Group Homomorphisms

Definition. A **group homomorphism** $\phi : G \to H$ is a set map which respects the group operations.

$$\boldsymbol{\phi(a \cdot b) = \phi(a) \cdot \phi(b)}$$

Example. Linear transformations of vector spaces $T : V \to W$ are group homomorphisms, because one of the requirements for linear transformations is $T(\vec{x} + \vec{y}) = T(\vec{x}) + T(\vec{y})$.

Example. Conjugation by $g \in G$ defines a linear transformation $c_g : G \to G$ by $\boldsymbol{c_g(x) = gxg^{-1}}$ because $c_g(x)\, c_g(y) = (gxg^{-1})\,(gyg^{-1}) = gxg^{-1}gyg^{-1} = gxyg^{-1} = g(xy)g^{-1} = c_g(xy)$.

Example. For each element in a group $g \in G$ there is a group homomorphism $\phi_g : \mathbb{Z} \to G$ defined by

$$\boldsymbol{\phi_g(n) = g^n}.$$

This is a homomorphism because

$$\phi_g(n+m) = g^{n+m} = g^n\, g^m = \phi_g(n)\, \phi_g(m).$$

Note that the image of ϕ_g is precisely $\phi_g(\mathbb{Z}) = \langle g \rangle \subset G$.

Example. Reduction mod n gives homomorphisms $\mathbb{Z} \to \mathbb{Z}_n$ and $\mathbb{Z}_m \to \mathbb{Z}_n$ if n divides m (for example $\mathbb{Z}_{12} \to \mathbb{Z}_4$ and $\mathbb{Z}_{12} \to \mathbb{Z}_3$).

Example. Recall that the complex circle is $S = \big\{ z \in \mathbb{C} \;\big|\; |z| = 1 \big\}$ with multiplication as the group operation. The map wrapping $\mathbb{R}$ around the complex circle by

$$\phi(\theta) = e^{i\theta} = \cos(\theta) + i \sin(\theta)$$

defines a group homomorphism $\phi : \mathbb{R} \to S$ from the additive real numbers to the complex circle because

$$\phi(\alpha + \beta) = e^{i(\alpha+\beta)} = e^{i\alpha}\, e^{i\beta} = \phi(\alpha)\, \phi(\beta)$$

(This becomes the sum laws for sines and cosines if you convert to $a + bi$ form.)

Example. Recall that GL_2 is the group of 2×2 matrices with non-zero determinant, using matrix multiplication as the group operation (this is the "general linear" group). Matrix determinant gives a group homomorphism $\det : GL_2 \to \mathbb{R}$ because determinant is multiplicative

$$\det(AB) = \det(A)\det(B)$$

Example. [1] $\mathbb{R}[x]$, pronounced "$\mathbb{R}$ adjoin x", is all polynomials using the variable x. This forms a group under polynomial addition. Because derivatives are linear, derivative gives a group homomorphism

$$\tfrac{d}{dx} : \mathbb{R}[x] \to \mathbb{R}[x]$$

Conversely, we may define $\int : \mathbb{R}[x] \to \mathbb{R}[x]$ to be the anti-derivative satisfying $F(0) = 0$. This will also be a group homomorphism!

Example. If G is a permutation group, then define the sign of a permutation to be

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ is even} \\ -1, & \text{if } \sigma \text{ is odd} \end{cases}$$

Then $\operatorname{sgn} : G \to \{\pm 1\}$ is a homomorphism to the multiplicative group $\{\pm 1\}$.

Example. Recall that $G \times H = \{(g, h) \mid g \in G \text{ and } h \in h\}$. Then the projection map $\pi_1 : G \times H \to G$ by $\pi_1(g, h) = g$ as well as the inclusion map $i_1 : G \to G \times H$ by $i_1(g) = (g, e)$ are both group homomorphisms (as well as the corresponding maps π_2 and i_2). In group theory, we often write $G \oplus H$ instead of $G \times H$.

Example. The map $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x, y) = x - y$ is a group homomorphism.

