The First Isomorphism Theorem

- Let \( H \triangleleft G \), and let \( \phi : G \to K \) be a group homomorphism such that \( H \subseteq \ker \phi \). The **Universal Property of the Quotient** states that there is a unique homomorphism \( \hat{\phi} : G/H \to K \) such that \( \hat{\phi} \cdot \pi = \phi \), where \( \pi : G \to G/H \) is the quotient map.

- If \( f : G \to H \) is a group map, the **First Isomorphism Theorem** states that \( G/\ker f \cong \text{im } f \).

Let \( H \triangleleft G \). Then \( G/H \) becomes a group under coset multiplication. Define the **quotient map** (or **canonical projection**) \( \pi : G \to G/H \) by

\[
\pi(g) = gH.
\]

**Lemma.** If \( H \triangleleft G \), the quotient map \( \pi : G \to G/H \) is a surjective homomorphism with kernel \( H \).

**Proof.** If \( a, b \in G \), then

\[
\pi(ab) = (ab)H = aH \cdot bH = \pi(a)\pi(b).
\]

Therefore, \( \pi \) is a group map.

Obviously, if \( gH \in G/H \), then \( \pi(g) = gH \). Hence, \( \pi \) is surjective.

Finally, I’ll show that \( \ker \pi = H \). If \( h \in H \), then \( \pi(h) = hH = H \), and \( H \) is the identity in \( G/H \). Therefore, \( h \in \ker \pi \), i.e. \( H \subseteq \ker \pi \).

Conversely, suppose \( g \in \ker \pi \). Then \( \pi(g) = H \), so \( gH = H \), so \( g \in H \). Therefore, \( \ker \pi \subseteq H \), and hence \( H = \ker \pi \). \( \square \)

The preceding lemma shows that **every normal subgroup is the kernel of a homomorphism**: If \( H \) is a normal subgroup of \( G \), then \( H = \ker \pi \), where \( \pi : G \to G/H \) is the quotient map. On the other hand, the kernel of a homomorphism is a normal subgroup. Hence:

- Normal subgroups are exactly the kernels of group homomorphisms.

Normality was defined with the idea of imposing a condition on subgroups which would make the set of cosets into a group. Now an apparently independent notion — that of a homomorphism — gives rise to the same idea! This strongly suggests that the definition of a normal subgroup was a good one.

You can think of quotient groups in an even more subtle way. The general theme is something like this. In modern mathematics, it is important to study not only objects — like groups — but the maps between objects — in this case, group homomorphisms. The maps, after all, describe the relationships between different objects. (This theme is elaborated in a branch of mathematics called **category theory**.)

It turns out that more is true. In a sense, the maps carry all of the information about the objects; one could even be perverse and “build up” objects out of maps! I won’t go to such extremes, but in some cases, an object can be characterized by certain maps. Here’s an important example.

**Theorem.** (**Universal Property of the Quotient**) Let \( H \triangleleft G \), and let \( \phi : G \to K \) be a group homomorphism such that \( H \subseteq \ker \phi \). Then there is a unique homomorphism \( \hat{\phi} : G/H \to K \) such that the following diagram commutes:

\[
\begin{array}{ccc}
G & \xrightarrow{\pi} & G/H \\
\downarrow{\phi} & & \downarrow{\hat{\phi}} \\
 & & K
\end{array}
\]

(To say that the diagram commutes means that \( \hat{\phi} \cdot \pi = \phi \).)
**Proof.** Define \( \tilde{\phi} : G/H \to K \) by
\[
\tilde{\phi}(gH) = \phi(g).
\]
This is forced by the requirement that \( \tilde{\phi} \pi = \phi \), since plugging \( g \in G \) into both sides yields \( \tilde{\phi}(g) = \phi(g) \), or \( \tilde{\phi}(gH) = \phi(g) \).

I need to check that this map is **well-defined**. The point is that a given coset \( gH \) may in general be written as \( g'H \), where \( g \neq g' \). I must verify that the result \( \phi(g) \) or \( \phi(g') \) is the same regardless of how I write the coset.

(If \( \phi(g) \neq \phi(g') \) in this situation, then a single input — the coset \( gH = g'H \) — produces different outputs, which contradicts what it means to be a function.)

Suppose then that \( gH = g'H \), so \( g = g'h \) for some \( h \in H \).
\[
\tilde{\phi}(gH) = \phi(g) = \phi(g'h) = \phi(g') \phi(h) = \phi(g') \cdot 1 = \phi(g') = \tilde{\phi}(g'H).
\]
This shows that \( \tilde{\phi} \) is indeed well-defined.

