1.4 Group Homomorphisms

Recognizing the maps that perserve a given mathematical structure allows one to compare objects and identify equivalence ones.

1.4.1 Definition. Let $(G, \star)$ and $(H, *)$ be two groups; the notation distinguishes the two group operations. A ***group homomorphism*** is a map $\varphi : G \to H$ such that $\varphi(f \star g) = \varphi(f) * \varphi(g)$ for all $f, g \in G$.

It follows, immediately from the definition, that the composition of group homomorphisms is again a group homomorphism and the identity map on a group is a group homomorphism.

1.4.2 Example. For all $n \in \mathbb{N}$, the map $\det : \operatorname{GL}(n, \mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism, because the determinant of a matrix product is the product of the determinants ◇

1.4.3 Example. For all $n \in \mathbb{N}$, the sign map $\operatorname{sgn} : \mathfrak{S}_n \to \mu_2$ is a group homomorphism. ◇

1.4.4 Example. For any subgroup H of a group G, the inclusion map $\iota : H \to G$ is a group homomorphism. ◇

1.4.5 Lemma. *Let $\varphi : G \to H$ a group homomorphism.*

(i) *A group homomorphism maps the identity element in its source to the identity element in its target; $\varphi(e_G) = e_H$.*
(ii) *A group homomorphism maps inverses to inverses; for all $g \in G$, we have $\varphi(g^{-1}) = (\varphi(g))^{-1}$.*
(iii) *For all $n \in \mathbb{Z}$ and all $g \in G$, we have $\varphi(g^n) = (\varphi(g))^n$.*

For any element $g \in G$, Lemma 1.4.5 establishes that the map $\eta_g : \mathbb{Z} \to G$ defined by $\eta_g(n) := g^n$ is a group homomorphism.

Proof.

(i) The identity axiom for a group and the definition of a group homomorphism give $\varphi(e_G) = \varphi(e_G \star e_G) = \varphi(e_G) * \varphi(e_G)$. Since the element $\varphi(e_G)$ is invertible in H, it follows that $\varphi(e_G) = e_H$.
(ii) Using part (i), we have $e_H = \varphi(e_G) = \varphi(g \star g^{-1}) = \varphi(g) * \varphi(g^{-1})$, so we deduce that $\varphi(g^{-1}) = \varphi(g)^{-1}$.
(iii) Using part (ii), we may assume that n is a nonnegative integer. We proceed by induction on n. The empty product in a group is the identity, so part (i) proves $(\varphi(g))^0 = e_H = \varphi(e_G) = \varphi(g^0)$ and the base case holds. The induction hypothesis implies that

$$\begin{aligned} \varphi(g^{n+1}) &= \varphi(g \star g^n) = \varphi(g) * \varphi(g^n) \\ &= \varphi(g) * (\varphi(g))^n = (\varphi(g))^{n+1} . \end{aligned}$$ □

Following Definition 1.3.3, a group homomorphism $\varphi : G \to H$ is an ***isomorphism*** if there exists a group homomorphism $\psi : H \to G$ such that $\psi \circ \varphi = \mathrm{id}_G$ and $\varphi \circ \psi = \mathrm{id}_H$.

1.4.6 Proposition. *A group homomorphism is an isomorphism if and only if the underlying map of sets is bijective.*

Proof.

(⇐) Suppose that $\varphi : G \to H$ is a group isomorphism. Since the underlying map of sets has an inverse, it is a bijection.
(⇒) Suppose that the underlying map of sets is bijective. It follows that there exists a set map $\varphi^{-1} : H \to G$ such that $\varphi^{-1} \circ \varphi = \mathrm{id}_G$ and $\varphi \circ \varphi^{-1} = \mathrm{id}_H$. It remains to show that this set map is a

Two groups G and H are ***isomorphic***, denoted by $G \cong H$, if there exists an isomorphism $\varphi : G \to H$.

group homomorphism. Since φ is a group homomorphism, it follows that, for all $g, h \in H$, we have

$$\varphi(\varphi^{-1}(g) \star \varphi^{-1}(h)) = \varphi(\varphi^{-1}(g)) * \varphi(\varphi^{-1}(h)) = g * h\,,$$

which implies that $\varphi^{-1}(g * h) = \varphi^{-1}(g) \star \varphi^{-1}(h)$. Thus, the inverse map $\varphi^{-1} : H \to G$ is a group homomorphism. □

1.4.7 Example. The group homomorphism $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ is an isomorphism whose inverse is $\log : (\mathbb{R}_{>0}, \cdot) \to (\mathbb{R}, +)$. ◇

1.4.8 Example. The matrix subgroup $\left\{\left[\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right] \mid r \in \mathbb{R}\right\}$ is isomorphic to $\mathbb{R}$. The map $\varphi : \mathbb{R} \to \mathrm{SL}(2, \mathbb{R})$ defined by $\varphi(r) := \left[\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right]$ is a group homomorphism because $\varphi(r+s) = \left[\begin{smallmatrix} 1 & r+s \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & s \\ 0 & 1 \end{smallmatrix}\right] = \varphi(r)\,\varphi(s)$. The inverse map sends the matrix $\left[\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right]$ to the number r. ◇

A group homomorphism determines two important subgroups.

