) = ax$. Suppose that $f(g) = f(h)$. Then $ag = ah$, and by cancellation, $g = h$, so f is an injection. And clearly if $y \in aH$, then $y = ah$ for some $h \in H$, so $f(h) = ah = y$. So f is surjective, and therefore a bijection. ■

♠ **Definition 2.14.** Let G be a group. The number of elements in G is called the **order** of G, denoted $|G|$. If G has finitely many elements we call it a **finite group**. Otherwise, we say G has **infinite order**.

♠ **Theorem 2.15** (Lagrange's Theorem)**.** Let G be a finite group. If H is a subgroup of G, then the order of H divides the order of G.

Proof. By Theorem 2.12, the cosets of H partition G. And by Theorem 2.13, each coset of H has size $|H|$. If there are n distinct cosets of H, then the quantity $n|H|$ counts each element of G exactly once. Therefore

$$|G| = n|H|,$$

so the order of H is a divisor of the order of G.

■

Example 2.16. Take the subset $\{0, 2, 4\}$ of $\mathbb{Z}_6$. By computing every possible sum in this set, we see this is actualy a subgroup of $\mathbb{Z}_6$. Note that Lagrange's Theorem holds, as $|\mathbb{Z}_6| = 6$ and $|\{0, 2, 4\}| = 3$, and $3|6$. By the contrapositive of the theorem, we also see that any subset of $\mathbb{Z}_6$ with cardinality other than $1, 2, 3$, or 6 can't be a subgroup of $\mathbb{Z}_6$.

Example 2.17. Consider $\mathbb{Z}_p$, where p is prime. By Lagrange's Theorem, the only possible orders for subgroups of $\mathbb{Z}_p$ are 1 and p. Therefore $\mathbb{Z}_p$ has no proper nontrivial subgroups.

3 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 3.1. 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 3.2. 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:

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

so our theorem is proven. We can feel free to use these alternate definitions of normal subgroups interchangeably.

■

Example 3.3. Any subgroup of an abelian group is normal. If H is a subgroup of an abelian group G, then let $h \in H$ and $g \in G$. We see that $ghg^{-1} = gg^{-1}h = eh = h \in H$, so by the second property of Theorem 3.2, H is normal. In particular, this shows that all subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$ for any $n \in \mathbb{Z}^+$ are normal.

Example 3.4. Let H be the subgroup $\{e, \mu_2\}$ of D_3, described in Example 2.6. Note that

$$\rho_1 H = \{\rho_1, \mu_3\}, \text{but}$$
$$H\rho_1 = \{\rho_1, \mu_1\}.$$

Therefore $\rho_1 H \neq H\rho_1$, so H is not a normal subgroup of D_3. Alternatively, we could note that $\rho_1\mu_2\rho_1^{-1} = (\rho_1\mu_2)\,\rho_2 = \mu_3\rho_2 = \mu_1 \notin H$ to show that H is not normal in D_3.

Example 3.5. Now let N be the subgroup $\{e, \rho_1, \rho_2\}$ of D_3. The left and right cosets are given below.

$$eN = \{e, \rho_1, \rho_2\} \qquad He = \{e, \rho_1, \rho_2\}$$
$$\mu_1 H = \{\mu_1, \mu_3, \mu_2\} \qquad H\mu_1 = \{\mu_1, \mu_2, \mu_3\}$$

These are the only cosets of N in D_3 by Theorem 2.10. (An identical result holds for right cosets as well.) Therefore we can see that $aN = Na$ for all $a \in N$, so N is normal in D_3. This is a special case of the theorem below.

♠ **Theorem 3.6.** Let G be a group with a subgroup H. If $|G|/|H| = 2$, then H is a normal subgroup of G.

