A view at the galaxy of universal properties

By Jack Valerio Straus

Introduction

You might have noticed that a common way to understand mathematical objects is to think about functions between them. For example,

(i) Group Theory has group Homomorphisms

(ii) Topology explores Homeomorphisms

(iii) Differential Geometry inspects Diffeomorphisms

Each one of these objects makes up a star in the galaxy of math but how are these stars connected? This is the question that universal properties seek to answer. Universal properties endow us with a few powerful facts and abilities,

(i) Expose what is a feature of a map vs what is a feature of an object.

(ii) Allow generalization of certain proofs

(iii) Sweeps away messy unnecessary details of proofs

Prerequisites

Prior to our exploration of universal properties we must define an important preliminary concept. Let $\sim$ be an equivalence relation defined on the set A. We define the quotient set of A as follows,

$$A/\sim := \{\, [a] \,:\, a \in A\}$$

In plain words, the Quotient set of A is the set of all equivalence classes of A under the equivalence relation $\sim$.

Using the Quotient set we define the following function,

$$\pi : A \longrightarrow A/\sim \qquad \pi(a) = [a]$$

π is called the natural projection. π offers a natural and canonical way to map a set onto its quotient set under an equivalence relation.

Let's explore the natural projection with an example. Consider the set $\mathbb{Z}$ and define $a \sim b$ if and only if $2|(b-a)$. The first question we ask ourselves is what does the quotient set of $\mathbb{Z}$ look like under $\sim$. It doesn't take much effort to realize the equivalence relation partitions the integers into two equivalence classes, namely the even integers and the odd ones.

$$\mathbb{Z}/\sim = \{[2], [1]\}$$

Turning our attention to figure 1 we can now understand why π is called the natural projection. The function π projects the integers into two classes, it quite literally collapses the integers into a smaller space.

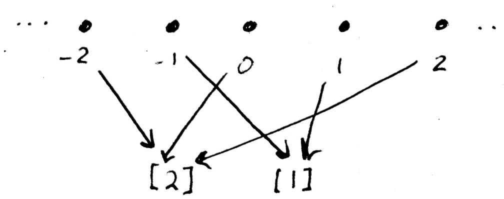

Figure 1: Natural projection of $\mathbb{Z}$ using $\sim$ as defined above

Equipped with the knowledge of a natural projection we can meet our first universal property.

The Universal Property of Quotients

Let A be a set equipped with an equivalence relation $\sim$ and consider a function $g : A \longrightarrow B$. When g satisfies the property that for all $a, a' \in A$,

$$a \sim a' \Rightarrow g(a) = g(a')$$

then there exists $f : A/\sim \longrightarrow B$ such that the diagram in figure 2 commutes, that is $g = f \circ \pi$ with $f([a]) = g(a)$.

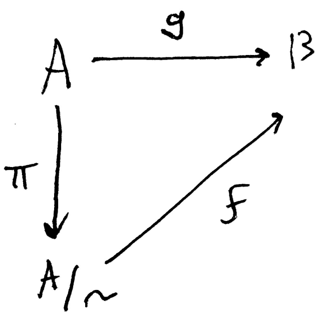

Figure 2

A natural question is what is so universal about this property? The key feature of the theorem that introduces the idea of universal is that the only restriction we've put on A and B is that they're sets. We didn't specify them as groups, rings, modules, or manifolds. This approach to studying mathematical objects helps us distill when something is universal to sets or just a result of a special kind of set. Another important task is to prove that the Universal Property of Quotients is even true, which we will now do.

We know that π exists since we have an equivalence relation defined over A. Therefore, to prove the Universal Property of Quotients we need to show that f is well defined, that is f is a function, and that $g = f \circ \pi$.

Proof

Let us first show that f is well defined. Consider $[a] = [b]$ then $a \sim b$ and by assumption we conclude,

$$f([a]) = g(a) = g(b) = f([b])$$

thus f is a well defined function. Now let $a \in A$,

$$f \circ \pi(a) = f(\pi(a)) = f([a]) = f(a)$$

Therefore, $g = f \circ \pi$ ■

Example

Define the following function $g : \mathbb{Z} \longrightarrow \{0, 1\}$,

$$g(a) = \text{the remainder of a when divided by 2}$$

Now consider the equivalence relation $a \sim b$ if and only if $2|(b-a)$. Is there a function f such that $g = f \circ \pi$? The Universal Property of Quotients makes this question nearly trivial. All we have to check is the following: does g satisfies the property that for all $a, a' \in \mathbb{Z}$,

$$a \sim a' \Rightarrow g(a) = g(a')$$

Clearly, the answer is yes and thus by the Universal Property of Quotients we know there exists a function

$$f : \mathbb{Z}/\sim \longrightarrow \{0, 1\} \text{ with } f([1]) = 1 \text{ and } f([0]) = 0$$

such that the diagram in figure 3 commutes.

