Canonical decomposition and the first isomorphism theorem

Tiny Explanations 2

Carl Joshua Quines

May 11, 2020

Aluffi's *Algebra Chapter 0* introduces the concept of the canonical decomposition of a function. I'm kind of sad that I've never seen this concept being used anywhere else, because I think it's a nice way to explain the first isomorphism theorem.

Consider such a function like $f : \{1, 2, 3, 4, 5, 6\} \to \{a, b, c, d, e\}$ that looks like this:

$$\begin{tikzcd}
1 \arrow[dr] & \\
& a \\
2 \arrow[ur] & \\
& b \\
3 \arrow[dr] & \\
& c \\
4 \arrow[dr] & \\
& d \\
5 \arrow[ur] & \\
& e \\
6 \arrow[uuur] &
\end{tikzcd}$$

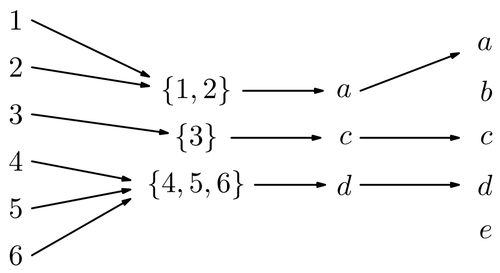
This function defines an equivalence relation $\sim$, where two things are equivalent if they get mapped to the same thing. So $1 \sim 2$ because they both get mapped to a, and $4 \sim 6$ because they both get mapped to e, but $2 \not\sim 3$ because they both get mapped to different things.

Then we can define $A/\sim$, the quotient of A under the equivalence relation, which just consists of the subsets of A that are equivalent to each other. Here, $A/\sim$ would have three elements: $\{1, 2\}$, $\{3\}$, and $\{4, 5, 6\}$. There is a very natural function $A \twoheadrightarrow A/\sim$ that takes the element to the corresponding subset.

Now f factors through $A/\sim$. *Factor through* is a fancy phrase that means we can rewrite f as a composition of two functions that go through the set $A/\sim$. This gives something like this:

$$\begin{tikzcd}
1 \arrow[dddr] & & \\
& & a \\
2 \arrow[dr] & & \\
& \{1,2\} \arrow[uur] & b \\
3 \arrow[dr] & & \\
& \{3\} \arrow[r] & c \\
4 \arrow[dr] & & \\
& \{4,5,6\} \arrow[r] & d \\
5 \arrow[ur] & & \\
& & e \\
6 \arrow[uuur] & &
\end{tikzcd}$$

The second function here, the one that takes $A/\sim$ to B, also splits naturally into two functions. This function factors through the set $\operatorname{im} f$, the image of f, which in this case consists of a, c, and d. Our final diagram looks like this:



Now take a moment to think about these three functions, in order. The first one, $A \twoheadrightarrow A/\sim$, is surjective. The second one, $A/\sim \to \operatorname{im} f$, is bijective. And the third one, $\operatorname{im} f \hookrightarrow B$, is injective. Suddenly, we've taken our function and written it as a composition of a surjection, a bijection, and an injection! And it's clear that any function can be decomposed like this:

$$A \twoheadrightarrow A/\sim \xrightarrow{\cong} \operatorname{im} f \hookrightarrow B.$$

Alright, now, I promised that this is related to the first isomorphism theorem. So let's look at some group homomorphisms:

Example. Let G be the nonzero integers modulo 7, with the operation of multiplication. This is a group: the identity is 1, and every element has an inverse, like 3's inverse is 5 because $3 \cdot 5 = 1$.

Now consider the function $\mathbb{Z}^+ \to G$ that takes n to 2^n mod 7. To check that this is a homomorphism, it needs to preseve the group operation. The operation of $\mathbb{Z}^+$ is addition, and the operation in G is multiplication. And we can check that $a + b$ is taken to $2^a \cdot 2^b$, so this is a homomorphism.

What are the equivalence classes? They're $\{\ldots, -3, 0, 3, 6, \ldots\}$, $\{\ldots, -2, 1, 4, 7, \ldots\}$, and $\{\ldots, -1, 2, 5, 8, \ldots\}$. The image is 2^0, 2^1, or 2^2, which are 1, 2, and 4. The canonical decomposition tells us that each of these equivalence classes correspond to one of these three numbers.

Example. Consider the function $\mathbb{C}^\times \to \mathbb{R}^\times$ that takes z to its magnitude. To check this is a homomorphism, it needs to preserve the group operation. But indeed, ab is taken to $|a||b|$. (Note that the first multiplication here is in $\mathbb{C}$, and the second multiplication here is in $\mathbb{R}$.)

