Chapter 4

Normal subgroups and quotient groups

4.1 Group Homomorphisms

Many areas of mathematics involve the study of functions between sets that are of interest. Generally we are not interested in *all* functions but only those that interact well with particular properties or themes - for example in calculus we are usually interested in continuous or maybe differentiable functions - these are the ones to which the principles of calculus apply. In linear algebra, we don't study all functions between vector spaces, we study the ones that preserve addition and multiplcation by scalars, and refer to these as *linear transformations*. Likewise in group theory, we are interested in functions between groups that preserve the group operations in the sense of the following definition.

Definition 4.1.1. *Let* G *and* H *be groups with operations* $\star_G$ *and* $\star_H$ *respectively. A function* $\phi : G \to H$ *is a* group homomorphism *if for all elements* x *and* y *of* G

$$\phi(x \star_G y) = \phi(x) \star_H \phi(y).$$

This is saying that $\phi : G \to H$ is a group homomorphism if for any pair of elements x and y of G, combining them in G and then applying ϕ always gives the same result as separately applying ϕ to the two of them and then combining their images using the group operation in H.

EXAMPLES OF GROUP HOMOMORPHISMS

1. **The Determinant**
   Let $\mathbb{Q}^{\times}$ denote the group of non-zero rational numbers under multiplication, and as usual let $GL(3, \mathbb{Q})$ denote the group of invertible 3×3 matrices with rational entries, under multiplication.

   The function $\det : GL(3, \mathbb{Q}) \to \mathbb{Q}^{\times}$ that sends every matrix to its determinant is a group homomorphism, since $\det(AB) = \det(A)\det(B)$ if A and B are 3×3 matrices with rational entries.

2. Let H denote the group $\{1, -1\}$ under multiplication (the 1 and -1 here are just the ordinary numbers 1 and -1, H is a group of order 2). We may define a function ϕ from the group $\mathbb{Z}$ of integers under addition to H by

   $$\phi(n) = \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases}$$

   Then ϕ is a group homomorphism. To see this suppose that m and n are elements of $\mathbb{Z}$. There are four cases to check.

   - If m and n are both even then so is $m + n$ and

     $$\phi(m)\phi(n) = 1 \times 1 = 1 = \phi(m + n).$$

- If m is even and n is odd then $m+n$ is odd and

$$\phi(m)\phi(n) = 1 \times (-1) = -1 = \phi(m+n).$$

- If m is odd and n is even then $m+n$ is odd and

$$\phi(m)\phi(n) = (-1) \times 1 = -1 = \phi(m+n).$$

- If m and n are both odd then $m+n$ is even and

$$\phi(m)\phi(n) = (-1) \times (-1) = 1 = \phi_n(m+n).$$

3. The function τ from $\mathbb{Z}$ to $\mathbb{Z}$ defined for $a \in \mathbb{Z}$ by $\tau(a) = 3a$ is a homomorphism from the additive group $(\mathbb{Z}, +)$ to itself. To see this, note for $a, b \in \mathbb{Z}$ that

$$\tau(a+b) = 3(a+b) = 3a + 3b = \tau(a) + \tau(b).$$

Exercise: Show that the function f from $\mathbb{Z}$ to $\mathbb{Z}$ defined for $a \in \mathbb{Z}$ by $f(a) = a + 1$ is *not* a group homomorphism (from $(\mathbb{Z}, +)$ to itself).

If $\phi : G \to H$ *is* a group homomorphism, then there is a subgroup of G and a subgroup of H naturally associated with ϕ. These are defined below.

Definition 4.1.2. *Suppose that $\phi : G \to H$ is a homomorphism of groups. Then*

1. *The* kernel *of ϕ is the subset of G consisting of all those elements whose image under ϕ is id_H.*

$$\ker\phi = \{g \in G : \phi(g) = \mathrm{id}_H\}.$$

2. *The* image *of ϕ is the subset of H consisting of all those elements that are the images under ϕ of elements of G.*

$$\mathrm{Im}\phi = \{h \in H : h = \phi(g) \text{ for some } g \in G\}.$$

It is fairly routine to prove that the kernel and image of ϕ are not only subsets but subgroups of G and H respectively. This is the content of the next two lemmas.

