1.8 Isomorphism Theorems

Copyright © 2020, Gregory G. Smith
Last updated: 2020–09–13

The isomorphism theorems describe relations between quotients, homomorphisms, and subobjects.

1.8.1 Theorem (First Isomorphism). *Let $\varphi : G \to H$ be a group homomorphism with kernel $K := \operatorname{Ker}(\varphi)$. The induced map $\widetilde{\varphi} : G/K \to \operatorname{Im}(\varphi)$ defined by $\widetilde{\varphi}(gK) := \varphi(g)$ is an isomorphism from the quotient group to the image. Writing $\pi : G \to G/\operatorname{Ker}(\varphi)$ for the canonical surjection and $\iota : \operatorname{Im}(\varphi) \to H$ for the canonical injection, we also have $\varphi = \iota \circ \widetilde{\varphi} \circ \pi$.*

Originally formulated for modules by Emmy Noether (1927), versions exist for groups, rings, vector spaces, modules, Lie algebra, and various other algebraic structures.

Proof. Saying that two elements $f, g \in G$ represent the same left coset means that $fK = gK$ which is equivalent to $f^{-1}g \in K$. Since φ is a group homomorphism, we have $\varphi(f) = \varphi(g)$ if and only if $\varphi(f^{-1}g) = e_H$. It follows that $\widetilde{\varphi}$ is a well-defined map from G/K. The kernel K being a normal subgroup and the map φ being a group homomorphism imply that

$$\widetilde{\varphi}\big((fK)(gK)\big) = \widetilde{\varphi}(fgK) = \varphi(fg) = \varphi(f)\,\varphi(g) = \widetilde{\varphi}(fK)\,\widetilde{\varphi}(gK),$$

so the map $\widetilde{\varphi}$ is a group homomorphism. By construction, the map $\widetilde{\varphi}$ is surjective and its kernel is the left coset K. Therefore, the map $\widetilde{\varphi}$ is an isomorphism. The second part follows immediately from the definition of $\widetilde{\varphi}$. □

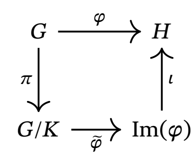

Figure 1.8: Commutative diagram arising from Theorem 1.8.1

1.8.2 Corollary. *All cyclic groups of a given finite order are isomorphic.*

Proof. Let m be a positive integer and let $G := \langle g \rangle$ denote a cyclic group of order m. Lemma 1.4.5 establishes that the map $\eta_g : \mathbb{Z} \to G$, defined for all $n \in \mathbb{Z}$ by $\eta_g(n) := g^n$, is a group homomorphism. Since g generates G, the map η_g is surjective. Lemma 1.2.10 proves that $\operatorname{Ker}(\eta) = \langle m \rangle$. Thus, the First Isomorphism Theorem shows that G is isomorphic to the quotient group $\mathbb{Z}/\langle m \rangle$. □

1.8.3 Example. The exponential function $\xi : \mathbb{R} \to S^1$, defined by $\xi(x) := \exp(2\pi \mathrm{i} x) = \cos(2\pi x) + \mathrm{i}\sin(2\pi x)$, is a surjective group homomorphism. Since $\operatorname{Ker}(\xi) = \{x \in \mathbb{R} \mid \exp(2\pi \mathrm{i} x) = 1\} = \mathbb{Z}$, the First Isomorphism Theorem shows that $\mathbb{R}/\mathbb{Z} \cong S^1$. ◇

1.8.4 Lemma. *Let H be a subgroup of a group G. For any normal subgroup K of G, the product HK is a subgroup of G and $HK = KH$.*

Proof. Suppose that $h \in H$ and $k \in K$. Since K is normal, we have $k' := hkh^{-1} \in K$ and $hk = (hkh^{-1})h = k'h \in KH$, so $HK \subseteq KH$. We also have $k'' := h^{-1}kh \in K$ and $kh = h(h^{-1}kh) = hk'' \in HK$, so $KH \subseteq HK$. We conclude that $HK = KH$.

