Chapter 1 – Introduction to Group Theory

Harley Caham Combest

Fa2025 MATH5353 Lecture Notes – Mk1

Exercises from Algebra (3rd Edition) by Dummit & Foote
Solutions largely from Greg Kikola

. . . .

1.1: Basic Axioms and Examples

. . . .

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. We recall that an operation $*$ is associative if

$$(x * y) * z \;=\; x * (y * z)$$

for all x, y, z in the set. Let us test each case carefully.

. . . .

(1) $\boldsymbol{a * b = a - b}$ **on** $\mathbb{Z}$**.** Take $a = 1$, $b = 2$, $c = 3$. Then

$$(1 * 2) * 3 = (1 - 2) * 3 = (-1) * 3 = -1 - 3 = -4,$$

while

$$1 * (2 * 3) = 1 * (2 - 3) = 1 * (-1) = 1 - (-1) = 2.$$

Since $-4 \neq 2$, associativity fails.

. . . .

(2) $\boldsymbol{a * b = a + b + ab}$ on $\mathbb{R}$. Let $a, b, c \in \mathbb{R}$. Compute the left side:

$$(a * b) * c = (a + b + ab) * c.$$

By definition of $*$,

$$(a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c.$$

Expanding gives

$$= a + b + ab + c + ac + bc + abc.$$

Now compute the right side:

$$a * (b * c) = a * (b + c + bc).$$

Again by definition,

$$a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc).$$

Expand the terms:

$$= a + b + c + bc + ab + ac + abc.$$

Comparing the two expansions, we see they are identical:

$$a + b + ab + c + ac + bc + abc \;=\; a + b + c + bc + ab + ac + abc.$$

Thus $(a * b) * c = a * (b * c)$ for all $a, b, c \in \mathbb{R}$, so this operation is associative.

. . . .

(3) $\boldsymbol{a * b = \frac{a+b}{5}}$ on $\mathbb{Q}$. Test with $a = 5$, $b = 20$, $c = 15$. Then

$$(5 * 20) * 15 = \left(\tfrac{5+20}{5}\right) * 15 = 5 * 15 = \tfrac{5+15}{5} = \tfrac{20}{5} = 4,$$

while

$$5 * (20 * 15) = 5 * \left(\tfrac{20+15}{5}\right) = 5 * 7 = \tfrac{5+7}{5} = \tfrac{12}{5}.$$

Since $4 \neq 12/5$, associativity fails.

. . . .

(4) $(a, b) * (c, d) = (ad + bc,\ bd)$ on $\mathbb{Z} \times \mathbb{Z}$. Take three arbitrary pairs $(a, b), (c, d), (e, f)$. Compute the left side:

$$\big((a, b) * (c, d)\big) * (e, f) = (ad + bc,\ bd) * (e, f).$$

Applying the definition again,

$$= ((ad + bc)f + bde,\ bdf).$$

Now the right side:

$$(a, b) * \big((c, d) * (e, f)\big) = (a, b) * (cf + de,\ df).$$

By definition,

$$= (a(df) + b(cf + de),\ bdf).$$

Expand the first component:

$$a(df) + b(cf + de) = adf + bcf + bde.$$

Compare with the left side's first component:

$$(ad + bc)f + bde = adf + bcf + bde.$$

They match exactly, and the second components were both bdf. Hence associativity holds.

. . . .

(5) $a * b = \frac{a}{b}$ on $\mathbb{Q} \setminus \{0\}$. Check with $a = 125$, $b = 25$, $c = 5$. Then

$$(125 * 25) * 5 = \left(\tfrac{125}{25}\right) * 5 = 5 * 5 = \tfrac{5}{5} = 1,$$

but

$$125 * (25 * 5) = 125 * \left(\tfrac{25}{5}\right) = 125 * 5 = \tfrac{125}{5} = 25.$$

Since $1 \neq 25$, associativity fails.

. . . .

Conclusion. Operations (2) and (4) are associative; the others are not.

. . . .

□

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

. . . .

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. We recall that an operation $*$ is commutative if

$$x * y \;=\; y * x$$

for all inputs. We check each from Exercise 1.

. . . .

(1) On $\mathbb{Z}$, $a * b = a - b$. Choose $a = 1$, $b = 2$. Then

$$a * b = 1 * 2 = 1 - 2 = -1,$$

while

$$b * a = 2 * 1 = 2 - 1 = 1.$$

Since $-1 \neq 1$, the rule is *not* commutative.

. . . .

(2) On $\mathbb{R}$, $a * b = a + b + ab$. Compute both orders symbolically:

$$a * b = a + b + ab,$$

$$b * a = b + a + ba.$$

Because addition and multiplication are commutative in $\mathbb{R}$, we have

$$b + a = a + b \quad \text{and} \quad ba = ab,$$

hence

$$b * a = (b + a) + (ba) = (a + b) + (ab) = a * b.$$

Therefore this rule *is* commutative.

. . . .

(3) On $\mathbb{Q}$, $a * b = \dfrac{a+b}{5}$. Swapping a, b yields

$$b * a = \frac{b+a}{5}.$$

Since $b + a = a + b$ in $\mathbb{Q}$, we get

$$b * a = \frac{b+a}{5} = \frac{a+b}{5} = a * b.$$

Thus this rule *is* commutative.

. . . .

(4) On $\mathbb{Z} \times \mathbb{Z}$, $(a, b) * (c, d) = (ad + bc,\ bd)$. Compute in both orders:

$$(a, b) * (c, d) = (ad + bc,\ bd),$$

$$(c, d) * (a, b) = (cb + da,\ db).$$

In $\mathbb{Z}$ we have $cb = bc$, $da = ad$, and $db = bd$, so

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

Hence this rule *is* commutative.

. . . .

(5) On $\mathbb{Q} \setminus \{0\}$, $a * b = \dfrac{a}{b}$. Take $a = 1$, $b = 2$. Then

$$a * b = \frac{1}{2}, \qquad b * a = \frac{2}{1} = 2,$$

and $\frac{1}{2} \neq 2$, so the rule is *not* commutative.

. . . .

Conclusion. Commutative: (2), (3), (4). Not commutative: (1), (5).

□

Exercise 3 (D&F §1.1, Ex. 3). *Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).*

Intuition. "Add mod n" really means: add in $\mathbb{Z}$ first, then reduce the result mod n. Since ordinary integer addition is associative, reducing at the end should give the same residue class whether we grouped $(\bar{a}+\bar{b})+\bar{c}$ or $\bar{a}+(\bar{b}+\bar{c})$. Our job is to translate that obvious picture into equalities with bars.

Proof. Fix $a, b, c \in \mathbb{Z}$ and write their residue classes as $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$. (We use the bar to denote the image under the quotient map $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\pi(x) = \bar{x}$.) By the given well-definedness of addition in $\mathbb{Z}/n\mathbb{Z}$, we have for all $x, y \in \mathbb{Z}$:

$$\bar{x} + \bar{y} = \overline{x+y}.$$

Now compute both groupings and compare, showing every step.

Left grouping.

$$(\bar{a}+\bar{b})+\bar{c} \;=\; \overline{a+b}+\bar{c} \;=\; \overline{(a+b)+c}.$$

Right grouping.

$$\bar{a}+(\bar{b}+\bar{c}) \;=\; \bar{a}+\overline{b+c} \;=\; \overline{a+(b+c)}.$$

In $\mathbb{Z}$ we have the associativity identity $(a+b)+c = a+(b+c)$, hence

$$\overline{(a+b)+c} \;=\; \overline{a+(b+c)}\,.$$

Therefore,

$$(\bar{a}+\bar{b})+\bar{c} \;=\; \overline{(a+b)+c} \;=\; \overline{a+(b+c)} \;=\; \bar{a}+(\bar{b}+\bar{c}).$$

Since $a, b, c \in \mathbb{Z}$ were arbitrary, addition in $\mathbb{Z}/n\mathbb{Z}$ is associative. □

Exercise 4 (D&F §1.1, Ex. 4)**.** *Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).*

. . . .

Intuition. "Multiply mod n" means: multiply in $\mathbb{Z}$ first, then reduce modulo n. Since ordinary integer multiplication is associative, reducing at the end should give the same residue class whether we group $(\bar{a}\cdot\bar{b})\cdot\bar{c}$ or $\bar{a}\cdot(\bar{b}\cdot\bar{c})$.We now make each equality explicit.

. . . .

Proof. Fix $a, b, c \in \mathbb{Z}$ and write $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$ for their residue classes. (Here $\bar{x}$ denotes the image of x under the quotient map $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.) By the given well-definedness of multiplication in $\mathbb{Z}/n\mathbb{Z}$, for all $x, y \in \mathbb{Z}$ we have

$$\bar{x}\cdot\bar{y} \;=\; \overline{xy}.$$

Compute both groupings and compare, writing out each step.

. . . .

Left grouping.

$$(\bar{a}\cdot\bar{b})\cdot\bar{c} \;=\; \overline{ab}\cdot\bar{c} \;=\; \overline{(ab)c}.$$

Right grouping.

$$\bar{a}\cdot(\bar{b}\cdot\bar{c}) \;=\; \bar{a}\cdot\overline{bc} \;=\; \overline{a(bc)}.$$

In $\mathbb{Z}$ we have associativity $(ab)c = a(bc)$, hence

$$\overline{(ab)c} \;=\; \overline{a(bc)}\,.$$

Therefore,

$$(\bar{a}\cdot\bar{b})\cdot\bar{c} \;=\; \overline{(ab)c} \;=\; \overline{a(bc)} \;=\; \bar{a}\cdot(\bar{b}\cdot\bar{c}).$$

Since $a, b, c \in \mathbb{Z}$ were arbitrary, multiplication in $\mathbb{Z}/n\mathbb{Z}$ is associative. □

Exercise 5 (D&F §1.1, Ex. 5)**.** *Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.*

. . . .

Intuition. Multiplying residue classes always leaves $\bar{0}$ stuck: $\bar{0}$ times anything is $\bar{0}$. Groups demand an inverse *for every element*. But the only way $\bar{0}$ could have a multiplicative inverse $\bar{b}$ is if $\bar{0} \cdot \bar{b} = \bar{1}$—impossible, because $\bar{0} \cdot \bar{b} = \bar{0}$ for all $\bar{b}$.

. . . .

Proof. Fix an integer $n > 1$. Consider $\mathbb{Z}/n\mathbb{Z}$ with multiplication of residue classes (assumed well defined). We recall the group axioms: a group requires closure, associativity, an identity element, and an inverse for *each* element.

. . . .

Identity exists. Let $\bar{1}$ denote the residue class of 1. For any $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$,

$$\bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a} \qquad \text{and} \qquad \bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a},$$

so $\bar{1}$ is a multiplicative identity.

$\bar{0}$ *is present and distinct from* $\bar{1}$. Since $n > 1$, both 0 and 1 are integers and $0 \not\equiv 1 \pmod{n}$. Equivalently, if $\bar{0} = \bar{1}$ then $n \mid (0 - 1) = -1$, which is impossible for $n > 1$. Hence $\bar{0} \neq \bar{1}$ and $\bar{0} \in \mathbb{Z}/n\mathbb{Z}$.

. . . .

$\bar{0}$ *has no inverse.* Suppose toward a contradiction that there exists $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ with

$$\bar{0} \cdot \bar{b} = \bar{1}.$$

But for any $\bar{b}$,

$$\bar{0} \cdot \bar{b} = \overline{0 \cdot b} = \bar{0} \neq \bar{1},$$

contradiction. Therefore no such $\bar{b}$ exists; i.e., $\bar{0}$ has no multiplicative inverse.

. . . .

Since at least one element $(\bar{0})$ lacks an inverse, the set $\mathbb{Z}/n\mathbb{Z}$ fails the group axiom "every element has an inverse." Consequently, for all $n > 1$, $\big(\mathbb{Z}/n\mathbb{Z}, \cdot\big)$ is *not* a group. $\square$

Exercise 6 (D&F §1.1, Ex. 6)**.** *Determine which of the following sets are groups under addition:*

1. *the set of rational numbers (including* $0 = 0/1$*) in lowest terms whose denominators are* odd*;*
2. *the set of rational numbers (including* $0 = 0/1$*) in lowest terms whose denominators are* even*;*
3. *the set of rational numbers of absolute value* < 1*;*
4. *the set of rational numbers of absolute value* ≥ 1 *together with* 0*;*
5. *the set of rational numbers whose (lowest-terms) denominators are* 1 *or* 2*;*
6. *the set of rational numbers whose (lowest-terms) denominators are* 1*,* 2*, or* 3*.*

. . . .

Intuition. Under addition, associativity comes for free from $\mathbb{Q}$; identity is 0; inverses are negatives. So the real issue is *closure.* We test each set for closure (and note identity/inverses explicitly when it *is* a group).

. . . .

Proof. We consider each subset of $\mathbb{Q}$ in turn.

. . . .

(a) Odd denominators (in lowest terms).

Let $A = \{a \in \mathbb{Q} : a = p/q \text{ in lowest terms with } q \text{ odd}\} \cup \{0\}$ (note $0 = 0/1$ has odd denominator).

Take $a = p/q,\ b = r/s \in A$ with q, s odd and $(p, q) = (r, s) = 1$.

Then

$$a + b = \frac{p}{q} + \frac{r}{s} = \frac{ps + rq}{qs}.$$

Write $\dfrac{ps + rq}{qs} = \dfrac{u}{v}$ in lowest terms. By reduction, $v \mid qs$. If $2 \mid v$, then $2 \mid qs$, impossible since q, s are odd. Hence v is odd. Therefore $a + b \in A$ (closure). Identity: $0 \in A$. Inverses: if $a = p/q \in A$, then $-a = (-p)/q \in A$ with the same odd denominator. Thus A is a group under addition.

. . . .

(b) Even denominators (in lowest terms), plus 0.

Let $B = \{a \in \mathbb{Q} : a = p/q$ in lowest terms with q even$\} \cup \{0\}$. Take $1/2 \in B$.
Then

$$\frac{1}{2} + \frac{1}{2} = \frac{2}{2} = 1 = \frac{1}{1},$$

whose lowest-terms denominator is 1 (odd), hence $1 \notin B$. So B is *not* closed under addition; thus not a group.

. . . .

(c) $\{|a| < 1\}$.

Take $3/4, 3/4$ (both have absolute value < 1). Then

$$\frac{3}{4} + \frac{3}{4} = \frac{6}{4} = \frac{3}{2} > 1,$$

so the sum leaves the set. Not closed; not a group.

. . . .

(d) $\{|a| \geq 1\} \cup \{0\}$.

Choose $12/5$ and $-8/5$; both satisfy $|12/5| \geq 1$, $|-8/5| \geq 1$.

Then

$$\frac{12}{5} + \left(-\frac{8}{5}\right) = \frac{4}{5}, \qquad \left|\frac{4}{5}\right| < 1,$$

so the sum is not in the set. Not closed; not a group.

. . . .

(e) Denominators 1 or 2 (in lowest terms).

Let $C = \{a \in \mathbb{Q} : \text{ the lowest-terms denominator of } a \text{ is 1 or 2}\}$. We check closure by cases (the other axioms are inherited: $0 \in C$, and $-a \in C$ if $a \in C$).

(i) integer + integer.

If $a = \frac{m}{1}$ and $b = \frac{n}{1}$, then

$$a + b = \frac{m}{1} + \frac{n}{1} = \frac{m+n}{1} \in C.$$

(ii) half + half.

If $a = \frac{m}{2}$, $b = \frac{n}{2}$ in lowest terms, then

$$a + b = \frac{m}{2} + \frac{n}{2} = \frac{m+n}{2}.$$

If $m + n$ is even, $\frac{m+n}{2} = \frac{(m+n)/2}{1} \in C$; if $m + n$ is odd, it remains a half (denominator 2), so still in C.

(iii) integer + half.

If $a = \frac{m}{1}$ and $b = \frac{n}{2}$, then

$$a + b = \frac{m}{1} + \frac{n}{2} = \frac{2m}{2} + \frac{n}{2} = \frac{2m+n}{2}.$$

If $2m + n$ is even, this reduces to an integer (denominator 1); if odd, it remains a half (denominator 2). In either case $a + b \in C$. Hence C is closed; with identity 0 and inverses $-a$, C is a group under addition.

. . . .

(f) Denominators $1, 2,$ or 3 (in lowest terms).

Take

$$\frac{1}{2}+\frac{1}{3}=\frac{3+2}{6}=\frac{5}{6},$$

whose lowest-terms denominator is $6 \notin \{1,2,3\}$. Not closed; not a group.

. . . .

Conclusion.

Groups under addition: (a) and (e). Not groups: (b), (c), (d), (f). □

Exercise 7 (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. We proceed in steps.

. . . .

(A) $*$ is a well-defined binary operation on G (closure).

Fix $x, y \in G$, so $0 \leq x < 1$ and $0 \leq y < 1$. Then

$$0 \leq x + y < 2.$$

There are two cases.
Case 1: $x + y < 1$. Then $\lfloor x + y \rfloor = 0$, hence

$$x * y = x + y - \lfloor x + y \rfloor = x + y - 0 = x + y.$$

Since $0 \leq x + y < 1$, we get $x * y \in G$.
Case 2: $1 \leq x + y < 2$. Then $\lfloor x + y \rfloor = 1$, hence

$$x * y = x + y - \lfloor x + y \rfloor = x + y - 1.$$

Since $1 \leq x + y < 2$, we have $0 \leq x + y - 1 < 1$, so $x * y \in G$.
In either case $x * y \in G$, so $*$ maps $G \times G \to G$.

. . . .

(B) Associativity.

Fix $x, y, z \in G$. We must show $(x * y) * z = x * (y * z)$. By definition,

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

Compute each side by cases on whether the intermediate sums cross 1.
Case 1: $x + y < 1$ and $y + z < 1$.
Then $\lfloor x + y \rfloor = 0$ and $\lfloor y + z \rfloor = 0$. Thus

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

and

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

Hence $(x * y) * z = x * (y * z)$.
Case 2: $1 \le x + y < 2$ and $1 \le y + z < 2$.
Then $\lfloor x + y \rfloor = 1$ and $\lfloor y + z \rfloor = 1$. Thus

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

and

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

Hence $(x * y) * z = x * (y * z)$.
Case 3: $1 \le x + y < 2$ and $y + z < 1$.
Then $\lfloor x + y \rfloor = 1$ and $\lfloor y + z \rfloor = 0$. Thus

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

Also

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

Since for any real t we have $\lfloor t - 1 \rfloor = \lfloor t \rfloor - 1$, it follows that

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

Therefore $(x * y) * z = x * (y * z)$.
Case 4: $x + y < 1$ and $1 \leq y + z < 2$.
This is symmetric to Case 3. We have $\lfloor x + y \rfloor = 0$ and $\lfloor y + z \rfloor = 1$, so

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

and

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

using $\lfloor t - 1 \rfloor = \lfloor t \rfloor - 1$ again. Hence $(x * y) * z = x * (y * z)$.
All possibilities are covered, so $*$ is associative on G.

. . . .

(C) Identity element.

Take $e = 0 \in G$. For any $x \in G$ we have

$$x * e = x + e - \lfloor x + e \rfloor = x + 0 - \lfloor x \rfloor = x - \lfloor x \rfloor = x$$

because $0 \leq x < 1$ implies $\lfloor x \rfloor = 0$. Similarly

$$e * x = e + x - \lfloor e + x \rfloor = 0 + x - \lfloor x \rfloor = x.$$

Thus 0 is a two-sided identity.

. . . .

(D) Inverses.

If $x = 0$, then $x^{-1} = 0$ works since $0 * 0 = 0$. If $x \in G$ with $x \neq 0$, set $y = 1 - x$. Then $0 < y \leq 1$ and, because $x < 1$, we have $y = 1 - x \in (0, 1]$. If $y = 1$ (which happens only when $x = 0$), we already handled it; for $x \neq 0$ we have $0 < y < 1$, so $y \in G$. Compute

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

and likewise $y * x = 0$. Hence every $x \in G$ has an inverse in G.

(E) Commutativity.

For any $x, y \in G$,

$$x * y = x + y - \lfloor x + y \rfloor = y + x - \lfloor y + x \rfloor = y * x,$$

using commutativity of real addition and $\lfloor x + y \rfloor = \lfloor y + x \rfloor$.

We have shown closure, associativity, identity, inverses, and commutativity. Therefore $(G, *)$ is an abelian group. □

Exercise 8 (D&F §1.1, Ex. 8)**.** *Let* $G = \{z \in \mathbb{C} \mid z^n = 1$ *for some* $n \in \mathbb{Z}_{>0}\}$*.*

1. *Prove that* G *is a group under multiplication (the group of roots of unity in* $\mathbb{C}$*).*
2. *Prove that* G *is not a group under addition.*

. . . .

Intuition. Multiplicatively, every z with $z^n = 1$ is nonzero, so inverses exist and stay in G; products of such elements still satisfy a root-of-unity equation. Additively, trouble appears immediately: $1 \in G$ but $1 + 1 = 2 \notin G$, and 0 (the would-be additive identity) is not a root of unity.

. . . .

Proof. We address each part.

. . . .

(a) G is a group under multiplication.

Closure. Take $z, w \in G$. Then $z^n = 1$ and $w^m = 1$ for some $n, m \in \mathbb{Z}_{>0}$. Compute

$$(zw)^{nm} \;=\; z^{nm}w^{nm} \;=\; (z^n)^m(w^m)^n \;=\; 1^m \cdot 1^n \;=\; 1,$$

so $zw \in G$.
Identity. $1 \in G$ because $1^1 = 1$. For any $z \in G$, $1 \cdot z = z \cdot 1 = z$.
Inverses. If $z \in G$ with $z^n = 1$, then $z \neq 0$ and z^{-1} exists in $\mathbb{C}$. Moreover,

$$(z^{-1})^n \;=\; (z^n)^{-1} \;=\; 1^{-1} \;=\; 1,$$

so $z^{-1} \in G$.
Associativity. Multiplication in $\mathbb{C}$ is associative, hence the restriction to G is associative.

Thus G satisfies closure, identity, inverses, and associativity under multiplication; G is a group (in fact abelian, since $\mathbb{C}^\times$ is abelian).

. . . .

(b) G is not a group under addition.

Failure of closure. Since $1^1 = 1$, we have $1 \in G$. But

$$1 + 1 = 2,$$

and there is no $n \in \mathbb{Z}_{>0}$ with $2^n = 1$ (indeed $|2^n| = 2^n > 1$ for all n), so $2 \notin G$. Hence G is not closed under $+$.
(Independent) failure of identity. If G were an additive group, it would contain 0 as identity; but $0^n = 0 \neq 1$ for all n, so $0 \notin G$. Thus the additive identity is missing as well.

. . . .

Therefore G is a group under multiplication but not under addition. □

Exercise 9 (D&F §1.1, Ex. 9)**.** *Let* $G = \{\, a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q} \,\}$*.*

1. *Prove that G is a group under addition.*
2. *Prove that the nonzero elements of G form a group under multiplication.*

. . . .

Intuition. Additively, everything is linear: sums and negatives stay in the same $a + b\sqrt{2}$ form. Multiplicatively, "rationalize the denominator": $(a + b\sqrt{2})^{-1} = \dfrac{a - b\sqrt{2}}{a^2 - 2b^2}$, and the denominator never vanishes unless $a = b = 0$ (which would be the zero element we exclude).

. . . .

Proof. We treat (a) and (b) separately.

. . . .

(a) G is a group under addition.

Closure. Take arbitrary $x = a + b\sqrt{2} \in G$ and $y = c + d\sqrt{2} \in G$ with $a, b, c, d \in \mathbb{Q}$. Then

$$x + y = (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}.$$

Since $a + c \in \mathbb{Q}$ and $b + d \in \mathbb{Q}$, we have $x + y \in G$.
Identity. $0 = 0 + 0\sqrt{2} \in G$, and for any $x = a + b\sqrt{2}$,

$$x + 0 = (a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2} = x.$$

Inverses. For $x = a + b\sqrt{2}$, define $-x = (-a) + (-b)\sqrt{2} \in G$. Then

$$x + (-x) = (a - a) + (b - b)\sqrt{2} = 0 + 0\sqrt{2} = 0.$$

Associativity (and commutativity). Both follow from associativity (and commutativity) of real addition, e.g.

$$(x + y) + z = (a + c + e) + (b + d + f)\sqrt{2} = x + (y + z),$$

for $z = e + f\sqrt{2}$. Hence G is an abelian group under $+$.

. . . .

(b) Nonzero elements of G form a group under multiplication.

Let $G^\times = G \setminus \{0\} = \{\, a + b\sqrt{2} \in G \mid a, b \in \mathbb{Q},\ (a,b) \neq (0,0)\,\}$.
Closure (and no zero divisors). Take $x = a + b\sqrt{2} \in G^\times$ and $y = c + d\sqrt{2} \in G^\times$. Then

$$xy = (a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}.$$

Since $ac + 2bd \in \mathbb{Q}$ and $ad + bc \in \mathbb{Q}$, we have $xy \in G$. We now show $xy \neq 0$, i.e. that $ac + 2bd = 0$ and $ad + bc = 0$ force $c = d = 0$.

Assume $ac + 2bd = 0$ and $ad + bc = 0$.

If $a = 0$, then $ad + bc = 0$ becomes $bc = 0$. Since $(a,b) \neq (0,0)$, we must have $b \neq 0$, hence $c = 0$. Then $ac + 2bd = 0$ becomes $2bd = 0$, so $d = 0$, contradicting $(c,d) \neq (0,0)$.

If $a \neq 0$, from $ad + bc = 0$ we get $d = -\dfrac{bc}{a}$. Substitute into $ac + 2bd = 0$:

$$ac + 2b\Big(-\frac{bc}{a}\Big) = 0 \quad \Longleftrightarrow \quad a^2c - 2b^2c = 0 \quad \Longleftrightarrow \quad c\,(a^2 - 2b^2) = 0.$$

If $c = 0$, then $ad + bc = ad + 0 = 0$ gives $d = 0$ (since $a \neq 0$), contradiction. Thus $a^2 - 2b^2 = 0$, i.e. $\left(\frac{a}{b}\right)^2 = 2$ with $a, b \in \mathbb{Q}$. This forces $a = b = 0$ (because $\sqrt{2} \notin \mathbb{Q}$), contradicting $(a,b) \neq (0,0)$. Therefore $xy \neq 0$ and $xy \in G^\times$; closure holds.
Identity. $1 = 1 + 0\sqrt{2} \in G^\times$, and for any $x = a + b\sqrt{2}$,

$$x \cdot 1 = (a + b\sqrt{2})(1 + 0\sqrt{2}) = a + b\sqrt{2} = x.$$

Inverses (explicit). Let $x = a + b\sqrt{2} \in G^\times$. Consider

$$x \cdot (a - b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - (b\sqrt{2})^2 = a^2 - 2b^2.$$

If $a^2 - 2b^2 = 0$, then $\left(\frac{a}{b}\right)^2 = 2$ with $a, b \in \mathbb{Q}$, which implies $a = b = 0$, contradicting $x \in G^\times$. Hence $a^2 - 2b^2 \neq 0$, and we may define

$$x^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in G^\times,$$

since $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$. Then

$$x \cdot x^{-1} = \frac{(a + b\sqrt{2})(a - b\sqrt{2})}{a^2 - 2b^2} = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1.$$

Associativity (and commutativity). Inherited from multiplication in $\mathbb{R}$, so

$$(xy)z = x(yz) \quad \text{and} \quad xy = yx$$

for all $x, y, z \in G^\times$.

We have verified closure in $G^\times$, identity 1, inverses for every element, and associativity. Hence $G^\times$ is a (abelian) group under multiplication.

□

Exercise 10 (D&F §1.1, Ex. 10)**.** *Prove that a finite group is abelian if and only if its group table is a symmetric matrix.*

. . . .

Intuition. A group table records all products $g_i g_j$. If swapping i and j leaves the entry unchanged, then $g_i g_j = g_j g_i$ for every pair—exactly the definition of "abelian." So table symmetry *is* commutativity written as a matrix.

. . . .

Proof. Let $G = \{g_1, g_2, \dots, g_n\}$ be a finite group. Its (Cayley) group table is the $n \times n$ matrix $T = (T_{ij})$ with entries

$$T_{ij} = g_i g_j.$$

A matrix is symmetric if $T_{ij} = T_{ji}$ for all $1 \leq i, j \leq n$.

. . . .

(⇒) If G is abelian, then the table is symmetric.

Assume $g_i g_j = g_j g_i$ for all i, j. Then

$$T_{ij} = g_i g_j = g_j g_i = T_{ji}$$

for every i, j, hence T is symmetric.

. . . .

(⇐) If the table is symmetric, then G is abelian.

Assume $T_{ij} = T_{ji}$ for all i, j. Then by the definition of the entries,

$$g_i g_j = T_{ij} = T_{ji} = g_j g_i$$

for every pair i, j. Hence all elements commute and G is abelian.

. . . .

Thus a finite group is abelian if and only if its group table is symmetric. □

Exercise 11 (D&F §1.1, Ex. 11)**.** *Find the orders of each element of the additive group $\mathbb{Z}/12\mathbb{Z}$.*

. . . .

Intuition. In $(\mathbb{Z}/12\mathbb{Z}, +)$ the order of $\bar{x}$ is the smallest $k \geq 1$ with

$$k \cdot \bar{x} = \overline{kx} = \bar{0}.$$

Equivalently, we want $12 \mid kx$. The obstruction is the common factor $\gcd(12, x)$: the more x shares with 12, the fewer steps it takes to hit $\bar{0}$.

. . . .

Proof. Fix $x \in \{0, 1, \dots, 11\}$ and let $d = \gcd(12, x)$. Write $12 = d \cdot m$ and $x = d \cdot x'$ with $\gcd(m, x') = 1$. Then

$$\overline{kx} = \bar{0} \quad \Longleftrightarrow \quad 12 \mid kx \quad \Longleftrightarrow \quad dm \mid k\,(dx') \quad \Longleftrightarrow \quad m \mid kx'.$$

Since $\gcd(m, x') = 1$, the least $k \geq 1$ with $m \mid kx'$ is $k = m$. Therefore

$$|\bar{x}| = \frac{12}{\gcd(12, x)}.$$

We now list the values.

. . . .

Table of orders in $\mathbb{Z}/12\mathbb{Z}$:

x	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$
$\lvert x \rvert$	1	12	6	4	3	12	2	12	3	4	6	12

. . . .

