

2 Quotient Groups

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-09-05

Subobjects have a counterpart in which the canonical injections are replaced by surjections. When they exist, these quotient objects provide another way of relating smaller objects to larger ones. In group theory, quotients are indispensable.

The English term “quotient group” first appears in [Arthur Cayley \(1893\)](#).

2.0 Group Homomorphisms

Recognizing the maps that preserve a given mathematical structure enables one to compare objects and identify equivalent ones. What, then, are the morphisms between groups?

2.0.1 Definition. Let $(G, \star)$ and $(H, *)$ be groups, where the five- and six-point stars distinguish the products. A **group homomorphism** is a map $\varphi : G \rightarrow H$ such that, for any elements f and g in G , we have

$$\varphi(f \star g) = \varphi(f) * \varphi(g).$$

The definition immediately implies that the composition of group homomorphisms is again a group homomorphism, and the identity map on a group is a group homomorphism.

2.0.2 Example. For any nonnegative integer n , the determinant map $\det : \text{GL}(n, \mathbb{R}) \rightarrow \mathbb{R}^\times$ is a group homomorphism: the determinant of a product is equal to the product of the determinants $\diamond$

2.0.3 Example. For any nonnegative integer n , Problem 1.4.6 shows that the map $\text{sgn} : \mathfrak{S}_n \rightarrow \mu_2$ is a group homomorphism. $\diamond$

2.0.4 Example. For any subgroup H of a group G , the inclusion map $\iota : H \rightarrow G$ is a group homomorphism. $\diamond$

The inclusion map being a group homomorphism should be the definition of a subgroup.

2.0.5 Lemma (basic properties). Let $\varphi : G \rightarrow H$ a group homomorphism.

- (identity) Every group homomorphism maps the identity element in its source to the identity in its target: $\varphi(e_G) = e_H$.
- (inverse) Every group homomorphism maps inverses to inverses: for any element g in G , we have $\varphi(g^{-1}) = (\varphi(g))^{-1}$.
- (exponential) Every group homomorphism is compatible with integer exponentiation: for any integer n and any element g in the source G , we have $\varphi(g^n) = (\varphi(g))^n$.

For any element g in a group G , the exponential property shows that the map $\eta_g : \mathbb{Z} \rightarrow G$ defined by $\eta_g(n) := g^n$, for any integer n , is a group homomorphism because

$$\begin{aligned} \eta_g(m + n) &= g^{m+n} \\ &= g^m g^n = \eta_g(m) \eta_g(n). \end{aligned}$$

Proof. The identity property in the source G 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 , we have $\varphi(e_G) = e_H$.

The identity property for a group homomorphism, the inverse property for H , and the definition of a group homomorphism give $e_H = \varphi(e_G) = \varphi(g \star g^{-1}) = \varphi(g) * \varphi(g^{-1})$, so $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Using the inverse property for a group homomorphism, we may assume that n is a nonnegative integer. We proceed by induction on n . The identity property gives $(\varphi(g))^0 = e_H = \varphi(e_G) = \varphi(g^0)$, so the base case holds. The induction hypothesis implies that

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

The empty product equals the identity element; $g^0 = \prod_{i \in \emptyset} g = e$. For any negative integer n , we also have $g^n = \prod_{i=1}^{-n} g^{-1}$.

2.0.6 Proposition. *A group homomorphism is an isomorphism if and only if it is bijective.*

Proof. Suppose that the map $\varphi: G \rightarrow H$ is a group isomorphism. Since the underlying map of sets has an inverse, it is a bijection.

Conversely, suppose that the underlying map of sets is bijective. Hence, there exists a set map $\varphi^{-1}: H \rightarrow G$ such that $\varphi^{-1} \circ \varphi = \text{id}_G$ and $\varphi \circ \varphi^{-1} = \text{id}_H$. It remains to show that the map φ^{-1} is a group homomorphism. Since φ is a group homomorphism, it follows that, for any elements h and h' in the target H , we have

$$\varphi(\varphi^{-1}(h) \star \varphi^{-1}(h')) = \varphi(\varphi^{-1}(h)) * \varphi(\varphi^{-1}(h')) = h * h'.$$

Applying φ^{-1} to both sides, we obtain $\varphi^{-1}(h * h') = \varphi^{-1}(h) \star \varphi^{-1}(h')$. Thus, the inverse map $\varphi^{-1}: H \rightarrow G$ is a group homomorphism. $\square$

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

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

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

A group homomorphism determines two important subgroups.

