MATH5353

Harley Caham Combest

Fa2025 Ch1 Intro to Groups Mk1

Ch 1: Lingua Franca

Overview. These are designed to test your memory on the tools of the trade: the words, the axioms, the theorems, etc of the basics of Introduction to Groups as presented in Ch1 of Dummit and Foote.

Definition: Group.

A *group* is a pair $(G, \cdot)$ consisting of a set G and a binary operation $\cdot : G \times G \to G$ such that:

1. (Associativity) $(ab)c = a(bc)$ for all $a, b, c \in G$.
2. (Identity) There exists $e \in G$ with $ea = ae = a$ for all $a \in G$.
3. (Inverses) For each $a \in G$ there exists $a^{-1} \in G$ with $aa^{-1} = a^{-1}a = e$.

Definition: Abelian Group.

A group G is *abelian* (or *commutative*) if $ab = ba$ for all $a, b \in G$.

Definition: Order of a Group.

If G has finitely many elements, its *order* is $|G| = \#G$. If G is not finite, we say G is infinite.

Definition: Order of an Element.

For $g \in G$, the *order* $|g|$ is the least positive integer n such that $g^n = e$, if such an n exists; otherwise $|g| = \infty$. We adopt the conventions $g^0 = e$ and $g^{-n} = (g^{-1})^n$ for $n > 0$.

Proposition: Uniqueness of Identity.

In any group, the identity element is unique.

Intuition. If two elements both act as identity, they must coincide since each forces the other to stay fixed.

Proof. **Step 1.** Suppose e and f are both identities in G.

Step 2. Because f is a right identity, $ef = e$.

Step 3. Because e is a left identity, $ef = f$.

Step 4. Hence $e = f$. The identity element is unique.

□

Proposition: Uniqueness of Inverses.

In any group, every element has a unique inverse.

. . . . . .

Intuition. Two different "undoers" of the same element must agree when multiplied through the element they invert.

. . . . . .

Proof. **Step 1.** Let $a \in G$, and suppose b and c are inverses of a. Then $ab = ba = e$ and $ac = ca = e$.

Step 2. Compute $b = be = b(ac) = (ba)c = ec = c$.

Step 3. Therefore $b = c$. Every element's inverse is unique.

□

Proposition: Cancellation Law.

In a group, if $ax = ay$ then $x = y$; and if $xa = ya$ then $x = y$.

. . . . . .

Intuition. Since every element is invertible, we can cancel a common factor by multiplying by its inverse on the appropriate side.

. . . . . .

Proof. **Step 1 (Left cancellation).** Assume $ax = ay$. Multiply on the left by a^{-1}:

$$a^{-1}(ax) = a^{-1}(ay) \Rightarrow (a^{-1}a)x = (a^{-1}a)y \Rightarrow ex = ey \Rightarrow x = y.$$

Step 2 (Right cancellation). Assume $xa = ya$. Multiply on the right by a^{-1}:

$$(xa)a^{-1} = (ya)a^{-1} \Rightarrow x(aa^{-1}) = y(aa^{-1}) \Rightarrow xe = ye \Rightarrow x = y.$$

□

Proposition: Inverse of a Product.

For any a, b in a group, the inverse of their product is $(ab)^{-1} = b^{-1}a^{-1}$.

. . . . . .

Intuition. To undo a product ab, you must first undo b, then undo a—hence the order of factors reverses.

. . . . . .

Proof. **Step 1.** Compute $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$.
Step 2. Compute $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$.
Step 3. Hence $b^{-1}a^{-1}$ is a two–sided inverse of ab, so $(ab)^{-1} = b^{-1}a^{-1}$.

□

Proposition: Double Inverse.

For any element a in a group, $(a^{-1})^{-1} = a$.

.....

Intuition. Inverting twice restores the original element.

.....

Proof. **Step 1.** By definition, $aa^{-1} = a^{-1}a = e$.

Step 2. The element a satisfies $a^{-1}a = aa^{-1} = e$, so a is an inverse of a^{-1}.

Step 3. By uniqueness of inverses, $(a^{-1})^{-1} = a$.

□

Proposition: Exponent Laws in a Group.

For all integers m, n and any a in a group,

$$a^m a^n = a^{m+n}, \qquad (a^m)^n = a^{mn}.$$

Intuition. Associativity lets us group repeated factors however we like; inverses extend the exponent rules to negatives.

Proof. **Step 1 (Positive exponents).** For $m, n > 0$, concatenating m and n copies of a gives a^{m+n}.

Step 2 (Zero exponent). Define $a^0 = e$ so that the law still holds when one exponent is 0.

Step 3 (Negative exponents). Define $a^{-n} = (a^{-1})^n$ for $n > 0$; then $a^m a^{-m} = e$.

Step 4. Using these definitions, $a^m a^n = a^{m+n}$ holds for all $m, n \in \mathbb{Z}$.

Step 5. For the second law, expand $(a^m)^n$ as a^{mn} using Step 1 and extend to negatives analogously.

□

Proposition: Solving Linear Equations in a Group.

In any group, the equations $ax = b$ and $xa = b$ have unique solutions:

$$x = a^{-1}b \quad \text{and} \quad x = ba^{-1}.$$

Intuition. Since all elements are invertible, we can "divide" by a on the proper side to isolate x.

Proof. **Step 1 (Left equation).** Start with $ax = b$. Left-multiply by a^{-1}:

$$a^{-1}(ax) = a^{-1}b \Rightarrow (a^{-1}a)x = a^{-1}b \Rightarrow ex = a^{-1}b \Rightarrow x = a^{-1}b.$$

Step 2. If $ax = ax'$, left cancellation gives $x = x'$; uniqueness follows.
Step 3 (Right equation). Start with $xa = b$. Right-multiply by a^{-1}:

$$(xa)a^{-1} = ba^{-1} \Rightarrow x(aa^{-1}) = ba^{-1} \Rightarrow xe = ba^{-1} \Rightarrow x = ba^{-1}.$$

Step 4. If $xa = x'a$, right cancellation gives $x = x'$; uniqueness follows.

□

Proposition: Order–Divisibility Property.

If $|g| = n < \infty$, then $g^k = e$ if and only if n divides k.

. . . . . .

Intuition. The smallest positive power returning g to e is n; all others are multiples of n.

. . . . . .

Proof. **Step 1.** Assume $g^k = e$. Divide $k = qn + r$ with $0 \leq r < n$.
Step 2. Then $g^k = g^{qn+r} = (g^n)^q g^r = e^q g^r = g^r$.
Step 3. Hence $g^r = e$. By minimality of n, $r = 0$, so $n \mid k$.
Step 4. Conversely, if $n \mid k$, then $k = qn$ and $g^k = (g^n)^q = e^q = e$.
Step 5. Therefore $g^k = e \iff n \mid k$.

□

Definition: Dihedral Group.

For each integer $n \geq 3$, the *dihedral group* D_{2n} (sometimes denoted D_n) is the group of rigid symmetries of a regular n–gon in the plane. It has $2n$ elements: n rotations and n reflections. A convenient presentation is

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ srs = r^{-1} \rangle,$$

where r represents rotation by $360^\circ/n$ and s represents reflection across some axis of symmetry.

Proposition: Structure of Elements in D_{2n}.

Every element of D_{2n} can be written uniquely as either r^k or sr^k with $0 \leq k < n$.

. . . . . .

Intuition. Each element of D_{2n} is either a pure rotation (r^k) or a reflection (sr^k). The relation $srs = r^{-1}$ guarantees that any product can be reduced to one of these two forms.

. . . . . .

Proof. **Step 1.** The generators satisfy $r^n = 1$ and $s^2 = 1$, so any word in r, s can be reduced using these relations.

Step 2. Move all s's to the left using $sr = r^{-1}s$. Repeatedly applying this yields every word in the form r^k or sr^k.

Step 3. There are $2n$ distinct such elements: n of type r^k and n of type sr^k.

Step 4. Distinctness follows since $r^i = r^j \Rightarrow i \equiv j \pmod{n}$ and $r^i \neq sr^j$ (the latter fixes no vertices that s moves).

Step 5. Thus each element of D_{2n} is uniquely one of r^k or sr^k.

□

Proposition: Orders of Elements in D_{2n}.

In $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ srs = r^{-1} \rangle$,

$$|r| = n, \quad |s| = 2, \quad |sr^k| = 2 \text{ for all } k.$$

.....

Intuition. Rotations correspond to multiples of $360°/n$, giving order n. Reflections flip across an axis, always squaring to the identity, hence order 2.

.....

Proof. **Step 1.** Since $r^n = 1$ and n is minimal, $|r| = n$.

Step 2. By definition, $s^2 = 1$, so $|s| = 2$.

Step 3. For a general reflection sr^k, compute:

$$(sr^k)^2 = sr^k sr^k = s(r^k s)r^k.$$

Step 4. Using $sr = r^{-1}s$, we have $r^k s = sr^{-k}$. Substitute to get

$$(sr^k)^2 = s(sr^{-k})r^k = (ss)r^{-k}r^k = 1.$$

Step 5. Hence $|sr^k| = 2$ for all k.

□

Proposition: Reflection–Rotation Relation.

In the dihedral group D_{2n}, the generators satisfy $srs = r^{-1}$, and therefore $sr^k s = r^{-k}$ for all integers k.

. . . . . .

Intuition. Reflecting, rotating, then reflecting again reverses orientation, effectively applying the inverse rotation. Reflections conjugate r to its inverse.

. . . . . .

Proof. **Step 1.** The defining relation gives $srs = r^{-1}$.

Step 2. Multiply this relation repeatedly to generalize:

$$sr^k s = (srs)(srs)\cdots(srs) \ (k \text{ factors}) = r^{-k}.$$

Step 3. Verify by induction on k: Base case $k = 1$ holds by assumption. If $sr^k s = r^{-k}$, then

$$sr^{k+1}s = s(r^k r)s = (sr^k s)(srs) = r^{-k}r^{-1} = r^{-(k+1)}.$$

Step 4. Thus $sr^k s = r^{-k}$ for all integers k.

□

Proposition: Multiplication Rules in D_{2n}.

Let $D_{2n} = \{r^k,\, sr^k \mid 0 \le k < n\}$. Then multiplication is governed by

$$r^i r^j = r^{i+j}, \quad (sr^i)(sr^j) = r^{i-j}, \quad (sr^i)r^j = sr^{i-j}, \quad r^i(sr^j) = sr^{i+j},$$

with all exponents taken mod n.