Spot checks (explicit equalities).

$$3 \cdot \bar{4} = \overline{12} = \bar{0} \;\text{ while }\; 1 \cdot \bar{4} = \bar{4} \neq \bar{0},\; 2 \cdot \bar{4} = \bar{8} \neq \bar{0} \;\Rightarrow\; |\bar{4}| = 3,$$

$$2 \cdot \bar{6} = \overline{12} = \bar{0} \;\text{ while }\; 1 \cdot \bar{6} = \bar{6} \neq \bar{0} \;\Rightarrow\; |\bar{6}| = 2,$$

$$4 \cdot \bar{3} = \overline{12} = \bar{0} \;\text{ with }\; 1, 2, 3 \text{ steps nonzero} \;\Rightarrow\; |\bar{3}| = 4.$$

This agrees with $|\bar{x}| = 12/\gcd(12, x)$ for each listed x, completing the computation. □

Exercise 12 (D&F §1.1, Ex. 12). *Find the orders of the following elements of the multiplicative group* $(\mathbb{Z}/12\mathbb{Z})^\times$*:* $\bar{1}$, $-\bar{1}$, $\bar{5}$, $\bar{7}$, $-\bar{7}$, $\overline{13}$*.*

. . . .

Intuition. Work modulo 12, reduce each representative to $\{\bar{1}, \bar{5}, \bar{7}, \bar{1}\bar{1}\}$ (the units mod 12), and compute the smallest positive k with $\bar{x}^k = \bar{1}$. Squares collapse quickly here: $\bar{5}^2 = \bar{7}^2 = \bar{1}\bar{1}^2 = \bar{1}$.

. . . .

Proof. Recall $(\mathbb{Z}/12\mathbb{Z})^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{1}\bar{1}\}$ and that $\overline{-1} = \bar{1}\bar{1}$, $\overline{-7} = \bar{5}$, $\overline{13} = \bar{1}$.

. . . .

$\bar{1}$.

$$\bar{1}^1 = \bar{1} \quad \Rightarrow \quad |\bar{1}| = 1.$$

$-\bar{1} = \bar{1}\bar{1}$.

$$\bar{1}\bar{1}^1 = \bar{1}\bar{1} \neq \bar{1}, \qquad \bar{1}\bar{1}^2 = \overline{121} = \bar{1} = \bar{1} \ \Rightarrow \ |\bar{1}\bar{1}| = 2.$$

$\bar{5}$.

$$\bar{5}^1 = \bar{5} \neq \bar{1}, \qquad \bar{5}^2 = \overline{25} = \bar{1} = \bar{1} \ \Rightarrow \ |\bar{5}| = 2.$$

$\bar{7}$.

$$\bar{7}^1 = \bar{7} \neq \bar{1}, \qquad \bar{7}^2 = \overline{49} = \bar{1} = \bar{1} \ \Rightarrow \ |\bar{7}| = 2.$$

$-\bar{7} = \overline{-7} = \bar{5}$. Same as $\bar{5}$, hence $|\overline{-7}| = 2$.
$\overline{13} = \bar{1}$. Same as $\bar{1}$, hence $|\overline{13}| = 1$.

. . . .

Conclusion (table).

x	$\bar{1}$	$-\bar{1}$	$\bar{5}$	$\bar{7}$	$-\bar{7}$	$\overline{13}$
$\lvert x \rvert$	1	2	2	2	2	1

□

Exercise 13 (D&F §1.1, Ex. 13)**.** *Find the orders of the following elements of the additive group $\mathbb{Z}/36\mathbb{Z}$:* $\bar{1}$, $\bar{2}$, $\bar{6}$, $\bar{9}$, $\overline{10}$, $\overline{12}$, $-\bar{1}$, $-\overline{10}$, $-\overline{18}$.

Intuition. In $(\mathbb{Z}/36\mathbb{Z}, +)$ the order of $\bar{x}$ is the least $k \geq 1$ with

$$k \cdot \bar{x} = \overline{kx} = \bar{0} \quad \Longleftrightarrow \quad 36 \mid kx.$$

The larger $\gcd(36, x)$ is, the fewer steps it takes to hit $\bar{0}$. This leads to the standard formula

$$|\bar{x}| = \frac{36}{\gcd(36, x)}.$$

Proof. Fix $x \in \mathbb{Z}$ and let $d = \gcd(36, x)$. Write $36 = dm$ and $x = dx'$ with $\gcd(m, x') = 1$. Then

$$\overline{kx} = \bar{0} \iff 36 \mid kx \iff dm \mid k(dx') \iff m \mid kx'.$$

Since $\gcd(m, x') = 1$, the least $k \geq 1$ with $m \mid kx'$ is $k = m$. Hence $|\bar{x}| = 36/\gcd(36, x)$.

We now apply the formula entry by entry (note $-\bar{a} = \overline{-a}$, so $\gcd(36, -a) = \gcd(36, a)$).

Table of orders in $\mathbb{Z}/36\mathbb{Z}$ (split):

x	$\bar{1}$	$\bar{2}$	$\bar{6}$	$\bar{9}$	$\overline{10}$	$\overline{12}$	$-\bar{1}$	$-\overline{10}$	$-\overline{18}$
$\lvert\bar{x}\rvert$	36	18	6	4	18	3	36	18	2

Spot checks (explicit equalities).

$$18 \cdot \bar{2} = \overline{36} = \bar{0} \text{ and } k \cdot \bar{2} \neq \bar{0} \text{ for } 1 \leq k < 18 \;\Rightarrow\; |\bar{2}| = 18,$$

$$4 \cdot \bar{9} = \overline{36} = \bar{0} \text{ and } 1, 2, 3 \text{ steps are nonzero } \Rightarrow |\bar{9}| = 4,$$

$$3 \cdot \overline{12} = \overline{36} = \bar{0} \Rightarrow |\overline{12}| = 3, \qquad 2 \cdot (-\overline{18}) = \overline{-36} = \bar{0} \Rightarrow |-\overline{18}| = 2.$$

This matches the table above, completing the computation. □

Exercise 14 (D&F §1.1, Ex. 14)**.** *Find the orders of the following elements of the multiplicative group* $(\mathbb{Z}/36\mathbb{Z})^{\times}$*:* $\bar{1},\ -\bar{1},\ \bar{5},\ \overline{13},\ \overline{-13},\ \overline{17}$.

Intuition. Work modulo 36 inside the unit group $\{\bar{x} \in \mathbb{Z}/36\mathbb{Z} : \gcd(x, 36) = 1\}$. For each listed element, compute the smallest positive k with $\bar{x}^{\,k} = \bar{1}$ by explicit reductions. (Useful notes: $\overline{-1} = \overline{35}$ has order 2; $\overline{17}^{\,2} = \overline{289} = \bar{1}$; 13 lands on 1 at the third power.)

Proof. All computations are in $\mathbb{Z}/36\mathbb{Z}$.

$\bar{1}$.

$$\bar{1}^{\,1} = \bar{1} \;\Rightarrow\; |\bar{1}| = 1.$$

$-\bar{1} = \overline{35}$.

$$\overline{35}^{\,1} = \overline{35} \neq \bar{1}, \qquad \overline{35}^{\,2} = \overline{1225} = \overline{1224 + 1} = \bar{1} = \bar{1} \;\Rightarrow\; |-\bar{1}| = 2.$$

$\bar{5}$.

$$\bar{5}^{\,2} = \overline{25}, \quad \bar{5}^{\,3} = \overline{125} = \overline{125 - 108} = \overline{17},$$
$$\bar{5}^{\,4} = \overline{17 \cdot 5} = \overline{85} = \overline{85 - 72} = \overline{13}, \quad \bar{5}^{\,5} = \overline{13 \cdot 5} = \overline{65} = \overline{65 - 36} = \overline{29},$$
$$\bar{5}^{\,6} = \overline{29 \cdot 5} = \overline{145} = \overline{145 - 144} = \bar{1}.$$

No smaller positive power gave $\bar{1}$, so $|\bar{5}| = 6$.

$\overline{13}$.

$$\overline{13}^{\,2} = \overline{169} = \overline{169 - 144} = \overline{25}, \qquad \overline{13}^{\,3} = \overline{25 \cdot 13} = \overline{325} = \overline{325 - 324} = \bar{1},$$

hence $|\overline{13}| = 3$.

$\overline{-13} = \overline{23}$.

$\overline{23}^2 = \overline{529} = \overline{529 - 504} = \overline{25}, \quad \overline{23}^3 = \overline{25 \cdot 23} = \overline{575} = \overline{575 - 540} = \overline{35},$

$\overline{23}^4 = \overline{35 \cdot 23} = \overline{805} = \overline{805 - 792} = \overline{13}, \quad \overline{23}^5 = \overline{13 \cdot 23} = \overline{299} = \overline{299 - 288} = \overline{11},$

$$\overline{23}^6 = \overline{11 \cdot 23} = \overline{253} = \overline{253 - 252} = \bar{1},$$

so $|\overline{-13}| = 6$.

. . . .

$\overline{17}$.

$$\overline{17}^2 = \overline{289} = \overline{289 - 288} = \bar{1} \;\Rightarrow\; |\overline{17}| = 2.$$

. . . .

Conclusion (table).

x	$\bar{1}$	$-\bar{1}$	$\bar{5}$	$\overline{13}$	$\overline{-13}$	$\overline{17}$
$\lvert x\rvert$	1	2	6	3	6	2

□

Exercise 15 (D&F §1.1, Ex. 15)**.** *Let G be a group. Prove that for all $a_1, a_2, \dots, a_n \in G$,*

$$(a_1 a_2 \cdots a_n)^{-1} \;=\; a_n^{-1}\, a_{n-1}^{-1} \cdots a_1^{-1}.$$

. . . .

Intuition. To "undo" a sequence of moves $a_1, a_2, \dots, a_n$, we must undo them in the opposite order with the opposite moves: first a_n^{-1}, then a_{n-1}^{-1}, …, finally a_1^{-1}. Group associativity lets us cancel step by step from the outside in.

. . . .

Proof. We prove the statement by induction on $n \in \mathbb{Z}_{\geq 1}$.

. . . .

Base case $n = 1$.

For any $a_1 \in G$,

$$(a_1)^{-1} = a_1^{-1},$$

which matches the formula.

. . . .

Inductive step.

Assume the statement holds for some $k \geq 1$, i.e.

$$(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1}\, a_{k-1}^{-1} \cdots a_1^{-1}.$$

We prove it for $k+1$ elements. Write

$$a_1 a_2 \cdots a_k a_{k+1} \;=\; \big(a_1 a_2 \cdots a_k\big)\, a_{k+1}.$$

Using the group rule $(xy)^{-1} = y^{-1} x^{-1}$,

$$(a_1 \cdots a_k a_{k+1})^{-1} \;=\; a_{k+1}^{-1}\, \big(a_1 \cdots a_k\big)^{-1}.$$

Apply the induction hypothesis to $(a_1 \cdots a_k)^{-1}$:

$$(a_1 \cdots a_k a_{k+1})^{-1} \;=\; a_{k+1}^{-1} \left(a_k^{-1}\, a_{k-1}^{-1} \cdots a_1^{-1}\right) \;=\; a_{k+1}^{-1}\, a_k^{-1}\, a_{k-1}^{-1} \cdots a_1^{-1}.$$

This is precisely the required formula for $k+1$ elements.

. . . .

By induction, the identity holds for all $n \geq 1$:

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1}\, a_{n-1}^{-1} \cdots a_1^{-1}.$$

□

Exercise 16 (D&F §1.1, Ex. 16)**.** *Let x be an element of a group G. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.*

. . . .

Intuition. If applying x twice does nothing ($x^2 = 1$), then one or two applications already return you to the identity; the least such number is 1 or 2. Conversely, if the order is 1 or 2, squaring must give 1.

. . . .

Proof. We show both implications.

. . . .

(⇒) If $x^2 = 1$, then $|x| \in \{1, 2\}$.

By hypothesis, $x^2 = 1$. By definition of order, $|x|$ is the least positive integer n with $x^n = 1$. Since $x^2 = 1$, we have at least one such positive integer, namely $n = 2$. Therefore

$$1 \leq |x| \leq 2.$$

Hence either $|x| = 1$ or $|x| = 2$, as required.

. . . .

(⇐) If $|x| = 1$ or $|x| = 2$, then $x^2 = 1$.

If $|x| = 1$, then by definition $x = 1$, and so

$$x^2 = 1^2 = 1.$$

If $|x| = 2$, then by definition $x^2 = 1$. In either case $x^2 = 1$ holds.

. . . .

Thus $x^2 = 1$ if and only if $|x| \in \{1, 2\}$. □

Exercise 17 (D&F §1.1, Ex. 17)**.** *Let x be an element of a group G. Prove that if $|x| = n$ for some positive integer n, then*

$$x^{-1} = x^{n-1}.$$

. . . .

Intuition. "Order n" means $x^n = 1$. To peel off one x from x^n, multiply by x^{-1} on the left (or right); associativity turns $x^{-1}x^n$ into $(x^{-1}x)\,x^{n-1} = 1 \cdot x^{n-1}$, revealing x^{n-1} as the inverse.

. . . .

Proof. Assume $|x| = n$. By definition, $x^n = 1$.

Left–multiply both sides by x^{-1}:

$$x^{-1}x^n = x^{-1} \cdot 1.$$

By associativity,

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

Since $x^{-1}x = 1$, we obtain

$$1 \cdot x^{n-1} = x^{-1} \quad\Longrightarrow\quad x^{n-1} = x^{-1}.$$

(Equivalently, right–multiplying $x^n = 1$ by x^{-1} gives $x^{n-1} = x^{-1}$ as well.) Thus, if $|x| = n$, then $x^{-1} = x^{n-1}$. □

Exercise 18 (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. We prove the three statements are equivalent by showing

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

. . . .

($xy = yx \Rightarrow y^{-1}xy = x$).

Assume $xy = yx$. Left–multiply by y^{-1}:

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

By associativity,

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

Since $y^{-1}y = 1$ and $1x = x$, we obtain

$$y^{-1}xy = x.$$

. . . .

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

Assume $y^{-1}xy = x$. Left–multiply by x^{-1}:

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

By associativity,

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

so

$$x^{-1}y^{-1}xy = 1.$$

. . . .

($x^{-1}y^{-1}xy = 1 \Rightarrow xy = yx$).

Assume $x^{-1}y^{-1}xy = 1$. Left–multiply by x:

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

By associativity,

$$(xx^{-1})y^{-1}xy = x \quad \Longrightarrow \quad 1 \cdot y^{-1}xy = x \quad \Longrightarrow \quad y^{-1}xy = x.$$

Now left–multiply by y:

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

Again by associativity,

$$(yy^{-1})xy = yx \quad \Longrightarrow \quad 1 \cdot xy = yx \quad \Longrightarrow \quad xy = yx.$$

. . . .

Thus all three statements are equivalent:

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

□

Exercise 19 (D&F §1.1, Ex. 19)**.** *Let $x \in G$ for G a group and let $a, b \in \mathbb{Z}_{>0}$.*

1. *Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.*
2. *Prove that $(x^a)^{-1} = x^{-a}$.*
3. *Establish part (1) for arbitrary integers a and b (positive, negative, or 0).*

. . . .

Intuition. Read x^n as "n copies of x multiplied in a row" (and $x^0 = 1$, $x^{-n} = (x^{-1})^n$). Then $a + b$ copies should split as a-copies followed by b-copies, and repeating a block of a-copies, b times, gives ab copies. Inverses flip each copy to x^{-1} and reverse the order—yielding $(x^a)^{-1} = (x^{-1})^a = x^{-a}$.

. . . .

Proof. We proceed part by part, showing each string of equalities explicitly.

. . . .

(1) For $a, b \in \mathbb{Z}_{>0}$, $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.

Write $x^a = \underbrace{x \cdot x \cdots x}_{a \text{ factors}}$ and $x^b = \underbrace{x \cdot x \cdots x}_{b \text{ factors}}$. Then

$$x^a x^b = \underbrace{x \cdots x}_{a}\ \underbrace{x \cdots x}_{b} = \underbrace{x \cdots x}_{a+b} = x^{a+b}.$$

Similarly, $(x^a)^b$ is the product of b copies of x^a:

$$(x^a)^b = \underbrace{(x^a)(x^a) \cdots (x^a)}_{b} = \underbrace{\overbrace{x \cdots x}^{a}\ \overbrace{x \cdots x}^{a}\ \cdots\ \overbrace{x \cdots x}^{a}}_{b \text{ blocks}} = \underbrace{x \cdots x}_{ab} = x^{ab}.$$

. . . .

(2) For $a \in \mathbb{Z}_{>0}$, $(x^a)^{-1} = x^{-a}$.

Recall $x^{-a} = (x^{-1})^a$ by definition of negative powers. We show $(x^a)^{-1} = (x^{-1})^a$ by induction on a.
Base $a = 1$. $(x^1)^{-1} = x^{-1} = (x^{-1})^1$.
Inductive step. Assume $(x^k)^{-1} = (x^{-1})^k$ for some $k \geq 1$. Then

$$(x^{k+1})\,(x^{-1})^{k+1} = \big((x^k)x\big)\,\big(x^{-1}(x^{-1})^k\big) = x^k\,(xx^{-1})\,(x^{-1})^k = x^k\,1\,(x^{-1})^k = x^k(x^{-1})^k.$$

By the inductive hypothesis, $x^k(x^{-1})^k = 1$, hence

$$(x^{k+1})\,(x^{-1})^{k+1} = 1.$$

Thus $(x^{k+1})^{-1} = (x^{-1})^{k+1}$. By induction, $(x^a)^{-1} = (x^{-1})^a = x^{-a}$ for all $a \geq 1$.

. . . .

(3) Extend $x^{a+b} = x^a x^b$ to all $a, b \in \mathbb{Z}$.

We use the conventions $x^0 = 1$ and $x^{-n} = (x^{-1})^n$ for $n > 0$.
Zero cases. For any integer a,

$$x^{a+0} = x^a = x^a \cdot 1 = x^a x^0, \qquad x^{0+b} = x^b = 1 \cdot x^b = x^0 x^b.$$

Mixed signs: $a > 0$, $b < 0$. Write $b = -m$ with $m \in \mathbb{Z}_{>0}$.
If $a + b = a - m > 0$, then

$$x^{a+b}\,x^{-b} = x^{(a-m)}\,x^m = x^{(a-m)+m} = x^a \quad\Longrightarrow\quad x^{a+b} = x^a\,x^b.$$

(We multiplied on the right by $x^{-b} = x^m$ and used the positive-exponent law from (1).)
If $a + b = a - m < 0$, then $-(a + b) = m - a > 0$ and

$$x^{-(a+b)}\,x^a = x^{(m-a)}\,x^a = x^{(m-a)+a} = x^m = x^{-b}.$$

Right–multiply by x^{-a}:

$$x^{-(a+b)} = x^{-b}\,x^{-a}.$$

Now take inverses and use $(uv)^{-1} = v^{-1}u^{-1}$ and part (2):

$$\bigl(x^{-(a+b)}\bigr)^{-1} = \bigl(x^{-b}\,x^{-a}\bigr)^{-1} \quad\Longrightarrow\quad x^{a+b} = (x^{-a})^{-1}\,(x^{-b})^{-1} = x^{a}\,x^{b}.$$

Mixed signs: $a < 0$, $b > 0$. This is symmetric to the previous case (swap a and b); the same argument yields $x^{a+b} = x^a x^b$.
Both negative: $a = -r$, $b = -s$ with $r, s > 0$. Then $a + b = -(r + s)$ and

$$x^{a+b} = x^{-(r+s)} = \bigl(x^{r+s}\bigr)^{-1} = \bigl(x^r x^s\bigr)^{-1} = (x^s)^{-1}(x^r)^{-1} = x^{-s}x^{-r} = x^b x^a.$$

Since x^b and x^a commute with themselves as powers of the same element, $x^b x^a = x^a x^b$, so indeed $x^{a+b} = x^a x^b$.

. . . .

We have established $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$ for positive a, b, proved $(x^a)^{-1} = x^{-a}$, and extended $x^{a+b} = x^a x^b$ to all integers a, b, as required. □

Exercise 20 (D&F §1.1, Ex. 20)**.** *For x an element in a group G, show that x and x^{-1} have the same order.*

. . . .

Intuition. "Order n" means $x^n = 1$. Inverting both sides preserves equality and turns x^n into $(x^{-1})^n$, so the same n works for x^{-1}. Symmetrically, any power that kills x^{-1} also kills x.

. . . .

Proof. Recall: the order $|x|$ is the least $n \in \mathbb{Z}_{>0}$ with $x^n = 1$, if such an n exists; otherwise $|x| = \infty$. We show the finite–order case in both inequalities and then note the infinite case.

. . . .

If $|x|$ is finite, then $|x^{-1}| \leq |x|$.

Let $|x| = n$. Then

$$x^n = 1.$$

Taking inverses of both sides,

$$(x^n)^{-1} = 1^{-1}.$$

Using $(uv)^{-1} = v^{-1}u^{-1}$ repeatedly (or $(x^a)^{-1} = x^{-a}$ from Ex. 19), we have

$$(x^n)^{-1} = (x^{-1})^n \qquad \text{and} \qquad 1^{-1} = 1.$$

Hence

$$(x^{-1})^n = 1,$$

so x^{-1} has finite order and $|x^{-1}| \leq n = |x|$.

. . . .

If $|x^{-1}|$ is finite, then $|x| \leq |x^{-1}|$.

Let $|x^{-1}| = k$. Then

$$(x^{-1})^k = 1.$$

Taking inverses,

$$\left((x^{-1})^k\right)^{-1} = 1^{-1}.$$

Again using the inverse law for powers,

$$\left((x^{-1})^k\right)^{-1} = x^k \qquad \text{and} \qquad 1^{-1} = 1,$$

so

$$x^k = 1.$$

Thus x has finite order and $|x| \leq k = |x^{-1}|$.

. . . .

Combining the two inequalities in the finite case yields $|x| = |x^{-1}|$. If x had infinite order but x^{-1} finite (or conversely), one of the two arguments above would force the other to be finite as well, a contradiction. Hence x has infinite order if and only if x^{-1} has infinite order.

. . . .

Therefore x and x^{-1} always have the same order. □

Exercise 21 (D&F §1.1, Ex. 21)**.** *Let G be a finite group and let $x \in G$ have order n. Prove that if n is odd, then*

$$x = (x^2)^k \quad \textit{for some } k \in \mathbb{Z}_{\geq 1}.$$

. . . .

Intuition. If $|x| = n$ is odd, then $n = 2k-1$ for some k. Since $x^n = 1$, multiplying by x pushes the exponent up by one: $x^{2k-1}x = x^{2k} = x$. But $x^{2k} = (x^2)^k$, so $x = (x^2)^k$.

. . . .

Proof. Assume $|x| = n$ and n is odd. Then there is $k \in \mathbb{Z}_{\geq 1}$ with

$$n = 2k - 1.$$

By definition of order,

$$x^n = 1 \quad \Longrightarrow \quad x^{2k-1} = 1.$$

Multiply both sides on the right by x:

$$x^{2k-1}\, x \;=\; 1 \cdot x.$$

Using the exponent law $x^a x^b = x^{a+b}$ (from group associativity),

$$x^{(2k-1)+1} \;=\; x \quad \Longrightarrow \quad x^{2k} = x.$$

Now rewrite the left-hand side as a power of x^2:

$$x^{2k} = (x^2)^k.$$

Therefore

$$x = (x^2)^k,$$

as required. □

Exercise 22 (D&F §1.1, Ex. 22)**.** *If x and g are elements of a group G, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a, b \in G$.*

. . . .

Intuition. Conjugating by g is just a "change of coordinates." Powers pass cleanly through:

$$(g^{-1}xg)^k = g^{-1}x^k g.$$

So $x^n = 1$ iff $(g^{-1}xg)^n = 1$, hence the orders match. Taking $x = ab$ and $g = b$ gives

$$b^{-1}(ab)b = ba,$$

so $|ab| = |ba|$.

. . . .

Proof. We first prove the power–pushing identity by induction: for every $k \in \mathbb{Z}_{\geq 1}$,

$$(g^{-1}xg)^k = g^{-1}x^k g.$$

Base $k = 1$.

$$(g^{-1}xg)^1 = g^{-1}xg.$$

Inductive step. Assume $(g^{-1}xg)^k = g^{-1}x^k g$. Then

$$(g^{-1}xg)^{k+1} = (g^{-1}xg)^k\,(g^{-1}xg) = \big(g^{-1}x^k g\big)\,(g^{-1}xg) = g^{-1}x^k(gg^{-1})xg = g^{-1}x^{k+1}g.$$

Thus the identity holds for all $k \geq 1$.

. . . .

Equality of orders. Suppose $|x| = n$ is finite. Then $x^n = 1$, hence

$$(g^{-1}xg)^n \;=\; g^{-1}x^n g \;=\; g^{-1}1\,g \;=\; 1,$$

so $|g^{-1}xg| \leq n$.

Conversely, if $|g^{-1}xg| = k$ is finite, then $(g^{-1}xg)^k = 1$, so

$$1 = (g^{-1}xg)^k = g^{-1}x^k g \quad\Longrightarrow\quad x^k = g\,1\,g^{-1} = 1,$$

hence $|x| \leq k$. Therefore $|x| = |g^{-1}xg|$ in the finite case, and the same argument shows x has infinite order iff $g^{-1}xg$ does.

. . . .

Deduction $|ab| = |ba|$. Let $x = ab$ and $g = b$. Then

$$g^{-1}xg = b^{-1}(ab)b = ba,$$

so by the conjugacy invariance just proved,

$$|ab| = |ba|.$$

□

Exercise 23 (D&F §1.1, Ex. 23)**.** *Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers s and t, prove that*

$$\left|x^{s}\right| = t.$$

. . . .

Intuition. "Order n" means $x^n = 1$ and no smaller positive power of x is 1. For x^s, the t-th power is

$$(x^s)^t = x^{st} = x^n = 1,$$

so the order of x^s divides t. If $(x^s)^k = 1$, then $x^{sk} = 1$, hence $n \mid sk$. Since $n = st$, this forces $t \mid k$, so the *smallest* such k is t.

. . . .

Proof. Assume $|x| = n$ with $n = st$ and $s, t \in \mathbb{Z}_{>0}$.
Step 1: $(x^s)^t = 1$.

$$(x^s)^t = x^{st} = x^n = 1.$$

Hence $\left|x^{s}\right|$ is a positive integer dividing t.

. . . .

Step 2: Minimality of t. Suppose $(x^s)^k = 1$ for some $k \in \mathbb{Z}_{>0}$. Then

$$(x^s)^k = 1 \implies x^{sk} = 1.$$

By the definition of $|x| = n$, this is equivalent to

$$n \mid sk.$$

Using $n = st$,

$$st \mid sk \implies t \mid k.$$

Therefore every positive k with $(x^s)^k = 1$ is a multiple of t, so the least such k is t.

. . . .

Combining the two steps, $\left|x^{s}\right| = t$. □

Exercise 24 (D&F §1.1, Ex. 24)**.** *If a and b are commuting elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]*

. . . .

Intuition. When $ab = ba$, powers "separate cleanly": each time we append another ab we can slide the new a past all existing b's, and the new b past all existing a's, so $(ab)^{k+1} = a^{k+1}b^{k+1}$. Negative exponents follow from $(ab)^{-1} = b^{-1}a^{-1}$ and the fact that inverses also commute.

. . . .

Proof. Assume throughout that $ab = ba$.

. . . .

Step 1 (positive exponents by induction).

We show $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}_{>0}$.
Base $n = 1$.

$$(ab)^1 = ab = a^1 b^1.$$

Inductive step. Assume $(ab)^k = a^k b^k$ for some $k \geq 1$. Then

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

Because $ab = ba$, a commutes with b^k (prove by a one-line induction on k), so $b^k a = ab^k$. Hence

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

Thus by induction $(ab)^n = a^n b^n$ for all $n \geq 1$.

. . . .

Step 2 (the zero exponent).

By convention $x^0 = 1$ for any $x \in G$. Hence

$$(ab)^0 = 1 = a^0 b^0.$$

Step 3 (negative exponents).

Let $n = -m$ with $m \in \mathbb{Z}_{>0}$. Then

$$(ab)^n = (ab)^{-m} = \big((ab)^{-1}\big)^m.$$

Using the inverse-of-a-product rule,

$$(ab)^{-1} = b^{-1}a^{-1}.$$

From $ab = ba$ it follows that a^{-1} and b^{-1} also commute, so we may apply the positive-exponent case to b^{-1} and a^{-1}:

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

Since $n = -m$, we have $a^{-m} = a^n$ and $b^{-m} = b^n$, hence

$$(ab)^n = a^n b^n.$$

Combining the three steps, $(ab)^n = a^n b^n$ holds for all $n \in \mathbb{Z}$. □

Exercise 25 (D&F §1.1, Ex. 25)**.** *Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.*

. . . .

Intuition. If every element is an *involution* ($x^2 = 1$), then $x = x^{-1}$ for all x. Apply this to a product ab: since $(ab)^2 = 1$, we have $ab = (ab)^{-1}$. But $(ab)^{-1} = b^{-1}a^{-1}$, and with $a^{-1} = a$, $b^{-1} = b$, this collapses to $ab = ba$.

. . . .

Proof. Assume $x^2 = 1$ for all $x \in G$.

. . . .

Step 1: Every element equals its inverse.

Fix $x \in G$. From $x^2 = 1$ we have

$$x \cdot x = 1.$$

By definition of inverse, this implies $x^{-1} = x$.

. . . .

Step 2: Compute $(ab)^{-1}$ explicitly.

For arbitrary $a, b \in G$,

$$(ab)(b^{-1}a^{-1}) = a\,(bb^{-1})\,a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1,$$

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

so

$$(ab)^{-1} = b^{-1}a^{-1}.$$

. . . .

Step 3: Conclude $ab = ba$.

Since $x^2 = 1$ holds for *every* x, it holds for $x = ab$:

$$(ab)^2 = 1 \quad \Longrightarrow \quad ab = (ab)^{-1}.$$

Using Step 2 and Step 1,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

As $a, b \in G$ were arbitrary, G is abelian. □

Exercise 26 (D&F §1.1, Ex. 26)**.** *Assume H is a nonempty subset of the group $(G, \cdot)$ which is closed under the binary operation on G and is closed under inverses; i.e., for all $h, k \in H$, $hk \in H$ and $h^{-1} \in H$. Prove that H is a group under the operation $\cdot$ restricted to H (such a subset H is called a subgroup of G).*

. . . .

Intuition. We already know the law and associativity from G. Nonempty + "closed under inverses" gives us $a, a^{-1} \in H$, so $aa^{-1} = e \in H$, producing an identity inside H. The given closure then keeps all products in H. Thus H inherits every group axiom.

. . . .

Proof. We use multiplicative notation (juxtaposition) for the group law and verify the axioms on H.

. . . .

Associativity on H.

For any $x, y, z \in H$, since $H \subseteq G$ and the operation is the same as in G,

$$(xy)z \;=\; x(yz)$$

in G, hence also as elements of H (the operation is merely restricted).

. . . .

Identity element belongs to H.

