9. Quotient Groups

Given a group G and a subgroup H, under what circumstances can we find a homomorphism $\phi\colon G \longrightarrow G'$, such that H is the kernel of ϕ?

Clearly a necessary condition is that H is normal in G. Somewhat surprisingly this trivially necessary condition is also in fact sufficient.

The idea is as follows. Given G and H there is an obvious map of *sets*, where H is the inverse image of a point. We just put X to be the collection of left cosets of H in G. Then there is an obvious function

$$\phi\colon G \longrightarrow X.$$

The map ϕ just does the obvious thing, it sends g to $\phi(g) = [g] = gH$, the left coset corresponding to g. The real question is, can we make X into a group?

Suppose that we are given two left cosets $[a] = aH$ and $[b] = bH$. The obvious way to try to define a multiplication in X is to set

$$(aH)(bH) = [a][b] = [ab] = (ab)H.$$

Unfortunately there is a problem with this attempt to define a multiplication. The problem is that the multiplication map is not necessarily well-defined.

To give an illustrative example of the problems that arise defining maps on equivalences classes by choosing representatives, consider the following example. Let Y be the set of all people and let $\sim$ be the equivalence relation such that $x \sim y$ iff x and y have the same colour eyes. Then the equivalence classes are simply all possible colours of people's eyes. We denote the set of all equivalence classes by $Y/\sim$. Consider trying to define a function,

$$f\colon Y/\sim \longrightarrow \mathbb{R},$$

on the equivalences classes to the real numbers. Given a colour, pick a person with that colour eyes, and send that colour to the height of that person.

This is clearly absurd. Given any colour, there are lots of people with that colour eyes, and nearly everyone's height will be different, so we don't get a well-defined function this way.

In fact the problem is that we might represent a left-coset in a different way. Suppose that $a'H = aH$ and $b'H = bH$, so that $[a'] = [a]$ and $[b'] = [b]$. Then we would also have another way to define the multiplication, that is

$$(a'H)(b'H) = [a'][b'] = [a'b'] = (a'b')H.$$

For the multiplication to be well-defined, we need

$$[a'b'] = [ab].$$

In other words we need that $a'b' \in abH$. Now we do know that $a' = ah$ and $b' = bk$ for h and $k \in H$. It follows then that

$$a'b' = (ah)(bk).$$

We want to manipulate the right hand side, until it is of the form abh' where $h' \in H$. Now in *general* it is *absolutely guaranteed* that this is going to fail. The point is, if this method did work, then there would be a homomorphism whose kernel is equal to H. So at the very least, we had better assume that H is normal in G.

Now we would like to move the b through the h. As H is normal in G, we have

$$b^{-1}Hb \subset H.$$

In particular $b^{-1}hb = l \in H$. Thus $hb = bl$. It follows that

$$\begin{aligned} a'b' &= (ah)(bk) \\ &= a(hb)k \\ &= a(bl)k \\ &= (ab)(lk) \\ &= (ab)h', \end{aligned}$$

where $h' = lk \in H$.

Thus, almost by a miracle, if H is normal in G, then the set of left cosets of H in G becomes a group.

Theorem 9.1. *Let G be a group and let H be a normal subgroup.*

Then the left cosets of H in G form a group, denoted G/H. G/H is called the **quotient of G modulo H**. *The rule of multiplication in G is defined as*

$$(aH)(bH) = abH.$$

Furthermore there is a **natural** *surjective homomorphism*

$$\phi\colon G \longrightarrow G/H,$$

defined as $\phi(g) = gH$. Moreover the kernel of ϕ is H.

Proof. We have already checked that this rule of multiplication is well-defined.

We check the three axioms for a group. We first check associativity. Suppose that a, b and c are in G. Then

$$\begin{aligned}(aH)(bHcH) &= (aH)(bcH)\\ &= (a(bc))H\\ &= ((ab)c)H\\ &= (ab)H(cH)\\ &= (aHbH)cH.\end{aligned}$$

Thus this rule of multiplication is associative.

It is easy to see that $eH = H$ plays the role of the identity. Indeed $aHeH = aeH = aH = eHaH$.

Finally given a left coset aH, $a^{-1}H$ is easily seen to be the inverse of aH.

Thus G/H certainly does form a group.

It is easy to see that ϕ is a surjective homomorphism. Finally the inverse image of the identity is equal to all those elements g of G such that $gH = H$. Almost by definition of an equivalence relation, it follows that $g \in H$, so that $\operatorname{Ker}\phi = H$. □

At this point it is useful to introduce a little bit of category theory:

Definition 9.2. *A category $\mathcal{C}$ consists of two things. The first is the* **objects** *of the category. The second is, given any two objects, X and Y, we associate a collection of* **morphisms**, *denoted* $\operatorname{Hom}(X, Y)$. *Given three objects, X, Y and Z and two morphisms $f \in Hom(X, Y)$, $g \in \operatorname{Hom}(Y, Z)$, there is a rule of composition,*

$$g \circ f \in \operatorname{Hom}(X, Z).$$

A category satisfies the following two axioms.

(1) Composition is associative. That is, given $f \in \operatorname{Hom}(X, Y)$, $g \in \operatorname{Hom}(Y, Z)$, $h \in \operatorname{Hom}(Z, W)$, we have

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

(2) There is an element $I_X \in \operatorname{Hom}(X, X)$ that acts as an identity, so that if $f \in \operatorname{Hom}(X, Y)$ and $g \in \operatorname{Hom}(Y, X)$ we have,

$$f \circ I_X = f,$$

and

$$I_X \circ g = g.$$

Given $f \in \operatorname{Hom}(X, Y)$ we say that $g \in \operatorname{Hom}(Y, X)$ is the inverse of f if $f \circ g = I_Y$ and $g \circ f = I_X$. In this case we say that f is an **isomorphism** *and we say that X and Y are* **isomorphic**.

