The First Isomorphism Theorem

R. C. Daileda

Let G be a group. For any $H < G$, the "reduction mod H" map

$$\begin{aligned} \pi : G &\to G/H, \\ a &\mapsto aH, \end{aligned}$$

which sends each element of G to its coset in G/H is called the *natural surjection.* When $H \triangleleft G$, we have

$$\pi(ab) = (ab)H = (aH)(bH) = \pi(a)\pi(b),$$

for all $a, b \in G$. This means that π is actually a surjective *homomorphism* in this case, which we call the *natural epimorphism.* Since H is the identity coset in G/H, notice that $a \in \ker \pi$ if and only if

$$aH = \pi(a) = H \iff a \in H.$$

Thus

$$\ker \pi = H.$$

That is, every normal subgroup of G is the kernel of a homomorphism with domain G. The converse is also true.

Lemma 1. *Let $f : G \to G'$ be a homomorphism of groups. Then* $\ker f \triangleleft G$.

Proof. Let $x \in G$ and let $a \in \ker f$. Then $f(a) = e'$ is the identity in G' so that

$$f(xax^{-1}) = f(x)f(a)f(x)^{-1} = f(x)e'f(x)^{-1} = f(x)f(x)^{-1} = e',$$

which shows that $xax^{-1} \in \ker f$. Since $a \in \ker f$ was arbitrary, this proves

$$x(\ker f)x^{-1} \subseteq \ker f.$$

And since $x \in G$ was arbitrary this proves $\ker f \triangleleft G$. □

Given a group G and a subgroup H, Lemma 1 provides perhaps the easiest way to show that H is normal in G: simply identify H as the kernel of a homomorphism $f : G \to G'$.

There is actually a deeper connection between normal subgroups and kernels. Let $f : G \to G'$ be a group homomorphism. We have seen that f is injective if and only if $\ker f$ is trivial. Until now this is the only real utility we've found for the kernel of a homomorphism. But when $\ker f$ is nontrivial it actually provides a precise measurement of the failure of the injectivity of f.

To see why, for $a, b \in G$ we define $a \sim b$ if and only if $f(a) = f(b)$. It is an easy exercise to see that $\sim$ is an equivalence relation on G (indeed, on the domain of any function between two sets). Since

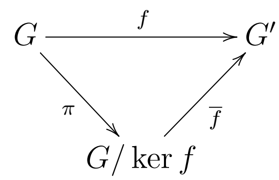
$$f(a) = f(b) \quad \Leftrightarrow \quad e = f(b)^{-1} f(a) = f(b^{-1} a) \quad \Leftrightarrow \quad b^{-1} a \in \ker f \quad \Leftrightarrow \quad a \equiv b \pmod{\ker f},$$

the relation $\sim$ is just congruence modulo $\ker f$. So the equivalence class of $a \in G$ under $\sim$ is just the coset $a(\ker f)$:

$$a(\ker f) = \{b \in G \mid f(b) = f(a)\}. \tag{1}$$

Because the equivalence classes in $G/\sim$ group elements according to their value under f, there is a natural bijection $G/\sim \to \operatorname{im} f$ which sends the class of a to $f(a)$. But (1) shows that $G/\sim = G/\ker f$, which brings us to:

Theorem 1 (First Isomorphism Theorem)**.** *Let $f : G \to G'$ be a homomorphism of groups. The rule $\overline{f}(a \ker f) = f(a)$ yields a well-defined monomorphism $\overline{f} : G/\ker f \to G'$. If $\pi : G \to G/\ker f$ is the natural epimorphism, then $\overline{f}$ is the unique homomorphism so that the diagram*



is commutative, i.e. so that $f = \overline{f} \circ \pi$.