It remains to show that the product HK is a subgroup of G. Since $e_G \in H$ and $e_G \in K$, the product HK is nonempty. Given elements $h'k', hk \in HK$, it follows that $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ and $h'k'(hk)^{-1} \in HKHK = HHKK = HK$. □

1.8.5 Theorem (Second Isomorphism). *Let G be a group, let H be a subgroup of G, and let K be a normal subgroup of G. The product KH is a subgroup of G, the intersection $K \cap H$ is a normal subgroup of H, and the quotient groups $H/(K \cap H)$ and KH/K are isomorphic.*

Let K and H be subgroups of a group G such that $K \subseteq H$. If K is a normal subgroup of G, then K is a normal subgroup of H; indeed, the condition $gkg^{-1} \in K$ for all $g \in G$ implies that $hkh^{-1} \in K$ for all $h \in H$.

Proof. Since K is a normal subgroup of G, Lemma 1.8.4 establishes that K is a normal subgroup of HK. For all $g \in KH$, we claim that the left coset $gK \in KH/K$ is of the form hK for some $h \in H$. By definition, we have $g = kh$ for some $k \in K$ and $h \in H$. We also have $k'' := h^{-1}kh \in K$ and $kh = hh^{-1}kh = hk'$, so $khK = hk'K = hK$. It follows that the map $\varphi : H \to KH/K$ defined by $\varphi(h) := hK$ is surjective. Since $\varphi = \pi|_H$ where $\pi : G \to G/K$ is the canonical map, the map φ is a group homomorphism. Because $\operatorname{Ker}(\pi) = K$, we have $\operatorname{Ker}(\varphi) = K \cap H$ so $K \cap H$ is a normal subgroup of H. Thus, the First Isomorphism Theorem gives $H/(K \cap H) \cong KH/K$. □

1.8.6 Theorem (Third Isomorphism). *Let H and K be normal subgroups of a group G. When K is also a subgroup of H, the quotient H/K is a normal subgroup of G/K and the quotient G/H is isomorphic to $(G/K)/(H/K)$.*

Proof. As K is a normal subgroup of the group G, the identity map on G induces a surjective group homomorphism $\varphi : G/K \to G/H$ defined by $\varphi(gK) := gH$. Since we have

$$\operatorname{Ker}(\varphi) = \{gK \mid gH = H\} = \{gK \mid g \in H\} = H/K\,,$$

the quotient group H/K is a normal subgroup of G/K. Thus, the First Isomorphism Theorem gives $G/H \cong (G/K)/(H/K)$. □

1.8.7 Theorem (Correspondence). *Given a normal subgroup K of a group G, the canonical map $\pi : G \to G/K$ induces a bijection between the set of all subgroups of G containing K and the set of all subgroups of the quotient G/K.*

Most properties of subgroups are preserved under this bijection. For instance, given any two subgroups H and H' of G containing K, we have
- $H \subseteq H'$ if and only if $H/K \subseteq H'/K$
- $[H' : H] = [H'/K : H/K]$ whenever $H \subseteq H'$
- $(H \cap H')/K = (H/K) \cap (H'/K)$
- H is a normal subgroup of G if and only if H/K is a normal subgroup of the quotient G/K.

Proof. Given a subgroup H of G containing K, the induced image $\pi(H) = \{hK \mid h \in H\} = H/K$ is a subgroup of the quotient G/K because $g, h \in H$ implies that $(gK)(hK)^{-1} = gh^{-1}K \in H/K$.

Given a subgroup U of the quotient G/K, consider the preimage $\pi^{-1}(U) = \{g \in G \mid \pi(g) \in U\}$. The left coset K is the identity in the quotient group G/K, so the preimage $\pi^{-1}(U)$ contains the subgroup K. For any $f, g \in \pi^{-1}(U)$, it follows that $\pi(f), \pi(g) \in U$ and $\pi(f)\pi(g)^{-1} = \pi(fg^{-1}) \in U$. Since $fg^{-1} \in \pi^{-1}(U)$, we deduce that $\pi^{-1}(U)$ is a subgroup of G containing subgroup K.

