4. The kernel

We now come to the key:

Definition 4.1. *Let $\phi\colon G \longrightarrow G'$ be a group homomorphism. The* ***kernel*** *of ϕ, denoted $\operatorname{Ker}\phi$, is the inverse image of the identity,*

$$\operatorname{Ker}\phi = \phi^{-1}[\{e'\}] = \{\, g \in G \,|\, \phi(g) = e' \,\}.$$

By (3.10.4) the kernel is a subgroup of G.

Example 4.2. *Let $A \in M_{m,n}(\mathbb{R})$ be an $m \times n$ matrix with real entries. Define a map*

$$\phi\colon \mathbb{R}^n \longrightarrow \mathbb{R}^m \qquad \text{by the rule} \qquad \vec{v} \longrightarrow A\vec{v}.$$

We check that ϕ is a group homomorphism. Suppose that $\vec{v}$ and $\vec{w}$ are in $\mathbb{R}^n$. We have

$$\begin{aligned}\phi(\vec{v} + \vec{w}) &= A(\vec{v} + \vec{w})\\ &= A\vec{v} + A\vec{w}\\ &= \phi(\vec{v}) + \phi(\vec{w}).\end{aligned}$$

Thus ϕ is a group homomorphism. In this case the kernel of ϕ is the null space of A, the set of solutions to the homogeneous equation

$$A\vec{x} = \vec{0}.$$

Theorem 4.3. *Let $\phi\colon G \longrightarrow G'$ be a group homomorphism and let $H = \operatorname{Ker}\phi$.*

Then

$$\phi^{-1}[\{\phi(a)\}] = \{\, g \in G \,|\, \phi(g) = \phi(a) \,\} = aH = Ha.$$

In particular the partition of G into left cosets is exactly the same as the partition of G into right cosets.

Proof. We want to prove that

$$\{\, g \in G \,|\, \phi(g) = \phi(a) \,\} = aH.$$

We first show that the LHS is a subset of the RHS. Pick an element g of the LHS, so that $\phi(g) = \phi(a)$. Then, multiplying on the left by $\phi(a)^{-1}$, we have

$$\phi(a)^{-1}\phi(g) = e'.$$

By (3.10.2) we know that $\phi(a^{-1}) = \phi(a)^{-1}$ and so

$$e' = \phi(a^{-1})\phi(g) = \phi(a^{-1}g).$$

Thus $a^{-1}g \in H$. Therefore $a^{-1}g = h \in H$ so that $g = ah \in aH$. Thus the LHS is a subset of the RHS.

Now pick an element g of the RHS, so that $g \in aH$. Then we can find $h \in H$ so that $g = ah$. In this case $h = a^{-1}g$. We have

$$\begin{aligned} e' &= \phi(h) \\ &= \phi(a^{-1}g) \\ &= \phi(a^{-1})\phi(g) \\ &= \phi(a)^{-1}\phi(g). \end{aligned}$$

Multiplying both sides on the left by $\phi(a)$ we see that $\phi(g) = \phi(a)$. Thus the RHS is a subset of the LHS. Therefore

$$\{\, g \in G \mid \phi(g) = \phi(a) \,\} = aH.$$

By symmetry

$$\{\, g \in G \mid \phi(g) = \phi(a) \,\} = Ha.$$

This is the first statement.

We want to show that the left cosets and the right cosets give the same partition. Pick $a \in G$. Then a belongs to a left coset and a right coset and we just have to show they are the same. But

$$aH = \{\, g \in G \mid \phi(g) = \phi(a) \,\} = Ha.$$

This is the second statement. □

One can rephrase the first part of (4.3) as follows. The inverse image of any element of $\phi[G]$ is a left coset of H. For example if H is finite then the inverse image of every point of $\phi[G]$ has the same size, the number of elements of H.

Another way to state the second part is that the elements of $\phi[G]$ are nothing more than the left cosets of H. In fact the elements of $\phi[G]$ are also the right cosets of H.

Example 4.4. *Let $\phi\colon \mathbb{C}^* \longrightarrow \mathbb{R}^+$ be the map which sends a non-zero complex number to its modulus, $\phi(z) = |z|$.*

Here $\mathbb{C}^* = \mathbb{C} - \{0\}$ and $\mathbb{R}^+$ is the set of positive real numbers under multiplication. The modulus of a complex number is the distance to the origin; if we use polar coordinates to represent the complex number as $z = re^{i\theta}$, then $|z| = r$.

Then ϕ is a group homomorphism.

$$\begin{aligned} \phi(z_1 z_2) &= |z_1 z_2| \\ &= |z_1||z_2| \\ &= \phi(z_1)\phi(z_2). \end{aligned}$$

The identity in $\mathbb{R}^+$ is 1 so the kernel U of ϕ consists of all complex numbers of modulus one. This is the unit circle in the complex plane. The inverse image of the real number r is all complex numbers of modulus r; this is a circle of radius r centred at the origin.

Example 4.5. *Recall we defined a map in (3.8)*

$$\gamma\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n \qquad \text{by the rule} \qquad \gamma(m) = r,$$

where r is the remainder after you divide n into m,

The kernel of ϕ is all integers with zero remainder, that is, all integers divisible by n. The inverse image of 1 is the set of all integers with remainder one. Any such integer is 1 plus a multiple of n. More generally the inverse image of r is the set of all integers with remainder r. Any such integer is r plus a multiple of n.

Corollary 4.6. *A group homomorphism $\phi\colon G \longrightarrow G'$ is one to one if and only if* $\operatorname{Ker}\phi = \{e\}$.

Proof. One direction is clear. If ϕ is one to one then the inverse image of e' contains only one element, e, so that $\operatorname{Ker}\phi = \{e\}$.

Now suppose that $\operatorname{Ker}\phi = \{e\}$. Then (4.3) implies that the inverse image of $\phi(a)$ is the coset $aH = \{a\}$. Thus ϕ is one to one. $\square$

Definition 4.7. *A subgroup H of G is called **normal** if $gH = Hg$, that is, the left coset containing g is the same as the right coset containing g, for all $g \in G$.*

Corollary 4.8. *If $\phi\colon G \longrightarrow G'$ is a group homomorphism then the kernel is a normal subgroup of G.*

Proof. This is the second statement of (4.3). $\square$