.....

Intuition. The relations $r^n = 1$, $s^2 = 1$, and $srs = r^{-1}$ control how rotations and reflections compose. The key is $sr = r^{-1}s$, which swaps the order of s and r but inverts the exponent.

.....

Proof. **Step 1.** From $r^n = 1$, we have $r^i r^j = r^{i+j} \pmod n$.

Step 2. For $(sr^i)(sr^j)$, use $sr^i s = r^{-i}$:

$$(sr^i)(sr^j) = s(r^i s)r^j = s(sr^{-i})r^j = r^{-i}r^j = r^{i-j}.$$

Step 3. For $(sr^i)r^j$, use $sr = r^{-1}s$:

$$(sr^i)r^j = sr^{i-j}.$$

Step 4. For $r^i(sr^j)$:

$$r^i(sr^j) = (r^i s)r^j.$$

Using $r^i s = sr^{-i}$, we get $r^i(sr^j) = sr^{-i+j} = sr^{i+j} \pmod n$.

Step 5. All multiplication rules are thus verified.

□

Proposition: Center of D_{2n}.

The center $Z(D_{2n})$ is

$$Z(D_{2n}) = \begin{cases} \{1,\, r^k\}, & \text{if } n \text{ is even (with } k = n/2), \\ \{1\}, & \text{if } n \text{ is odd.} \end{cases}$$

Intuition. A rotation r^k commutes with every element iff it commutes with reflections. That happens precisely when $r^k = r^{-k}$, i.e. $r^{2k} = 1$. Reflections never commute with all elements.

Proof. **Step 1.** Let $z \in Z(D_{2n})$. Then z commutes with both r and s.

Step 2. If $z = r^k$, then $r^k s = sr^k$. But $sr^k = r^{-k}s$, so $r^k s = sr^k$ implies $r^{-k} = r^k$, i.e. $r^{2k} = 1$.

Step 3. Therefore $n \mid 2k$. If n is even, $k \equiv 0$ or $k \equiv n/2 \bmod n$; if n is odd, only $k \equiv 0$.

Step 4. Hence when n even, $\{1, r^{n/2}\}$ lies in the center; when odd, only $\{1\}$.

Step 5. Reflections sr^i fail to commute with r:

$$(sr^i)r = sr^{i+1}, \quad r(sr^i) = sr^{i-1}.$$

These are equal only if $r^{i+1} = r^{i-1}$, i.e. $r^2 = 1$, impossible for $n \geq 3$.

Step 6. Thus no reflection lies in $Z(D_{2n})$. The result follows.

□

Proposition: Central Involution in D_{2n} (when n even).

If $n = 2k \geq 4$, then $z = r^k$ has order 2, commutes with all elements of D_{2n}, and is the only nonidentity element that does so.

. . . . . .

Intuition. When n is even, rotation halfway around the polygon reverses every vertex, behaving like a reflection squared. This rotation r^k commutes with both r and s, hence lies in the center—and no other nontrivial element does.

. . . . . .

Proof. **Step 1.** Since $r^{2k} = r^n = 1$, $z = r^k$ has order 2.

Step 2. For rotations, $zr^i = r^{k+i} = r^{i+k} = r^i z$, so z commutes with all r^i.

Step 3. For reflections, using $sr = r^{-1}s$ and $r^k = r^{-k}$:

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

Step 4. Hence z commutes with every element, so $z \in Z(D_{2n})$.

Step 5. If r^t is central, then $sr^t = r^t s$. Using $sr^t = r^{-t}s$, this forces $r^{-t} = r^t$, hence $r^{2t} = 1$. Thus $t \equiv 0$ or $t \equiv k \bmod n$.

Step 6. Therefore the only nonidentity central element is r^k.

□

Definition: Symmetric Group.

The *symmetric group* on n symbols, denoted S_n, is the set of all bijections (permutations)

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

under composition of functions. The identity element is the identity permutation, and the inverse of σ is its inverse function σ^{-1}.

Proposition: Order of S_n.

The symmetric group S_n has order $n!$.

Intuition. Each permutation is a unique rearrangement of n objects. There are n choices for the image of 1, $(n-1)$ for 2, etc., giving $n! = n(n-1)\cdots 1$ total bijections.

Proof. **Step 1.** A permutation σ is a bijection of $\{1, \ldots, n\}$ onto itself.

Step 2. The number of bijections from an n-element set to itself is $n!$.

Step 3. Hence $|S_n| = n!$.

□

Definition: Cycle.

A *cycle* $(a_1\, a_2\, \ldots\, a_k)$ in S_n is the permutation sending

$$a_1 \mapsto a_2,\ a_2 \mapsto a_3,\ \ldots,\ a_{k-1} \mapsto a_k,\ a_k \mapsto a_1,$$

and fixing all other elements of $\{1, \ldots, n\}$. The integer k is called the *length* of the cycle.

Definition: Transposition.

A *transposition* is a 2–cycle $(a\,b)$ exchanging a and b while fixing all other elements.

Proposition: Disjoint Cycles Commute.

If two cycles $\alpha, \beta \in S_n$ have disjoint supports (they move disjoint sets of symbols), then $\alpha\beta = \beta\alpha$.

. . . . . .

Intuition. If two permutations act on disjoint sets of symbols, each fixes all points the other moves; their actions therefore do not interfere.

. . . . . .

Proof. **Step 1.** Let $\alpha = (a_1 \ \dots \ a_k)$ and $\beta = (b_1 \ \dots \ b_m)$ with $\{a_i\} \cap \{b_j\} = \varnothing$.

Step 2. For any x in $\{1, \dots, n\}$, consider three cases.

Step 3. If x is moved by α but not by β, then $\beta(x) = x$, so $\alpha\beta(x) = \alpha(x) = \beta\alpha(x)$.

Step 4. If x is moved by β but not α, the argument is symmetric.

Step 5. If x is fixed by both, both compositions fix x.

Step 6. Hence $\alpha\beta(x) = \beta\alpha(x)$ for all x, so α and β commute.

□

Proposition: Decomposition into Disjoint Cycles.

Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. This decomposition is unique up to the order in which the cycles are written.

Intuition. Each element i of $\{1, \ldots, n\}$ traces an orbit under repeated application of σ. Each orbit gives one cycle; disjoint orbits yield disjoint cycles.

Proof. **Step 1.** For each i, follow its orbit $i, \sigma(i), \sigma^2(i), \ldots$ until it repeats. This yields a cycle $(i\, \sigma(i)\, \ldots)$.

Step 2. Each element of $\{1, \ldots, n\}$ belongs to exactly one such orbit.

Step 3. The cycles are disjoint since orbits are disjoint.

Step 4. The product of these disjoint cycles equals σ.

Step 5. Uniqueness: the orbits are intrinsic to σ, so their corresponding cycles are uniquely determined up to ordering.

□

Proposition: Order of a Permutation.

If σ decomposes into disjoint cycles of lengths $l_1, l_2, \ldots, l_r$, then

$$|\sigma| = \operatorname{lcm}(l_1, l_2, \ldots, l_r).$$

Intuition. A permutation returns to the identity only when each disjoint cycle has completed an integer number of turns. The smallest such number is the least common multiple of their lengths.

Proof. **Step 1.** Let $\sigma = \tau_1 \tau_2 \cdots \tau_r$ be disjoint cycles with lengths l_i.
Step 2. Because the τ_i commute, $\sigma^m = \tau_1^m \cdots \tau_r^m$.
Step 3. $\sigma^m = 1$ iff $\tau_i^m = 1$ for all i.
Step 4. For each τ_i, $\tau_i^m = 1$ iff $l_i \mid m$.
Step 5. Hence $\sigma^m = 1$ iff each $l_i \mid m$; minimal such m is $\operatorname{lcm}(l_1, \ldots, l_r)$.

□

Proposition: Conjugation of a Cycle.

For any $\sigma \in S_n$ and any k–cycle $(a_1\, a_2\, \ldots\, a_k)$,

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

.....

Intuition. Conjugation relabels symbols according to σ. The cycle structure is preserved but the actual symbols are replaced by their images under σ.

.....

Proof. **Step 1.** Let $c = (a_1\, a_2\, \ldots\, a_k)$.

Step 2. For any $x \in \{1, \ldots, n\}$, examine $y = \sigma^{-1}(x)$.

Step 3. If $y = a_i$ for some $i < k$, then

$$\sigma c \sigma^{-1}(x) = \sigma c(y) = \sigma(a_{i+1}).$$

Step 4. If $y = a_k$, then $\sigma c \sigma^{-1}(x) = \sigma(a_1)$.

Step 5. If $y \notin \{a_1, \ldots, a_k\}$, both sides fix x.

Step 6. Thus $\sigma c \sigma^{-1}$ permutes $\sigma(a_i)$ in the same cyclic order, i.e.

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

□

Definition: Even and Odd Permutations.

A permutation $\sigma \in S_n$ is called *even* if it can be written as a product of an even number of transpositions, and *odd* if it requires an odd number. The parity of σ is well-defined (independent of the chosen decomposition).

Definition: Alternating Group.

The *alternating group* A_n is the subgroup of S_n consisting of all even permutations:

$$A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}.$$

It has order $|A_n| = n!/2$ for $n \geq 2$.

Definition: Subgroup.

A nonempty subset H of a group G is called a *subgroup* (written $H \leq G$) if H is closed under the group operation and inverses; that is,

$$ab^{-1} \in H \quad \text{for all } a, b \in H.$$

The group operation and identity on H are those inherited from G.

Proposition: Subgroup Test.

Let G be a group and $H \subseteq G$. Then H is a subgroup of G if and only if it is nonempty and for all $a, b \in H$, $ab^{-1} \in H$.

Intuition. Checking all three group axioms directly is tedious; the test reduces them to a single closure property using inverses and the identity implicitly.

Proof. **Step 1 ($\Rightarrow$).** If $H \leq G$, then H is closed under products and inverses. Thus for $a, b \in H$, $b^{-1} \in H$ and $ab^{-1} \in H$.

Step 2 ($\Leftarrow$). Assume H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$.

Step 3. Pick $h \in H$. Then $hh^{-1} = e \in H$, so the identity belongs to H.

Step 4. For any $x \in H$, $e, x \in H$ implies $ex^{-1} = x^{-1} \in H$.