Proof. Equation (1) shows that $f(a) = f(b)$ if and only if $a(\ker f) = b(\ker f)$, so that $\overline{f}$ is well-defined. It is a homomorphism since

$$\overline{f}((a \ker f)(b \ker f)) = \overline{f}((ab) \ker f) = f(ab) = f(a) f(b) = \overline{f}(a \ker f) \overline{f}(b \ker f).$$

And it is injective since

$$\overline{f}(a \ker f) = e' \quad \Leftrightarrow \quad f(a) = e' \quad \Leftrightarrow \quad a \in \ker f \quad \Leftrightarrow \quad a \ker f = \ker f,$$

which shows that $\ker \overline{f}$ is the trivial subgroup of $G/\ker f$. Finally, for any $a \in G$ we have

$$(\overline{f} \circ \pi)(a) = \overline{f}(\pi(a)) = \overline{f}(a \ker f) = f(a),$$

so that $\overline{f} \circ \pi = f$. If $g : G/\ker f \to G'$ is any other map so that $g \circ \pi = f$, then for any $a \ker f \in G/\ker f$,

$$g(a \ker f) = g(\pi(a)) = (g \circ \pi)(a) = f(a) = \overline{f}(a \ker f) \quad \Rightarrow \quad g = \overline{f}.$$

□

Corollary 1. *Let $f : G \to G'$ be a homomorphism of groups. Then the induced map $\overline{f}$ of Theorem 1 yields an isomorphism*

$$G/\ker f \cong \operatorname{im} f.$$

Proof. Every monomorphism is an isomorphism between its domain and its image. Since $\operatorname{im} f = \operatorname{im} \overline{f}$ by construction, the result follows from Theorem 1. $\square$

Corollary 1 and the discussion leading up to Lemma 1 show that the quotients of a group G correspond directly with its homomorphic images. So in some sense all of the information needed to construct homomorphisms *out of* a group G is already contained *inside* G!

The First Isomorphism Theorem is a powerful tool for constructing homomorphisms out of quotient groups. As such, it provides one of the most efficient means of identifying quotient groups (up to isomorphism).

Example 1. Let $f : \mathbb{R} \to S^1$ be given by $f(x) = e^{2\pi i x} = \cos(2\pi x) + i \sin(2\pi x)$. Then f is an epimorphism (additive to multiplicative) since

$$f(x + y) = e^{2\pi i(x+y)} = e^{2\pi i x + 2\pi i y} = e^{2\pi i x} e^{2\pi i y} = f(x)f(y)$$

for all $x, y \in \mathbb{R}$. And for any $z = e^{i\theta} \in S^1$, if $x = \frac{\theta}{2\pi} \in \mathbb{R}$, then $f(x) = e^{2\pi i \cdot \frac{\theta}{2\pi}} = e^{i\theta} = z$. We see that $x \in \ker f$ if and only if $f(x) = e^{2\pi i x} = 1$ if and only if $2\pi x \in 2\pi\mathbb{Z}$ if and only if $x \in \mathbb{Z}$. Therefore, by the first isomorphism theorem

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

Intuitively speaking, this says that if we start with the real line, and then identify all of the integers to a single point, the resulting quotient space is a circle.

Example 2. Let $n \in \mathbb{N}$ and define $f : S^1 \to S^1$ by $f(z) = z^n$. Then for any $z, w \in S^1$ we have

$$f(zw) = (zw)^n = z^n w^n = f(z)f(w),$$

since S^1 is abelian. The map f is also surjective. Given $w \in S^1$, write $w = e^{i\theta}$. Then $z = e^{i\theta/n} \in S^1$ and $f(z) = (e^{i\theta/n})^n = e^{i\theta} = w$. And $z \in \ker f$ if and only if $f(z) = z^n = 1$, which means that $z \in \boldsymbol{\mu}_n$, the group of nth roots of unity. So by the First Isomorphism Theorem we have

$$S^1/\boldsymbol{\mu}_n \cong S_1.$$

Example 3. Define $f : \mathbb{C}^\times \to S^1$ by $f(z) = z/|z|$. This is a homomorphism since