Because $H \neq \varnothing$, choose $a \in H$. By the inverse-closure hypothesis, $a^{-1} \in H$. By the product-closure hypothesis, $aa^{-1} \in H$. In G, $aa^{-1} = e$ (the identity of G), hence

$$e \;=\; aa^{-1} \in H.$$

For any $h \in H$, since e is the identity in G,

$$eh = h \quad \text{and} \quad he = h,$$

so e acts as the identity on H as well.

. . . .

Inverses lie in H.

This is given: for every $h \in H$, $h^{-1} \in H$, and in G we have

$$hh^{-1} = e = h^{-1}h,$$

so each element of H has an inverse in H.

. . . .

Closure in H.

This is also given: for all $h, k \in H$, $hk \in H$.

. . . .

Thus H satisfies associativity (inherited), has an identity $e \in H$, is closed under the operation, and every element has an inverse in H. Therefore H, with the restricted operation, is a group (a subgroup of G). □

Exercise 27 (D&F §1.1, Ex. 27)**.** *Prove that if x is an element of the group G then $H = \{x^n \mid n \in \mathbb{Z}\}$ is a subgroup of G (called the cyclic subgroup of G generated by x).*

. . . .

Intuition. Start with all integer powers of a single element x. Multiplying x^m by x^n simply *adds* exponents, and inverting x^m simply *negates* its exponent. So this set is closed under the group law and under inverses, and it already contains the identity $x^0 = 1$.

. . . .

Proof. Let $H = \{x^n : n \in \mathbb{Z}\} \subseteq G$. We verify the subgroup conditions (cf. Ex. 26).

. . . .

Nonempty (and identity present).

Since $0 \in \mathbb{Z}$, we have $x^0 = 1 \in H$. Thus $H \neq \varnothing$ and $1 \in H$.

. . . .

Closure under the operation.

Take arbitrary $a, b \in H$. Then $a = x^m$ and $b = x^n$ for some $m, n \in \mathbb{Z}$. Using the exponent law from Ex. 19,

$$ab = x^m x^n = x^{m+n} \in H.$$

. . . .

Closure under inverses.

Let $a \in H$ with $a = x^m$. By Ex. 19,

$$a^{-1} = (x^m)^{-1} = x^{-m} \in H.$$

. . . .

Associativity is inherited from G (the operation is the same). With $1 \in H$, closure, and inverses established, H is a subgroup of G. □

Exercise 28 (D&F §1.1, Ex. 28)**.** *Let* $(A, \cdot)$ *and* $(B, \circ)$ *be groups and let* $A \times B$ *be their direct product. Verify all the group axioms for* $A \times B$*:*

(a) prove that the associative law holds;

(b) prove that $(1, 1)$ *is the identity of* $A \times B$*;*

(c) prove that the inverse of (a, b) *is* (a^{-1}, b^{-1})*.*

. . . .

Intuition. The rule on $A \times B$ is *componentwise*:

$$(a_1, b_1) \cdot_{A\times B} (a_2, b_2) \;=\; (a_1 \cdot a_2,\ b_1 \circ b_2).$$

Since A and B already know how to associate, where their identities live, and how to invert, doing everything in parallel in each coordinate should inherit all axioms immediately.

. . . .

Proof. The binary operation on $A \times B$ is defined by

$$(a_1, b_1)(a_2, b_2) := (a_1 \cdot a_2,\ b_1 \circ b_2).$$

(Here 1 denotes the identity in the relevant group—context determines whether in A or in B.)

. . . .

Closure.

If $(a_1, b_1), (a_2, b_2) \in A \times B$, then $a_1 \cdot a_2 \in A$ and $b_1 \circ b_2 \in B$, hence

$$(a_1, b_1)(a_2, b_2) = (a_1 \cdot a_2,\ b_1 \circ b_2) \in A \times B.$$

. . . .

(a) Associativity.

For $(a_i, b_i) \in A \times B$ $(i = 1, 2, 3)$,

$$\begin{aligned} (a_1, b_1)\big((a_2, b_2)(a_3, b_3)\big) &= (a_1, b_1)\,(a_2 \cdot a_3,\ b_2 \circ b_3) \\ &= \big(a_1 \cdot (a_2 \cdot a_3),\ b_1 \circ (b_2 \circ b_3)\big) \\ &= \big((a_1 \cdot a_2) \cdot a_3,\ (b_1 \circ b_2) \circ b_3\big) \\ &= (a_1 \cdot a_2,\ b_1 \circ b_2)\,(a_3, b_3) \\ &= \big((a_1, b_1)(a_2, b_2)\big)(a_3, b_3), \end{aligned}$$

using associativity in A and in B in the middle equality.

. . . .

(b) Identity.

Let $(1, 1)$ denote the pair of identities from A and B. For any $(a, b) \in A \times B$,

$$(a, b)(1, 1) = (a \cdot 1,\ b \circ 1) = (a, b), \qquad (1, 1)(a, b) = (1 \cdot a,\ 1 \circ b) = (a, b).$$

Thus $(1, 1)$ is a two-sided identity in $A \times B$.

. . . .

(c) Inverses.

For $(a, b) \in A \times B$ let (a^{-1}, b^{-1}) be the componentwise inverse. Then

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

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

so (a^{-1}, b^{-1}) is the two-sided inverse of (a, b).

. . . .

Therefore $A \times B$ satisfies closure, associativity, has identity $(1, 1)$, and every element has an inverse; hence $A \times B$ is a group under componentwise multiplication, as required. □

Exercise 29 (D&F §1.1, Ex. 29)**.** *Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.*

. . . .

Intuition. The product law on $A \times B$ is componentwise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \cdot a_2,\ b_1 \circ b_2).$$

So (a_1, b_1) commuting with (a_2, b_2) is exactly the pair of statements $a_1 \cdot a_2 = a_2 \cdot a_1$ in A and $b_1 \circ b_2 = b_2 \circ b_1$ in B.

. . . .

Proof. We prove both directions.

. . . .

(⇒) If $A \times B$ is abelian, then A and B are abelian.

Assume $(a_1, b_1)(a_2, b_2) = (a_2, b_2)(a_1, b_1)$ for all $a_i \in A$, $b_i \in B$. Then

$$(a_1 \cdot a_2,\ b_1 \circ b_2) = (a_2 \cdot a_1,\ b_2 \circ b_1).$$

Equality of ordered pairs forces equality in each component, hence

$$a_1 \cdot a_2 = a_2 \cdot a_1 \quad \text{and} \quad b_1 \circ b_2 = b_2 \circ b_1$$

for all choices of a_i, b_i. Therefore A and B are abelian.

. . . .

(⇐) If A and B are abelian, then $A \times B$ is abelian.

Assume $a_1 \cdot a_2 = a_2 \cdot a_1$ in A and $b_1 \circ b_2 = b_2 \circ b_1$ in B for all elements. Then for any $(a_1, b_1), (a_2, b_2) \in A \times B$,

$$(a_1, b_1)(a_2, b_2) = (a_1 \cdot a_2,\ b_1 \circ b_2) = (a_2 \cdot a_1,\ b_2 \circ b_1) = (a_2, b_2)(a_1, b_1).$$

Thus $A \times B$ is abelian.

. . . .

Hence $A \times B$ is abelian if and only if both A and B are abelian. □

Exercise 30 (D&F §1.1, Ex. 30)**.** *Prove that the elements $(a, 1)$ and $(1, b)$ of $A \times B$ commute and deduce that the order of (a, b) is the least common multiple of $|a|$ and $|b|$.*

. . . .

Intuition. In the direct product, everything is *componentwise*. So $(a, 1)$ acts only on the A-coordinate and $(1, b)$ only on the B-coordinate—hence they commute. Powers also split: $(a, b)^n = (a^n, b^n)$. Therefore the smallest n killing both coordinates is exactly $\operatorname{lcm}(|a|, |b|)$.

. . . .

Proof. Work in $A \times B$ with the componentwise law $(a_1, b_1)(a_2, b_2) = (a_1a_2,\ b_1b_2)$.

. . . .

(1) $(a, 1)$ and $(1, b)$ commute.

Compute both products:

$$(a, 1)(1, b) = (a \cdot 1,\ 1 \cdot b) = (a, b),$$

$$(1, b)(a, 1) = (1 \cdot a,\ b \cdot 1) = (a, b).$$

Thus $(a, 1)(1, b) = (1, b)(a, 1)$.

. . . .

(2) Powers split: $(a, b)^n = (a^n, b^n)$ for all $n \in \mathbb{Z}_{>0}$.

Induction on n. For $n = 1$ it is immediate. If $(a, b)^k = (a^k, b^k)$, then

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

Hence the formula holds for all $n \geq 1$.

. . . .

(3) Deduce the order of (a, b).

Assume $|a|, |b| < \infty$ and set $\ell = \operatorname{lcm}(|a|, |b|)$. Then

$$(a, b)^\ell = (a^\ell, b^\ell) = (1, 1),$$

since $|a| \mid \ell$ and $|b| \mid \ell$. Therefore $|(a, b)| \le \ell$.

Conversely, if $(a, b)^k = (1, 1)$, then by (2)

$$(a^k, b^k) = (1, 1) \quad \Longrightarrow \quad a^k = 1 \text{ and } b^k = 1,$$

so $|a| \mid k$ and $|b| \mid k$. Thus k is a common multiple of $|a|$ and $|b|$, hence $\ell \le k$. Therefore $|(a, b)| = \ell = \operatorname{lcm}(|a|, |b|)$.

. . . .

Conclusion. $(a, 1)$ and $(1, b)$ commute, and $|(a, b)| = \operatorname{lcm}(|a|, |b|)$ (for finite $|a|, |b|$). □

Exercise 31 (D&F §1.1, Ex. 31). *Prove that any finite group G of even order contains an element of order 2.*

. . . .

Intuition. Pair every element g that is *not* its own inverse with g^{-1}. These come in disjoint 2-element packets. Since $|G|$ is even, what remains after removing all such packets still has even size—and it contains e. Hence there is some nonidentity a with $a = a^{-1}$, i.e. $a^2 = e$.

. . . .

Proof. Let G be finite with $|G|$ even. Define

$$t(G) \;=\; \{\, g \in G \;:\; g \neq g^{-1} \,\}.$$

Step 1: $t(G)$ has even cardinality (pairing by inverses).
Consider the map $\iota : t(G) \to t(G)$ given by $\iota(g) = g^{-1}$. If $g \in t(G)$ then $g \neq g^{-1}$, hence $g^{-1} \neq (g^{-1})^{-1} = g$, so $g^{-1} \in t(G)$. Moreover,

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

so ι is an involution with no fixed points on $t(G)$. Thus $t(G)$ is a disjoint union of 2-element sets $\{g, g^{-1}\}$, so $|t(G)|$ is even.

. . . .

Step 2: There exists a nonidentity element equal to its own inverse.
Since $|G|$ is even and $|t(G)|$ is even, their difference

$$|G \setminus t(G)| \;=\; |G| - |t(G)|$$

is even. Note $e \notin t(G)$ because $e = e^{-1}$, hence $e \in G \setminus t(G)$ and $G \setminus t(G) \neq \varnothing$. Because $|G \setminus t(G)|$ is even and already contains e, there exists $a \in G \setminus t(G)$ with $a \neq e$.

By definition of $G \setminus t(G)$ we have $a = a^{-1}$, hence

$$a^2 \;=\; a \cdot a \;=\; e, \qquad \text{with } a \neq e.$$

Therefore a has order 2.

This proves that every finite group of even order contains an element of order 2. □

Exercise 32 (D&F §1.1, Ex. 32)**.** *If x is an element of finite order n in a group G, prove that the elements*

$$1,\ x,\ x^2,\ \dots,\ x^{n-1}$$

are all distinct. Deduce that $|x| \le |G|$.

. . . .

Intuition. "Order n" means $x^n = 1$ and no smaller positive power is 1. If two powers x^s and x^t (with $s < t$) were equal, canceling x^s would give $x^{t-s} = 1$ with $1 \le t - s < n$, contradicting the minimality of n.

. . . .

Proof. Assume $|x| = n < \infty$, so $x^n = 1$ and $x^m \ne 1$ for every integer m with $1 \le m < n$.

. . . .

Distinctness of $1, x, \dots, x^{n-1}$.

Suppose for contradiction that $x^s = x^t$ for some integers with $0 \le s < t \le n-1$. Right–multiply both sides by x^{-s}:

$$x^s x^{-s} = x^t x^{-s}.$$

Compute each side explicitly:

$$1 = x^t x^{-s} = x^{\,t+(-s)} = x^{\,t-s}.$$

Since $t - s \ge 1$ and $t - s \le n - 1$, this says $x^m = 1$ for some integer m with $1 \le m < n$, contradicting the definition of n as the order of x. Therefore no such $s < t$ exist, and

$$1,\ x,\ x^2,\ \dots,\ x^{n-1}$$

are pairwise distinct.

. . . .

Deduction: $|x| \leq |G|$.

The cyclic subgroup generated by x is

$$\langle x \rangle = \{x^k : \ k \in \mathbb{Z}\}.$$

Because $x^n = 1$ and the n elements $1, x, \ldots, x^{n-1}$ are distinct, we have

$$|\langle x \rangle| = n = |x|.$$

Since $\langle x \rangle \subseteq G$, it follows that

$$|x| = |\langle x \rangle| \leq |G|.$$

□

Exercise 33 (D&F §1.1, Ex. 33)**.** *Let x be an element of finite order n in the group G.*

1. *Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.*
2. *Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.*

. . . .

Intuition. "x^i equals its inverse" means $x^i = x^{-i}$, which forces

$$x^i \cdot x^i = x^i x^{-i} = 1 \quad \Longrightarrow \quad x^{2i} = 1.$$

So the order n must divide $2i$. If n is *odd*, this makes $n \mid i$ (impossible for $1 \leq i \leq n-1$). If n is *even*, say $n = 2k$, then $2k \mid 2i$ means $k \mid i$, leaving only the midpoint $i = k$ among $1 \leq i < 2k$.

. . . .

Proof. Assume throughout that $|x| = n < \infty$, so $x^n = 1$ and n is minimal with this property.

. . . .

(a) If n is odd, then $x^i \neq x^{-i}$ for $1 \leq i \leq n-1$.

Suppose, toward a contradiction, that $x^i = x^{-i}$ for some i with $1 \leq i \leq n-1$. Multiply both sides on the right by x^i:

$$x^i \cdot x^i = x^{-i} \cdot x^i.$$

Compute both sides explicitly:

$$x^{2i} = x^{-i+i} = x^0 = 1.$$

Thus $x^{2i} = 1$, so the order n divides $2i$:

$$n \mid 2i.$$

Since n is odd, $\gcd(n, 2) = 1$, hence from $n \mid 2i$ it follows that $n \mid i$. But $1 \leq i \leq n-1$, contradiction. Therefore no such i exists, i.e. $x^i \neq x^{-i}$ for all $i = 1, \ldots, n-1$.

. . . .

(b) If $n = 2k$ and $1 \leq i < n$, then $x^i = x^{-i} \iff i = k$.

($\Rightarrow$) Assume $x^i = x^{-i}$ with $1 \leq i < n = 2k$. As above,

$$x^{2i} = 1 \quad \Longrightarrow \quad n \mid 2i \quad \Longrightarrow \quad 2k \mid 2i \quad \Longrightarrow \quad k \mid i.$$

Since $1 \leq i < 2k$ and $k \mid i$, the only possibility is $i = k$.
($\Leftarrow$) Conversely, if $i = k$ then

$$x^i = x^k, \qquad x^{-i} = x^{-k},$$

and

$$x^k \cdot x^k = x^{2k} = x^n = 1.$$

Thus x^k is its own inverse, i.e. $x^k = x^{-k}$.

. . . .

Both statements follow. □

Exercise 34 (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. Assume $|x| = \infty$. We show that if $x^m = x^n$ for integers m, n, then $m = n$.

Suppose $x^m = x^n$. Without loss of generality take $n \leq m$. Right–multiply by x^{-n}:

$$x^m = x^n \quad \Longrightarrow \quad x^m x^{-n} = x^n x^{-n}.$$

Compute each side:

$$x^{m-n} = x^{n-n} = x^0 = 1.$$

If $m > n$ then $m - n \in \mathbb{Z}_{>0}$ and $x^{m-n} = 1$ contradicts $|x| = \infty$. Hence $m \not> n$, so $m = n$.

Therefore no two distinct integers yield the same power, i.e. the elements $\{x^n : n \in \mathbb{Z}\}$ are all distinct. □

Exercise 35 (D&F §1.1, Ex. 35)**.** *If x is an element of finite order n in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all the distinct elements of the cyclic subgroup of G generated by x).*

. . . .

Intuition. "Order n" means $x^n = 1$. For any integer exponent k, divide k by n: $k = qn + r$ with $0 \leq r < n$. Then $x^k = x^{qn+r} = (x^n)^q x^r = 1^q x^r = x^r$. Thus every power collapses into the first n powers $1, x, \ldots, x^{n-1}$.

. . . .

Proof. Assume $|x| = n < \infty$, so $x^n = 1$. Let $k \in \mathbb{Z}$ be arbitrary. By the Division Algorithm there exist unique integers q and r with

$$k = qn + r \qquad \text{and} \qquad 0 \leq r < n.$$

Compute:

$$x^k = x^{qn+r} = x^{qn}\, x^r = (x^n)^q\, x^r = 1^q\, x^r = x^r,$$

where $0 \leq r < n$. Hence x^k equals one of $1, x, x^2, \ldots, x^{n-1}$.

Since in Exercise 32 we showed that $1, x, \ldots, x^{n-1}$ are pairwise distinct when $|x| = n$, these are precisely the n distinct elements of the cyclic subgroup $\langle x \rangle = \{x^m : m \in \mathbb{Z}\}$. □

Exercise 36 (D&F §1.1, Ex. 36)**.** *Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4. Use the cancellation laws to show that there is a unique group table for G. Deduce that G is abelian.*

. . . .

Intuition. With $|G| = 4$ and no element of order 4, every nonidentity has order ≤ 3. An even-order group has an element of order 2, and once one involution is present, cancellation forces all remaining products. A short check shows every nonidentity must square to 1, yielding the Klein four group.

. . . .

Proof. Let $G = \{1, a, b, c\}$ and assume no element has order 4.

. . . .

Step 1: Pick an involution.

Since $|G|$ is even, there exists $x \in G$ with $x^2 = 1$. Relabel so that

$$a^2 = 1.$$

. . . .

Step 2: Determine ab, ba, ac, ca by cancellation.

For ab there are four possibilities in $\{1, a, b, c\}$.

$$ab \neq 1 \quad (\text{else } b = a^{-1} = a),$$

$$ab \neq a \quad (\text{else left–cancel } a \text{ to get } b = 1),$$

$$ab \neq b \quad (\text{else right–cancel } b \text{ to get } a = 1).$$

Hence

$$ab = c.$$

The same argument (interchanging the roles of left/right cancellation and of b, c) gives

$$ba = c, \qquad ac = b, \qquad ca = b.$$

Step 3: Relate b^2 and c^2, then rule out order 3.

Using $b = ca$ and $b = ac$ we compute

$$b^2 = (ca)(ac) = c(a^2)c = c \cdot 1 \cdot c = c^2,$$

so

$$b^2 = c^2.$$

If $b^2 \neq 1$, then $|b| = 3$ (orders are ≤ 3 and $b \neq 1$), hence $b^3 = 1$. Then

$$a = a\,b^3 = (ab)\,b^2 = c\,b^2 = c\,c^2 = c^3.$$

Since $a \neq 1$, we have $c^3 \neq 1$, so $|c| \neq 3$. Thus $|c| = 2$ and $c^2 = 1$, and by $b^2 = c^2$ we get

$$b^2 = 1.$$

Step 4: Finish the table and read off commutativity.

We already have $a^2 = b^2 = c^2 = 1$, and from Step 2,

$$ab = ba = c, \qquad ac = ca = b.$$

For the remaining products, use cancellation again (e.g. $bc \neq 1, b, c$ so $bc = a$; similarly $cb = a$). The unique table is therefore:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

This table is symmetric about the diagonal, so $xy = yx$ for all $x, y \in G$; hence G is abelian.

. . . .

Thus there is a unique group table under the hypotheses, and $G \cong C_2 \times C_2$. □

1.2: Dihedral Groups

Exercise 37 (D&F §1.2, Ex. 1)**.** *Compute the order of each of the elements in the following groups:*

(a) D_6

(b) D_8

(c) D_{10}

. . . .

Intuition. In $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$, the subgroup $\langle r \rangle$ is cyclic of order n, and each reflection sr^k has order 2. Thus: identities have order 1, rotations have order dividing n, and reflections have order 2. The only subtlety lies in identifying which powers r^k have smaller order.

. . . .

Proof. Step 1: Elements of D_6*.*

Here $n = 3$, so $D_6 = \{1, r, r^2, s, sr, sr^2\}$.

$$|1| = 1, \quad |r| = 3, \quad |r^2| = 3, \quad |s| = |sr| = |sr^2| = 2.$$

. . . .

Step 2: Elements of D_8*.*

Here $n = 4$, so $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

$|1| = 1, \quad |r| = 4, \quad |r^2| = 2, \quad |r^3| = 4, \quad |s| = |sr| = |sr^2| = |sr^3| = 2.$

. . . .

Step 3: Elements of D_{10}*.*

Here $n = 5$, a prime. So $\langle r \rangle$ is cyclic of order 5, and each nontrivial r^k $(k = 1, \dots, 4)$ has order 5. Each reflection has order 2.

$|1| = 1, \quad |r| = |r^2| = |r^3| = |r^4| = 5, \quad |s| = |sr| = |sr^2| = |sr^3| = |sr^4| = 2.$

. . . .

Thus in each case the rotation subgroup has the expected orders dividing n, and all reflections square to 1. □

Exercise 38 (D&F §1.2, Ex. 2)**.** *Use the generators and relations for $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1}\rangle$ to show that if x is any element of D_{2n} which is not a power of r, then*

$$rx = xr^{-1}.$$

. . . .

Intuition. Every non-rotation in D_{2n} is a reflection of the form sr^k. The braid relation $rs = sr^{-1}$ lets us move r past s at the expense of inverting the r–power, which exactly yields the identity $r(sr^k) = (sr^k)r^{-1}$.

. . . .

Proof. Step 1: Normal form.

Each element of D_{2n} is either a rotation r^ℓ or a reflection sr^k. Hence, if x is not a power of r, we may write $x = sr^k$ for some integer k.

. . . .

Step 2: Push r past s using $rs = sr^{-1}$.

Compute

$$r\,x \;=\; r\,(sr^k) \;=\; (rs)\,r^k \;=\; (sr^{-1})\,r^k \;=\; s\,r^{k-1}.$$

On the other hand,

$$x\,r^{-1} \;=\; (sr^k)\,r^{-1} \;=\; s\,r^{k-1}.$$

Thus $r\,x = x\,r^{-1}$.

. . . .

Therefore, for any non-rotation $x \in D_{2n}$, we have $rx = xr^{-1}$ as claimed. □

Exercise 39 (D&F §1.2, Ex. 3)**.** *Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order* 2*. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order* 2*.*

....

Intuition. Every non-rotation in D_{2n} is a reflection sr^k. The braid relation $rs = sr^{-1}$ implies $r^k s = sr^{-k}$, and this makes $(sr^k)^2 = 1$. Since $r = s(sr)$, the pair s, sr generates all rotations and hence the whole group.

....

Proof. Step 1: Normal form.

In $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$, each element is either a rotation r^ℓ or a reflection sr^k. Thus a non-rotation has the form sr^k.

....

Step 2: Every reflection has order 2*.*

From $rs = sr^{-1}$, by induction we get $r^k s = sr^{-k}$ for all integers k. Hence

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

Thus every element not a power of r has order 2.

....

Step 3: D_{2n} is generated by s and sr.

First, $r = s(sr)$, so $r \in \langle s, sr \rangle$ and hence $\langle r \rangle \subseteq \langle s, sr \rangle$. Since $s \in \langle s, sr \rangle$ as well, every reflection $sr^k = s\, r^k$ also lies in $\langle s, sr \rangle$. Therefore $\langle s, sr \rangle$ contains all rotations and all reflections, i.e. it equals D_{2n}. Moreover, $s^2 = (sr)^2 = 1$ by Step 2, so both generators have order 2.

....

Hence all non-rotations have order 2, and $D_{2n} = \langle s, sr \rangle$ with $|s| = |(sr)| = 2$. $\square$

Exercise 40 (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: $z = r^k$ has order 2.

Since $r^n = 1$ with $n = 2k$, we have $z^2 = r^{2k} = 1$. By §1.1, Ex. 33 (even case), $r^k = r^{-k}$.

. . . .

Step 2: z commutes with every element.

Every element is r^ℓ or sr^ℓ. For rotations,

$$zr^\ell = r^{k+\ell} = r^{\ell+k} = r^\ell z.$$

For s, using $r^m s = sr^{-m}$ and $r^k = r^{-k}$,

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

Hence z commutes with r^ℓ and sr^ℓ for all ℓ.

. . . .

Step 3: No reflection is central when $n \geq 4$.

Let $x = sr^t$. Then

$$rx = rsr^t = sr^{t-1}, \qquad xr = sr^{t+1}.$$

If $rx = xr$ we would have $sr^{t-1} = sr^{t+1}$, hence $r^2 = 1$, contradicting $n \geq 4$. Thus no reflection commutes with all elements.

. . . .

Step 4: The only central rotations are 1 *and* r^k*.*

If r^t is central, then $r^t s = sr^t$, so $sr^{-t} = sr^t$ and hence $r^{2t} = 1$. With $n = 2k$, §1.1, Ex. 33 yields $t \equiv 0$ or $t \equiv k \pmod{n}$. Thus the only nonidentity central rotation is r^k.

. . . .

Combining Steps 3–4, the only nonidentity element commuting with all of D_{2n} is $z = r^k$. □

Exercise 41 (D&F §1.2, Ex. 5)**.** *If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.*

Intuition. By D&F §1.1, Ex. 33 (odd case), no nontrivial power r^t equals its inverse when $|r| = n$ is odd, so no nonidentity rotation can centralize s. Reflections never commute with r (same calculation as in Ex. 4). Hence only 1 is central.

Proof. Step 1: No reflection is central (for $n \geq 3$).

Let $x = sr^t$. Then

$$rx = rsr^t = sr^{t-1}, \qquad xr = sr^{t+1}.$$

If $rx = xr$ we obtain $sr^{t-1} = sr^{t+1}$, hence $r^2 = 1$, contradicting $n \geq 3$. Thus no reflection commutes with all elements.

Step 2: The only central rotation is 1.

Let r^t commute with s. From $r^t s = sr^t$ and $rs = sr^{-1}$ we get

$$sr^{-t} = sr^t \implies r^{2t} = 1.$$

Since $|r| = n$ is odd, D&F §1.1, Ex. 33 implies $n \mid t$, so $r^t = 1$. Hence no nonidentity rotation centralizes D_{2n}.

Combining Steps 1–2, the center of D_{2n} (with n odd, $n \geq 3$) is $\{1\}$. □

Exercise 42 (D&F §1.2, Ex. 6). *Let x and y be elements of order 2 in a group G. Prove that if $t = xy$ then*

$$t\,x \;=\; x\,t^{-1}.$$

(So if $n = |xy| < \infty$, then x and t satisfy the same relations in G as s and r do in D_{2n}.)

. . . .

Intuition. Because $x^2 = y^2 = 1$, we have $x = x^{-1}$ and $y = y^{-1}$. Setting $t = xy$, the product $t^{-1} = y^{-1}x^{-1} = yx$ reverses the factors. A short shuffle shows $tx = xyx = x\,t^{-1}$.

. . . .

Proof. Step 1: Compute t^{-1}.

With $t = xy$ and $x^2 = y^2 = 1$,

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

. . . .

Step 2: Derive $tx = xt^{-1}$.

Using $x = x^{-1}$ and $y = y^{-1}$,

$$tx = xyx = x\,y^{-1}x^{-1} = x\,(xy)^{-1} = x\,t^{-1}.$$

Hence $tx = xt^{-1}$.

. . . .

Step 3: Dihedral relations (finite order case).

If $n = |t| = |xy| < \infty$, then $x^2 = 1$, $t^n = 1$, and from Step 2,

$$xt = t^{-1}x \quad\Longleftrightarrow\quad tx = xt^{-1}.$$

Thus x and t satisfy the relations of the standard generators s and r of D_{2n}.

. . . .

This proves the claim. □

Exercise 43 (D&F §1.2, Ex. 7)**.** *Show that $\langle a, b \mid a^2 = b^2 = (ab)^n = 1\rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and b follow from those for r and s.]*

. . . .

Intuition. Take $a = s$ and $b = sr$. Then $ab = s(sr) = r$, so $(ab)^n = r^n = 1$, and $b^2 = (sr)^2 = 1$. Conversely, starting with $a^2 = b^2 = 1$ and $(ab)^n = 1$, set $s = a$ and $r = ab$; then $b = sr$ and $rs = sr^{-1}$ follows from $b^2 = 1$.

. . . .

Proof. Step 1: From $\langle a, b \mid a^2 = b^2 = (ab)^n = 1\rangle$ derive the dihedral relations.

Assume $a^2 = b^2 = 1$ and $(ab)^n = 1$. Define

$$s := a, \qquad r := ab.$$

Then

$$r^n = (ab)^n = 1, \qquad s^2 = a^2 = 1.$$

Also $b = a^{-1}(ab) = sr$ (since $a^{-1} = a$). Using $b^2 = 1$:

$$1 = b^2 = (sr)(sr) = s(rs)r.$$

Left–multiply by s and right–multiply by r^{-1} to obtain

$$rs = sr^{-1}.$$

Thus r, s satisfy $r^n = 1$, $s^2 = 1$, and $rs = sr^{-1}$, i.e. the defining relations of D_{2n}.

. . . .

Step 2: From the dihedral relations recover $a^2 = b^2 = (ab)^n = 1$.

Conversely, assume $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$ and set

$$a := s, \qquad b := sr.$$

Then

$$a^2 = s^2 = 1, \qquad b^2 = (sr)(sr) = s(rs)r = s(sr^{-1})r = s^2r^{-1}r = 1.$$

Moreover,

$$ab = s(sr) = s^2r = r \quad \Longrightarrow \quad (ab)^n = r^n = 1.$$

Hence a, b satisfy precisely $a^2 = b^2 = (ab)^n = 1$.

. . . .

Steps 1–2 show the two presentations are equivalent; therefore

$$\langle a, b \mid a^2 = b^2 = (ab)^n = 1 \rangle \ \cong \ D_{2n}.$$

□

Exercise 44 (D&F §1.2, Ex. 8)**.** *Find the order of the cyclic subgroup of D_{2n} generated by r.*

Intuition. In $D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle$, r is rotation by $2\pi/n$. The subgroup $\langle r \rangle$ consists of all rotations by integer multiples of $2\pi/n$, namely $1, r, \dots, r^{\,n-1}$ — n distinct elements.

Proof. Step 1: Describe $\langle r \rangle$.

