

3 Groups in Action

Copyright © 2025 by Gregory G. Smith
Last updated: 2025-09-24

To gain a deeper understanding of groups, one must capitalize on intrinsic isomorphisms and the ubiquity of group actions.

3.0 Isomorphism Theorems

We describe some universal features of homomorphisms, quotients, and subobjects. The first of these generalizes the result that every function can be factored as a surjection followed by an injection.

3.0.1 First Isomorphism Theorem (Noether). *Let $\varphi: G \rightarrow H$ be a group homomorphism and set $K := \text{Ker}(\varphi)$. The map $\hat{\varphi}: G/K \rightarrow \text{Im}(\varphi)$, defined by $\hat{\varphi}(gK) := \varphi(g)$ for any element g in G , is a group isomorphism. When $\pi: G \rightarrow G/K$ denotes the canonical surjection and $\iota: \text{Im}(\varphi) \rightarrow H$ is the canonical injection, we also have $\varphi = \iota \circ \hat{\varphi} \circ \pi$.*

Proof. Lemma 2.2.4 shows that the elements f and g in G represent the same left coset of K if and only if the product $f^{-1}g$ belongs to K . Since φ is a group homomorphism, we have $\varphi(f) = \varphi(g)$ if and only if $\varphi(f^{-1}g) = \varphi(f)^{-1}\varphi(g) = e_H$. As $K = \text{Ker}(\varphi)$, it follows that $\hat{\varphi}$ 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

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

so the induced map $\hat{\varphi}$ is a group homomorphism. By construction, the map $\hat{\varphi}$ is surjective, and its kernel is the left coset K . Therefore, the map $\hat{\varphi}$ is an isomorphism. The factorization $\varphi = \iota \circ \hat{\varphi} \circ \pi$ follows from the definition of the induced map $\hat{\varphi}$. $\square$

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

Proof. Fix a positive integer m and let $G := \langle g \rangle$ be a cyclic group of order m . Lemma 2.0.5 implies that the map $\eta_g: \mathbb{Z} \rightarrow G$, defined by $\eta_g(n) := g^n$ for any integer n , is a group homomorphism. Since g generates G , the map η_g is surjective. Lemma 1.2.11 proves that $\text{Ker}(\eta_g) = \langle m \rangle$. Thus, the First Isomorphism Theorem shows that G is isomorphic to the quotient group $\mathbb{Z}/\langle m \rangle$. $\square$

3.0.3 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. For any h in H and any k in K , the normality of K implies that $k' := hkh^{-1} \in K$ 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 $KH \subseteq HK$. It follows that $HK = KH$.

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

Originally formulated for modules by [Emmy Noether \(1927\)](#), versions of the four “isomorphism theorems” exist for groups, rings, vector spaces, modules, Lie algebra, and various other algebraic structures.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \pi \downarrow & & \uparrow \iota \\ G/\text{Ker}(\varphi) & \xrightarrow[\cong]{\hat{\varphi}} & \text{Im}(\varphi) \end{array}$$

Figure 3.1: The commutative diagram for the First Isomorphism Theorem

As an example, we have $\mathbb{Z}/\langle m \rangle \cong \mu_m$ for any positive integer m .

3.0.4 Second Isomorphism Theorem. *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.*

Proof. Since K is a normal subgroup of G , Lemma 3.0.3 shows that K is a normal subgroup of HK . Consider the map $\varphi: H \rightarrow KH/K$ defined by $\varphi(h) := hK$ for any h in H . This map is the restriction of the canonical map $\pi: G \rightarrow G/K$ to the subgroup H , so it is a group homomorphism. To see that φ is surjective, we first claim that, for any g in KH , the coset $gK \in KH/K$ equals hK for some h in H . By definition, there exists k in K and h in H such that $g = kh$. The normality of the subgroup K implies that $k'' := h^{-1}kh \in K$ and $g = kh = hh^{-1}kh = hk''$, so $gK = khK = hk''K = hK = \varphi(h)$. Thus, φ is surjective. The kernel of φ is $\{h \in H \mid hK = K\} = H \cap K$, so $K \cap H$ is a normal subgroup of H . Thus, the First Isomorphism Theorem gives $H/(K \cap H) \cong KH/K$. $\square$