[1] There are a number of constructions related to this. $\mathbb{R}[x]$ is **finite** polynomials in x; $\mathbb{R}[x, x^{-1}]$ is **finite** "Laurent" polynomials with positive and negative powers of x; $\mathbb{R}[[x]]$ is **infinite** "formal power series" (which has $(1-x)^{-1} = 1 + x + x^2 + x^3 + \cdots$); and $\mathbb{R}((x))$ is **infinite** "formal Laurent series" with positive and negative powers.

Example. If $H < G$, then the **inclusion** homomorphism is $i : H \hookrightarrow G$ defined by $i(h) = h$.

Example. The **trivial** homomorphism $* : G \to H$ sends everything to the identity $*(g) = e_H$.

Let's prove some basic facts about group homomorphisms!

Proposition. *Homomorphism is preserved by composition.*

If $\phi : G \to H$ and $\psi : H \to K$ are homomorphisms, then $(\psi \circ \phi) : G \to K$ is a homomorphism.

Proof. $\psi\big(\phi(xy)\big) \;=\; \psi\big(\phi(x)\,\phi(y)\big) \;=\; \psi\big(\phi(x)\big)\,\psi\big(\phi(y)\big).$ □

Proposition. *Group homomorphisms $\phi : G \to H$ respect identity elements.*

$\boldsymbol{\phi(e_G) = e_H}$ *(where $e_G \in G$ and $e_H \in H$ are the respective identity elements).*

Proof. $\phi(e_G)\,\phi(e_G) = \phi(e_G\,e_G) = \phi(e_G)$. Multiplying on the left by $\phi(e_G)^{-1}$ yields $\phi(e_G) = e_H$. □

Proposition. *Group homomorphisms $\phi : G \to H$ respect inverses.*

$\boldsymbol{\phi(g^{-1}) = \phi(g)^{-1}}$ *(where $g^{-1} \in G$ and $\phi(g)^{-1} \in H$ are inverses in the respective groups).*

Proof. $\phi(g^{-1})\,\phi(g) = \phi(g^{-1}g) = \phi(e) = e$ so $\phi(g^{-1}) = \phi(g)^{-1}$. □

Corollary. *More generally,* $\boldsymbol{\phi(g^n) = \phi(g)^n}$.

Proof. If $n > 0$ then $\phi(g^n) = \phi(\underbrace{g \cdots g}_{n}) = \underbrace{\phi(g) \cdots \phi(g)}_{n} = \phi(g)^n$. Similarly for $n < 0$ using $\phi(g^{-1}) = \phi(g)^{-1}$. □

Corollary. *If $|g|$ is finite, then $\big|\phi(g)\big|$ is finite and divides $|g|$.*

Proof. If $|g| = n$ then $g^n = e$, so $\phi(g)^n = \phi(g^n) = \phi(e) = e$. Thus $\big|\phi(g)\big|$ divides n. □

Corollary. *If $g \in G$ has order m, then $\phi_g : \mathbb{Z}_n \to G$ by $\phi_g(k) = g^k$ is a homomorphism iff m divides n.*

Proof. The previous corollary gives the $\Rightarrow$ direction because $|\phi_g(1)| = |g| = m$ and $|1| = n$ in $\mathbb{Z}_n$.
For the other direction, if m doesn't divide n, then $g^n \neq e$. This contradicts $g^n = \phi_g(n) = \phi_g(0) = g^0 = e$. □

Proposition. *Group homomorphisms $\phi : G \to H$ respect subgroups.*

If $K < G$ then $\phi(K) < H$.

Proof. We know $e \in K$, so $e \in \phi(K)$. Similarly if $\phi(k) \in \phi(K)$ then $k^{-1} \in K$, so $\phi(k)^{-1} = \phi(k^{-1}) \in \phi(K)$.
Finally, if $\phi(k_1), \phi(k_2) \in \phi(K)$ then $(k_1k_2) \in K$, so $\phi(k_1)\phi(k_2) = \phi(k_1k_2) \in \phi(K)$. □

Corollary. *The image of a homomorphism is a subgroup.*[2]

If $\phi : G \to H$ then $\operatorname{Im}\phi = \phi(G) < H$.