I was forced to define \( \tilde{\phi} \) as I did in order to make the diagram commute. Hence, \( \tilde{\phi} \) is unique.

Now I'll show that \( \tilde{\phi} \) is a homomorphism. Let \( a, b \in G \). Then
\[
\tilde{\phi}((ab)H) = \tilde{\phi}((aH)(bH)) = \phi(ab) = \phi(a) \phi(b) = \tilde{\phi}(aH) \tilde{\phi}(bH).
\]

Therefore, \( \tilde{\phi} \) is a homomorphism. \( \Box \)

The universal property of the quotient is an important tool in constructing group maps.

- To define a map out of a quotient group \( G/H \), define a map out of \( G \) which maps \( H \) to \( 1 \).

The map you construct goes from \( G \) to \( G' \); the universal property automatically constructs a map \( G/H \to G' \) for you. The advantage of using the universal property rather than defining a map out of \( G/H \) directly is that you don't repeat the verification that the map is well-defined — it's been done once and for all in the proof above.

Should you ever need to know how the magic map \( \tilde{\phi} \) is defined, refer to the proof (and the commutativity of the diagram).

**Remarks.**

1. Many other constructions are characterized by universal properties. In each case, one finds that the appropriate conditions imply the existence of a unique map with certain properties.

2. The use of diagrams of maps — particularly commutative ones — is pervasive in modern mathematics. They are a powerful language, and another outgrowth of the categorical point of view. In general, one
says a diagram **commutes** if following the “paths” indicated by the arrows (maps) in different ways between two objects produces the same result. For example, to say that

\[
\begin{array}{cccc}
A & \xrightarrow{f} & B \\
\downarrow{g} & & \downarrow{h} \\
C & \xrightarrow{i} & D
\end{array}
\]

commutes means that \( h \cdot f = i \cdot g \). 

---

**Example. (Using the universal property to construct a group map)** To illustrate how the universal property is used, suppose you wanted to construct a homomorphism from the quotient group \( \mathbb{Z} \times \mathbb{Z} / \langle (5, 2) \rangle \) to \( \mathbb{Z} \). How would you do it?

The universal property tells me to construct a group map from \( \mathbb{Z} \times \mathbb{Z} \) to \( \mathbb{Z} \) which contains \( \langle (5, 2) \rangle \) in its kernel — that is, which sends \( \langle (5, 2) \rangle \) to 0. Now \( \langle (5, 2) \rangle \) consists of all multiples of \( (5, 2) \), so what I’m looking for is a group map which sends \( \langle (5, 2) \rangle \) to 0.

To ensure that what I get is a group map, I should probably guess a linear function — something like \( f(x, y) = ax + by \).

If \( f(5, 2) = 0 \), then \( 5a + 2b = 0 \). There is no question of solving this equation for \( a \) and \( b \), since there is one equation and two variables. But I just need *some* \( a \) and \( b \) that work — and one “obvious” way to do this is to set \( a = 2 \) and \( b = -5 \), since

\[
5(2) + 2(-5) = 0.
\]

Notice that \( a = 8, b = -20 \) would work, too. In fact, there are infinitely many possibilities.

So I define \( f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \) by

\[
f(x, y) = 2x - 5y.
\]

It’s easy to check that this is a group map, and I constructed it so that \( \langle (5, 2) \rangle \subset \ker f \). Therefore, the universal property automatically produces a group map \( \tilde{f} : \mathbb{Z} \times \mathbb{Z} / \langle (5, 2) \rangle \to \mathbb{Z} \). It is defined by

\[
\tilde{f} ((x, y) + \langle (5, 2) \rangle) = 2x - 5y.
\]

Why not just define the map this way to begin with? If you did, you’d have to check that the map was well-defined. It’s less messy to use the universal property to construct the map as above.

---

Next, I want to prove a powerful result that you can use to construct isomorphisms of quotient groups. The idea is simple, and uses the universal property of the quotient. First, I’ll prove a very useful lemma.

**Lemma.** Let \( \phi : G \to H \) be a group map. \( \phi \) is injective if and only if \( \ker \phi = \{1\} \).

**Proof.** \((\Rightarrow)\) Suppose \( \phi \) is injective. Since \( \phi(1) = 1 \), \( \{1\} \subset \ker \phi \). Conversely, let \( g \in \ker \phi \), so \( \phi(g) = 1 \). Then \( \phi(g^{-1}) = 1 = \phi(1) \), so by injectivity \( g = 1 \). Therefore, \( \ker \phi \subset \{1\} \), so \( \ker \phi = \{1\} \).

