14. 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 $x \sim y$ if and only if x and y have the same colour hair. Then the equivalence classes are simply all possible colours of people's hair. 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 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 completely 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

$$bH = Hb.$$

In particular

$$hb \in Hb = bH,$$

so that we may find $l \in H$ such that $hb = bl$. 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 14.1. *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/H 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

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

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 $\operatorname{Ker} \phi = H$. □