Let $G = \langle r \rangle$. Then every element of G is r^k for some $k \in \mathbb{Z}$.

Step 2: Geometric interpretation.

If $k > 0$, r^k is rotation by $2k\pi/n$; if $k < 0$, r^k is rotation by $-2(-k)\pi/n$.

Step 3: Reduce exponents modulo n.

If $|k| \geq n$, the rotation r^k equals r^ℓ for some $0 \leq \ell < n$ (same angle modulo 2π). Hence

$$G = \{\, 1, r, r^2, \dots, r^{\,n-1} \,\}.$$

Step 4: Count.

The rotations $1, r, \dots, r^{\,n-1}$ are distinct, so $|G| = n$.

Therefore the cyclic subgroup $\langle r \rangle$ has order n. □

Exercise 45 (D&F §1.2, Ex. 9)**.** *Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.*

. . . .

Intuition. Label the 4 vertices. A rotation is determined by where it sends an ordered adjacent pair of vertices: 4 choices for the first vertex's image, then 3 choices for the second (adjacent to the first). The remaining vertices follow uniquely.

. . . .

Proof. Step 1: Fix the image of one vertex.

Label the vertices $\{1, 2, 3, 4\}$. A rotation sends vertex 1 to any of the 4 vertices: 4 choices.

. . . .

Step 2: Fix the image of an adjacent vertex.

Each vertex of a tetrahedron is adjacent to the other 3. Once the image of 1 is chosen, the image of 2 must be one of the 3 vertices adjacent to the image of 1: 3 choices.

. . . .

Step 3: Uniqueness and count.

With the images of 1 and 2 fixed, the positions of the remaining two vertices are forced (rigid motion). Hence the number of rotations is $4 \cdot 3 = 12$.

. . . .

Therefore $|G| = 12$. □

Exercise 46 (D&F §1.2, Ex. 10)**.** *Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.*

. . . .

Intuition. A rotation is determined by the images of an ordered adjacent pair of vertices: 8 choices for the first vertex's image and, once chosen, 3 choices for an adjacent second.

. . . .

Proof. Step 1: Choose the image of one vertex.

Label the 8 vertices. A rotation may send a fixed vertex (say 1) to any of the 8 vertices: 8 choices.

. . . .

Step 2: Choose the image of an adjacent vertex.

Each cube vertex has exactly 3 adjacent vertices. After fixing the image of 1, the image of an adjacent vertex (say 2) must be one of the 3 neighbors of the chosen image of 1: 3 choices.

. . . .

Step 3: Determination and count.

With the images of an ordered adjacent pair fixed, the rotation is uniquely determined (rigidity of the cube). Hence the number of rotations is $8 \cdot 3 = 24$.

. . . .

Therefore $|G| = 24$. □

Exercise 47 (D&F §1.2, Ex. 11)**.** *Let G be the group of rigid motions in $\mathbb{R}^3$ of an octahedron. Show that $|G| = 24$.*

. . . .

Intuition. A rotation is determined by the images of an ordered adjacent pair of vertices: 6 choices for the first vertex's image and, once chosen, 4 choices for an adjacent second.

. . . .

Proof. Step 1: Choose the image of one vertex.

An octahedron has 6 vertices. A rotation may send a fixed vertex to any of the 6 vertices: 6 choices.

. . . .

Step 2: Choose the image of an adjacent vertex.

Each octahedron vertex has exactly 4 adjacent vertices. After fixing the image of the first vertex, the image of an adjacent second must be one of those 4 neighbors: 4 choices.

. . . .

Step 3: Determination and count.

With the images of an ordered adjacent pair fixed, the rotation is uniquely determined. Therefore

$$|G| = 6 \cdot 4 = 24.$$

. . . .

Thus the rotation group of the octahedron has order 24. □

Exercise 48 (D&F §1.2, Ex. 12)**.** *Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.*

. . . .

Intuition. A rotation is determined by the images of an ordered adjacent pair of vertices: 20 choices for the first vertex's image and, once chosen, 3 choices for an adjacent second.

. . . .

Proof. Step 1: Choose the image of one vertex.

A dodecahedron has 20 vertices. A rotation may send a fixed vertex to any of the 20 vertices: 20 choices.

. . . .

Step 2: Choose the image of an adjacent vertex.

Each vertex has exactly 3 adjacent (neighboring) vertices. After fixing the image of the first vertex, the image of an adjacent second must be one of those 3 neighbors: 3 choices.

. . . .

Step 3: Determination and count.

With the images of an ordered adjacent pair fixed, the rotation is uniquely determined. Therefore

$$|G| = 20 \cdot 3 = 60.$$

. . . .

Thus the rotation group of the dodecahedron has order 60. □

Exercise 49 (D&F §1.2, Ex. 13)**.** *Let G be the group of rigid motions in $\mathbb{R}^3$ of an icosahedron. Show that $|G| = 60$.*

. . . .

Intuition. A rotation is determined by the images of an ordered adjacent pair of vertices: 12 choices for the first vertex's image and, once chosen, 5 choices for an adjacent second.

. . . .

Proof. Step 1: Choose the image of one vertex.

An icosahedron has 12 vertices. A rotation may send a fixed vertex to any of the 12 vertices: 12 choices.

. . . .

Step 2: Choose the image of an adjacent vertex.

Each vertex has exactly 5 adjacent (neighboring) vertices. After fixing the image of the first vertex, the image of an adjacent second must be one of those 5 neighbors: 5 choices.

. . . .

Step 3: Determination and count.

With the images of an ordered adjacent pair fixed, the rotation is uniquely determined. Therefore

$$|G| = 12 \cdot 5 = 60.$$

. . . .

Thus the rotation group of the icosahedron has order 60. □

Exercise 50 (D&F §1.2, Ex. 14)**.** *Find a set of generators for $\mathbb{Z}$.*

. . . .

Intuition. Viewing $(\mathbb{Z}, +)$ as a cyclic group, one element suffices: repeatedly add 1 (or subtract it) to reach any integer.

. . . .

Proof. Step 1: $\langle 1 \rangle = \mathbb{Z}$.

The subgroup generated by 1 under addition is

$$\langle 1 \rangle = \{k \cdot 1 : k \in \mathbb{Z}\} = \{\, k \in \mathbb{Z} \,\} = \mathbb{Z}.$$

Indeed, for $n \geq 0$, $n = 1 + \cdots + 1$ (n times), and for $n < 0$, $n = (-1) + \cdots + (-1)$ ($|n|$ times), which also equals $(-|n|) \cdot 1$.

. . . .

Thus $\{1\}$ is a generating set for $\mathbb{Z}$ (equivalently, $\{-1\}$ also generates). □

Exercise 51 (D&F §1.2, Ex. 15)**.** *Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.*

. . . .

Intuition. As in the previous exercise, the class $\overline{1}$ generates additively; the single relation is $n\,\overline{1} = \overline{0}$.

. . . .

Proof. Step 1: Generator.
Every element is a residue class $\overline{k}$, and $\overline{k} = k\,\overline{1}$, so $\{\overline{1}\}$ generates $\mathbb{Z}/n\mathbb{Z}$.

. . . .

Step 2: Relation.
Since $n \equiv 0 \pmod{n}$, we have $\overline{n} = \overline{0}$, i.e. $n\,\overline{1} = \overline{0}$.

. . . .

Thus a presentation is $\langle\, \overline{1} \mid n\,\overline{1} = \overline{0}\,\rangle$. □

Exercise 52 (D&F §1.2, Ex. 16)**.** *Show that the group* $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1\rangle$ *is the dihedral group* D_4 *(where* x_1 *may be replaced by the letter* r *and* y_1 *by* s*).*

. . . .

Intuition. In D_4 we have $\langle r, s \mid r^2 = s^2 = 1,\ rs = sr^{-1}\rangle$, but $r^2 = 1$ gives $r = r^{-1}$, so $rs = sr$. That relation is equivalent to $(rs)^2 = 1$. With $x_1 = r$, $y_1 = s$, the two presentations match.

. . . .

Proof. Step 1: From the dihedral presentation to $(x_1y_1)^2 = 1$*.*

In D_4, $r^2 = s^2 = 1$ and $rs = sr^{-1}$. Since $r = r^{-1}$, we have $rs = sr$. Let $x_1 = r$, $y_1 = s$. Then

$$(x_1y_1)^2 = (rs)^2 = rsrs = r^2s^2 = 1.$$

. . . .

Step 2: From $(x_1y_1)^2 = 1$ *back to the dihedral relation.*

Assume $x_1^2 = y_1^2 = 1$ and $(x_1y_1)^2 = 1$, i.e. $x_1y_1x_1y_1 = 1$. Set $r = x_1$, $s = y_1$. Then $rsrs = 1$. Left–multiply by r and right–multiply by s:

$$r(rsrs)s = (rr)(ss) \ \Rightarrow\ rs = sr.$$

With $r^2 = 1$ we have $r = r^{-1}$, so $rs = sr^{-1}$, the dihedral braid relation. Together with $r^2 = s^2 = 1$, this is the standard presentation of D_4.

. . . .

Therefore $\langle x_1, y_1 \mid x_1^2 = y_1^2 = (x_1y_1)^2 = 1\rangle \cong D_4$. □

Exercise 53 (D&F §1.2, Ex. 17)**.** *Let*

$$X_{2n} \;=\; \langle\, x, y \mid x^n = y^2 = 1,\; xy = yx^2 \,\rangle.$$

(a) Show that if $n = 3k$, then X_{2n} has order 6, and it has the same generators and relations as D_6 when x is replaced by r and y by s.

(b) Show that if $(3, n) = 1$, then $x = 1$. Deduce that in this case $|X_{2n}| = 2$.

. . . .

Intuition. From the relations one can force the "hidden" identity $x = x^4$, hence $x^3 = 1$. When $3 \mid n$ this gives $r^3 = 1$ with $r = x$ and the braid becomes $rs = sr^{-1}$ (since $r^2 = r^{-1}$), i.e. the D_6 relations. If $(3, n) = 1$, combining $x^3 = 1$ and $x^n = 1$ forces $x = 1$, leaving only $\{1, y\}$ with $y^2 = 1$.

. . . .

Proof. Step 1: Derive $x^3 = 1$ from the presentation.

Using $y^2 = 1$ and $xy = yx^2$,

$$x = x \cdot y^2 = (xy)\, y = (yx^2)\, y.$$

Also $xy = yx^2$ implies $yxy = x^2$ (left–multiply by y and use $y^2 = 1$), hence $yx = x^2y$. Thus

$$(xy)\, y = (yx^2)\, y = (yx)(xy) = (x^2y)(xy) = x^2(yx)y = x^2(x^2y)y = x^4.$$

Therefore $x = x^4$, and by cancellation $x^3 = 1$.

. . . .

Step 2: Case $n = 3k$. Identify $X_{2n} \cong D_6$.

Set $r := x$ and $s := y$. From Step 1, $r^3 = 1$ and from the presentation $s^2 = 1$. Moreover $xy = yx^2$ becomes

$$rs = sr^2 = sr^{-1} \qquad (\text{since } r^3 = 1 \Rightarrow r^2 = r^{-1}).$$

Hence r, s satisfy $r^3 = s^2 = 1$ and $rs = sr^{-1}$, the defining relations of D_6. Thus $X_{2n} \cong D_6$ and $|X_{2n}| = 6$.

. . . .

Step 3: Case $(3, n) = 1$. *Collapse to order* 2.

From Step 1 and $x^n = 1$ we have $x^3 = x^n = 1$. If $n = 3k + 1$, then

$$x = (x^3)^k x = x^{3k+1} = x^n = 1.$$

If $n = 3k + 2$, then

$$x^{-1} = (x^3)^{k+1} x^{-1} = x^{3k+2} = x^n = 1,$$

so again $x = 1$. Therefore $X_{2n} = \{1, y\}$ with $y^2 = 1$, and $|X_{2n}| = 2$.

. . . .

This proves parts (a) and (b). □

Exercise 54 (D&F §1.2, Ex. 18)**.** *Let $Y = \langle u, v \mid u^4 = v^3 = 1,\ uv = v^2u^2\rangle$.*

(a) Show that $v^2 = v^{-1}$.

(b) Show that v commutes with u^3.

(c) Show that v commutes with u.

(d) Show that $uv = 1$.

(e) Show that $u = 1$, deduce that $v = 1$, and conclude that $Y = 1$.

. . . .

Intuition. Use $v^3 = 1$ to get $v^2 = v^{-1}$. Then compute v^2u^3v and reduce via the defining relation $uv = v^2u^2$ to u^3, which forces v to commute with u^3. From $u^4 = 1$ we have $u^9 = u$, so commuting with u^3 yields commuting with u. With u and v commuting, a short product manipulation collapses uv to 1, and then $u = v = 1$.

. . . .

Proof. Step (a): $v^2 = v^{-1}$.

Since $v^3 = 1$, we have $v \cdot v^2 = 1$, whence $v^2 = v^{-1}$.

. . . .

Step (b): v commutes with u^3.

Compute

$$v^2u^3v = (v^2u^2)(uv) = (uv)(v^2u^2) = u\,v^3\,u^2 = u^3,$$

using $uv = v^2u^2$ twice and $v^3 = 1$. Hence $u^3 = v^2u^3v$. Left–multiply by v:

$$vu^3 = v(v^2u^3v) = v^3u^3v = u^3v,$$

so v commutes with u^3.

. . . .

Step (c): v commutes with u.

From $u^4 = 1$ we get $u^9 = u$. Using commutation with u^3,

$$uv = u^9 v = u^6 u^3 v = u^6 v\, u^3 = u^3 v\, u^6 = v\, u^9 = vu.$$

Thus $uv = vu$.

. . . .

Step (d): $uv = 1$.

Since u and v commute,

$uv = (uv)(u^4v^3) = u^5v^4 = u^2u^3v^2v^2 = (v^2u^2)(u^3v^2) = (uv)(u^3v^2) = u^4v^3 = 1,$

using $uv = v^2u^2$ and again $u^4 = v^3 = 1$.

. . . .

Step (e): $u = v = 1$ and Y is trivial.

From $u^4v^3 = 1$ and Step (d),

$$1 = u^4v^3 = u^3(uv)v^2 = u^3v^2 = u^2(uv)v = u^2v = u(uv) = u,$$

so $u = 1$. Then $v = uv = 1$. Hence $Y = \{1\}$.

. . . .

All parts (a)–(e) are proved. □

. . . .

1.3: Symmetric Groups

. . . .

Exercise 55 (D&F §1.3, Ex. 1)**.** *Let $\sigma, \tau \in S_5$ be defined by*

$\sigma: \ 1 \mapsto 3, \ 2 \mapsto 4, \ 3 \mapsto 5, \ 4 \mapsto 2, \ 5 \mapsto 1, \qquad \tau: \ 1 \mapsto 5, \ 2 \mapsto 3, \ 3 \mapsto 2, \ 4 \mapsto 4, \ 5 \mapsto$

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

Intuition. Follow the orbit of each element to build disjoint cycles; for products, apply the rightmost map first. Once an element's cycle is recorded, skip it (disjoint cycles commute).

Proof. Step 1: σ and τ in cycles.
Trace orbits:

$$\sigma = (1\ 3\ 5)(2\ 4), \qquad \tau = (1\ 5)(2\ 3).$$

Step 2: σ^2.
Since $(1\ 3\ 5)^2 = (1\ 5\ 3)$ and $(2\ 4)^2 = 1$, we have

$$\sigma^2 = (1\ 5\ 3).$$

Step 3: $\sigma\tau$ (apply τ then σ).
Track 2: $2 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 5 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 3 \xrightarrow{\tau} 2$, giving a 4-cycle $(2\ 5\ 1\ 3)$. Checking 4: $4 \xrightarrow{\tau} 4 \xrightarrow{\sigma} 2$, so it falls into this cycle:

$$\sigma\tau = (2\ 5\ 3\ 4).$$

Step 4: $\tau\sigma$ (apply σ then τ).
Track 1: $1 \xrightarrow{\sigma} 3 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 4$, and continuing closes

$$\tau\sigma = (1\ 2\ 4\ 3).$$

. . . .

Step 5: $\tau^2\sigma$*.*

Since τ is a product of 2-cycles, $\tau^2 = 1$, hence

$$\tau^2\sigma = \sigma = (1\ 3\ 5)(2\ 4).$$

. . . .

Collecting all results,

$$\sigma = (1\ 3\ 5)(2\ 4), \quad \tau = (1\ 5)(2\ 3), \quad \sigma^2 = (1\ 5\ 3),$$

$$\sigma\tau = (2\ 5\ 3\ 4), \quad \tau\sigma = (1\ 2\ 4\ 3), \quad \tau^2\sigma = (1\ 3\ 5)(2\ 4).$$

□

Exercise 56 (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: σ in cycles.
Trace $1 \to 13 \to 5 \to 10 \to 1$ and $3 \to 15 \to 8 \to 3$, and $4 \to 14 \to 11 \to 7 \to 12 \to 9 \to 4$, while $2, 6$ are fixed:

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

Step 2: τ in cycles.
Trace $1 \leftrightarrow 14$, $3 \leftrightarrow 10$, $8 \leftrightarrow 11$, $5 \to 12 \to 7 \to 5$, and $2 \to 9 \to 15 \to 13 \to 4 \to 2$, with 6 fixed:

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

Step 3: σ^2.
Square each disjoint cycle of σ:

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

Hence

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

. . . .

Step 4: $\sigma\tau$ (apply τ then σ).

Track $1:\ 1 \xrightarrow{\tau} 14 \xrightarrow{\sigma} 11 \xrightarrow{\tau} 8 \xrightarrow{\sigma} 3 \xrightarrow{\tau} 10 \xrightarrow{\sigma} 1$, giving (1 11 3). Track $2:\ 2 \xrightarrow{\tau} 9 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 2$, giving (2 4). Track $5:\ 5 \xrightarrow{\tau} 12 \xrightarrow{\sigma} 9 \xrightarrow{\tau} 15 \xrightarrow{\sigma} 8 \xrightarrow{\tau} 11 \xrightarrow{\sigma} 7 \xrightarrow{\tau} 5$, and continuing closes a 6-cycle (5 9 8 7 10 15). Finally $13 \leftrightarrow 14$ under $\sigma\tau$:

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

. . . .

Step 5: $\tau\sigma$ (apply σ then τ).

Track $1:\ 1 \xrightarrow{\sigma} 13 \xrightarrow{\tau} 4 \xrightarrow{\sigma} 14 \xrightarrow{\tau} 1$, giving (1 4). Track $2:\ 2 \xrightarrow{\sigma} 2 \xrightarrow{\tau} 9 \xrightarrow{\sigma} 4 \xrightarrow{\tau} 2$, giving (2 9). Track $3:\ 3 \xrightarrow{\sigma} 15 \xrightarrow{\tau} 13 \xrightarrow{\sigma} 5 \xrightarrow{\tau} 12 \xrightarrow{\sigma} 9 \xrightarrow{\tau} 15$ and continue to close

$$(3\ 13\ 12\ 15\ 11\ 5),$$

and tracking 8 yields (8 10 14). Thus

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

. . . .

Step 6: $\tau^2\sigma$.

Compute τ^2 from Step 2 (each cycle squared), then compose with σ; tracing 1 produces the 13-cycle

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

with 6 and 9 fixed by $\tau^2\sigma$. Hence

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

. . . .

Collecting all decompositions:

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

□

Exercise 57 (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. Set A (from Exercise 1).
We had

$$\sigma = (1\,3\,5)(2\,4), \tau = (1\,5)(2\,3), \sigma^2 = (1\,5\,3), \sigma\tau = (2\,5\,3\,4), \tau\sigma = (1\,2\,4\,3), \tau^2\sigma = \sigma.$$

Therefore

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

. . . .

Set B (from Exercise 2).
We had

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

Thus

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

. . . .

All requested orders are computed. □

Exercise 58 (D&F §1.3, Ex. 4)**.** *(4) Compute the order of each of the elements in the following groups: (a) S_3 (b) S_4.*

Intuition. An element's order is the least common multiple of the lengths of the cycles in its disjoint-cycle decomposition. Thus, classify elements by cycle type and then record the order of each.

Proof. Part (a): S_3 — abstract classification.

type	representatives	count	order
1	1	1	1
(ab)	$(12), (13), (23)$	3	2
(abc)	$(123), (132)$	2	3

Explicit permutation–order table for S_3.

Permutation	Order	Permutation	Order	Permutation	Order
1	1	(12)	2	(13)	2
(23)	2	(123)	3	(132)	3

Part (b): S_4 — abstract classification.

type	representatives	count	order
1	1	1	1
(ab)	$(12), (13), (14), (23), (24), (34)$	6	2
$(ab)(cd)$	$(12)(34), (13)(24), (14)(23)$	3	2
(abc)	all 3-cycles in S_4	8	3
$(abcd)$	all 4-cycles in S_4	6	4

Explicit permutation–order table for S_4.

Permutation	Order	Permutation	Order	Permutation	Order
1	1	(12)	2	(13)	2
(14)	2	(23)	2	(24)	2
(34)	2	(12)(34)	2	(13)(24)	2
(14)(23)	2	(123)	3	(132)	3
(124)	3	(142)	3	(134)	3
(143)	3	(234)	3	(243)	3
(1234)	4	(1243)	4	(1324)	4
(1342)	4	(1423)	4	(1432)	4

□

Exercise 59 (D&F §1.3, Ex. 5)**.** *Find the order of* (1 12 8 10 4)(2 13)(5 11 7)(6 9).

. . . .

Intuition. For disjoint cycles, the order of the product is the least common multiple of the individual cycle lengths.

. . . .

Proof. Write

$$\sigma = (1\ 12\ 8\ 10\ 4)\,(2\ 13)\,(5\ 11\ 7)\,(6\ 9).$$

The cycles have lengths $5, 2, 3, 2$, respectively. Since the cycles are disjoint, the order is

$$|\sigma| = \operatorname{lcm}(5, 2, 3, 2) = \operatorname{lcm}(5, 3, 2) = 30.$$

□

Exercise 60 (D&F §1.3, Ex. 6)**.** *Write out the cycle decomposition of each element of order* 4 *in* S_4.

. . . .

Intuition. In S_4, an element has order 4 iff its disjoint-cycle type is a single 4-cycle. (Transpositions and products of two disjoint transpositions have order 2; 3-cycles have order 3.)

. . . .

Proof. The elements of order 4 in S_4 are precisely the 4-cycles. Enumerating all 4-cycles on $\{1, 2, 3, 4\}$:

$$(1\ 2\ 3\ 4), \quad (1\ 2\ 4\ 3), \quad (1\ 3\ 2\ 4), \quad (1\ 3\ 4\ 2), \quad (1\ 4\ 2\ 3), \quad (1\ 4\ 3\ 2).$$

Each listed permutation is already in cycle decomposition (a single 4-cycle), and a 4-cycle has order 4. No other cycle type in S_4 yields order 4. □

Exercise 61 (D&F §1.3, Ex. 7)**.** *Write out the cycle decomposition of each element of order* 2 *in* S_4*.*

. . . .

Intuition. In S_4, an element has order 2 precisely when its cycle decomposition is a product of disjoint 2-cycles. This includes both single transpositions and products of two disjoint transpositions.

. . . .

Proof. The transpositions (2-cycles) in S_4 are:

$$(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4).$$

Each has order 2.

. . . .

The products of two disjoint transpositions in S_4 are:

$$(1\ 2)(3\ 4),\quad (1\ 3)(2\ 4),\quad (1\ 4)(2\ 3).$$

Each also has order 2.

. . . .

Thus the complete list of elements of order 2 in S_4 is

$$(1\ 2),\ (1\ 3),\ (1\ 4),\ (2\ 3),\ (2\ 4),\ (3\ 4),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3).$$

□

Exercise 62 (D&F §1.3, Ex. 8)**.** *Prove that if* $\Omega = \{1, 2, 3, \ldots\}$ *then* S_Ω *is an infinite group* (do not say $\infty! = \infty$).

. . . .

Intuition. Exhibit infinitely many *distinct* permutations in S_Ω. A simple choice is one transposition for each n, swapping the pair $(2n-1, 2n)$ and fixing everything else—these are all different.

. . . .

Proof. For each $n \in \mathbb{Z}_{>0}$ define $\sigma_n \in S_\Omega$ by

$$\sigma_n(2n-1) = 2n, \quad \sigma_n(2n) = 2n-1, \quad \text{and} \quad \sigma_n(k) = k \text{ for all } k \in \Omega \backslash \{2n-1, 2n\}.$$

Thus $\sigma_n = (2n-1\ 2n)$ is a transposition, hence a bijection of Ω, so $\sigma_n \in S_\Omega$.

We claim the σ_n are pairwise distinct. If $i \neq j$, then

$$\sigma_i(2i-1) = 2i \neq 2i-1 = \sigma_j(2i-1),$$

since σ_j fixes $2i-1$ when $j \neq i$. Therefore $\sigma_i \neq \sigma_j$.

Hence $\{\sigma_n : n \in \mathbb{Z}_{>0}\}$ is an infinite subset of S_Ω, so S_Ω is infinite. □

Exercise 63 (D&F §1.3, Ex. 9)**.** *(a) Let σ be the* 12*-cycle* $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12)$*. For which positive integers i is σ^i also a* 12*-cycle?*
(b) Let τ be the 8*-cycle* $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$*. For which positive integers i is τ^i also an* 8*-cycle?*
(c) Let ω be the 14*-cycle* $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)$*. For which positive integers i is ω^i also a* 14*-cycle?*

Intuition. If π is an m-cycle, then π^i breaks into $\gcd(m,i)$ disjoint cycles, each of length $m/\gcd(m,i)$. Thus π^i is again an m-cycle exactly when $\gcd(m,i)=1$ (i.e. i is coprime to m).

Proof. We use the standard fact: for an m-cycle π, the orbit of any element under π^i has size $m/\gcd(m,i)$, so π^i is an m-cycle iff $\gcd(m,i)=1$.

Part (a): $m=12$.
σ^i is a 12-cycle $\iff \gcd(12,i)=1$. Hence $i \equiv 1,5,7,11 \pmod{12}$ (and all integers congruent to these classes mod 12).

Part (b): $m=8$.
τ^i is an 8-cycle $\iff \gcd(8,i)=1$. Hence $i \equiv 1,3,5,7 \pmod 8$ (and all integers congruent to these classes mod 8).

Part (c): $m=14$.
ω^i is a 14-cycle $\iff \gcd(14,i)=1$. Hence $i \equiv 1,3,5,9,11,13 \pmod{14}$ (and all integers congruent to these classes mod 14).

This matches the general coprimality criterion: π^i is an m-cycle iff $(i,m)=1$. □

Exercise 64 (D&F §1.3, Ex. 10)**.** *Prove that if σ is the m-cycle $(a_1\ a_2\ \dots\ a_m)$, then for all $i \in \{1, 2, \dots, m\}$,*

$$\sigma^i(a_k) = a_{k+i},$$

where $k+i$ is interpreted modulo m as its least positive residue. Deduce that $|\sigma| = m$.

. . . .

Intuition. An m-cycle advances indices by one step each application. Repeating i times advances by i steps, read modulo m. This immediately implies that no power smaller than m can return every point, while the mth power does.

. . . .

Proof. Write $\sigma = (a_1\ a_2\ \dots\ a_m)$. By definition, $\sigma(a_k) = a_{k+1}$ with indices taken modulo m (so $a_{m+1} = a_1$, etc.).

. . . .

Step 1: $\sigma^i(a_k) = a_{k+i}$ for all $i \geq 1$.
We argue by induction on i. For $i = 1$ this is the defining property. Assume $\sigma^i(a_k) = a_{k+i}$ for some $i \geq 1$. Then

$$\sigma^{i+1}(a_k) = \sigma\big(\sigma^i(a_k)\big) = \sigma(a_{k+i}) = a_{k+i+1},$$

again with indices reduced modulo m. This completes the induction.

. . . .

Step 2: Deduce $|\sigma| = m$.
From Step 1 with $k = 1$ we have $\sigma^i(a_1) = a_{1+i}$. If $1 \leq i < m$, then $a_{1+i} \neq a_1$, so $\sigma^i \neq 1$. On the other hand, for $i = m$ we get $\sigma^m(a_k) = a_{k+m} = a_k$ for every k, hence $\sigma^m = 1$. Therefore the order of σ is exactly m.

. . . .

Thus $\sigma^i(a_k) = a_{k+i}$ (indices mod m), and $|\sigma| = m$. □

Exercise 65 (D&F §1.3, Ex. 11)**.** *Let $\sigma = (1\,2\,\ldots\,m)$ be an m-cycle. Show that σ^i is also an m-cycle if and only if* $\gcd(i, m) = 1$.

. . . .

Intuition. Think of σ as a clock with m positions. Each application of σ moves one tick forward. Applying σ^i means jumping i ticks each time. - If i and m are relatively prime, then repeated jumps of i eventually visit every tick — one complete lap. - If i and m share a factor $d > 1$, then you only hit every dth tick, breaking the cycle into d smaller loops.

. . . .

Proof. (⇒) Suppose σ^i is an m-cycle. Let $d = \gcd(i, m)$. Write $i = dx$ and $m = dy$. Then

$$(\sigma^i)^y = \sigma^{iy} = \sigma^{dxy} = (\sigma^m)^x = 1.$$

Thus the order of σ^i divides $y = \frac{m}{d}$. But an m-cycle must have order exactly m. Hence $m \leq \frac{m}{d}$, forcing $d = 1$.

(⇐) Conversely, assume $\gcd(i, m) = 1$. Consider the orbit of m under σ^i:

$$m \mapsto i^* \mapsto (2i)^* \mapsto \cdots \mapsto ((m-1)i)^* \mapsto m,$$

where k^* denotes the least positive residue of k modulo m.

Because i has a multiplicative inverse modulo m, the numbers

$$i^*, (2i)^*, \ldots, ((m-1)i)^*$$

are all distinct. Thus the orbit has size m, and σ^i is indeed an m-cycle.

Therefore, σ^i is an m-cycle if and only if $\gcd(i, m) = 1$. □

Exercise 66 (D&F §1.3, Ex. 12). *(a) If $\tau = (1\,2)(3\,4)(5\,6)(7\,8)(9\,10)$, determine whether there is an n-cycle σ ($n \geq 10$) and an integer k with $\tau = \sigma^k$.*

(b) If $\tau = (1\,2)(3\,4\,5)$, determine whether there is an n-cycle σ ($n \geq 5$) and an integer k with $\tau = \sigma^k$.

. . . .

Intuition. A power of an n-cycle is "walk k steps at a time around one big circle." - When k and n share a common divisor $d > 1$, the walk breaks the big circle into d equal smaller loops; each loop is a cycle of length n/d. - To manufacture a given product of disjoint cycles, choose σ so that "every kth hop" exactly lands on the desired pairs/blocks.

. . . .

