The Universal Property of the Quotient

Let $H \lhd G$. Then G/H becomes a group under coset multiplication. Define the **quotient map** (or **canonical projection**) $\pi : G \to G/H$ by

$$\pi(g) = gH.$$

Proposition. If $H \lhd G$, the quotient map $\pi : G \to G/H$ is a surjective homomorphism with kernel H.

Proof. If $a, b \in G$, then

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

Therefore, π is a group map.

Obviously, if $gH \in G/H$, then $\pi(g) = gH$. Hence, π is surjective.

Finally, I'll show that $\ker \pi = H$. If $h \in H$, then $\pi(h) = hH = H$, and H is the identity in G/H. Therefore, $h \in \ker \pi$, so $H \subset \ker \pi$.

Conversely, suppose $g \in \ker \pi$. Then $\pi(g) = H$, so $gH = H$, so $g \in H$. Therefore, $\ker \pi \subset H$, and hence $H = \ker \pi$. $\square$

The preceding lemma shows that *every normal subgroup is the kernel of a homomorphism*: If H is a normal subgroup of G, then $H = \ker \pi$, where $\pi : G \to G/H$ is the quotient map. On the other hand, the kernel of a homomorphism is a normal subgroup.

Corollary. Normal subgroups *are exactly* the kernels of group homomorphisms. $\square$

Normality was defined with the idea of imposing a condition on subgroups which would make the set of cosets into a group. Now an apparently independent notion — that of a homomorphism — gives rise to the same idea! This strongly suggests that the definition of a normal subgroup was a good one.

You can think of quotient groups in an even more subtle way. The general theme is something like this. In modern mathematics, it is important to study not only objects — like groups — but the maps between objects — in this case, group homomorphisms. The maps, after all, describe the *relationships* between different objects. (This theme is elaborated in a branch of mathematics called **category theory**.)

It turns out that more is true. In a sense, the maps carry *all of the information* about the objects; one could even be perverse and "build up" objects out of maps! I won't go to such extremes, but in some cases, an object can be *characterized* by certain maps. Here's an important example.

Theorem. (**Universal Property of the Quotient**) Let $H \lhd G$, and let $\phi : G \to K$ be a group homomorphism such that $H \subset \ker \phi$. Then there is a unique homomorphism $\tilde{\phi} : G/H \to K$ such that the following diagram commutes:

$$\begin{tikzcd} G \arrow[d, "\pi"'] \arrow[dr, "\phi"] & \\ G/H \arrow[r, "\tilde{\phi}"'] & K \end{tikzcd}$$

(To say that the diagram **commutes** means that $\tilde{\phi} \cdot \pi = \phi$.)

Proof. Define $\tilde{\phi} : G/H \to K$ by

$$\tilde{\phi}(gH) = \phi(g).$$

This is forced by the requirement that $\tilde{\phi}\pi = \phi$, since plugging $g \in G$ into both sides yields $\tilde{\phi}\pi(g) = \phi(g)$, or $\tilde{\phi}(gH) = \phi(g)$.

I need to check that this map is **well-defined**. The point is that a given coset gH may in general be written as $g'H$, where $g \neq g'$. I must verify that the result $\phi(g)$ or $\phi(g')$ is the same regardless of how I write the coset.

(If $\phi(g) \neq \phi(g')$ in this situation, then a single input — the coset $gH = g'H$ — produces different outputs, which contradicts what it means to be a function.)

So suppose that $gH = g'H$, so $g = g'h$ for some $h \in H$.

$$\tilde{\phi}(gH) = \phi(g) = \phi(g'h) = \phi(g')\phi(h) = \phi(g') \cdot 1 = \phi(g') = \tilde{\phi}(g'H).$$

This shows that $\tilde{\phi}$ is indeed well-defined.

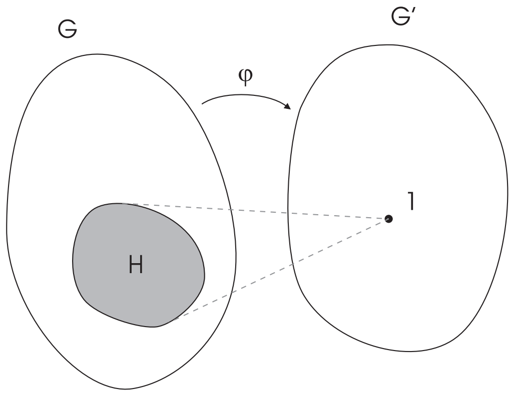
I was forced to define $\tilde{\phi}$ as I did in order to make the diagram commute. Hence, $\tilde{\phi}$ is unique.