3.0.5 Third Isomorphism Theorem. *For any nested pair (K, H) of normal subgroups in a group G , 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 G , the identity map $\text{id}_G: G \rightarrow G$ induces a surjective group homomorphism $\varphi: G/K \rightarrow G/H$ defined by $\varphi(gK) := gH$ for any element g in G . Since we have

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

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

3.0.6 Correspondence Theorem. *Let G be a group. For any normal subgroup K of G , the canonical map $\pi: G \rightarrow G/K$ induces a bijection between the set of all subgroups of G containing K and the set of all subgroups of the quotient G/K .*

Proof. For any 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 $(gK)(hK)^{-1} = gh^{-1}K \in H/K$.

For any 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 elements f and g in $\pi^{-1}(U)$, it follows that $\pi(f)$ and $\pi(g)$ are in U , so $\pi(f)\pi(g)^{-1} = \pi(fg^{-1}) \in U$. Since $fg^{-1} \in \pi^{-1}(U)$, we deduce that $\pi^{-1}(U)$ is a subgroup of G containing subgroup K .

By construction, the maps induced on subgroups by π and π^{-1} are mutual inverses. Thus, the canonical map $\pi: G \rightarrow G/K$ induces a bijection between the set of subgroups of G containing K and the set of subgroups of the quotient group G/K . $\square$

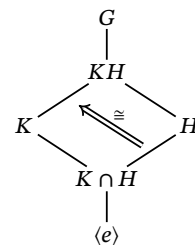


Figure 3.2: Hasse diagram for the Second Isomorphism Theorem

A pair (K, H) of subgroups in G is *nested* if $K \subseteq H$. If K is a normal subgroup of G , then K is a normal subgroup of H : the condition $gkg^{-1} \in K$ for any g in G implies that $hkh^{-1} \in K$ for any h in H .

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 $H/K \subseteq H'/K$
- $[H' : H] = [H'/K : H/K]$ if $H \subseteq H'$
- $(H \cap H')/K = (H/K) \cap (H'/K)$
- H is a normal subgroup of G if and only if H/K is a normal subgroup of the quotient G/K .

3.1 Orbits and Stabilizers

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

3.1.1 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 $\text{orb}_G(x) := \{gx \in X \mid g \in G\}$ and the *stabilizer* of x is the subgroup $\text{stab}_G(x) := \{g \in G \mid gx = x\}$. 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 $\langle e \rangle$.

For any elements g and h in $\text{stab}_G(x)$, we have $h^{-1}x = h^{-1}hx = ex = x$ and $gh^{-1}x = gx = x$, so $gh^{-1} \in \text{stab}_G(x)$. Hence, Lemma 1.2.2 implies that $\text{stab}_G(x)$ is a subgroup of the group G .

3.1.2 Example. Let n be a nonnegative integer. By definition, the symmetric group $\mathfrak{S}_n$ acts transitively on the finite set $[n]$ and the stabilizer of the element n in $[n]$ is the subgroup $\mathfrak{S}_{n-1}$ of $\mathfrak{S}_n$. $\diamond$

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

3.1.4 Example. Suppose that a group G acts on itself by conjugation. The *conjugacy class* of an element g in G is the orbit

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

and the stabilizer $\text{stab}_G(g) = \{h \in G \mid hgh^{-1} = g\} = C_G(g)$ is the centralizer of the element g . $\diamond$

3.1.5 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 the subgroup gHg^{-1} in $\mathcal{P}^*(G)$. The orbit $\text{orb}_G(H)$ consists of all conjugates of the subgroup H . Remark 2.3.4 implies that the subgroup H has a trivial orbit if and only if H is normal. The stabilizer

Let f and h be elements of a subgroup H of a group G . For any element g in G , it follows that $fh^{-1} \in H$ and $gfg^{-1}(ghg^{-1})^{-1} = gfh^{-1}g^{-1} \in gHg^{-1}$, so Lemma 1.2.2 demonstrates that $gHg^{-1} \in \mathcal{P}^*(G)$ is a subgroup of G .

$$N_G(H) := \text{stab}_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

is the *normalizer* of the subgroup H . $\diamond$

3.1.6 Proposition. Whenever a group G acts on a set X , the G -orbits partition the elements in X .

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

(*reflexive*) For the identity e in G , we have $x = ex$, so $x \equiv x$.