Solution. (a) Yes, and explicitly. Take the 10-cycle

$$\sigma = (1\,3\,5\,7\,9\,2\,4\,6\,8\,10).$$

Compute σ^5: hopping 5 steps in this ordering swaps each odd with the following even,

$$\sigma^5 = (1\,2)(3\,4)(5\,6)(7\,8)(9\,10) = \tau,$$

so τ is indeed a 5th power of an n-cycle (here $n = 10$). (Heuristic check: $k = 5$ and $n = 10$ give $d = \gcd(5, 10) = 5$, so the big 10-cycle splits into 5 disjoint 2-cycles—exactly the target.)

(b) No. Suppose $\tau = (1\,2)(3\,4\,5)$ were σ^k for some n-cycle σ with $n \geq 5$.

If $n > 5$, then σ^k must fix every point $6, 7, \ldots, n$. But a power of an n-cycle either fixes *every* point (when it is the identity) or fixes *no* point outside its orbit structure. Hence σ^k cannot have those fixed points unless $\sigma^k = 1$, contradicting $\tau \neq 1$. Thus $n = 5$.

Now $n = 5$ is prime. For a 5-cycle σ, σ^k is a 5-cycle iff $\gcd(k, 5) = 1$ and is the identity iff $5 \mid k$. In either case σ^k cannot equal a product of a 2-cycle and a 3-cycle. Therefore no such σ, k exist. □

Exercise 67 (D&F §1.3, Ex. 13)**.** *Show that a permutation $\sigma \in S_n$ has order* 2 *if and only if its cycle decomposition is a product of disjoint* 2*-cycles* and at least one 2-cycle appears *(equivalently: every moved point lies in a transposition, and $\sigma \neq 1$).*

. . . .

Intuition. An involution is a "pairwise flip." Squaring a transposition gives the identity, and disjoint transpositions don't interfere. If there are no flips at all, you get the identity, whose order is 1.

. . . .

Proof. ($\Rightarrow$) If $\sigma^2 = 1$ and $\sigma \neq 1$, then any moved i satisfies $\sigma(i) = j$ and $\sigma(j) = i$, so $(i\, j)$ occurs in the decomposition. No cycle of length ≥ 3 can occur (a t-cycle with $t \geq 3$ does not square to 1), hence every nontrivial cycle is a 2-cycle and the cycles are disjoint. Thus σ is a nontrivial product of disjoint 2-cycles.

($\Leftarrow$) If

$$\sigma = (a_1\, b_1) \cdots (a_k\, b_k)$$

is a product of disjoint 2-cycles, then $(a_r\, b_r)^2 = 1$ and the factors commute, so $\sigma^2 = 1$. If $k \geq 1$ (i.e. at least one 2-cycle appears), then $\sigma \neq 1$, hence $|\sigma| = 2$. If $k = 0$ (no 2-cycles), then $\sigma = 1$ and $|\sigma| = 1$. □

Conclusion. *σ has order* 2 *iff it is a nontrivial product of disjoint* 2*-cycles. Equivalently, $\sigma = 1$ exactly when no* 2*-cycles appear.*

Exercise 68 (D&F §1.3, Ex. 14)**.** *Let p be a prime. Show that a permutation $\sigma \in S_n$ has order p if and only if its cycle decomposition is a product of commuting p-cycles. Exhibit failure for composite p.*

. . . .

Intuition. Disjoint cycles act on disjoint supports, so powers act componentwise. If $|\sigma| = p$ (prime), every nontrivial component must have length dividing p, hence length p. Conversely, if σ is a product of p-cycles, the pth power kills each component, and no smaller power can do so because each p-cycle already has minimal period p.

. . . .

Proof. Notation. Write the disjoint cycle decomposition

$$\sigma = \tau_1\tau_2 \cdots \tau_k,$$

where each τ_i is a cycle (possibly a 1-cycle, i.e. a fixed point). Disjoint cycles commute.

($\Rightarrow$) Assume $|\sigma| = p$. Show that each nontrivial τ_i is a p-cycle.

1. Since $|\sigma| = p$, we have $\sigma^p = 1$ and $\sigma^r \neq 1$ for $1 \leq r < p$.
2. Because the τ_i are disjoint and commute,

$$1 = \sigma^p = (\tau_1 \cdots \tau_k)^p = \tau_1^p \cdots \tau_k^p.$$

3. Disjoint supports imply factorwise identity: for each i and each x in the support of τ_i, all τ_j with $j \neq i$ fix x, so $(\tau_1^p \cdots \tau_k^p)(x) = \tau_i^p(x)$. Thus $\tau_i^p = 1$ for every i.
4. Therefore the length ℓ_i of τ_i divides p. Since p is prime, $\ell_i \in \{1, p\}$.
5. Hence every nontrivial cycle is a p-cycle. Because the cycles are disjoint, they commute.

($\Leftarrow$) Assume σ is a product of disjoint p-cycles. Prove $|\sigma| = p$.

1. Suppose $\sigma = \tau_1 \cdots \tau_k$ with $|\tau_i| = p$ for each i (fixed points, if any, are 1-cycles and can be ignored).

2. Since the factors commute and each $\tau_i^p = 1$, we get
$$\sigma^p = \tau_1^p \cdots \tau_k^p = 1.$$
So $|\sigma|$ divides p.

3. It remains to rule out $|\sigma| = 1$. Assume for contradiction that $\sigma = 1$. Then every τ_i must be the identity, but each τ_i was a p-cycle, not the identity. Contradiction.

4. Alternatively (minimality check): if $\sigma^r = 1$ for some $1 \leq r < p$, restrict to the support of any τ_i. All τ_j with $j \neq i$ act trivially there, so $(\sigma^r)|_{\mathrm{supp}(\tau_i)} = \tau_i^r = 1$. But $|\tau_i| = p$ forces $p \mid r$, impossible for $1 \leq r < p$. Hence no smaller positive power than p kills σ.

5. Therefore $|\sigma| = p$.

Failure for composite p. Let p be composite, e.g. $p = 6$. In S_6 the permutation
$$(1\,2)(3\,4\,5)$$
has order $\mathrm{lcm}(2, 3) = 6$, yet it is not a product of disjoint 6-cycles (there are none on $\{1, \ldots, 6\}$). Thus the prime hypothesis is essential. □

Conclusion. For prime p, a permutation has order p if and only if it is a product of disjoint (hence commuting) p-cycles. For composite p, this characterization fails.

Exercise 69 (D&F §1.3, Ex. 15)**.** *Let $\sigma \in S_n$ have disjoint cycle decomposition*

$$\sigma = \tau_1 \tau_2 \cdots \tau_r,$$

where each τ_j is a cycle of length $m_j \geq 1$. Prove that

$$|\sigma| = \operatorname{lcm}(m_1, \dots, m_r).$$

. . . .

Intuition. Disjoint cycles act on disjoint sets of symbols, so they do not interfere. A power σ^k applies the kth power to each component: $\sigma^k = \tau_1^k \cdots \tau_r^k$. Each τ_j returns to the start exactly every m_j steps. Therefore *all* components reset precisely when k is a common multiple of the m_j's; the smallest such k is their lcm.

. . . .

Proof. Write $\sigma = \tau_1 \cdots \tau_r$ with pairwise disjoint supports and $|\tau_j| = m_j$.

Step 1: Powers act componentwise on disjoint cycles. Since disjoint cycles commute, for every $k \geq 1$,

$$\sigma^k = (\tau_1 \cdots \tau_r)^k = \tau_1^k \cdots \tau_r^k.$$

Step 2: Characterize when $\sigma^k = 1$. Because the supports are disjoint, $\sigma^k = 1$ if and only if each factor is the identity:

$$\sigma^k = 1 \quad \Longleftrightarrow \quad \tau_j^k = 1 \text{ for all } j.$$

But $|\tau_j| = m_j$ means $\tau_j^k = 1$ exactly when $m_j \mid k$. Thus

$$\sigma^k = 1 \quad \Longleftrightarrow \quad m_j \mid k \text{ for every } j \quad \Longleftrightarrow \quad \operatorname{lcm}(m_1, \dots, m_r) \mid k.$$

Step 3: Minimality. By Step 2, the set of positive integers k with $\sigma^k = 1$ is precisely the set of common multiples of the m_j's, whose least positive element is $L := \operatorname{lcm}(m_1, \dots, m_r)$. Hence $|\sigma| = L$. □

Conclusion. The order of a permutation is the least common multiple of the lengths of the cycles in its disjoint cycle decomposition.

Exercise 70 (D&F §1.3, Ex. 16)**.** *Show that if $n \geq m$ then the number of m-cycles in S_n is*

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}.$$

. . . .

Intuition. An m-cycle is just a way to choose m distinct symbols from $\{1,\ldots,n\}$ and arrange them *around a circle*. Linear listings overcount the same circle by a factor of m (you can start the cycle at any of its m positions and get the same cycle). So: "count linear arrangements" and then "divide by m."

. . . .

Proof. Step 1 (choose an ordered m-tuple of distinct symbols). Pick the entries of the would-be cycle one by one: n choices for the first slot, $n-1$ for the second, ..., $n-m+1$ for the m-th. This yields

$$n(n-1)(n-2)\cdots(n-m+1)$$

distinct *linear* m-tuples. Each such tuple corresponds to writing a cycle as $(a_1\, a_2\, \ldots\, a_m)$.

Step 2 (identify which linear tuples represent the same cycle). For a fixed m-cycle $(a_1\, a_2\, \ldots\, a_m)$ there are exactly m linear representations obtained by cyclically rotating the starting point:

$$(a_1\, a_2\, \ldots\, a_m) = (a_2\, a_3\, \ldots\, a_m\, a_1) = \cdots = (a_m\, a_1\, \ldots\, a_{m-1}).$$

No other linear tuple represents this same cycle, because a different set or a different cyclic order gives a different mapping. Therefore each *cycle* is counted exactly m times in Step 1.

Step 3 (divide out the overcount). Hence the number of distinct m-cycles is

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}.$$

This matches the stated formula. □

Conclusion. For $n \geq m$, the number of m-cycles in S_n is $\dfrac{n(n-1)\cdots(n-m+1)}{m}$.

Exercise 71 (D&F §1.3, Ex. 17). *Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjoint 2-cycles is*

$$\frac{n(n-1)(n-2)(n-3)}{8}.$$

. . . .

Intuition. Think of building such a permutation step by step: - First, you need to pick four distinct symbols that will be "moved around." - Next, you must break those four symbols into two pairs, since each transposition swaps exactly two. - Finally, you note that the *order doesn't matter*: swapping $\{a, b\}$ then $\{c, d\}$ is the same as swapping $\{c, d\}$ then $\{a, b\}$, and inside each pair the order doesn't matter either.

So the problem boils down to: "How many ways are there to choose four symbols and split them into two unlabeled pairs?"

That's why the count turns into $\binom{n}{4}\cdot 3$, or equivalently $\frac{n(n-1)(n-2)(n-3)}{8}$.

. . . .

Proof. Method 1 (sequential choice).

1. Choose the first 2-cycle: $\binom{n}{2} = \frac{n(n-1)}{2}$ options.
2. Choose the second, disjoint 2-cycle from the remaining $n-2$ symbols: $\binom{n-2}{2} = \frac{(n-2)(n-3)}{2}$ options.
3. Since $(a\,b)(c\,d) = (c\,d)(a\,b)$, each permutation has been counted twice. Divide by 2.

The total count is

$$\frac{\binom{n}{2}\binom{n-2}{2}}{2} = \frac{\frac{n(n-1)}{2}\cdot\frac{(n-2)(n-3)}{2}}{2} = \frac{n(n-1)(n-2)(n-3)}{8}.$$

Method 2 (direct grouping). Choose 4 symbols from n: $\binom{n}{4}$ ways. Partition them into two unordered pairs: 3 ways. So the total is

$$\binom{n}{4}\cdot 3 = \frac{n(n-1)(n-2)(n-3)}{24}\cdot 3 = \frac{n(n-1)(n-2)(n-3)}{8}.$$

Both methods agree, proving the claim. □

Conclusion. For $n \geq 4$, there are $\dfrac{n(n-1)(n-2)(n-3)}{8}$ permutations in S_n that are products of two disjoint 2-cycles.

Exercise 72 (D&F §1.3, Ex. 18)**.** *Find all numbers n such that S_5 contains an element of order n.*

. . . .

Intuition. You only have *five seats* to move: every permutation of $\{1, 2, 3, 4, 5\}$ breaks into disjoint cycles whose lengths add to 5. The order of the permutation is the *lcm of those cycle lengths*. So list all partitions of 5, take lcms, and collect the resulting orders.

. . . .

Proof. By Exercise 15, if $\sigma \in S_5$ has disjoint cycle lengths $m_1, \ldots, m_r$, then $|\sigma| = \operatorname{lcm}(m_1, \ldots, m_r)$. All possible disjoint-cycle types are the partitions of 5:

$$5, \quad 4{+}1, \quad 3{+}2, \quad 3{+}1{+}1, \quad 2{+}2{+}1, \quad 2{+}1{+}1{+}1, \quad 1{+}1{+}1{+}1{+}1.$$

Taking least common multiples of the parts gives the set of possible orders:

cycle type	order
(5)	5
(4)(1)	4
(3)(2)	$\operatorname{lcm}(3, 2) = 6$
(3)(1)(1)	3
(2)(2)(1)	2
(2)(1)(1)(1)	2
(1)(1)(1)(1)(1)	1

Thus the possible orders in S_5 are precisely $\{1, 2, 3, 4, 5, 6\}$. □

Conclusion. S_5 contains elements of order n exactly for $n \in \{1, 2, 3, 4, 5, 6\}$.

Exercise 73 (D&F §1.3, Ex. 19). *Find all numbers n such that S_7 contains an element of order n.*

. . . .

Intuition. Every permutation of $\{1, \ldots, 7\}$ breaks into disjoint cycles whose lengths add to 7. By Ex. 15, the order is the *lcm of those cycle lengths.* So list the partitions of 7, take lcms, and collect the distinct values.

. . . .

Proof. All disjoint-cycle types correspond to partitions of 7:

$7;\quad 6+1;\quad 5+2,\ 5+1+1;\quad 4+3,\ 4+2+1,\ 4+1+1+1;$
$3+3+1,\ 3+2+2,\ 3+2+1+1,\ 3+1+1+1+1;$
$2+2+2+1,\ 2+2+1+1+1,\ 2+1+1+1+1+1;\quad 1+1+1+1+1+1+1.$

Taking least common multiples of the nontrivial parts gives:

cycle type	order
(7)	7
$(6)(1)$	6
$(5)(2),\ (5)(1)(1)$	10, 5
$(4)(3),\ (4)(2)(1),\ (4)(1)(1)(1)$	12, 4, 4
$(3)(3)(1),\ (3)(2)(2),\ (3)(2)(1)(1),\ (3)(1)(1)(1)(1)$	3, 6, 6, 3
$(2)(2)(2)(1),\ (2)(2)(1)(1)(1),\ (2)(1)(1)(1)(1)(1)$	2, 2, 2
$(1)^7$	1

Hence the possible orders in S_7 are exactly

$$\{1, 2, 3, 4, 5, 6, 7, 10, 12\}.$$

□

Conclusion. S_7 contains elements of order n precisely for $n \in \{1, 2, 3, 4, 5, 6, 7, 10, 12\}$.

Exercise 74 (D&F §1.3, Ex. 20)**.** *Find a set of generators and relations for S_3.*

. . . .

Intuition. S_3 is the group of all symmetries of a triangle. Two moves obviously generate all symmetries: a *flip* α across an axis (a transposition, order 2) and a *rotation* β by 120° (a 3-cycle, order 3). The only extra constraint you need is that "flip then rotate" behaves like a half-turn: $(\alpha\beta)$ has order 2. Those three facts pin the group down.

. . . .

Proof. Let $\alpha = (1\,2)$ and $\beta = (1\,2\,3)$ in S_3. Then

$$\alpha^2 = 1, \qquad \beta^3 = 1, \qquad (\alpha\beta)^2 = 1.$$

We claim that the presentation

$$\langle\, \alpha, \beta \mid \alpha^2 = \beta^3 = (\alpha\beta)^2 = 1 \,\rangle$$

defines S_3.

Step 1: $\langle \alpha, \beta \rangle = S_3$. Since α is a transposition and β is a 3-cycle, they generate all of S_3: indeed $(1\,3) = \beta\alpha$ and $(2\,3) = \alpha\beta$, so all three transpositions and the 3-cycles lie in $\langle \alpha, \beta \rangle$, hence $\langle \alpha, \beta \rangle = S_3$.

Step 2: The relations hold in S_3. Direct computation gives $\alpha^2 = 1$ and $\beta^3 = 1$. Also

$$\alpha\beta = (1\,2)(1\,2\,3) = (2\,3), \quad \text{so} \quad (\alpha\beta)^2 = (2\,3)^2 = 1.$$

Thus there is a surjective homomorphism

$$\phi :\ G := \langle\, \alpha, \beta \mid \alpha^2 = \beta^3 = (\alpha\beta)^2 = 1 \,\rangle \ \twoheadrightarrow\ S_3$$

sending the generators to the indicated permutations.

Step 3: Normal forms in G (size ≤ 6). From $(\alpha\beta)^2 = 1$ we get $\alpha\beta\alpha = \beta^{-1}$ (multiply on the right by $\beta\alpha$), hence

$$\alpha\beta = \beta^{-1}\alpha, \qquad \beta\alpha = \alpha\beta^{-1}.$$

Using these, any word in α, β can be rewritten by pushing every α to the left, reducing powers with $\alpha^2 = 1$ and $\beta^3 = 1$, to one of the six forms

$$1,\ \beta,\ \beta^2,\ \alpha,\ \alpha\beta,\ \alpha\beta^2.$$

Therefore $|G| \leq 6$.

Step 4: Isomorphism. The images under ϕ of the six normal forms are the six distinct elements $1, (1\,2\,3), (1\,3\,2), (1\,2), (2\,3), (1\,3)$ of S_3. Hence ϕ is a bijection and $G \cong S_3$.

Conclusion. A presentation for S_3 is

$$\boxed{S_3 \cong \langle\, \alpha, \beta \mid \alpha^2 = \beta^3 = (\alpha\beta)^2 = 1 \,\rangle,\ \text{with } \alpha = (1\,2),\ \beta = (1\,2\,3).}$$

□

. . . .

1.4: Matrix Groups

. . . .

Exercise 75 (D&F §1.4, Ex. 1)**.** *Prove that* $|GL_2(\mathbb{F}_2)| = 6$*.*

. . . .

Intuition. Over $\mathbb{F}_2 = \{0, 1\}$ there are only $2^4 = 16$ matrices. Invertibility just means the determinant is 1 (since the only nonzero element is 1), so we're counting 2×2 matrices with determinant 1.

. . . .

Proof. A matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ over $\mathbb{F}_2$ is invertible iff $\det(A) = ad - bc = 1$ in $\mathbb{F}_2$.

A quick count: choose a nonzero first column in 3 ways and a second column not collinear with it in 2 ways. Hence

$$|GL_2(\mathbb{F}_2)| = 3 \cdot 2 = 6.$$

Conclusion.

$$\boxed{|GL_2(\mathbb{F}_2)| = 6.}$$

□

Exercise 76 (D&F §1.4, Ex. 2)**.** *Write out all the elements of* $GL_2(\mathbb{F}_2)$ *and compute the order of each.*

Intuition. With only six invertible matrices, we can list them explicitly and square/cube as needed. Recall that in characteristic 2, $-I = I$, so the only possible orders besides 1 are 2 and 3.

Proof. The six invertible matrices are

$$I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \quad A = \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}, \quad B = \begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}, \quad C = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}, \quad D = \begin{bmatrix}1 & 1\\1 & 0\end{bmatrix}, \quad E = \begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$$

Direct computation gives

$$|I| = 1, \quad |A| = |B| = |C| = 2, \quad |D| = |E| = 3.$$

Conclusion.

$$\boxed{\text{Orders: } 1, 2, 2, 2, 3, 3 \text{ for } I, A, B, C, D, E \text{ respectively.}}$$

□

Exercise 77 (D&F §1.4, Ex. 3). *Show that $GL_2(\mathbb{F}_2)$ is non-abelian.*

. . . .

Intuition. With six elements and mixed orders, the structure looks like S_3, which is non-abelian. It suffices to find one pair of matrices that fail to commute.

. . . .

Proof. Take

$$D = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Then

$$DA = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = AD.$$

Thus $DA \neq AD$, proving that $GL_2(\mathbb{F}_2)$ is non-abelian.

Conclusion.

$$\boxed{GL_2(\mathbb{F}_2) \text{ is non-abelian.}}$$

□

Exercise 78 (D&F §1.4, Ex. 4)**.** *Show that if n is not prime then $\mathbb{Z}/n\mathbb{Z}$ is not a field.*

. . . .

Intuition. Composite moduli create zero divisors: if $n = ab$ with $1 < a, b < n$, then $\overline{a} \cdot \overline{b} = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$ while $\overline{a}, \overline{b} \neq \overline{0}$. A field can't have nonzero zero divisors.

. . . .

Proof. Suppose n is composite, so $n = ab$ with $1 < a, b < n$. Then in $\mathbb{Z}/n\mathbb{Z}$,

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{n} = \overline{0},$$

with $\overline{a}, \overline{b} \neq \overline{0}$. Thus $\mathbb{Z}/n\mathbb{Z}$ has a nonzero zero divisor and so cannot be a field.

Conclusion.

$$\boxed{\text{If } n \text{ is composite, then } \mathbb{Z}/n\mathbb{Z} \text{ is not a field.}}$$

□

Exercise 79 (D&F §1.4, Ex. 5). *Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.*

. . . .

Intuition. If F is finite, there are finitely many $n \times n$ matrices, hence finitely many invertible ones. If F is infinite, the scalar matrices αI with $\alpha \in F^\times$ already give infinitely many invertible matrices.

. . . .

Proof. If $|F| = q < \infty$, then the set of $n \times n$ matrices over F has size q^{n^2}, so $GL_n(F)$ is finite.

Conversely, if F is infinite, then each $\alpha \in F^\times$ yields an invertible scalar matrix $\alpha I_n \in GL_n(F)$, and $\alpha \mapsto \alpha I_n$ is injective (for every $\alpha \in F$ with $\alpha \neq 0$, the matrix αI has a nonzero determinant). Hence $GL_n(F)$ is infinite.

Conclusion.

$$\boxed{GL_n(F) \text{ is finite } \iff F \text{ is finite.}}$$

□

Exercise 80 (D&F §1.4, Ex. 6)**.** *If $|F| = q$ is finite, prove that $|GL_n(F)| < q^{n^2}$.*

. . . .

Intuition. There are q^{n^2} total $n \times n$ matrices. At least one is singular (e.g. the zero matrix), so the invertible ones are strictly fewer.

. . . .

Proof. There are q^{n^2} matrices in $M_n(F)$. Since at least one (e.g. the zero matrix) is not invertible, it follows that

$$|GL_n(F)| \leq q^{n^2} - 1 < q^{n^2}.$$

Conclusion.

$$\boxed{|GL_n(F)| < q^{n^2}.}$$

□

Exercise 81 (D&F §1.4, Ex. 7)**.** *Let p be a prime. Prove that $|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p$.*

. . . .

Intuition. Count all 2×2 matrices (p^4 total) and subtract the singular ones. A 2×2 matrix is singular iff its two rows are linearly dependent, i.e. one row is a scalar multiple of the other.

. . . .

Proof. There are p^4 total 2×2 matrices over $\mathbb{F}_p$. We count the singular ones by cases.

Case 1: the first row is zero. Then the second row is arbitrary: p^2 choices.

Case 2: the first row is nonzero. There are $p^2 - 1$ choices for the first row. The second row must be a scalar multiple of the first, giving p choices (including the zero row). Hence $(p^2 - 1)\,p = p^3 - p$ matrices here.

Therefore the number of singular matrices is

$$p^2 + (p^3 - p) = p^3 + p^2 - p.$$

Subtracting from the total yields

$$|GL_2(\mathbb{F}_p)| = p^4 - (p^3 + p^2 - p) = p^4 - p^3 - p^2 + p.$$

Conclusion.

$$\boxed{|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.}$$

□

Exercise 82 (D&F §1.4, Ex. 7)**.** *Let p be a prime. Prove that $|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p$.*

. . . .

Intuition. Count *singular* matrices directly via the determinant condition $ad - bc = 0$. Split by whether the top-left entry a is zero or not: - If $a = 0$, then $bc = 0$ forces a simple "either $b = 0$ or $c = 0$" count while d is free. - If $a \neq 0$, then d is completely determined by b and c via $d = bca^{-1}$. Subtract these singulars from the p^4 total to get the invertibles.

. . . .

Proof. Every 2×2 matrix over $\mathbb{F}_p$ has the form

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad a, b, c, d \in \mathbb{F}_p.$$

We count those with $\det(A) = ad - bc = 0$.

Case 1: $a = 0$. Then $bc = 0$ and d is arbitrary. - If $b = 0$, then c has p choices and d has p choices: $p \cdot p = p^2$. - If $b \neq 0$ (there are $p - 1$ choices), then $c = 0$ and d has p choices: $(p - 1) \cdot p = p^2 - p$. Thus Case 1 contributes $p^2 + (p^2 - p) = 2p^2 - p$ matrices.

Case 2: $a \neq 0$. There are $p - 1$ choices for a, and then b, c are arbitrary (p^2 choices). The determinant equation $ad = bc$ forces $d = bca^{-1}$, uniquely determined by a, b, c. Hence Case 2 contributes $(p - 1)p^2 = p^3 - p^2$ matrices.

Therefore the number of singular matrices is

$$(2p^2 - p) + (p^3 - p^2) = p^3 + p^2 - p.$$

Since there are p^4 total 2×2 matrices,

$$|GL_2(\mathbb{F}_p)| = p^4 - (p^3 + p^2 - p) = p^4 - p^3 - p^2 + p.$$

Conclusion.

$$\boxed{|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p.}$$

□

Exercise 83 (D&F §1.4, Ex. 8)**.** *Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any field F.*

. . . .

Intuition. Exhibit one pair of invertible matrices that fail to commute. Do this first in 2×2, then embed those matrices as block-diagonals inside $n \times n$ to pass to all $n \geq 2$.

. . . .

Proof. Base case $n = 2$. Set

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad D = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in GL_2(F).$$

Then

$$DA = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = AD,$$

so $GL_2(F)$ is non-abelian.

Inductive step. Assume $GL_{n-1}(F)$ is non-abelian for some $n \geq 3$, so there exist $X, Y \in GL_{n-1}(F)$ with $XY \neq YX$. Form the block-diagonal matrices

$$\widetilde{X} = \begin{bmatrix} X & 0 \\ 0 & 1 \end{bmatrix}, \qquad \widetilde{Y} = \begin{bmatrix} Y & 0 \\ 0 & 1 \end{bmatrix} \in GL_n(F).$$

Then

$$\widetilde{X}\,\widetilde{Y} = \begin{bmatrix} XY & 0 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} YX & 0 \\ 0 & 1 \end{bmatrix} = \widetilde{Y}\,\widetilde{X},$$

so $GL_n(F)$ is non-abelian. By induction, the result holds for all $n \geq 2$.

Conclusion.

$$\boxed{GL_n(F) \text{ is non-abelian for every field } F \text{ and every } n \geq 2.}$$

□

Exercise 84 (D&F §1.4, Ex. 9)**.** *Prove that the binary operation of matrix multiplication of* 2×2 *matrices with real entries is associative.*

Intuition. Matrix multiplication is built from addition and multiplication of real numbers, and those operations are associative and commutative (for addition) in $\mathbb{R}$. So when you expand both $(AB)C$ and $A(BC)$ entrywise, you get the same linear combinations of the same products.

Proof. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \quad C = \begin{bmatrix} i & j \\ k & \ell \end{bmatrix} \in M_2(\mathbb{R}).$$

Compute $(AB)C$:

$$AB = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}, \qquad (AB)C = \begin{bmatrix} (ae+bg)i+(af+bh)k & (ae+bg)j+(af \\ (ce+dg)i+(cf+dh)k & (ce+dg)j+(cf \end{bmatrix}$$

Compute $A(BC)$:

$$BC = \begin{bmatrix} ei+fk & ej+f\ell \\ gi+hk & gj+h\ell \end{bmatrix}, \qquad A(BC) = \begin{bmatrix} a(ei+fk)+b(gi+hk) & a(ej+f\ell)+b(gj \\ c(ei+fk)+d(gi+hk) & c(ej+f\ell)+d(gj \end{bmatrix}$$

Entrywise comparison shows equality; for instance, using associativity and commutativity in $\mathbb{R}$,

$$(ae+bg)i+(af+bh)k = a(ei)+b(gi)+a(fk)+b(hk) = a(ei+fk)+b(gi+hk),$$

and similarly for the other three entries. Hence $(AB)C = A(BC)$.

Conclusion.

$$\boxed{\text{Matrix multiplication is associative on } M_2(\mathbb{R}).}$$

□

Exercise 85 (D&F §1.4, Ex. 10)**.** *Let*

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \;\middle|\; a, b, c \in \mathbb{R},\ a \neq 0,\ c \neq 0 \right\}.$$

(a) Compute the product of $\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ *and* $\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ *to show* G *is closed under multiplication.*

(b) Find $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}^{-1}$ *and deduce* G *is closed under inverses.*

(c) Deduce that G *is a subgroup of* $GL_2(\mathbb{R})$*.*

(d) Prove that the set of elements of G *with equal diagonal entries* ($a = c$) *is also a subgroup of* $GL_2(\mathbb{R})$*.*

. . . .

Intuition. Upper-triangular matrices multiply to upper-triangular matrices, and nonzero diagonal entries multiply to nonzero diagonals, so closure under multiplication is automatic. Inverting a triangular matrix keeps it triangular with inverted diagonal entries, so closure under inverses is also immediate. The "equal diagonals" condition is preserved under both multiplication and inversion.

. . . .

Proof. **(a) Closure under multiplication.** Let $X = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $Y = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ with $a_i, c_i \neq 0$. Then

$$XY = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix} \in G,$$

since $a_1a_2 \neq 0$ and $c_1c_2 \neq 0$.

(b) Inverses. Let $X = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ with $a, c \neq 0$. Seek X^{-1} in the same triangular form

$$Y = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}.$$

Enforce $XY = I$:

$$XY = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} ax & ay + bz \\ 0 & cz \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus

$ax = 1 \Rightarrow x = a^{-1}, \qquad cz = 1 \Rightarrow z = c^{-1}, \qquad ay+bz = 0 \Rightarrow y = -a^{-1}bz.$

Substitute $z = c^{-1}$ to get $y = -a^{-1}bc^{-1}$. Hence

$$X^{-1} = Y = \begin{bmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{bmatrix}.$$

(Verification from the other side:)

$$YX = \begin{bmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{bmatrix} \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} a^{-1}a + (-a^{-1}bc^{-1}) \cdot 0 & a^{-1}b + (-a^{-1}bc^{-1})c \\ 0 \cdot a + c^{-1} \cdot 0 & 0 \cdot b + c^{-1}c \end{bmatrix} = \left[\begin{matrix} 1 \\ 0 \end{matrix}\right.$$

Therefore $X^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}bc^{-1} \\ 0 & c^{-1} \end{bmatrix} \in G$.

