Ch1 Flashcards

Harley Caham Combest

Fa2025 2025-10-24 MATH5353

Chapter 1 — Introduction to Groups

This chapter introduces the group axioms through basic examples, then develops several cornerstone families (dihedral and symmetric groups, matrix and quaternion groups), and the fundamental morphism notions (homomorphisms/isomorphisms) culminating with group actions as a unifying lens. Key tools include uniqueness of identity/inverses, cancellation, orders of elements, generators/relations, and permutation representations.

- **Binary operations & closure.** A binary operation $*\colon G \times G \to G$ may be associative/commutative; subsets closed under $*$ inherit these properties.
- **Group axioms.** $(G, *)$ with associativity, identity e, and inverses a^{-1}; abelian if $ab = ba$. Notation simplifies products (ab, x^n, x^{-n}, $x^0 = 1$).
- **Canonical examples.** $(\mathbb{Z}, +)$; $(\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times, \cdot)$; additive groups $\mathbb{Z}/n\mathbb{Z}$; multiplicative units $(\mathbb{Z}/n\mathbb{Z})^\times$; direct products $A \times B$.
- **Basic consequences.** Identity and inverses are unique; $(ab)^{-1} = b^{-1}a^{-1}$; generalized associativity; unique solutions to $ax = b$ and $ya = b$; cancellation laws. *Order* $|x|$ is the least $n > 0$ with $x^n = 1$ (or ∞).

1.1 Basic Axioms and Examples

Intuition. Formalize “composition with undoing” and study its structural consequences across familiar number systems and constructed sets.

Core facts.

- *Uniqueness.* Identity and inverses are unique; $(x^{-1})^{-1} = x$; $(ab)^{-1} = b^{-1}a^{-1}$.
- *Cancellation/solving.* $au = av \Rightarrow u = v$, $ub = vb \Rightarrow u = v$; solutions $x = a^{-1}b$, $y = ba^{-1}$.
- *Order of an element.* Examples: in $(\mathbb{R}^\times, \cdot)$, -1 has order 2; in $\mathbb{Z}/9\mathbb{Z}$, $[6]$ has order 3; in $(\mathbb{Z}/7\mathbb{Z})^\times$, $[2]$ has order 3.

1.2 Dihedral Groups

Intuition. Symmetries of a regular n-gon (rotations and reflections) form a prototypical nonabelian group of order $2n$.

Structure.

- D_{2n} has n rotations and n reflections; $|D_{2n}| = 2n$. With generators r (rotation by $2\pi/n$) and s (a reflection), every element is r^i or sr^i, $0 \le i < n$. Relations:

  $$r^n = 1, \quad s^2 = 1, \quad rs = sr^{-1}.$$

  Hence the presentation $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$.

- Consequences: $|r| = n$, $|s| = 2$, D_{2n} is nonabelian ($rs \neq sr$). Computations reduce via $r^n = 1$, $s^2 = 1$, and $r^i s = sr^{-i}$.

1.3 Symmetric Groups

Intuition. All permutations of a set form a group under composition; on $\{1, \ldots, n\}$ this is S_n with $|S_n| = n!$. Cycle notation captures structure efficiently.

Key points.

- *Cycle decomposition.* Any $\sigma \in S_n$ factors uniquely (up to order of disjoint cycles and cyclic rotation inside each cycle) into disjoint cycles; disjoint cycles commute; σ^{-1} is obtained by reversing each cycle.
- *Orders.* $\operatorname{ord}(\sigma) = \operatorname{lcm}$ of the lengths of the cycles in its decomposition. S_n is nonabelian for $n \geq 3$.

1.4 Matrix Groups

Intuition. Invertible $n \times n$ matrices over a field F form the general linear group $GL_n(F)$ under matrix multiplication.

Highlights.

- $GL_n(F) = \{A \in M_n(F) \mid \det A \neq 0\}$ is a group; inverses exist iff $\det A \neq 0$; $\det(AB) = \det A \cdot \det B$.
- If $|F| = q < \infty$, then

  $$|GL_n(F)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

  Examples: $|GL_2(\mathbb{F}_2)| = 6$ and it is nonabelian.

1.5 The Quaternion Group

Intuition. $Q_8 = \{1, -1, \pm i, \pm j, \pm k\}$ is a minimal nonabelian group of order 8 with $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, $ki = j$, with reversed products picking up a minus sign.

Notes. Associativity holds (nontrivially), -1 is central, and each noncentral element has order 4.

1.6 Homomorphisms and Isomorphisms

Intuition. A homomorphism $\varphi : G \to H$ preserves products; an isomorphism is a bijective homomorphism—"same group up to relabeling."

Principles.

- Homomorphism preserves powers: $\varphi(x^n) = \varphi(x)^n$ ($n \in \mathbb{Z}$). Isomorphisms preserve element orders and abelian/nonabelian type.
- Presentations: mapping generators to elements satisfying the same defining relations extends uniquely to a homomorphism. E.g., $D_6 \cong S_3$ via $r \mapsto (123)$, $s \mapsto (12)$.

1.7 Group Actions

Intuition. An action $G \curvearrowright A$ is a rule $g \cdot a$ compatible with the group law; equivalently, a homomorphism $G \to S_A$. Actions turn algebra into motion (permutations), enabling counting and structure theorems.

Toolkit.

- Each g acts as a permutation of A; the associated map $G \to S_A$ is a homomorphism. Trivial vs. faithful actions; kernels and stabilizers are subgroups.
- Examples: the natural action of S_n on $\{1, \ldots, n\}$ and derived sets; D_{2n} on polygon vertices; left regular action G on itself by $x \mapsto gx$. Cayley's viewpoint follows from faithfulness of the left regular action.

Why this chapter matters. It lays the language (axioms, orders, presentations), the archetypes (D_{2n}, S_n, $GL_n(F)$, Q_8), the morphisms (homomorphisms/isomorphisms), and the lens of actions that powers later results (class equations, Sylow theory, and classifications).

1.1.1 Exercise 1 (a). Determine whether the operation $\star$ on $\mathbb{Z}$ defined by $a{\star}b = a{-}b$ is associative.

As General Proposition: Integer subtraction is not associative.

As Conditional Proposition: The binary operation $\star$ on $\mathbb{Z}$ given by $a \star b = a - b$ is not associative; i.e., there exist $x, y, z \in \mathbb{Z}$ with $(x \star y) \star z \neq x \star (y \star z)$.

. . . .

Intuition. Subtraction depends on order; rebracketing changes the order in which a minus sign applies, so outcomes can differ.

. . . .

Proof (counterexample).

Step 1 (Compute left-bracketed value). $(1\star 2)\star 3 = (1-2)-3 = -1-3 = -4$.

Step 2 (Compute right-bracketed value). $1\star(2\star 3) = 1-(2-3) = 1-(-1) = 2$.

Step 3 (Conclude nonassociativity). Since $-4 \neq 2$, the operation is not associative.

1.1.1 Exercise 1 (b). Determine whether the operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$ is associative.

As General Proposition: The real binary operation $a \star b = a + b + ab$ is associative.

As Conditional Proposition: For all $a, b, c \in \mathbb{R}$, $(a \star b) \star c = a \star (b \star c)$

. . . .

Intuition. Note $a \star b = (1+a)(1+b) - 1$, so $\star$ inherits associativity from real multiplication. We can also verify by direct expansion.

. . . .