Step 5. For $x, y \in H$, since $y^{-1} \in H$, closure gives $x(y^{-1})^{-1} = xy \in H$.

Step 6. Hence H contains e, inverses, and is closed under multiplication, so $H \leq G$.

□

Definition: Proper Subgroup.

If H is a subgroup of G and $H \neq G$, we call H a *proper subgroup* of G, denoted $H < G$.

Proposition: Intersection of Subgroups.

The intersection of any collection of subgroups of a group G is itself a subgroup of G.

. . . . . .

Intuition. All properties of a group (closure, inverses, identity) are universal statements, preserved under intersection.

. . . . . .

Proof. **Step 1.** Let $\{H_i\}_{i\in I}$ be subgroups of G, and set $H = \bigcap_{i\in I} H_i$.
Step 2. Each H_i contains e_G, so $e_G \in H$; thus $H \neq \varnothing$.
Step 3. If $a, b \in H$, then $a, b \in H_i$ for all i, so $ab^{-1} \in H_i$ for all i.
Step 4. Hence $ab^{-1} \in \bigcap_i H_i = H$.
Step 5. By the subgroup test, $H \leq G$.

□

Definition: Subgroup Generated by a Set.

For $A \subseteq G$, the *subgroup generated by* A is

$$\langle A \rangle = \bigcap \{H \leq G \mid A \subseteq H\}.$$

It is the smallest subgroup of G containing A. If $A = \{a\}$, $\langle A \rangle = \{a^n : n \in \mathbb{Z}\}$ is the cyclic subgroup generated by a.

Proposition: Generated Subgroup Properties.

For any $A \subseteq G$, $\langle A \rangle$ is a subgroup of G, contains A, and is contained in every subgroup of G that contains A.

. . . . . .

Intuition. By definition, $\langle A \rangle$ is the intersection of all subgroups containing A; intersections of subgroups are subgroups, making $\langle A \rangle$ the minimal one containing A.

. . . . . .

Proof. **Step 1.** By definition $\langle A \rangle = \bigcap \{H \leq G : A \subseteq H\}$.

Step 2. Each H in the family is a subgroup, so by the intersection proposition, $\langle A \rangle$ is a subgroup.

Step 3. Each H in the intersection contains A, hence $A \subseteq \langle A \rangle$.

Step 4. If K is any subgroup containing A, then K is among those intersected, so $\langle A \rangle \subseteq K$.

Step 5. Therefore $\langle A \rangle$ is the smallest subgroup containing A.

□

Definition: Cyclic Group.

A group G is called *cyclic* if there exists $g \in G$ such that $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Such an element g is called a *generator* of G.

Proposition: Subgroups of Cyclic Groups.

If $G = \langle g \rangle$ is a cyclic group of order n, then the subgroups of G are precisely the $\langle g^d \rangle$ for all divisors d of n. In particular, G has exactly one subgroup of order d for each $d \mid n$.

. . . . . .

Intuition. Every element in a cyclic group is a power of g; the order of g^k divides n, so each divisor gives one unique subgroup.

. . . . . .

Proof. **Step 1.** Let $|G| = n$. For $d \mid n$, $(g^d)^{n/d} = g^n = e$, so $|\langle g^d \rangle| = n/d$.

Step 2. Every subgroup $H \leq G$ is cyclic (since all its elements are powers of g).

Step 3. Let $H = \langle g^k \rangle$. Then $|H| = n/\gcd(n, k)$.

Step 4. Setting $d = \gcd(n, k)$ gives $H = \langle g^d \rangle$ with $|H| = n/d$.

Step 5. Thus each divisor d of n corresponds to a unique subgroup $\langle g^d \rangle$ of order n/d, establishing a bijection between divisors of n and subgroups of G.

□

Definition: Cyclic Group.

A group G is called *cyclic* if there exists $g \in G$ such that $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Such an element g is called a *generator* of G.

Proposition: Structure of Cyclic Groups.

Every cyclic group $G = \langle g \rangle$ is isomorphic to either $\mathbb{Z}$ (if $|G| = \infty$) or $\mathbb{Z}_n$ (if $|G| = n < \infty$).

Intuition. Cyclic groups consist solely of powers of a single element. Mapping each integer k to g^k respects addition and reproduces the group operation exactly.

Proof. **Step 1.** Define $\varphi : \mathbb{Z} \to G$ by $\varphi(k) = g^k$.

Step 2. φ is a homomorphism because $\varphi(a + b) = g^{a+b} = g^a g^b = \varphi(a)\varphi(b)$.

Step 3. If G is infinite, $g^k = g^m$ implies $k = m$; $\ker \varphi = \{0\}$, so φ is injective and surjective. Hence $G \cong \mathbb{Z}$.

Step 4. If G has order n, then $g^n = e$. $\ker \varphi = n\mathbb{Z}$, and by the First Isomorphism Theorem,

$$G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

Step 5. Therefore cyclic groups are precisely $\mathbb{Z}$ or $\mathbb{Z}_n$ up to isomorphism.

□

Proposition: Order of Powers in Cyclic Groups.

If $G = \langle g \rangle$ has order $n < \infty$, then for every integer k,

$$|\langle g^k \rangle| = \frac{n}{\gcd(n, k)}.$$

Intuition. The element g^k repeats after $\frac{n}{\gcd(n,k)}$ steps because $g^n = e$ and the smallest positive power of g^k that yields e occurs when its total exponent is a multiple of n.

Proof. **Step 1.** Let $|g| = n$. Then $(g^k)^m = e$ iff $g^{km} = e$ iff $n \mid km$.
Step 2. The smallest positive integer m satisfying $n \mid km$ is $m = n/\gcd(n, k)$.
Step 3. Hence $|\langle g^k \rangle| = n/\gcd(n, k)$.

□

Proposition: Subgroups of a Cyclic Group.

If $G = \langle g \rangle$ has order n, then for each divisor d of n there is exactly one subgroup of order d, namely $\langle g^{n/d} \rangle$.

. . . . . .

Intuition. Every subgroup of a cyclic group is cyclic. The order of g^k is $n/\gcd(n,k)$, so setting this equal to d identifies the unique generator of the subgroup of order d.

. . . . . .

Proof. **Step 1.** Let $d \mid n$. Then $(g^{n/d})^d = g^n = e$, so $|\langle g^{n/d} \rangle| \mid d$.

Step 2. If the order were smaller than d, say $m < d$, then $(g^{n/d})^m = g^{mn/d} = e$, forcing $n \mid mn/d$, so $d \mid m$, contradiction.

Step 3. Hence $|\langle g^{n/d} \rangle| = d$.

Step 4. Any subgroup $H \leq G$ is cyclic, say $H = \langle g^k \rangle$, and $|H| = n/\gcd(n,k) = d$. Then $\gcd(n,k) = n/d$, so $H = \langle g^{n/d} \rangle$.

Step 5. Thus there is exactly one subgroup of each order $d \mid n$.

□

Proposition: Cyclic Groups are Abelian.

Every cyclic group is abelian.

. . . . . .

Intuition. All elements are powers of a single generator, and powers of the same element commute under multiplication.

. . . . . .

Proof. **Step 1.** Let $G = \langle g \rangle$. Then any $x, y \in G$ can be written $x = g^m$, $y = g^n$.

Step 2. Compute $xy = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = yx$.

Step 3. Hence $xy = yx$ for all $x, y \in G$, so G is abelian.

□

Proposition: Infinite Cyclic Groups.

Every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

. . . . . .

Intuition. The map from integers to powers of a generator is a bijective homomorphism when the group has no finite order element.

. . . . . .

Proof. **Step 1.** Let $G = \langle g \rangle$ and assume $|g| = \infty$.
Step 2. Define $\varphi : \mathbb{Z} \to G$ by $\varphi(k) = g^k$.
Step 3. φ is a homomorphism because $\varphi(a + b) = g^{a+b} = g^a g^b = \varphi(a)\varphi(b)$.
Step 4. If $\varphi(k) = \varphi(m)$ then $g^k = g^m \Rightarrow g^{k-m} = e$. Since $|g| = \infty$, this forces $k = m$.
Step 5. φ is injective and surjective, so $G \cong (\mathbb{Z}, +)$.

□

Proposition: Finite Cyclic Groups.

Every cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$.

. . . . . .

Intuition. The group operation corresponds to addition modulo n; mapping k to g^k preserves this structure.

. . . . . .

Proof. **Step 1.** Let $G = \langle g \rangle$ with $|g| = n$.

Step 2. Define $\varphi : \mathbb{Z}_n \to G$ by $\varphi(\overline{k}) = g^k$.

Step 3. Well-defined: if $k \equiv m \pmod{n}$, then $k - m = qn$, so $g^k = g^{m+qn} = g^m (g^n)^q = g^m$.

Step 4. Homomorphism: $\varphi(\overline{k} + \overline{m}) = \varphi(\overline{k+m}) = g^{k+m} = g^k g^m = \varphi(\overline{k})\varphi(\overline{m})$.

Step 5. Surjective because every g^k is in the image. Injective because $g^k = g^m \Rightarrow n \mid (k - m)$, so $\overline{k} = \overline{m}$.

Step 6. Hence φ is an isomorphism $\mathbb{Z}_n \cong G$.

□

Definition: Homomorphism.

A map $\varphi : G \to H$ between groups is a *homomorphism* if for all $x, y \in G$,

$$\varphi(xy) = \varphi(x)\varphi(y).$$

If φ is bijective, it is an *isomorphism*. An isomorphism from G to itself is an *automorphism*. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$.

Definition: Kernel and Image.

For a homomorphism $\varphi : G \to H$, the *kernel* and *image* are defined by

$$\ker \varphi = \{g \in G : \varphi(g) = e_H\}, \qquad \operatorname{Im} \varphi = \{\varphi(g) \mid g \in G\}.$$

Both are subgroups: $\ker \varphi \leq G$ and $\operatorname{Im} \varphi \leq H$.

Proposition: Basic Properties of Homomorphisms.

For any homomorphism $\varphi : G \to H$ and any $x, y \in G$:

1. $\varphi(e_G) = e_H$.
2. $\varphi(x^{-1}) = \varphi(x)^{-1}$.
3. $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

Intuition. A homomorphism respects multiplication, so it must carry the group structure faithfully—preserving identity, inverses, and all powers.