2.0.8 Proposition. *Let $\varphi: G \rightarrow H$ be any group homomorphism.*

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

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

Proof. The image is nonempty because $\varphi(e_G) = e_H$. For any h and h' in $\text{Im}(\varphi)$, there exists g and g' in G such that $\varphi(g) = h$ and $\varphi(g') = h'$. The definition of a group homomorphism and inverse property give $\varphi(g' \star g^{-1}) = \varphi(g') * \varphi(g)^{-1} = h' * h^{-1}$. As $h' * h^{-1}$ is in $\text{Im}(\varphi)$, Lemma 1.2.2 shows that $\text{Im}(\varphi)$ is a subgroup.

As $\varphi(e_G) = e_H$, the kernel is nonempty. For any g' and g in $\text{Ker}(\varphi)$, we have $\varphi(g' \star g^{-1}) = \varphi(g') * \varphi(g)^{-1} = e_H * e_H^{-1} = e_H$. Since $g' * g^{-1}$ is in $\text{Ker}(\varphi)$, Lemma 1.2.2 shows that $\text{Ker}(\varphi)$ is a subgroup. $\square$

2.0.9 Example. The group homomorphism $\det: \text{GL}(n, \mathbb{R}) \rightarrow \mathbb{R}^\times$ has $\text{Im}(\det) = \mathbb{R}^\times$ and $\text{Ker}(\det) = \text{SL}(n, \mathbb{R})$. $\diamond$

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

Proof. Let $\varphi: G \rightarrow H$ be a group homomorphism. Suppose that φ is injective. The identity property for φ shows that $\varphi(e_G) = e_H$, and injectivity ensures that e_G is the only element in G sent to e_H . Thus, the kernel of the map φ is the trivial subgroup $\langle e_G \rangle$ of G .

Conversely, suppose that φ has a trivial kernel. For any elements f and g in G , the equality $\varphi(f) = \varphi(g)$ is equivalent to the equality $\varphi(f \star g^{-1}) = e_H$. Since $\text{Ker}(\varphi) = \langle e_G \rangle$, we deduce that $f \star g^{-1} = e_G$ and $f = g$. Hence, the map φ is injective. $\square$

2.1 Permutation Groups

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

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

(*associativity*) For any elements f and g in the group G and any element x in the set X , we have $(fg)x = f(gx)$.

(*identity*) For the identity element e in the group G and any element x in the set X , we have $ex = x$.

2.1.2 Example. For any nonnegative integer n , the symmetric group $\mathfrak{S}_n$ acts, by definition, on the finite set $[n] := \{1, 2, \dots, n\}$. $\diamond$

2.1.3 Example. The general linear group $\text{GL}(n, \mathbb{R})$ acts on column vectors v in $\mathbb{R}^n$ by left multiplication. $\diamond$

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

2.1.5 Example. The dihedral group D_n , which is the automorphism group of a regular polygon with n edges, acts on the set of vertices of the polygon. $\diamond$

2.1.6 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 . For any element g in G , the map $\sigma_g : X \rightarrow X$ is defined by $\sigma_g(x) := gx$ for all x in X . The associativity of the group action implies that, for any elements g and h in G , we have $\sigma_g \circ \sigma_h = \sigma_{gh}$. The identity property for the group action implies that $\sigma_e = \text{id}_X$. As every element in the group G has an inverse, we see that $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{gg^{-1}} = \text{id}_X = \sigma_{g^{-1}g} = \sigma_{g^{-1}} \circ \sigma_g$, which proves that, for any element g in G , the map σ_g is bijective. Hence, the map $\sigma : G \rightarrow \mathfrak{S}_X$, defined by $g \mapsto \sigma_g$ for any element g in G , is group homomorphism.

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

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

The identity property for group homomorphisms gives $\varphi(e) = \text{id}_X$, so $ex = (\varphi(e))(x) = x$. Thus, the map $G \times X \rightarrow X$ defined, for any g in the group G and any x in the set X , by $(g, x) \mapsto (\varphi(g))(x)$ has the associativity and identity properties. $\square$

Every group acts on itself.