(c) Subgroup of $GL_2(\mathbb{R})$. By (a) and (b), G is nonempty (it contains I), closed under multiplication and inverses, hence $G \leq GL_2(\mathbb{R})$.

(d) Equal-diagonal subgroup. Let

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \,\middle|\, a \in \mathbb{R}^{\times},\ b \in \mathbb{R} \right\} \subseteq G.$$

If $X_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & a_1 \end{bmatrix}$ and $X_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & a_2 \end{bmatrix}$, then

$$X_1X_2 = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1a_2 \\ 0 & a_1a_2 \end{bmatrix} \in H.$$

Moreover,

$$X^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}ba^{-1} \\ 0 & a^{-1} \end{bmatrix} \in H.$$

Thus H is nonempty and closed under multiplication and inverses, so $H \leq GL_2(\mathbb{R})$.

Conclusion.

$$\boxed{G = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : \ a, c \neq 0 \right\} \leq GL_2(\mathbb{R}) \quad \text{and} \quad H = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : \ a \neq 0 \right\} \leq GL_2(\mathbb{R}).}$$

□

Exercise 86 (D&F §1.4, Ex. 11). *Let*

$$H(F) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; a, b, c \in F \right\}.$$

Let

$$X = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, \qquad Y = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix} \in H(F).$$

(a) Compute XY and deduce that $H(F)$ is closed under multiplication. Exhibit explicit matrices with $XY \neq YX$ (so $H(F)$ is non-abelian).

(b) Find an explicit formula for X^{-1} and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law in $H(F)$ and deduce that $H(F)$ is a group of order $|F|^3$ when F is finite. (Do not assume matrix multiplication is associative.)

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(e) Prove that every nonidentity element of $H(\mathbb{R})$ has infinite order.

. . . .

Intuition. $H(F)$ is the group of unitriangular 3×3 matrices. Multiplication just adds the a's and c's, and adds b's with a little "carry" term af from the upper-right corner. That tiny cross term makes the group non-abelian and also explains the power formulas.

. . . .

Proof. **(a) Closure under multiplication (expanded).** Let

$$X = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix}.$$

Compute XY entry by entry:

$$XY = \begin{bmatrix} (1)(1)+(a)(0)+(b)(0) & (1)(d)+(a)(1)+(b)(0) & (1)(e)+(a)(f)+(b)(1) \\ (0)(1)+(1)(0)+(c)(0) & (0)(d)+(1)(1)+(c)(0) & (0)(e)+(1)(f)+(c)(1) \\ (0)(1)+(0)(0)+(1)(0) & (0)(d)+(0)(1)+(1)(0) & (0)(e)+(0)(f)+(1)(1) \end{bmatrix}.$$

Simplify row by row:

- First row: $[1,\ a+d,\ af+b+e]$ - Second row: $[0,\ 1,\ c+f]$ - Third row: $[0,\ 0,\ 1]$

So

$$XY = \begin{bmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{bmatrix} \in H(F).$$

This shows closure explicitly.

$$X = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}, \quad Y = \begin{bmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{bmatrix},$$

compute YX entry by entry:

$$YX = \begin{bmatrix} (1)(1)+(d)(0)+(e)(0) & (1)(a)+(d)(1)+(e)(0) & (1)(b)+(d)(c)+(e)(1) \\ (0)(1)+(1)(0)+(f)(0) & (0)(a)+(1)(1)+(f)(0) & (0)(b)+(1)(c)+(f)(1) \\ (0)(1)+(0)(0)+(1)(0) & (0)(a)+(0)(1)+(1)(0) & (0)(b)+(0)(c)+(1)(1) \end{bmatrix}.$$

Simplify row by row to obtain

$$YX = \begin{bmatrix} 1 & a+d & b+dc+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{bmatrix}.$$

Compare with

$$XY = \begin{bmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{bmatrix}.$$

The only potential difference is the $(1,3)$-entry: $af+b+e$ versus $b+dc+e$. In general $af \neq dc$, so $XY \neq YX$. For instance, take

$$X = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \ (a=1, c=0, b=0), \qquad Y = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \ (d=0, f=1, e=0).$$

Then

$$XY = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad YX = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix},$$

so $XY \neq YX$. This explicitly exhibits noncommutativity in $H(F)$.

(b) Inverses (fully expanded). Let

$$X = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in H(F).$$

Seek X^{-1} in the same shape:

$$Y = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}.$$

Solve from $XY = I$:

$$XY = \begin{bmatrix} 1 & a+x & af+b+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Thus

$$a + x = 0 \Rightarrow x = -a, \qquad c + z = 0 \Rightarrow z = -c, \qquad af + b + y = 0.$$

But here f refers to the $(2,3)$ entry of Y, i.e. z; substitute $z = -c$:

$$az + b + y = 0 \ \Rightarrow \ a(-c) + b + y = 0 \ \Rightarrow \ y = ac - b.$$

Hence the candidate inverse is

$$X^{-1} = Y = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}.$$

Verify $YX = I$ as well:

$$YX = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (-a)+a & (ac-b)+(-a)c+b \\ 0 & 1 & (-c)+c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Therefore $H(F)$ is closed under inverses and

$$\boxed{\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}.}$$

(c) Associativity and size. Compute both $(XY)Z$ and $X(YZ)$ with

$$Z = \begin{bmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{bmatrix}.$$

Using the product from (a),

$$(XY)Z = \begin{bmatrix} 1 & (a+d)+g & af+b+e\ +\ (a+d)i+h \\ 0 & 1 & (c+f)+i \\ 0 & 0 & 1 \end{bmatrix},$$

while

$$X(YZ) = \begin{bmatrix} 1 & a+(d+g) & a(f+i)+b+(d\,i+e+h) \\ 0 & 1 & c+(f+i) \\ 0 & 0 & 1 \end{bmatrix}.$$

These agree entrywise (rearranging terms), so multiplication in $H(F)$ is associative. If $|F| = q < \infty$, each of a, b, c has q choices, hence $|H(F)| = q^3$.

(d) Element orders in $H(\mathbb{Z}/2\mathbb{Z})$. Write $X(a,b,c) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ with $a, b, c \in \{0, 1\}$. A standard power formula (proved by induction) is

$$X(a,b,c)^n = \begin{bmatrix} 1 & na & nb + \binom{n}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{bmatrix}.$$

Over $\mathbb{Z}/2\mathbb{Z}$, $2 = 0$ and $\binom{2}{2} = 1$, so

$$X(a,b,c)^2 = \begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Hence every element has order dividing 4. A quick check gives:

$$\text{order } 1: \quad I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$\text{order } 2: \quad \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix};$$

$$\text{order } 4: \quad \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

(Indeed, $X(1,b,1)^2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \neq I$ but squaring again gives I.)

(e) Infinite order in $H(\mathbb{R})$ via an inductive power formula.

Claim (power formula). For any field F and any

$$X(a,b,c) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \in H(F),$$

one has for every integer $n \geq 1$,

$$X(a,b,c)^n = \begin{bmatrix} 1 & na & nb + \binom{n}{2} ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{bmatrix}.$$

Proof by induction on n. For $n = 1$ the formula is immediate. Assume it holds for some $n \geq 1$:

$$X^n = \begin{bmatrix} 1 & na & nb + \binom{n}{2} ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{bmatrix}.$$

Using the multiplication rule from part (a),

$$\begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_1 + a_2 & b_1 + a_1c_2 + b_2 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{bmatrix}.$$

Take $(a_1, b_1, c_1) = (na,\ nb + \binom{n}{2}ac,\ nc)$ and $(a_2, b_2, c_2) = (a, b, c)$. Then

$$X^{n+1} = X^n X = \begin{bmatrix} 1 & (n+1)a & \left(nb + \binom{n}{2}ac\right) + (na)c + b \\ 0 & 1 & (n+1)c \\ 0 & 0 & 1 \end{bmatrix}.$$

The $(1,3)$–entry simplifies using $\binom{n+1}{2} = \binom{n}{2} + n$:

$$\left(nb + \binom{n}{2}ac\right) + nac + b = (n+1)b + \left(\binom{n}{2} + n\right)ac = (n+1)b + \binom{n+1}{2}ac.$$

Thus the formula holds for $n+1$, completing the induction. □

Conclusion (infinite order over $\mathbb{R}$). Let $X(a, b, c) \in H(\mathbb{R})$ with $X \neq I$. By the formula,

$$X(a, b, c)^n = \begin{bmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{bmatrix}.$$

If $a \neq 0$, then the $(1,2)$–entry is $na \neq 0$ for all $n \geq 1$; if $c \neq 0$, then the $(2,3)$–entry is $nc \neq 0$ for all $n \geq 1$. If $a = c = 0$ but $b \neq 0$, then the $(1,3)$–entry is $nb \neq 0$ for all $n \geq 1$. Hence no nonidentity element can return to I in finitely many steps.

$$\boxed{\text{Every nonidentity element of } H(\mathbb{R}) \text{ has infinite order.}}$$

□

. . . .

1.5: The Quaternion Group

. . . .

Exercise 87 (D&F §1.5, Ex. 1)**.** *Compute the order of each of the elements in Q_8.*

. . . .

Intuition. The order of an element g is the smallest $n > 0$ with $g^n = 1$. - 1 and -1 are scalars, so their orders are immediate. - i, j, k square to -1, so they need four powers to return to 1. - Negatives of these also cycle back to 1 in four steps.

. . . .

Proof. By definition,

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}, \qquad i^2 = j^2 = k^2 = -1, \quad ij = k, \; jk = i, \; ki = j.$$

Identity and -1.

$$1^1 = 1 \quad \Rightarrow \quad |1| = 1, \qquad (-1)^2 = 1 \quad \Rightarrow \quad |-1| = 2.$$

i, j, k**.** Since $i^2 = -1$, we have $i^4 = (i^2)^2 = (-1)^2 = 1$.

Thus $|i| = 4$. Similarly $|j| = 4$ and $|k| = 4$.

Negatives of i, j, k. For example,

$$(-i)^2 = (-1)^2 \cdot i^2 = 1 \cdot (-1) = -1,$$

so $(-i)^4 = (-1)^2 = 1$. Thus $|-i| = 4$. The same calculation shows $|-j| = |-k| = 4$.

Conclusion.

$$\boxed{|1| = 1, \quad |-1| = 2, \quad |i| = |j| = |k| = |-i| = |-j| = |-k| = 4.}$$

□

Exercise 88 (D&F §1.5, Ex. 2)**.** *Write out the group tables for S_3, D_8, and Q_8.*

Intuition. List a convenient generating set and a consistent element order, then fill the Cayley table by the defining relations.
For S_3, use transpositions and 3-cycles; for $D_8 = \langle r, s \mid r^4 = s^2 = 1,\ srs = r^{-1}\rangle$, track how s flips powers of r; for Q_8, use $i^2 = j^2 = k^2 = -1$ and $ij = k$, $jk = i$, $ki = j$.

Proof. $S_3 = \{1, (12), (13), (23), (123), (132)\}$.

	1	(12)	(13)	(23)	(123)	(132)
1	1	(12)	(13)	(23)	(123)	(132)
(12)	(12)	1	(132)	(123)	(23)	(13)
(13)	(13)	(123)	1	(132)	(12)	(23)
(23)	(23)	(132)	(123)	1	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	1
(132)	(132)	(23)	(12)	(13)	1	(123)

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

	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r^3	r^2	r
sr	sr	sr^2	sr^3	s	r	1	r^3	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r	1	r^3
sr^3	sr^3	s	sr	sr^2	r^3	r^2	r	1

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ **with** $i^2 = j^2 = k^2 = -1$**,** $ij = k$**,** $jk = i$**,** $ki = j$**.**

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Each table follows by straightforward application of the defining relations and closure.

□

Exercise 89 (D&F §1.5, Ex. 3). *Find a set of generators and relations for Q_8.*

. . . .

Intuition. $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ is generated by i and j with $i^2 = j^2 = -1$ and $ij = k$.
The element -1 is central and equals $i^2 = j^2 = k^2$. Encapsulate these behaviors as concise relations.

. . . .

Proof. **A 4-generator presentation.**
One valid presentation is

$$Q_8 = \langle\, -1,\, i,\, j,\, k \;\mid\; i^2 = j^2 = k^2 = ijk = -1, \;\; (-1) \text{ central}\,\rangle.$$

Here -1 is explicitly central and $ijk = -1$ forces the standard multiplication rules $ij = k$, $jk = i$, $ki = j$, together with $ji = -k$, $kj = -i$, $ik = -j$.

A minimal 2-generator presentation (often used).
Setting $x = i$ and $y = j$, the relations of Q_8 are captured by

$$Q_8 \;\cong\; \big\langle x, y \;\big|\; x^4 = 1,\; x^2 = y^2,\; y^{-1}xy = x^{-1} \big\rangle.$$

Indeed, in Q_8 we have $i^4 = 1$, $i^2 = j^2 = -1$, and

$$y^{-1}xy = j^{-1}ij = (-j)ij = -(ji)j = -(-k)j = kj = -i = i^{-1},$$

so $y^{-1}xy = x^{-1}$ holds. Conversely, these relations force a normal form with at most the eight elements

$$\{1,\; x,\; x^2,\; x^3,\; y,\; yx,\; yx^2,\; yx^3\},$$

and the induced multiplication reproduces the quaternion rules, yielding an isomorphism to Q_8.

Conclusion.

$$\boxed{Q_8 = \langle -1, i, j, k \mid i^2 = j^2 = k^2 = ijk = -1,\ (-1) \text{ central}\rangle}$$

and

$$\boxed{Q_8 = \langle x, y \mid x^4 = 1,\ x^2 = y^2,\ y^{-1}xy = x^{-1}\rangle.}$$

□

. . . .

1.6: Homomorphisms and Isomorphisms

. . . .

Exercise 90 (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. **(a) Positive powers via induction.**
Base $n = 1$: $\varphi(x^1) = \varphi(x) = \varphi(x)^1$.
Inductive step: Suppose $\varphi(x^n) = \varphi(x)^n$ for some $n \geq 1$. Then

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

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

(b) Inverses and all integers.
First observe $\varphi(1_G) = 1_H$ (since $\varphi(1_G)\varphi(1_G) = \varphi(1_G)$ and cancel). Hence

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

so $\varphi(x^{-1}) = \varphi(x)^{-1}$. For $n \in \mathbb{Z}_{>0}$,

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

Combining with part (a) gives $\varphi(x^n) = \varphi(x)^n$ for every $n \in \mathbb{Z}$.

Conclusion.

$$\boxed{\forall x \in G,\ \forall n \in \mathbb{Z}, \quad \varphi(x^n) = \varphi(x)^n}.$$

□

Exercise 91 (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. **Orders are preserved by isomorphisms.**

Let $|x| = n \in \mathbb{Z}_{>0}$. Since φ is a homomorphism,

$\varphi(x)^n = \varphi(x^n) = \varphi(1) = 1$, so $|\varphi(x)| \leq n$.

If $|\varphi(x)| = k$, then $\varphi(x)^k = 1$ implies $\varphi(x^k) = 1$.

Because φ is injective, $x^k = 1$, hence $k \geq n$.

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

If $|x| = \infty$ and $|\varphi(x)| = m < \infty$, then $\varphi(x)^m = 1$ gives $\varphi(x^m) = 1$, hence $x^m = 1$ (injectivity), a contradiction.

Thus $|\varphi(x)| = \infty$ as well.

Counting elements of a given order.

Since φ is a bijection and preserves orders elementwise, it induces a bijection between elements of order n in G and in H.

Hence isomorphic groups have the same number of elements of each order $n \in \mathbb{Z}_{>0}$.

Failure for general homomorphisms.

If φ is only a homomorphism, the conclusion can fail.

For example, let $H = \{1\}$ and define $\theta : G \to H$ by $\theta(x) = 1$ for all $x \in G$.

Then every image has order 1, regardless of the orders in G.

Conclusion.

$$\boxed{\varphi \text{ isomorphism } \implies |\varphi(x)| = |x| \ \forall x \in G,}$$

and isomorphic groups match counts of order-n elements.

□

Exercise 92 (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. **Isomorphisms preserve "abelian".**

Assume $\varphi : G \to H$ is an isomorphism. If G is abelian and $x, y \in H$, write $x = \varphi(a)$, $y = \varphi(b)$ with $a, b \in G$ (surjectivity). Then

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

so H is abelian.

Conversely, if H is abelian, apply the previous argument to $\varphi^{-1} : H \to G$ to conclude G is abelian. Thus G abelian $\iff$ H abelian under isomorphism.

When a homomorphism forces the image to be abelian.

If $\varphi : G \to H$ is *surjective* and G is abelian, then for any $x, y \in H$ choose $a, b \in G$ with $\varphi(a) = x$, $\varphi(b) = y$. Since $ab = ba$,

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

so H is abelian.

Injective alone does not suffice.
There exist injective homomorphisms from abelian groups into nonabelian groups (e.g. embeddings into a nonabelian overgroup); hence injectivity by itself cannot force the codomain to be abelian.

Conclusion.

$$\boxed{\begin{gathered}\varphi : G \cong H \implies (G \text{ abelian} \iff H \text{ abelian}),\\ \text{and if } \varphi \text{ is only a homomorphism, surjectivity is needed.}\end{gathered}}$$

□

Exercise 93 (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. In $\mathbb{R}^\times$, if $x \in \mathbb{R}^\times$ has finite order, then $x^n = 1$ for some $n \geq 1$. Over $\mathbb{R}$, the only real roots of $t^n - 1$ with $n \geq 1$ are $t = 1$ and, when n is even, $t = -1$. Hence the only elements of finite order in $\mathbb{R}^\times$ are

$$1 \text{ (order 1)} \quad \text{and} \quad -1 \text{ (order 2)}.$$

All other real nonzero numbers have infinite order under multiplication.

In contrast, $\mathbb{C}^\times$ contains i with $i^4 = 1$ and $i^k \neq 1$ for $1 \leq k < 4$, so $|i| = 4$. Thus $\mathbb{C}^\times$ has an element of order 4, while $\mathbb{R}^\times$ does not.

Since isomorphisms preserve orders of elements, the two groups cannot be isomorphic.

Conclusion.

$$\boxed{\mathbb{R}^\times \ncong \mathbb{C}^\times}.$$

□

Exercise 94 (D&F §1.6, Ex. 5)**.** *Prove that the additive groups* $\mathbb{R}$ *and* $\mathbb{Q}$ *are not isomorphic.*

. . . .

Intuition. Any isomorphism must be a bijection. But $(\mathbb{R}, +)$ is uncountable while $(\mathbb{Q}, +)$ is countable, so there cannot be a bijection between the underlying sets.

. . . .

Proof. Suppose, for contradiction, that $\varphi : (\mathbb{R}, +) \to (\mathbb{Q}, +)$ is an isomorphism. Then φ is in particular a bijection of sets.

However, $\mathbb{R}$ is uncountable, whereas $\mathbb{Q}$ is countable. No bijection can exist between a countable set and an uncountable set. This contradiction shows that such an isomorphism φ cannot exist.

Conclusion.

$$\boxed{(\mathbb{R}, +) \ \not\cong \ (\mathbb{Q}, +)}\,.$$

□

Exercise 95 (D&F §1.6, Ex. 6)**.** *Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.*

. . . .

Intuition. If $\varphi : \mathbb{Q} \to \mathbb{Z}$ were an isomorphism, then $a := \varphi(1)$ would have to be divisible by *every* positive integer (since $\varphi(\frac{1}{n})$ would be an integer whose n-fold sum is a). The only integer divisible by all n is 0, which forces φ to be non-injective.

. . . .

Proof. Suppose for contradiction that $\varphi : (\mathbb{Q}, +) \to (\mathbb{Z}, +)$ is an isomorphism. Let $a = \varphi(1) \in \mathbb{Z}$.

For any $n \in \mathbb{Z}_{>0}$,

$$a = \varphi(1) = \varphi\Big(n \cdot \tfrac{1}{n}\Big) = n\,\varphi\Big(\tfrac{1}{n}\Big),$$

so $n \mid a$. Hence a is divisible by every positive integer, which implies $a = 0$.

But then for any $m \in \mathbb{Z}$,

$$\varphi(m) = \varphi(m \cdot 1) = m\,\varphi(1) = m \cdot 0 = 0,$$

so φ is not injective—contradiction. Therefore no isomorphism exists between $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$.

Conclusion.

$$\boxed{(\mathbb{Z}, +) \ \not\cong\ (\mathbb{Q}, +)}$$

□

Exercise 96 (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. Recall

$$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}, \qquad r^4 = 1,\ s^2 = 1,\ srs = r^{-1}.$$

Then $|r| = 4$, $|r^2| = 2$, and each of s, sr, sr^2, sr^3 has order 2. Hence D_8 has *five* elements of order 2:

$$r^2,\ s,\ sr,\ sr^2,\ sr^3.$$

On the other hand,

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

has exactly one element of order 2, namely -1; all of $i, \pm i, \pm j, \pm k$ have order 4.

Because an isomorphism must preserve element orders and their counts, D_8 and Q_8 cannot be isomorphic.

Conclusion.

$$\boxed{D_8 \ \not\cong\ Q_8}.$$

□

Exercise 97 (D&F §1.6, Ex. 8)**.** *Prove that if $n \neq m$, then S_n and S_m are not isomorphic.*

. . . .

Intuition. Isomorphisms are bijections. But $|S_n| = n!$ and $|S_m| = m!$; when $n \neq m$ these sizes differ, so no bijection exists.

. . . .

Proof. For $n \in \mathbb{Z}_{>0}$, the symmetric group S_n has order $n!$. If $n \neq m$, then $n! \neq m!$.

Suppose, for contradiction, that $\varphi : S_n \to S_m$ is an isomorphism with $n \neq m$. Then φ is a bijection of sets, forcing $|S_n| = |S_m|$, i.e. $n! = m!$, contrary to $n \neq m$.

Therefore no isomorphism can exist when $n \neq m$.

Conclusion.

$$\boxed{n \neq m \implies S_n \ncong S_m}$$

□

Exercise 98 (D&F §1.6, Ex. 9)**.** *Prove that D_{24} and S_4 are not isomorphic.*

. . . .

Intuition. Compare element orders. D_{24} (order 24) has a rotation of order 12, while S_4 has no element of order 12 (possible orders in S_4 are $1, 2, 3, 4$ only).

. . . .

Proof. D_{24} **has elements of order** 12.
Let $D_{24} = \langle r, s \mid r^{12} = s^2 = 1,\ srs = r^{-1}\rangle$. Then $|r| = 12$, so in particular r (and also r^5, r^7, r^{11}) has order 12.

S_4 **has no element of order** 12.
The order of a permutation is the l.c.m. of its disjoint cycle lengths. In S_4 the only cycle-type possibilities are:

$$(),\ (ab),\ (ab)(cd),\ (abc),\ (abcd),$$

with orders $1, 2, 2, 3, 4$, respectively. Thus S_4 has no element of order 12.

Since isomorphisms preserve orders of elements, a group with an element of order 12 cannot be isomorphic to one without such an element. Hence $D_{24} \not\cong S_4$.

Conclusion.

$$\boxed{D_{24} \not\cong S_4}$$

□

Exercise 99 (D&F §1.6, Ex. 10). *Let Δ and Ω be finite sets with $|\Delta| = |\Omega|$ and let $\theta : \Delta \to \Omega$ be a bijection. Define*

$$\varphi : S_\Delta \longrightarrow S_\Omega, \qquad \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1}.$$

Prove:

(a) φ is well defined (i.e. sends permutations of Δ to permutations of Ω).

(b) φ is a bijection $S_\Delta \to S_\Omega$.

(c) φ is a homomorphism: $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

. . . .

Intuition. "Relabeling" the underlying set by a bijection θ turns any permutation on Δ into a permutation on Ω via conjugation $\theta(\cdot)\theta^{-1}$. Conjugation preserves composition and is invertible (inverse is conjugation by θ^{-1}).

. . . .

Proof. **(a) Well defined.**
For $\sigma \in S_\Delta$, the map $\varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} : \Omega \to \Omega$ is a composition of bijections, hence a bijection. Thus $\varphi(\sigma) \in S_\Omega$.

(b) φ is a bijection.
Define $\psi : S_\Omega \to S_\Delta$ by $\psi(\tau) = \theta^{-1} \circ \tau \circ \theta$. Then for $\sigma \in S_\Delta$,

$$(\psi \circ \varphi)(\sigma) = \theta^{-1} \circ (\theta \circ \sigma \circ \theta^{-1}) \circ \theta = \sigma,$$

and for $\tau \in S_\Omega$,

$$(\varphi \circ \psi)(\tau) = \theta \circ (\theta^{-1} \circ \tau \circ \theta) \circ \theta^{-1} = \tau.$$

Hence $\psi = \varphi^{-1}$, so φ is bijective.

(c) Homomorphism property.
For $\sigma, \tau \in S_\Delta$,

$$\varphi(\sigma \circ \tau) = \theta \circ (\sigma \circ \tau) \circ \theta^{-1} = (\theta \circ \sigma \circ \theta^{-1}) \circ (\theta \circ \tau \circ \theta^{-1}) = \varphi(\sigma) \circ \varphi(\tau).$$

Thus φ is a group isomorphism.

Conclusion.

$$\boxed{S_\Delta \;\cong\; S_\Omega \;\text{ via }\; \sigma \mapsto \theta \circ \sigma \circ \theta^{-1}}.$$

□

Exercise 100 (D&F §1.6, Ex. 11)**.** *Let A and B be groups. Prove that $A \times B \cong B \times A$.*

. . . .

Intuition. Swap the coordinates. The map $(a, b) \mapsto (b, a)$ clearly respects the product and has itself as inverse.

. . . .

Proof. **Define the map.**
Let $\varphi : A \times B \to B \times A$ by $\varphi(a, b) = (b, a)$.

Homomorphism.
For $(a, b), (c, d) \in A \times B$,

$$\varphi\big((a, b)(c, d)\big) = \varphi(ac, bd) = (bd, ac) = (b, a)(d, c) = \varphi(a, b)\,\varphi(c, d),$$

so φ is a homomorphism.

Bijective (explicit inverse).
Define $\psi : B \times A \to A \times B$ by $\psi(b, a) = (a, b)$. Then $\psi \circ \varphi = \mathrm{id}_{A\times B}$ and $\varphi \circ \psi = \mathrm{id}_{B\times A}$, hence φ is a bijection with inverse ψ.

Conclusion.

$$\boxed{A \times B \;\cong\; B \times A \quad \text{via} \quad (a, b) \mapsto (b, a).}$$

$\square$

Exercise 101 (D&F §1.6, Ex. 12)**.** *Let A, B, C be groups and set $G = A \times B$, $H = B \times C$. Prove that $G \times C \cong A \times H$.*

. . . .

Intuition. Just "regroup the parentheses." The map $((a, b), c) \mapsto (a, (b, c))$ is the obvious coordinate shuffle; it preserves componentwise multiplication and has an obvious inverse.

. . . .

Proof. **Define the map.**
Let $\varphi : G \times C \to A \times H$ be

$$\varphi\bigl((a, b), c\bigr) = \bigl(a, (b, c)\bigr).$$

Homomorphism.
For $((a_1, b_1), c_1), ((a_2, b_2), c_2) \in G \times C$,

$$\varphi\bigl((a_1a_2, b_1b_2), c_1c_2\bigr) = \bigl(a_1a_2, (b_1b_2, c_1c_2)\bigr) = \bigl(a_1, (b_1, c_1)\bigr)\bigl(a_2, (b_2, c_2)\bigr) = \varphi\bigl((a_1, b_1), c_1\bigr)\,\varphi$$

Bijective (explicit inverse).
Define $\psi : A \times H \to G \times C$ by $\psi\bigl(a, (b, c)\bigr) = \bigl((a, b), c\bigr)$. Then

$$\psi\circ\varphi\bigl((a, b), c\bigr) = \psi\bigl(a, (b, c)\bigr) = \bigl((a, b), c\bigr), \qquad \varphi\circ\psi\bigl(a, (b, c)\bigr) = \varphi\bigl((a, b), c\bigr) = \bigl(a, (b, c)\bigr).$$

Hence $\psi = \varphi^{-1}$ and φ is a bijection.

Conclusion.

$$\boxed{G \times C \;\cong\; A \times H \quad \text{via} \quad ((a, b), c) \longmapsto (a, (b, c)).}$$

□

Exercise 102 (D&F §1.6, Ex. 13). *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.*

(a) Prove that $\varphi(G) = \{ \varphi(g) \mid g \in G \}$ is a subgroup of H.

(b) Prove that if φ is injective, then $G \cong \varphi(G)$.

. . . .

Intuition. Images of homomorphisms are stable under the operation and inverses because "φ respects multiplication and inversion." For (b), restrict the codomain to $\varphi(G)$; then φ becomes a bijective homomorphism, i.e. an isomorphism.

. . . .

Proof. **(a) $\varphi(G)$ is a subgroup of H.**
Nonempty: $\varphi(1_G) = 1_H \in \varphi(G)$.
Closure: If $a = \varphi(\alpha)$ and $b = \varphi(\beta)$ lie in $\varphi(G)$, then

$$ab = \varphi(\alpha)\varphi(\beta) = \varphi(\alpha\beta) \in \varphi(G).$$

Inverses: If $a = \varphi(\alpha) \in \varphi(G)$, then

$$a^{-1} = \varphi(\alpha)^{-1} = \varphi(\alpha^{-1}) \in \varphi(G).$$

Thus $\varphi(G) \leq H$.

(b) Injective ⇒ isomorphism onto the image.
Consider the same function with restricted codomain,

$$\varphi^* : G \longrightarrow \varphi(G), \qquad \varphi^*(g) = \varphi(g).$$

This is a homomorphism and is surjective by definition of $\varphi(G)$. If φ is injective, then so is φ^*, hence φ^* is a bijective homomorphism—an isomorphism. Therefore $G \cong \varphi(G)$.

Conclusion.

$$\boxed{\varphi(G) \leq H \quad \text{and} \quad \varphi \text{ injective} \implies G \cong \varphi(G)}.$$

□

Exercise 103 (D&F §1.6, Ex. 14)**.** *Let G and H be groups and let $\varphi : G \to H$ be a homomorphism. Prove that* $\ker\varphi$ *is a subgroup of* G*. Prove that φ is injective if and only if* $\ker\varphi = \{1\}$ *(i.e., the kernel of phi is the identity subgroup of G).*

. . . .

Intuition. The kernel is the "preimage of the identity." Homomorphisms preserve multiplication and inverses, so this set is automatically closed under the group law. For injectivity: two elements have the same image exactly when their quotient lies in the kernel. So a trivial kernel forces distinct elements to map distinctly, and conversely.

