Homomorphisms

1 Definition and examples

Recall that, if G and H are groups, an *isomorphism* $f\colon G \to H$ is a bijection $f\colon G \to H$ such that, for all $g_1, g_2 \in G$,

$$f(g_1 g_2) = f(g_1) f(g_2).$$

There are many situations where we are given a function $f\colon G \to H$, which is not necessarily a bijection, but such that f still satisfies the functional equation $f(g_1 g_2) = f(g_1) f(g_2)$. We make this a definition:

Definition 1.1. Let G and H be groups. A *homomorphism* $f\colon G \to H$ is a function $f\colon G \to H$ such that, for all $g_1, g_2 \in G$,

$$f(g_1 g_2) = f(g_1) f(g_2).$$

Example 1.2. There are many well-known examples of homomorphisms:

1. Every isomorphism is a homomorphism.
2. If H is a subgroup of a group G and $i\colon H \to G$ is the inclusion, then i is a homomorphism, which is essentially the statement that the group operations for H are induced by those for G. Note that i is always injective, but it is surjective $\iff H = G$.
3. The function $f\colon G \to H$ defined by $f(g) = 1$ for all $g \in G$ is a homomorphism (the *trivial homomorphism*). Note that f is not injective if G is not the trivial group and it is not surjective if H is not the trivial group.
4. The determinant $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism. This is the content of the identity $\det(AB) = \det A \det B$. Here det is surjective, since , for every nonzero real number t, we can find an invertible $n \times n$ matrix A much that $\det A = t$. For example, one can take A to be the diagonal matrix satisfying $A\mathbf{e}_1 = t\mathbf{e}_1$, and $A\mathbf{e}_i = \mathbf{e}_i$ for $i > 1$. However, det is not injective for $n \geq 2$.

5. (The complex exponential.) Define $f\colon \mathbb{C} \to \mathbb{C}^*$ by

$$f(z) = e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

Here, if $z = x + iy$, then

$$e^z = e^x e^{iy} = e^x(\cos y + i \sin y).$$

The fact that f is a homomorphism follows from the identity

$$e^{z_1+z_2} = e^{z_1} e^{z_2}.$$

The complex exponential is surjective: every element of $\mathbb{C}^*$ is of the form e^z for some $z \in \mathbb{Z}$. But it is not injective. In fact, $e^{z_1} = e^{z_2} \iff z_2 = z_1 + 2n\pi i$ for some $n \in \mathbb{Z}$. This is in contrast to the real exponential $e^x\colon \mathbb{R} \to \mathbb{R}^*$ is injective but not surjective (its image is the subgroup of positive real numbers).

6. The absolute value function $f\colon \mathbb{C}^* \to \mathbb{R}^*$ is a homomorphism, since

$$|z_1 z_2| = |z_1||z_2|.$$

Here f is not surjective, since its image is the set of positive real numbers. It is also not injective: $f(z_1) = f(z_2) \iff |z_1| = |z_2| \iff u = z_2/z_1$ has absolute value 1, i.e. is an element of $U(1) \iff$ there exists a $u \in U(1)$ such that $z_2 = uz_1$.

7. The sign function $\operatorname{sign}\colon \mathbb{R}^* \to \{\pm 1\}$ defined by

$$\operatorname{sign}(x) = \frac{x}{|x|} = \begin{cases} +1, & \text{if } x > 0; \\ -1, & \text{if } x < 0. \end{cases}$$