Proof. Use $G < G$ in the proposition above. □

Proposition. *If $K < G$ is cyclic, then $\phi(K)$ is also cyclic.*
If $K < G$ is abelian, then $\phi(K)$ is also abelian.

Proof. For the first statement, if $K = \langle k \rangle$, then $\phi(k') = \phi(k^n) = \phi(k)^n$; so $\phi(K) = \big\langle \phi(k) \big\rangle$.
For the second statement, if K is abelian, then $\phi(a)\,\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\,\phi(a)$. □

The **image** of $\phi : G \to H$ is the subgroup $\operatorname{Im}\phi = \phi(G) < H$. Opposite this is the **kernel** of ϕ!

[2] For this reason, we will use capital I for Im.

Definition. Given a group homomorphism $\phi : G \to H$, the **inverse image** of an element $h \in H$ is the **set**

$$\phi^{-1}(h) \;=\; \{g \in G \mid \phi(g) = h\}.$$

Definition. The **kernel** of a homomorphism is the inverse image of the identity

$$\text{Ker } \phi \;=\; \phi^{-1}(e) \;=\; \{g \in G \mid \phi(g) = e \in H\}.$$

Example. The kernel of matrix determinant $\det : GL_2 \to \mathbb{R}$ is the "special linear" group of matrices with determinant 1, $\text{Ker}(\det) = SL_2$

Example. The kernel of the derivative homomorphism $\frac{d}{dx} : \mathbb{R}[x] \to \mathbb{R}[x]$ is the constant polynomials, $\text{Ker}(\frac{d}{dx}) = \{f(x) = c \mid c \in \mathbb{R}\} \subset \mathbb{R}[x]$

Example. The kernel of the sign homomorphism on the symmetric group $\text{sgn} : S_n \to \{\pm 1\}$ is the alternating group, $\text{Ker}(\text{sgn}) = A_n$.

Example. The kernel of the homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $\phi(x, y) = x - y$ is the **diagonal** $\text{Ker}\, \phi = \{(x, x) \mid x \in \mathbb{R}\}$.

Proposition. *Kernel is trivial if and only if homomorphisms are injections!*

$\text{Ker}\, \phi = \{e\}$ if and only if ϕ is an injection.

Proof. If $\phi(a) = \phi(b)$, then $\phi(ab^{-1}) = \phi(a)\,\phi(b)^{-1} = e$; so $ab^{-1} \in \text{Ker}\, \phi$. Thus if $\text{Ker}\, \phi = \{e\}$, then $ab^{-1} = e$; so $a = b$. For the reverse direction, note that if $a \in \text{Ker}\, \phi$, then $\phi(a) = e = \phi(e)$. Thus if ϕ is an injection, then $a = e$, so $\text{Ker}\, \phi = \{e\}$. □

Corollary. *If $\phi : G \twoheadrightarrow H$ is a surjective homomorphism with $\text{Ker}\, \phi = \{e\}$, then ϕ is an isomorphism.*

Proof. Surjections which are injections are bijections. Bijections which respect product are isomorphisms. □

Proposition. *Kernel of $\phi : G \to H$ is a normal subgroup of G!* [3]

Proof. $\phi(e) = e$ so $e \in \text{Ker}\, \phi$. If $\phi(g) = e$ then $\phi(g^{-1}) = \phi(g)^{-1} = e^{-1} = e$; so $\text{Ker}\, \phi$ is closed under inverses. Similarly, if $\phi(g) = \phi(g') = e$ then $\phi(gg') = \phi(g)\,\phi(g') = e\,e = e$; so $\text{Ker}\, \phi$ is closed under products. Thus $\text{Ker}\, \phi$ is a subgroup.