By construction, these two induced maps are mutual inverses. Thus, the canonical map $\pi : G \to G/K$ induces a bijection between the set of all subgroups of G containing K and the set of all subgroups of the quotient G/K. □

1.9 Orbits and Stablizers

Copyright © 2020, Gregory G. Smith
Last updated: 2020–09–14

Having a group act on a set reveals some valuable subgroups and subsets. These fundamental ideas have a surprisingly wide range of applications within group theory and beyond.

1.9.1 Definition. Let G be a group acting on a set X and fix $x \in X$. The ***orbit*** of the element x is the subset $\operatorname{orb}_G(x) := \{g\,x \mid g \in G\} \subseteq X$. The ***stabilizer*** of x is the subgroup $\operatorname{stab}_G(x) := \{g \in G \mid gx = x\}$ of G. The group G acts ***transitively*** on the set X if there is only one orbit, and it acts ***freely*** on X if every stabilizer is the trivial group $\{e\}$.

For all $g, h \in \operatorname{stab}_G(x)$, we have $h^{-1}x = h^{-1}hx = ex = x$ and $gh^{-1}x = gx = x$, so $gh^{-1} \in \operatorname{stab}_G(x)$. Hence, Lemma 1.2.2 implies that $\operatorname{stab}_G(x)$ is a subgroup.

1.9.2 Example. The symmetric group $\mathfrak{S}_n$ acts transitively on finite set $[n]$. The stabilizer of $n \in [n]$ is the subgroup $\mathfrak{S}_{n-1}$ of $\mathfrak{S}_n$. ◇

1.9.3 Example. Since any unit vector is part of an orthonormal basis, $\mathrm{O}(n, \mathbb{R})$ and $\mathrm{SO}(n, \mathbb{R})$ act transitively on the sphere $S^{n-1} \subset \mathbb{R}^n$. ◇

1.9.4 Example. For any integer greater than 1, the dihedral group D_n acts transitively on the vertices of the regular polygon with n edges. For any vertex v of the regular polygon, we have $|\operatorname{stab}_{D_n}(v)| = 2$ because the stabilizer contains the identity and a reflection. ◇

1.9.5 Example. Suppose that a group G acts on its underlying set by left translation. For any $g \in G$, we see that $\operatorname{orb}_G(g) = G$ because $\lambda_{hg^{-1}}(g) = hg^{-1}(g) = h$ for all $h \in G$. We also have $\operatorname{stab}_G(g) = \{e\}$ because $g = \lambda_h(g) = hg$ implies that $h = e$. ◇

1.9.6 Example. Suppose that a group G acts on itself by conjugation. For any $g \in G$, the orbit

$$\operatorname{orb}_G(g) = \{f \in G \mid f := hgh^{-1} \text{ for some } h \in G\}$$

is the ***conjugacy class*** of g, and the stabilizer

$$\operatorname{stab}_G(g) = \{h \in G \mid hgh^{-1} = g\} = C_G(g)$$

is the centralizer of the element g. ◇

1.9.7 Example. Every group G acts on its subgroups by conjugation. An element $g \in G$ acts on the subgroup H of G by sending it to gHg^{-1}. The orbit $\operatorname{orb}_G(H)$ consists of all conjugates of the subgroup H. Hence, the subgroup H has a trivial orbit if and only if H is normal. The stabilizer $N_G(H) := \operatorname{stab}_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is the ***normalizer*** of the subgroup H. ◇

For all gfg^{-1}, ghg^{-1}, we have $gfg^{-1}(ghg^{-1})^{-1} = gfh^{-1}g^{-1} \in gHg^{-1}$, so Lemma 1.2.2 implies that gHg^{-1} is a subgroup of G.

1.9.8 Proposition. *When a group G acts on a set X, the set X is the disjoint union of the orbits.*

Proof. It suffices to prove that orbits are equivalence classes: $x \equiv y$ if and only if there is $g \in G$ with $y = gx$. We verify that this is an equivalence relation.

(transitive) If $x \equiv y$ and $y \equiv z$ then $y = gx$ and $z = hy$ for some $g, h \in G$. Hence, $z = hgx$. Since $hg \in G$, we have $x \equiv z$.