Now I'll show that $\tilde{\phi}$ is a homomorphism. Let $a, b \in G$. Then

$$\tilde{\phi}\left((aH)(bH)\right) = \tilde{\phi}\left((ab)H\right) = \phi(ab) = \phi(a)\phi(b) = \tilde{\phi}(aH)\tilde{\phi}(bH).$$

Therefore, $\tilde{\phi}$ is a homomorphism. □

The universal property of the quotient is an important tool in constructing group maps: To define a map out of a quotient group G/H, define a map out of G which maps H to 1.



The map *you* construct goes from G to G'; the universal property *automatically* constructs a map $G/H \to G'$ for you. The advantage of using the universal property rather than defining a map out of G/H directly is that you don't repeat the verification that the map is well-defined — it's been done once and for all in the proof above.

Should you ever need to know how the magic map $\tilde{\phi}$ is defined, refer to the proof (and the commutativity of the diagram).

Remarks. (a) Many other constructions are characterized by universal properties. In each case, one finds that the appropriate conditions imply the existence of a unique map with certain properties.

(a) The use of diagrams of maps — particularly commutative ones — is pervasive in modern mathematics. They are a powerful language, and another outgrowth of the categorical point of view. In general, one says a diagram **commutes** if following the "paths" indicated by the arrows (maps) in different ways between two objects produces the same result. For example, consider the diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ g\downarrow & & \downarrow h \\ C & \xrightarrow[i]{} & D \end{array}$$

To say that this diagram commutes means that $h \cdot f = i \cdot g$. □

Example. Use the universal property to show that $f : \mathbb{Z}_8 \to \mathbb{Z}_{12}$ given by $f(x) = 3x$ is a well-defined group map.

I can regard $\mathbb{Z}_8$ as $\dfrac{\mathbb{Z}}{8\mathbb{Z}}$. To define f, begin by defining $f' : \mathbb{Z} \to \mathbb{Z}_{12}$ by

$$f'(x) = 3x.$$

Let $8n \in 8\mathbb{Z}$. Then since 24 is a multiple of 12,

$$f'(8n) = 3 \cdot 8n = 24n = 0.$$

This means that f' maps the subgroup $8\mathbb{Z}$ of $\mathbb{Z}$ to the identity $0 \in \mathbb{Z}_{12}$. By the universal property of the quotient, f' induces a map $f : \dfrac{\mathbb{Z}}{8\mathbb{Z}} \to \mathbb{Z}_{12}$ given by

$$f(x + 8\mathbb{Z}) = 3x.$$

I can identify $x + 8\mathbb{Z}$ with $x \pmod 8 \in \mathbb{Z}_8$ by reducing mod 8 if needed. (Thus, $11 + 8\mathbb{Z} \in \dfrac{\mathbb{Z}}{8\mathbb{Z}}$ is identified with $3 \in \mathbb{Z}_8$.) Then the definition of f becomes

$$f(x) = 3x.$$

This is the group map I wanted to construct. $\square$

Example. (**Using the universal property to construct a group map**) Use the universal property to construct a homomorphism from the quotient group $\dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (5, 2) \rangle}$ to $\mathbb{Z}$.

The universal property tells me to construct a group map from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ which contains $\langle (5, 2) \rangle$ in its kernel — that is, which sends $\langle (5, 2) \rangle$ to 0. Now $\langle (5, 2) \rangle$ consists of all multiples of $(5, 2)$, so what I'm looking for is a group map which sends $(5, 2)$ to 0.

To ensure that what I get is a *group map*, I should probably guess a linear function — something like

$$f(x, y) = ax + by.$$

If $f(5, 2) = 0$, then $5a + 2b = 0$. There is no question of *solving* this equation for a and b, since there is one equation and two variables. But I just need *some* a and b that work — and one "obvious" way to do this is to set $a = 2$ and $b = -5$, since

$$5(2) + 2(-5) = 0.$$

Notice that $a = 8$, $b = -20$ would work, too. In fact, there are infinitely many possibilities.

So I define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by

$$f(x, y) = 2x - 5y.$$

It's easy to check that this is a group map, and I constructed it so that $\langle (5, 2) \rangle \subset \ker f$. Therefore, the universal property *automatically* produces a group map $\tilde{f} : \dfrac{\mathbb{Z} \times \mathbb{Z}}{\langle (5, 2) \rangle} \to \mathbb{Z}$. It is defined by

$$\tilde{f}\left((x, y) + \langle (5, 2) \rangle\right) = 2x - 5y.$$

Why not just define the map this way to begin with? If you did, you'd have to check that the map was *well-defined*. It's less messy to use the universal property to construct the map as above. $\square$