(*symmetric*) When $x \equiv y$, there exists an element g in G such that $y = gx$. It follows that $x = g^{-1}y$, so $y \equiv x$.

(*transitive*) When $x \equiv y$ and $y \equiv z$, there exists elements g and h in G such that $y = gx$ and $z = hy$. It follows that $z = hgx$. Since $hg \in G$, we have $x \equiv z$. $\square$

3.1.7 Theorem. *Let G be a group acting on the set X . For any element x in X , the cardinality of its orbit is the index of its stabilizer:*

$$|\text{orb}_G(x)| = [G : \text{stab}_G(x)].$$

Proof. Set $H := \text{stab}_G(x)$ and let G/H denote the set of left cosets of the subgroup H in G . We claim that the map $\psi : G/H \rightarrow \text{orb}_G(x)$, defined by $\psi(gH) := gx$ for any element g in G , is a bijection.

We first show that ψ is well-defined. Lemma 2.2.4 proves that the elements f and g in G represent the same left coset of H if and only if $f^{-1}g \in H$. Hence, there exists an element h in H such that $fh = g$. As h belongs to the stabilizer, we have $hx = x$ and $gx = fhx = fx$, so the map ψ is well-defined.

We next show that ψ is injective. For any elements f and g in G satisfying $fx = \psi(fH) = \psi(gH) = gx$, we see that $g^{-1}fx = x$. Thus, we deduce that $g^{-1}f \in H$ and Lemma 2.2.4 yields $fH = gH$.

Lastly, we show that ψ is surjective. For any element y in $\text{orb}(x)$, there exists an element g in G such that $y = gx$, which implies that $y = gx = \psi(gH)$. $\square$

3.1.8 Example. Let G be a finite group. An element x in G has a unique conjugate if and only if it is in the centre $Z(G)$. Partitioning G into conjugacy classes, we obtain the *class equation*:

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

where one element x_i in G is selected from each conjugacy class having more than one element. $\diamond$

3.1.9 Corollary. *Let G be a finite group acting on a set X . For any element x in X , we have $|G| = |\text{orb}_G(x)| \cdot |\text{stab}_G(x)|$.*

Proof. Combine Theorem 2.2.9 and Theorem 3.1.7. $\square$

3.1.10 Example. For any finite group G , the number of conjugates of an element g in G is $[G : C_G(g)]$ and, thereby, a divisor of $|G|$. $\diamond$

3.1.11 Example. Let G be a finite group. The number of conjugates of a subgroup H is $[G : N_G(H)]$ and, thereby, a divisor of $|G|$. $\diamond$

3.1.12 Example. Let G be the subgroup of $\text{SO}(3, \mathbb{R})$ 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 centre, so $|\text{stab}(s)| = 5$. 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 $|\text{stab}(v)| = 3$. Since there are 20 vertices, we have $|G| = 3 \cdot 20 = 60$. Similarly, if e is an edge, then we have $|\text{stab}(e)| = 2$ so $|G| = 2 \cdot 30 = 60$. $\diamond$

3.2 The First Sylow Theorem

For any finite group, Lagrange Theorem establishes that the order of every subgroup divides the order of the group. For prime powers, the First Sylow Theorem proclaims a partial converse.

3.2.1 Definition. A finite group is a *p-group* if its order is a power of the prime number p .

3.2.2 Example. The cyclic group μ_4 and the Klein 4-group are both 2-groups of order 4, but they are not isomorphic; see Example 2.2.12. The dihedral group D_4 is a nonabelian 2-group of order 8. $\diamond$

3.2.3 Proposition. Let G be a p -group acting on a finite set X . Setting $X^G := \{x \in X \mid gx = x \text{ for all } g \in G\}$, we have $|X^G| \equiv |X| \pmod{p}$.