\((\Leftarrow)\) Suppose \( \ker \phi = \{1\} \). I want to show that \( \phi \) is injective. Suppose \( \phi(a) = \phi(b) \). I want to show that \( a = b \).

\[
\phi(a) = \phi(b), \quad \phi(a)\phi(b)^{-1} = 1, \quad \phi(a)\phi(b^{-1}) = 1, \quad \phi(ab^{-1}) = 1.
\]

Hence, \( ab^{-1} \in \ker \phi = \{1\} \), so \( ab^{-1} = 1 \), and \( a = b \). Therefore, \( \phi \) is injective.
Example. (Proving that a group map is injective) Define $f : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$f(x, y) = (3x + 2y, x + y).$$

Prove that $f$ is injective.

As usual, $\mathbb{R}^2$ is a group under vector addition. Since I can write $f$ in the form $f([x \ y]) = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$, $f$ is a linear transformation, so it’s a group map.

To show $f$ is injective, I’ll show that the kernel of $f$ consists of only the identity: $\ker f = \{(0, 0)\}$. Suppose $(x, y) \in \ker f$. Then

$$\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since $\det \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = 1 \neq 0$, I know by linear algebra that the matrix equation has only the trivial solution: $(x, y) = (0, 0)$. This proves that if $(x, y) \in \ker f$, then $(x, y) = (0, 0)$, so $\ker f \subset \{(0, 0)\}$. Since $(0, 0) \in \ker f$, it follows that $\ker f = \{(0, 0)\}$.

Hence, $f$ is injective.  

Theorem. (The First Isomorphism Theorem) Let $\phi : G \to H$ be a group map, and let $\pi : G \to G/\ker \phi$ be the quotient map. There is an isomorphism $\tilde{\phi} : G/\ker \phi \to \text{im } \phi$ such that the following diagram commutes:

$$
\begin{array}{ccc}
G & \xrightarrow{\pi} & G/\ker \phi \\
\downarrow & \nearrow \phi \\
\text{im } \phi & \xrightarrow{\tilde{\phi}} & \text{im } \phi
\end{array}
$$

Proof. Since $\phi$ maps $G$ onto $\text{im } \phi$ and $\ker \phi \subset \ker \phi$, the universal property of the quotient yields a map $\tilde{\phi} : G/\ker \phi \to \text{im } \phi$ such that the diagram above commutes. Since $\phi$ is onto, so is $\tilde{\phi}$; in fact, if $\phi(g) \in \text{im } \phi$, by commutativity $\tilde{\phi}(\pi(g)) = \phi(g)$.

It remains to show that $\tilde{\phi}$ is injective.

By the previous lemma, it suffices to show that $\ker \tilde{\phi} = \{1\}$. Since $\tilde{\phi}$ maps out of $G/\ker \phi$, the “1” here is the identity element of the group $G/\ker \phi$, which is the subgroup $\ker \phi$. So I need to show that $\ker \tilde{\phi} = \{\ker \phi\}$.

However, this follows immediately from commutativity of the diagram. For $g \ker \phi \in \ker \tilde{\phi}$ if and only if $\tilde{\phi}(g \ker \phi) = 1$. This is equivalent to $\tilde{\phi}(\pi(g)) = 1$, or $\phi(g) = 1$, or $g \in \ker \phi$ — i.e. $\ker \tilde{\phi} = \{\ker \phi\}$.  

Example. (Using the First Isomorphism Theorem to show two groups are isomorphic) Use the First Isomorphism Theorem to prove that

$$\frac{\mathbb{R}^*}{\{1, -1\}} \cong \mathbb{R}^+.$$ 

$\mathbb{R}^*$ is the group of nonzero real numbers under multiplication. $\mathbb{R}^+$ is the group of positive real numbers under multiplication. $\{1, -1\}$ is the group consisting of 1 and $-1$ under multiplication (it’s isomorphic to $\mathbb{Z}_2$).
I’ll define a group map from \( \mathbb{R}^* \) onto \( \mathbb{R}^+ \) whose kernel is \( \{1,-1\} \).
Define \( \phi : \mathbb{R}^* \rightarrow \mathbb{R}^+ \) by
\[
\phi(x) = |x|.
\]
Since
\[
\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y),
\]
\( \phi \) is a group map.

If \( z \in \mathbb{R}^+ \) is a positive real number, then
\[
\phi(z) = |z| = z \quad \text{since } z \text{ is positive.}
\]
Therefore, \( \phi \) is surjective: \( \text{im } \phi = \mathbb{R}^+ \).