1.4.9 Proposition. *Let $\varphi : G \to H$ be a group homomorphism.*

(i) *The* **image** $\mathrm{Im}(\varphi) := \{h \in H \mid h = \varphi(g)$ *for some* $g \in G\}$ *of the map φ is a subgroup of its target H.*

(ii) *The* **kernel** $\mathrm{Ker}(\varphi) := \{g \in G \mid \varphi(g) = e_H\}$ *of the map φ is a subgroup of its source G.*

Proof.

(i) Given elements h' and h in the image of the map φ, there are elements g and g' in G such that $\varphi(g') = h'$ and $\varphi(g) = h$. Since φ is a group homomorphism, Lemma 1.4.5 implies that $\varphi(g' \star g^{-1}) = \varphi(g') * \varphi(g)^{-1} = h' * h^{-1}$. As $h' * h^{-1} \in \mathrm{Im}(\varphi)$, Lemma 1.2.2 shows that $\mathrm{Im}(\varphi)$ is a subgroup of H.

(ii) Given elements g' and g in the kernel of the map φ, we have $\varphi(g' \star g^{-1}) = \varphi(g') * \varphi(g)^{-1} = e_H * e_H^{-1} = e_H$. As $g' * g^{-1} \in \mathrm{Ker}(\varphi)$, Lemma 1.2.2 shows that $\mathrm{Ker}(\varphi)$ is a subgroup of G. □

1.4.10 Example. The group homomorphism $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^{\times}$ has $\mathrm{Im}(\det) = \mathbb{R}^{\times}$ and $\mathrm{Ker}(\det) = \mathrm{SL}(n, \mathbb{R})$. ◇

1.4.11 Corollary. *A group homomorphism is injective if and only if its kernel is trivial.*

Proof. Let $\varphi : G \to H$ be a group homomorphism.

($\Rightarrow$) Suppose that φ is injective. Lemma 1.4.5 shows that $\varphi(e_G) = e_H$ and injectivity ensures that e_G is the only element sent to e_H. Thus, the kernel of the map φ is the trivial subgroup $\{e_G\}$.

($\Leftarrow$) Suppose that φ has a trivial kernel. For any elements $f, g \in G$, the equation $\varphi(f) = \varphi(g)$ is equivalent to $\varphi(f \star g^{-1}) = e_H$. Since $\mathrm{Ker}(\varphi) = \{e_G\}$, we deduce that $f \star g^{-1} = e_G$ and $f = g$. Hence, the map φ is injective. □

1.5 Permutation Groups

As an alternative to their characterization as automorphism groups, abstract groups may be realized as subgroups of a symmetric group.

1.5.1 Definition. A group G ***acts*** on a set X if there exists a map $G \times X \to X$, denoted by $(g, x) \mapsto g\,x$, such that

(associativity) For all $g, h \in G$ and all $x \in X$, we have $(gh)x = g(hx)$.
(identity) For the identity element $e \in G$ and all $x \in X$, we have $ex = x$.

1.5.2 Example. For all nonnegative integers n, the symmetric group $\mathfrak{S}_n$ acts, by definition, on the finite set $[n] := \{1, 2, \dots, n\}$. ◇

1.5.3 Example. The properties of matrix multiplication imply that the general linear group $\mathrm{GL}(n, \mathbb{R})$ acts on column vectors $\mathrm{v} \in \mathbb{R}^n$ by left multiplication. ◇

1.5.4 Example. The ***orthogonal group*** $\mathrm{O}(n, \mathbb{R})$, which consists of the distance-preserving linear maps, acts on the unit sphere in $\mathbb{R}^n$. ◇

1.5.5 Example. The dihedral group D_n, which consists of the automorphisms of a regular polygon with n edges, acts on the set of vertices of the polygon. ◇

1.5.6 Proposition. *A group G acts on a set X if and only if there exists a group homomorphism from G to the symmetric group $\mathfrak{S}_X$.*

Proof. Suppose that G acts on the set X. Given an element $g \in G$, consider the map $\sigma_g : X \to X$ defined by $\sigma_g(x) := g\,x$. Associativity of the group action establishes that, for all $g, h \in G$, the functional equation $\sigma_g \circ \sigma_h = \sigma_{gh}$ holds. The identity property of the group action implies that $\sigma_e = \mathrm{id}_X$. As every element in G has an inverse, we see that $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{gg^{-1}} = \mathrm{id}_X = \sigma_{g^{-1}g} = \sigma_{g^{-1}} \circ \sigma_g$, which proves that, for all $g \in G$, the map σ_g is bijective. We conclude that the map $\sigma : G \to \mathfrak{S}_X$, defined by $g \mapsto \sigma_g$, is group homomorphism.