Throughout this section, the letter p denotes a prime integer.

The subset X^G is the fixed-point set: the elements in X that do not change under the group action.

Proof. Proposition 3.1.6 implies that the subset $X \setminus X^G$ is a disjoint union of orbits having cardinality greater than 1. Corollary 3.1.9 shows that the cardinality of each such orbit is a nontrivial power of p and, thereby, divisible by p . $\square$

3.2.4 Corollary. The centre of a p -group is nontrivial.

Proof. Let G be a p -group acting on itself by conjugation. The fixed-point set is $Z(G) = \{g \in G \mid f g f^{-1} = g \text{ for all } f \in G\}$. It follows that $|Z(G)| \equiv |G| \equiv 0 \pmod{p}$, so $|Z(G)| \neq 1$ and $Z(G) \neq \langle e \rangle$. $\square$

3.2.5 Definition. A *Sylow p -subgroup* is p -group of largest possible order: for any group G where $|G| = p^r m$ and m is not a multiple of p , a Sylow p -subgroup has order p^r .

A subgroup that is a p -group is a Sylow p -subgroup if and only if its index is not a multiple of p .

3.2.6 Example. Any cyclic subgroup of $\mathfrak{S}_p$ generated by a cycle of length p is a Sylow p -group because p does not divide $(p-1)!$. $\diamond$

3.2.7 Lemma (Wielandt). For a positive integer $n = p^r m$ where the prime p does not divide m , we have $\binom{n}{p^r} \not\equiv 0 \pmod{p}$.

Helmut Wielandt (1959) gives a much simpler proof for the existence of the Sylow groups.

Proof. Fix a group G of order p^r and a set T of cardinality m . Set $X := G \times T$. Consider the set Y consisting of the subsets of X having cardinality p^r . By construction, we have $|X| = n$ and $|Y| = \binom{n}{p^r}$. The group G acts on X by $g(f, t) := (gf, t)$ for any g and f in G and any t in T . This action extends to Y . The fixed-point set Y^G is the set of orbits of X . Elements in Y^G are subsets of X having the form $G \times \{t\}$ where $t \in T$, so $|Y^G| = m$. Lastly, Proposition 3.2.3 implies that $\binom{n}{p^r} = |Y| \equiv |Y^G| = m \not\equiv 0 \pmod{p}$. $\square$

3.2.8 First Sylow Theorem. For any prime number p , every finite group has a Sylow p -subgroup.

All three eponymous theorems originate in Ludwig Sylow (1872).

Proof. Let G be a finite group with $|G| = n = p^r m$ where r is a non-negative integer and m is not a multiple of p . Setting X to be the set of subsets of G having cardinality p^r , Lemma 3.2.7 establishes that $|X| = \binom{n}{p^r} \not\equiv 0 \pmod{p}$. Left translation induces an action of G on X . Since $|X|$ is the sum of the cardinalities of the G -orbits, there is U in X whose G -orbit has nonzero cardinality modulo p . Thus, Corollary 3.1.9 implies that $p^r m = |G| = |\text{stab}_G(U)| |\text{orb}_G(U)|$, so p^r divides $|\text{stab}_G(U)|$. However, $\text{stab}_G(U)$ consists of the elements g in G such that $gU = U$. If u in U , then $\text{stab}_G(U) \subseteq Uu^{-1}$ whence $|\text{stab}_G(U)| \leq |U| = p^r$. We conclude that $|\text{stab}_G(U)| = p^r$. $\square$

3.2.9 Corollary (Cauchy). *Any group whose order is divisible by a prime number p contains an element of order p .*

Proof. By the First Sylow Theorem, there exists a subgroup of order p^r for some positive integer r . Choose a nonidentity element g in this subgroup. By the Lagrange Theorem, the order of g divides p^r . Hence, there exists an integer k such that $0 < k \leq r$ and g has order p^k . It follows that the element $g^{p^{k-1}}$ has order p . $\square$

3.2.10 Example (Classifying groups of order 6). We claim that there are two isomorphism classes for groups of order 6: the class of the cyclic group μ_6 and the class of the symmetric group $\mathfrak{S}_3$.