Finally, \( \phi \) clearly sends 1 and \(-1\) to the identity \( 1 \in \mathbb{R}^+ \), and those are the only two elements of \( \mathbb{R}^* \) which map to 1. Therefore, \( \ker \phi = \{1,-1\} \).

By the First Isomorphism Theorem,
\[
\frac{\mathbb{R}^*}{\{1,-1\}} = \frac{\mathbb{R}^*}{\ker \phi} \approx \text{im } \phi = \mathbb{R}^+.
\]

Note that I didn’t construct a map \( \frac{\mathbb{R}^*}{\{1,-1\}} \rightarrow \mathbb{R}^+ \) explicitly; the First Isomorphism Theorem constructs the isomorphism for me.

**Example.** (Using the First Isomorphism Theorem to show two groups are isomorphic) Prove that
\[
\mathbb{Z} \times \mathbb{Z} / \langle(3,1)\rangle \approx \mathbb{Z}.
\]

First, I need to define a group map \( \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \). I’d like it to be surjective, and I want the kernel to be \( \langle(3,1)\rangle \).

To ensure that the function I define is a group map, I should use a *linear* function. So I’m thinking of something of the form \( f(m,n) = am + bn \).

In order for \( \ker f \) to be \( \langle(3,1)\rangle \), I want to choose \( a \) and \( b \) so that \( f(3,1) = 0 \). This means I want \( a \cdot 3 + b \cdot 1 = 0 \). An easy way to arrange this is to switch the 3 and the 1, then negate one of the numbers (say the 3). This gives \( a = 1 \), \( b = -3 \).

Following this line of thought, I define \( f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \) by
\[
f(m,n) = m - 3n.
\]

First, I’ll show that \( f \) is a group map:
\[
f[(m_1,n_1) + (m_2,n_2)] = f(m_1 + m_2, n_1 + n_2) =
\]
\[
(m_1 + m_2) - 3(n_1 + n_2) = (m_1 - 3n_1) + (m_2 - 3n_2) = f(m_1, n_1) + f(m_2, n_2).
\]

To show that \( \ker f = \langle(3,1)\rangle \), I’ll show that each of these sets is contained in the other. First, I’ll show \( \langle(3,1)\rangle \subset \ker f \). To do this, I’ll take an element of \( \langle(3,1)\rangle \) and show that it’s in \( \ker f \). An element of \( \langle(3,1)\rangle \) has the form \( k \cdot (3,1) \) for some \( k \in \mathbb{Z} \), and to be in \( \ker f \) means that \( f \) maps the element to 0. So I do the computation:
\[
f[k \cdot (3,1)] = f(3k,k) = 3k - 3k = 0.
\]
This proves that \( k \cdot (3,1) \in \ker f \). Hence, \( \langle(3,1)\rangle \subset \ker f \).
To show that \( \ker f \subset \langle (3, 1) \rangle \), I take an element in \( \ker f \) and show that it’s in \( \langle (3, 1) \rangle \). Suppose that \((m, n) \in \ker f \). Then \( f(m, n) = 0 \), so \( m - 3n = 0 \), or \( m = 3n \). Then
\[
(m, n) = (3n, n) = n \cdot (3, 1) \in \langle (3, 1) \rangle.
\]
Thus, \( \ker f \subset \langle (3, 1) \rangle \), so \( \ker f = \langle (3, 1) \rangle \).

Next, I have to show that \( f \) is surjective, i.e. that \( \text{im} f = \mathbb{Z} \). To do this, I take an arbitrary element \( p \in \mathbb{Z} \) and find an input \((m, n)\) such that \( f(m, n) = p \). In this situation, you’re trying to “solve” for \( m \) and \( n \) in terms of \( p \), but there are usually many \((m, n)\)’s which will work.

Now \( f(m, n) = m - 3n \), so this will equal \( p \) if \( m = p \) and \( n = 0 \). In other words, \( f(p, 0) = p \). Hence, \( \text{im} f = \mathbb{Z} \).

Hence, the First Isomorphism Theorem says that
\[
\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (3, 1) \rangle} \cong \mathbb{Z}.
\]

Here’s what this means pictorially. A coset of \( \langle (3, 1) \rangle \) in \( \mathbb{Z} \times \mathbb{Z} \) consists of the lattice points on the line \( y = \frac{1}{3}x + \frac{1}{3}n \). The isomorphism essentially maps this coset to the \( x \)-intercept \( -n \in \mathbb{Z} \).