$$f(zw) = \frac{zw}{|zw|} = \frac{zw}{|z|\,|w|} = \frac{z}{|z|}\frac{w}{|w|} = f(z)f(w)$$

for all $z, w \in \mathbb{C}^\times$. It is surjective since for any $z \in S^1$ we have $z \in \mathbb{C}^\times$ and

$$f(z) = \frac{z}{|z|} = \frac{z}{1} = z.$$

The kernel of f consists of those $z \in \mathbb{C}^\times$ for which $f(z) = z/|z| = 1$ or, equivalently, $z = |z| \neq 0$. This certainly implies that $z \in \mathbb{R}^+$. Conversely, if $z \in \mathbb{R}^+$, then $z = |z|$ and consequently $f(z) = 1$. The First Isomorphism Theorem then tells us that

$$\mathbb{C}^\times/\mathbb{R}^+ \cong S^1.$$

Example 4. Now define $g : \mathbb{C}^\times \to \mathbb{R}^+$ by $g(z) = |z|$. This is a homomorphism since

$$g(zw) = |zw| = |z|\,|w| = g(z)g(w)$$

for any $z, w \in \mathbb{C}^\times$. It is surjective since given any $x \in \mathbb{R}^+$, one has $x \in \mathbb{C}^\times$ and $g(x) = |x| = x$. And $z \in \ker g$ if and only if $g(z) = |z| = 1$ if and only if $z \in S^1$. So this time the First Isomorphism Theorem tells us that

$$\mathbb{C}^\times / S^1 \cong \mathbb{R}^+.$$

Example 5. Let's put the preceding two examples together. Define $(f \times g) : \mathbb{C}^\times \to S^1 \times \mathbb{R}^+$ by $(f \times g)(z) = (f(z), g(z))$. The reader can check that $f \times g$ is a homomorphism. It is surjective since if we are given any $(z, x) \in S^1 \times \mathbb{R}^+$, then $xz \in \mathbb{C}^\times$ and

$$(f \times g)(xz) = \left(\frac{xz}{|xz|}, |xz|\right) = \left(\frac{xz}{|x|\,|z|}, |x|\,|z|\right) = \left(\frac{xz}{x \cdot 1}, x \cdot 1\right) = (z, x).$$

Finally, $z \in \ker(f \times g)$ if and only if $(f \times g)(z) = (f(z), g(z)) = (1, 1)$. This is equivalent to

$$z \in \ker f \cap \ker g = \mathbb{R}^+ \cap S^1 = \{1\},$$

since the only positive real number on the unit circle is 1. So $\ker(f \times g)$ is trivial and we obtain

$$\mathbb{C}^\times \cong S^1 \times \mathbb{R}^+,$$

by the First Isomorphism Theorem. This provides an algebraic proof of the existence and uniqueness of polar decompositions $z = re^{i\theta}$ of complex numbers: $r = |z|$ and $e^{i\theta} = z/|z|$.

Example 6. Let A be an additive abelian group and let $B, C < A$. The inclusion maps $\iota_B : B \to A$ and $\iota_C : C \to A$ given by $\iota_B(b) = b$ and $\iota_C(c) = c$ are clearly homomorphisms. It follows that their sum $\iota_B \oplus \iota_C : B \times C \to A$, which is given by $(\iota_B \oplus \iota_C)(b, c) = \iota_B(b) + \iota_C(c)$, is also a homomorphism. Its image is clearly the subgroup $B + C < A$. And $(b, c) \in \ker(\iota_B \oplus \iota_C)$ if and only if $(\iota_B \oplus \iota_C)(b, c) = b + c = 0$. This implies $-c = b \in B$, so that $c \in B \cap C$ and hence $b \in B \cap C$. Conversely, if $b \in B \cap C$ then $(b, -b) \in B \times C$ and $(\iota_B \oplus \iota_C)(b, -b) = b - b = 0$. Hence

$$\ker(\iota_B \oplus \iota_C) = \{(b, -b) \mid b \in B \cap C\} \cong B \cap C,$$

and the First Isomorphism Theorem gives

$$(B \times C)/\{(b, -b) \mid b \in B \cap C\} \cong B + C.$$

We see immediately that the internal sum $B + C$ is direct, so that $B + C = B \oplus C \cong B \times C$, if and only if $B \cap C = \{0\}$, a result we have derived earlier.