Consider a group G of order 6. Applying Corollary 3.2.9, let f be an element of order 3 and let g be an element of order 2 in G . We first show that the six products $f^i g^j$, where $0 \leq i \leq 2$ and $0 \leq j \leq 1$, are distinct. Indeed, the equation $f^i g^j = f^r g^s$ implies that $f^{i-r} = g^{s-j}$. Every power of f except the identity has order 3 and every power of g except the identity has order 2, so $f^{i-r} = g^{s-j} = e$, $r = i$, and $s = j$. We deduce that $G = \{e, f, f^2, g, fg, f^2g\}$. The product gf must be one of these elements. It is not possible that $gf = g$ because $f \neq e$. Similarly, we see that $gf \neq e$, $gf \neq f$, and $gf \neq f^2$. It follows that $gf = fg$ or $gf = f^2g$. Either of these relations, combined with $f^3 = e$ and $g^2 = e$, completely determine the multiplication table for the group. Thus, there are at most two isomorphism classes of groups of order 6 and we already know two: μ_6 and $\mathfrak{S}_3$. $\diamond$

3.2.11 Corollary. *Any group of order p^2 is abelian.*

Proof. Let G be a group of order p^2 . Its centre $Z(G)$ is a subgroup, so it has order 1, p , or p^2 . Corollary 3.2.4 proves that $|Z(G)| > 1$ and Corollary 3.2.9 shows that $Z(G)$ has an element f of order p . The cyclic group $H := \langle f \rangle$ is a subgroup of $C_G(g)$ for all g in G . If $g \in G$ and $g \notin H$, then we have $|C_G(g)| > p$. Since $|C_G(g)|$ divides p^2 , we obtain $|C_G(g)| = p^2$, $C_G(g) = G$, and $g \in Z(G)$. Since every element of G belongs to $Z(G)$, the group G must be abelian. $\square$

This presentation reverses history: [Augustin Louis Cauchy \(1844\)](#) was a crucial ingredient in the original proof of the First Sylow Theorem.

We deduce that the symmetric group $\mathfrak{S}_3$ must be isomorphic to the dihedral group D_3 .

★	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	fg	f^2g	e	f	f^2
fg	fg	f^2g	g	f	f^2	e
f^2g	f^2g	g	fg	f^2	e	f

★	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	fg	f	e	f
f^2g	f^2g	fg	g	f^2	f	e

Figure 3.3: The two multiplication tables for groups of order 6

3.3 The Other Sylow Theorems

The First Sylow Theorem states that, for every prime factor p of the order of a finite group, there exists a Sylow p -subgroup. The Second and Third Sylow Theorems refine this existence result.

Throughout this section, the letter p continues to denote a prime integer.

3.3.1 Second and Third Sylow Theorems. *Let G be a finite group.*

- ii. *Every subgroup that is a p -group is contained in a Sylow p -subgroup.*
- iii. *The Sylow p -subgroups of G are conjugate to one another and their number is congruent to 1 mod p .*

Proof. Let H be a subgroup of G that is a p -group. By First Sylow Theorem, there exists a Sylow p -subgroup P of the group G . Let G/P be the set of left cosets of P and consider the action of H on G/P by left translation. As $|G/P| \not\equiv 0 \pmod{p}$, Proposition 3.2.3 implies that there exists an element g in G such that $h(gP) = gP$ for any element h in H . It follows that $g^{-1}hg \in P$ or $H \subseteq gPg^{-1}$ proving the Second Sylow Theorem. When H is a Sylow p -subgroup, we have $|H| = |P| = |gPg^{-1}|$ and $H = gPg^{-1}$ proving the first part of the Third Sylow Theorem.