Proof. We see by the proof of Lagrange's Theorem that there are exactly two cosets of H in G. Therefore these are precisely H and $G - H$. If $a \in H$, then clearly aH and Ha are simply H itself. And if $a \notin H$, then a must be in $G - H = aH = Ha$, so H is normal in G. ■

4 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 4.1. Let G and G' be groups. A **homomorphism** between G and G' is a function $\phi : G \to G'$ such that the *homomorphism property*

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

is satisfied 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

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

Example 4.2. Consider the groups $\mathbb{Z}$ and $\mathbb{Z}_n$ under addition. Note that both of these groups use additive notation. We claim that the map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ taking every integer x to its remainder when divided by n is a homomorphism. We only have to check the above property. If $a = q_1 n + r_1$ and $b = q_2 n + r_2$ using the division algorithm, then

$$\begin{aligned} a + b &= q_1 n + r_1 + q_2 n + r_2 \\ &= (q_1 + q_2)n + (r_1 + r_2), \end{aligned}$$

but $r_1 + r_2$ may be greater than n. So if $r_1 + r_2 = q_3 n + r_3$, then

$$\begin{aligned} a + b &= (q_1 + q_2)n + (q_3 n + r_3) \\ &= (q_1 + q_2 + q_3)n + r_3. \end{aligned}$$

Therefore $\phi(a + b) = r_3$. But we also have $\phi(a) = r_1$ and $\phi(b) = r_2$. Since $\phi(a) + \phi(b)$ is an addition in $\mathbb{Z}_n$, it's the remainder of $r_1 + r_2$ when divided by n, which was defined above to be r_3. Therefore $\phi(a) + \phi(b) = r_3 = \phi(a + b)$, so ϕ is a homomorphism.

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 4.3. 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 $\phi(e) = e' \in \phi(H)$. Let $h', g' \in \phi(H)$. So there exist $h, g \in H$ 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 ϕ 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. This means we're justified in describing them as maps that preserve structure. There is in fact a stricter kind of structure-preserving map between groups, described in the definition below.

Definition 4.4. Let G and G' be groups. We say a map $\phi : G \to G'$ is a **group isomorphism** if it is a homomorphism and 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.

Example 4.5. Consider the groups $\mathbb{Z}_3$ and the subgroup $H = \{e, \rho_1, \rho_2\}$ of D_3. We claim that the map $\phi : \mathbb{Z}_3 \to H$ given by

$$\phi(0) = e \qquad \phi(1) = \rho_1 \qquad \phi(2) = \rho_2$$

is an isomorphism. It's clearly a bijection, and we only have to check that it's a homomorphism. There are simpler ways to check this, but the group is small enough that we can test every possible input to ϕ. It helps that we know $\mathbb{Z}_3$ is abelian, so we can reduce the number of inputs to check by half. We can also check by looking at the Cayley table in Figure 1.14 that H is also abelian.

a	b	$a+b$	$\phi(a)$	$\phi(b)$	$\phi(a)\phi(b)$	$\phi(a+b)$
0	0	0	e	e	e	e
0	1	1	e	ρ_1	ρ_1	ρ_1
0	2	2	e	ρ_2	ρ_2	ρ_2
1	1	2	ρ_1	ρ_1	ρ_2	ρ_2
1	2	0	ρ_1	ρ_2	e	e
2	2	1	ρ_2	ρ_2	ρ_1	ρ_1

The last two columns match, so this is indeed an isomorphism.

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 4.6. Let $\phi : G \to G'$ be a group homomorphism. The set

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

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

Theorem 4.7. 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.

■

Example 4.8. Let $\phi : \mathbb{Z} \to \mathbb{Z}_4$ be the homomorphism defined in Example 4.2. The kernel of ϕ is the set of all $n \in \mathbb{Z}$ such that the remainder of n divided by 4 is 0. In other words, this is all multiples of four. This is indeed the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$, and it is automatically normal because $\mathbb{Z}$ is abelian.

We'll end this section with a useful way to test if a homomorphism is injective, although we won't be using it after this.

♠ **Theorem 4.9.** Let $\phi : G \to G'$ be a group homomorphism. Then ϕ is injective if and only if $\ker \phi = \{e\}$.

Proof. Suppose that ϕ is injective. Then if $\phi(a) = e'$, the fact than $\phi(e) = e'$ proves that $a = e$. Therefore $\ker \phi = \{e\}$. Conversely, if we know $\ker \phi = \{e\}$, suppose that $\phi(a) = \phi(b)$. Then we have

$$\begin{aligned} \phi(a)\phi(b)^{-1} &= e' \\ \phi(a)\phi(b^{-1}) &= e' \\ \phi(ab^{-1}) &= e'. \end{aligned}$$

Therefore $ab^{-1} \in \ker \phi$, so $ab^{-1} = e$. Multiplying on the right by b, we see that $a = b$, so ϕ is injective.