Proof. **Step 1.** Since $e_G e_G = e_G$, apply φ:

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G).$$

Multiply by $\varphi(e_G)^{-1}$ to get $\varphi(e_G) = e_H$.

Step 2. From $xx^{-1} = e_G$ we get $\varphi(x)\varphi(x^{-1}) = \varphi(e_G) = e_H$, so $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Step 3. For $n > 0$, prove by induction that $\varphi(x^n) = \varphi(x)^n$. Then extend to $n < 0$ using Step 2.

□

Proposition: Kernel and Image are Subgroups.

For any homomorphism $\varphi : G \to H$, the kernel $\ker \varphi$ is a subgroup of G, and the image $\operatorname{Im} \varphi$ is a subgroup of H.

Intuition. The kernel collects all elements mapping to the identity—it is closed under multiplication and inverses. Similarly, the image is closed under the same operations in H.

Proof. **Step 1.** For $\ker \varphi$: If $x, y \in \ker \varphi$, then $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H = e_H$, so $xy^{-1} \in \ker \varphi$.

Step 2. Hence $\ker \varphi$ satisfies the subgroup test, so $\ker \varphi \leq G$.

Step 3. For $\operatorname{Im} \varphi$: If $\varphi(x), \varphi(y) \in \operatorname{Im} \varphi$, then $\varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) \in \operatorname{Im} \varphi$.

Step 4. Thus $\operatorname{Im} \varphi \leq H$.

□

Proposition: Isomorphism Preserves Order.

If $\varphi : G \to H$ is an isomorphism, then $|\varphi(x)| = |x|$ for all $x \in G$.

Intuition. Isomorphisms preserve the algebraic structure exactly; therefore, they carry each element's repetition pattern (its order) onto its image.

Proof. **Step 1.** If x has order n, then $x^n = e_G$. Applying φ gives $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$.
Step 2. Thus $|\varphi(x)| \leq n$.
Step 3. If $\varphi(x)$ has order m, then $\varphi(x)^m = e_H$. Applying φ^{-1} gives $x^m = e_G$, so $|x| \leq m$.
Step 4. Therefore $|\varphi(x)| = |x|$.

□

Proposition: Isomorphism Preserves Abelian Property.

If $\varphi : G \to H$ is an isomorphism, then G is abelian if and only if H is abelian.

. . . . . .

Intuition. An isomorphism transfers multiplication structure exactly—if $ab = ba$ holds in G, then $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$ holds in H, and vice versa.

. . . . . .

Proof. **Step 1.** Assume G is abelian. For all $a, b \in G$:

$$\varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a),$$

so H is abelian.

Step 2. Conversely, if H is abelian, apply the same reasoning to $\varphi^{-1} : H \to G$ to conclude G is abelian.

□

Proposition: Surjective Homomorphism from Abelian Group.

If $\varphi : G \to H$ is a *surjective* homomorphism and G is abelian, then H is abelian.

. . . . . .

Intuition. Every element of H is an image of some element of G. If G's elements commute, their images must also commute.

. . . . . .

Proof. **Step 1.** Take any $x, y \in H$. Since φ is surjective, there exist $a, b \in G$ such that $\varphi(a) = x$, $\varphi(b) = y$.

Step 2. Then $xy = \varphi(a)\varphi(b) = \varphi(ab) = \varphi(ba) = \varphi(b)\varphi(a) = yx$.

Step 3. Thus H is abelian.

□

Proposition: $\mathbb{R}^\times$ and $\mathbb{C}^\times$ Are Not Isomorphic.

The multiplicative groups of nonzero real and complex numbers are not isomorphic.

. . . . . .

Intuition. Isomorphisms preserve the multiset of element orders. $\mathbb{C}^\times$ has elements of order 4 (like i), but $\mathbb{R}^\times$ has only 1 and -1 of finite order.

. . . . . .

Proof. **Step 1.** In $\mathbb{R}^\times$, if $x^n = 1$, then $x = 1$ or $x = -1$ (the only real nth roots of unity).

Step 2. Hence finite-order elements in $\mathbb{R}^\times$ are $\{1, -1\}$ with orders 1 and 2.

Step 3. In $\mathbb{C}^\times$, $i^4 = 1$ and $i^k \neq 1$ for $1 \leq k < 4$, so $\mathbb{C}^\times$ has an element of order 4.

Step 4. Since an isomorphism would preserve element orders, such an isomorphism cannot exist.

□

Proposition: D_8 and Q_8 Are Not Isomorphic.

The dihedral group D_8 and the quaternion group Q_8 are not isomorphic.

. . . . . .

Intuition. The pattern of element orders differs: D_8 has five elements of order 2, while Q_8 has only one element of order 2.

. . . . . .

Proof. **Step 1.** $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ with $r^4 = 1$, $s^2 = 1$, $srs = r^{-1}$.

Step 2. Elements of order 2 in D_8 are r^2, s, sr, sr^2, sr^3 (five elements).

Step 3. $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ with $i^2 = j^2 = k^2 = -1$.

Step 4. Q_8 has exactly one element of order 2, namely -1.

Step 5. Isomorphic groups must have the same number of elements of each order. Since they do not, $D_8 \ncong Q_8$.

□

Proposition: Square Map Criterion.

The map $\psi : G \to G$ defined by $\psi(g) = g^2$ is a homomorphism if and only if G is abelian.

. . . . . .

Intuition. $(ab)^2 = a^2b^2$ holds exactly when $ab = ba$. Commutativity is both necessary and sufficient for squaring to respect multiplication.

. . . . . .

Proof. **Step 1 ($\Rightarrow$).** Assume ψ is a homomorphism. Then

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

But $(ab)^2 = abab$, so $abab = a^2b^2 \Rightarrow ab = ba$. Hence G is abelian.

Step 2 ($\Leftarrow$). If G is abelian, then $(ab)^2 = abab = a^2b^2 = \psi(a)\psi(b)$, so ψ is a homomorphism. □

Definition: Automorphism Group.

For any group G, $\mathrm{Aut}(G)$ denotes the set of all isomorphisms from G onto itself, with composition as the group operation. It is called the *automorphism group* of G.

Proposition: $\mathrm{Aut}(G)$ **is a Group.**

$\mathrm{Aut}(G)$ forms a group under composition of functions.

. . . . . .

Intuition. Composition of bijective homomorphisms is again a bijective homomorphism; the identity map and inverses are also such maps, satisfying the group axioms.

. . . . . .

Proof. **Step 1.** If $\varphi, \psi \in \mathrm{Aut}(G)$, both are bijective homomorphisms, so $\psi \circ \varphi$ is also a bijective homomorphism. Hence closed under composition.

Step 2. Composition of functions is associative.

Step 3. The identity map id_G is a bijective homomorphism, acting as the identity element.

Step 4. If $\varphi \in \mathrm{Aut}(G)$, its inverse function φ^{-1} is also a bijective homomorphism (since $\varphi(\varphi^{-1}(xy)) = xy$). Thus inverses exist.

Step 5. All group axioms hold; therefore $\mathrm{Aut}(G)$ is a group under composition.

□

Definition: Group Action.

A *(left) group action* of a group G on a set A is a function

$$G \times A \to A, \qquad (g, a) \mapsto g \cdot a$$

such that for all $g_1, g_2 \in G$ and all $a \in A$:

1. $1 \cdot a = a$,
2. $(g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a)$.

If these hold, we say "G acts on A on the left."

Definition: Faithful, Transitive, and Free Actions.

Let G act on A.

- The action is *faithful* if the only element fixing every $a \in A$ is 1_G.
- It is *transitive* if for all $a, b \in A$ there exists $g \in G$ with $g \cdot a = b$.
- It is *free* if $g \cdot a = a$ for some a implies $g = 1_G$.

Definition: Orbit and Stabilizer.

Given a group action of G on A and $a \in A$:

- The *orbit* of a is $\mathrm{Orb}(a) = \{g \cdot a \mid g \in G\}$.
- The *stabilizer* of a is $\mathrm{Stab}(a) = \{g \in G \mid g \cdot a = a\}$.

Proposition: Stabilizer is a Subgroup.

For any $a \in A$, $\mathrm{Stab}(a)$ is a subgroup of G.

. . . . . .

Intuition. The elements that fix a are closed under products and inverses: combining symmetries that fix a still fixes a.

. . . . . .

Proof. **Step 1.** $1_G \in \mathrm{Stab}(a)$ since $1_G \cdot a = a$.

Step 2. If $g, h \in \mathrm{Stab}(a)$, then $h \cdot a = a$, so

$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a,$$

hence $gh \in \mathrm{Stab}(a)$.

Step 3. If $g \in \mathrm{Stab}(a)$, then $g \cdot a = a$. Apply g^{-1} to both sides:

$$a = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a,$$

so $g^{-1} \in \mathrm{Stab}(a)$.

Step 4. Thus $\mathrm{Stab}(a) \leq G$.

□

Proposition: Orbits Partition the Set.

The orbits of a group action of G on A form a partition of A.

. . . . . .

Intuition. Every element of A lies in exactly one orbit: two points are in the same orbit if one can be moved to the other by some group element.

. . . . . .

Proof. **Step 1.** For any $a \in A$, $a \in \mathrm{Orb}(a)$, so the union of all orbits covers A.
Step 2. If $\mathrm{Orb}(a) \cap \mathrm{Orb}(b) \neq \varnothing$, choose $x = g \cdot a = h \cdot b$.
Step 3. Then $b = h^{-1}g \cdot a$, so b lies in the orbit of a; hence $\mathrm{Orb}(b) \subseteq \mathrm{Orb}(a)$.
Step 4. By symmetry $\mathrm{Orb}(a) = \mathrm{Orb}(b)$. Therefore distinct orbits are disjoint.
Step 5. The orbits thus form a partition of A.

□

Proposition: Orbit–Stabilizer Theorem.

Let G act on a finite set A, and fix $a \in A$. Then

$$|G| = |\mathrm{Orb}(a)| \cdot |\mathrm{Stab}(a)|.$$

Intuition. Each group element sends a to some point of its orbit; all elements sending a to the same point differ by multiplication by stabilizer elements.

Proof. **Step 1.** Define $\theta : G \to \mathrm{Orb}(a)$ by $\theta(g) = g \cdot a$.

Step 2. The fibers of θ are $\{g \in G \mid g \cdot a = b\}$ for $b \in \mathrm{Orb}(a)$.