Finally, note that if $\phi(g) = e$, then for any $a \in G$, we have $\phi(aga^{-1}) = \phi(a)\,\phi(g)\,\phi(a)^{-1} = \phi(a)\,e\,\phi(a)^{-1} = e$; so $aga^{-1} \in \text{Ker}\, \phi$. Thus $a\,(\text{Ker}\, \phi)\,a^{-1} \subset \text{Ker}\, \phi$; so $\text{Ker}\, \phi$ is normal. □

Corollary. *$\phi(a) = \phi(b)$ if and only if they are in the same coset of the kernel – i.e. $a\ \text{Ker}\, \phi = b\ \text{Ker}\, \phi$.*

Proof. $\phi(a) = \phi(b)$ if and only if $\phi(a^{-1}b) = \phi(a)^{-1}\phi(b) = e$, so $a^{-1}b \in \text{Ker}\, \phi$. Previously we showed this is equivalent to $a\,\text{Ker}\, \phi = b\,\text{Ker}\, \phi$. □

Corollary. *Inverse images are cosets of the kernel.*

If $\phi(g) = h$ then $\phi^{-1}(h) = g\ \text{Ker}\, \phi$.

Proof. $b \in \phi^{-1}(a)$ if and only if $\phi(b) = \phi(a)$ if and only if $b \in a\,\text{Ker}\, \phi$. □

Corollary. *Inverse images all have the same order.*

For all $g \in G$, we have $\left|\phi^{-1}(g)\right| \;=\; \left|\phi^{-1}(e)\right| \;=\; \left|\text{Ker}\, \phi\right|$.

Proof. Cosets all have the same order. □

Example. In linear algebra, the kernel of a linear transformation is a vector space, $\ker(T) = \{\vec{x} \mid T(\vec{x}) = \vec{0}\}$. The set of all solutions to $T(\vec{x}) = \vec{y}$ is $\vec{x} = \vec{x}_h + \ker(T)$ where $\vec{x}_h$ is a single particular solution $T(\vec{x}_h) = \vec{y}$. This is equivalent to saying $T^{-1}(\vec{y})$ is a coset of $\ker(T)$.

[3] That's why I used capital "K" for $\text{Ker}\, \phi$

Proposition. *Composition makes kernels bigger.*

Given homomorphisms $G \xrightarrow{\phi} H \xrightarrow{\psi} K$*, we have* $\operatorname{Ker}\phi \lhd \operatorname{Ker}(\psi \circ \phi)$.

Proof. If $\phi(g) = e$ then $\psi\big(\phi(g)\big) = \psi(e) = e$, so $g \in \operatorname{Ker}(\psi \circ \phi)$. Since $\operatorname{Ker}\phi < \operatorname{Ker}(\psi \circ \phi) < G$ and both are normal in G, then $\operatorname{Ker}\phi \lhd \operatorname{Ker}(\psi \circ \phi)$. □

Question. Can we describe the index $\big[\operatorname{Ker}(\psi \circ \phi) : \operatorname{Ker}\phi\big]$ in terms of $|H|$ and $|K|$?

We OBVIOUSLY want DESPERATELY to talk about the quotient $G/\operatorname{Ker}\phi$... but we need one more idea to do this fully. Oh, the suspense!!! Oh, how tantalizing!!!

Subgroups $H < G$ get inclusion homomorphisms $i : H \hookrightarrow G$.

Normal subgroups $N \lhd G$ get additional **quotient homomorphisms** $q : G \twoheadrightarrow G/N$. All together, normal subgroups have special (short exact) sequences of homomorphisms $N \hookrightarrow G \twoheadrightarrow G/N$.

Definition. For each normal subgroup $N \lhd G$ the **quotient map** $q : G \twoheadrightarrow G/N$ is $q(g) = [g]$.

Proposition. *Quotient maps are surjective group homomorphisms.*

Proof. Surjective because for any $[g] \in G/N$, we have $q(g) = [g]$.
Homomorphism because $q(ab) = [ab] = [a]\,[b] = q(a)\,q(b)$. □

Proposition. *Normal subgroups are kernels of their quotient homomorphisms!*

If $q : G \twoheadrightarrow G/N$ *is the quotient homomorphism, then* $\operatorname{Ker} q = N$.