Proof (direct computation).

Step 1 (Expand left side). $(a{\star}b){\star}c = (a{+}b{+}ab){\star}c = (a{+}b{+}ab){+}c{+}(a{+}b{+}ab)c$.
Step 2 (Distribute and collect). $= a + b + c + ab + ac + bc + abc$.
Step 3 (Expand right side). $a{\star}(b{\star}c) = a{\star}(b{+}c{+}bc) = a{+}(b{+}c{+}bc){+}a(b{+}c{+}bc)$.
Step 4 (Distribute and collect). $= a + b + c + bc + ab + ac + abc$.
Step 5 (Compare). Both sides equal $a + b + c + ab + ac + bc + abc$; hence $(a \star b) \star c = a \star (b \star c)$.
Step 6 (Conclude). $\star$ is associative on $\mathbb{R}$.

1.1.1 Exercise 1 (c). Determine whether the operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$ is associative.

As General Proposition: The averaging-type operation $a \star b = (a+b)/5$ is not associative.

As Conditional Proposition: There exist $x, y, z \in \mathbb{Q}$ with $(x \star y) \star z \neq x \star (y \star z)$.

. . . .

Intuition. Linear averaging with a fixed scale factor generally fails associativity unless the factor is 1; rebracketing inserts the factor twice in different positions.

. . . .

Proof (counterexample).

Step 1 (Compute left-bracketed value). $(5 \star 20) \star 15 = \left(\frac{5+20}{5}\right) \star 15 = 5 \star 15 = \frac{5+15}{5} = \frac{20}{5} = 4.$

Step 2 (Compute right-bracketed value). $5 \star (20 \star 15) = 5 \star \left(\frac{20+15}{5}\right) = 5 \star 7 = \frac{5+7}{5} = \frac{12}{5}.$

Step 3 (Conclude nonassociativity). Since $4 \neq \frac{12}{5}$, the operation is not associative.

1.1.2 Exercise 2 (a). Decide whether $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$ is commutative.

As General Proposition: Integer subtraction is not commutative.

As Conditional Proposition: The binary operation $\star$ on $\mathbb{Z}$ given by $a \star b = a - b$ is not commutative; i.e., there exist $x, y \in \mathbb{Z}$ with $x \star y \neq y \star x$.

Intuition. Swapping the operands reverses which term is being subtracted, typically changing the sign of the result.

Proof (counterexample).
Step 1 (Compute $1 \star 2$). $1 \star 2 = 1 - 2 = -1$.
Step 2 (Compute $2 \star 1$). $2 \star 1 = 2 - 1 = 1$.
Step 3 (Conclude noncommutativity). Since $-1 \neq 1$, we have $1 \star 2 \neq 2 \star 1$; thus $\star$ is not commutative on $\mathbb{Z}$.

1.1.2 Exercise 2 (b). Decide whether $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$ is commutative.

As General Proposition: The operation $a \star b = a + b + ab$ on $\mathbb{R}$ is commutative.

As Conditional Proposition: For all $a, b \in \mathbb{R}$, $a \star b = b \star a$.

. . . .

Intuition. The expression is symmetric in a and b because real addition and multiplication each commute; also $a \star b = (1+a)(1+b) - 1$, which is visibly symmetric.

. . . .

Proof (direct calculation).

Step 1 (Write both orders). $a \star b = a + b + ab$ and $b \star a = b + a + ba$.

Step 2 (Use commutativity of + and $\cdot$). $b + a = a + b$ and $ba = ab$.

Step 3 (Identify equality). Hence $b \star a = b + a + ba = a + b + ab = a \star b$.

Step 4 (Conclude). Therefore $\star$ is commutative on $\mathbb{R}$.

1.1.2 Exercise 2 (c). Decide whether $\star$ on $\mathbb{Q}$ defined by $a \star b = \dfrac{a+b}{5}$ is commutative.

As General Proposition: The averaging-type operation $a \star b = (a+b)/5$ on $\mathbb{Q}$ is commutative.

As Conditional Proposition: For all $a, b \in \mathbb{Q}$, $a \star b = b \star a$.

. . . .

Intuition. Swapping a and b leaves $a+b$ unchanged; dividing by a fixed constant preserves equality.

. . . .

Proof (direct calculation).

Step 1 (Write both orders). $a \star b = \dfrac{a+b}{5}$ and $b \star a = \dfrac{b+a}{5}$.

Step 2 (Use commutativity of addition). $a+b = b+a$.

Step 3 (Identify equality). Thus $\dfrac{a+b}{5} = \dfrac{b+a}{5}$, so $a \star b = b \star a$.

Step 4 (Conclude). Therefore $\star$ is commutative on $\mathbb{Q}$.

1.1.7 Exercise 7. Let $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ and for $x, y \in G$ let $x \star y$ be the fractional part of $x + y$:

$$x \star y \;=\; \{x + y\} \;=\; x + y - \lfloor x + y \rfloor,$$

where $\lfloor \cdot \rfloor$ is the greatest integer $\leq$ the argument. Prove that $\star$ is a well-defined binary operation on G and that $(G, \star)$ is an abelian group (the "real numbers mod 1").

As General Proposition: The set $G = [0, 1)$ forms an abelian group under $x \star y = \{x + y\}$.

As Conditional Proposition: With $G = [0, 1)$ and $x \star y = x + y - \lfloor x + y \rfloor$, the operation $\star$ is a well-defined binary operation on G, associative and commutative, with identity 0 and inverse $x^{-1} = 0$ if $x = 0$ and $x^{-1} = 1 - x$ if $0 < x < 1$.

. . . .

Intuition. The rule $x \star y = \{x+y\}$ is simply "add and wrap back into $[0,1)$." Because adding or subtracting an integer does not change fractional parts, rebracketing sums only changes them by integers; hence associativity and commutativity descend from ordinary addition. The identity is 0, and the inverse of x is the amount needed to reach the next integer, namely $1-x$ (or 0 if $x=0$).

. . . .

Proof.

Step 1 (Well-definedness/closure). For $x, y \in [0,1)$ we have $0 \le x+y < 2$, so $n := \lfloor x+y \rfloor \in \{0,1\}$. Then

$$x \star y = x + y - n \in [0,1),$$

hence $\star$ maps $G \times G$ into G.

Step 2 (Commutativity). Since $x+y = y+x$ and $\lfloor x+y \rfloor = \lfloor y+x \rfloor$,

$$x \star y = x + y - \lfloor x+y \rfloor = y + x - \lfloor y+x \rfloor = y \star x.$$

Step 3 (Identity element). For any $x \in G$, $\lfloor x \rfloor = 0$, hence

$$x \star 0 = x + 0 - \lfloor x \rfloor = x, \qquad 0 \star x = 0 + x - \lfloor x \rfloor = x.$$

Thus 0 is a two-sided identity.

Step 4 (Inverses). If $x = 0$, then 0 is its own inverse. If $0 < x < 1$, set $y = 1 - x \in (0,1)$. Then

$$x \star y = x + (1-x) - \lfloor 1 \rfloor = 1 - 1 = 0, \quad y \star x = (1-x) + x - \lfloor 1 \rfloor = 0,$$

so y is a two-sided inverse of x.

