Isomorphisms and Well-definedness

Jonathan Love

October 30, 2016

Suppose you want to show that two groups G and H are isomorphic. There are a couple of ways to go about doing this depending on the situation, and for a beginning Algebra student it's sometimes not clear what exactly goes into such a proof. In this paper, we discuss some methods that can be used to solve this problem, give reasons why you may want to choose one method over another, and discuss some potential pitfalls and common misunderstandings - in particular, what it means to check if a function is "well-defined."

This paper is not a style guide for how to write proofs; there are no hard-and-fast rules here, and some of the comments are not totally rigorous. The aim is only to help you develop some intuition for when a given technique may be useful to you, and if so, some things to keep in mind while using it.

1 Overview

- Of all the methods I will discuss, I would say that Methods 3, 4, and 6 are the most important to remember:
  - If one group is a quotient group, try to apply the First Isomorphism Theorem (Method 6).
  - If one group has a presentation, define a homomorphism on the generators of the group, check that it preserves the relations, and show that the map is a bijection (Method 4).
  - Otherwise, define a map on every element of the group, check that it is well-defined, check that it is a homomorphism, and check that it is a bijection (Method 3).
- Method 7 (direct product and semidirect product recognition theorems) is also a must-know. Methods 8 and 9 don't come up as often in the context of proving two groups are isomorphic, but will be helpful if you can remember them.
- Methods 1 and 2 are tempting to use if you don't really know what you're doing, but should be avoided if possible.

Without further ado, let's describe the methods!

Method 1. *Find presentations for G and H and show that they are the same.*

This, in general, is actually a really bad method. One reason is that finding presentations is hard. Finding a generating set may not be so bad, and it's usually possible to compute a few relations, but how do you know you've found enough of them? (Challenge: find a presentation for S_4) And even if you have two valid presentations of G and H, how do you show that they define isomorphic groups? (Challenge: what commonly known group is $\langle x, y, z \mid xy = y^2x, yz = z^2y, zx = x^2z\rangle$ isomorphic to?)

Here are some better ways to tackle the problem.

2 Defining an Isomorphism

There are three stages that go into defining an isomorphism between G and H:

1. Define a function $\phi : G \to H$.
2. Show that ϕ is a homomorphism.
3. Show that ϕ is a bijection.

Now, once you have a well-defined function ϕ, the last two steps are usually fairly straightforward (though check out the "Once ϕ is defined" section for some warnings). But getting ϕ in the first place can be a little tricky. The methods discussed in this section will focus on that step.

2.1 Defining ϕ

Method 2. *Explicitly describe where every element goes.*

Advantage: Checking injectivity and surjectivity is usually pretty straightforward if you can see all of the elements in front of you.

Disadvantage: Good luck checking that ϕ is a homomorphism. Even if G has only 4 elements, you'll have to check 16 different products (and will almost certainly make a mistake somewhere). And this is strictly impossible if G is infinite. Use this only for very small groups.

Method 3. *Define ϕ by a rule, and check that it is well-defined.*

This is a very common approach: "take arbitrary $g \in G$, do something to it, and out pops an element of H." But what does it mean to check that it is well-defined?

If your rule depends on how you write g, every allowed way of writing g must define the same element of H.

Example 1 (Not well-defined)**.** Suppose we try to define $t : \mathbb{Q} \to \mathbb{Z}$ as follows: write $x \in \mathbb{Q}$ as $x = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, and set $t(x) = a$. If I let $x = \frac{2}{3}$, then I can also write it as $\frac{-4}{-6}$. So should $t(x) = 2$ or $t(x) = -4$? The rule allows both options, so t is not well-defined.

One common situation where this pops up is when G is a **quotient group**:

Example 2 (Not well-defined)**.** Suppose we try to define $p : \mathbb{Z}/15\mathbb{Z} \to S_4$ by $\overline{n} \mapsto (1\,2)^n$. But according to this rule, we should have $\overline{1} \mapsto (1\,2)$ and $\overline{16} \mapsto e$. $\overline{1}$ and $\overline{16}$ are two different ways of writing the same element of the quotient group $\mathbb{Z}/15\mathbb{Z}$ (that is, they are different representatives of the same coset), but the rule doesn't output the same element of S_4. So p is not well-defined.