Step 3. If $g, h \in G$ satisfy $g \cdot a = h \cdot a$, then $h^{-1}g \cdot a = a$, so $h^{-1}g \in \mathrm{Stab}(a)$, i.e. $g \in h\,\mathrm{Stab}(a)$.

Step 4. Conversely, if $g \in h\,\mathrm{Stab}(a)$, then $g \cdot a = h \cdot a$. Hence fibers are precisely the cosets $h\,\mathrm{Stab}(a)$.

Step 5. Distinct orbits of a correspond to disjoint cosets. Thus $|\mathrm{Orb}(a)|$ equals the number of left cosets of $\mathrm{Stab}(a)$ in G.

Step 6. Therefore $|G| = |\mathrm{Orb}(a)|\,|\mathrm{Stab}(a)|$.

□

Definition: Transitive Action.

An action of G on A is *transitive* if there exists only one orbit; equivalently, for all $a, b \in A$ there is $g \in G$ such that $g \cdot a = b$.

Definition: Regular (Simply Transitive) Action.

A group action is called *regular* (or *simply transitive*) if it is both transitive and free. Equivalently, for each $a, b \in A$, there is exactly one $g \in G$ such that $g \cdot a = b$.

Proposition: Conjugation Action.

Every group G acts on itself by conjugation:

$$g \cdot a := gag^{-1}, \qquad g, a \in G.$$

Intuition. Conjugation measures how elements are twisted by one another. It defines orbits (conjugacy classes) and stabilizers (centralizers).

Proof. **Step 1.** Identity check: $(1) \cdot a = 1a1^{-1} = a$.

Step 2. Compatibility: for $g_1, g_2 \in G$,

$$g_1 \cdot (g_2 \cdot a) = g_1(g_2 a g_2^{-1})g_1^{-1} = (g_1 g_2)a(g_1 g_2)^{-1} = (g_1 g_2) \cdot a.$$

Step 3. Both action axioms hold; hence this defines a left group action.

□

Definition: Conjugacy Class and Centralizer.

For a group G acting on itself by conjugation:

- The *conjugacy class* of $g \in G$ is $\mathrm{Cl}(g) = \{xgx^{-1} \mid x \in G\}$.
- The *centralizer* of g is $C_G(g) = \{x \in G \mid xg = gx\}$.

Then $\mathrm{Stab}(g) = C_G(g)$ and $\mathrm{Orb}(g) = \mathrm{Cl}(g)$, so

$$|G| = |C_G(g)|\,|\mathrm{Cl}(g)|.$$

Proposition: Action by Right-Inverse Rule.

Let G be a group and set $A = G$. Define $g \cdot a := ag^{-1}$ for $g, a \in G$. Then this is a (left) group action of G on itself.

. . . . . .

Intuition. Although the operation seems "backwards," the inverse fixes the associativity condition:

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (ag_2^{-1}) = (ag_2^{-1})g_1^{-1} = a(g_2^{-1}g_1^{-1}) = a(g_1g_2)^{-1} = (g_1g_2) \cdot a.$$

. . . . . .

Proof. **Step 1.** Identity: $1 \cdot a = a1^{-1} = a$.

Step 2. Compatibility: for $g_1, g_2, a \in G$,

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (ag_2^{-1}) = (ag_2^{-1})g_1^{-1} = a(g_2^{-1}g_1^{-1}) = a(g_1g_2)^{-1} = (g_1g_2) \cdot a.$$

Step 3. Both axioms hold; this defines a left action.

□

Ch 1: Priority Problems

Overview. These are designed to test your memory on a few selected problems on the basics of Introduction to Groups as presented in Ch1 of Dummit and Foote.

List.

1. 1.1: 1, 2, 7, 18, 34
2. 1.2: 4
3. 1.3: 2, 3
4. External Problems: 1, 2, 3, 4
5. 1.6: 1, 2, 3, 4, 7, 18, 20
6. 1.7: 15

Exercise 1 (D&F §1.1, Ex. 1)**.** *Determine which of the following binary operations are associative:*

1. *on* $\mathbb{Z}$, $a * b = a - b$;
2. *on* $\mathbb{R}$, $a * b = a + b + ab$;
3. *on* $\mathbb{Q}$, $a * b = \dfrac{a+b}{5}$;
4. *on* $\mathbb{Z} \times \mathbb{Z}$, $(a, b) * (c, d) = (ad + bc,\, bd)$;
5. *on* $\mathbb{Q} \setminus \{0\}$, $a * b = \dfrac{a}{b}$.

. . . . . .

Intuition. Associativity survives when the operation is secretly "just usual multiplication/addition in disguise." It fails when scaling/ordering matters (e.g., division, subtraction, averaging).

. . . . . .

Proof. **Step 1.** Recall: $*$ is associative iff $(x * y) * z = x * (y * z)$ for all x, y, z in the set.

Step 2. Case (1) on $\mathbb{Z}$ with $a*b = a-b$: take $a = 1$, $b = 2$, $c = 3$. Then $(1*2)*3 = (-1)*3 = -4$ while $1 * (2 * 3) = 1 * (-1) = 2$; hence not associative.

Step 3. Case (2) on $\mathbb{R}$ with $a * b = a + b + ab$: for arbitrary a, b, c,

$$(a * b) * c = (a + b + ab) + c + (a + b + ab)c = a + b + ab + c + ac + bc + abc,$$

and

$$a * (b * c) = a + (b + c + bc) + a(b + c + bc) = a + b + c + bc + ab + ac + abc.$$

These match; hence associative.

Step 4. Case (3) on $\mathbb{Q}$ with $a * b = \frac{a+b}{5}$: choose $a = 5$, $b = 20$, $c = 15$. Then $(5 * 20) * 15 = 4$ but $5 * (20 * 15) = 12/5$; not associative.

Step 5. Case (4) on $\mathbb{Z} \times \mathbb{Z}$ with $(a, b) * (c, d) = (ad + bc, bd)$: for $(a, b), (c, d), (e, f)$,

$$((a, b) * (c, d)) * (e, f) = ((ad + bc)f + bde,\ bdf),$$

$$(a, b) * ((c, d) * (e, f)) = (adf + bcf + bde,\ bdf).$$

Components agree; hence associative.

Step 6. Case (5) on $\mathbb{Q} \setminus \{0\}$ with $a * b = \frac{a}{b}$: take $a = 125$, $b = 25$, $c = 5$. Then $(125 * 25) * 5 = 1$ but $125 * (25 * 5) = 25$; not associative.

Step 7. Conclusion: (2) and (4) are associative; (1), (3), (5) are not. □

Exercise 2 (D&F §1.1, Ex. 2)**.** *Decide which of the binary operations from Exercise 1 are commutative.*

1. *on* $\mathbb{Z}$, $a * b = a - b$;
2. *on* $\mathbb{R}$, $a * b = a + b + ab$;
3. *on* $\mathbb{Q}$, $a * b = \dfrac{a+b}{5}$;
4. *on* $\mathbb{Z} \times \mathbb{Z}$, $(a, b) * (c, d) = (ad + bc,\, bd)$;
5. *on* $\mathbb{Q} \setminus \{0\}$, $a * b = \dfrac{a}{b}$.

Intuition. Swapping inputs should not change the outcome. Rules built from symmetric expressions (like $a + b + ab$ or $\frac{a+b}{5}$) will likely commute; "directional" rules (subtraction, division) typically won't. For pairs, if each component is a symmetric polynomial in the swapped variables, commutativity should follow.

Proof. **Step 1.** Recall: $*$ is commutative iff $x * y = y * x$ for all inputs.

Step 2. Case (1) $\mathbb{Z}$, $a * b = a - b$: $1 * 2 = -1 \neq 1 = 2 * 1$; not commutative.

Step 3. Case (2) $\mathbb{R}$, $a * b = a + b + ab$: $a * b = a + b + ab = b + a + ba = b * a$; commutative.

Step 4. Case (3) $\mathbb{Q}$, $a * b = \dfrac{a+b}{5}$: $b * a = \dfrac{b+a}{5} = \dfrac{a+b}{5} = a * b$; commutative.

Step 5. Case (4) $\mathbb{Z} \times \mathbb{Z}$, $(a, b) * (c, d) = (ad + bc, bd)$:

$$(a, b) * (c, d) = (ad + bc, bd) = (cb + da, db) = (c, d) * (a, b);$$

commutative.

Step 6. Case (5) $\mathbb{Q} \setminus \{0\}$, $a * b = \dfrac{a}{b}$: $1 * 2 = \frac{1}{2} \neq 2 = 2 * 1$; not commutative.

Step 7. Conclusion: (2), (3), (4) commute; (1), (5) do not. □

Exercise 3 (D&F §1.1, Ex. 7)**.** *Let* $G = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ *and for* $x, y \in G$ *let* $x * y$ *be the fractional part of* $x + y$ *(i.e.* $x * y = x + y - \lfloor x + y \rfloor$ *where* $\lfloor a \rfloor$ *is the greatest integer* $\leq a$*). Prove that* $*$ *is a well-defined binary operation on* G *and that* $(G, *)$ *is an abelian group.*

Intuition. "Add mod 1": add in $\mathbb{R}$, then wrap once if you crossed 1. Since ordinary addition is associative and commutative, and wrapping is done by subtracting 0 or 1 exactly, we expect a clean abelian group with identity 0 and inverse $1 - x$ (or 0 for $x = 0$).

Proof. **Step 1.** (Closure) For $x, y \in [0, 1)$ we have $0 \le x + y < 2$. If $x + y < 1$, then $x * y = x + y \in [0, 1)$. If $1 \le x + y < 2$, then $x * y = x + y - 1 \in [0, 1)$.

Step 2. (Associativity) We show $(x * y) * z = x * (y * z)$ for all $x, y, z \in G$ by a case split on whether $x + y$ and $y + z$ are at least 1.

Step 2.1. *Case A:* $x + y < 1$ *and* $y + z < 1$.

Then $\lfloor x + y \rfloor = 0$ and $\lfloor y + z \rfloor = 0$.

Compute $(x * y) * z$:

$$x * y = (x + y) - 0 = x + y, \qquad (x * y) * z = (x + y) + z - \lfloor x + y + z \rfloor.$$

Compute $x * (y * z)$:

$$y * z = (y + z) - 0 = y + z, \qquad x * (y * z) = x + (y + z) - \lfloor x + y + z \rfloor.$$

Conclusion in Case A: both sides equal $x + y + z - \lfloor x + y + z \rfloor$.