Given most advanced mathematics classes, there is normally a naturally associated category.

For us, the most natural category is the category of groups. The objects are the collection of all groups and the morphisms are homomorphisms. Composition of morphisms is composition of functions. It is not hard to see that all the axioms are satisfied. In fact the only thing we have not checked is that composition of homomorphisms is a homomorphism, which is an exercise for the reader.

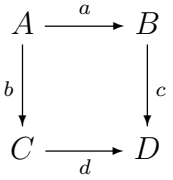
Two groups are isomorphic iff they are isomorphic as objects of the category.

Another very natural category is the category of sets. Here a morphism is any function.

Yet another category is the category of topological spaces. The objects are topological spaces and the morphisms are continuous maps. Two topological spaces are then homeomorphic iff they are isomorphic as objects of this category. The category of metric spaces is a subcategory of the category of topological spaces.

The category of vector spaces, is the category whose objects are vector spaces and whose morphisms are linear maps.

Definition 9.3. *Let*



be a collection of objects and morphisms belonging to a category.

We say that the diagram **commutes** *if the two morphisms from A to D are the same, that is*

$$c \circ a = d \circ b.$$

In a category, the focus of interest is not the objects, but the morphisms between the objects. In this sense, we would like to characterise the notion of the quotient group in a way that does not make explicit reference to the elements of G/H, but rather define everything in terms of homomorphisms between groups. Even though this is somewhat abstract, there is an obvious advantage to this approach; as a set G/H is rather complicated, its elements are left cosets, which are themselves sets. But really we only need to know what G/H is up to isomorphism.

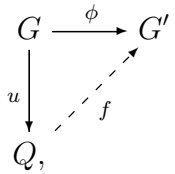
Definition 9.4. *Let G be a group and let H be a normal subgroup.*

The **categorical quotient** *of G by H is a group Q together with a homomorphism $u\colon G \longrightarrow Q$, such that*

- *the kernel of u is H.*

which is universal amongst all such homomorphisms in the following sense.

Suppose that $\phi\colon G \longrightarrow G'$ is any homomorphism such that the kernel of ϕ contains H. Then there is a unique induced homomorphism



which makes the diagram commute.

Note that in the definition of the categorical quotient, the most important part of the definition refers to the homomorphism u, and the universal property that it satisfies.

Theorem 9.5. *The category of groups admits categorical quotients.*

That is to say, given a group G and a normal subgroup H, there is a categorical quotient group Q. Furthermore, Q is unique, up to a unique isomorphism.

Proof. We first prove existence. Let G/H be the quotient group and let $u\colon G \longrightarrow G/H$ be the natural homomorphism. I claim that this pair forms a categorical quotient. Thus we have to prove that u is universal.

To this end, suppose that we are given a homomorphism $\phi\colon G \longrightarrow G'$, whose kernel contains H. Define a map

$$f\colon G/H \longrightarrow G'$$

by sending gH to $\phi(g)$. It is clear that the condition that the diagram commutes, forces this definition of f. We have to check that f is well-defined.

Suppose that $g_1H = g_2H$. We need to check that $\phi(g_1) = \phi(g_2)$. As $g_1H = g_2H$, it follows that $g_2 = g_1h$, for some $h \in H$. In this case

$$\begin{aligned}\phi(g_2) &= \phi(g_1h)\\ &= \phi(g_1)\phi(h)\\ &= \phi(g_1),\end{aligned}$$

where we used the fact that h is in the kernel of ϕ. Thus the map f is well-defined.

Now we check that f is a homomorphism. Suppose that x and y are in G/H. Then $x = g_1H$ and $y = g_2H$, for some g_1 and g_2 in G. In this

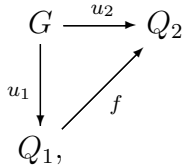
case

$$\begin{aligned} f(xy) &= f(g_1 g_2 H) \\ &= \phi(g_1 g_2) \\ &= \phi(g_1)\phi(g_2) \\ &= f(g_1 H) f(g_2 H) = f(x) f(y). \end{aligned}$$

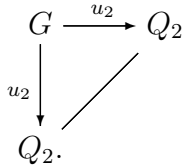
Thus f is a homomorphism. Finally we check that the diagram above commutes. Suppose that $g \in G$. Going along the top we get $\phi(g)$. Going down first, we get gH and then going diagonally we get $f(gH) = \phi(g)$, by definition of f. It is clear that f is the only map which makes the diagram commute.

Thus G/H is a categorical quotient. In particular categorical quotients exist.

Now we prove that categorical quotients are unique, up to unique isomorphism. Suppose that Q_1 and Q_2 are two such categorical quotients. As Q_1 is a categorical quotient and there is a homomorphism $u_2 \colon G \longrightarrow Q_2$ it follows that there is an induced homomorphism $f \colon Q_1 \longrightarrow Q_2$, which makes the following diagram commute



By symmetry there is a homomorphism $g \colon Q_2 \longrightarrow Q_1$, which makes the same diagram commute, with 1 and 2 switched. Consider the composition $f \circ g \colon Q_2 \longrightarrow Q_2$. This is a homomorphism which make the following diagram commute



However there is one homomorphism that makes the diagram commute, namely the identity. By uniqueness, $f \circ g$ must be the identity. Similarly $g \circ f$ must be the identity. So f and g are inverses of each other, and hence isomorphisms. Note that f itself is unique, since its existence was given to us by the universal property of u_1.

Thus the quotient is unique, up to a unique isomorphism. $\square$

18.703 Modern Algebra

Spring 2013