Step 5 (Associativity via fractional-part algebra). For any real t and integer k, $\{t-k\} = \{t\}$ because

$$\{t-k\} = (t-k) - \lfloor t-k \rfloor = (t-k) - (\lfloor t \rfloor - k) = t - \lfloor t \rfloor = \{t\}.$$

Let $x, y, z \in G$ and put $u = x + y$. Then

$$(x \star y) \star z = \{\{x+y\}+z\} = \{(x+y-\lfloor x+y \rfloor)+z\} = \{u+z-\lfloor u \rfloor\} = \{u+z\} = \{x+y+z\}.$$

Similarly,

$$x \star (y \star z) = \{x+\{y+z\}\} = \{x+(y+z-\lfloor y+z \rfloor)\} = \{x+y+z-\lfloor y+z \rfloor\} = \{x+y+z\}.$$

Therefore $(x \star y) \star z = x \star (y \star z)$ for all $x, y, z \in G$.

Step 6 (Conclusion). The operation $\star$ is closed on G, associative and commutative; 0 is the identity; and every $x \in G$ has an inverse in G (namely 0 if $x = 0$, else $1 - x$). Hence $(G, \star)$ is an abelian group.

1.1.18 Exercise 18. Let x, y be elements of a group G. Prove that

$$xy = yx \quad \Longleftrightarrow \quad y^{-1}xy = x \quad \Longleftrightarrow \quad x^{-1}y^{-1}xy = 1.$$

As General Proposition: An element x commutes with y iff x is fixed by conjugation by y iff the commutator $x^{-1}y^{-1}xy$ equals the identity.

As Conditional Proposition: For any $x, y \in G$, the following are equivalent:

(1) $xy = yx$.

(2) $y^{-1}xy = x$.

(3) $x^{-1}y^{-1}xy = 1$.

. . . .

Intuition. Conjugation measures “failure to commute”: if x and y commute, then conjugating x by y leaves it unchanged. The commutator $[x, y] = x^{-1}y^{-1}xy$ is exactly the element that becomes 1 precisely when x and y commute.

. . . .

Proof.

Step 1 (Show (1) $\Rightarrow$ (2)**).** Assume $xy = yx$. Left-multiply by y^{-1} to get $y^{-1}xy = y^{-1}yx = x$.

Step 2 (Show (2) $\Rightarrow$ (1)**).** Assume $y^{-1}xy = x$. Left-multiply by y to obtain $xy = yx$.

Step 3 (Conclude (1) $\Leftrightarrow$ (2)**).** Steps 1–2 give equivalence of (1) and (2).

Step 4 (Show (2) $\Rightarrow$ (3)**).** From $y^{-1}xy = x$, left-multiply by x^{-1} to get $x^{-1}y^{-1}xy = x^{-1}x = 1$, establishing (3).

Step 5 (Show (3) $\Rightarrow$ (2)**).** If $x^{-1}y^{-1}xy = 1$, then right-multiply by y^{-1} to get $x^{-1}y^{-1}x = y^{-1}$. Now left-multiply by x to deduce $y^{-1}x = xy^{-1}$. Right-multiply by y to obtain $x = y^{-1}xy$, which is (2).

Step 6 (Transitive equivalence). By Steps 3–5, (1), (2), and (3) are all equivalent.

1.1.34 Exercise 34. If x is an element of infinite order in a group G, prove that the elements x^n $(n \in \mathbb{Z})$ are all distinct.

As General Proposition: If $\langle x \rangle$ is infinite, then the map $\mathbb{Z} \to G$, $n \mapsto x^n$, is injective, so the powers $\{x^n : n \in \mathbb{Z}\}$ are pairwise distinct.

As Conditional Proposition: Let G be a group and $x \in G$ have infinite order. Then for all $m, n \in \mathbb{Z}$, $x^m = x^n$ implies $m = n$; equivalently, all x^n are distinct.

. . . .

Intuition. "Infinite order" means no nonzero power of x equals the identity. If two powers matched, say $x^m = x^n$, then moving one to the other side would yield a nontrivial power $x^{m-n} = 1$, contradicting infinitude.

. . . .

Proof.

Step 1 (Assume two equal powers). Take any $m, n \in \mathbb{Z}$ and suppose $x^m = x^n$.

Step 2 (Reduce to a single power). Multiply on the right by x^{-n} to get $x^{m-n} = 1$.

Step 3 (Use infinite order). Since x has infinite order, the only integer k with $x^k = 1$ is $k = 0$. Thus $m - n = 0$.

Step 4 (Conclude injectivity). From $m - n = 0$ we obtain $m = n$. Hence distinct integers yield distinct powers: if $m \neq n$ then $x^m \neq x^n$.

Step 5 (Finish). Therefore the set $\{x^n : n \in \mathbb{Z}\}$ consists of pairwise distinct elements.

1.2.4 Exercise 4. If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}.

As General Proposition: In the dihedral group $D_{2n} = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$ with $n = 2k \geq 4$, the center is $Z(D_{2n}) = \{1, r^k\}$; in particular r^k has order 2 and is central.

As Conditional Proposition: Let $G = D_{2n}$ with $n = 2k \geq 4$. Then $z := r^k$ satisfies $z^2 = 1$ and $zg = gz$ for all $g \in G$, and if $w \in G \setminus \{1\}$ commutes with every element of G then $w = r^k$.

. . . .

Intuition. Half a full rotation flips the polygon to the opposite configuration; doing it twice restores the original—hence order 2. Conjugating by a reflection inverts rotations; but $r^k = r^{-k}$ when $n = 2k$, so r^k is fixed by conjugation and thus commutes with reflections as well as rotations. Any other rotation fails to commute with a reflection, and no reflection commutes with a rotation when $n \geq 4$.

. . . .

Proof.

Step 1 (Order of r^k). Since $n = 2k$, we have $(r^k)^2 = r^{2k} = r^n = 1$ and $r^k \neq 1$ (because $k < n$). Thus r^k has order 2.

Step 2 (Commutation with rotations). For any i, $r^k r^i = r^{k+i} = r^{i+k} = r^i r^k$, so r^k commutes with every rotation.

Step 3 (Commutation with reflections). Using $sr = r^{-1}s$,

$$sr^k = r^{-k}s.$$

Because $n = 2k$, we have $r^{-k} = r^{n-k} = r^k$, hence $sr^k = r^k s$. Therefore r^k commutes with every reflection sr^i:

$$r^k(sr^i) = (r^k s)r^i = (sr^k)r^i = sr^{k+i} = sr^{i+k} = (sr^i)r^k.$$

Thus r^k commutes with all elements of D_{2n}.

Step 4 (No other rotation is central). Let r^t commute with s. Then

$$r^t s = sr^t = r^{-t}s \quad \Rightarrow \quad r^t = r^{-t} \quad \Rightarrow \quad r^{2t} = 1.$$

Since $|r| = n = 2k$, we must have $2t \equiv 0 \pmod{2k}$, so $t \equiv 0$ or $t \equiv k$. Hence among rotations, only 1 and r^k commute with s.

Step 5 (No reflection is central). Suppose $w = sr^t$ commutes with r. Then

$$(sr^t)r = sr^{t+1}, \qquad r(sr^t) = (rs)r^t = (sr^{-1})r^t = sr^{t-1}.$$

Commuting would force $sr^{t+1} = sr^{t-1}$, hence $r^{t+1} = r^{t-1}$ and $r^2 = 1$, contradicting $n \geq 4$. Thus no reflection commutes with r, so no reflection is central.

