3. Homomorphisms

We would like a way to compare two groups. One possibility way to compare is to ask if two groups are isomorphic but this is far too strong and so not a very interesting comparison. If G is a group and H is a subgroup then there is a natural inclusion map $i\colon H \longrightarrow G$; this map sends h to h. This map is not an isomorphism (unless $H = G$) but in some intuitively obvious fashion H is smaller than G and the map i reflects this fact.

Even if i is not onto it does respect the group structure in H and G, since to multiply in H, simply multiply in G. The idea then is to write down the definition of an isomorphism and just forget the conditions that the map is one to one and onto.

Definition 3.1. *Let $\phi\colon G \longrightarrow G'$ be a map between two groups. We say that ϕ is a **(group) homomorphism** if*

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

for all a and $b \in G$.

In words, we can multiply in G and apply ϕ, or we can apply ϕ and multiply in G' and either way the answer is the same. It is easy to see that the inclusion map above is a group homomorphism.

Given any two groups G and G' there is always at least one group homomorphism from G to G'. It is the map which sends every element of G to the identity in G'. It is not hard to see that this map is always a group homomorphism.

Lemma 3.2. *Let $\phi\colon G \longrightarrow G'$ be a group homomorphism.*

If G is abelian and ϕ is onto then G' is abelian.

Proof. Suppose that a' and b' are elements of G'. As ϕ is onto we may find elements a and b of G such that $\phi(a) = a'$ and $\phi(b) = b'$. We have

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

Therefore G' is abelian. □

Example 3.3. *Let $\phi\colon S_n \longrightarrow \mathbb{Z}_2$ be the map which sends a permutation to zero if the permutation is even and to one if the permutation is odd.*

We check that ϕ is a group homomorphism. We have to check that

$$\phi(\rho\sigma) = \phi(\rho) + \phi(\sigma).$$

There are four cases. If ρ and σ are both even then ρ and σ are a product of an even number of transpositions. In this case $\rho\sigma$ is also a product of an even number of transpositions. Thus all three permutations are even and we are reduced to checking

$$0 = 0 + 0$$

which is surely okay. The other cases are just as easy. Thus ϕ is a group homomorphism.

Example 3.4. *Let F be the group of all functions from $\mathbb{R}$ to $\mathbb{R}$ under pointwise addition. Let $c \in \mathbb{R}$ be any real number. Define a map*

$$\phi_c \colon F \longrightarrow \mathbb{R}$$

by the rule $\phi_c(f) = f(c)$.

Suppose that f and $g \in F$. Recall that $f + g$ is the function which sends x to $f(x) + g(x)$. We have

$$\begin{aligned} \phi_c(f+g) &= (f+g)(c) \\ &= f(c) + g(c) \\ &= \phi_c(f) + \phi_c(g). \end{aligned}$$

Thus ϕ is a group homomorphism.

Example 3.5. *Let $\mathrm{GL}(n, \mathbb{R})$ be the group of all invertible $n \times n$ matrices with real entries under multiplication. Define a map*

$$\phi \colon \ \mathrm{GL}(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$$

by sending a matric A to its determinant $\det A$.

Suppose that A and $B \in \mathrm{GL}(n, \mathbb{R})$. We have

$$\begin{aligned} \phi(AB) &= \det(AB) \\ &= \det A \det B \\ &= \phi(A)\phi(B). \end{aligned}$$

Thus ϕ is a group homomorphism.

Example 3.6. *Let $r \in \mathbb{Z}$ be an integer and let*

$$\phi \colon \mathbb{Z} \longrightarrow \mathbb{Z} \qquad \text{be given by} \qquad n \longrightarrow rn.$$

Suppose that m and $n \in \mathbb{Z}$. We have

$$\begin{aligned}\phi(m+n) &= r(m+n)\\ &= rm + rn\\ &= \phi(m) + \phi(n).\end{aligned}$$

Thus ϕ is a group homomorphism.

Example 3.7. *Let $H \times G$ be the product of two groups. Define a map by the rule*

$$\pi\colon H \times G \longrightarrow H \qquad \textit{by the rule} \qquad (h, g) \longrightarrow h.$$

Suppose that $(h_i, g_i) \in H \times G$. We have

$$\begin{aligned}\pi(h_1, g_1)(h_2, g_2) &= \pi(h_1h_2, g_1g_2)\\ &= h_1h_2\\ &= \pi(h_1, g_1)\pi(h_2, g_2).\end{aligned}$$

Thus π is a group homomorphism.