One way to make a function well-defined is to **cut down on options**. For example, I could redefine t by writing $x \in \mathbb{Q}$ as $x = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b > 0$, and a, b relatively prime, and *then* set $t(x) = a$. I could redefine p by taking $\overline{n} \mapsto (1\,2)^n$, where $0 \leq n < 15$. In both cases, I made the function well-defined by choosing a *unique* way of writing each element of G.

The problem with cutting down the options is that it usually makes it really annoying to check whether ϕ is a homomorphism - and often there's no obvious choice of a unique representative to pick. In general, you want to keep all the options open; you just need to **check that every way of writing g gives the same element of H.**

Example 3 (Well-defined)**.** Define $q : \mathbb{Z}/15\mathbb{Z} \to S_4$ by $\overline{n} \mapsto (1\,2\,3)^n$. Suppose $\overline{n} = \overline{n'}$; then $n' = n + 15k$ for some integer k. Now

$$(1\,2\,3)^{n'} = (1\,2\,3)^{n+15k} = (1\,2\,3)^n \left((1\,2\,3)^3\right)^{5k} = (1\,2\,3)^n$$

because $(1\,2\,3)$ has order 3. Hence q is well-defined.

Note that even if there are multiple ways of writing elements $g \in G$, **if your rule only depends on functions that have already been defined, then it is not necessary to check every way of writing g.** For example, if G is a group, then the map $G \to G$ given by $g \mapsto g^3$ is automatically well-defined, because the group operation is a function that's already been defined.

Note: We talk about functions being well-defined or not, but strictly speaking, every function is well-defined. If you attempt to define a function, and then find out that it isn't well-defined (as in Examples 1 and 2 above), it's not that you get a "non-well-defined function," *you just don't have a function.* **When we say "t is not well-defined," we really mean "if a function t satisfying the above definition existed, then we would get a contradiction."**

Method 4. *Define ϕ on the generators, extend to all products, and check that it preserves the relations.*

This is actually just a special case of the previous method. First you give a rule: for any $g \in G$, write it as a product of the generators of G, and apply ϕ to each generator to get an element of H. Now we just need to check that the function is well-defined, otherwise this might happen:

Example 4 (Not well-defined)**.** We attempt to define $f_r : D_8 \to D_8$ as follows: given $x \in D_8$, write x in terms of the generators r, s of D_8. Let $f_r(x)$ be the element of D_8 obtained by removing every power of s from this expression.

Alternatively, we set $f_r(s) = 1$ and $f_r(r) = r$, and then we extend f_r multiplicatively. It's clear that this gives the same definition as above.

Now rs and sr^{-1} are two different expressions for the same element x. So what happens when you remove every power of s? Is $f_r(x) = r$ or $f_r(x) = r^{-1}$? Different expressions for x result in different values, so f_r is not well-defined.

As we saw in Method 3, to check a function is well-defined, we need to show that every way of writing an element of G gives the same result. This can seem daunting at first; in D_8 we have $rs = sr^{-1} = srsr^2s = r^{-3}sr^5s^3r^{17}s^{-4}r^{-8}s^{11} = \ldots$ How can we check that all these ways of writing an element give the same output?

If ϕ is defined on the generators of G and extended multiplicatively, it is well-defined if and only if it preserves the relations of G (that is, for each relation $g_1 \cdots g_n = h_1 \cdots h_m$ in terms of generators $g_1, \ldots, g_n, h_1, \ldots, h_m$ of G, we have $\phi(g_1) \cdots \phi(g_n) = \phi(h_1) \cdots \phi(h_m)$).

This is because the relations of G are exactly what you use to get from any way of expressing g as a product of the generators to any other way. So if ϕ preserves all the relations, then it will give the same output no matter how you write g as a product of the generators.