Step 6 (Conclusion). By Steps 4–5, the only elements commuting with both generators r and s are 1 and r^k. Therefore $Z(D_{2n}) = \{1, r^k\}$; in particular, $z = r^k$ is the unique nonidentity element commuting with all of D_{2n}.

1.3.2 Exercise 2. Let $\sigma, \tau \in S_{15}$ be given by the two-line descriptions shown. Find the cycle decompositions of $\sigma,\ \tau,\ \sigma^2,\ \sigma\tau,\ \tau\sigma,\ \tau^2\sigma$.

As General Proposition: A permutation's cycle form is obtained by iterating images until returning to the start, omitting fixed points. Products are composed *right-to-left*: $(\alpha\beta)(i) = \alpha(\beta(i))$.

As Conditional Proposition: With the displayed σ, τ, the required cycle decompositions are

$$\begin{aligned}
\sigma &= (1\,13\,5\,10)(3\,15\,8)(4\,14\,11\,7\,12\,9), \\
\tau &= (1\,14)(2\,9\,15\,13\,4)(3\,10)(5\,12\,7)(8\,11), \\
\sigma^2 &= (1\,5)(3\,8\,15)(4\,11\,12)(7\,9\,14)(10\,13), \\
\sigma\tau &= (1\,11\,3)(2\,4)(5\,9\,8\,7\,10\,15)(13\,14), \\
\tau\sigma &= (1\,4)(2\,9)(3\,13\,12\,15\,11\,5)(8\,10\,14), \\
\tau^2\sigma &= (1\,2\,15\,8\,3\,4\,14\,11\,12\,13\,7\,5\,10).
\end{aligned}$$

Intuition. To pass from two-line notation to cycles, start at the smallest unused symbol, repeatedly apply the permutation, and stop when you return; repeat on the next unused symbol. For products, apply the rightmost map first at each step—this is the only place errors usually creep in.

Proof (by explicit tracing).

Step 1 (Cycle form of σ). Track $1 \mapsto 13 \mapsto 5 \mapsto 10 \mapsto 1$ giving $(1\,13\,5\,10)$. Next $3 \mapsto 15 \mapsto 8 \mapsto 3$ gives $(3\,15\,8)$. Starting at 4: $4 \mapsto 14 \mapsto 11 \mapsto 7 \mapsto 12 \mapsto 9 \mapsto 4$ gives $(4\,14\,11\,7\,12\,9)$. All remaining points (e.g. $2, 6$) are fixed and omitted.

Step 2 (Cycle form of τ). Trace $1 \mapsto 14 \mapsto 1$ giving $(1\,14)$. Next $2 \mapsto 9 \mapsto 15 \mapsto 13 \mapsto 4 \mapsto 2$ gives $(2\,9\,15\,13\,4)$. Then $(3\,10)$, $(5\,12\,7)$, and $(8\,11)$ follow similarly.

Step 3 (σ^2). Square each cycle of σ independently: for a k-cycle $(a_1\,\ldots\,a_k)$, σ^2 advances two steps. This yields $(1\,5)$ from $(1\,13\,5\,10)$; $(3\,8\,15)$ from $(3\,15\,8)$; $(4\,11\,12)$ and $(7\,9\,14)$ from the 6-cycle; and $(10\,13)$.

Step 4 ($\sigma\tau$ with right-to-left convention). For each i, compute $i \xmapsto{\tau} \tau(i)$ then apply σ. Tracing orbits gives $(1\,11\,3)$, $(2\,4)$, $(5\,9\,8\,7\,10\,15)$, $(13\,14)$.

Step 5 ($\tau\sigma$). Now apply σ first, then τ. Tracing produces $(1\,4)$, $(2\,9)$, $(3\,13\,12\,15\,11\,5)$, $(8\,10\,14)$.

Step 6 ($\tau^2\sigma$). First compute τ^2 by squaring each cycle of τ, then compose with σ (right-to-left). Tracing one long orbit yields

$$\tau^2\sigma = (1\,2\,15\,8\,3\,4\,14\,11\,12\,13\,7\,5\,10).$$

Step 7 (Conclude). All cycle decompositions match the orbits obtained by repeated application under the stated composition convention, completing the computation.

1.3.3 Exercise 3. For each of the permutations whose cycle decompositions were computed in the preceding two exercises, compute its order.

As General Proposition: The order of a permutation equals the least common multiple of the lengths of the cycles in its disjoint cycle decomposition.

As Conditional Proposition: For the permutations from Exercise 1.3.2,

$$|\sigma| = 12, \qquad |\tau| = 30, \qquad |\sigma^2| = 6, \qquad |\sigma\tau| = 6, \qquad |\tau\sigma| = 6, \qquad |\tau^2\sigma| = 13.$$

Intuition. Disjoint cycles act independently; a point returns to itself when each cycle containing it has completed an integer number of turns. Thus the whole permutation repeats exactly after the least common multiple of all cycle lengths.

Proof (cycle lengths ⇒ lcm).
Step 1 (Recall cycle forms). From Exercise 1.3.2:

$$\begin{aligned}
\sigma &= (1\,13\,5\,10)(3\,15\,8)(4\,14\,11\,7\,12\,9),\\
\tau &= (1\,14)(2\,9\,15\,13\,4)(3\,10)(5\,12\,7)(8\,11),\\
\sigma^2 &= (1\,5)(3\,8\,15)(4\,11\,12)(7\,9\,14)(10\,13),\\
\sigma\tau &= (1\,11\,3)(2\,4)(5\,9\,8\,7\,10\,15)(13\,14),\\
\tau\sigma &= (1\,4)(2\,9)(3\,13\,12\,15\,11\,5)(8\,10\,14),\\
\tau^2\sigma &= (1\,2\,15\,8\,3\,4\,14\,11\,12\,13\,7\,5\,10).
\end{aligned}$$

Step 2 (Compute $|\sigma|$). Cycle lengths: $4, 3, 6$; hence $|\sigma| = \mathrm{lcm}(4, 3, 6) = 12$.
Step 3 (Compute $|\tau|$). Cycle lengths: $2, 5, 2, 3, 2$; hence $|\tau| = \mathrm{lcm}(2, 5, 3) = 30$.
Step 4 (Compute $|\sigma^2|$). Cycle lengths: $2, 3, 3, 3, 2$; hence $|\sigma^2| = \mathrm{lcm}(2, 3) = 6$.
Step 5 (Compute $|\sigma\tau|$). Cycle lengths: $3, 2, 6, 2$; hence $|\sigma\tau| = \mathrm{lcm}(3, 2, 6, 2) = 6$.
Step 6 (Compute $|\tau\sigma|$). Cycle lengths: $2, 2, 6, 3$; hence $|\tau\sigma| = \mathrm{lcm}(2, 2, 6, 3) = 6$.
Step 7 (Compute $|\tau^2\sigma|$). Single cycle of length 13; hence $|\tau^2\sigma| = 13$.
Step 8 (Conclusion). By the lcm principle for disjoint cycles, the stated orders follow.

1.?. Additional Exercise 1. (1) Show that if a and b are commuting elements of a group G (i.e. $ab = ba$), then $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. Then, find a group G with noncommuting elements a, b where $(ab)^n \neq a^n b^n$ for some positive integer n.

As General Proposition: If $a, b \in G$ commute, then for every integer n, $(ab)^n = a^n b^n$. Moreover, if a, b do not commute, the identity $(ab)^n = a^n b^n$ can fail.