8. If $F\colon \mathbb{R}^n \to \mathbb{R}^m$ is a linear map, corresponding to the matrix A, then F is a homomorphism.

9. Given an integer n, the function $f\colon \mathbb{Q}^* \to \mathbb{Q}^*$ defined by $f(t) = t^n$, is a homomorphism, since $f(t_1 t_2) = f(t_1) f(t_2)$. The corresponding functions $f\colon \mathbb{R}^* \to \mathbb{R}^*$ and $\mathbb{C}^* \to \mathbb{C}^*$, are also homomorphisms. More generally, if G is an **abelian** group (written multiplicatively) and $n \in \mathbb{Z}$ is a fixed integer, then the function $f\colon G \to G$ defined by $f(g) = g^n$

is a homomorphism, by the laws of exponents for an abelian group: for all $g, h \in G$,

$$f(gh) = (gh)^n = g^n h^n = f(g)f(h).$$

For example, if $G = \mathbb{R}^*$ and $n \in \mathbb{N}$, then f is injective and surjective if n is odd. If n is even, then $(-t)^n = t^n$, so that f is not injective, and the image of f is the set of positive real numbers, so that f is also not surjective.

10. Let G be a group (written multiplicatively) and let $g \in G$ be fixed. Then the function $f\colon \mathbb{Z} \to G$ defined by $f(n) = g^n$ is a homomorphism (laws of exponents). A special case of this example is the homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $f(a) = [a] = a \cdot [1]$. A related example is the function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $f([a]_n) = [a]_m$. Note that f is only well-defined if m divides n. Under this assumption,

$$f([a]_n + [b]_n) = f([a+b]_n) = [a+b]_m = [a]_m + b]_m = f([a]_n) + f([b]_n),$$

so that f is a (surjective) homomorphism.

11. If G_1 and G_2 are two groups, and $G_1 \times G_2$ is the product group, then $\pi_1\colon G_1 \times G_2 \to G_1$, defined by $\pi_1(g_1, g_2) = g_1$, is a homomorphism. This is a consequence of the way the group operation is defined in the product:

$$\pi_1((g_1, g_2)(h_1, h_2)) = \pi_1(g_1h_1, g_2h_2) = g_1h_1 = \pi_1(g_1, g_2)\pi_1(h_1, h_2).$$

Similarly, the function $\pi_2\colon G_1 \times G_2 \to G_2$, defined by $\pi_1(g_1, g_2) = g_2$, is a homomorphism. We call π_1 and π_2 the *projections onto the first and second factors*.

12. The function $P\colon S_n \to GL_n(\mathbb{R})$ discussed in class, defined by

$$P(\sigma)(\mathbf{e}_i) = \mathbf{e}_{\sigma(i)}$$

is a homomorphism.

13. For the group S_n, the sign function $\varepsilon\colon S_n \to \{\pm 1\}$ is a homomorphism.

Example 1.3. The following are **not** homomorphisms:

1. The function $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n + 1$. In this case.

$$f(n+m) = n + m + 1 \neq f(n) + f(m) = n + m + 2.$$

2. The function $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = n^2$. In this case,

$$f(n+m) = (n+m)^2 = n^2 + 2nm + m^2 \neq n^2 + m^2,$$

unless one of n, m is 0. Similar examples work for $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

3. The Euler ϕ-function $\mathbb{N} \to \mathbb{N}$ is not a homomorphism. First, $\mathbb{N}$ is not even a group under multiplication. Second, the formula $\phi(nm) = \phi(n)\phi(m)$ only holds for n and m relatively prime, not for all n and m.

4. For a general group G, written multiplicatively, the function $f(g) = g^{-1}$ is not a homomorphism if G is not abelian. Similarly, $f(g) = g^2$ is a homomorphism $\iff$ G is abelian, since

$$f(gh) = (gh)^2 = ghgh,$$

and $ghgh = g^2h^2 \iff gh = hg$.