We illustrate this with an example:

Example 5 (Well-defined)**.** Define $f_s : D_8 \to D_8$ by setting $f_s(s) = s$ and $f_s(r) = 1$, and then extending f_s multiplicatively. Note that

$$\begin{aligned} f_s(r)^n &= 1^n = 1 = f_s(1), \\ f_s(s)^2 &= s^2 = 1 = f_s(1), \\ f_s(r)f_s(s) &= 1s = s1^{-1} = f_s(s)f_s(r)^{-1}, \end{aligned}$$

so f_s preserves the relations of D_8. Hence it is well-defined.

If you have a presentation for G, then *Method 4 is almost always the best method*. Why? Because when it's defined this way, ϕ is *automatically* a homomorphism. You defined it to preserve products, and as long as it's well-defined you get homomorphism for free! (So for example, f_s defined above is a homomorphism.)

Method 5. *Try swapping G and H.*

This isn't actually a method in itself (you still have to use one of the previous methods), but it's good to keep in mind: sometimes defining a function from H is a lot easier than defining a function from G! For example, if you have a presentation for H but not G, then use method 4 to get a function $\phi : H \to G$.

2.2 Once ϕ is defined

Recall that we still need prove:

2. Show that ϕ is a homomorphism.
3. Show that ϕ is a bijection.

Here are a few pointers to keep in mind:

- Steps 2 and 3 don't have to be done in order. *However*, if you do Step 3 first, you are not allowed to use properties of homomorphisms in your proof. For example, suppose you prove that $\phi(x) = 0$ implies $x = 0$. This doesn't mean ϕ is injective, unless you've already proven that ϕ is a homomorphism. If you're not sure, it's safest to follow the steps in order.
- If G and H are finite, then Step 3 can be done by proving (a) ϕ injective and surjective, (b) ϕ injective and $|G| = |H|$, or (c) ϕ surjective and $|G| = |H|$. Note that (b) and (c) do *not* work for infinite groups, even if they have the same cardinality.
- Regarding the above point, be very careful not to use circular logic. A very common mistake is to say "We proved ϕ is injective. Using ϕ we can see that $|G| = |H|$. As a result, ϕ is a bijection." This is invalid, because you can't use ϕ to conclude $|G| = |H|$ unless you already *know* ϕ is a bijection. If you want to use $|G| = |H|$, you have to count the size of each group independently.

3 Alternate Routes: Theorems

Method 6. *Use an isomorphism theorem.*

This tends to work great **if G is a quotient group**, say $G = A/B$. If you need to show $A/B \cong H$, try to define a homomorphism (using the methods described above) from A to H, check that it is surjective, and that the kernel is B; then you can apply the first isomorphism theorem. This is usually easier than the normal way, because checking if a function on A is well-defined tends to be simpler than checking if a function on A/B is well-defined.

Likewise, be on the lookout for situations when you can use the other isomorphism theorems. Can you write $A = SB$ for some other subgroup $S \leq A$? Then maybe you can use the second isomorphism theorem. Are A and B themselves both quotient groups, or is there a normal subgroup $K \trianglelefteq B$? Maybe you can use the third isomorphism theorem.

Method 7. *Use a recognition theorem.*

Is one of your groups a **direct product**? Try to apply Dummit & Foote Section 5.4 Theorem 9. A **semidirect product**? Try to apply Dummit & Foote Section 5.5 Theorem 12.

Method 8. *Use a classification theorem.*

Do you know that G and H are **both finite abelian groups**? Try to write them both out in their elementary or primary decomposition.

Method 9. *Identify a group by its action on some set.*

If you are trying to show G **is isomorphic to a subgroup of** S_n, you can look for a set of n or fewer elements that G acts on. If $|G| = n$, maybe you can use G acting on itself by left multiplication. Otherwise, maybe there is a conjugacy class $C \subseteq G$ with n elements, and G acts on C by conjugation.

In any of these cases, the group action defines a homomorphism $G \to S_n$ (see Dummit & Foote Section 4.1), and you may be able to use this to define an isomorphism between G and its image.

Method 10. *Other theorems?*

Group theory is full of theorems that describe isomorphisms. Feel free to use them if you can recall the conditions under which they apply!