As Conditional Proposition: Let G be any group. If $ab = ba$, then $(ab)^n = a^n b^n$ holds for all $n \in \mathbb{Z}$. As a counterexample in a nonabelian group, in S_3 with $a = (12)$ and $b = (23)$ we have $(ab)^2 \neq a^2 b^2$.

. . . .

Intuition. When a and b commute, you may "bubble" a's past b's without changing the product; induction shows $(ab)^n$ reorders to $a^n b^n$. For negative powers, invert and reuse the positive case. In a nonabelian group those swaps are illegal; a classic choice is S_3 where transpositions don't commute, and the formula fails immediately.

. . . .

Proof.

Step 1 (Base case $n = 0$). $(ab)^0 = 1 = a^0 b^0$.

Step 2 (Induction step for $n \geq 0$). Assume $(ab)^n = a^n b^n$ for some $n \geq 0$. Then, using $ab = ba$,

$$(ab)^{n+1} = (ab)^n (ab) = a^n b^n ab = a^n a\, b^n b = a^{n+1} b^{n+1}.$$

Thus, by induction, $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}_{\geq 0}$.

Step 3 (Commutation persists under inverses). From $ab = ba$ we get $a^{-1}b = ba^{-1}$ (multiply $ab = ba$ on the left by a^{-1} and on the right by b^{-1}), hence a^{-1} and b^{-1} also commute.

Step 4 (Negative exponents). For $m > 0$,

$$(ab)^{-m} = \big((ab)^{-1}\big)^m = (b^{-1}a^{-1})^m = b^{-m}a^{-m} = a^{-m}b^{-m},$$

where the third equality is Step 2 applied to the commuting pair (b^{-1}, a^{-1}), and the fourth uses commutativity of a^{-m} and b^{-m}. Hence $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.

Step 5 (Counterexample when $ab \neq ba$). Take $G = S_3$, $a = (12)$, $b = (23)$. Then $a^2 = b^2 = 1$, so $a^2 b^2 = 1$. But $ab = (12)(23) = (123)$ has order 3, hence

$$(ab)^2 = (123)^2 = (132) \neq 1 = a^2 b^2.$$

Therefore $(ab)^2 \neq a^2 b^2$ in this noncommuting case.

Step 6 (Conclusion). The identity $(ab)^n = a^n b^n$ holds for all integers n precisely under the commuting hypothesis; absent commutativity it can fail, as exhibited in S_3.

1.?. Additional Exercise 2. (2) Prove that disjoint cycles commute. I.e., if $\sigma \in S_k$ has cycle representation $(a_1\, a_2\, \ldots\, a_\ell)$ and $\tau \in S_k$ has cycle representation $(b_1\, b_2\, \ldots\, b_m)$ and the sets $\{a_i\}_{i=1}^{\ell}$ and $\{b_j\}_{j=1}^{m}$ are disjoint, then $\sigma \circ \tau = \tau \circ \sigma$.

As General Proposition: Permutations with disjoint supports commute: if $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \varnothing$, then $\sigma\tau = \tau\sigma$.

As Conditional Proposition: Let $\sigma = (a_1\, a_2\, \ldots\, a_\ell)$ and $\tau = (b_1\, b_2\, \ldots\, b_m)$ be cycles on $\{1, \ldots, k\}$ with $\{a_1, \ldots, a_\ell\} \cap \{b_1, \ldots, b_m\} = \varnothing$. Then for every x in $\{1, \ldots, k\}$ we have $(\sigma\tau)(x) = (\tau\sigma)(x)$; hence $\sigma\tau = \tau\sigma$.

. . . .

Intuition. Each cycle "moves" only the elements in its own support and fixes all others. If the two supports are disjoint, then while one cycle acts, the other does nothing on those elements (it fixes them). Thus the actions are independent and can be performed in either order with the same result.

. . . .

Proof (pointwise equality on three cases).

Step 1 (Notation and convention). Composition is right-to-left: $(\alpha\beta)(x) = \alpha(\beta(x))$. The supports are disjoint: $\{a_1, \dots, a_\ell\} \cap \{b_1, \dots, b_m\} = \varnothing$.

Step 2 (Case $x \in \{a_1, \dots, a_\ell\}$). Then $\tau(x) = x$ because τ fixes every a_i. Hence

$$(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x).$$

Also $\sigma(x) \in \{a_1, \dots, a_\ell\}$, so $\tau(\sigma(x)) = \sigma(x)$; thus

$$(\tau\sigma)(x) = \tau(\sigma(x)) = \sigma(x) = (\sigma\tau)(x).$$

Step 3 (Case $x \in \{b_1, \dots, b_m\}$). Symmetrically, $\sigma(x) = x$, so

$$(\sigma\tau)(x) = \sigma(\tau(x)) = \tau(x) = (\tau\sigma)(x),$$

since σ fixes $\tau(x) \in \{b_1, \dots, b_m\}$.

Step 4 (Case x outside both supports). If $x \notin \{a_i\} \cup \{b_j\}$, then $\sigma(x) = x = \tau(x)$; hence

$$(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x) = x = (\tau\sigma)(x).$$

Step 5 (Conclude equality of permutations). In all cases, $(\sigma\tau)(x) = (\tau\sigma)(x)$ for every x; therefore $\sigma\tau = \tau\sigma$.

1.?. Additional Exercise 3. (3) Prove that the order of a permutation $\sigma \in S_n$ is the least common multiple of the lengths of the cycles in its cycle decomposition.

As General Proposition: If σ decomposes as a product of disjoint cycles

$$\sigma = C_1 C_2 \cdots C_r, \qquad C_i \text{ a } k_i\text{-cycle},$$

then $|\sigma| = \operatorname{lcm}(k_1, \ldots, k_r)$.

As Conditional Proposition: Let $\sigma \in S_n$ have disjoint-cycle form $C_1 \cdots C_r$ with lengths $k_1, \ldots, k_r$. Then $\sigma^m = 1$ iff $k_i \mid m$ for all i, hence $|\sigma| = \min\{m \geq 1 : \ \sigma^m = 1\} = \operatorname{lcm}(k_1, \ldots, k_r)$.

. . . .

Intuition. Disjoint cycles act independently on disjoint supports. A k-cycle returns every element in its support to its starting point exactly after k applications. For the whole permutation to reset, *every* cycle must have completed an integer number of revolutions—precisely when the exponent is a common multiple of all cycle lengths. The first time this can happen is the least common multiple.

. . . .

Proof.

Step 1 (Disjointness $\Rightarrow$ commutation). Since the cycles $C_1, \ldots, C_r$ have disjoint supports, they commute and fix each other's supports. Thus, for every $m \geq 1$,

$$\sigma^m = (C_1 \cdots C_r)^m = C_1^m \cdots C_r^m.$$

Step 2 (When a single cycle resets). If C is a k-cycle, then $C^m = 1$ iff $k \mid m$. Indeed, C advances each element by one position per application, returning to the start after exactly k steps.

Step 3 (Characterize $\sigma^m = 1$). Using Step 1 and Step 2,

$$\sigma^m = 1 \quad \Longleftrightarrow \quad C_i^m = 1 \text{ for all } i \quad \Longleftrightarrow \quad k_i \mid m \text{ for all } i.$$

Step 4 (Minimal such exponent). The set of positive integers m with $k_i \mid m$ for all i is exactly the set of positive multiples of $\operatorname{lcm}(k_1, \ldots, k_r)$. Hence the least m with $\sigma^m = 1$ is $m = \operatorname{lcm}(k_1, \ldots, k_r)$.