For example, consider the point \((2, 1) \in \mathbb{Z} \times \mathbb{Z} \). Since
\[
(2, 1) - (3, 1) = (-1, 0),
\]
\((2, 1)\) and \((-1, 0)\) are in the same coset of \( \langle (3, 1) \rangle \).

What is the line through \((2, 1)\) and \((-1, 0)\)? It has slope \( \frac{1}{3} \), so its equation is
\[
y = \frac{1}{3}(x + 1) = \frac{1}{3}x + \frac{1}{3}.
\]
The \( x \)-intercept is \(-1 \) — and sure enough,
\[
f(2, 1) = 2 - 3 \cdot 1 = -1. \quad \Box
\]

**Lemma.** If \( \phi : G \rightarrow H \) is a surjective group map and \( K \triangleleft G \), then \( \phi(K) \triangleleft H \).

**Proof.** \( 1 \in K \), so \( 1 = \phi(1) \in \phi(K) \), and \( \phi(K) \neq \emptyset \).
Let \( a, b \in K \), so \( \phi(a), \phi(b) \in \phi(K) \). Then
\[
\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(K), \text{ since } ab^{-1} \in K.
\]

Therefore, \( \phi(K) \) is a subgroup.

(Notice that this does not use the fact that \( K \) is normal. Hence, I’ve actually proved that the image of a subgroup is a subgroup.)

Now let \( h \in H, a \in K \), so \( \phi(a) \in \phi(K) \). I want to show that \( h\phi(a)h^{-1} \in \phi(K) \). Since \( \phi \) is surjective, \( h = \phi(g) \) for some \( g \in G \). Then
\[
h\phi(a)h^{-1} = \phi(g)\phi(a)\phi(g)^{-1} = \phi(gag^{-1}).
\]

But \( gag^{-1} \in K \) because \( K \) is normal. Hence, \( \phi(gag^{-1}) \in \phi(K) \). It follows that \( \phi(K) \) is a normal subgroup of \( H \). \( \square \)

**Theorem. (The Second Isomorphism Theorem)** Let \( K, H \trianglelefteq G, K < H \). Then
\[
\frac{G}{K} \cong \frac{G}{H} \cdot \frac{H}{K}.
\]

**Proof.** I’ll use the First Isomorphism Theorem. To do this, I need to define a group map \( \frac{G}{K} \to \frac{G}{H} \).

To define this group map, I’ll use the Universal Property of the Quotient.

The quotient map \( \pi : G \to \frac{G}{H} \) is a group map. By the lemma preceding the Universal Property of the Quotient, \( H = \ker \pi \). Since \( K \subseteq H \), it follows that \( K \subseteq \ker \pi \).

Since \( \pi : G \to \frac{G}{H} \) is a group map and \( K \subseteq \ker \pi \), the Universal Property of the Quotient implies that there is a group map \( \tilde{\pi} : \frac{G}{K} \to \frac{G}{H} \) given by
\[
\tilde{\pi}(gK) = gH.
\]

If \( gH \in \frac{G}{H} \), then \( \tilde{\pi}(gK) = gH \). Therefore, \( \tilde{\pi} \) is surjective.

I claim that \( \ker \tilde{\pi} = \frac{H}{K} \).

First, if \( hK \in \frac{H}{K} \) (so \( h \in H \)), then \( \tilde{\pi}(hK) = hH = H \). Since \( H \) is the identity in \( \frac{G}{H} \), it follows that \( hK \in \ker \tilde{\pi} \).

Conversely, suppose \( gK \in \ker \tilde{\pi} \), so
\[
\tilde{\pi}(gK) = H, \quad \text{or} \quad gH = H.
\]

The last equation implies that \( g \in H \), so \( gK \in \frac{H}{K} \).

Thus, \( \ker \tilde{\pi} = \frac{H}{K} \).

By the First Isomorphism Theorem,
\[
\frac{G}{K} \frac{H}{K} \cong \frac{G}{\ker \tilde{\pi}} \approx \text{im} \tilde{\pi} = \frac{G}{H}. \quad \square
\]

There is also a Third Isomorphism Theorem (sometimes called the Modular Isomorphism, or the Noether Isomorphism). It asserts that if \( H < G \) and \( K \trianglelefteq G \), then
\[
\frac{H}{H \cap K} \cong \frac{HK}{K}.
\]

You can prove it using the First Isomorphism Theorem, in a manner similar to that used in the proof of the Second Isomorphism Theorem.