5. Quotient groups I

Suppose that we are given one to one correspondence between a set S and a group G. Then we can make S into a group, using the correspondence and the fact that G is a group. If $\leftrightarrow$ denotes the correspondence, so that $s \leftrightarrow g$ just means that s corresponds to g then the product in S is described as follows:

$$\text{if} \quad s_1 \leftrightarrow g_1, \quad s_2 \leftrightarrow g_2 \quad \text{and} \quad t \leftrightarrow g_1 g_2 \quad \text{then} \quad s_1 s_2 = t.$$

Now suppose we use function notation, so that the correspondence is given by $\mu\colon S \longrightarrow G$. In this language we have that if

$$\text{if} \quad \mu(s_1) = g_1, \quad \mu(s_2) = g_2 \quad \text{and} \quad \mu(t) = g_1 g_2 \quad \text{then} \quad s_1 s_2 = t.$$

Note that then μ is an isomorphism of the group S, with the induced multiplication, and the group G.

Now suppose that we have a group homomorphism $\phi\colon G \longrightarrow G'$. We have already observed that the image $\phi[G]$ of G is in one to one correspondence with the set S of left cosets of H in G. Using the logic above, it follows that the set of left cosets becomes a group. We denote this group by G/H and call it G modulo H.

How does multiplication in G/H work? Well,

$$aH \leftrightarrow \phi(a) \qquad \text{and} \qquad bH \leftrightarrow \phi(b).$$

Now

$$\phi(a)\phi(b) = \phi(ab),$$

as we have a group homomorphism. So

$$abH \leftrightarrow \phi(a)\phi(b).$$

Therefore the group law on left cosets is:

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

Definition-Theorem 5.1. *Let $\phi\colon G \longrightarrow G'$ be a group homomorphism with kernel H.*

Then the set of left cosets forms a group G/H with multiplication defined by

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

Note that the identity coset is eH, since $\phi(e) = e'$. The inverse of aH is $a^{-1}H$, since the inverse of $\phi(a)$ is $\phi(a^{-1})$.

It is important to realise that this discussion hides an interesting subtlety. It is very unusual that we can define the product of two left cosets simply by choosing a representative from each coset. What is surprising is that using this method one comes out with a well-defined multiplication.

Compare this with the process of assigning a number to a letter by picking someone whose first name begins with that letter and then taking the height of that person in centimetres. This doesn't really make sense, since two people with the same first initial will usually have different heights.

Let's check by hand that the product above is well-defined. Suppose that $a'H = aH$ and $b'H = bH$. Then $a' = ah_1$ and $b' = bh_2$, for some h_1 and h_2. On the other hand, we may find $h_3 \in H$ so that

$$h_1 b = bh_3 \qquad \text{since} \qquad bH = Hb.$$

It follows that

$$\begin{aligned} a'b' &= (ah_1)(bh_2) \\ &= a(h_1 b)h_2 \\ &= a(bh_3)h_2 \\ &= (ab)(h_3 h_2). \end{aligned}$$

Thus

$$a'b'H = abH,$$

and the multiplication is indeed well-defined.

Example 5.2. *Let $\gamma\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$ be the map which sends an integer m to its remainder r modulo n, $\gamma(m) = r$.*

Then the kernel of γ is all multiples of n, $n\mathbb{Z}$ and the quotient group

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$$

For example, let's take the case of $n = 7$. The left cosets are

$$0 + 7\mathbb{Z}, \quad 1 + 7\mathbb{Z}, \quad 2 + 7\mathbb{Z}, \quad 3 + 7\mathbb{Z}, \quad 4 + 7\mathbb{Z}, \quad 5 + 7\mathbb{Z}, \quad 6 + 7\mathbb{Z}.$$

We have

$$(4 + 7\mathbb{Z}) + (6 + 7\mathbb{Z}) = 10 + 7\mathbb{Z} = 3 + 7\mathbb{Z}.$$

On the other hand

$$4 + 7\mathbb{Z} = -3 + 7\mathbb{Z} \qquad \text{and} \qquad 6 + 7\mathbb{Z} = 20 + 7\mathbb{Z},$$

and

$$(-3 + 7\mathbb{Z}) + (20 + 7\mathbb{Z}) = 17 + 7\mathbb{Z} = 3 + 7\mathbb{Z},$$

the same answer as before.