The First Isomorphism Theorem

Tim Sullivan

University of Warwick

`tim.sullivan@warwick.ac.uk`

April 2, 2014

The First Isomorphism Theorem for groups is probably the single most confusing thing that mathematics undergraduates meet during their first year at Warwick. Having (for the most part) mastered convergence, continuity and other nasties, all the talk of cosets and quotient groups seems to be the straw that breaks the camel's back. This is a great pity, since the First Isomorphism Theorem is actually a very natural statement, be it couched in the language of groups, rings, modules, vector spaces, algebras or whatever. So, let's try to clear these somewhat muddy waters.

Throughout, any fact, lemma or proposition that isn't fully justified can be taken as an exercise.

— T.J.S.

1   First Isomorphism Theorem for Sets

We'll begin with a silly but accesible example, leading into the natural statement of 'the First Isomorphism Theorem for sets'.

Suppose that you have a (finite) set C of cows. Cows, of course, exist to be sent to market; let M be the set of markets to which you might send your cows. When you decide to sell off your herd, there's a natural function

$$f \colon C \to M$$
$$\text{cow} \mapsto \text{intended market for that cow.}$$

Now, when it comes to actually packing the cows off to market, you could go through them one at a time: consider each cow $c \in C$, and send it to its destination $f(c) \in M$. However, this is clearly quite inefficient: why not first group the cows together according to destination, and then send them in batches? So, create a set of pens $\mathcal{P}$; for each market $m_i \in M$, put in pen $P_i \in \mathcal{P}$ all the cows that go to market m_i. In symbols,

$$P_i := \{c \in C | f(c) = m_i\}.$$

Of course, the P_i are subsets of C; $\mathcal{P}$ is a collection of subsets of C. In fact, $\mathcal{P}$ is a *partition* of C: the P_i are pairwise disjoint and their union is C. (Pedantic readers will wonder what index set I is being used to index the markets m_i, $i \in I$, and pens P_i, $i \in I$. This is a good question, and the quick answer is that actually $I = M$! A different construction, which uses equivalence relations instead of an index set, is given on the next page.)

There is a natural 'penning function' π,

$$\pi \colon C \to \mathcal{P}$$

$$\text{cow} \mapsto \text{pen corresponding to intended market for that cow.}$$

Consider the markets that actually receive some cows, i.e. the image $f(C) \subseteq M$. Now, here is the obvious statement that is 'the First Isomorphism Theorem for sets': *the set of 'used' markets, $f(C)$, and the set of pens, $\mathcal{P}$, are in bijection.*

$$
\begin{array}{ccc}
{}^{\backprime}C & \xrightarrow{\ f\ } & M \\
\pi \downarrow & & \uparrow i \\
\mathcal{P} & \xrightarrow[\ \bar{f}\ ]{} & f(C)
\end{array}
$$

Here,

- $\pi \colon C \to \mathcal{P}$ is the 'penning function', which is *surjective*;

- $i \colon f(C) \to M$ denotes the natural inclusion map, given by $i(m) := m$ for $m \in f(C)$, and which is *injective*;

- and $\bar{f} \colon \mathcal{P} \to f(C)$ is *bijective*.

What is this mysterious $\bar{f}\colon \mathcal{P} \to f(C)$? Simply this: $\bar{f}(P) := f(c)$ for any $c \in P$ – and this is a perfectly valid definition, since we already know that all the cows $c \in P$ go to the same market in $f(C) \subseteq M$.

Why is $\bar{f}$ a bijection? Well, it's injective because if P, P' are distinct pens, their member cows must go to different markets, otherwise they'd be in the same pen. In symbols: let $P, P' \in \mathcal{P}$ be distinct, $c \in P$, $c' \in P'$. Then

$$P \neq P' \implies \pi(c) \neq \pi(c') \implies f(c) \neq f(c') \implies \bar{f}(P) \neq \bar{f}(P').$$

As for surjectivity, this is obvious: every market in $f(C)$ receives at least one cow, and so is $f(P)$ for at least one pen P.

