8. Homomorphisms and kernels

An isomorphism is a bijection which respects the group structure, that is, it does not matter whether we first multiply and take the image or take the image and then multiply. This latter property is so important it is actually worth isolating:

Definition 8.1. *A map $\phi\colon G \longrightarrow H$ between two groups is a* **homomorphism** *if for every g and h in G,*

$$\phi(gh) = \phi(g)\phi(h).$$

Here is an interesting example of a homomorphism. Define a map

$$\phi\colon G \longrightarrow H$$

where $G = \mathbb{Z}$ and $H = \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ is the standard group of order two, by the rule

$$\phi(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd.} \end{cases}$$

We check that ϕ is a homomorphism. Suppose that x and y are two integers. There are four cases. x and y are even, x is even, y is odd, x is odd, y is even, and x and y are both odd.

Now if x and y are both even or both odd, then $x + y$ is even. In this case $\phi(x+y) = 0$. In the first case $\phi(x) + \phi(y) = 0 + 0 = 0$ and in the second case $\phi(x) + \phi(y) = 1 + 1 = 0$.

Otherwise one is even and the other is odd and $x + y$ is odd. In this case $\phi(x + y) = 1$ and $\phi(x) + \phi(y) = 1 + 0 = 1$. Thus we get a homomorphism.

Here are some elementary properties of homomorphisms.

Lemma 8.2. *Let $\phi\colon G \longrightarrow H$ be a homomorphism.*

(1) $\phi(e) = f$, that is, ϕ maps the identity in G to the identity in H.
(2) $\phi(a^{-1}) = \phi(a)^{-1}$, that is, ϕ maps inverses to inverses.
(3) If K is subgroup of G, then $\phi(K)$ is a subgroup of H.

Proof. Let $a = \phi(e)$, where e is the identity in G. Then

$$\begin{aligned} a &= \phi(e) \\ &= \phi(ee) \\ &= \phi(e)\phi(e) \\ &= aa. \end{aligned}$$

Thus $a^2 = a$. Cancelling we get $a = f$, the identity in H. Hence (1).

Let $b = a^{-1}$.

$$\begin{aligned} f &= \phi(e) \\ &= \phi(ab) \\ &= \phi(a)\phi(b), \end{aligned}$$

and

$$\begin{aligned} f &= \phi(e) \\ &= \phi(ba) \\ &= \phi(b)\phi(a). \end{aligned}$$

But then $\phi(b)$ is the inverse of $\phi(a)$, so that $\phi(a^{-1}) = \phi(a)^{-1}$. Hence (2).

Let $X = \phi(K)$. It suffices to check that X is non-empty and closed under products and inverses. X contains f the identity of H, by (1). X is closed under inverses by (2) and closed under products, almost by definition. Thus X is a subgroup. □

Instead of looking at the image, it turns out to be much more interesting to look at the inverse image of the identity.

Definition-Lemma 8.3. *Let $\phi\colon G \longrightarrow H$ be a group homomorphism. The* **kernel of** *ϕ, denoted* $\operatorname{Ker}\phi$*, is the inverse image of the identity.*

Then $\operatorname{Ker}\phi$ *is a subgroup of G.*

Proof. We have to show that the kernel is non-empty and closed under products and inverses.

Note that $\phi(e) = f$ by (8.2). Thus $\operatorname{Ker}\phi$ is certainly non-empty. Now suppose that a and b are in the kernel, so that $\phi(a) = \phi(b) = f$.

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) \\ &= ff \\ &= f. \end{aligned}$$

Thus $ab \in \operatorname{Ker}\phi$ and so the kernel is closed under products. Finally suppose that $\phi(a) = e$. Then $\phi(a^{-1}) = \phi(a)^{-1} = f$, where we used (8.2). Thus the kernel is closed under inverses, and the kernel is a subgroup. □

Here are some basic results about the kernel.

Lemma 8.4. *Let $\phi\colon G \longrightarrow H$ be a homomorphism.*

Then f is injective iff $\operatorname{Ker}\phi = \{e\}$.

Proof. If f is injective, then at most one element can be sent to the identity $f \in H$. Since $\phi(e) = f$, it follows that $\operatorname{Ker}\phi = \{e\}$.

Now suppose that $\operatorname{Ker}\phi = \{e\}$ and suppose that $\phi(x) = \phi(y)$. Let $g = x^{-1}y$. Then

$$\begin{aligned}\phi(g) &= \phi(x^{-1}y)\\ &= \phi(x)^{-1}\phi(y)\\ &= f.\end{aligned}$$

Thus g is in the kernel of ϕ and so $g = e$. But then $x^{-1}y = e$ and so $x = y$. But then ϕ is injective. □

It turns out that the kernel of a homomorphism enjoys a much more important property than just being a subgroup.