(symmetric) If $x \equiv y$, then $y = gx$ for some $g \in G$. Hence, $x = g^{-1}y$ so $y \equiv x$.

(reflexive) Since $e \in G$, $x = ex$ and $x \equiv x$. □

1.9.9 Theorem. *Assume that the group G acts on the set X. For all $x \in X$, the cardinality of its orbit is $|\mathrm{orb}_G(x)| = [G : \mathrm{stab}_G(x)]$.*

Proof. Let E be the set of all left cosets of the subgroup $\mathrm{stab}_G(x)$ in G. We claim that the map $\psi : E \to \mathrm{orb}_G(x)$ defined, for all $g \in G$, by $\psi\big(g\,\mathrm{stab}_G(x)\big) := gx$ is a bijection.

(well-defined) Suppose that $g, h \in G$ satisfy $g\,\mathrm{stab}_G(x) = h\,\mathrm{stab}_G(x)$. It follows that there exists $f \in \mathrm{stab}_G(x)$ such that $h = gf$. As $fx = x$, we see that $hx = gfx = gx$.

(injective) Suppose that $gx = \psi\big(g\,\mathrm{stab}_G(x)\big) = \psi\big(h\,\mathrm{stab}_G(x)\big) = hx$. It follows that $h^{-1}gx = x$. We deduce that $h^{-1}g \in \mathrm{stab}_G(x)$ and $g\,\mathrm{stab}_G(x) = h\,\mathrm{stab}_G(x)$.

(surjective) Suppose that $y \in \mathrm{orb}(x)$. It follows that there exists $g \in G$ such that $y = gx$. Hence, we have $y = gx = \psi\big(g\,\mathrm{stab}_G(x)\big)$. □

1.9.10 Example. Let G be a finite group. An element $x \in G$ has a unique conjugate if and only if it belongs to the center $Z(G)$. By partitioning G into conjugacy classes, we obtain the ***class equation***:

$$|G| = |Z(G)| + \textstyle\sum_i [G : C_G(x_i)]$$

where one element x_i is selected from each conjugacy class having more that one element. ◇

When a finite group acts on a set, the cardinality of any orbit divides the order of the group.

1.9.11 Corollary (Counting formula)**.** *Assume that the finite group G acts on the set X. For all $x \in X$, we have $|G| = |\mathrm{orb}_G(x)|\,|\mathrm{stab}_G(x)|$.*

Proof. Combine Theorem 1.6.9 and Theorem 1.9.9. □

Every finite subgroup of $\mathrm{SO}(3, \mathbb{R})$ is one of the following:

- a cyclic group of rotations by multiples of $2\pi/k$ about a line;
- a dihedral group consisting of the automorphisms of a regular polygon with k edges;
- a tetrahedral group consisting of the 12 rotations carrying a regular tetrahedron to itself;
- a octahedral group consisting of the 24 rotations carrying a regular octahedron to itself;
- the icosahedral group consisting of 60 rotations carrying a regular dodecahedron or regular icosahedron to itself.

1.9.12 Example. For any finite group G, the number of conjugates of $x \in G$ is the index of its centralizer and hence a divisor of $|G|$. ◇

1.9.13 Example. Let G be a finite group. The number of conjugates of a subgroup H is $[G : N_G(H)]$ and hence a divisor of $|G|$. ◇

1.9.14 Example. Let G be the subgroup G of $\mathrm{SO}(3, \mathbb{R})$ that preserves a regular dodecahedron. The stabilizer of a pentagonal face s is the group of rotations by $2\pi/5$ about a perpendicular through its center, so $|\mathrm{stab}(s)| = 5$. There are 12 faces and G acts transitively on them, so $|G| = 5 \cdot 12 = 60$. Alternatively, G operates transitively on the vertices v. There are 3 rotations which fix a vertex so $|\mathrm{stab}(v)| = 3$. Since there are 20 vertices, we have $|G| = 3 \cdot 20 = 60$. Similarly, if e is an edge, then we have $|\mathrm{stab}(e)| = 2$ so $|G| = 2 \cdot 30 = 60$. ◇