Step 5 (Conclusion). By definition of order, $|\sigma| = \min\{m \geq 1 : \sigma^m = 1\} = \operatorname{lcm}(k_1, \ldots, k_r)$.

1.?. Additional Exercise 4. (4) Show that for all $\sigma \in S_n$,

$$\sigma\,(1\ 2\ \cdots\ k)\,\sigma^{-1} \;=\; \big(\sigma(1)\ \sigma(2)\ \cdots\ \sigma(k)\big).$$

What more general statement should be true? (No need to prove the more general statement.)

As General Proposition: Conjugation in S_n relabels a cycle by applying the outer permutation to each entry:

$$\sigma\,(a_1\,a_2\,\ldots\,a_k)\,\sigma^{-1} \;=\; \big(\sigma(a_1)\,\sigma(a_2)\,\ldots\,\sigma(a_k)\big).$$

As Conditional Proposition: For $c = (1\,2\,\ldots\,k)$ and any $\sigma \in S_n$,

$$\sigma c \sigma^{-1} = \big(\sigma(1)\ \sigma(2)\ \cdots\ \sigma(k)\big).$$

. . . .

Intuition. Conjugation by σ is "relabeling by σ": first move a label back by σ^{-1}, apply c, then move forward by σ. Thus each j in the cycle is sent to the image of its successor, and points outside the cycle remain fixed—exactly the behavior of the cycle with all entries relabeled by σ.

. . . .

Proof (pointwise verification).

Step 1 (Convention). Composition is right-to-left: $(\alpha\beta)(x) = \alpha(\beta(x))$. Let $c = (1\,2\,\ldots\,k)$.

Step 2 (Action on the moved points). For $1 \le j < k$,

$$(\sigma c \sigma^{-1})\big(\sigma(j)\big) = \sigma(c(j)) = \sigma(j+1).$$

For $j = k$,

$$(\sigma c \sigma^{-1})\big(\sigma(k)\big) = \sigma(c(k)) = \sigma(1).$$

Hence $\sigma c \sigma^{-1}$ cyclically permutes the set $\{\sigma(1), \ldots, \sigma(k)\}$ by

$$\sigma(1) \mapsto \sigma(2) \mapsto \cdots \mapsto \sigma(k) \mapsto \sigma(1).$$

Step 3 (Action on the fixed points). If $x \notin \{\sigma(1), \ldots, \sigma(k)\}$, then $\sigma^{-1}(x) \notin \{1, \ldots, k\}$, so c fixes $\sigma^{-1}(x)$. Therefore

$$(\sigma c \sigma^{-1})(x) = \sigma\big(\sigma^{-1}(x)\big) = x.$$

Thus $\sigma c \sigma^{-1}$ fixes every point outside $\{\sigma(1), \ldots, \sigma(k)\}$.

Step 4 (Identify the cycle). Steps 2–3 show that $\sigma c \sigma^{-1}$ is exactly the cycle

$$\big(\sigma(1)\ \sigma(2)\ \cdots\ \sigma(k)\big).$$

This proves the claim.

More general statement (no proof required). For any $\tau \in S_n$ with disjoint-cycle decomposition

$$\tau = (a_{11}\, a_{12}\, \ldots)\,(a_{21}\, a_{22}\, \ldots)\cdots,$$

and any $\sigma \in S_n$,

$$\sigma\,\tau\,\sigma^{-1} = \big(\sigma(a_{11})\,\sigma(a_{12})\,\ldots\big)\,\big(\sigma(a_{21})\,\sigma(a_{22})\,\ldots\big)\cdots;$$

in particular, conjugation preserves cycle type (length multiset) and hence preserves order.

1.6.1 Exercise 1 (a). Let $\varphi : G \to H$ be a homomorphism. Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$.

As General Proposition: Homomorphisms preserve positive powers: for every group homomorphism φ and $n \geq 1$, $\varphi(x^n) = \varphi(x)^n$.

As Conditional Proposition: If $\varphi : G \to H$ satisfies $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$, then for each $x \in G$ and $n \in \mathbb{Z}^+$, $\varphi(x^n) = \big(\varphi(x)\big)^n$.

. . . .

Intuition. Expand x^n as $x \cdots x$ (n factors). A homomorphism turns a product into the product of the images, so we obtain n copies of $\varphi(x)$—that is, $\varphi(x)^n$.

. . . .

Proof (induction on n).

Step 1 (Base case $n = 1$). $\varphi(x^1) = \varphi(x) = \varphi(x)^1$.

Step 2 (Inductive hypothesis). Assume $\varphi(x^n) = \varphi(x)^n$ for some fixed $n \geq 1$.

Step 3 (Inductive step). Using the homomorphism property,

$$\varphi(x^{n+1}) = \varphi(x^n x) = \varphi(x^n)\varphi(x) = \varphi(x)^n \, \varphi(x) = \varphi(x)^{n+1}.$$

Step 4 (Conclusion). By induction, $\varphi(x^n) = \varphi(x)^n$ holds for all $n \in \mathbb{Z}^+$.

1.6.1 Exercise 1 (b). Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

As General Proposition: Homomorphisms preserve identity and inverses; hence they preserve all integer powers.

As Conditional Proposition: For any homomorphism $\varphi : G \to H$ and all $x \in G$, we have $\varphi(1_G) = 1_H$, $\varphi(x^{-1}) = \varphi(x)^{-1}$, and consequently $\varphi(x^n) = \varphi(x)^n$ for every $n \in \mathbb{Z}$.

. . . .

Intuition. Apply φ to $xx^{-1} = 1_G$ to see that $\varphi(x^{-1})$ must be the inverse of $\varphi(x)$. Then write a negative power as a positive power of x^{-1}. Include $n = 0$ via identities.

. . . .

Proof.

Step 1 (Identity preserved). Since $1_G \cdot 1_G = 1_G$,

$$\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G),$$

so by cancellation in H, $\varphi(1_G) = 1_H$.

Step 2 (Inverse preserved). From $xx^{-1} = 1_G$,

$$\varphi(x)\,\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1_G) = 1_H,$$

hence $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Step 3 (Case $n = 0$). $\varphi(x^0) = \varphi(1_G) = 1_H = (\varphi(x))^0$.

Step 4 (Case $n < 0$). Let $n = -m$ with $m \in \mathbb{Z}^+$. Then

$$\varphi(x^n) = \varphi(x^{-m}) = \varphi\big((x^{-1})^m\big) = \big(\varphi(x^{-1})\big)^m = \big(\varphi(x)^{-1}\big)^m = \varphi(x)^{-m} = \varphi(x)^n,$$

where the third equality uses part (a) applied to x^{-1}.

Step 5 (Conclusion). Combining Steps 3–4 with part (a) (the $n > 0$ case) yields $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

1.6.2 Exercise 2. If $\varphi : G \to H$ is an isomorphism, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?

As General Proposition: Isomorphisms preserve element orders (finite or infinite). Consequently, isomorphic groups have the same number of elements of each order. This fails for arbitrary homomorphisms.