. . . .

Proof. **Step 1.** $\ker\varphi$ **is a subgroup.**
- Nonempty: $\varphi(1_G) = 1_H$, so $1_G \in \ker\varphi$.
- Closure: If $a, b \in \ker\varphi$, then $\varphi(ab) = \varphi(a)\varphi(b) = 1_H \cdot 1_H = 1_H$, hence $ab \in \ker\varphi$.
- Inverses: If $a \in \ker\varphi$, then $\varphi(a^{-1}) = \varphi(a)^{-1} = 1_H^{-1} = 1_H$, so $a^{-1} \in \ker\varphi$.

Thus $\ker\varphi \leq G$.

Step 2. If φ **injective, then** $\ker\varphi = \{1_G\}$**.**
Suppose $a \in \ker\varphi$. Then $\varphi(a) = 1_H = \varphi(1_G)$. Injectivity gives $a = 1_G$. So $\ker\varphi = \{1_G\}$.

Step 3. If $\ker\varphi = \{1_G\}$**, then** φ **is injective.**
Suppose $\varphi(x) = \varphi(y)$. Then

$$1_H = \varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}),$$

so $xy^{-1} \in \ker\varphi = \{1_G\}$. Thus $x = y$. Hence φ is injective.

Conclusion.

$$\boxed{\ker\varphi \leq G \quad \text{and} \quad \varphi \text{ injective} \iff \ker\varphi = \{1_G\}.}$$

□

Exercise 104 (D&F §1.6, Ex. 15)**.** *Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercise 14).*

. . . .

Intuition. On $(\mathbb{R}^2, +)$ and $(\mathbb{R}, +)$, addition is coordinatewise. Projecting to the first coordinate clearly respects addition. The kernel should be all vectors whose first coordinate is 0.

. . . .

Proof. **Homomorphism.**
For $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$,

$$\pi\big((x_1, y_1)+(x_2, y_2)\big) = \pi(x_1+x_2,\ y_1+y_2) = x_1+x_2 = \pi(x_1, y_1)+\pi(x_2, y_2),$$

so π is a group homomorphism $(\mathbb{R}^2, +) \to (\mathbb{R}, +)$.

Kernel.
By definition,

$$\ker \pi = \{(x, y) \in \mathbb{R}^2 :\ \pi(x, y) = 0\} = \{(x, y) \in \mathbb{R}^2 :\ x = 0\} = \{(0, y) \in \mathbb{R}^2 : y \in \mathbb{R}\}.$$

Conclusion.

$$\boxed{\pi \text{ is a homomorphism and } \ker \pi = \{(0, y) \in \mathbb{R}^2 : y \in \mathbb{R}\}}.$$

□

Exercise 105 (D&F §1.6, Ex. 16)**.** *Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps*

$$\pi_1 : G \to A \quad \textit{and} \quad \pi_2 : G \to B$$

defined by $\pi_1((a,b)) = a$ and $\pi_2((a,b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).

Intuition. Multiplication in $A \times B$ is coordinatewise. Projecting to a coordinate respects multiplication automatically. The kernel of a projection is "everything with that coordinate equal to the identity."

Proof. **Homomorphism checks.**
For $(a,b),(c,d) \in A \times B$,

$$\pi_1\big((a,b)(c,d)\big) = \pi_1(ac,bd) = ac = \pi_1(a,b)\,\pi_1(c,d),$$

so π_1 is a homomorphism. Similarly,

$$\pi_2\big((a,b)(c,d)\big) = \pi_2(ac,bd) = bd = \pi_2(a,b)\,\pi_2(c,d),$$

so π_2 is a homomorphism.

Kernels.
By definition,

$$\ker\pi_1 = \{(a,b) \in A \times B : \pi_1(a,b) = 1_A\} = \{(1_A,b) : b \in B\},$$
$$\ker\pi_2 = \{(a,b) \in A \times B : \pi_2(a,b) = 1_B\} = \{(a,1_B) : a \in A\}.$$

Each is a subgroup of $A \times B$ by Exercise 14 (kernels are subgroups).

Conclusion.

$$\boxed{\pi_1, \pi_2 \text{ are homomorphisms}, \qquad \ker\pi_1 = \{(1_A,b) : b \in B\}, \quad \ker\pi_2 = \{(a,1_B) : a \in A}$$

□

Exercise 106 (D&F §1.6, Ex. 17)**.** *Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.*

. . . .

Intuition. The inversion map reverses multiplication: $(ab)^{-1} = b^{-1}a^{-1}$. It will be a homomorphism exactly when reversing order does nothing—that is, when $a^{-1}b^{-1} = b^{-1}a^{-1}$ for all a, b, equivalently when $ab = ba$.

. . . .

Proof. **(⇒) If G is abelian, inversion is a homomorphism.** Assume $ab = ba$ for all $a, b \in G$. Then for any a, b,

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

so the map $\iota : G \to G$, $\iota(g) = g^{-1}$, satisfies $\iota(ab) = \iota(a)\,\iota(b)$ and is a homomorphism.

(⇐) If inversion is a homomorphism, then G is abelian. Assume ι is a homomorphism. For any $a, b \in G$,

$$\iota(ab) = (ab)^{-1} = b^{-1}a^{-1} = \iota(a)\,\iota(b) = a^{-1}b^{-1}.$$

Taking inverses of both sides gives

$$ab = \left(a^{-1}b^{-1}\right)^{-1} = ba.$$

Hence G is abelian.

Conclusion.

$$\boxed{\iota(g) = g^{-1} \text{ is a homomorphism } \iff G \text{ is abelian.}}$$

□

Exercise 107 (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. **(⇒) If $g \mapsto g^2$ is a homomorphism, then G is abelian.** Assume $\psi(g) = g^2$ satisfies $\psi(ab) = \psi(a)\psi(b)$ for all $a, b \in G$. Then

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

But $(ab)^2 = abab$, so $abab = aabb$. Left–multiply by a^{-1} and right–multiply by b^{-1} to obtain

$$bab = abb \implies ba = ab.$$

Since a, b were arbitrary, G is abelian.

(⇐) If G is abelian, then $g \mapsto g^2$ is a homomorphism.
If $ab = ba$ for all a, b, then

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

so ψ is a homomorphism.

Conclusion.

$$\boxed{g \mapsto g^2 \text{ is a homomorphism} \iff G \text{ is abelian.}}$$

□

Exercise 108 (D&F §1.6, Ex. 19)**.** *Let* $G = \{\, z \in \mathbb{C} \mid z^n = 1$ *for some* $n \in \mathbb{Z}_{>0} \,\}$*. Prove that for any fixed integer* $k > 1$ *the map* $G \to G$ *defined by* $z \mapsto z^k$ *is a surjective homomorphism but is not an isomorphism.*

. . . .

Intuition. G is the group of all complex roots of unity under multiplication. The k-th power map respects multiplication automatically. Surjectivity holds because every root of unity has a k-th root which is again a root of unity (just increase the order by a factor of k). Non-isomorphism: all k-th roots of unity map to 1, so the kernel is nontrivial when $k > 1$.

. . . .

Proof. **Homomorphism.**
For $z, w \in G$, we have $(zw)^k = z^k w^k$, so $z \mapsto z^k$ is a group homomorphism $G \to G$.

Surjectivity.
Let $\zeta \in G$. Then $\zeta = e^{2\pi i m/n}$ for some integers m, n with $n \geq 1$. Set $\eta = e^{2\pi i m/(kn)}$. Then $\eta \in G$ (it is a (kn)-th root of unity) and $\eta^k = e^{2\pi i m/n} = \zeta$. Hence every element of G has a preimage, so the map is surjective.

Not an isomorphism (nontrivial kernel).
The kernel is $\{z \in G : z^k = 1\} = \mu_k$, the set of k-th roots of unity, which has $k > 1$ elements. Thus the homomorphism is not injective and therefore not an isomorphism.

Conclusion.

$$\boxed{z \mapsto z^k \text{ is a surjective homomorphism } (G \to G) \text{ but not an isomorphism for } k > 1.}$$

□

Exercise 109 (D&F §1.6, Ex. 20)**.** *Let G be a group and let* Aut(G) *be the set of all isomorphisms from G onto G. Prove that* Aut(G) *is a group under function composition (called the automorphism group of G and the elements of* 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. **Closure under composition.**
If $\varphi, \psi \in \mathrm{Aut}(G)$, then both are bijective homomorphisms $G \to G$. The composition $\psi \circ \varphi$ is a homomorphism and a bijection, hence an automorphism. Thus $\psi \circ \varphi \in \mathrm{Aut}(G)$.

Associativity.
Function composition is associative: for all $\alpha, \beta, \gamma : G \to G$, we have $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$.

Identity element.
The identity map $\mathrm{id}_G : G \to G$ is a bijective homomorphism, hence $\mathrm{id}_G \in \mathrm{Aut}(G)$, and for any $\varphi \in \mathrm{Aut}(G)$ we have $\mathrm{id}_G \circ \varphi = \varphi = \varphi \circ \mathrm{id}_G$.

Inverses.
If $\varphi \in \mathrm{Aut}(G)$, then φ is a bijection with inverse map $\varphi^{-1} : G \to G$. Since φ is a homomorphism, its inverse is also a homomorphism (indeed, for $x, y \in G$,

$$\varphi\big(\varphi^{-1}(xy)\big) = xy = \varphi\big(\varphi^{-1}(x)\varphi^{-1}(y)\big) \Rightarrow\ \varphi^{-1}(xy) = \varphi^{-1}(x)\,\varphi^{-1}(y)),$$

so $\varphi^{-1} \in \mathrm{Aut}(G)$. Moreover, $\varphi \circ \varphi^{-1} = \mathrm{id}_G = \varphi^{-1} \circ \varphi$.

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

Conclusion.

$$\boxed{\mathrm{Aut}(G) \text{ is a group under composition (the automorphism group of } G\text{).}}$$

□

Exercise 110 (D&F §1.6, Ex. 21)**.** *Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$ (cf. Exercise 20).*

. . . .

Intuition. We view $\mathbb{Q}$ as the additive group $(\mathbb{Q}, +)$. Multiplying by a fixed rational $k \neq 0$ clearly respects addition (distributivity) and is bijective with inverse multiplication by $1/k$.

. . . .

Proof. **Homomorphism.**
Define $\varphi : \mathbb{Q} \to \mathbb{Q}$ by $\varphi(q) = kq$ with fixed $k \in \mathbb{Q}^{\times}$ (AKA fix a nonzero k in The Rational Numbers). For all $a, b \in \mathbb{Q}$,

$$\varphi(a + b) = k(a + b) = ka + kb = \varphi(a) + \varphi(b),$$

so φ is a group homomorphism $(\mathbb{Q}, +) \to (\mathbb{Q}, +)$.
Bijectivity.
Surjectivity: Given $y \in \mathbb{Q}$, take $x = y/k \in \mathbb{Q}$ (since $k \neq 0$ and $1/k \in \mathbb{Q}$). Then $\varphi(x) = y$.
Injectivity: If $\varphi(a) = \varphi(b)$, then $ka = kb$, hence $a = b$ because $k \neq 0$.
Since φ is a bijective homomorphism, it is an automorphism of $(\mathbb{Q}, +)$.
Equivalently, the inverse φ^{-1} is multiplication by $1/k \in \mathbb{Q}$.

Conclusion.

$$\boxed{\forall k \in \mathbb{Q}^{\times}, \quad (\mathbb{Q}, +) \xrightarrow{q \mapsto kq} (\mathbb{Q}, +) \text{ is an automorphism.}}$$

□

Exercise 111 (D&F §1.6, Ex. 22)**.** *Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).*

Intuition. In an abelian group, elements commute, so powers "distribute" over products: $(ab)^k = a^k b^k$ for any integer k. For $k = -1$ this is the inversion map $a \mapsto a^{-1}$, which is its own inverse and hence a bijective homomorphism.

Proof. **Homomorphism for a fixed $k \in \mathbb{Z}$.**
Let $\varphi : A \to A$ be defined by $\varphi(a) = a^k$. For all $a, b \in A$:
- If $k \geq 0$ then

$$(ab)^k = (ab)(ab) \cdots (ab) \quad (k \text{ factors}) = a^k b^k,$$

since A is abelian.
- If $k < 0$, write $k = -m$ with $m > 0$. Then

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

Thus in either case $\varphi(ab) = \varphi(a)\varphi(b)$, so φ is a homomorphism.
Case $k = -1$: φ is an automorphism.
When $k = -1$, $\varphi(a) = a^{-1}$. We already have φ is a homomorphism because A is abelian. Moreover, φ is bijective with inverse equal to itself: $\varphi^{-1} = \varphi$ since $(a^{-1})^{-1} = a$. Hence φ is an automorphism.

Conclusion.

$$\boxed{a \mapsto a^k \text{ is a homomorphism on any abelian group } A; \text{ for } k = -1 \text{ it is an automorph}}$$

□

Exercise 112 (D&F §1.6, Ex. 23)**.** *Let G be a finite group which possesses an automorphism σ such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called fixed point free of order 2). [Show that every element of G can be written in the form $x^{-1}\sigma(x)$ and apply σ to such an expression.]*

. . . .

Intuition. Build $\varphi(x) = x^{-1}\sigma(x)$. Injectivity on finite G makes it bijective, so every g is $x^{-1}\sigma(x)$. Applying σ to this representation shows $\sigma(g) = g^{-1}$, i.e. σ acts as inversion. A homomorphism that equals inversion forces $ab = ba$.

. . . .

Proof. **Step 1. The map $\varphi(x) = x^{-1}\sigma(x)$ is bijective.**
Define $\varphi : G \to G$ by $\varphi(x) = x^{-1}\sigma(x)$. If $\varphi(x) = \varphi(y)$, then

$$x^{-1}\sigma(x) = y^{-1}\sigma(y) \implies \sigma(y) = yx^{-1}\sigma(x).$$

Apply σ and use $\sigma^2 = \text{id}$:

$$y = \sigma(\sigma(y)) = \sigma\big(yx^{-1}\sigma(x)\big) = \sigma(yx^{-1})\,\sigma(\sigma(x)) = \sigma(yx^{-1})\,x.$$

Right–multiply by x^{-1} to get $\sigma(yx^{-1}) = yx^{-1}$. Since σ is fixed point free, $yx^{-1} = 1$, so $x = y$. Thus φ is injective; G finite $\Rightarrow$ φ bijective. Hence every $g \in G$ has the form $g = x^{-1}\sigma(x)$.

Step 2. σ acts as inversion.
Take $g = x^{-1}\sigma(x)$. Then

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

Hence $\sigma(g) = g^{-1}$ for all $g \in G$.

Step 3. Commutativity of G.
For any $a, b \in G$,

$$\sigma(ab) = \sigma(a)\sigma(b) = a^{-1}b^{-1}.$$

But from Step 2 we also have $\sigma(ab) = (ab)^{-1} = b^{-1}a^{-1}$. Therefore $a^{-1}b^{-1} = b^{-1}a^{-1}$, so $ab = ba$.

Conclusion.

$$\boxed{\text{If G is finite and admits a fixed point free involutive automorphism σ, then G is ab}}$$

□

Exercise 113 (D&F §1.6, Ex. 24)**.** *Let G be a finite group and let x and y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$. [See Exercise 6 in Section 2.]*

. . . .

Intuition. Set $t = xy$. Because $x^2 = y^2 = 1$, one checks $xtx = t^{-1}$, i.e. x conjugates t to t^{-1}. Thus $\langle x, t\rangle$ satisfies the dihedral relations $t^n = 1$, $x^2 = 1$, $xtx = t^{-1}$ with $n = |t|$. Show every element has a unique normal form $x^i t^j$ ($i \in \{0, 1\}$, $0 \le j < n$), giving $|G| = 2n$, then identify G with D_{2n} by $r \mapsto t$, $s \mapsto x$.

. . . .

Proof. **Step 1. Dihedral relations in G.**
Let $t = xy$ and $n = |t| \in \mathbb{Z}_{>0}$. Since $x^2 = y^2 = 1$,

$$xtx = x(xy)x = (xx)yx = yx = (xy)^{-1} = t^{-1}.$$

Thus $t^n = 1$, $x^2 = 1$, and $xtx = t^{-1}$ hold in G. Hence $\langle x, t\rangle$ is a quotient of the abstract dihedral group $\langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1}\rangle$.

Step 2. Normal form and cardinality $|G| = 2n$.
Since $G = \langle x, y\rangle$ and $y = xt$, we have $G = \langle x, t\rangle$. Using $xt = t^{-1}x$ (equivalently $xtx = t^{-1}$), repeatedly move x's leftward to write any word uniquely as

$$x^i t^j, \qquad i \in \{0, 1\}, \quad 0 \le j < n.$$

Uniqueness: if $x^i t^j = x^{i'} t^{j'}$, move the x's to the same side to obtain $t^j = t^{j'}$ if $i = i'$, or $x = t^{j-j'}x$ if $i \ne i'$, whence $t^{j-j'} = 1$; since $|t| = n$, this forces $j \equiv j' \pmod{n}$ and then $i = i'$. Therefore the $2n$ elements $\{x^i t^j\}$ are all distinct, so $|G| = 2n$.

Step 3. Explicit isomorphism with D_{2n}.
Let $D_{2n} = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$. Define

$$\varphi : D_{2n} \longrightarrow G, \qquad \varphi(s^i r^j) = x^i t^j \quad (i \in \{0, 1\},\ 0 \le j < n).$$

This is well defined because x, t satisfy the same relations as s, r. It is a homomorphism by construction. It is surjective since every element of G is some $x^i t^j$. Finally $|D_{2n}| = 2n = |G|$, so φ is a bijection. Hence φ is an isomorphism and $G \cong D_{2n}$.

Conclusion.

$$\boxed{G = \langle x, y \rangle \text{ with } x^2 = y^2 = 1,\ x \neq y,\ n = |xy| \implies G \cong D_{2n}.}$$

□

Exercise 114 (D&F §1.6, Ex. 25)**.** *Let $n \in \mathbb{Z}_{>0}$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.*

(a) Prove that the matrix

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

is the matrix of the linear transformation which rotates the x, y-plane about the origin counterclockwise by θ radians.

(b) Prove that the map $\varphi : D_{2n} \to GL_2(\mathbb{R})$ defined on generators by

$$\varphi(r) = R, \qquad \varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} =: \ S$$

extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.

(c) Prove that the homomorphism φ in part (b) is injective.

. . . .

Intuition. R is the standard rotation matrix; it preserves distance and rotates angles by θ. S reflects across the line $y = x$. These realize the dihedral relations: $R^n = I$, $S^2 = I$, and $SRS = R^{-1}$. Injectivity: if $\varphi(s^i r^j) = I$, then $\det(S^i R^j) = (-1)^i = 1$ forces $i = 0$, whence $R^j = I$ and $j \equiv 0 \pmod{n}$.

. . . .

Proof. **(a) R is rotation by θ.**
For $(x, y) \in \mathbb{R}^2$,

$$R\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix}.$$

Then

$$\|(x,y)\|^2 = x^2+y^2 \quad \text{and} \quad \left\|R(x,y)\right\|^2 = (x\cos\theta - y\sin\theta)^2 + (x\sin\theta + y\cos\theta)^2 = x^2+y^2,$$

so R preserves distance. A direct dot-product calculation shows that the angle with the x-axis increases by θ, hence R is counterclockwise rotation by θ.

(b) φ respects the dihedral relations.
In $D_{2n} = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1} \rangle$ it suffices to check these on matrices.
First,

$$R^n = I \quad (\text{rotation by } n\theta = 2\pi), \qquad S^2 = I.$$

Now compute SRS explicitly:

$$SR = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix}.$$

Then

$$(SR)S = \begin{pmatrix} \sin\theta & \cos\theta \\ \cos\theta & -\sin\theta \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

But this is exactly

$$R^{-1} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Thus $SRS = R^{-1}$. All defining relations hold, so φ extends uniquely to a homomorphism $D_{2n} \to GL_2(\mathbb{R})$.
(c) φ is injective.
Every element of D_{2n} has the form $s^i r^j$ with $i \in \{0, 1\}$ and $0 \le j < n$. Suppose $\varphi(s^i r^j) = I$. Taking determinants,

$$1 = \det(I) = \det\big(\varphi(s^i r^j)\big) = \det(S)^i \det(R)^j = (-1)^i \cdot 1^j,$$

so $i = 0$. Hence $R^j = I$, which implies $j \equiv 0 \pmod{n}$. Therefore the only element mapping to I is the identity, so $\ker\varphi = \{1\}$ and φ is injective.

Conclusion.

$$\boxed{R \text{ is rotation by } \theta, \quad \varphi : D_{2n} \hookrightarrow GL_2(\mathbb{R}) \text{ with } \varphi(r) = R,\ \varphi(s) = S \text{ is a faithful repres}}$$

□

Exercise 115 (D&F §1.6, Ex. 26). *Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by*

$$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \quad \textit{and} \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

extends to a homomorphism. Prove that φ is injective.

Intuition. We just check the quaternion relations in matrices: $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, and -1 central. Once the images satisfy the defining relations, the universal property of presentations gives a homomorphism. Injectivity follows because the subgroup these matrices generate has exactly 8 elements.

Proof. **Step 1. Check the defining relations in $GL_2(\mathbb{C})$.**
Set

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \Phi_i = \varphi(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \Phi_j = \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then

$$\Phi_i^2 = \begin{pmatrix} i^2 & 0 \\ 0 & (-i)^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I, \qquad \Phi_j^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

Hence we may set $\varphi(-1) = -I$, which commutes with all matrices.

Compute $\Phi_i\Phi_j$ and $\Phi_j\Phi_i$:

$$\Phi_i\Phi_j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \qquad \Phi_j\Phi_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} =$$

Define $\Phi_k := \Phi_i\Phi_j = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$. Then $\Phi_k^2 = \bigl(\Phi_i\Phi_j\bigr)^2 = \Phi_i(\Phi_j\Phi_i)\Phi_j = \Phi_i(-\Phi_i\Phi_j)\Phi_j = -(\Phi_i^2)(\Phi_j^2) = -(-I)(-I) = -I$. We have thus realized

$$\Phi_i^2 = \Phi_j^2 = \Phi_k^2 = -I, \qquad \Phi_i\Phi_j = \Phi_k, \qquad \Phi_j\Phi_i = -\Phi_k,$$

and $-I$ is central. These are exactly the quaternion relations.

Step 2. Extension to a homomorphism.
Since the images Φ_i, Φ_j satisfy the defining relations of Q_8, there exists a unique homomorphism

$$\varphi : Q_8 \longrightarrow GL_2(\mathbb{C})$$

with $\varphi(i) = \Phi_i$ and $\varphi(j) = \Phi_j$; in particular $\varphi(k) = \Phi_k$ and $\varphi(-1) = -I$.

Step 3. Injectivity.
Let $H \le GL_2(\mathbb{C})$ be the subgroup generated by $\{\Phi_i, \Phi_j\}$. From the relations above, the set

$$\{I, -I,\ \Phi_i, -\Phi_i,\ \Phi_j, -\Phi_j,\ \Phi_k, -\Phi_k\}$$

is closed under multiplication and has 8 distinct elements, so $|H| = 8$. The map $\varphi : Q_8 \to H$ is surjective by construction and $|Q_8| = |H| = 8$; hence φ is bijective onto H, in particular injective.

Conclusion.

$$\boxed{\begin{array}{c}\varphi : Q_8 \hookrightarrow GL_2(\mathbb{C}) \text{ is an injective homomorphism,} \\ \varphi(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.\end{array}}$$

□

1.7: Group Actions

Exercise 116 (D&F §1.7, Ex. 1)**.** *Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times$, $a \in F$ and ga is the usual product in F of the two field elements* (state clearly which axioms in the definition of a field are used)*.*

. . . .

Intuition. Each $g \in F^\times$ "scales" F by ordinary multiplication. The action axioms reduce to (1) associativity of multiplication in F, and (2) the multiplicative identity $1 \in F^\times$ acting trivially.

. . . .

Proof. **Step 1. Define the candidate action.** For $g \in F^\times$ and $a \in F$, set

$$g \cdot a := ga,$$

the usual field product.

Step 2. Verify the action axioms (and list used field axioms).

1. *Compatibility with composition* (uses associativity of multiplication in F): For all $g, h \in F^\times$ and $a \in F$,

$$g \cdot (h \cdot a) = g \cdot (ha) = (gh)a = (gh) \cdot a.$$

2. *Identity acts trivially* (uses existence of a multiplicative identity 1 in F): For all $a \in F$,

$$1 \cdot a = 1a = a.$$

These two properties show that $F^\times$ acts on F via $(g, a) \mapsto g \cdot a$. □

Conclusion.

$$\boxed{F^\times \times F \to F,\ (g, a) \mapsto g \cdot a = ga \text{ is a valid left group action.}}$$

Exercise 117 (D&F §1.7, Ex. 2)**.** *Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.*

. . . .

Intuition. Each $z \in \mathbb{Z}$ "translates" the integer line by z. The action axioms reduce to (1) associativity of addition in $\mathbb{Z}$, and (2) the additive identity 0 acting trivially.

. . . .

Proof. **Step 1. Define the action as a map.**

$$\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \qquad (z, a) \longmapsto z \cdot a := z + a.$$

Step 2. Verify the action axioms (and list used group axioms).

1. *Compatibility with the group law* (uses associativity of + in $\mathbb{Z}$): For all $z_1, z_2, a \in \mathbb{Z}$,

$$z_1 \cdot (z_2 \cdot a) = z_1 \cdot (z_2 + a) = (z_1 + z_2) + a = (z_1 + z_2) \cdot a.$$

2. *Identity acts trivially* (uses existence of additive identity 0): For all $a \in \mathbb{Z}$,

$$0 \cdot a = 0 + a = a.$$

Hence $(z, a) \mapsto z \cdot a$ defines a (left) group action of $(\mathbb{Z}, +)$ on $\mathbb{Z}$. □

Conclusion.

$$\boxed{\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ (z, a) \mapsto z \cdot a = z + a \text{ is a valid left group action (translation).}}$$

Exercise 118 (D&F §1.7, Ex. 3)**.** *Show that the additive group* $\mathbb{R}$ *acts on the* x, y*-plane* $\mathbb{R} \times \mathbb{R}$ *by*

$$r \cdot (x, y) = (x + ry,\ y).$$

. . . .

Intuition. Each real number r performs a horizontal *shear* with factor r: the y-coordinate is fixed, and the x-coordinate is translated by r times y. For an additive action we need: (1) associativity of $+$ in $\mathbb{R}$ to compose shears, and (2) 0 acts trivially.

. . . .

Proof. **Step 1. Define the action as a map.**

$$\mathbb{R} \times (\mathbb{R}^2) \longrightarrow \mathbb{R}^2, \qquad (r, (x, y)) \longmapsto r \cdot (x, y) := (x + ry,\ y).$$

Step 2. Verify the action axioms.

1. *Compatibility with the group law* (uses associativity of $+$ in $\mathbb{R}$): For all $r_1, r_2 \in \mathbb{R}$ and $(x, y) \in \mathbb{R}^2$,

   $$r_1 \cdot \big(r_2 \cdot (x, y)\big) = r_1 \cdot (x + r_2 y,\ y) = \big(x + r_2 y + r_1 y,\ y\big) = \big(x + (r_1 + r_2) y,\ y\big) = (r_1 + r_2) \cdot ($$

2. *Identity acts trivially* (uses existence of additive identity 0): For all $(x, y) \in \mathbb{R}^2$,

   $$0 \cdot (x, y) = (x + 0 \cdot y,\ y) = (x, y).$$

Thus $(r, (x, y)) \mapsto r \cdot (x, y)$ is a (left) group action of $(\mathbb{R}, +)$ on $\mathbb{R}^2$. □

Conclusion.

$$\boxed{\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2,\ (r, (x, y)) \mapsto (x + ry,\ y) \text{ is a valid left group action (horizontal shear}}$$

Exercise 119 (D&F §1.7, Ex. 4)**.** *Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G* (cf. Exercise 26 of Section 1)*:*

(a) the kernel of the action,

(b) $\{\, g \in G \mid g \cdot a = a \,\}$ — this subgroup is called the stabilizer of a in G.

. . . .

Intuition. The kernel contains elements acting as the identity on *every* point; the stabilizer fixes *one* chosen point. Closure and inverses follow directly from the action axioms.

. . . .

Proof. **Setup.** Write the action as a map

$$\alpha : \ G \times A \longrightarrow A, \qquad (g, x) \longmapsto g \cdot x.$$

Define the *kernel of the action* by

$$\operatorname{Ker}(\alpha) := \{\, g \in G : \ g \cdot x = x \text{ for all } x \in A \,\},$$

and the *stabilizer* of a by

$$G_a := \{\, g \in G : \ g \cdot a = a \,\}.$$

(a) $\operatorname{Ker}(\alpha)$ **is a subgroup.**

- *Nonempty:* $1 \cdot x = x$ for all $x \Rightarrow 1 \in \operatorname{Ker}(\alpha)$.
- *Closed under product:* If $g, h \in \operatorname{Ker}(\alpha)$ and $x \in A$, then

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

  so $gh \in \operatorname{Ker}(\alpha)$.

- *Closed under inverses:* If $g \in \mathrm{Ker}(\alpha)$, then for all x,

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

  hence $g^{-1} \in \mathrm{Ker}(\alpha)$.

Therefore $\mathrm{Ker}(\alpha) \leq G$.

(b) G_a is a subgroup.

- *Nonempty:* $1 \cdot a = a \Rightarrow 1 \in G_a$.
- *Closed under product:* If $g, h \in G_a$, then

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

  so $gh \in G_a$.
- *Closed under inverses:* If $g \in G_a$, then

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

  hence $g^{-1} \in G_a$.

Thus $G_a \leq G$. □

Conclusion.

$$\boxed{\mathrm{Ker}(\alpha) \leq G \text{ and } G_a \leq G.}$$

Exercise 120 (D&F §1.7, Ex. 5)**.** *Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$* (cf. Exercise 14 in Section 6)*.*

. . . .

Intuition. The kernel of the action consists of $g \in G$ that fix *every* $a \in A$. The permutation representation sends g to the permutation $a \mapsto g \cdot a$. Being the identity permutation is exactly the same as fixing every $a \in A$.

. . . .

Proof. **Step 1. Notation.** Let the action be

$$\alpha : \; G \times A \longrightarrow A, \qquad (g, a) \longmapsto g \cdot a.$$

Define the associated permutation representation

$$\varphi : \; G \longrightarrow S_A, \qquad \varphi(g)(a) := g \cdot a \quad (\forall a \in A).$$

By construction, $\varphi(g)$ is a bijection of A for each g.