Example 7 (The Chinese Remainder Theorem)**.** For any $m \in \mathbb{N}$, we have the natural epimorphism $\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by $\pi_m(k) = k + m\mathbb{Z}$. So if we are given another

$n \in \mathbb{N}$, we can construct the product map $(\pi_m \times \pi_n) : \mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$, which is defined by $(\pi_m \times \pi_n)(k) = (\pi_m(k), \pi_n(k))$. We see that $k \in \ker(\pi_m \times \pi_n)$ if and only if $(k + m\mathbb{Z}, k + n\mathbb{Z}) = (m\mathbb{Z}, n\mathbb{Z})$. This holds if and only if $k \in m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{lcm}(m,n)\mathbb{Z}$. The First Isomorphism Theorem therefore yields

$$\mathbb{Z}/\operatorname{lcm}(m,n)\mathbb{Z} \cong \operatorname{im}(\pi_m \times \pi_n). \tag{2}$$

Therefore

$$|\operatorname{im}(\pi_m \times \pi_n)| = |\mathbb{Z}/\operatorname{lcm}(m,n)\mathbb{Z}| = \operatorname{lcm}(m,n).$$

Because the codomain of $\pi_m \times \pi_n$ is finite, the Pigeonhole Principle implies that $\pi_m \times \pi_n$ is surjective if and only if

$$mn = |(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})| = |\operatorname{im}(\pi_m \times \pi_n)| = \operatorname{lcm}(m,n).$$

Since $mn = \gcd(m,n)\operatorname{lcm}(m,n)$, this condition is equivalent to $\gcd(m,n) = 1$. In this case (2) becomes

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}), \tag{3}$$

the isomorphism being given by $k + mn\mathbb{Z} \mapsto (k + m\mathbb{Z}, k + n\mathbb{Z})$.

The isomorphism (3) is an algebraic version of what is more commonly known as the *Chinese Remainder Theorem* (CRT). It tells us that if m and n are relatively prime, then for any $a, b \in \mathbb{Z}$ there exists a solution $x \in \mathbb{Z}$ to the system of simultaneous congruences

$$\begin{aligned} x &\equiv a \pmod{m}, \\ x &\equiv b \pmod{n}, \end{aligned} \tag{4}$$

and that x is unique up to addition of multiples of mn. To see how this follows from (3), notice that if we take $(a + m\mathbb{Z}, b + n\mathbb{Z}) \in (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$, then there is exactly one $x + mn\mathbb{Z} \in \mathbb{Z}/mn\mathbb{Z}$ so that

$$(a + m\mathbb{Z}, b + n\mathbb{Z}) = (\pi_m \times \pi_n)(x + mn\mathbb{Z}) = (x + m\mathbb{Z}, x + n\mathbb{Z}).$$

Example 8 (Classification of Cyclic Groups)**.** Let $G = \langle g \rangle$ be a cyclic group generated by g. Define $f : \mathbb{Z} \to G$ by $f(n) = g^n$. For any $m, n \in \mathbb{Z}$ we have

$$f(m + n) = g^{m+n} = g^m g^n = f(m)f(n),$$

proving that f is a homomorphism which is surjective since every member of G is a power of g. Furthermore

$$\ker f = \{n \in \mathbb{Z} \mid g^n = e\}.$$

If G is infinite, then g must have infinite order so that $g^n = e$ if and only if $n = 0$. This implies $\ker f = \{0\}$ and hence f is an isomorphism. That is, $\mathbb{Z} \cong G$. If $|G| = |g| = m \in \mathbb{N}$, then we know that

$$\ker f = \{n \in \mathbb{Z} \mid g^n = e\} = m\mathbb{Z}.$$

In this case the First Isomorphism Theorem then implies that $\mathbb{Z}/m\mathbb{Z} \cong G$. Thus:

$$G = \langle g \rangle \cong \begin{cases} \mathbb{Z} & \text{if } |g| = \infty, \\ \mathbb{Z}/m\mathbb{Z} & \text{if } |g| = m. \end{cases}$$