The following is a straightforward property of homomorphisms:

Proposition 1.4. *Let G and H be groups, written multiplicatively and let $f\colon G \to H$ be a homomorphism. Then*

(i) *$f(1) = 1$, where the 1 on the left is the identity in G and the 1 on the right is the identity in H. In other words, f takes the identity in G to the identity in H.*

(ii) *For all $g \in G$, $f(g^{-1}) = (f(g))^{-1}$.*

Proof. (i) Since $1 \cdot 1 = 1$, $f(1 \cdot 1) = f(1)$. But $f(1 \cdot 1) = f(1)f(1)$. Thus $f(1)f(1) = f(1)$. Canceling, we obtain $f(1) = 1$. (ii) We have $f(gg^{-1}) = f(1) = 1$, by (i). But $f(gg^{-1}) = f(g)f(g^{-1})$. Thus $f(g)f(g^{-1}) = 1$, so that $f(g^{-1}) = (f(g))^{-1}$. □

Many examples of this proposition should be familiar. For example, for the homomorphism $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}^*$ of (4) above, we have the familiar properties $\det(I) = 1$ and $\det(A^{-1}) = (\det A)^{-1}$. Similarly, for the real or complex exponential e^z, we know that $e^0 = 1$ and that $e^{-z} = 1/e^z$.

Proposition 1.5. *Let G_1, G_2, G_3 be groups and let $f_1\colon G_1 \to G_2$ and $f_2\colon G_2 \to G_3$ be homomorphisms. Then $f_2 \circ f_1\colon G_1 \to G_3$ is a homomorphism. In other words, the composition of two homomorphisms is a homomorphism.*

Proof. This is a straightforward computation left as an exercise. □

For example, suppose that $f\colon G_1 \to H_2$ is a homomorphism and that H_2 is given as a subgroup of a group G_2. Let $i\colon H_2 \to G_2$ be the inclusion, which is a homomorphism by (2) of Example 1.2. The $i \circ f$ is a homomorphism. Similarly, the restriction of a homomorphism to a subgroup is a homomorphism (defined on the subgroup).

2 Kernel and image

We begin with the following:

Proposition 2.1. *Let G_1 and G_2 be groups and let $f\colon G_1 \to G_2$ be a homomorphism. Then*

(i) *If $H_1 \leq G_1$, the $f(H_1) \leq G_2$. In other words, the image of a subgroup is a subgroup.*

(ii) *If $H_2 \leq G_2$, the $f^{-1}(H_2) \leq G_1$. In other words, the preimage of a subgroup is a subgroup.*

Proof. (i) We need to check closure, identity and inverses. Closure: Suppose given two elements of $f(H_1)$, necessarily of the form $f(h)$ and $f(h')$, where $h, h' \in H_1$. Then $f(h)f(h') = f(hh')$. Since H_1 is a subgroup of G_1, $hh' \in H_1$. By definition, $f(hh') \in f(H_1)$. Thus, the product $f(h)f(h') \in f(H_1)$, so that $f(H_1)$ is closed under multiplication. Identity: As H_1 is a subgroup of G_1, $1 \in H_1$. Then $f(1) \in f(H_1)$. By (i) of Proposition 1.4, $f(1) = 1$. Thus $1 \in f(H_1)$. Inverses: given an element of $f(H_1)$, necessarily of the form $f(h)$, where $h \in H_1$, we have by (ii) of Proposition 1.4 that $(f(h))^{-1} = f(h^{-1})$. Since H_1 is a subgroup of G_1, $h^{-1} \in H_1$. Thus $f(h^{-1}) = (f(h))^{-1} \in f(H_1)$. Hence $f(H_1)$ is closed under taking inverses, so is a subgroup of G_2.

(ii) Recall that, by definition, $f^{-1}(H_2) = \{g \in G_1 : f(g) \in H_2\}$. Again we must check closure, identity and inverses. Closure: Suppose given two elements g, g' of $f^{-1}(H_2)$. We must show that $gg' \in f^{-1}(H_2)$. By definition, $f(g), f(g') \in H_2$, and we must check that $f(gg') \in H_2$. But

$$f(gg') = f(g)f(g') \in H_2,$$

since $H_2 \leq G_2$ and $f(g), f(g') \in H_2$. Hence $gg' \in f^{-1}(H_2)$. Identity: we must check that $1 \in f^{-1}(H_2)$, i.e. that $f(1) \in H_2$. But $f(1) = 1$ by (i) of Proposition 1.4, and $1 \in H_2$ since $H_2 \leq G_2$. Hence $1 \in f^{-1}(H_2)$. Inverses:

Suppose that $g \in f^{-1}(H_2)$, i.e. that $f(g) \in H_2$. Then $f(g^{-1}) = f(g)^{-1}$, by (ii) of Proposition 1.4, and $f(g)^{-1} \in H_2$ since $f(g) \in H_2$ and $H_2 \leq G_2$. Thus $g^{-1} \in f^{-1}(H_2)$. It follows that $f^{-1}(H_2) \leq G_1$. □

Definition 2.2. Let G_1 and G_2 be groups and let $f\colon G_1 \to G_2$ be a homomorphism. The *image* of f is the subgroup $f(G_1) \leq G_2$; it is a subgroup of G_2 by (i) of Proposition 2.1. The *kernel* of f is the subgroup $f^{-1}(1) \leq G_1$, i.e. the preimage of 1 (or equivalently $\{1\}$). It is a subgroup of G_1 by (ii) of Proposition 2.1, since $\{1\} \leq G_2$. We write $\operatorname{Im} f$ and $\operatorname{Ker} f$ for the subgroup $\operatorname{Im} f$ of G_2 and the subgroup $\operatorname{Ker} f$ of G_1, respectively. For emphasis, we recall that

$$\operatorname{Ker} f = \{g \in G_1 : f(g) = 1\}.$$

If G_2 is written additively we would replace the condition $f(g) = 1$ by $f(g) = 0$.

Example 2.3. We now run through the examples of Example 1.2 and describe the kernel and image.

1. If $f\colon G_1 \to G_2$ is an isomorphism, then $\operatorname{Ker} f = \{1\}$ and $\operatorname{Im} f = G_2$.
2. If $i\colon H \to G$ is the inclusion of a subgroup, then $\operatorname{Ker} i = \{1\}$ and $\operatorname{Im} i = H$.
3. If $f\colon G \to H$ is the trivial homomorphism, then $\operatorname{Ker} f = G$ and $\operatorname{Im} f = \{1\}$. Clearly, a homomorphism $f\colon G \to H$ is the trivial homomorphism $\iff \operatorname{Ker} f = G$.
4. The kernel of $\det\colon GL_n(\mathbb{R}) \to \mathbb{R}^*$ is by definition $SL_n(\mathbb{R})$. The image of det is $\mathbb{R}^*$ since det is surjective.
5. If $f\colon \mathbb{C} \to \mathbb{C}^*$ is the complex exponential, $f(z) = e^z$, then $\operatorname{Ker} f = \{2n\pi i : n \in \mathbb{Z}\} = \langle 2\pi i \rangle$, and $\operatorname{Im} f = \mathbb{C}^*$ as the complex exponential is surjective. For the real exponential $e^x\colon \mathbb{R} \to \mathbb{R}^*$, $\operatorname{Ker} e^x = \{0\}$ and $\operatorname{Im} e^x = \mathbb{R}^{>0}$, the subgroup of positive real numbers.
6. For the absolute value function $f\colon \mathbb{C}^* \to \mathbb{R}^*$ defined by $f(z) = |z|$, $\operatorname{Ker} f = U(1)$ by definition, and $\operatorname{Im} f = \mathbb{R}^{>0}$.
7. For the sign function $\operatorname{sign}\colon \mathbb{R}^* \to \{\pm 1\}$, $\operatorname{Ker} \operatorname{sign} = \mathbb{R}^{>0}$, and $\operatorname{Im} \operatorname{sign} = \{\pm 1\}$.
8. If $F\colon \mathbb{R}^n \to \mathbb{R}^m$ is a linear map, corresponding to the matrix A, then $\operatorname{Ker} F$ is what is usually called the kernel or the nullspace of F.

