The Fundamental Homomorphism Theorem

Matthew Gregoire

May 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. It's quite an elegant piece of mathematics, but looking back I was shocked at how poorly it was explained in my textbook. To achieve this 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.

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 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.

♠

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 $* : G \times G \to G$.

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 $* : G \times G \to G$ 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.

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 this 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 litte 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:

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

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 1.6. 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 $a * a^{-1} = a^{-1} * a = e$. Also $(a^{-1})^{-1} = a$, 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 $a * \tilde{a}^{-1} = \tilde{a}^{-1} * a = e$, 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 are not simply associative. They have other nice properties as well. 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. Function composition is associative as well. Finally, if $f, g \in F$, then $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$, because:

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

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 F forms a group under function composition. Take $f(x) = x + 1$ and $g(x) = x^3$. Both of these are invertible functions. We also see that $(f \circ g)(x) = x^3 + 1$, while $(g \circ f)(x) = (x + 1)^3$. Therefore F is not an abelian group.

♠   Finally, to get a little more 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. 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 this 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: 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 2. This might seem a strange thing to consider. But now we ask ourselves: how we can transform this triangle so that it lands back
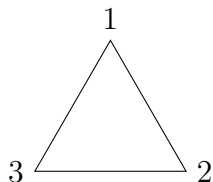
Figure 2

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.
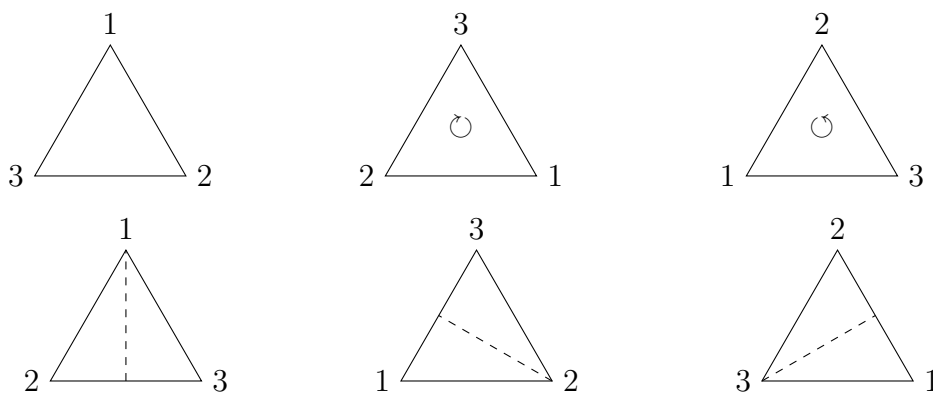

Figure 3: The six symmetries of an equilateral triangle.

From left to right and top to bottom as shown in Figure 3, 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 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. The composition of bijections from a set to itself is associative, so composition of transformations is associative. Therefore this set is a group under composition. We'll call this group D_3, the **dihedral group on 3 vertices**.

Last but not least, the Cayley table for D_3 is shown in Figure 4. Notice that this group is nonabelian, as promised! This group has many interesting symmetries, and will serve as our prototypical example of a nonabelian group.

$\circ$	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 4: Cayley table for D_3.

2   Subgroups and Cosets

From here on out, we'll use multiplicative notation exclusively 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 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 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. This is called the **improper subgroup** of G.

Example 2.5. Take the set $\{\ldots, -8, -4, 0, 4, 8, \ldots\} \subseteq \mathbb{Z}$ 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 4, 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 a 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. We have:

$$0 + 4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$1 + 4\mathbb{Z} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$2 + 4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$3 + 4\mathbb{Z} = \{\ldots, -5, -1, 3, 5, 11, \ldots\}$$

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, $-6 + 4\mathbb{Z} = \{\ldots, -14, -10, -6, -2, 2, 6, 10, \ldots\} = 2 + 4\mathbb{Z}$. 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:

$$eH = \{e, \mu_1\}$$
$$\rho_1 H = \{\rho_1, \mu_2\}$$
$$\rho_2 H = \{\rho_2, \mu_3\}$$

We can also verify (using the Cayley table in Figure 4) 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 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 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 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. Also, from this we immediately have the following.

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

Proof. First, we immediately see that $eH = \{eh \mid h \in H\} = H$. 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 y 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, it's a **finite group**, and has **infinite order** otherwise.

♠ **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 $n|H|$ counts each element of G exactly once. Therefore

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

11

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

■

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

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

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:

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

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

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

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

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 4.2. 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 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. There's in fact a stricter kind of structure-preserving map between groups, described in the definition below.

Definition 4.3. 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 4.4. 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 4.5. 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. ∎

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 maps 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 $bh_2 \in bH$,

$$(aH)(bH) = (ah_1 H)(bh_2 H) = (ab)H = (ah_1 bh_2)H.$$

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:

$$(Ha^{-1})(Hx) = (Ha^{-1})(Ha)$$
$$H(a^{-1}x) = H$$

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 $h_1 b = bh_3$ for some $h_3 \in H$. Therefore, $a(h_1 b) h_2 = abh_3 h_2$. So we have:

$$(ah_1 H)(bh_2 H) = (ah_1 bh_2 H)$$
$$= ab(h_3 h_2) H$$
$$= abH$$

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

∎

Well, you might wonder what the point of defining an operation on the cosets of a group 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 5.2. 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:

$$(aN)[(bN)(cN)] = aN(bcN) = a(bc)N = (ab)cN$$
$$= (abN)cN = [(aN)(bN)] cN,$$

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

∎

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

Theorem 5.3. 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.

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 $\phi(a) = \mu(\gamma(a))$ for all $a \in G$.

Proof. By Theorem 4.5, 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 $a \in^{-1} \ker(\phi) = K$. 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 $\mu(\gamma(a)) = \mu(aK) = \phi(a)$, 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 $\lambda(\phi(a)) = \phi(a)$ trivially as an injective homomorphism between $\phi(G)$ and G'. So we can "factor" ϕ completely as:

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