Let P act by conjugation on the set X of Sylow p -subgroups in G . The element P in X is a fixed point under this action; we claim that it is the only one. Suppose that Q in X is a fixed point. It follows that Q is a Sylow p -subgroup of G normalized by P , so P is contained in the normalizer $N_G(Q)$. Both P and Q are Sylow p -subgroups of $N_G(Q)$, so the first part of the Third Sylow Theorem shows that there exists an element n in $N_G(Q)$ such that $P = nQn^{-1} = Q$. Finally, Proposition 3.2.3 demonstrates that $|X| \equiv |X^P| = 1 \pmod{p}$. $\square$

3.3.2 Example. The symmetric group $\mathfrak{S}_3$ of order 6 has a normal Sylow 3-subgroup: $\langle (3\ 1\ 2) \rangle = \{\text{id}_3, (3\ 1\ 2), (3\ 2\ 1)\}$. It also contains three Sylow 2-subgroups of order 2:

$$\langle (2\ 1) \rangle = \{\text{id}_3, (2\ 1)\}, \quad \langle (3\ 1) \rangle = \{\text{id}_3, (3\ 1)\}, \quad \langle (3\ 2) \rangle = \{\text{id}_3, (3\ 2)\}. \quad \diamond$$

3.3.3 Example. For an odd positive integer n , the dihedral group D_n has n Sylow 2-subgroups of order 2. Each of these cyclic groups is generated by a reflection and they are all conjugate under rotations.

For an even positive integer n , the dihedral group D_n also has n Sylow 2-subgroups. Each Sylow 2-subgroup is isomorphic to $\mu_2 \times \mu_2$ because the dihedral group D_n contains no element of order 4. Each of these groups is generated by a reflection and a rotation by π . $\diamond$

The next three corollaries show that Sylow p -subgroups are compatible with group homomorphisms, subgroups, and quotients.

3.3.4 Corollary. *Let $\varphi: G \rightarrow H$ be a group homomorphism between finite groups. For any Sylow p -subgroup P in the source G , there exists a Sylow p -subgroup Q in the target H such that $\varphi(P) \subseteq Q$.*

Proof. Apply the Second Sylow Theorem to $\varphi(P)$. $\square$

3.3.5 Corollary. *Let H be a subgroup of the group G . For any Sylow p -subgroup P in H , there exists a Sylow p -subgroup Q in G such that $P = Q \cap H$. Conversely, when H is a normal subgroup and Q is a Sylow p -subgroup of G , the group $Q \cap H$ is a Sylow p -subgroup of H .*

Proof. The subgroup P is contained in a Sylow p -group Q of G and $Q \cap H$ is a maximal subgroup of H whose order is a prime power of p containing P . Hence, the intersection $Q \cap H$ is equal to P .

Let P' be a Sylow p -subgroup of H . There is an element g in G such that $gP'g^{-1} \subseteq Q$. Since H is normal, the conjugate subgroup $P = gP'g^{-1}$ is contained in H , whence in $Q \cap H$. As the order of $Q \cap H$ is a power of the prime p and P is a Sylow p -subgroup of H , we deduce that $P = Q \cap H$. $\square$

3.3.6 Corollary. *Let K be a normal subgroup of a group G . The image in the quotient G/K of a Sylow p -subgroup of G is a Sylow p -subgroup and every Sylow p -subgroup of the quotient G/K is obtained this way.*

Proof. Let $G' := G/K$ and let P' be the image in the quotient group G' of a Sylow p -subgroup P in G . The group G acts transitively on the quotient G'/P' , so the quotient G'/P' has the same cardinality as G/H for some subgroup H of G containing P . It follows that $[G' : P']$ divides $[G : P]$ and hence is not a multiple of p . We deduce that P' is a Sylow p -subgroup of G' . Let Q' be another Sylow p -subgroup of G' . The Third Sylow Theorem implies that $Q' = g'P'(g')^{-1}$ for some g' in G' . Choosing an element g in G as a representative for the left coset g' , we see that Q' is the image of $Q = gPg^{-1}$. $\square$

3.3.7 Proposition. *For any nonnegative integer r , a group of order p^r has a normal subgroup of order p^k for all $0 \leq k \leq r$.*