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

2.1.7 Example. For any element g in a group G , the *left translation* map $\lambda_g: G \rightarrow G$ is defined, for any element x in G , by $\lambda_g(x) := gx$. For any elements g, h , and x in G , we 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 any element x in G , we also have $\lambda_e(x) = ex = x$, so $\lambda_e = \text{id}_G$. Therefore, every group acts on itself by left translation. $\diamond$

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

Proof. Consider the map $\lambda: G \rightarrow \mathfrak{S}_G$ defined, for any element g in G , by $\lambda(g) := \lambda_g$. Since $\lambda(g)\lambda(h) = \lambda_g\lambda_h = \lambda_{gh} = \lambda(gh)$ for any elements g and 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 any element x in G . Evaluating at the identity element e in G , we see that the equation $\lambda(g) = \lambda(h)$ implies that $g = \lambda_g(e) = \lambda_h(e) = h$, so λ is injective. Thus, the group G is isomorphic to the image of λ . $\square$

2.1.9 Example. The four elements of the Klein 4-group correspond, under left translation, 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 1.2. $\diamond$

2.1.10 Example. The six elements of the dihedral group D_3 correspond, under left translation to the permutations 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 $\mathfrak{S}_6$. By labeling the vertices in the equilateral triangle, we see that D_3 is isomorphic to $\mathfrak{S}_3$. $\diamond$

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

2.1.11 Example. For any element g in a group G , the *right translation* map $\rho_g: G \rightarrow G$ is defined, for any element x in G , by $\rho_g(x) := xg^{-1}$. For any elements g, h , and 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 any element x in G , we also have $\rho_e(x) = xe^{-1} = x$, so $\rho_e = \text{id}_G$. Therefore, every group acts on itself by right translation. $\diamond$

2.1.12 Example. For any element g in a group G , the *conjugation* map $\gamma_g: G \rightarrow G$ is defined, for any element x in G , by $\gamma_g(x) := gxg^{-1}$. For any elements g, h , and 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 any element x in G , we also have $\gamma_e(x) = exe^{-1} = x$, so $\gamma_e = \text{id}_G$. Therefore, every group acts on itself by conjugation. $\diamond$

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

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

By setting $f := (4\ 3\ 2)(6\ 1\ 5)$ and $g := (2\ 1)(5\ 3)(6\ 4)$, the multiplication table for the subgroup $\langle f, g \rangle$ of $\mathfrak{S}_6$ is

$\star$	e	f	f^2	g	fg	f^2g
e	e	f	f^2	g	fg	f^2g
f	f	f^2	e	fg	f^2g	g
f^2	f^2	e	f	f^2g	g	fg
g	g	f^2g	fg	e	f^2	f
fg	fg	g	f^2g	f	e	f^2
f^2g	f^2g	fg	g	f^2	f	e

2.2 Cosets

The choice of a subgroup reveals a surprising amount about a group.

2.2.1 Definition. Let H be a subgroup of a group G . The *left coset* of H with respect to an element g in G is the set

$$gH := \{gh \in G \mid h \in H\}.$$

Similarly, the *right coset* of H with respect to the element g is the set $Hg := \{hg \in G \mid h \in H\}$.

The concept and notation for a coset was used by Évariste Galois (1846). However, the term *coset* was introduced by George Miller (1910).

2.2.2 Example. Viewing $\mathbb{R}^2$ as an additive abelian group, a line L through the origin is a subgroup. For any point p in $\mathbb{R}^2$, the left coset $p + L$ is the affine line containing p parallel to L . $\diamond$

2.2.3 Example. Consider the cyclic subgroup $H := \langle(2 \ 1)\rangle$ of the symmetric group $\mathfrak{S}_3$. The distinct left cosets and right cosets are

$$\begin{aligned} H &= (2 \ 1)H = \{(1), (2 \ 1)\} = H(2 \ 1) \\ (3 \ 1)H &= (3 \ 1 \ 2)H = \{(3 \ 1), (3 \ 2 \ 1)\} = H(3 \ 1) = H(3 \ 2 \ 1) \\ (3 \ 2)H &= (3 \ 2 \ 1)H = \{(3 \ 2), (3 \ 1 \ 2)\} = H(3 \ 2) = H(3 \ 1 \ 2). \end{aligned}$$

For any g in $\mathfrak{S}_3$, observe that $gH = Hg^{-1}$. $\diamond$

2.2.4 Lemma (basic properties). Let H be a subgroup of a group G .

(partition) The left cosets of H partition the elements in G .