Proof. $a \in \operatorname{Ker} q$ if and only if $q(a) = e$. But $q(a) = [a]$; and $[a] = [e]$ in G/N if and only if $a \in N$. □

When we quotient by the kernel, a simple and beautiful thing happens!

Theorem [1st Isomorphism Thm]. *A group homomorphism* $\phi : G \to H$ *descends to an isomorphism onto its image* $\bar{\phi} : G/\operatorname{Ker}\phi \xrightarrow{\cong} \operatorname{Im}\phi$.

Proof. We previously showed $\phi(a) = \phi(b)$ if and only if a and b are in the same coset of $\operatorname{Ker}\phi$. This is equivalent to the statement $[a] = [b]$ in $G/\operatorname{Ker}\phi$. □

Corollary. *Group homomorphisms* $\phi : G \to H$ *factor as compositions of surjections and injections.*

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, two heads, bend right] & & H \\
& G/\operatorname{Ker}\phi \arrow[ur, hook, bend right] &
\end{tikzcd}$$

Corollary. *If* $\phi : G \to H$ *is a homomorphism from a finite group* G*, then* $|G| = |\operatorname{Im}\phi| \cdot |\operatorname{Ker}\phi|$.

Proof. By the first isomorphism theorem, $\big|G/\operatorname{Ker}\phi\big| = \big|\operatorname{Im}\phi\big|$. □

Recall that we earlier showed $|\phi(g)|$ divides $|g|$. Now we can make a similar group-level statement.

Corollary. *If* $\phi : G \to H$ *is a homomorphism between finite groups, then* $\big|\phi(G)\big|$ *divides both* $|G|$ *and* $|H|$.

Proof. By the previous corollary, $\big|\phi(G)\big| \cdot \big|\operatorname{Ker}\phi\big| = |G|$. Also, $\big|\phi(G)\big|$ divides $\big|H\big|$ because $\phi(G) < H$. □

Example. The only homomorphism $\phi : \mathbb{Z}_7 \to \mathbb{Z}_5$ is the trivial map $\phi(k) = 0$. This is because the order $\big|\phi(\mathbb{Z}_7)\big|$ must divide both $\big|\mathbb{Z}_5\big| = 5$ and $\big|\mathbb{Z}_7\big| = 7$. So $\big|\phi(\mathbb{Z}_7)\big| = 1$, which means $\phi(\mathbb{Z}_7) = \{0\}$.

Example. If G is an abelian group, let $G^k = \{g^k\}$ and $G^{(k)} = \{g \mid g^k = e\}$. Then $\phi : G \to G^k$ is a homomorphism with $\operatorname{Ker}\phi = G^{(k)}$, so $G/G^{(k)} \cong G^k$.

The 2^{nd} Isomorphism Theorem tells us how to understand **quotients of products**.

Theorem [2^{nd} Isomorphism Thm]. *If $K < G$ and $N \lhd G$ then $KN/N \cong K/K \cap N$.*

Proof. Consider the map $\phi : K \to KN/N$ given by $\phi(k) = [k] = kN$. This is a homomorphism because it is a composition of inclusion and quotient homomorphisms $K \hookrightarrow KN \twoheadrightarrow KN/N$. According to the first isomorphism theorem, $K/\operatorname{Ker}\phi \cong \operatorname{Im}\phi$.

$\operatorname{Im}\phi = KN/N$ because any element $[kn] \in KN/N$ satisfies $[kn] = (kn)N = kN = [k] = \phi(k)$.

$K/K \cap N = K/\operatorname{Ker}\phi$ because $\phi(k) = e$ if and only if $k \in N$ (so $\operatorname{Ker}\phi = K \cap N$). □

The 3^{rd} Isomorphisms Theorem tells us **quotients of quotients** are merely **change of base**!

Theorem [3^{rd} Isomorphism Thm]. *If $M, N \lhd G$ with $M < N$ then $(G/M)/(N/M) \cong G/N$.*

Proof. Consider the map $\phi : G/M \to G/N$ given by $\phi(gM) = gN$. This is well-defined because $M < N$; so $a = bm$ for $m \in M < N$ is also $a = bm$ for $m \in N$. The map is clearly a homomorphism. The first isomorphism theorem says $(G/M)/(\operatorname{Ker}\phi) \cong \operatorname{Im}\phi$.