There's another way of writing $\mathcal{P}$: as C modulo an equivalence relation. We have a natural equivalence relation on cows: two cows are equivalent if they go to the same market. In symbols, $c \sim c' \iff f(c) = f(c')$. The *equivalence class* of $c \in C$ is simply all the cows it's equivalent to:

$$[c] := \{c' \in C \,|\, c \sim c'\}.$$

We write $\frac{C}{\sim}$ for the set of equivalence classes of $\sim$ in C. But $\frac{C}{\sim}$ is just the same as $\mathcal{P}$: the pens $P \in \mathcal{P}$ are the equivalence classes $[c] \in \frac{C}{\sim}$. As before, π is the function that assigns to each cow its pen / equivalence class: $\pi(c) := [c]$.

Let's tidy all this up in one statement, and then move on:

Theorem 1.1 (The First Isomorphism Theorem for Sets)**.** *Let X, Y be sets and $f\colon X \to Y$ any function. Let $\sim$ on X be the relation $x \sim y \iff f(x) = f(y)$. Then there is a bijection $\bar{f}\colon \frac{X}{\sim} \to f(X) \subseteq Y$, i.e.*

$$
\begin{array}{ccc}
X & \xrightarrow{\;f\;} & Y \\
{\scriptstyle \pi}\downarrow & & \uparrow{\scriptstyle i} \\
\frac{X}{\sim} & \xrightarrow[\;\bar{f}\;]{} & f(X)
\end{array}
$$

with $\pi\colon X \to \frac{X}{\sim}$ the surjective projection map and $i\colon f(X) \to Y$ the injective inclusion map. Moreover, $\bar{f}([x]) = f(x)$.

2 First Isomorphism Theorem for Groups

By now, you should know what a group is: a non-empty set G equipped with an associative, invertible binary operation. We'll write the group operations

as juxtaposition. 1 (or 1_G) will denote the identity element in G. A *subgroup* of G is simply a non-empty subset of G that is also a group under the same operation as G.

Let's introduce something new: a *coset*. The *right coset* of $S \subseteq G$ by g is

$$Sg := \{sg | s \in S\} \subseteq G.$$

Similarly, the *left coset* of $S \subseteq G$ by g is

$$gS := \{gs | s \in S\} \subseteq G.$$

The group element g is often called a *representative* of the coset gS (or Sg). I like to think of S as being a 'blob' in the group, and that g moves this blob around: try drawing the cosets $x + [0, 1]$ in the additive group $\mathbb{R}$ for a few values of $x \in \mathbb{R}$.

We shall assume the following two propositions, though neither is difficult to prove.

Proposition 2.1. *A non-empty subset S of a group G is a a subgroup if and only if for all $g, h \in S$, $gh^{-1} \in S$.*

Proposition 2.2. *For a subgroup K of a group G, the following are equivalent:*

(i) for all $g \in G$, $gK = Kg$;

(ii) for all $g \in G$ and $k \in K$, $gkg^{-1} \in K$.

If either (and hence both) is true then we say that K is normal *in G and write $K \trianglelefteq G$.*

When $K \trianglelefteq G$ we denote by $\frac{G}{K}$ the set of right (or, equivalently) left cosets of K in G:

$$\frac{G}{K} := \{gK | g \in G\} = \{Kg | g \in G\}.$$

Recall that a function of groups $f \colon G \to H$ is called a *homomorphism* if for all $g, h \in H$, $f(gh) = f(g)f(h)$. A homomorphism is called an *isomorphism* if it is also a bijection. If $f \colon G \to H$ is an isomorphism we say G and H are *isomorphic* and write $G \cong H$.

Suppose we have a homomorphism of groups $f\colon G \to H$. Theorem 1.1 tells us that there's a bijection $\bar{f}$ between $\frac{G}{\sim}$ and $f(G) \subseteq H$ as sets – but the First Isomorphism Theorem for groups tells us even more: *that these two objects are isomorphic as groups.* This is essentially because the homomorphism property forces the equivalence classes $[g]$ have a very special form: they are the cosets of $\ker f$ in G.