Example 3.8. *Define*

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

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

Suppose that $s_i \in \mathbb{Z}$. Then we can find q_i and r_i such that

$$s_i = q_i n + r_i \qquad \text{where} \qquad 0 < r_i < n,$$

$i = 1$ and 2. Here q_i is the quotient and r_i is the remainder when you divide n into s_i.

We may also write

$$r_1 + r_2 = q_3 n + r_3.$$

Adding these equations together we get:

$$s_1 + s_2 = (q_1 + q_2)n + r_1 + r_2 = (q_1 + q_2 + q_3)n + r_3.$$

Now $\gamma(s_i) = r_i$. Therefore we have

$$\begin{aligned}\gamma(s_1 + s_2) &= r_3\\ &= r_1 + r_2\\ &= \gamma(s_1) + \gamma(s_2),\end{aligned}$$

where all of the equalities take place in $\mathbb{Z}_n$. Thus γ is a group homomorphism.

One can also check that the composition of group homomorphisms is a group homomorphism. In other words, if we have $\phi\colon G \longrightarrow G'$ and $\psi\colon G' \longrightarrow G''$ two group homomorphisms then the composition $\psi \circ \phi\colon G \longrightarrow G''$ is a group homomorphism.

Definition 3.9. *Let $\phi\colon X \longrightarrow Y$ be a map of sets. If A is a subset of X the* ***image*** *of A, denoted $\phi[A]$, is*

$$\phi[A] = \{\, \phi(a) \,|\, a \in A, \} \subset Y.$$

The image of X, $\phi[X]$, is called the ***range*** *of ϕ.*

If B is a subset of Y the ***inverse image*** *of B, denoted $\phi^{-1}[B]$, is*

$$\phi^{-1}[B] = \{\, x \in X \,|\, \phi(x) \in B, \} \subset X.$$

Theorem 3.10. *Let $\phi\colon G \longrightarrow G'$ be a homomorphism of groups.*

(1) If e is the identity in G then $\phi(e) = e'$ is the identity in G'.
(2) If $a \in G$ then $\phi(a^{-1}) = \phi(a)^{-1}$.
(3) If H is a subgroup of G then $\phi[H]$ is a subgroup of G'.
(4) If K' is a subgroup of G' then $\phi^{-1}[K']$ is a subgroup of G.

Proof. Suppose that $a \in G$. We have

$$\phi(a) = \phi(ae) = \phi(a)\phi(e).$$

Multiplying both sides on the left by $\phi(a)^{-1}$ we get that $\phi(e) = e'$. This is (1).

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

Multiplying both sides on the left by $\phi(a)^{-1}$ we get that $\phi(a^{-1}) = \phi(a)^{-1}$. This is (2).

Suppose that $\phi(a)$ and $\phi(b)$ are two elements of $\phi[H]$, where a and b are two elements of H. Then

$$\phi(a)\phi(b) = \phi(ab) \in \phi[H],$$

as $ab \in H$. Thus $\phi[H]$ is closed under composition. $e' = \phi(e) \in \phi[H]$. Finally, $\phi(a)^{-1} = \phi(a^{-1}) \in \phi[H]$ and so $\phi[H]$ is closed under inverses. Thus $\phi[H]$ is a subgroup. This is (3).

Suppose that a and $b \in \phi^{-1}[K']$. Then $\phi(a)$ and $\phi(b) \in K'$. It follows that

$$\phi(ab) = \phi(a)\phi(b) \in K'.$$

Thus $ab \in \phi^{-1}[K']$ and so $\phi^{-1}[K']$ is closed under composition. $\phi(e) = e'$ and so $e' \in \phi^{-1}[K']$. If $a \in \phi^{-1}[K']$ then

$$\phi(a^{-1}) = \phi(a)^{-1} \in K',$$

and so $a^{-1} \in K'$. Thus $\phi^{-1}[K']$ is closed under inverses. Thus $\phi^{-1}[K']$ is a subgroup. This is (4). $\square$