Definition 8.5. *Let G be a group and let H be a subgroup of G.*

We say that H is **normal** *in G and write $H \lhd G$, if for every $g \in G$, $gHg^{-1} \subset H$.*

Lemma 8.6. *Let $\phi\colon G \longrightarrow H$ be a homomorphism.*

Then the kernel of ϕ is a normal subgroup of G.

Proof. We have already seen that the kernel is a subgroup. Suppose that $g \in G$. We want to prove that

$$g \operatorname{Ker}\phi g^{-1} \subset \operatorname{Ker}\phi.$$

Suppose that $h \in \operatorname{Ker}\phi$. We need to prove that $ghg^{-1} \in \operatorname{Ker}\phi$.

Now

$$\begin{aligned}\phi(ghg^{-1}) &= \phi(g)\phi(h)\phi g^{-1}\\ &= \phi(g)f\phi(g)^{-1}\\ &= \phi(g)\phi(g)^{-1} = f.\end{aligned}$$

Thus $ghg^{-1} \in \operatorname{Ker}\phi$. □

It is interesting to look at some examples of subgroups, to see which are normal and which are not.

Lemma 8.7. *Let G be an abelian group and let H be any subgroup.*

Then H is normal in G.

Proof. Clear, as for every $h \in H$ and $g \in G$,

$$ghg^{-1} = h \in H.$$ □

So let us look at the first interesting example of a group which is not abelian.

Take $G = D_3$. Let us first look at $H = \{I, R, R^2\}$. Then H is normal in G. In fact, pick $g \in D_3$. If g belongs to H, there is nothing to prove. Otherwise g is a flip. Let us suppose that it is F_1. Now pick $h \in H$ and consider ghg^{-1}. If $h = I$ then it is clear that $ghg^{-1} = I \in H$.

So suppose that $h = R$. Then

$$\begin{aligned} ghg^{-1} &= F_1 R F_1 \\ &= R^2 \in H. \end{aligned}$$

Similarly, if $h = R^2$, then $ghg^{-1} = R \in H$.

Thus H is normal in G.

Now suppose that $H = \{I, F_1\}$. Take $h = F_1$ and $g = R$. Then

$$\begin{aligned} ghg^{-1} &= RF_1R^2 \\ &= F_2. \end{aligned}$$

So $gHg^{-1} \neq H$.

Lemma 8.8. *Let H be a subgroup of a group G.*

TFAE

(1) H is normal in G.
(2) For every $g \in G$, $gHg^{-1} = H$.
(3) $Ha = aH$, for every $a \in G$.
(4) The set of left cosets is equal to the set of right cosets.
(5) H is a union of conjugacy classes.

Proof. Suppose that (1) holds. Suppose that $g \in G$. Then

$$gHg^{-1} \subset H.$$

Now replace g with $g-1$, then

$$g^{-1}Hg \subset H,$$

so that multiplying on the left by g^{-1} and the right by g

$$H \subset gHg^{-1}.$$

But then (2) holds.

If (2) holds, then (3) holds, simply by multiplying the equality

$$aHa^{-1} = H,$$

on the right by a.

If (3) holds, then (4) certainly holds.

Suppose that (4) holds. Let $g \in G$. Then $g \in gH$ and $g \in Hg$. If the set of left cosets is equal to the set of right cosets, then this means

$gH = Hg$. Now take this equality and multiply it on the right by g^{-1}. Then certainly $gHg^{-1} \subset H$, so that H is normal in G. Hence (1).

Thus (1), (2), (3) and (4) are all equivalent.

Suppose that (5) holds. Then $H = \cup A_i$, where A_i are conjugacy classes. Then

$$\begin{aligned} gHg^{-1} &= \cup gA_ig^{-1} \\ &= \cup A_i \\ &= H. \end{aligned}$$

Thus H is normal.

Finally suppose that (2) holds. Suppose that $a \in H$ and that A is the conjugacy class to which a belongs. Pick $b \in A$. Then there is an element $g \in G$ such that $gag^{-1} = b$. Then $b \in gHg^{-1} = H$. So $A \subset H$. But then H is a union of conjugacy classes. $\square$

Using this the example above becomes much easier with S_3. In the first case we are looking at $H = \{e, (1, 2, 3), (1, 3, 2)\}$. In this case H is in fact a union of conjugacy classes. (Recall that the conjugacy classes of S_n are entirely determined by the cycle type). So H is obviously normal. Now take $H = \{e, (1, 2)\}$, and let $g = (2, 3)$. Then

$$\begin{aligned} gHg^{-1} &= \{geg^{-1}, g(1, 2)g^{-1}\} \\ &= \{e, (1, 3)\}. \end{aligned}$$

Thus H is not normal in this case.

Given this, we can give one more interesting example of a normal subgroup.

Let $G = S_4$. Then let $H = \{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$. We have already seen that H is a subgroup of G. On the other hand, H is a union of conjugacy classes. Indeed the three non-trivial elements of H represent the only permutations with cycle type $(2, 2)$. Thus H is normal in G.