Let's start by looking at the *kernel* of f:

$$\ker f := \{g \in G \mid f(g) = 1_H \in H\}.$$

At the very least, the identity $1_G \in G$ is in the kernel. In fact, $\ker f$ forms a subgroup of G: for if $g, h \in \ker f$,

$$f(gh^{-1}) = f(g)f(h^{-1}) = 1_H 1_H^{-1} = 1_H,$$

so $gh^{-1} \in \ker f$. It's also normal: if $g \in G$ and $k \in \ker f$,

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)1_H f(g)^{-1} = 1_H.$$

So, to summarize, $\ker f$ is a normal subgroup of G whose elements are precisely the $g \in G$ that go to the identity in H: in the old language, $\ker f = [1_G]$. Also, $\ker f$ is just the coset $1_G \ker f$.

Now, there's the usual snag that just as an equivalence class can have many representatives, so a coset can be given in many different ways. When are 'two' cosets actually the same?

Lemma 2.3. *Suppose that $K \trianglelefteq G$. Then*

$$g \in hK \iff gK = hK \iff g = hk \text{ for some } k \in K \iff h^{-1}g \in K,$$

and the same for right cosets.

Now suppose that K is the kernel, $K := \ker f$. Then

$$g \in hK \iff h^{-1}g \in K \iff f(h^{-1}g) = 1_H \iff f(g) = f(h).$$

In other words: *the cosets of $\ker f$ in G are precisely the equivalence classes of $\sim$ in G, where $g \sim h \iff f(g) = f(h)$,* i.e.

$$\frac{G}{\sim} = \frac{G}{\ker f}$$

As before, there's a natural projection map $\pi\colon G \to \frac{G}{K}$ given by $\pi(g) := gK$.

Now, we know how to multiply elements of G because G is a group. Can we multiply cosets, elements of $\frac{G}{K}$? If not, then there's no sense in which we can have a group homomorphism with $\frac{G}{K}$ as its domain or target. Fortunately, the answer is yes, like this:

$$(gK)(hK) := (gh)K.$$

The fact that $K \trianglelefteq G$ is exactly what we need to make sure that this definition works:

Lemma 2.4. *When $K \trianglelefteq G$, the above operation on $\frac{G}{K}$ is well-defined in the sense that*

$$gK = g'K \ \text{ and } \ hK = h'K \implies (gK)(hK) = (g'K)(h'K).$$

$\frac{G}{K}$ with this law of multiplication is called the *quotient group* of G by K. We now have the First Isomorphism Theorem for groups:

Theorem 2.5 (The First Isomorphism Theorem for Groups)**.** *Let G, H be groups and $f\colon G \to H$ a homomorphism of groups with kernel $K := \ker f$. Then there is an isomorphism $\bar{f}\colon \frac{G}{K} \to f(G) \subseteq H$, i.e.*

$$
\begin{array}{ccc}
G & \xrightarrow{\ f\ } & H \\[2pt]
\pi \downarrow & & \uparrow i \\[2pt]
\dfrac{G}{K} & \xrightarrow[\ \bar{f}\ ]{} & f(G)
\end{array}
$$

with $\pi\colon G \to \frac{G}{K}$ the surjective projection homomorphism and $i\colon f(G) \to H$ the injective inclusion homomorphism. Moreover, $\bar{f}(gK) = f(g)$.

Proof. We already know that $\ker f \trianglelefteq G$, and so the group operation on $\frac{G}{K}$ is well-defined. It's not hard to see that $f(G)$ is a subgroup of H: if $h, h' \in f(G)$, then there are $g, g' \in G$ with $f(g) = h$, $f(g') = h'$, and then $f(gg') = hh' \in f(G)$. It's also easy to see that $\bar{f}$ is both injective and surjective, and a homomorphism.

We're not done, though. Logically, this bit comes first: we have to check that $\bar{f}$ is actually well-defined! Remember that the same coset can have different representatives, so we need to be sure that if we give $\bar{f}$ the same

6

coset by two different names it will still give us the same answer. This is quick to check, though, and is rather like checking injectivity (the $\implies$ direction is the well-defined-ness check; the $\impliedby$ direction is the injectivity check):

$$
\begin{aligned}
gK = hK &\iff h^{-1}g \in K \\
&\iff f(h^{-1}g) = 1_H \\
&\iff f(h)^{-1}f(g) = 1_H \\
&\iff f(g) = f(h) \\
&\iff \bar{f}(gK) = \bar{f}(hK),
\end{aligned}
$$

and this completes the proof. $\qquad\square$

I'd like to end with a couple of examples.