Step 2.2. *Case B:* $x + y < 1$ *and* $y + z \ge 1$.

Then $\lfloor x + y \rfloor = 0$ and $\lfloor y + z \rfloor = 1$.

Compute $(x * y) * z$:

$$x * y = x + y, \qquad (x * y) * z = (x + y) + z - \lfloor x + y + z \rfloor.$$

Compute $x * (y * z)$:

$$y * z = (y + z) - 1, \qquad x * (y * z) = x + (y + z - 1) - \lfloor x + y + z - 1 \rfloor.$$

Use $\lfloor t - 1 \rfloor = \lfloor t \rfloor - 1$ to get

$$x * (y * z) = x + y + z - 1 - \big(\lfloor x + y + z \rfloor - 1\big) = x + y + z - \lfloor x + y + z \rfloor.$$

Conclusion in Case B: $(x * y) * z = x * (y * z)$.

Step 2.3. *Case C:* $x + y \ge 1$ *and* $y + z < 1$.

Then $\lfloor x + y \rfloor = 1$ and $\lfloor y + z \rfloor = 0$.

Compute $(x * y) * z$:

$$x * y = (x + y) - 1, \qquad (x * y) * z = (x + y - 1) + z - \lfloor x + y + z - 1 \rfloor.$$

Again $\lfloor t - 1 \rfloor = \lfloor t \rfloor - 1$ gives

$$(x * y) * z = x + y + z - 1 - \big(\lfloor x + y + z \rfloor - 1\big) = x + y + z - \lfloor x + y + z \rfloor.$$

Compute $x * (y * z)$:

$$y * z = y + z, \qquad x * (y * z) = x + (y + z) - \lfloor x + y + z \rfloor.$$

Conclusion in Case C: $(x * y) * z = x * (y * z)$.

Step 2.4. *Case D:* $x + y \geq 1$ *and* $y + z \geq 1$.

Then $\lfloor x + y \rfloor = 1$ and $\lfloor y + z \rfloor = 1$.

Compute $(x * y) * z$:

$$x * y = (x + y) - 1, \qquad (x * y) * z = (x + y - 1) + z - \lfloor x + y + z - 1 \rfloor.$$

Using $\lfloor t - 1 \rfloor = \lfloor t \rfloor - 1$,

$$(x * y) * z = x + y + z - 1 - \big(\lfloor x + y + z \rfloor - 1\big) = x + y + z - \lfloor x + y + z \rfloor.$$

Compute $x * (y * z)$:

$$y * z = (y + z) - 1, \qquad x * (y * z) = x + (y + z - 1) - \lfloor x + y + z - 1 \rfloor = x + y + z - \lfloor x + y + z \rfloor.$$

Conclusion in Case D: $(x * y) * z = x * (y * z)$.

Step 2.5. All four cases yield the same expression $x + y + z - \lfloor x + y + z \rfloor$ on both sides; hence $*$ is associative.

Step 3. (Identity) With $e = 0$, $\lfloor x \rfloor = 0$ for $x \in [0, 1)$ gives $x * 0 = x$ and $0 * x = x$.

Step 4. (Inverses) For $x = 0$, inverse is 0. For $x \neq 0$, $y = 1 - x \in (0, 1)$ and $x * y = 1 - \lfloor 1 \rfloor = 0 = y * x$.

Step 5. (Commutativity) $x * y = x + y - \lfloor x + y \rfloor = y + x - \lfloor y + x \rfloor = y * x$.

Step 6. Conclusion: $(G, *)$ is an abelian group. □

Exercise 4 (D&F §1.1, Ex. 18)**.** *Let x and y be elements of a group G. Prove that*

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

Intuition. "$xy = yx$" says x and y commute. Conjugating x by y measures the failure to commute: if $y^{-1}xy = x$, conjugation does nothing, so they commute. Packing the same idea into a single element, the *commutator* $[x, y] = x^{-1}y^{-1}xy$ equals 1 exactly when the "failure to commute" vanishes.

Proof. **Step 1.** ($xy = yx \Rightarrow y^{-1}xy = x$) From $xy = yx$, left-multiply by y^{-1} to get $y^{-1}xy = x$.

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

Step 3. ($x^{-1}y^{-1}xy = 1 \Rightarrow xy = yx$) Left-multiply by x to get $y^{-1}xy = x$, then left-multiply by y to obtain $xy = yx$.

Step 4. Conclusion: the three statements are equivalent. □

Exercise 5 (D&F §1.1, Ex. 34)**.** *If x is an element of infinite order in G, prove that the elements x^n, $n \in \mathbb{Z}$, are all distinct.*

Intuition. "Infinite order" means *no* positive power of x equals 1. If two powers coincide, say $x^m = x^n$ with $m \neq n$, cancel to get $x^{m-n} = 1$ with $m - n \neq 0$—contradicting the definition.

Proof. **Step 1.** Assume $|x| = \infty$ and suppose $x^m = x^n$.
Step 2. WLOG $n \leq m$. Right-multiply by x^{-n} to obtain $x^{m-n} = 1$.
Step 3. Since $|x| = \infty$, no positive power equals 1, hence $m - n = 0$ and $m = n$.
Step 4. Conclusion: the powers $\{x^n : n \in \mathbb{Z}\}$ are all distinct. □

Exercise 6 (D&F §1.2, Ex. 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}.*

Intuition. By D&F §1.1, Ex. 33, when $|r| = n = 2k$ we have $r^k = r^{-k}$, so r^k is an involution. Then r^k clearly commutes with all rotations, and $r^k s = sr^{-k} = sr^k$ shows it commutes with s. A reflection cannot be central (it fails to commute with r), and a central rotation must satisfy $r^t = r^{-t}$, forcing $t \equiv 0$ or $t \equiv k$.

Proof. **Step 1.** (Order) With $n = 2k$, $z = r^k$ satisfies $z^2 = r^{2k} = 1$ and $r^k = r^{-k}$, so $|z| = 2$.

Step 2. (Commutes with rotations) For any ℓ, $zr^\ell = r^{k+\ell} = r^{\ell+k} = r^\ell z$.

Step 3. (Commutes with s) Using $r^m s = sr^{-m}$ and $r^k = r^{-k}$, we have $zs = r^k s = sr^{-k} = sr^k = sz$.

Step 4. (No reflection is central for $n \geq 4$) If $x = sr^t$ were central, $rx = xr$ would force $sr^{t-1} = sr^{t+1}$, hence $r^2 = 1$, contradicting $n \geq 4$.

Step 5. (Only central rotations) If r^t is central, then $r^t s = sr^t$ gives $sr^{-t} = sr^t$, so $r^{2t} = 1$. With $n = 2k$ this yields $t \equiv 0$ or $t \equiv k \pmod{n}$.

Step 6. Conclusion: the unique nonidentity central element is $z = r^k$. □

Exercise 7 (D&F §1.3, Ex. 2)**.** *Let $\sigma, \tau \in S_{15}$ be defined by*

$$\sigma: \begin{array}{lllll} 1 \mapsto 13, & 2 \mapsto 2, & 3 \mapsto 15, & 4 \mapsto 14, & 5 \mapsto 10, \\ 6 \mapsto 6, & 7 \mapsto 12, & 8 \mapsto 3, & 9 \mapsto 4, & 10 \mapsto 1, \\ 11 \mapsto 7, & 12 \mapsto 9, & 13 \mapsto 5, & 14 \mapsto 11, & 15 \mapsto 8 \end{array}$$

$$\tau: \begin{array}{lllll} 1 \mapsto 14, & 2 \mapsto 9, & 3 \mapsto 10, & 4 \mapsto 2, & 5 \mapsto 12, \\ 6 \mapsto 6, & 7 \mapsto 5, & 8 \mapsto 11, & 9 \mapsto 15, & 10 \mapsto 3, \\ 11 \mapsto 8, & 12 \mapsto 7, & 13 \mapsto 4, & 14 \mapsto 1, & 15 \mapsto 13 \end{array}$$

Find the cycle decompositions of σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, and $\tau^2\sigma$.

Intuition. Build each permutation by following orbits until they close. For products, apply the rightmost map first. Disjoint cycles commute, so once an element's cycle is recorded, skip it.

Proof. **Step 1.** Compute σ explicitly by tracing images.
Start at 1: $1 \mapsto 13 \mapsto 5 \mapsto 10 \mapsto 1$ gives (1 13 5 10).
Start at 3: $3 \mapsto 15 \mapsto 8 \mapsto 3$ gives (3 15 8).
Start at 4: $4 \mapsto 14 \mapsto 11 \mapsto 7 \mapsto 12 \mapsto 9 \mapsto 4$ gives (4 14 11 7 12 9).
Elements 2 and 6 satisfy $2 \mapsto 2$, $6 \mapsto 6$ (fixed).
Therefore

$$\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9), \quad \text{with } 2, 6 \text{ fixed.}$$

Step 2. Compute τ explicitly by tracing images.
Start at 1: $1 \mapsto 14 \mapsto 1$ gives (1 14).
Start at 3: $3 \mapsto 10 \mapsto 3$ gives (3 10).
Start at 8: $8 \mapsto 11 \mapsto 8$ gives (8 11).
Start at 5: $5 \mapsto 12 \mapsto 7 \mapsto 5$ gives (5 12 7).
Start at 2: $2 \mapsto 9 \mapsto 15 \mapsto 13 \mapsto 4 \mapsto 2$ gives (2 9 15 13 4).
Element 6 is fixed.
Therefore

$$\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11), \quad \text{with } 6 \text{ fixed.}$$

Step 3. Compute σ^2 by squaring each disjoint cycle (and show the images).
For (1 13 5 10):

$$1 \mapsto 5, \quad 13 \mapsto 10, \quad 5 \mapsto 1, \quad 10 \mapsto 13 \ \Rightarrow\ (1\ 5)(13\ 10).$$

For (3 15 8):

$$3 \mapsto 8, \quad 15 \mapsto 3, \quad 8 \mapsto 15 \ \Rightarrow\ (3\ 8\ 15).$$

For (4 14 11 7 12 9):

$$4 \mapsto 11 \mapsto 12 \mapsto 4 \ \Rightarrow\ (4\ 11\ 12), \qquad 7 \mapsto 9 \mapsto 14 \mapsto 7 \ \Rightarrow\ (7\ 9\ 14).$$

Thus

$$\sigma^2 = (1\ 5)(13\ 10)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14).$$

Step 4. Compute $\sigma\tau$ (apply τ first, then σ), tracing each orbit.
For 1:

$$\tau(1) = 14,\ \sigma(14) = 11 \Rightarrow 1 \mapsto 11; \quad \tau(11) = 8,\ \sigma(8) = 3 \Rightarrow 11 \mapsto 3; \quad \tau(3) = 10,\ \sigma(10) = 1 \Rightarrow 3 \mapsto 1.$$

Hence (1 11 3).
For 2:

$$\tau(2) = 9,\ \sigma(9) = 4 \Rightarrow 2 \mapsto 4; \quad \tau(4) = 2,\ \sigma(2) = 2 \Rightarrow 4 \mapsto 2.$$

Hence (2 4).