9. For the function $f\colon \mathbb{Q}^* \to \mathbb{Q}^*$ defined by $f(t) = t^n$, $\operatorname{Ker} f = \{1\}$ if n is odd and is $\{\pm 1\}$ if n is even. The image of f is harder to describe; it is the set of rational numbers which are n^{th} powers. For the analogous function $f\colon \mathbb{R}^* \to \mathbb{R}^*$ (which we carelessly also denote by f), it is still the case that $\operatorname{Ker} f = \{1\}$ if n is odd and is $\{\pm 1\}$ if n is even. In this case, $\operatorname{Im} f = \mathbb{R}^*$ if n is odd and $\operatorname{Im} f = \mathbb{R}^{>0}$ if n is even. Finally, for $f\colon \mathbb{C}^* \to \mathbb{C}^*$ defined by $f(z) = z^n$, and $n > 0$, $\operatorname{Ker} f = \mu_n$, by definition, where $\#(\mu_n) = n$, and $\operatorname{Im} f = \mathbb{C}^*$ (every complex number is an n^{th} power). What happens if $n < 0$? If $n = 0$? For an arbitrary abelian group G, taking $n \in \mathbb{N}$ for simplicity, for the function $f\colon G \to G$ defined by $f(g) = g^n$, $\operatorname{Ker} f$ is the subgroup of n-torsion points of G (this was defined in a homework problem) and $\operatorname{Im} f$ is the subgroup of n^{th} powers.

10. Given a group G (written multiplicatively) and an element $g \in G$, for the function $f\colon \mathbb{Z} \to G$ defined by $f(n) = g^n$, $\operatorname{Ker} f = \{0\}$ if g has infinite order and $\operatorname{Ker} f = \langle n \rangle$ if g has finite order n. By definition, $\operatorname{Im} f = \langle g \rangle$. For the special case $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $f(a) = [a]$, $\operatorname{Ker} f = \langle n \rangle$ and $\operatorname{Im} f = \mathbb{Z}/n\mathbb{Z}$.

11. For $\pi_1\colon G_1 \times G_2 \to G_1$, defined by $\pi_1(g_1, g_2) = g_1$, $\operatorname{Ker} \pi_1 = \{1\} \times G_2$ and $\operatorname{Im} \pi_1 = G_1$. Similarly, $\operatorname{Ker} \pi_2 = G_1 \times \{1\}$ and $\operatorname{Im} \pi_2 = G_2$.

12. For the homomorphism $P\colon S_n \to GL_n(\mathbb{R})$ defined by $P(\sigma)(\mathbf{e}_i) = \mathbf{e}_{\sigma(i)}$, it is easy to see that P is injective. By definition $\operatorname{Im} P$ is the subgroup of $GL_n(\mathbb{R})$ of permutation matrices.

13. For the group S_n, and the homomorphism $\varepsilon\colon S_n \to \{\pm 1\}$, $\operatorname{Ker} \varepsilon = A_n$ by definition, and $\operatorname{Im} \varepsilon = \{\pm 1\}$ as long as $n \geq 2$.

An important fact about homomorphisms is the following (you may have seen the corresponding statement in linear algebra for linear maps):

Proposition 2.4. *Let $f\colon G \to H$ be a homomorphism. Then f is injective $\iff$ $\operatorname{Ker} f = \{1\}$.*

Proof. $\implies$: Suppose that f is injective. We must show that $h \in \operatorname{Ker} f \iff h = 1$. Note that $1 \in \operatorname{Ker} f$ by (i) of Proposition 1.4. Conversely, suppose that $h \in \operatorname{Ker} f$. Then by definition $f(h) = 1 = f(1)$. Since f is injective, $h = 1$.