(equivalence) The elements f and g in G belong to the same left coset of H if and only if the product $g^{-1}f$ belongs to H .

(bijection) For any element g in G , the map $h \mapsto gh$ is a bijection from the left coset $H = eH$ to the left coset gH .

Proof. It suffices to prove that left cosets are equivalence classes. The elements f and g in G are *congruent* $f \equiv g$ if there is an h in H such that $f = gh$. We verify that this is an equivalence relation.

(reflexive) Since identity element e in G belongs to H , we see that, for any element g in G , we have $g = ge$ and $g \equiv g$.

(symmetric) When $f \equiv g$, there exists an h in H such that $f = gh$, so $g = fh^{-1}$. Since $h^{-1} \in H$, it follows that $g \equiv f$.

(transitive) Suppose that $f \equiv g$ and $g \equiv g'$. Hence, there exists elements h and h' in H such $f = gh$ and $g = g'h'$, so $f = g'(h'h)$. Since $h'h \in H$, it follows that $f \equiv g'$.

To establish the equivalence property, observe that the relation $f \in gH$ is equivalent to $f \equiv g$ or $g^{-1}f \in H$.

The map that sends $f \in gH$ to the element $g^{-1}f \in H$ is the inverse to $h \mapsto gh$. Thus, the given map is a bijection. $\square$

2.2.5 Definition. For any subgroup H of a group G , the *index* $[G : H]$ is the number of distinct left cosets of H in G . Equivalently, the set $G/H := \{gH \mid g \in G\}$ of all left cosets has cardinality $[G : H]$.

The map $gH \mapsto Hg^{-1}$ defines a bijection between left and right cosets of H in G , so the index is also the number of distinct right cosets.

2.2.6 Example. Example 2.2.3 shows that $[\mathfrak{S}_3 : \langle (2\ 1) \rangle] = 3$. $\diamond$

2.2.7 Example. For a positive integer n , consider the cyclic subgroup $\langle n \rangle$ in the additive abelian group $\mathbb{Z}$. For any integer m , the left coset $m + \langle n \rangle$ consists of all integers that have the same remainder upon division by n as m . Since the possible remainders are the integers from 0 to $n - 1$, it follows that $[\mathbb{Z} : \langle n \rangle] = n$. $\diamond$

2.2.8 Example. For any positive integer n , consider the subgroup $\text{SL}(n, \mathbb{R})$ of $\text{GL}(n, \mathbb{R})$. The matrices A and B in $\text{GL}(n, \mathbb{R})$ belong to the same left coset of $\text{SL}(n, \mathbb{R})$ if and only if we have $\det(A^{-1}B) = 1$ or $\det(A) = \det(B)$. We deduce that $[\text{GL}(n, \mathbb{R}) : \text{SL}(n, \mathbb{R})] = \infty$. $\diamond$

2.2.9 Theorem (Lagrange). *For any subgroup H of a group G , we have*
 $|G| = |H| \cdot [G : H]$.

In particular, when G is a finite group, the order and index of any subgroup are divisors of the order of G .

Proof. The cosets of H partition the group G into $[G : H]$ sets and each coset has $|H|$ elements. It follows that $|G| = |H| \cdot [G : H]$. $\square$

2.2.10 Corollary. *Let G be a finite group.*

(order divisibility) For any element g in G , the order of g divides $|G|$.

(finite order) For any element g in G , we have $g^{|G|} = e$.

Proof. By definition, the order of an element g is the order of the cyclic subgroup $\langle g \rangle$. By Theorem 2.2.9, we deduce that the order of g divides $|G|$. Combining order divisibility with the finite order property in Lemma 1.2.11 proves the second part. $\square$

2.2.11 Corollary. *Every group of prime order is cyclic.*

Proof. Let G be a finite group of prime order. Choose an element $g \neq e$ in G and consider the cyclic subgroup $H := \langle g \rangle$. The inclusion $\{e, g\} \subseteq H$ implies that $|H| > 1$. As $|H|$ is a divisor of $|G|$ and $|G|$ is prime, we see that $|H| = |G|$, so $H = G$, and G is cyclic. $\square$

2.2.12 Example (Classifying groups of order at most 5). Let G be a finite group with $|G| \leq 5$. If $|G| \in \{1, 2, 3, 5\}$, then Corollary 2.2.11 shows that G is cyclic. When $|G| = 4$, Corollary 2.2.10 implies that every nonidentity element has order 2 or 4. There are two cases.