For 5:

$$\begin{aligned}\tau(5) = 12,\ \sigma(12) = 9 &\Rightarrow 5 \mapsto 9;\\ \tau(9) = 15,\ \sigma(15) = 8 &\Rightarrow 9 \mapsto 8;\\ \tau(8) = 11,\ \sigma(11) = 7 &\Rightarrow 8 \mapsto 7;\\ \tau(7) = 5,\ \sigma(5) = 10 &\Rightarrow 7 \mapsto 10;\\ \tau(10) = 3,\ \sigma(3) = 15 &\Rightarrow 10 \mapsto 15;\\ \tau(15) = 13,\ \sigma(13) = 5 &\Rightarrow 15 \mapsto 5.\end{aligned}$$

Hence (5 9 8 7 10 15).

For 13:

$$\tau(13) = 4,\ \sigma(4) = 14 \Rightarrow 13 \mapsto 14; \quad \tau(14) = 1,\ \sigma(1) = 13 \Rightarrow 14 \mapsto 13.$$

Hence (13 14).

Elements 6 and (already used) others are now exhausted; indeed $\tau(6) = 6$, $\sigma(6) = 6$ (fixed).

Therefore

$$\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14).$$

Step 5. Compute $\tau\sigma$ (apply σ first, then τ), tracing each orbit.

For 1:

$$\sigma(1) = 13,\ \tau(13) = 4 \Rightarrow 1 \mapsto 4; \quad \sigma(4) = 14,\ \tau(14) = 1 \Rightarrow 4 \mapsto 1.$$

Hence (1 4).

For 2:

$$\sigma(2) = 2,\ \tau(2) = 9 \Rightarrow 2 \mapsto 9; \quad \sigma(9) = 4,\ \tau(4) = 2 \Rightarrow 9 \mapsto 2.$$

Hence (2 9).

For 3:

$$\begin{aligned}\sigma(3) = 15,\ \tau(15) = 13 &\Rightarrow 3 \mapsto 13;\\ \sigma(13) = 5,\ \tau(5) = 12 &\Rightarrow 13 \mapsto 12;\\ \sigma(12) = 9,\ \tau(9) = 15 &\Rightarrow 12 \mapsto 15;\\ \sigma(15) = 8,\ \tau(8) = 11 &\Rightarrow 15 \mapsto 11;\\ \sigma(11) = 7,\ \tau(7) = 5 &\Rightarrow 11 \mapsto 5;\\ \sigma(5) = 10,\ \tau(10) = 3 &\Rightarrow 5 \mapsto 3.\end{aligned}$$

Hence (3 13 12 15 11 5).

For 8:

$$\sigma(8) = 3,\ \tau(3) = 10 \Rightarrow 8 \mapsto 10; \quad \sigma(10) = 1,\ \tau(1) = 14 \Rightarrow 10 \mapsto 14; \quad \sigma(14) = 11,\ \tau(11) = 8 \Rightarrow 14 \mapsto 8.$$

Hence (8 10 14).

Element 6 is fixed since $\sigma(6) = 6$ and $\tau(6) = 6$.

Therefore

$$\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14).$$

Step 6. Compute $\tau^2\sigma$ by tracing $x \mapsto \tau(\tau(\sigma(x)))$.

For 1:

$$\sigma(1) = 13,\ \tau(13) = 4,\ \tau(4) = 2 \Rightarrow 1 \mapsto 2.$$

For 2:

$$\sigma(2) = 2,\ \tau(2) = 9,\ \tau(9) = 15 \Rightarrow 2 \mapsto 15.$$

For 15:

$$\sigma(15) = 8,\ \tau(8) = 11,\ \tau(11) = 8 \Rightarrow 15 \mapsto 8.$$

For 8:

$$\sigma(8) = 3,\ \tau(3) = 10,\ \tau(10) = 3 \Rightarrow 8 \mapsto 3.$$

For 3:

$$\sigma(3) = 15,\ \tau(15) = 13,\ \tau(13) = 4 \Rightarrow 3 \mapsto 4.$$

For 4:

$$\sigma(4) = 14,\ \tau(14) = 1,\ \tau(1) = 14 \Rightarrow 4 \mapsto 14.$$

For 14:

$$\sigma(14) = 11,\ \tau(11) = 8,\ \tau(8) = 11 \Rightarrow 14 \mapsto 11.$$

For 11:

$$\sigma(11) = 7,\ \tau(7) = 5,\ \tau(5) = 12 \Rightarrow 11 \mapsto 12.$$

For 12:

$$\sigma(12) = 9,\ \tau(9) = 15,\ \tau(15) = 13 \Rightarrow 12 \mapsto 13.$$

For 13:

$$\sigma(13) = 5,\ \tau(5) = 12,\ \tau(12) = 7 \Rightarrow 13 \mapsto 7.$$

For 7:

$$\sigma(7) = 12,\ \tau(12) = 7,\ \tau(7) = 5 \Rightarrow 7 \mapsto 5.$$

For 5:

$$\sigma(5) = 10,\ \tau(10) = 3,\ \tau(3) = 10 \Rightarrow 5 \mapsto 10.$$

For 10:

$$\sigma(10) = 1,\ \tau(1) = 14,\ \tau(14) = 1 \Rightarrow 10 \mapsto 1.$$

Thus we have the 13-cycle

$$(1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10).$$

Check the remaining points:
For 6: $\sigma(6) = 6,\ \tau(6) = 6,\ \tau(6) = 6$ so 6 is fixed.
For 9: $\sigma(9) = 4,\ \tau(4) = 2,\ \tau(2) = 9$ so 9 is fixed.
Therefore

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

with 6 and 9 fixed.

Step 7. Conclusion: all requested decompositions are as listed. □

Exercise 8 (D&F §1.3, Ex. 3)**.** *For each permutation whose cycle decomposition was computed in Exercises 1–2, determine its order.*

. . . . . .

Intuition. If a permutation is a product of disjoint cycles, its order is the least common multiple of the cycle lengths. A single k-cycle has order k.

. . . . . .

Proof. **Step 1.** Use the fact: $|\sigma| = \operatorname{lcm}\big(\text{cycle lengths of } \sigma\big)$.

Step 2. Set A (from Ex. 1): from the given decompositions,

$$|\sigma| = \operatorname{lcm}(3,2) = 6, \quad |\tau| = 2, \quad |\sigma^2| = 3, \quad |\sigma\tau| = 4, \quad |\tau\sigma| = 4, \quad |\tau^2\sigma| = 6.$$

Step 3. Set B (from Ex. 2): using the cycles,

$$\begin{aligned} |\sigma| &= \operatorname{lcm}(4,3,6) = 12, \quad |\tau| = \operatorname{lcm}(2,5,2,3,2) = 30, \\ |\sigma^2| &= \operatorname{lcm}(2,3,3,3,2) = 6, \quad |\sigma\tau| = \operatorname{lcm}(3,2,6,2) = 6, \\ |\tau\sigma| &= \operatorname{lcm}(2,2,6,3) = 6, \quad |\tau^2\sigma| = 13. \end{aligned}$$

Step 4. Conclusion: the orders are as displayed above. □

Exercise 9 (D&F §1.6, Ex. 1)**.** *Let $\varphi : G \to H$ be a homomorphism.*

(a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}_{>0}$.

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

Intuition. A homomorphism preserves products, so it preserves *any* finite product of the same element—i.e. positive powers—by induction. Then use $\varphi(x^{-1}) = \varphi(x)^{-1}$ to extend from positive to all integer exponents.

Proof. **Step 1.** (a) Base case $n = 1$: $\varphi(x^1) = \varphi(x) = \varphi(x)^1$.
Step 2. (a) Inductive step: if $\varphi(x^n) = \varphi(x)^n$, then $\varphi(x^{n+1}) = \varphi(x)\varphi(x^n) = \varphi(x)^{n+1}$.
Step 3. (a) By induction, $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}_{>0}$.
Step 4. (b) Since $\varphi(1_G) = 1_H$, from $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = 1_H$ we obtain $\varphi(x^{-1}) = \varphi(x)^{-1}$.
Step 5. (b) For $n > 0$, $\varphi(x^{-n}) = \varphi((x^n)^{-1}) = \varphi(x^n)^{-1} = \varphi(x)^{-n}$.
Step 6. Conclusion: $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. □

Exercise 10 (D&F §1.6, Ex. 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 $n \in \mathbb{Z}_{>0}$. Is the result true if φ is only assumed to be a homomorphism?*

Intuition. An isomorphism is a bijective homomorphism. Homomorphisms respect powers, and bijectivity lets us pull back equations from H to G. That forces the order to match exactly. Without bijectivity (mere homomorphism), orders can collapse (e.g. map everything to the identity).

Proof. **Step 1.** If $|x| = n < \infty$, then $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$, hence $|\varphi(x)| \leq n$.

Step 2. If $|\varphi(x)| = k$, then $\varphi(x)^k = e_H$ gives $\varphi(x^k) = e_H$, so by injectivity $x^k = e_G$ and $n \leq k$.

Step 3. Therefore $|\varphi(x)| = n$ when $|x| = n < \infty$.

Step 4. If $|x| = \infty$ and $|\varphi(x)| < \infty$, then $\varphi(x)^m = e_H$ for some $m > 0$ would imply $x^m = e_G$, a contradiction.

Step 5. Hence $|x| = \infty \Rightarrow |\varphi(x)| = \infty$.

Step 6. Since φ is bijective and preserves order elementwise, it bijects elements of order n; counts match.

Step 7. For a mere homomorphism, the conclusion fails (e.g. the trivial homomorphism collapses all orders to 1).

