3-22-2018

The First Isomorphism Theorem

The **First Isomorphism Theorem** helps identify quotient groups as "known" or "familiar" groups. I'll begin by proving a useful lemma.

Proposition. Let $\phi : G \to H$ be a group map. ϕ is injective if and only if $\ker \phi = \{1\}$.

Proof. $(\to)$ Suppose ϕ is injective. Since $\phi(1) = 1$, $\{1\} \subset \ker \phi$. Conversely, let $g \in \ker \phi$, so $\phi(g) = 1$. Then $\phi(g) = 1 = \phi(1)$, so by injectivity $g = 1$. Therefore, $\ker \phi \subset \{1\}$, so $\ker \phi = \{1\}$.

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

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

Hence, $ab^{-1} \in \ker \phi = \{1\}$, so $ab^{-1} = 1$, and $a = b$. Therefore, ϕ is injective. $\square$

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. I can write f in the form

$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Since f has been represented as multiplication by a constant matrix, it 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. $\square$

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 $\tilde{\phi} : G/\ker \phi \to \operatorname{im} \phi$ such that the following diagram commutes:

$$\begin{array}{ccc} G & & \\ {\scriptstyle \pi}\downarrow & \searrow {\scriptstyle \phi} & \\ G/\ker \phi & \underset{\tilde{\phi}}{\longrightarrow} & \operatorname{im}\ \phi \end{array}$$

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

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

$\mathbb{R}^*$ 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 $\phi : \mathbb{R}^* \to \mathbb{R}^+$ by

$$\phi(x) = |x|.$$

ϕ is a group map:

$$\phi(xy) = |xy| = |x||y| = \phi(x)\phi(y).$$

If $z \in \mathbb{R}^+$ is a positive real number, then

$$\phi(z) = |z| = z.$$

Therefore, ϕ is surjective: $\operatorname{im}\phi = \mathbb{R}^+$.

Finally, ϕ 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,

$$\frac{\mathbb{R}^*}{\{1,-1\}} = \frac{\mathbb{R}^*}{\ker\phi} \approx \operatorname{im}\phi = \mathbb{R}^+.$$

Note that I didn't construct a map $\dfrac{\mathbb{R}^*}{\{1,-1\}} \to \mathbb{R}^+$ explicitly; the First Isomorphism Theorem constructs the isomorphism for me. □

Example. $\mathbb{R}^2$ is a group under componentwise addition and $\mathbb{R}$ is a group under addition. Let

$$H = \left\{ x \cdot (\sqrt{5}, -\pi) \;\middle|\; x \in \mathbb{R} \right\}.$$

Prove that $\dfrac{\mathbb{R}^2}{H} \approx \mathbb{R}$.

Define $f : \mathbb{R}^2 \to \mathbb{R}$ by

$$f(x, y) = \pi x + \sqrt{5} y.$$

Note that

$$f\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} \pi & \sqrt{5} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Since f can be expressed as multiplication by a constant matrix, it's a linear transformation, and hence a group map.

Let $x \cdot (\sqrt{5}, -\pi) \in H$. Then

$$f[x \cdot (\sqrt{5}, -\pi)] = f(\sqrt{5}x, -\pi x) = \pi(\sqrt{5}x) + \sqrt{5}(-\pi x) = 0.$$

Therefore, $x \cdot (\sqrt{5}, -\pi) \in \ker f$, and hence $H \subset \ker f$.

Let $(x, y) \in \ker f$. Then

$$\begin{aligned} f(x, y) &= 0 \\ \pi x + \sqrt{5} y &= 0 \\ \sqrt{5} y &= -\pi x \\ y &= -\frac{\pi}{\sqrt{5}} x \end{aligned}$$

Hence,

$$(x, y) = \left(x, -\frac{\pi}{\sqrt{5}} x\right) = \frac{1}{\sqrt{5}} x \cdot (\sqrt{5}, -\pi) \in H.$$

Therefore, $\ker f \subset H$. Hence, $\ker f = H$.

Let $z \in \mathbb{R}$. Note that

$$f\left(\frac{1}{\pi} z, 0\right) = \pi \cdot \frac{1}{\pi} z + \sqrt{5} \cdot 0 = z.$$

Hence, $\operatorname{im} f = \mathbb{R}$.

Thus,

$$\frac{\mathbb{R}^2}{H} = \frac{\mathbb{R}^2}{\ker f} \approx \operatorname{im} f = \mathbb{R}. \quad \square$$

Example. $\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise addition and $\mathbb{Z}$ is a group under addition. Prove that

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (12, 17) \rangle} \approx \mathbb{Z}.$$

Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$f(x, y) = 17x - 12y.$$

f can be represented by matrix multiplication:

$$\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 17 & -12 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Hence, it's a group map.

Let $n(12, 17) = (12n, 17n) \in \langle (12, 17) \rangle$. Then

$$f((12n, 17n) = 17(12n) - 12(17n) = 0.$$

Thus, $\langle (12, 17) \rangle \subset \ker f$.