■

♠ We know that $\phi(G)$ is a subgroup of G' for any homomorphism $\phi : G \to G'$. Since ϕ definitely maps G *onto* $\phi(G)$, this means that G is actually isomorphic to $\phi(G)$ if and only if ϕ is injective, that is, if and only if $\ker \phi = \{e\}$. While not strictly useful for our purposes, this shows some of the power of kernels of homomorphisms. This theme will be expanded upon through the rest of this document.

5 Factor Groups

At this point, all of the concepts we've defined start to come together. First, we need just a little more machinery to operate on cosets.

Theorem 5.1. Let H be a subgroup of G, and consider two left cosets aH and bH of H. Then the operation $(aH)(bH) = (ab)H$ is well-defined if and only if H is a normal subgroup.

Before proving this, let's think about what we need to show. Left coset multiplication, which is a new operation on cosets, is well-defined as a binary operation if and only if it satisfies Definition 1.1. That is, it needs to map each pair of left cosets to a *unique* corresponding coset. Recall that $aH = cH$ is equivalent to $c \in aH$ by Theorem 2.10. Therefore, left coset multiplication is well-defined if and only if, for all $ah_1 \in aH$ and $bh_2 \in bH$,

$$(aH)(bH) = (ah_1H)(bh_2H) = (ab)H = (ah_1bh_2)H.$$

With this reformulation, we can now proceed to the proof.

Proof. Assume that the operation is well-defined. We want to show that H is normal. Let $a \in G$. We'll show that $aH = Ha$.

Let $x \in aH$, so $xH = aH$. Computing with our operation, which by assumption is well-defined, we have

$$(xH)(a^{-1}H) = (xa^{-1})H.$$

But we could also compute the same product with different representatives, as the following.

$$(aH)(a^{-1}H) = (aa^{-1})H = eH = H$$

Therefore $(xa^{-1})H = H$. Using the first bulleted property of Theorem 2.10, this implies that $xa^{-1} \in H$, so there exists an $h \in H$ such that $xa^{-1} = h$, or $x = ha \in Ha$. Therefore $aH \subseteq Ha$.

Similarly, let $x \in Ha$. By the same reasoning, we have

$$\begin{aligned}(Ha^{-1})(Hx) &= (Ha^{-1})(Ha)\\ H(a^{-1}x) &= H.\end{aligned}$$

Therefore $a^{-1}x = h$ for some $h \in H$, which means that $x = ah \in aH$, so $Ha \subseteq aH$. Therefore $aH = Ha$, and H is normal.

Conversely, suppose that H is normal. We need to show that coset multiplication is well-defined. Let aH and bH be cosets, and let $ah_1 \in aH$ and $ah_2 \in bH$. Then our operation states that $(ah_1)H(bh_2)H = (ah_1bh_2)H$. Because H is normal, we know that $Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Therefore, $a\,(h_1b)\,h_2 = abh_3h_2$. So we have

$$\begin{aligned}(ah_1H)\,(bh_2H) &= (ah_1bh_2H)\\ &= ab\,(h_3h_2)\,H\\ &= abH.\end{aligned}$$

This means coset multiplication doesn't depend on choices of representatives, and is therefore well-defined.

■

Example 5.2. Consider the subgroup $H = \{e, \mu_2\}$ of D_3. As shown in Example 3.4, H is not normal in D_3. Therefore multiplication of cosets of H is not well-defined. Indeed, we can see that

$$\rho_1H = \mu_3H = \{\rho_1, \mu_3\}, \qquad \mu_1H = \rho_2H = \{\mu_1, \rho_2\}.$$

However, if we attempt to multiply these cosets using the operation defined above, we have

$$\begin{aligned}(\rho_1H)\,(\mu_1H) &= (\rho_1\mu_1)\,H\\ &= \mu_2H\\ &= H,\end{aligned}$$

while choosing different representatives, we have

$$\begin{aligned}(\mu_3H)\,(\rho_2H) &= (\mu_3\rho_2)\,H\\ &= \mu_1H\\ &\neq H.\end{aligned}$$

From this example we can see that choosing different representatives of the cosets actually changes the output! So coset multiplication of H is indeed not well-defined.