$\operatorname{Im}\phi = G/N$ because ϕ is clearly a surjection (if $gN \in G/N$ then $\phi(gM) = gN$ for $gM \in G/M$).

$\operatorname{Ker}\phi = N/M$ because $\phi(gM) = eN$ if and only if $gN = \phi(gM) = eN = N$, equivalent to $g \in N$. □

There's one final REALLY COOL and IMPORTANT thing we can define. **Pullbacks of subgroups!** [4]

Definition. Given a group homomorphism $\phi : G \to H$, the **pullback** of a subset $K \subset H$ is the set

$$\phi^{-1}K = \{g \in G \mid \phi(g) \in K\}.$$

Proposition. *Pullback of subgroups are subgroups!*

Pullback of normal subgroups are normal subgroups!

Proof. Suppose that $\phi : G \to H$ and $K < H$. We consider $\phi^{-1}K \subset G$.

For the first statement, note that $\phi(e) = e \in K$; so $e \in \phi^{-1}K$. If $g \in \phi^{-1}K$ then $\phi(g^{-1}) = \phi(g)^{-1} \in K$; so $g^{-1} \in \phi^{-1}K$. Finally if $g, g' \in \phi^{-1}K$ then $\phi(gg') = \phi(g)\phi(g') \in K$; so $(gg') \in \phi^{-1}K$. Thus $\phi^{-1}K$ is a group.

For the second statement, if $K \lhd H$ then $hkh^{-1} \in K$ for all $k \in K$ and $h \in H$. Let $x \in \phi^{-1}K$, and $g \in G$. Since $\phi(x) \in K$ and $\phi(g) \in H$ we have $\phi(gxg^{-1}) = \phi(g)\,\phi(x)\,\phi(g)^{-1} \in K$. Thus $gxg^{-1} \in \phi^{-1}K$; so $\phi^{-1}K$ is normal. □

Remark. Pullbacks are better than images! While images do preserve subgroups $K < G \Rightarrow \phi(K) < H$; usually images will not preserve normality $K \lhd G \not\Rightarrow \phi(K) \lhd H$. (Though at least they preserve normality *within images* $K \lhd G \Rightarrow \phi(K) \lhd \phi(G)$.) If we advanced further, pullbacks would become **very** important!

Combining pullbacks with quotient maps allows us to quickly prove the Correspondence Theorem. The Correspondence Theorem tells us what it means to be a **subgroup in a quotient group**. This extends our understanding of quotients from the 3^{rd} Isomorphism Theorem.[5]

Note that if $q : G \twoheadrightarrow G/N$ then subgroups $H < G$ are sent by the quotient map to $q(H) = H/N$.

Theorem [Correspondence Thm]. *Pullback through the quoteint map gives an equivalence between subgroups of G/N and subgroups of G which contain N.*

$$q^{-1} : \{\textit{subgroups of } G/N\} \xrightarrow{\cong} \{\textit{subgroups } H \mid N < H < G\}.$$

Proof. If $K < G/N$ then the pullback of K through the quotient map $q : G \twoheadrightarrow G/N$ is a subgroup $q^{-1}K < G$. Furthermore $N < q^{-1}K$ because if $x \in N$ then $q(x) = [x] = [e] \in G/N$; and $[e] \in K$ since K is a subgroup.

To show this is a bijection, note that pullback is the inverse of image. If $N < H < G$, then $N \lhd G$ implies $N \lhd H$. The quotient map $q : G \twoheadrightarrow G/N$ maps $\phi(H) = H/N$, and the pullback is $\phi^{-1}(H/N) = H$. □

[4] This kind of "pullback" exists in multiple areas of mathematics. In general, structures will often "pull back" through maps, even when they don't "push forward". Pullbacks tend to have very nice properties and play important roles!

[5] Many areas of mathematics have similar "quotient objects." Similar to here, they are always paired with theorems telling how to deal with quotient and sub-objects of quotients.