Let $(x,y) \in \ker f$. Then

$$\begin{aligned} f(x,y) &= 0 \\ 17x - 12y &= 0 \\ 17x &= 12y \end{aligned}$$

Now $17 \mid 12y$ but $(12,17) = 1$. By Euclid's lemma, $17 \mid y$. Say $y = 17n$. Then

$$17x = 12(17n), \quad \text{so} \quad x = 12n.$$

Therefore,

$$(x,y) = (12n, 17n) = n(12,17) \in \langle (12,17) \rangle.$$

Thus, $\ker f \subset \langle (12,17) \rangle$.
Hence, $\langle (12,17) \rangle = \ker f$.
Let $z \in \mathbb{Z}$. Note that

$$1 = (17, -12) = 5 \cdot 17 + 7 \cdot (-12).$$

Multiplying by z, I get

$$z = 17(5z) - 12(7z).$$

Then

$$f(5z, 7z) = 17(5z) - 12(7z) = z.$$

This proves that $\operatorname{im} f = \mathbb{Z}$.
Hence,

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\langle (12,17) \rangle} = \frac{\mathbb{Z} \times \mathbb{Z}}{\ker f} \approx \operatorname{im} f = \mathbb{Z}. \quad \square$$

Example. $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ is a group under componentwise addition. Consider the subgroup

$$H = \left\{ x \cdot (1,2,3) \;\middle|\; x \in \mathbb{R} \right\}.$$

Prove that $\dfrac{\mathbb{R} \times \mathbb{R} \times \mathbb{R}}{H} \approx \mathbb{R} \times \mathbb{R}$.

($\mathbb{R} \times \mathbb{R}$ is a group under componentwise addition.)

Define $f : \mathbb{R} \times \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by

$$f(x,y,z) = (y - 2x, z - 3x).$$

Note that

$$f\left(\begin{bmatrix} x \\ y \\ z \end{bmatrix} \right) = \begin{bmatrix} -2 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}.$$

Since f is defined by matrix multiplication, it is a linear transformation. Hence, it's a group map.
Let $x \cdot (1,2,3) = (x, 2x, 3x) \in H$. Then

$$f(x, 2x, 3x) = (2x - 2x, 3x - 3x) = (0,0).$$

Hence, $(x, 2x, 3x) \in \ker f$, and $H \subset \ker f$.
Let $(x,y,z) \in \ker f$. Then

$$\begin{aligned} f(x,y,z) &= (0,0) \\ (y - 2x, z - 3x) &= (0,0) \end{aligned}$$

Equating the first components, I have $y - 2x = 0$, so $y = 2x$. Equating the second components, I have $z - 3x = 0$, so $z = 3x$. Thus,

$$(x, y, z) = (x, 2x, 3x) \in H.$$

Therefore, $\ker f \subset H$, and so $H = \ker f$.

Let $(a, b) \in \mathbb{R} \times \mathbb{R}$. Then

$$f(0, a, b) = (a - 2 \cdot 0, b - 3 \cdot 0) = (a, b).$$

Hence, $\operatorname{im} f = \mathbb{R} \times \mathbb{R}$.

Thus,

$$\frac{\mathbb{R} \times \mathbb{R} \times \mathbb{R}}{H} = \frac{\mathbb{R} \times \mathbb{R} \times \mathbb{R}}{\ker f} \approx \operatorname{im} f = \mathbb{R} \times \mathbb{R}.$$

The first equality follows from $H = \ker f$. The isomorphism follows from the First Isomorphism Theorem. The second equality follows from $\operatorname{im} f = \mathbb{R} \times \mathbb{R}$. □

Proposition. If $\phi : G \to H$ is a surjective group map and $K \lhd G$, then $\phi(K) \lhd H$.

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 ϕ is surjective, $h = \phi(g)$ for some $g \in G$. Then

$$h\phi(a)h^{-1} = \phi(g)\phi(a)\phi(g)^{-1} = \phi\left(gag^{-1}\right).$$

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

Theorem. (**The Second Isomorphism Theorem**) Let $K, H \lhd G$, $K < H$. Then

$$\frac{\dfrac{G}{K}}{\dfrac{H}{K}} \approx \frac{G}{H}.$$

Proof. I'll use the First Isomorphism Theorem. To do this, I need to define a group map $\dfrac{G}{K} \to \dfrac{G}{H}$.

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

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

Since $\pi : G \to \dfrac{G}{H}$ is a group map and $K \subset \ker \pi$, the Universal Property of the Quotient implies that there is a group map $\tilde{\pi} : \dfrac{G}{K} \to \dfrac{G}{H}$ given by

$$\tilde{\pi}(gK) = gH.$$

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

I claim that $\ker \tilde{\pi} = \dfrac{H}{K}$.

First, if $hK \in \dfrac{H}{K}$ (so $h \in H$), then $\tilde{\pi}(hK) = hH = H$. Since H is the identity in $\dfrac{G}{H}$, 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 $gK \in \dfrac{H}{K}$.

Thus, $\ker \tilde{\pi} = \dfrac{H}{K}$.

By the First Isomorphism Theorem,

$$\frac{\dfrac{G}{K}}{\dfrac{H}{K}} = \frac{\dfrac{G}{K}}{\ker \tilde{\pi}} \approx \operatorname{im} \tilde{\pi} = \frac{G}{H}. \quad \square$$

There is also a **Third Isomorphism Theorem** (sometimes called the **Modular Isomorphism**, or the **Noether Isomorphism**). It asserts that if $H < G$ and $K \lhd G$, then

$$\frac{H}{H \cap K} \approx \frac{HK}{K}.$$

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