This shows that, up to isomorphism, the only cyclic groups are $\mathbb{Z}$ and its quotients, and there is exactly one cyclic group (again, up to isomorphism) of any given order.

Example 9 (Subgroups of Cyclic Groups)**.** Let $G = \langle g \rangle$ be a cyclic group. If G is infinite, the preceding example tells us that $\mathbb{Z} \cong G$, the isomorphism being given by $n \mapsto g^n$. This isomorphism provides a correspondence between the subgroups of G and the subgroups of $\mathbb{Z}$, which we know to have the form $m\mathbb{Z}$ for $m \in \mathbb{N}_0$. Since $m\mathbb{Z}$ maps to $\langle g^m \rangle$, we see that the subgroups of G are in one-to-one correspondence with the nonnegative integers.

Now suppose G is finite with order m and let $H \leq G$. Because cyclic groups are abelian, H is normal in G. And since quotients of cyclic groups are cyclic, G/H must be cyclic. Let $d = |H|$. Lagrange's Theorem implies that $d|m$ and $|G/H| = m/d$. Because gH generates G/H, we conclude that gH has order m/d in G/H. Thus

$$H = (gH)^{m/d} = g^{m/d}\, H \quad \Leftrightarrow \quad g^{m/d} \in H \quad \Leftrightarrow \quad \langle g^{m/d} \rangle \leq H.$$

Since the order of $g^{m/d}$ is

$$\left|g^{m/d}\right| = \frac{|g|}{\gcd(|g|, m/d)} = \frac{m}{\gcd(m, m/d)} = \frac{m}{m/d} = d = |H|,$$

we find that we in fact have $H = \langle g^{m/d} \rangle$.

Conversely, if $d \in \mathbb{N}$ and $d|m$, then $g^{m/d}$ has order d by the computation above, so that $\langle g^{m//d} \rangle$ is a subgroup of G of order d. Taken together with the conclusion of the preceding paragraph, this shows that for any $d|m$, $\langle g^{m/d} \rangle$ is the unique subgroup of G of order d. We summarize our findings as follows.

Theorem 2 (Subgroups of Cyclic Groups)**.** *Let $G = \langle g \rangle$ be a cyclic group. Then every subgroup of G is also cyclic. Furthermore:*

a. If G is infinite, then the distinct subgroups of G are given by $\langle g^m \rangle$ for $m \in \mathbb{N}_0$.

b. If G has order $m \in \mathbb{N}$, then for every $d|m$ there is a unique subgroup $H \leq G$ of order d, namely $H = \langle g^{m/d} \rangle$.

Put another way, Theorem 2 tells us that the subgroups of an infinite cyclic group correspond to the nonnegative integers $m \in \mathbb{N}_0$, while the subgroups of a finite cyclic group G correspond to the (positive) divisors of $|G|$.

Exercise 1. Let G be a finite cyclic group. Show that for every divisor d of $|G|$ there exists a unique $H \leq G$ so that G/H has order d.