As Conditional Proposition: Let $\varphi : G \to H$ be an isomorphism. Then for every $x \in G$,

$$|\varphi(x)| = |x|.$$

Hence, for each $n \in \mathbb{Z}^+$, φ induces a bijection between the sets $\{x \in G : \ |x| = n\}$ and $\{y \in H : \ |y| = n\}$, so the two sets have the same cardinality. If φ is merely a homomorphism, the conclusion may fail (e.g., the trivial homomorphism).

. . . .

Intuition. Isomorphisms preserve the group law and are bijective. Because powers are built by repeated multiplication, $\varphi(x^m) = \varphi(x)^m$ holds; thus the first (positive) time x^m hits 1 is exactly the first time $\varphi(x)^m$ hits 1. If no nonzero power of x is 1, the same is true of $\varphi(x)$ by bijectivity. Therefore orders match, and bijectivity transports "elements of order n" bijectively. A homomorphism without injectivity can collapse orders (e.g., map everything to 1).

. . . .

Proof.

Step 1 (Powers respected). Since φ is a homomorphism, for all $m \in \mathbb{Z}$ we have $\varphi(x^m) = \varphi(x)^m$.

Step 2 (Finite-order case: $|x| = n < \infty$). Then $x^n = 1$ and n is minimal with this property. Applying φ gives $\varphi(x)^n = \varphi(1) = 1$. Thus $|\varphi(x)|$ divides n.

Step 3 (Minimality transfers). Conversely, if $|\varphi(x)| = k$, then $\varphi(x)^k = 1$ implies $\varphi(x^k) = 1$. Because φ is injective, $x^k = 1$, so n divides k. Hence $k = n$ and $|\varphi(x)| = |x|$ when $|x| < \infty$.

Step 4 (Infinite-order case). Suppose $|x| = \infty$. If $|\varphi(x)|$ were finite, say $\varphi(x)^m = 1$ for some $m > 0$, then $\varphi(x^m) = 1$, and injectivity would give $x^m = 1$, a contradiction. Hence $|\varphi(x)| = \infty$.

Step 5 (Counting elements of a fixed order). For fixed $n \in \mathbb{Z}^+$, define

$$A_n = \{x \in G : \ |x| = n\}, \qquad B_n = \{y \in H : \ |y| = n\}.$$

By Steps 2–4, $x \in A_n \Leftrightarrow \varphi(x) \in B_n$. Since φ is bijective, $\varphi : A_n \to B_n$ is a bijection, so $|A_n| = |B_n|$.

Step 6 (Failure for mere homomorphisms). Let $H = \{1\}$ be the trivial group and $\theta : G \to H$ be the homomorphism $\theta(x) = 1$ for all $x \in G$. Then every element of H has order 1, while G may have elements of other orders. Thus order is not preserved and the counting statement fails for general homomorphisms.

Step 7 (Conclusion). Isomorphisms preserve (finite and infinite) orders and hence the counts of elements of each order; arbitrary homomorphisms need not.

1.6.3 Exercise 3. If $\varphi : G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\varphi : G \to H$ is a homomorphism, what additional conditions on φ (if any) are sufficient to ensure that if G is abelian, then so is H?

As General Proposition: Isomorphism preserves (and reflects) abelianness: $G \cong H \iff G$ abelian $\iff H$ abelian. For a general homomorphism, *surjectivity* is sufficient for abelianness to pass to the codomain: if φ is onto and G is abelian, then H is abelian. Without surjectivity the conclusion can fail.

As Conditional Proposition: Let $\varphi : G \to H$ be an isomorphism. Then G is abelian iff H is abelian. More generally, if $\varphi : G \to H$ is a surjective homomorphism and G is abelian, then H is abelian; however, if φ is not surjective, H need not be abelian.

. . . .

Intuition. An isomorphism is a relabeling that preserves products. If $ab = ba$ in G, then applying φ gives $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$ in H, and conversely by using φ^{-1}. For a general homomorphism, the image $\varphi(G)$ inherits abelianness from G; we get all of H abelian exactly when the image *is* H, i.e., when φ is onto.

. . . .

Proof.

Step 1 (Isomorphism ⇒ abelianness transfers $G \to H$). Assume $\varphi : G \to H$ is an isomorphism and G abelian. For any $x, y \in H$, choose $a, b \in G$ with $\varphi(a) = x$, $\varphi(b) = y$ (possible since φ is onto). Then
$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx$ **(since $ab = ba$ in G).**
Thus H is abelian.

Step 2 (Isomorphism ⇒ abelianness transfers $H \to G$). If H is abelian, apply Step 1 to the isomorphism $\varphi^{-1} : H \to G$ to conclude G is abelian. Hence G abelian ⇔ H abelian under isomorphism.

Step 3 (Surjective homomorphism suffices). Let $\varphi : G \to H$ be a surjective homomorphism and suppose G is abelian. For any $x, y \in H$, pick $a, b \in G$ with $\varphi(a) = x$, $\varphi(b) = y$ (surjectivity). Then
$xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx$ **(since $ab = ba$).**
Therefore H is abelian.

Step 4 (Why surjectivity is necessary). Without surjectivity, H can be nonabelian even though G is abelian. Example: take $G = \mathbb{Z}$ (abelian), $H = S_3$ (nonabelian), and define a homomorphism $\theta : \mathbb{Z} \to S_3$ by $\theta(n) = \begin{cases} e, & n \text{ even} \\ (12), & n \text{ odd.} \end{cases}$ Then θ is a homomorphism with abelian domain, but its image is the abelian subgroup $\{e, (12)\} \neq H$, and H itself remains nonabelian. Hence abelianness does not transfer to H in general unless φ is onto.

Step 5 (Conclusion). Isomorphisms preserve and reflect abelianness. For homomorphisms, surjectivity is a sufficient condition for abelianness of G to imply abelianness of H; absent surjectivity, the implication can fail.

1.6.4 Exercise 4. Prove that the multiplicative groups $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are not isomorphic.

As General Proposition: If two groups are isomorphic, they have the same multiset of element orders. In $\mathbb{R}^\times$ the only finite orders are 1 and 2, whereas $\mathbb{C}^\times$ contains elements of order 4 (e.g. $\pm i$). Hence $\mathbb{R}^\times \ncong \mathbb{C}^\times$.

As Conditional Proposition: Let $\varphi : \mathbb{R}^\times \to \mathbb{C}^\times$ be any group isomorphism candidate. Since isomorphisms preserve orders, the absence of order-4 elements in $\mathbb{R}^\times$ versus their presence in $\mathbb{C}^\times$ forbids φ from being bijective; therefore no isomorphism exists.

. . . .

Intuition. Real nonzero numbers on the unit circle are just ±1, so among reals only 1 (order 1) and -1 (order 2) have finite order. The complex unit circle S^1 has all roots of unity, including i with $i^4 = 1$ but $i^2 \neq 1$. Because isomorphisms preserve element orders, the groups cannot be isomorphic.

. . . .

Proof.

Step 1 (Finite orders in $\mathbb{R}^\times$). Let $r \in \mathbb{R}^\times$ have finite order $n \geq 1$, so $r^n = 1$. Then r is a real nth root of unity. The only real solutions of $x^n = 1$ are $x = 1$ (for all n) and $x = -1$ (only when n is even). Thus the only possibilities are $r = 1$ (order 1) or $r = -1$ (order 2).

Step 2 (Existence of order-4 in $\mathbb{C}^\times$). In $\mathbb{C}^\times$, take $z = i$. Then $i^4 = 1$ while $i^2 = -1 \neq 1$, hence $|i| = 4$. Likewise $|-i| = 4$.