You might wonder what the point of defining an operation on the cosets of a subgroup might be. As a matter of fact, if our coset multiplication is well-defined, the cosets themselves form a group! We can often think of the operations on cosets as operations of certain types or classes of elements in the original group.

Theorem 5.3. Let N be a normal subgroup of G. Then the set of cosets of N form a group under coset multiplication. We call this group a **factor group**, or **quotient group**, denoted G/N. This is read as "G mod N" or "G over N."

Proof. Since N is a normal subgroup of G, coset multiplication is well-defined. Let $aN, bN, cN \in G/N$. $eN = N$ serves as the identity element in G/N, because $(eN)(aN) = (ea)N = aN = (ae)N = (aN)(eN)$. In addition, $(a^{-1}N)\,(aN) = (a^{-1}a)\,N = eN = (aa^{-1})\,N = (aN)\,(a^{-1}N)$, so each coset has its own inverse. Finally, we have

$$\begin{aligned}(aN)\,[(bN)(cN)] &= aN(bcN) = a(bc)N = (ab)cN \\ &= (abN)cN = [(aN)(bN)]\,cN.\end{aligned}$$

So associativity in G/N follows from associativity in G. Therefore G/N is a group.

■

Example 5.4. Consider the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$ under addition. Because $\mathbb{Z}$ is abelian, every subgroup of $\mathbb{Z}$ is normal. Therefore $\mathbb{Z}/4\mathbb{Z}$ is a group whose elements are the cosets of $4\mathbb{Z}$, namely $0 + 4\mathbb{Z}$, $1 + 4\mathbb{Z}$, $2 + 4\mathbb{Z}$, and $3 + 4\mathbb{Z}$. The Cayley table for this factor group is shown in Figure 5.5. Because $\mathbb{Z}$ and its subgroups are additive, we write cosets additively and speak of coset *addition*.

Finally, let's connect the idea of a factor group to homomorphisms from the previous section.

Theorem 5.6. Let G be a group with a normal subgroup N, and let $\phi : G \to G/N$ be defined by $\phi(a) = aN$. Then ϕ is a homomorphism, sometimes called the *natural* or *canonical* homomorphism between these groups.

$+$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

Figure 5.5

Proof. Let $a, b \in G$. Because N is normal, coset multiplication is well-defined. Therefore $\phi(ab) = abN = (aN)(bN) = \phi(a)\phi(b)$, so the homomorphism property holds.

■

6 Fundamental Homomorphism Theorem

Now we finally have built all the machinery we need to tackle this theorem. The statement is as follows.

Theorem 6.1 (The Fundamental Homomorphism Theorem)**.** Let $\phi : G \to G'$ be a group homomorphism with kernel K. Then $\mu : G/K \to \phi(G)$ defined by $\mu(aK) = \phi(a)$ is an isomorphism. If $\gamma : G \to G/K$ is the canonical homomorphism given by $\gamma(a) = aK$, then $\mu(aK) = \mu(\gamma(a))$ for all $a \in G$, and μ is the unique isomorphism with this property.

Proof. By Theorem 4.7, K is a normal subgroup of G, so it makes sense to discuss G/K. First, let's check that μ is a homomorphism. Let $aK, bK \in G/K$. Because multiplication of cosets of K is well-defined, and ϕ is a homomorphism, we can see that

$$\begin{aligned}\mu(aKbK) &= \mu(abK)\\ &= \phi(ab)\\ &= \phi(a)\phi(b)\\ &= \mu(aK)\mu(bK),\end{aligned}$$

so the homomorphism property is satisfied. Suppose that $\mu(aK) = \mu(bK)$.

Therefore $\phi(a) = \phi(b)$, and because ϕ is a homomorphism,

$$\begin{aligned}\phi(a)\phi(b)^{-1} &= e' \\ \phi(a)\phi(b^{-1}) &= e' \\ \phi(ab^{-1}) &= e'.\end{aligned}$$

Therefore $ab^{-1} \in \ker(\phi) = K$. By Theorem 2.10, this implies that $aK = bK$, so μ is injective. Now let $\phi(a) \in \phi(G)$. Clearly $\mu(aK) = \phi(a)$, so μ is also surjective. Therefore μ is indeed an isomorphism.