(cyclic) Suppose that G has an element g of order 4. It follows that $G = \langle g \rangle$ and the group G is cyclic.

(noncyclic) Suppose that G does not have an element of order 4.

It follows that $G = \{e, f, g, h\}$ and $f^2 = g^2 = h^2 = e$.

If $f g = e$ then we would have $f g = f^2$ and $g = f$ which cannot be. Similarly, the product $f g$ cannot equal f or g , so we must have $f g = h$. Analogous arguments show that $g f = h$, $h f = g = f h$, and $g h = f = h g$. Thus, G is the Klein 4-group; see Figure 1.2. $\diamond$

The family of matrices

$$\left\{ \begin{bmatrix} r & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \mid r \in \mathbb{R}^\times \right\}$$

forms a complete set of coset representatives for the subgroup $\text{SL}(n, \mathbb{R})$ in the group $\text{GL}(n, \mathbb{R})$.

Joseph-Louis Lagrange (1771) gives a special case of this theorem in work that predates the definition of a group. Camille Jordan (1861) first proves the general form, but attributes the basic idea to Lagrange.

2.3 Normal Subgroups

Being the kernel of a group homomorphism distinguishes a crucial class of subgroups.

2.3.1 Definition. A subgroup K of a group G is *normal* if, for any element k in K and any element g in G , the product $g k g^{-1}$ is in K .

When K is a normal subgroup of a group G , some use the notation $K \trianglelefteq G$.

2.3.2 Example. Every subgroup of an abelian group is normal. $\diamond$

2.3.3 Example. The subgroup $\langle (2\ 1) \rangle$ in $\mathfrak{S}_3$ is not normal because $(3\ 1\ 2)(2\ 1)(3\ 1\ 2)^{-1} = (3\ 1\ 2)(2\ 1)(3\ 2\ 1) = (3\ 2) \notin \langle (2\ 1) \rangle$. $\diamond$

2.3.4 Remark. For any element k in a group G , a *conjugate* of k is any element in G of the form $g k g^{-1}$ for some g in G . With this terminology, we see that a subgroup K in a group G is normal if and only if the subset K contains all the conjugates of its elements.

The matrices A and B are *similar* if and only if they are conjugate: there exists a nonsingular matrix P in $GL(n, \mathbb{R})$ such that $B = P A P^{-1}$.

2.3.5 Example. Every upper triangular matrix is similar to a lower triangular matrix, so the subgroup of upper triangular matrices is not a normal subgroup of $GL(n, \mathbb{R})$. $\diamond$

2.3.6 Example. The centre $Z(G) := \{g \in G \mid hg = gh \text{ for all } h \in G\}$ is normal because it contains all the conjugates of its elements. $\diamond$

2.3.7 Lemma. *The kernel of a group homomorphism is normal.*

Proof. Let $\varphi: G \rightarrow H$ be a group homomorphism. For any element k in $\text{Ker}(\varphi)$ and any element g in G , we have

$$\varphi(g k g^{-1}) = \varphi(g) \varphi(k) \varphi(g^{-1}) = \varphi(g) e_H \varphi(g)^{-1} = e_H,$$

so $g k g^{-1}$ is in $\text{Ker}(\varphi)$ and the subgroup $\text{Ker}(\varphi)$ is normal. $\square$

2.3.8 Example. The subgroup $SL(n, \mathbb{R})$ in $GL(n, \mathbb{R})$ is the kernel of the map $\det: GL(n, \mathbb{R}) \rightarrow \mathbb{R}^\times$, so it is normal. $\diamond$

2.3.9 Lemma. *A subgroup K of a group G is normal if and only if, for any element g in G , we have $gK = Kg$.*

Proof. Suppose that K is a normal subgroup. For any element k in K and any element g in G , we have $gk \in gK$. Since K is normal, we see that $gk g^{-1} \in K$, so $gk = (gk g^{-1})g \in Kg$ and $gK \subseteq Kg$. We also have $kg \in Kg$ and normality gives $(g^{-1})k(g^{-1})^{-1} = g^{-1}kg \in K$, so $kg = g(g^{-1}kg) \in gK$ and $Kg \subseteq gK$. We conclude that $gK = Kg$.