Step 8. Conclusion: isomorphisms preserve orders and counts; homomorphisms need not. □

Exercise 11 (D&F §1.6, Ex. 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?*

Intuition. Isomorphisms preserve *all* group-theoretic structure; conjugating by φ transports products exactly, so commutativity is carried back and forth.
For a general homomorphism, surjectivity lets every element of H be the image of something in G; then commutativity in G forces commutativity in H. Injectivity alone is not enough.

Proof. **Step 1.** If G is abelian and φ is an isomorphism, then for $x = \varphi(a)$, $y = \varphi(b)$ we have $xy = \varphi(ab) = \varphi(ba) = yx$, so H is abelian.

Step 2. If H is abelian, apply Step 1 to $\varphi^{-1} : H \to G$ to deduce G is abelian.

Step 3. If φ is surjective and G abelian, then for any $x, y \in H$ choose $a, b \in G$ with $\varphi(a) = x$, $\varphi(b) = y$; thus $xy = \varphi(ab) = \varphi(ba) = yx$.

Step 4. Injectivity alone cannot force H to be abelian: abelian groups embed in nonabelian groups.

Step 5. Conclusion: under isomorphism, G abelian $\Leftrightarrow$ H abelian; for homomorphisms, surjectivity suffices. □

Exercise 12 (D&F §1.6, Ex. 4)**.** *Prove that the multiplicative groups* $\mathbb{R} - \{0\}$ *and* $\mathbb{C} - \{0\}$ *are not isomorphic.*

Intuition. Isomorphisms preserve the multiset of element orders. In $\mathbb{C}^\times$ there are elements of order 4 (e.g. i), but in $\mathbb{R}^\times$ the only elements with finite order are 1 (order 1) and -1 (order 2). This mismatch blocks any isomorphism.

Proof. **Step 1.** In $\mathbb{R}^\times$, finite-order elements are 1 (order 1) and -1 (order 2).
Step 2. In $\mathbb{C}^\times$, i has order 4.
Step 3. Since isomorphisms preserve orders, the groups cannot be isomorphic.
Step 4. Conclusion: $\mathbb{R}^\times \ncong \mathbb{C}^\times$. □

Exercise 13 (D&F §1.6, Ex. 7)**.** *Prove that D_8 and Q_8 are not isomorphic.*

Intuition. Isomorphisms preserve the multiset of element orders. In Q_8 the *only* element of order 2 is -1. In D_8 there are many elements of order 2 (the reflections, and also r^2). This mismatch rules out an isomorphism.

Proof. **Step 1.** In D_8, elements of order 2 are r^2, s, sr, sr^2, sr^3 (five total).
Step 2. In Q_8, the only element of order 2 is -1.
Step 3. Isomorphic groups must have equal counts of elements of each order; these differ.
Step 4. Conclusion: $D_8 \not\cong Q_8$. □

Exercise 14 (D&F §1.6, Ex. 18)**.** *Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.*

Intuition. A map is a homomorphism iff it respects products. For $g \mapsto g^2$, this means $(ab)^2 = a^2b^2$ for all a, b. But $(ab)^2 = abab$, so the condition becomes $abab = aabb$, which forces $ab = ba$. Conversely, if G is abelian then $(ab)^2 = a^2b^2$ holds automatically.

Proof. **Step 1.** ($\Rightarrow$) If $\psi(g) = g^2$ is a homomorphism, then $(ab)^2 = \psi(ab) = \psi(a)\psi(b) = a^2b^2$, hence $abab = aabb$ and $ab = ba$.

Step 2. ($\Leftarrow$) If G is abelian, then $(ab)^2 = abab = a^2b^2 = \psi(a)\psi(b)$, so ψ is a homomorphism.

Step 3. Conclusion: ψ is a homomorphism iff G is abelian. □

Exercise 15 (D&F §1.6, Ex. 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).*

Intuition. Automorphisms are the "symmetries" of G. Composition of bijective homomorphisms is again a bijective homomorphism; the identity map is an automorphism; inverses of automorphisms are automorphisms. Those are exactly the group axioms.

Proof. **Step 1.** Closure: the composition of bijective homomorphisms is a bijective homomorphism.

Step 2. Associativity: function composition is associative.

Step 3. Identity: id_G is a bijective homomorphism.

Step 4. Inverses: if φ is a bijective homomorphism, then φ^{-1} is also a homomorphism (since $\varphi(\varphi^{-1}(xy)) = xy = \varphi(\varphi^{-1}(x)\varphi^{-1}(y))$).

Step 5. Conclusion: $\mathrm{Aut}(G)$ is a group under composition. □

Exercise 16 (D&F §1.7, Ex. 15)**.** *Let G be any group and let $A = G$. Show that the maps*

$$g \cdot a \;:=\; a\, g^{-1} \qquad (g, a \in G)$$

satisfy the axioms of a (left) group action of G on itself.

Intuition. A left action needs $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$. With the rule $g \cdot a = a\, g^{-1}$ we get

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (a\, g_2^{-1}) = (a\, g_2^{-1})\, g_1^{-1} = a\, (g_2^{-1} g_1^{-1}) = a\, (g_1 g_2)^{-1} = (g_1 g_2) \cdot a.$$

So the "order reversal" from inverses is exactly what fixes the associativity constraint that failed in Exercise 14.

Proof. **Step 1.** Identity axiom: $1 \cdot a = a\, 1^{-1} = a$.

Step 2. Compatibility axiom: $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (a g_2^{-1}) = (a g_2^{-1}) g_1^{-1} = a(g_2^{-1} g_1^{-1}) = a(g_1 g_2)^{-1} = (g_1 g_2) \cdot a$.

Step 3. Conclusion: $(g, a) \mapsto a g^{-1}$ defines a left action of G on itself. □

Exercise 17. *(1) Show that if a and b commute in 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 such that $(ab)^n \neq a^n b^n$ for some positive integer n.*

Intuition. If a and b commute, you can slide all a's past all b's in any product. Induct for $n > 0$, and for $n < 0$ apply the result to a^{-1}, b^{-1} (which also commute).

Proof. **Step 1.** For $n \geq 0$, induction gives $(ab)^{n+1} = (ab)^n(ab) = a^n b^n ab = a^{n+1}b^{n+1}$ if $ab = ba$.

Step 2. For $n < 0$, write $n = -m$ and use $(ab)^{-1} = b^{-1}a^{-1}$ to get $(ab)^n = (b^{-1}a^{-1})^m = a^{-m}b^{-m} = a^n b^n$.

Step 3. Counterexample: in D_8 with $a = r$, $b = s$, $(ab)^2 = 1$ while $a^2b^2 = r^2 \neq 1$.

Step 4. Conclusion: $(ab)^n = a^n b^n$ for all n iff a and b commute. □

Exercise 18. *(2) Prove that disjoint cycles commute. That is, if $\sigma \in S_n$ has cycle representation $(a_1\ a_2\ \dots\ a_k)$ and $\tau \in S_n$ has cycle representation $(b_1\ b_2\ \dots\ b_m)$ with $\{a_i\}_{i=1}^k$ and $\{b_j\}_{j=1}^m$ disjoint, then $\sigma \circ \tau = \tau \circ \sigma$. (Composition is applied right-to-left.)*

Intuition. Each cycle moves only the points in its own support. If the supports are disjoint, then each permutation fixes the points moved by the other, so applying them in either order gives the same result on every element.

Proof. **Step 1.** If x lies in the support of σ but not τ, then τ fixes x and $(\sigma\circ\tau)(x) = \sigma(x) = (\tau\circ\sigma)(x)$.
Step 2. If x lies in the support of τ but not σ, the same symmetry gives equality.
Step 3. If x lies in neither support, both permutations fix x.
Step 4. Therefore $(\sigma \circ \tau)(x) = (\tau \circ \sigma)(x)$ for all x, so σ and τ commute. □

Exercise 19. *(3) Prove that the order of permutation $\sigma \in S_n$ is the least common multiple of the lengths of the cycles in its cycle decomposition. (Yes, I said this was true in class, but now I want you to prove it.)*

Intuition. A power of σ is the identity exactly when every cycle in its disjoint decomposition has cycled back to its start. That requires the exponent to be a multiple of each cycle's length. The minimal such exponent is the least common multiple.

Proof. **Step 1.** A t-cycle has order t.

Step 2. If $\sigma = \tau_1 \cdots \tau_k$ are disjoint cycles of lengths t_i, then $\sigma^m = \tau_1^m \cdots \tau_k^m$.

Step 3. $\sigma^m = 1$ iff each $\tau_i^m = 1$ iff $t_i \mid m$ for all i.

Step 4. The least such m is $\operatorname{lcm}(t_1, \ldots, t_k)$, which equals $|\sigma|$. □

Exercise 20. *(4) Show for all $\sigma \in S_n$, that $\sigma(1\ 2\ 3 \dots\ k) \circ \sigma^{-1} = (\sigma(1)\ \sigma(2)\ \sigma(3) \dots\ \sigma(k))$. What more general statement should be true? (No need to prove the more general statement)*

Intuition. Conjugation $\sigma(\,\cdot\,)\sigma^{-1}$ "relabels" each symbol by σ. So a cycle $(1\ 2\ \dots\ k)$ becomes the cycle that carries $\sigma(1) \mapsto \sigma(2) \mapsto \cdots \mapsto \sigma(k) \mapsto \sigma(1)$.

Proof. **Step 1.** Let $c = (1\ 2\ \dots\ k)$. For $x = \sigma(i)$ with $1 \le i < k$, we have $(\sigma c \sigma^{-1})(x) = \sigma(i+1)$.
Step 2. For $x = \sigma(k)$, $(\sigma c \sigma^{-1})(x) = \sigma(1)$.
Step 3. For $x \notin \{\sigma(1), \dots, \sigma(k)\}$, both permutations fix x.
Step 4. Therefore $\sigma c \sigma^{-1} = (\sigma(1)\ \sigma(2)\ \dots\ \sigma(k))$. □

More general statement. For any $\tau \in S_n$, the conjugate $\sigma\tau\sigma^{-1}$ is obtained by applying σ to every symbol in the disjoint-cycle decomposition of τ. Equivalently, conjugation by σ is a relabeling of points: it sends the cycle $(a_1\ a_2\ \dots\ a_t)$ to $(\sigma(a_1)\ \sigma(a_2)\ \dots\ \sigma(a_t))$ and preserves disjointness of cycles.