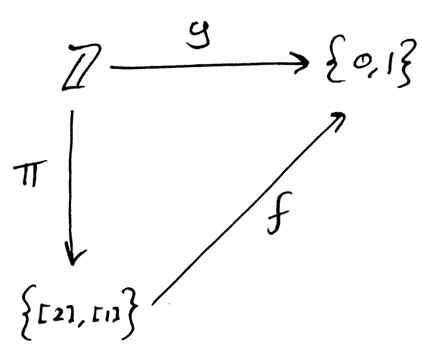

Figure 3

You can generate countless examples using the former idea. Now imagine if we didn't know of the Universal Property of Quotients, each one of these examples might appear special or seem to suggest that there is something unique about the sets. However, we now clearly understand that what is special is in fact the way we map between the sets.

The Universal Property of Quotients is one of many universal properties in the galaxy. Which suggests there are far more to spot out in the night sky. One of the most powerful universal properties goes by the name of the canonical decomposition of functions and directly results in the isomorphism theorems in the various disciplines of Abstract Algebra.

Application of the Universal Property of Quotients

Similar to the integers the canonical decomposition of functions allows us to break apart a function into more digestible pieces of information where each piece of information has a prescribed property. This result follows almost directly from the universal property of quotients and it says the following,

Canonical Decomposition of Functions

If $f : A \longrightarrow B$ is a function of sets then there exists two sets A' and B', alongside

i. a surjective function $\pi : A \longrightarrow A'$

ii. a bijective function $\hat{f} : A' \longrightarrow B'$

iii. a injective function $i : B' \longrightarrow B$

such that $f = i \circ \hat{f} \circ \pi$

Proof

i. Choose $B' = f(A)$ because $B' \subseteq B$ we can define the function $i : f(A) \longrightarrow B$ by $i(b) = b$ for all $b \in f(A)$. Clearly this function is injective since $B' \subseteq B$.

ii. For A' consider the equivalence relation $a \sim b$ if and only if $f(a) = f(b)$. It's left as an exercise to verify this statement because the proof is very straight forward. Now let $A' = A/\sim$ and define pi to be the canonical projection that is, $\pi : A \longrightarrow A/\sim$ with $\pi(a) = [a]$ for all $a \in A$. We've already discussed how this function is surjective and thus the proof is omitted.

iii. Due to the way we've defined our aforementioned equivalence relation on A we can use the universal property of quotients. Because $a \sim b \Rightarrow$

$f(a) = f(b)$. By the universal property of quotients, f induces a function $g : A \longrightarrow B$ such that $f = g \circ \pi$. However, the image of g equals the image $f(A) = B'$ thus g can be thought of as a function $\hat{f} : A/\sim \longrightarrow f(A)$ explicitly defined by, $\hat{f}([a]) = f(a)$. This the following discovery we arrive at the following true composition $g = i \circ \hat{f}$. but we know that $f = g \circ \pi$ which is if and only if $f = i \circ \hat{f} \circ \pi$. We've now arrived at the desired composition and the only property left to check for the canonical decomposition of functions is if $\hat{f}$ is a bijection.

iv. Let $b \in f(A)$ then there exists $a \in A$ such that $f(a) = b$ and by the fact that $\hat{f}([a]) = f(a)$ we come to the conclusion that

$$\hat{f}([a]) = f(a) = b$$

which shows that the function $\hat{f}$ is indeed surjective. Now to show injectivity assume that $\hat{f}(a\hat{f}(b)$ for $a, b \in A/\sim$ by $\hat{f}([a]) = f(a)$ we conclude that $f(a) = f(b)$ and by the definition of $\sim$ we have that $[a] = [b]$. which shows that $\hat{f}$ is injective and thus bijective since it is also surjective.

v. This concludes the proof of the canonical decomposition of functions and the commutative diagram in figure 4 illustrates what is happening in a more concrete way.

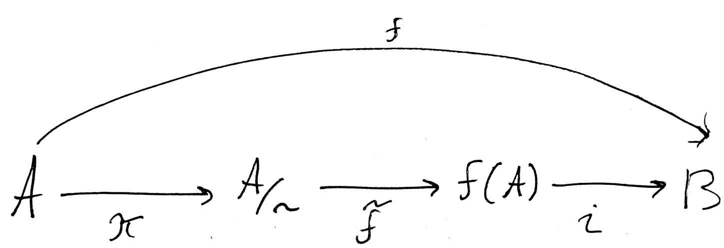

Figure 4

Application of the Canonical Decomposition of functions

I will illustrate the power of our new property by proving the first ring isomorphism theorem in two lines.

First isomorphism theorem for Rings

Let $f : R \longrightarrow S$ be a surjective ring homomorphism then $S \cong R/ker(f)$

Proof

By the canonical decomposition of functions,

$$R/ker(f) \cong f(R)$$

and since f is surjective $f(R) = S$ and our theorem follows.

Further Ideas

What's been shown in this document is brief peek at the galaxy. Universal properties are in fact a part of a much more abstract theory called Category Theory. For further exploration consider reading and exposition,

(i) Categories for the Working Mathematician by Saunders Mac Lane

(ii) Category Theory in Context by Emily Riehl