The equivalence classes are the z that have the same magnitude, which if you plotted them on the complex plane, form a circle centered at the origin. The image is the nonnegative real numbers. The canonical decomposition tells us that the circles centered at the origin correspond to the nonnegative real numbers.

We usually like writing $A/\sim$ in a different way. Instead of quotienting by the equivalence relation, we can "quotient" by the subsets themselves, since these determine $\sim$ entirely. So to return to our original example, $A/\sim$ can be written as

$$A/\left(\{1, 2\}, \{3\}, \{4, 5, 6\}\right).$$

Or in the example of $\mathbb{Z}^+ \to G$, we can write $\mathbb{Z}/\sim$ as

$$\mathbb{Z}/\left(\{\ldots, -3, 0, 3, 6, \ldots\}, \{\ldots, -2, 1, 4, 7, \ldots\}, \{\ldots, -1, 2, 5, 8, \ldots\}\right).$$

Or in the example of $\mathbb{C}^\times \to \mathbb{R}^\times$, we can write $\mathbb{C}/\sim$ as

$$\mathbb{C}/\left(\{|z| = r\} \text{ for } r \in \mathbb{R}^+\right).$$

This can get rather cumbersome. In the case of groups, then, we don't write *all* the equivalence classes; it's enough to write one equivalence class. But which one do we pick? Well, because we're working with groups, there's a natural distinguished element—the identity! So is it just enough to pick the equivalence class with the identity?

Example. Let's return to the example of $\mathbb{Z}^+ \to G$. If we knew that $\{\ldots, -3, 0, 3, 6, \ldots\}$, or $3\mathbb{Z}$, was the equivalence class with the identity, does that determine the other equivalence classes? Intuitively, just from looking at this set, the natural other classes are $\{\ldots, -2, 1, 4, 7, \ldots\}$ and $\{\ldots, -1, 2, 5, 8, \ldots\}$, which you get from taking $3\mathbb{Z}$ and adding something, like $3\mathbb{Z} + 1$, or $3\mathbb{Z} + 2$.

Example. What about the other example, the one from $\mathbb{C}^\times \to \mathbb{R}^\times$? Here, the equivalence class with the identity is $|z| = 1$, the unit circle, which we'll write as T. Then you get any other equivalence class by multiplying T with some element in $\mathbb{C}^\times$. For example, $5T$ is all the complex numbers with magnitude 5, which happens to be the same as $(3 + 4i)T$.

Because the equivalence class with the identity is clearly pretty special, it has a name: $\ker f$, the kernel of f. It's the equivalence class of $A/\sim$ that contains the identity, or equivalently, the subset of A that gets sent to the identity in B.

We just saw that for groups, $\ker f$ determines all the other equivalence classes in $A/\sim$. To find them, we simply take $\ker f$, and add or multiply the other elements in A with it. Because $\ker f$ is enough to describe all the equivalence classes, instead of writing $A/\sim$, we can (and usually do) write $A/\ker f$:

$$A \twoheadrightarrow A/\ker f \xrightarrow{\cong} \operatorname{im} f \hookrightarrow B.$$

So in the $\mathbb{Z}^+ \to G$ example, where the kernel was $3\mathbb{Z}$, the multiples of 3:

$$\mathbb{Z}^+ \twoheadrightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cong} \{1, 2, 4\} \hookrightarrow G.$$

And in the $\mathbb{C}^\times \to \mathbb{R}^\times$ example, where the kernel was T, the elements of $\mathbb{C}$ with magnitude 1:

$$\mathbb{C}^\times \twoheadrightarrow \mathbb{C}/T \xrightarrow{\cong} \mathbb{R}^+ \hookrightarrow \mathbb{R}^\times.$$

And finally, the middle function here, the one that's the bijection—that's the first isomorphism theorem! There's a bit of work here to show that all of these things are well-defined, in particular with the claim "$\ker f$ determines all the equivalence classes," but that's best left for a textbook. (It's not entirely clear, because not all subgroups are the kernel of some homomorphism.)

So this gives us two ways to think of G/H. First, it's the equivalence classes you get when you take H and multiply it with elements in G. This is the perspective that the notation G/H suggests: you're dividing G into H-sized equivalence classes. And second, it's $\operatorname{im} f$, where f is a homomorphism from G with H as the kernel. Both perspectives are useful. Useful examples to think about: $\mathbb{R}/\mathbb{Z}$, and $\mathbb{Q}/\mathbb{Z}$.

Similarly, if you have a group homomorphism $f : G \to H$, it's always a good idea to think: what's $\ker f$? What's $G/\ker f$? Which subgroup of H is it?