Example 10 (The Second Isomorphism Theorem)**.**

Let G be a group and consider a sequence of subgroups $K \leq H \leq G$. If $K \triangleleft G$, it is easy to verify that $K \triangleleft H$ and that the coset space H/K is a subgroup of G/K. If $H \triangleleft G$, then for any $gK \in G/K$ and $hK \in H/K$ we have

$$(gK)(hK)(gK)^{-1} = (ghg^{-1})K \in H/K,$$

since $ghg^{-1} \in H$. Thus $H/K \lhd G/K$. The First Isomorphism Theorem can be used to quickly identify the quotient group $(G/K)/(H/K)$. Specifically, we have:

Theorem 3 (Second Isomorphism Theorem)**.** *Let G be a group. If $K \lhd G$ and H is a subgroup of G containing K, then H/K is a subgroup of G/K. If H is normal in G, then H/K is a normal subgroup of G/K and*

$$(G/K)/(H/K) \cong G/H.$$

Proof. Consider the composition of the natural surjections

$$G \to G/K \to (G/K)/(H/K).$$

It is surjective and $g \in G$ belongs to the kernel if and only if $(gK)(H/K) = H/K$, that is $gK \in H/K$. This happens if and only if $gK = hK$ for some $h \in H$, so that $g^{-1}h \in K \leq H$ and hence $gH = hH = H$, i.e. $g \in H$. Therefore the kernel of the composed natural maps is precisely H, and the First Isomorphism Theorem yields

$$G/H \cong (G/K)/(H/K).$$

□

Before moving on, we pause to prove a generalization of the First Isomorphism Theorem that can be useful in certain situations. Specifically, when one wishes to construct a homomorphism of the form $\overline{f} : G/N \to H$, but is unable to find a suitable homomorphism $f : G \to H$ with $N = \ker f$. The proof is nearly identical to the proof of Theorem 1.

Theorem 4 (Generalized First Isomorphism Theorem)**.** *Let $f : G \to H$ be a group homomorphism. If J is a normal subgroup of G contained in $\ker f$, and $\pi : G \to G/J$ is the natural surjection, then the rule $\overline{f}(xJ) = f(x)$ yields a well-defined homomorphism $\overline{f} : G/J \to H$ which satisfies $f = \overline{f} \circ \pi$. Furthermore, $\overline{f}$ is injective if and only if $J = \ker f$.*

Remark. Note that when $J = \ker f$, Theorem 3 reduces to the usual First Isomorphism Theorem.

Proof. If $xJ = yJ$, then $y^{-1}x \in J \leq \ker f$, so that $f(y^{-1}x) = e$. But $f(y^{-1}x) = f(y)^{-1}f(x)$, so that we have $f(y)^{-1}f(x) = e$. Hence $f(x) = f(y)$, which shows that $\overline{f}$ is well-defined. It is a homomorphism since

$$\overline{f}((xJ)(yJ)) = \overline{f}(xyJ) = f(xy) = f(x)f(y) = \overline{f}(xJ)\overline{f}(yJ)$$

for all $xJ, yJ \in G/J$. And for $x \in G$ we have

$$(\overline{f} \circ \pi)(x) = \overline{f}(\pi(x)) = \overline{f}(xJ) = f(x)$$

by construction. Finally, $xJ \in \ker \overline{f}$ if and only if $e = \overline{f}(xJ) = f(x)$, so that

$$\ker \overline{f} = \{xJ \,|x \in \ker f\} = (\ker f)/J.$$

Therefore $\ker \overline{f}$ is trivial if and only if $(\ker f)/J$ is trivial, which is equivalent to $J = \ker f$. □

Example 11. Let G be a group and let $N_1 \leq N_2$ be normal subgroups of G. Then N_1 is contained in the kernel of the natural surjection $\pi : G \to G/N_2$. By the strong First Isomorphism Theorem, this means that $\overline{\pi}(xN_1) = \pi(x) = xN_2$ defines a homomorphism $\overline{\pi} : G/N_1 \to G/N_2$.

For a particular instance of this scenario, let $m, n \in \mathbb{N}$ with $m|n$ and take $G = \mathbb{Z}$. Then $n\mathbb{Z} \leq m\mathbb{Z}$, and we have an epimorphism $\overline{\pi} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ given by $a + n\mathbb{Z} \mapsto a + m\mathbb{Z}$.