Lemma 4.1.3. *Suppose that $\phi : G \to H$ is a homomorphism of groups. Then $\ker\phi$ is a subgroup of G.*

Proof. First we show that $\mathrm{id}_G \in \ker\phi$. Let $g \in G$ and let $h = \phi(g)$ in H. Then

$$h = \phi(g) = \phi(\mathrm{id}_G \star_G g) = \phi(\mathrm{id}_G) \star_H \phi(g) = \phi(\mathrm{id}_G) \star_H h.$$

Thus $\phi(\mathrm{id}_G)$ is an element of H that satifies

$$h = \phi(\mathrm{id}_G) \star_H h$$

for some element h of H. Multiplying both sides of the above equation on the right by h^{-1}, it follows that $\phi(\mathrm{id}_G) = \mathrm{id}_H$ and hence that $\mathrm{id}_G \in \ker\phi$.

Now suppose that $g_1, g_2 \in \ker\phi$. Then

$$\phi(g_1 \star_G g_2) = \phi(g_1) \star_H \phi(g_2) = \mathrm{id}_H \star_H \mathrm{id}_H = \mathrm{id}_H.$$

Hence $g_1 \star_G g_2 \in \ker\phi$ and $\ker\phi$ is closed uder the operation of G.

Finally let $g \in \ker\phi$. We need to show that $g^{-1} \in \ker\phi$ aswell. We know that $\phi(g) = \mathrm{id}_H$ and (from above) that $\phi(\mathrm{id}_G) = \mathrm{id}_H$. Now

$$\begin{aligned}
\mathrm{id}_H &= \phi(\mathrm{id}_G) \\
&= \phi(g \star_G g^{-1}) \\
&= \phi(g) \star_H \phi(g^{-1}) \\
&= \mathrm{id}_H \star_H \phi(g^{-1}) \\
&= \phi(g^{-1}).
\end{aligned}$$

Thus $g^{-1} \in \ker\phi$, as required. □

Remark: Note that the last part of the above proof shows that $\phi(g)$ and $\phi(g^{-1})$ are inverses of each other in H, for any element g of G.

Lemma 4.1.4. *Suppose that* $\phi : G \to H$ *is a homomorphism of groups. Then* $\mathrm{Im}\phi$ *is a subgroup of* H.

Proof. From the proof of Lemma 4.1.3 above we know that $\phi(\mathrm{id}_G) = \mathrm{id}_H$, so $\mathrm{id}_H \in \mathrm{Im}\phi$.
Suppose that $h_1, h_2 \in \mathrm{Im}\phi$. Then $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$ for some elements g_1 and g_2 of G. Then

$$\phi(g_1 \star_G g_2) = \phi(g_1) \star_H \phi(g_2) = h_1 \star_H h_2,$$

so $h_1 \star_H h_2 \in \mathrm{Im}\phi$ and $\mathrm{Im}\phi$ is closed under $\star_H$.

Finally suppose $h \in \mathrm{Im}\phi$. We need to show that $h^{-1} \in \mathrm{Im}\phi$ also. We know that $h = \phi(g)$ for some $g \in G$, and it then follows from the Remark above that $h^{-1} = \phi(g^{-1})$. □

Examples

1. *The Determinant*
   The kernel of the function $\det : GL(3, \mathbb{Q}) \to \mathbb{Q}^\times$ that sends every matrix to its determinant is the subgroup consisting of all those matrices of determinant 1 in $GL(3, \mathbb{Q})$. This is denoted $SL(3, \mathbb{Q})$ and called the *special linear group* of 3×3 matrices over $\mathbb{Q}$.

   The image of det is the full group $\mathbb{Q}^\times$ of non-zero rational numbers, since every non-zero rational number arises as the determinant of some 3×3 matrix with rational entries.

2. *The "parity function" for integers*
   Let $\phi : \mathbb{Z} \to \{1, -1\}$ be defined by by

   $$\phi(n) = \begin{cases} 1 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd} \end{cases}$$

   Then the kernel of ϕ is $2\mathbb{Z}$, the group of even integers in $\mathbb{Z}$. The image of ϕ is $\{1, -1\}$.

3. The homomorphism τ from $(\mathbb{Z}, +)$ to $(\mathbb{Z}, +)$ defined for $a \in \mathbb{Z}$ by $\tau(a) = 3a$ has trivial kernel $\{0\}$, and its image is the subgroup of $(\mathbb{Z}, +)$ consisting of all multiples of 3.