$\impliedby$: Suppose that $\operatorname{Ker} f = \{1\}$. If $f(g_1) = f(g_2)$, then $(f(g_1))^{-1} f(g_2) = 1$. By (ii) of Proposition 1.4, $(f(g_1))^{-1} = f(g_1^{-1})$. Thus

$$1 = (f(g_1))^{-1} f(g_2) = f(g_1^{-1}) f(g_2) = f(g_1^{-1} g_2).$$

It follows that $g_1^{-1}g_2 \in \operatorname{Ker} f$, and hence by hypothesis that $g_1^{-1}g_2 = 1$. Thus $g_1 = g_2$, and f is injective. $\square$

Remark 2.5. The proof above shows more generally that, if $f\colon G \to H$ is an arbitrary homomorphism and $g_1, g_2 \in G$, then $f(g_1) = f(g_2) \iff$ there exists an element $k \in \operatorname{Ker} f$ such that $g_2 = g_1 k$.

3 Cayley's theorem

Theorem 3.1 (Cayley's theorem)**.** *Let G be a finite group. Then there exists an $n \in \mathbb{N}$ such that G is isomorphic to a subgroup of S_n.*

Remark 3.2. (i) The proof will show that we can take $n = \#(G)$.

(ii) In the early days of algebra, all of the finite groups were explicitly given as subgroups of S_n, and so this theorem would not have had any real content.

Proof of Cayley's theorem. Let G be any group, finite or not. We shall construct an injective homomorphism $f\colon G \to S_G$. Setting $H = \operatorname{Im} f$, there is a corresponding homomorphism (which we carelessly again denote by f) from G to H. Then f remains injective, and it has become surjective by definition, so that it is an isomorphism. Finally, taking G to be finite, an enumeration of the elements of G as $g_1, \ldots, g_n$, where $n = \#(G)$, defines an isomorphism $h\colon S_G \to S_n$. Replacing the homomorphism $f\colon G \to H$ above with $h \circ f$ gives an isomorphism from G to a subgroup of S_n.

To find the homomorphism f, we must, for every $g \in G$, find a bijection $\lambda_g\colon G \to G$. The definition of λ_g has been foreshadowed from our very first days in group theory: define $\ell_g\colon G \to G$ by

$$\ell_g(x) = gx.$$

Thus the function ℓ_g is left multiplication by g, whence the ℓ. We have seen that ℓ_g is a bijection for every g, i.e. is an element of S_G (Corollary 4.7 of the handout on groups). Then define $f\colon G \to S_G$ by:

$$f(g) = \ell_g.$$

We first check that f is a homomorphism. We must show that $f(gh) = f(g)f(h)$, or equivalently that $\ell_{gh} = \ell_g \circ \ell_h$. To check this equality of functions, we check that the values on x are equal for every $x \in G$. But

$$\begin{aligned} \ell_{gh}(x) &= (gh)x; \\ (\ell_g \circ \ell_h)(x) = \ell_g(\ell_h(x)) = \ell_g(hx) &= g(hx) = (gh)x. \end{aligned}$$

Thus f is a homomorphism. Finally, we must show that f is injective. One can do this by applying Proposition 2.4, but it is easy to argue directly: If $\ell_g = \ell_h$, then the functions ℓ_g and ℓ_h have the same value on any $x \in G$, in particular on $x = 1$. Thus $\ell_g(1) = \ell_h(1)$. On the other hand, $\ell_g(1) = g \cdot 1 = g$, and similarly $\ell_h(1) = h$. Thus $g = h$ and f is injective. □

Remark 3.3. Instead of working with left multiplication, we could try to work with *right* multiplication $r_g \colon G \to G$, defined by $r_g(x) = xg$. Then r_g is still an element of S_G. However, the function $F \colon G \to S_G$ defined by $F(g) = r_g$ is not in general a homomorphism! Still, it is easy to see why F fails to be a homomorphism, and to fix the definition of F so that it become a homomorphism from G to S_G. We leave the details as a homework problem.

The proof of Cayley's theorem may seem as if it was done with smoke and mirrors. However, we will see interesting variations on the method of proof later.