Step 3 (Isomorphisms preserve order). If $\psi : G \to H$ is an isomorphism and $x \in G$ has order m, then $\psi(x)^m = \psi(x^m) = \psi(1) = 1$, and minimality of m transfers via bijectivity; hence $|\psi(x)| = |x|$.

Step 4 (Derive contradiction). If $\mathbb{R}^\times \cong \mathbb{C}^\times$, then by Step 3 the sets of attainable element orders must coincide. But by Step 1, $\mathbb{R}^\times$ has no element of order 4, whereas by Step 2, $\mathbb{C}^\times$ does. Contradiction.

Step 5 (Conclusion). Therefore $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$ are not isomorphic as groups under multiplication.

1.6.7 Exercise 7. Prove that D_8 and Q_8 are not isomorphic.

As General Proposition: If two finite groups are isomorphic, they have the same number of elements of each order. In D_8 there are five elements of order 2, while in Q_8 there is exactly one; hence $D_8 \ncong Q_8$.

As Conditional Proposition: Let $D_8 = \langle r, s \mid r^4 = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$ (symmetries of a square) and $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with $i^2 = j^2 = k^2 = ijk = -1$. Then D_8 and Q_8 are not isomorphic because their order-2 elements occur in different quantities.

. . . .

Intuition. Isomorphisms preserve orders of elements. Count the involutions (elements of order 2) in each group: D_8 has four reflections and the half-turn r^2, while Q_8 has only -1. Different counts forbid an isomorphism.

. . . .

Proof.

Step 1 (Orders in D_8). The elements are $1, r, r^2, r^3, s, sr, sr^2, sr^3$. We have $|r| = 4$, so $|r^2| = 2$. Each reflection s, sr, sr^2, sr^3 satisfies $(sr^k)^2 = 1$, so each has order 2. Thus D_8 has *five* elements of order 2: $\{r^2, s, sr, sr^2, sr^3\}$.
Step 2 (Orders in Q_8). In Q_8, -1 has order 2 and the six elements $\pm i, \pm j, \pm k$ each have order 4. Hence Q_8 has *exactly one* element of order 2.
Step 3 (Isomorphisms preserve orders). If $\varphi : G \to H$ is an isomorphism and $x \in G$ has order m, then $\varphi(x)$ has order m as well. Therefore G and H must have the same number of elements of each order.
Step 4 (Conclude nonisomorphism). Since D_8 and Q_8 have different numbers of elements of order 2 (five versus one), no isomorphism between them can exist. Hence $D_8 \not\cong Q_8$.

1.6.18 Exercise 18. Let G be any group. Prove that the map $\psi : G \to G$ defined by $\psi(g) = g^2$ is a homomorphism if and only if G is abelian.

As General Proposition: Squaring defines an endomorphism $\psi(g) = g^2$ precisely on abelian groups.

As Conditional Proposition: For a group G, the map $\psi(g) = g^2$ satisfies $\psi(ab) = \psi(a)\psi(b)$ for all $a, b \in G$ iff $ab = ba$ for all $a, b \in G$.

. . . .

Intuition. Being a homomorphism means $(ab)^2 = a^2b^2$ for all a, b. Expanding gives $abab = aabb$; canceling the outer a's and b's forces $ba = ab$. Conversely, if everything commutes, the square of a product is the product of squares.

. . . .

Proof.

Step 1 (If G is abelian, then ψ is a homomorphism). Assume $ab = ba$ for all $a, b \in G$. Then for any a, b,

$$\psi(ab) = (ab)^2 = abab = aabb = a^2b^2 = \psi(a)\psi(b).$$

Thus ψ is a homomorphism.

Step 2 (If ψ is a homomorphism, then G is abelian). Assume ψ is a homomorphism. Then for any a, b,

$$(ab)^2 = \psi(ab) = \psi(a)\psi(b) = a^2b^2,$$

i.e. $abab = aabb$.

Step 3 (Cancel to obtain commutativity). Left-multiply $abab = aabb$ by a^{-1} and right-multiply by b^{-1} to get

$$bab = abb \quad \Rightarrow \quad ba = ab.$$

Since a, b were arbitrary, G is abelian.

Step 4 (Conclusion). The squaring map $g \mapsto g^2$ is a group homomorphism exactly when G is abelian.

1.6.20 Exercise 20. Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms from G onto G. Prove that $\mathrm{Aut}(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\mathrm{Aut}(G)$ are called *automorphisms of* G).

As General Proposition: The set of all bijective homomorphisms $G \to G$ forms a group under composition.

As Conditional Proposition: With operation $(\phi, \psi) \mapsto \phi \circ \psi$, the quadruple $(\mathrm{Aut}(G), \circ, \mathrm{id}_G, \ \cdot^{-1})$ satisfies the group axioms: closure, associativity, identity, inverses.

. . . .

Intuition. Composing two structure-preserving bijections still preserves structure and remains bijective; the identity map is trivially such; and the inverse of a structure-preserving bijection also preserves structure. Since composition of functions is always associative, the group axioms follow mechanically.

. . . .

Proof.

Step 1 (Closure). Let $\phi, \psi \in \mathrm{Aut}(G)$. Then ϕ, ψ are bijective homomorphisms $G \to G$. For any $a, b \in G$,

$$(\phi \circ \psi)(ab) = \phi(\psi(ab)) = \phi(\psi(a)\psi(b)) = \phi(\psi(a))\,\phi(\psi(b)) = (\phi \circ \psi)(a)\,(\phi \circ \psi)(b),$$

so $\phi \circ \psi$ is a homomorphism. As a composition of bijections, it is bijective; hence $\phi \circ \psi \in \mathrm{Aut}(G)$.

Step 2 (Associativity). For all $\alpha, \beta, \gamma \in \mathrm{Aut}(G)$ and all $x \in G$,

$$((\alpha \circ \beta) \circ \gamma)(x) = \alpha(\beta(\gamma(x))) = (\alpha \circ (\beta \circ \gamma))(x),$$

so composition is associative on $\mathrm{Aut}(G)$.

Step 3 (Identity element). The identity map $\mathrm{id}_G : G \to G$ satisfies $\mathrm{id}_G(ab) = ab = \mathrm{id}_G(a)\mathrm{id}_G(b)$, hence $\mathrm{id}_G \in \mathrm{Aut}(G)$. For any $\phi \in \mathrm{Aut}(G)$ we have $\phi \circ \mathrm{id}_G = \mathrm{id}_G \circ \phi = \phi$; thus id_G is the identity element.

Step 4 (Inverses). If $\phi \in \mathrm{Aut}(G)$, then ϕ is a bijective homomorphism. For any $a, b \in G$, using surjectivity pick $u, v \in G$ with $\phi(u) = a$ and $\phi(v) = b$. Then

$$\phi(uv) = \phi(u)\phi(v) = ab.$$

Applying ϕ^{-1} yields $uv = \phi^{-1}(a)\phi^{-1}(b)$, so ϕ^{-1} is a homomorphism. Being the inverse of a bijection, it is bijective; hence $\phi^{-1} \in \mathrm{Aut}(G)$. Moreover, $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \mathrm{id}_G$.

Step 5 (Conclusion). Steps 1–4 establish closure, associativity, identity, and inverses for $(\mathrm{Aut}(G), \circ)$. Therefore $\mathrm{Aut}(G)$ is a group under composition.