Conversely, suppose that $gK = Kg$ for any element g in G . Given an element $k \in K$, there exists $k' \in K$ such that $gk = k'g$. It follows that, for any element g in G , we have $gk g^{-1} \in K$. $\square$

2.3.10 Definition. Let $\mathcal{P}^*(G)$ be the set of all nonempty subsets of a group G . The *induced product* on $\mathcal{P}^*(G)$ is defined, for any subsets X and Y in $\mathcal{P}^*(G)$, by $XY := \{xy \in G \mid \text{for all } x \in X \text{ and } y \in Y\}$.

The associativity of the product in G implies that the induced product on $\mathcal{P}^*(G)$ is also associative.

2.3.11 Remark. The singleton $\{e\}$ is the identity for the product on $\mathcal{P}^*(G)$. For any element g in G , the product of any singleton $\{g\}$ with a subgroup H is the left coset gH or the right coset Hg . For any subgroup H , we also have $HH = H$.

Normal subgroups become a source of new groups.

2.3.12 Theorem. Let G/K be the family of all left cosets of a subgroup K of a group G . When K is normal, we have $(gK)(hK) = ghK$, for any elements g and h in G , and G/K is a group under this operation.

Proof. We view $(gK)(hK)$ as the product of 4 elements in $\mathcal{P}^*(G)$. The associativity of the product in $\mathcal{P}^*(G)$ and the normality of K imply that $(gK)(hK) = g(Kh)K = g(hK)K = ghK$. Hence, the product on $\mathcal{P}^*(G)$ induces a binary operation on G/K . Since the product on $\mathcal{P}^*(G)$ is associative, this binary operation on G/K also is. The left coset $K = eK$ is the identity because

$$(eK)(gK) = egK = gK = geK = (gK)(eK).$$

The inverse of the left coset gK is $g^{-1}K$ because

$$(g^{-1}K)(gK) = g^{-1}gK = eK = gg^{-1}K = (gK)(g^{-1}K). \quad \square$$

Normal subgroups correspond to group homomorphisms.

2.3.13 Corollary. For any normal subgroup K in a group G , the canonical map $\pi: G \rightarrow G/K$, defined by $\pi(g) := gK$ for any element g in G , is a group homomorphism and $\text{Ker}(\pi) = K$.

Proof. Since $(gK)(hK) = ghK$ is equivalent to $\pi(g)\pi(h) = \pi(gh)$, the map π is a surjective group homomorphism. Since the left coset K is the identity element in the quotient group G/K , it follows that $\text{Ker}(\pi) = \{g \in G \mid \pi(g) = K\} = \{g \in G \mid gK = K\} = K$. $\square$

A group homomorphism with a compatible pair of normal subgroups give rise to another group homomorphism.

2.3.14 Corollary. Let $\varphi: G \rightarrow G'$ be a group homomorphism. Assume that K is a normal subgroup of G and K' is a normal subgroup of G' such that $\varphi(K) \subseteq K'$. The induced map $\bar{\varphi}: G/K \rightarrow G'/K'$, defined by $\bar{\varphi}(gK) := \varphi(g)K'$ for any element g in G , is a group homomorphism.

Proof. Let g and h be elements of the group G . When $gK = hK$, we see that $g^{-1}h \in K$ and $\varphi(g)^{-1}\varphi(h) = \varphi(g^{-1}h) \in \varphi(K) \subseteq K'$. The equivalence criterion in Lemma 2.2.4 shows that $\varphi(g)K' = \varphi(h)K'$, so $\bar{\varphi}$ is well-defined. Since φ is a group homomorphism and both K and K' are normal subgroups, we see that

$$\begin{aligned} \bar{\varphi}((gK)(hK)) &= \bar{\varphi}(ghK) = \varphi(gh)K' = \varphi(g)\varphi(h)K' \\ &= (\varphi(g)K')(\varphi(h)K') = \bar{\varphi}(gK)\bar{\varphi}(hK). \end{aligned}$$

Hence, the map $\bar{\varphi}$ is a group homomorphism. $\square$

We can also view the elements of G/K as equivalence classes, with the multiplication $(gK)(hK) = ghK$ being independent of the choice of representatives.