To check final property, let $a \in G$. Then $\mu(\gamma(a)) = \mu(aK) = \phi(a)$, as desired. To demonstrate uniqueness, suppose μ' is another isomorphism between G/K and $\phi(G)$ such that $\phi(a) = \mu'(\gamma(a))$ for all $a \in G$. Then we have $\mu(\gamma(a)) = \phi(a) = \mu'(\gamma(a))$ for all $a \in G$. Since every element of G/K is of the form $\gamma(a)$ for some $a \in G$, we see that μ and μ' agree at every element of their domain, and are thus the same function. So the theorem is proven. ■

Essentially this proof tells us the following: if we are given a homomorphism ϕ with a kernel K, which can be symbolized as the following:

$$G \xrightarrow{\phi} G'$$

Then we can always "factor" this map as the isomorphism μ applied to the surjecive map γ. We can also consider the identity map $\lambda : \phi(G) \to G'$ defined by $\lambda(\phi(a)) = \phi(a)$ as a trivial injective homomorphism between $\phi(G)$ and G'. So we can "factor" ϕ completely as:

$$G \xrightarrow[\text{surjection}]{\gamma} G/K \xrightarrow[\text{bijection}]{\mu} \phi(G) \xrightarrow[\text{injection}]{\lambda} G'$$

Example 6.2. Let ϕ be the homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_4$ defined in Example 4.2. We know that the kernel of ϕ is $4\mathbb{Z}$, and also ϕ clearly maps $\mathbb{Z}$ onto $\mathbb{Z}_4$. Therefore by the fundamental homomorphism theorem, $\mathbb{Z}/4\mathbb{Z}$ is isomorphic to $\mathbb{Z}_4$. This is the elegant algebraic way to *define* $\mathbb{Z}_4$, as a group of cosets of $4\mathbb{Z}$ (which are also congruence classes of $\mathbb{Z}$ modulo 4).

Example 6.3. Define $\phi : D_3 \to \mathbb{Z}_2$ by:

$$\phi(e) = \phi(\rho_1) = \phi(\rho_2) = 0 \qquad \phi(\mu_1) = \phi(\mu_2) = \phi(\mu_3) = 1.$$

It's easy to check that this is indeed a homomorphism by looking at Table 1.14. The product of two rotations or two reflections is a rotation, and the product of a rotation and a reflection is a reflection. Thus the homomorphism property is satisfied. We can see that $\ker \phi = \{e, \rho_1, \rho_2\}$. This gives us another proof that this is a normal subgroup of D_3 by Theorem 4.7. If $K = \ker \phi$, then D_3/K is isomorphic to $\phi(D_3) = \mathbb{Z}_2$. We compare their Cayley tables in Figure 6.4 to show that these really are the same group with relabeled elements.

$\circ$	K	$\mu_1 K$
K	K	$\mu_1 K$
$\mu_1 K$	$\mu_1 K$	K

$+$	0	1
0	0	1
1	1	0

Figure 6.4: Cayley tables for D_3/K and $\mathbb{Z}_2$

Afterword

Thank you for taking this journey all the way to the end! Hopefully at this point you have a deeper appreciation for this piece of mathematics. As noted in the introduction, the culmination of this document is sometimes introduced as the first in a set of group isomorphism theorems. The other theorems require a little more machinery, but if you understood everything in this document the other isomorphism theorems shouldn't be too daunting.

This result is an incredibly important step in understanding the theory of groups. Moreover, the fundamental homomorphism theorem presented here is specific to group homomorphisms. In the context of more advanced algebraic structures, such as rings and vector spaces, similar results hold. Understanding this theorem is a stepping stone to those more advanced topics.

I'd like to show thanks to John B. Fraleigh for his textbook *A First Course in Abstract Algebra*. I used the seventh edition of this textbook as the source for most of this material. Despite the poor coverage of the fundamental homomorphism theorem, this really is a fantastic book for an introduction to algebra. In addition, Charles C. Pinter's *A Book of Abstract Algebra* (second edition) was an invaluable resource for me. Its scope isn't as deep as Fraleigh's text, but the explanations in Pinter's book are highly accessible, and the exercises are well-organized. I'd recommend either of these books as a next step in learning more about algebraic structures.