Conversely, suppose that $\varphi : G \to \mathfrak{S}_X$ is a group homomorphism. Consider the map $G \times X \to X$ defined by $(g, x) \mapsto (\varphi(g))(x)$. Since the map φ is group homomorphism, it follows that, for all $g, h \in G$ and all $x \in X$, we have

$$(gh)(x) = \big(\varphi(gh)\big)(x) = \varphi(g)\big(\varphi(h)(x)\big) = g(hx)\,.$$

The operation associating the action of the group G on the set X to a group homomorphism $\sigma : G \to \mathfrak{S}_X$ and the operation associating a group homomorphism $\varphi : G \to \mathfrak{S}_X$ to the action of G on X are mutual inverses.

Since Lemma 1.4.5 demonstrates that $\varphi(e) = \mathrm{id}_X$, we also see that $ex = \big(\varphi(e)\big)(x) = x$. Therefore, the map $G \times X \to X$ defined by $(g, x) \mapsto \big(\varphi(g)\big)(x)$ has the associativity and identity properties. □

Every group acts on its underlying set.

1.5.7 Example (Left translation). Given an element g in a group G, the map $\lambda_g : G \to G$ is defined by $\lambda_g(x) := gx$. For all $g, h, x \in G$, we

Left translation is generally not a group homomorphism; $\lambda_g(xy) = gxy \neq gxgy = \lambda_g(x)\,\lambda_g(y)$.

have $(\lambda_g \circ \lambda_h)(x) = \lambda_g(hx) = g(hx) = (gh)x = \lambda_{gh}(x)$ which gives $\lambda_g \circ \lambda_h = \lambda_{gh}$. Moreover, for all $x \in G$, we also have $\lambda_e(x) = ex = x$, so $\lambda_e = \mathrm{id}_G$. Thus, every group acts on itself by left translation. ◇

Arthur Cayley (1854) first highlights this correspondence, although Camille Jordan (1870) appears to give the first complete proof.

1.5.8 Theorem (Cayley). *Every group G is isomorphic to a subgroup of the symmetric group $\mathfrak{S}_G$.*

Proof. Consider the map $\lambda : G \to \mathfrak{S}_G$ defined by $\lambda(g) := \lambda_g$. Since we have $\lambda(g)\,\lambda(h) = \lambda_g\,\lambda_h = \lambda_{gh} = \lambda(gh)$ for all $g, h \in G$, the map λ is a group homomorphism. The equation $\lambda(g) = \lambda(h)$ implies that $\lambda_g(x) = \lambda_h(x)$ for all $x \in G$, so we obtain $g = \lambda_g(e) = \lambda_h(e) = h$. Thus, the group homomorphism λ is injective and G is isomorphic to the image of λ. □

1.5.9 Example. Under left translation, we see that the elements in the Klein 4-group correspond to the permutations id_4, $(2\ 1)(4\ 3)$, $(3\ 1)(4\ 2)$, and $(3\ 2)(4\ 1)$ in $\mathfrak{S}_4$; compare with Figure 1.1. ◇

1.5.10 Example. Under left translation, the elements in the dihedral group D_3 corresponds to id_6, $(2\ 1)(5\ 3)(6\ 4)$, $(3\ 1)(5\ 4)(6\ 2)$, $(4\ 1)(5\ 2)(6\ 3)$, $(4\ 3\ 2)(6\ 1\ 5)$, and $(4\ 2\ 3)(6\ 5\ 1)$ in $\mathfrak{S}_6$. Enumerating the vertices in the triangle, we see that D_3 is isomorphic to $\mathfrak{S}_3$. ◇

Every group acts on its underlying set in a few different ways.

1.5.11 Example (Right action). Given an element g in a group G, the map $\rho_g : G \to G$ is defined by $\lambda_g(x) := xg^{-1}$. For all $g, h, x \in G$, we have $(\rho_g \circ \rho_h)(x) = \rho_g(xh^{-1}) = (xh^{-1})g^{-1} = x(gh)^{-1} = \rho_{gh}(x)$ which gives $\rho_g \circ \rho_h = \rho_{gh}$. Moreover, for all $x \in G$, we also have $\rho_e(x) = xe^{-1} = x$, so $\rho_e = \mathrm{id}_G$. Thus, every group acts on itself on the right. ◇

1.5.12 Example (Conjugation). Given an element g in a group G, the map $\gamma_g : G \to G$ is defined by $\gamma_g(x) := gxg^{-1}$. For all $g, h, x \in G$, we have

$$(\gamma_g \circ \gamma_h)(x) = \gamma_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \gamma_{gh}(x)$$

which gives $\gamma_g \circ \gamma_h = \gamma_{gh}$. Moreover, for all $x \in G$, we also have $\gamma_e(x) = exe^{-1} = x$, so $\gamma_e = \mathrm{id}_G$. Thus, every group acts on itself by conjugation. ◇