When K is a normal subgroup, we call G/K the *quotient* group. When $|G| < \infty$, Theorem 2.2.9 establishes that $|G/K| = [G : K] = |G|/|K|$.

Combined with Lemma 2.3.7, we deduce that a subgroup is normal if and only if it is the kernel of some group homomorphism.

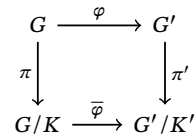


Figure 2.1: The commutative diagram for Corollary 2.3.14

2.4 Exercises

2.4.1 Problem. Determine which of the following statements are true. If a statement is false, then provide a counterexample.

- i. For any group G , there exists a unique group homomorphism from μ_1 to G and a unique group homomorphism from G to μ_1 .
- ii. The symmetric groups $\mathfrak{S}_0$ and $\mathfrak{S}_1$ are isomorphic.
- iii. All groups of order two are isomorphic.
- iv. There is an isomorphism $D_n \cong \mathfrak{S}_n$ for all positive integers n .
- v. The multiplicative group $\mathbb{C}^\times$ is isomorphic to $\mathbb{T} \times \mathbb{R}_{>0}$.
- vi. The map $\varphi: \mathbb{R} \rightarrow \mathrm{SL}(2, \mathbb{R})$, defined by $\varphi(r) := \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix}$ for any real number r , is a group isomorphism.
- vii. For any positive integer n , we have $[\mathrm{O}(n, \mathbb{R}) : \mathrm{SO}(n, \mathbb{R})] = 2$.
- viii. For any set X , the direct product $(\mu_2)^X$ is isomorphic to the group on the power set $\mathcal{P}(X)$ whose product is the symmetric difference operation.
- ix. The subgroup $\{(1), (2\ 1)(4\ 3), (3\ 1)(4\ 2), (3\ 2)(4\ 1)\}$ is a normal subgroup of $\mathfrak{S}_4$.
- x. For any nonnegative integer n , the group $\mathfrak{S}_n$ is isomorphic to the subgroup of $\mathrm{GL}(n, \mathbb{Z})$ consisting of matrices having exactly one entry equal to 1 in each row and each column, and all other entries equal to 0.
- xi. The Klein 4-group is isomorphic to quotient of the quaternion group by its centre.
- xii. Every subgroup of the quaternion group is normal.
- xiii. If H is a subgroup of a group G such that $[G : H] = 2$, then H is a normal subgroup.

2.4.2 Problem. Let H and K be two subgroups of a group G . For any element g in G , the set

$$H g K := \{f \in G \mid f = h g k \text{ for some } h \in H, k \in K\}$$

is called a *double coset*.

- i. Prove that the double cosets partition G .
- ii. Do all double cosets have the same cardinality?
- iii. When G has finite order, must the cardinality of a double coset divide $|G|$?

2.4.3 Problem. Let G be a group and let $\mathrm{Aut}(G)$ be its automorphism group. For any element g in G , consider the map $\gamma_g: G \rightarrow G$ defined, for any element f in G , by $\gamma_g(f) := g f g^{-1}$.

- i. For any element g in G , show that γ_g is an automorphism.
- ii. Prove that the map $\Gamma: G \rightarrow \mathrm{Aut}(G)$ defined, for any element g in G , by $\Gamma(g) := \gamma_g$ is a group homomorphism.
- iii. Show that $\mathrm{Ker}(\Gamma) = Z(G)$.
- iv. Prove that $\mathrm{Im}(\Gamma)$ is a normal subgroup of $\mathrm{Aut}(G)$.

2.4.4 Problem. Fix a nonnegative integer n . Two permutations σ and τ in the symmetric group $\mathfrak{S}_n$ have the *same cycle structure* if, for any nonnegative integer k , their factorizations into disjoint cycles have the same number of cycles of length k . The *cycle type* of a permutation is the list λ of cycles lengths from its factorization into disjoint cycles arranged in non-increasing order.

- i. For any permutations σ and τ in $\mathfrak{S}_n$, prove that the conjugate permutation $\sigma \tau \sigma^{-1}$ has the same cycle structure as τ and may be obtained by applying σ to the entries in the cycles of τ .
- ii. Prove that permutations are conjugate if and only if they have the same cycle type.