Examples 2.6. (i) (Time.) Consider time in hours as integers in $\mathbb{Z}$. Hour 0 can be whatever you like – if you're a fan of UNIX, you'll probably want to choose midnight, January 1, 1970. $\mathbb{Z}$, as you know, is an Abelian group under usual addition $+$. However, we don't usually give time this way: we give it in the range 1 o'clock to 12 o'clock. We implicitly make all 12 o'clocks the same: midnight tonight is a 12 o'clock just like mid-day tomorrow will be a 12 o'clock. $12\mathbb{Z}$, the collection of all the 12 o'clocks, is a normal subgroup of $\mathbb{Z}$. Its cosets are

$$
12\mathbb{Z} = 0 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, 2 + 12\mathbb{Z}, \ldots, 10 + 12\mathbb{Z}, 11 + 12\mathbb{Z}.
$$

Two cosets $n + 12\mathbb{Z}$ and $m + 12\mathbb{Z}$ are equal exactly when $n - m$ is a multiple of 12, i.e. $(n - m) \in 12\mathbb{Z}$. We can add these cosets in the natural way:

$$
(n + 12\mathbb{Z}) + (m + 12\mathbb{Z}) := (n + m) + 12\mathbb{Z}.
$$

When we think of time as going from 0 to 11, we add hours modulo 12: 3 hours after 11 o'clock is 2 o'clock, not 14 o'clock. This is suspiciously like adding the cosets of $12\mathbb{Z}$. In fact, if we write $\mathbb{Z}_{12}$ for the integers $\{0, 1, \ldots, 11\}$ with this addition modulo 12, the First Isomorphism Theorem tells us that

$$
\frac{\mathbb{Z}}{12\mathbb{Z}} \cong \mathbb{Z}_{12}.
$$

How can we realise this isomorphsim? Well, let $f \colon \mathbb{Z} \to \mathbb{Z}_{12}$ be function that assigns to every integer its remainder on division by 12. Then $f(\mathbb{Z}) = \mathbb{Z}_{12}$,

ker $f = 12\mathbb{Z}$, and

$$
\begin{array}{ccc}
\mathbb{Z} & \xrightarrow{\ f\ } & \mathbb{Z}_{12} \\
\pi\Big\downarrow & & \Big\uparrow i \\
\frac{\mathbb{Z}}{12\mathbb{Z}} & \xrightarrow[\ \bar{f}\ ]{} & \mathbb{Z}_{12}
\end{array}
$$

with $\bar{f}(n + 12\mathbb{Z}) = f(n)$.

(By the way, if you feel cheated by this example, as if it has said absolutlely nothing – then GOOD!)

(ii) (A string of pearls.) Consider the cyclic Abelian group $\mathbb{Z}_8$: draw it as an octagon, or as the eight 8th roots of unity in $\mathbb{C}$. Similarly, consider $\mathbb{Z}_4$, which you might like to think of as (isomorphic to) $\{1, i, -1, -i\} \subset \mathbb{C}$. Now let $f\colon \mathbb{Z}_8 \to \mathbb{Z}_4$ be the group homomorphism defined by

$$
\begin{array}{ll}
f(0) = f(4) := 0 & f(1) = f(5) := 1 \\
f(2) = f(6) := 2 & f(3) = f(7) := 3
\end{array}
$$

The reason that I titled this example 'a string of pearls' is that you can visualize this homomorphism f as tightening the loop $\mathbb{Z}_8$ so that two points lie above one another, turning the necklace into a two-layered choker. The kernel of f is $K := \{0, 4\}$, and so $\frac{G}{K} = \{K, 1 + K, 2 + K, 3 + K\}$. By now, the isomorphism $\frac{\mathbb{Z}_8}{K} \cong \mathbb{Z}_4$ should be obvious.

3 Rings and Beyond

Go on! Look up the definition of a ring and try the same construction. If that scares you, try the easier exercise of taking the quotient of a vector space V over a field $\mathbb{K}$ by a subspace $W \subseteq V$ – just remember that V has the structure of an Abelian group with respect to vector addition.