Proof. Let G be a group of order p^r . We proceed by induction on r . The case $r = 0$ is trivial. Corollary 3.2.4 shows that the centre of G is nontrivial. By Corollary 3.2.9, there exists a subgroup K of $Z(G)$ having order p . Since the elements in $Z(G)$ commute with every element in G , the subset K forms a normal subgroup of G . Given $1 < k \leq r$, we have $p^{k-1} \leq p^{r-1} = |G/K|$. The induction hypothesis establishes that the quotient group G/K has a normal subgroup H' of order p^{k-1} . Hence, the Correspondence Theorem shows that there is a normal subgroup H of G containing K with $H' = H/K$. As $|H/K| = p^{k-1}$, we deduce that $|H| = p^k$. $\square$

3.4 Exercises

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

- i. The exponential function induces a group isomorphism from the quotient $\mathbb{R}/\mathbb{Z}$ to the circle group $\mathbb{T}$.
- ii. The quotient group $\mathrm{GL}(n, \mathbb{R})/\mathrm{SL}(n, \mathbb{R})$ is isomorphic to $\mathbb{R}^\times$.
- iii. For any positive integer n , the orthogonal group $\mathrm{O}(n, \mathbb{R})$ act transitively on the unit sphere in $\mathbb{R}^n$.
- iv. When a group acts on itself by left translation, the orbit of every element equals the group and the stabilizer of every element is just a singleton.
- v. The cyclic group $\mathbb{Z}/\langle 12 \rangle$ has a unique Sylow 2-subgroup and a unique Sylow 3-subgroup.
- vi. The alternating group A_4 has a unique Sylow 2-subgroup and four Sylow 3-subgroups.
- vii. Let p be a prime number. The number of Sylow p -subgroups of $\mathfrak{S}_p$ is $(p-2)!$, so $(p-1)! \equiv -1 \pmod{p}$.
- viii. The permutation group $\mathfrak{S}_4$ is partitioned into five conjugacy classes of sizes 1, 3, 6, 6, and 8.

3.4.2 Problem. Let G be a group. The *commutator* of the elements f and g in G is the element $[f, g] := f^{-1}g^{-1}fg$ in G . The *commutator subgroup* $G^{(1)}$ of G is the subgroup generated by all commutators;

$$G^{(1)} := \langle f^{-1}g^{-1}fg \mid f, g \in G \rangle.$$

- i. Prove that $G^{(1)}$ is a normal subgroup and the quotient group $G/G^{(1)}$ is abelian.
- ii. Let $\pi: G \rightarrow G/G^{(1)}$ be the canonical group homomorphism. For any abelian group A , prove that every group homomorphism $\varphi: G \rightarrow A$ factors as $\varphi = \varphi^{(1)} \circ \pi$ where $\varphi^{(1)}: G/G^{(1)} \rightarrow A/A^{(1)}$ is the induced group homomorphism.
- iii. Show that a subgroup H of G contains $G^{(1)}$ if and only if H is normal and G/H is abelian.

3.4.3 Problem. Let $\langle m \rangle$ be the subgroup of integers $\mathbb{Z}$ generated by m and let $[r] := r\langle m \rangle$ denote the left coset in the quotient group $\mathbb{Z}/\langle m \rangle$ containing the integer r . Consider the set

$$(\mathbb{Z}/\langle m \rangle)^\times := \{\bar{r} \in \mathbb{Z}/\langle m \rangle \mid \gcd(r, m) = 1\}.$$

- i. Show that multiplication of integers induces a group structure on the set $(\mathbb{Z}/\langle m \rangle)^\times$.
- ii. For any positive integer n , the *totient* $\phi(n)$ is defined to be the number of positive integers less than or equal to n that are coprime to n . When $\gcd(r, m) = 1$, prove that $r^{\phi(m)} \equiv 1 \pmod{m}$.

iii. For any prime number p and any integer r , prove that

$$r^p \equiv r \pmod{p}.$$

3.4.4 Problem. The *icosahedral group* I consists of the rotational symmetries of a regular dodecahedron. It acts transitively on the vertices, edges and faces, and $|I| = 60$.

- i. Determine the number of elements in I of each order.
- ii. Determine the cardinality of each conjugacy class in I .
- iii. Show that I is a simple group (i.e. it has no nontrivial normal subgroups).