Step 2. $\mathrm{Ker}(\alpha) \subseteq \mathrm{Ker}(\varphi)$. If $g \in \mathrm{Ker}(\alpha)$, then $g \cdot a = a$ for all $a \in A$, hence $\varphi(g)(a) = a$ for all a, i.e. $\varphi(g) = \mathrm{id}_A$. Thus $g \in \mathrm{Ker}(\varphi)$.

Step 3. $\mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\alpha)$. Conversely, if $\varphi(g) = \mathrm{id}_A$, then for all $a \in A$ we have $\varphi(g)(a) = a$, i.e. $g \cdot a = a$. Hence $g \in \mathrm{Ker}(\alpha)$.

Combining Steps 2 and 3 gives $\mathrm{Ker}(\alpha) = \mathrm{Ker}(\varphi)$. □

Conclusion.

$$\boxed{\mathrm{Ker}(\alpha) = \mathrm{Ker}(\varphi)} \quad \text{for the action } \alpha \text{ and its permutation representation } \varphi.$$

Exercise 121 (D&F §1.7, Ex. 6)**.** *Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.*

. . . .

Intuition. Faithful means different group elements induce different permutations of A. Equivalently, the only element that acts like the identity permutation on *all* of A should be the identity element itself.

. . . .

Proof. **Setup.** Let the action be

$$\alpha : \; G \times A \longrightarrow A, \qquad (g, a) \longmapsto g \cdot a.$$

Its kernel is

$$\operatorname{Ker}(\alpha) := \{\, g \in G : \; g \cdot a = a \text{ for all } a \in A \,\}.$$

Let $\varphi : G \to S_A$ be the associated permutation representation, $\varphi(g)(a) = g \cdot a$.

(⇒) Faithful $\implies$ $\operatorname{Ker}(\alpha) = \{1\}$.

If the action is faithful, then φ is injective.

If $g \in \operatorname{Ker}(\alpha)$, then $g \cdot a = a$ for all a, so $\varphi(g) = \mathrm{id}_A = \varphi(1)$.

Injectivity gives $g = 1$. Hence $\operatorname{Ker}(\alpha) = \{1\}$.

($\Leftarrow$) $\operatorname{Ker}(\alpha) = \{1\} \implies$ **faithful.** Assume $\operatorname{Ker}(\alpha) = \{1\}$.

Suppose $\varphi(g) = \varphi(h)$.

Then for all $a \in A$, $g \cdot a = h \cdot a$, so

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

hence $g^{-1}h \in \operatorname{Ker}(\alpha) = \{1\}$, so $g = h$.

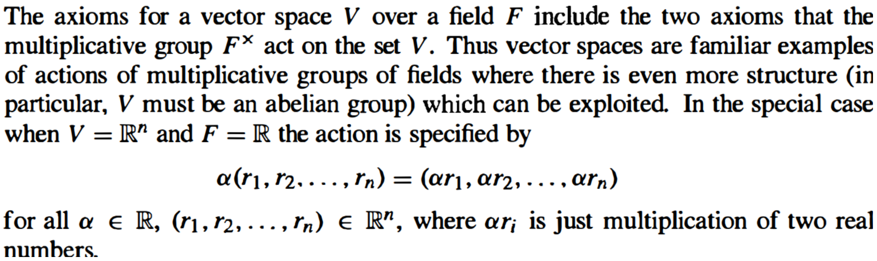
Therefore φ is injective and the action is faithful.

□

Conclusion.

$$\boxed{\text{The action is faithful} \iff \operatorname{Ker}(\alpha) = \{1\}.}$$

Exercise 122 (D&F §1.7, Ex. 7)**.** *Prove that in Example 2 in this section the action is faithful.*



The axioms for a vector space V over a field F include the two axioms that the multiplicative group $F^\times$ act on the set V. Thus vector spaces are familiar examples of actions of multiplicative groups of fields where there is even more structure (in particular, V must be an abelian group) which can be exploited. In the special case when $V = \mathbb{R}^n$ and $F = \mathbb{R}$ the action is specified by

$$\alpha(r_1, r_2, \ldots, r_n) = (\alpha r_1, \alpha r_2, \ldots, \alpha r_n)$$

for all $\alpha \in \mathbb{R}$, $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, where αr_i is just multiplication of two real numbers.

Intuition. In Example 2, a field's unit group $F^\times$ acts on a vector space V by scalar multiplication: distinct scalars produce distinct linear maps. If two scalars a, b satisfy $a \cdot v = b \cdot v$ for *all* $v \in V$, then $(a - b)v = 0$ for all v, forcing $a - b = 0$ (since $V \neq \{0\}$ and fields have no zero divisors).

Proof. **Setup.** Let V be a vector space over a field F and let

$$F^\times \times V \longrightarrow V, \qquad (a, v) \longmapsto a \cdot v := av$$

be the action from Example 2 (scalar multiplication).

Claim. The action is faithful, i.e. if $a, b \in F^\times$ satisfy $a \cdot v = b \cdot v$ for all $v \in V$, then $a = b$.

Proof of claim. Assume $a \cdot v = b \cdot v$ for all $v \in V$. Then for all $v \in V$,

$$0 = (a \cdot v) - (b \cdot v) = (a - b)v.$$

If $V = \{0\}$ the statement is vacuous; otherwise choose any $v_0 \in V$ with $v_0 \neq 0$. Then $(a - b)v_0 = 0$ forces $a - b = 0$ (since over a field, the only scalar annihilating a nonzero vector is 0). Hence $a = b$.

Therefore distinct elements of $F^\times$ induce distinct permutations of V; the action is faithful. $\square$

Conclusion.

$$\boxed{F^\times \curvearrowright V \text{ by } (a, v) \mapsto a \cdot v = av \text{ is faithful (Example 2).}}$$

Exercise 123 (D&F §1.7, Ex. 8). *Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by*

$$\sigma \cdot \{a_1, \dots, a_k\} = \{\sigma(a_1), \dots, \sigma(a_k)\}.$$

(a) Prove that this is a group action.

(b) Describe explicitly how the elements $(1\ 2)$ *and* $(1\ 2\ 3)$ *act on the six* 2*-element subsets of* $\{1, 2, 3, 4\}$.

. . . .

Intuition. Each permutation $\sigma \in S_A$ simply relabels elements of A; on a k-subset it sends each member through σ, and then we forget order because we are in the subset world. Associativity of composition in S_A gives the compatibility axiom, and the identity permutation fixes every subset.

. . . .

Proof. **(a) It is a group action.**
Action map.

$$S_A \times B \longrightarrow B, \qquad (\sigma, \{a_1, \dots, a_k\}) \longmapsto \sigma \cdot \{a_1, \dots, a_k\} := \{\sigma(a_1), \dots, \sigma(a_k)\}.$$

This is well-defined because σ is a bijection on A, so the image has exactly k distinct elements.

Compatibility (uses associativity of composition in S_A): For $\sigma_1, \sigma_2 \in S_A$ and $\{a_1, \dots, a_k\} \in B$,

$$\begin{aligned} \sigma_1 \cdot \bigl(\sigma_2 \cdot \{a_1, \dots, a_k\}\bigr) &= \sigma_1 \cdot \{\sigma_2(a_1), \dots, \sigma_2(a_k)\} \\ &= \{(\sigma_1 \circ \sigma_2)(a_1), \dots, (\sigma_1 \circ \sigma_2)(a_k)\} \\ &= (\sigma_1 \circ \sigma_2) \cdot \{a_1, \dots, a_k\}. \end{aligned}$$

Identity acts trivially:

$$\mathrm{id}_A \cdot \{a_1, \ldots, a_k\} = \{\mathrm{id}_A(a_1), \ldots, \mathrm{id}_A(a_k)\} = \{a_1, \ldots, a_k\}.$$

Therefore this is a (left) group action.

(b) Explicit action on 2-subsets of $\{1, 2, 3, 4\}$.
The six 2-element subsets are

$$\{1, 2\},\ \{1, 3\},\ \{1, 4\},\ \{2, 3\},\ \{2, 4\},\ \{3, 4\}.$$

Apply σ elementwise and then view the result as a set (order forgotten).

For the transposition (1 2):

$$\begin{aligned}
(1\ 2) \cdot \{1, 2\} &= \{2, 1\} = \{1, 2\},\\
(1\ 2) \cdot \{1, 3\} &= \{2, 3\},\\
(1\ 2) \cdot \{1, 4\} &= \{2, 4\},\\
(1\ 2) \cdot \{2, 3\} &= \{1, 3\},\\
(1\ 2) \cdot \{2, 4\} &= \{1, 4\},\\
(1\ 2) \cdot \{3, 4\} &= \{3, 4\}.
\end{aligned}$$

For the 3-cycle (1 2 3) (sending $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, and $4 \mapsto 4$):

$$\begin{aligned}
(1\ 2\ 3) \cdot \{1, 2\} &= \{2, 3\},\\
(1\ 2\ 3) \cdot \{1, 3\} &= \{2, 1\} = \{1, 2\},\\
(1\ 2\ 3) \cdot \{1, 4\} &= \{2, 4\},\\
(1\ 2\ 3) \cdot \{2, 3\} &= \{3, 1\} = \{1, 3\},\\
(1\ 2\ 3) \cdot \{2, 4\} &= \{3, 4\},\\
(1\ 2\ 3) \cdot \{3, 4\} &= \{1, 4\}.
\end{aligned}$$

This lists the action explicitly on all six 2-subsets. □

Conclusion.

The action $S_A \times B \to B$ given by $(\sigma, \{a_1, \ldots, a_k\}) \mapsto \{\sigma(a_1), \ldots, \sigma(a_k)\}$ is a valid group action.

Exercise 124 (D&F §1.7, Ex. 9). *Do both parts of the preceding exercise with "ordered k-tuples" in place of "k-element subsets," where the action on k-tuples is defined as above but with set braces replaced by parentheses* (note that, for example, the 2-tuples $(1, 2)$ and $(2, 1)$ are different even though the sets $\{1, 2\}$ and $\{2, 1\}$ are the same, so the sets being acted upon are different).

. . . .

Intuition. Replace subsets by ordered lists. A permutation $\sigma \in S_A$ sends a tuple by applying σ to each entry and keeping the order:

$$\sigma \cdot (a_1, \ldots, a_k) = (\sigma(a_1), \ldots, \sigma(a_k)).$$

Associativity of composition in S_A gives compatibility; id fixes every tuple.

. . . .

Proof. **(a) It is a group action.**
Action map.

$$S_A \times A^k \longrightarrow A^k, \qquad (\sigma,\, (a_1, \ldots, a_k)) \longmapsto (\sigma(a_1), \ldots, \sigma(a_k)).$$

Compatibility (uses associativity in S_A):

$$\begin{aligned} \sigma_1 \cdot \big(\sigma_2 \cdot (a_1, \ldots, a_k)\big) &= \sigma_1 \cdot \big(\sigma_2(a_1), \ldots, \sigma_2(a_k)\big) \\ &= \big((\sigma_1 \circ \sigma_2)(a_1), \ldots, (\sigma_1 \circ \sigma_2)(a_k)\big) \\ &= (\sigma_1 \circ \sigma_2) \cdot (a_1, \ldots, a_k). \end{aligned}$$

Identity acts trivially:

$$\mathrm{id}_A \cdot (a_1, \ldots, a_k) = (a_1, \ldots, a_k).$$

Hence this is a (left) group action.

(b) Explicit action for S_4 on ordered 2-tuples of $\{1, 2, 3, 4\}$. The 12 ordered pairs are

$$(1, 2), (2, 1), (1, 3), (3, 1), (1, 4), (4, 1), (2, 3), (3, 2), (2, 4), (4, 2), (3, 4), (4, 3).$$

For the transposition (1 2):

$$\begin{aligned}
(1, 2) &\mapsto (2, 1), \quad (2, 1) \mapsto (1, 2),\\
(1, 3) &\mapsto (2, 3), \quad (3, 1) \mapsto (3, 2),\\
(1, 4) &\mapsto (2, 4), \quad (4, 1) \mapsto (4, 2),\\
(2, 3) &\mapsto (1, 3), \quad (3, 2) \mapsto (3, 1),\\
(2, 4) &\mapsto (1, 4), \quad (4, 2) \mapsto (4, 1),\\
(3, 4) &\mapsto (3, 4), \quad (4, 3) \mapsto (4, 3).
\end{aligned}$$

For the 3-cycle (1 2 3):

$$\begin{aligned}
(1, 2) &\mapsto (2, 3), \quad (2, 1) \mapsto (3, 2),\\
(1, 3) &\mapsto (2, 1), \quad (3, 1) \mapsto (1, 2),\\
(1, 4) &\mapsto (2, 4), \quad (4, 1) \mapsto (4, 2),\\
(2, 3) &\mapsto (3, 1), \quad (3, 2) \mapsto (1, 3),\\
(2, 4) &\mapsto (3, 4), \quad (4, 2) \mapsto (4, 3),\\
(3, 4) &\mapsto (1, 4), \quad (4, 3) \mapsto (4, 1).
\end{aligned}$$

□

Conclusion.

The symmetric group S_A acts on A^k by $(\sigma, (a_1, \ldots, a_k)) \mapsto (\sigma(a_1), \ldots, \sigma(a_k))$. This is a valid group action, and the explicit images in part (b) are as computed above.

Exercise 125 (D&F §1.7, Ex. 10). *With reference to the preceding two exercises determine:*

(a) for which values of k the action of S_n on k-element subsets is faithful, and

(b) for which values of k the action of S_n on ordered k-tuples is faithful.

. . . .

Intuition. - *k-subsets:* if $1 \leq k < |A|$, we can choose a k-subset that exposes any difference between two distinct permutations. - *ordered k-tuples:* once $k \geq 1$, the first coordinate already detects a difference.

. . . .

Proof. **(a) Action on k-element subsets (with $1 \leq k < |A|$).**

Let $A = \{a_1, \ldots, a_n\}$ with $n = |A|$.

Take $\sigma_1 \neq \sigma_2 \in S_A$ and, WLOG, assume $\sigma_1(a_1) \neq \sigma_2(a_1)$.

Choose a k-subset $B \subseteq A$ such that

$$a_1 \in B \quad \text{and} \quad (\sigma_2^{-1}\sigma_1)(a_1) \notin B$$

(which is possible since $1 \leq k < |A|$).

Then $\sigma_1 \cdot B$ contains $\sigma_1(a_1)$, but $\sigma_2 \cdot B$ does not (for otherwise $(\sigma_2^{-1}\sigma_1)(a_1) \in B$).

Hence $\sigma_1 \cdot B \neq \sigma_2 \cdot B$ and the action is faithful for $1 \leq k < |A|$.

(b) Action on ordered k-tuples.

Let $\sigma_1 \neq \sigma_2 \in S_A$ and pick $a \in A$ with $\sigma_1(a) \neq \sigma_2(a)$.

For any $k \geq 1$, take $\mathbf{b} = (a, a_2, \dots, a_k) \in A^k$.

Then

$$\sigma_1 \cdot \mathbf{b} = (\sigma_1(a), \dots) \neq (\sigma_2(a), \dots) = \sigma_2 \cdot \mathbf{b},$$

so the action is faithful for all $1 \leq k \leq |A|$. □

Conclusion.

(a) The S_A-action on k-element subsets is faithful for all integers k with $1 \leq k < |A|$.
(b) The S_A-action on ordered k-tuples is faithful for all integers k with $1 \leq k \leq |A|$.

Exercise 126 (D&F §1.7, Ex. 11)**.** *Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square (where the vertices of the square are labelled as in Section 2).*

. . . .

Intuition. Let $D_8 = \langle r, s \mid r^4 = s^2 = 1,\ srs = r^{-1} \rangle$ act on the set of vertices $\{1, 2, 3, 4\}$. Rotations cyclically permute the vertices; reflections swap across an axis. Translating each symmetry into its induced permutation on $\{1, 2, 3, 4\}$ gives the desired cycle forms.

. . . .

Proof. **Step 1. Action and generators.** Label the square's vertices $\{1, 2, 3, 4\}$ in counterclockwise order. Let r be the 90° counterclockwise rotation and s a reflection (so $srs = r^{-1}$). The associated permutation representation $\varphi : D_8 \to S_4$ is given by $\varphi(g)(i) = g \cdot i$ for $g \in D_8$.

Step 2. Images of generators. By inspection on the labelled square:

$$\varphi(r) = (1\ 2\ 3\ 4), \qquad \varphi(s) = (2\ 4).$$

Then $\varphi(r^2) = (1\ 3)(2\ 4)$ and $\varphi(r^3) = (1\ 4\ 3\ 2)$. Using $srs = r^{-1}$ gives the reflection coset:

$$\varphi(sr) = (1\ 4)(2\ 3), \quad \varphi(sr^2) = (1\ 3), \quad \varphi(sr^3) = (1\ 2)(3\ 4).$$

Step 3. The eight cycle decompositions.

$$\begin{aligned} &\varphi(1) = 1, && \varphi(r) = (1\ 2\ 3\ 4), && \varphi(r^2) = (1\ 3)(2\ 4), && \varphi(r^3) = (1\ 4\ 3\ 2), \\ &\varphi(s) = (2\ 4), && \varphi(sr) = (1\ 4)(2\ 3), && \varphi(sr^2) = (1\ 3), && \varphi(sr^3) = (1\ 2)(3\ 4). \end{aligned}$$

These are precisely the eight permutations in S_4 arising from the D_8-action. □

Conclusion.

Under the vertex action $D_8 \curvearrowright \{1,2,3,4\}$ we obtain:

$$\begin{array}{llll} 1 \mapsto 1, & r \mapsto (1\ 2\ 3\ 4), & r^2 \mapsto (1\ 3)(2\ 4), & r^3 \mapsto (1\ 4\ 3\ 2), \\ s \mapsto (2\ 4), & sr \mapsto (1\ 4)(2\ 3), & sr^2 \mapsto (1\ 3), & sr^3 \mapsto (1\ 2)(3\ 4). \end{array}$$

Exercise 127 (D&F §1.7, Ex. 12)**.** *Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action (label vertices as usual).*

. . . .

Intuition. When n is even, a regular n-gon has $\frac{n}{2}$ lines through the center joining opposite vertices. Each symmetry either permutes these opposite pairs or (in the case of the 180° rotation) sends every vertex to its opposite, hence fixes every pair. The only elements that fix *all* pairs are the identity and the 180° rotation.

. . . .

Proof. **Step 1. The set and the action.** Label the vertices $1, 2, \dots, n$ counterclockwise. Since n is even, define for $k = 1, \dots, \frac{n}{2}$

$$P_k \;:=\; \Big\{\, k,\; k + \tfrac{n}{2} \,\Big\}$$

(indices taken modulo n). Let

$$\mathcal{P} \;:=\; \{P_1, \dots, P_{n/2}\}.$$

Define an action map

$$D_{2n} \times \mathcal{P} \longrightarrow \mathcal{P}, \qquad (x, P) \longmapsto x \cdot P := \{\, x \cdot v \mid v \in P \,\},$$

where $x \cdot v$ is the usual action of the symmetry x on the vertex v.

Well-defined. Every $x \in D_{2n}$ is a bijection of the vertex set, and it preserves the “opposite” relation: if v and $v + \frac{n}{2}$ are opposite, then $x(v)$ and $x(v + \frac{n}{2})$ are opposite. Hence $x \cdot P_k$ is again a pair of opposite vertices, i.e. an element of $\mathcal{P}$.

Step 2. Verify the action axioms. For $x, y \in D_{2n}$ and $P \in \mathcal{P}$,

$$x{\cdot}(y{\cdot}P) = \{\, x{\cdot}w \mid w \in y{\cdot}P \,\} = \{\, x{\cdot}(y{\cdot}v) \mid v \in P \,\} = \{\, (xy){\cdot}v \mid v \in P \,\} = (xy){\cdot}P,$$

using composition of symmetries; and $1 \cdot P = P$ for all P. Thus this is a (left) group action.

Step 3. Determine the kernel. We claim

$$\ker = \{\, x \in D_{2n} \mid x \cdot P = P \text{ for all } P \in \mathcal{P} \,\} = \{1,\ r^{\,n/2}\},$$

where r denotes the n-cycle (counterclockwise) rotation.

(i) $1, r^{n/2} \in \ker$. Trivially 1 fixes every P_k. The half-turn $r^{n/2}$ maps each vertex v to its opposite $v + \frac{n}{2}$, so it fixes each unordered pair $\{v, v + \frac{n}{2}\}$ and hence each P_k.

(ii) No other element lies in $\ker$. Let $x \in D_{2n}$. If $x = r^m$ is a nontrivial rotation with $m \not\equiv 0, \frac{n}{2} \pmod{n}$, then $r^m(k) = k + m$ is not equal to k or $k + \frac{n}{2}$ for some k, so $r^m \cdot P_k \neq P_k$; hence $x \notin \ker$. If x is a reflection, then it fixes some vertices and moves others to non-opposites; in particular, there exists k with $x \cdot P_k \neq P_k$ (e.g. in a square, a reflection swaps the two opposite pairs). Thus no reflection lies in ker.

Therefore $\ker = \{1, r^{n/2}\}$. □

Conclusion.

For even n, D_{2n} acts on the $\frac{n}{2}$ pairs of opposite vertices of a regular n-gon by transporting pairs. The kernel of this action is precisely $\{1,\ r^{\,n/2}\}$ (identity and the 180° rotation).

Exercise 128 (D&F §1.7, Ex. 13). *Find the kernel of the left regular action.*

. . . .

Intuition. The left regular action is $G \times G \to G$, $(g, a) \mapsto g \cdot a := ga$. An element g is in the kernel iff it fixes *every* $a \in G$, i.e. $ga = a$ for all a. By cancellation (or uniqueness of identity), this forces $g = 1$.

. . . .

Proof. **Step 1. Action and kernel.** Let

$$G \times G \longrightarrow G, \qquad (g, a) \longmapsto g \cdot a := ga$$

be the left regular action. Its kernel is

$\mathrm{Ker} = \{\, g \in G : \ g{\cdot}a = a \text{ for all } a \in G \,\} = \{\, g \in G : \ ga = a \text{ for all } a \in G \,\}.$

Step 2. Identify the kernel. If $g \in \mathrm{Ker}$, then in particular $ga = a$ with $a = 1$ gives $g \cdot 1 = 1$, i.e. $g = 1$. Conversely, $g = 1$ clearly fixes every a. Thus $\mathrm{Ker} = \{1\}$.
Conclusion. The left regular action is faithful. □

Conclusion.

$$\boxed{\text{Kernel of the left regular action} = \{1\} \text{ (hence the action is faithful).}}$$

Exercise 129 (D&F §1.7, Ex. 14)**.** *Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by*

$$g \cdot a \ := \ ag \qquad (g, a \in G)$$

do not *satisfy the axioms of a (left) group action of G on itself.*

. . . .

Intuition. A left action must satisfy $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$. With the rule $g \cdot a := ag$ (i.e. *right* multiplication by g), the left-hand side becomes $a g_2 g_1$, while the right-hand side is $a(g_1 g_2)$. These agree for all a precisely when g_1 and g_2 commute. If G is non-abelian, we can pick g_1, g_2 with $g_1 g_2 \neq g_2 g_1$ and the axiom fails.

. . . .

Proof. **Claim.** If G is non-abelian, the map $(g, a) \mapsto g \cdot a := ag$ does not define a left action.

Verification of the compatibility axiom fails. Choose $g_1, g_2 \in G$ with $g_1 g_2 \neq g_2 g_1$. For arbitrary $a \in G$,

$$\begin{aligned} g_1 \cdot \big(g_2 \cdot a\big) &= g_1 \cdot (a g_2) = (a g_2) g_1 = a(g_2 g_1), \\ (g_1 g_2) \cdot a &= a(g_1 g_2). \end{aligned}$$

Thus the action axiom $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ would force $a(g_2 g_1) = a(g_1 g_2)$ for all a, and by cancellation $g_2 g_1 = g_1 g_2$, a contradiction. Hence the compatibility axiom fails, so this is not a left action when G is non-abelian.

Remark. If G *is* abelian, then $a(g_2 g_1) = a(g_1 g_2)$ holds, so the rule does define a left action. □

Conclusion.

$$\boxed{\text{For non-abelian } G, \quad (g, a) \mapsto ag \text{ does } \textit{not} \text{ satisfy the left action axioms.}}$$

Exercise 130 (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. **Claim.** The map $(g, a) \mapsto g \cdot a := a\, g^{-1}$ defines a left action of G on G.

Identity axiom. For any $a \in G$,

$$1 \cdot a \ = \ a\, 1^{-1} \ = \ a\, 1 \ = \ a.$$

Compatibility axiom. For any $g_1, g_2, a \in G$,

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

Thus both axioms hold, so this is a left action. □

Remarks. (1) Conceptually, this is the right-regular action "twisted by inversion": $g \cdot a = a\, g^{-1}$ is the same as right-multiplication by g^{-1}. (2) Inversion turns product order around, which is why compatibility works for all groups (abelian or not).

Conclusion.

$$\boxed{\text{For any group } G,\ (g, a) \mapsto a\, g^{-1} \text{ is a valid left action of } G \text{ on } G.}$$

Recall cue (one-liner). *"Left acts by right-<u>inverse</u>: the inverse flips order, restoring the left-action law."*

Exercise 131 (D&F §1.7, Ex. 16)**.** *Let G be any group and let $A = G$. Show that the maps*

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

satisfy the axioms of a (left) group action of G on itself (this action is called conjugation*).*

. . . .

Intuition. Conjugation is "transporting a into g's coordinate frame" and back. The inverse on the right restores the order so that

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

Identity is immediate because $1a1^{-1} = a$.

. . . .

Proof. **Claim.** The map $(g, a) \mapsto g \cdot a := gag^{-1}$ defines a left action of G on G.

Identity axiom. For any $a \in G$,

$$1 \cdot a \;=\; 1\,a\,1^{-1} \;=\; a.$$

Compatibility axiom. For any $g_1, g_2, a \in G$,

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

Thus both axioms hold, so this is a left action. □

Remarks. (1) For fixed g, the map $a \mapsto gag^{-1}$ is an automorphism of G (an inner automorphism). (2) Stabilizer of a under conjugation is $C_G(a) = \{g \in G : ga = ag\}$ (the centralizer), and orbits are the conjugacy classes.

Conclusion.

$$\boxed{\text{For any group } G,\ (g,a) \mapsto gag^{-1} \text{ is a valid left action (conjugation).}}$$

Recall cue (one-liner). *"Sandwich it: g on the left, g^{-1} on the right — associativity does the rest."*

Exercise 132 (D&F §1.7, Ex. 17)**.** *Let G be a group and let G act on itself by conjugation, $x \mapsto gxg^{-1}$ for fixed $g \in G$.*

1. *Prove that conjugation by g is an automorphism of G.*
2. *Deduce that x and gxg^{-1} have the same order for all $x \in G$.*
3. *For any subset $A \subseteq G$, prove $|A| = |gAg^{-1}|$, where $gAg^{-1} = \{gag^{-1} \mid a \in A\}$.*

. . . .

Intuition. Conjugation by g is just "renaming the coordinates" of G: multiply by g on the left and undo it on the right. Because $gx_1x_2g^{-1} = (gx_1g^{-1})(gx_2g^{-1})$, it respects the group law; and because $x \mapsto g^{-1}xg$ is its inverse, it's a bijection. Automorphisms preserve orders and bijections preserve cardinalities, so the deductions follow immediately.

. . . .

Proof. Fix $g \in G$ and define $\varphi_g : G \to G$ by $\varphi_g(x) = gxg^{-1}$.
(1) φ_g is an automorphism. For $x_1, x_2 \in G$,

$$\varphi_g(x_1x_2) = g(x_1x_2)g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) = \varphi_g(x_1)\,\varphi_g(x_2),$$

so φ_g is a homomorphism. It is bijective with inverse $\varphi_{g^{-1}}$, since

$$\varphi_{g^{-1}}(\varphi_g(x)) = g^{-1}(gxg^{-1})g = x, \qquad \varphi_g(\varphi_{g^{-1}}(x)) = x.$$

Hence φ_g is an automorphism (an inner automorphism).
(2) Orders are preserved. Let $x \in G$ and $n \geq 1$. Then

$$\varphi_g(x)^n = (gxg^{-1})^n = gx^ng^{-1} = \varphi_g(x^n).$$

Thus $\varphi_g(x)$ has order n iff $x^n = 1$, i.e. $\operatorname{ord}(\varphi_g(x)) = \operatorname{ord}(x)$.
(3) Conjugation preserves subset sizes. The restriction $\varphi_g|_A \colon A \to gAg^{-1}$ is a bijection (inverse $\varphi_{g^{-1}}|_{gAg^{-1}}$), hence $|A| = |gAg^{-1}|$. □

Conclusion.

Conjugation $x \mapsto gxg^{-1}$ is an automorphism; it preserves element orders and subset cardinalities.

Recall cue (one-liner). *"Conjugation is just relabeling: gxg^{-1} — same structure, same orders, same sizes."*

Exercise 133 (D&F §1.7, Ex. 18)**.** *Let H be a group acting on a set A. Define a relation $\sim$ on A by*

$$a \sim b \iff \exists\, h \in H \text{ such that } a = h \cdot b.$$

Prove that $\sim$ is an equivalence relation. (For each $x \in A$, the equivalence class of x under $\sim$ is called the orbit *of x. The orbits under the action of H partition A.)*

. . . .

Intuition. "Being in the same orbit" means "reachable by the action of some group element." Identity gives reflexivity; inverses give symmetry; closure (product) gives transitivity. So the group axioms map exactly onto the equivalence axioms.

. . . .

Proof. We verify the three properties.

Reflexive. For any $a \in A$, $a = 1 \cdot a$, so $a \sim a$.

Symmetric. If $a \sim b$ then $a = h \cdot b$ for some $h \in H$. Since $h^{-1} \in H$, we have $b = h^{-1} \cdot a$, hence $b \sim a$.

Transitive. If $a \sim b$ and $b \sim c$ then $a = h_1 \cdot b$ and $b = h_2 \cdot c$ for some $h_1, h_2 \in H$. Then

$$a \;=\; h_1 \cdot (h_2 \cdot c) \;=\; (h_1 h_2) \cdot c,$$

so $a \sim c$.

Thus $\sim$ is an equivalence relation.

Partition by orbits. The equivalence classes of $\sim$ are exactly the orbits $H \cdot x = \{h \cdot x : h \in H\}$, so they are pairwise disjoint and their union is A. □

Conclusion.

$$\boxed{\text{“Same orbit” is an equivalence relation; the orbits partition A.}}$$

Recall cue (one-liner). *Identity* ⇒ *reflexive, inverses* ⇒ *symmetric, products* ⇒ *transitive.*

Exercise 134 (D&F §1.7, Ex. 19)**.** *Let H be a subgroup of the finite group G and let H act on G (so $A = G$) by left multiplication. For $x \in G$ let $\mathcal{O}$ be the orbit of x under this action.*

1. *Prove that the map $\varphi : H \to \mathcal{O}$ defined by $\varphi(h) = hx$ is a bijection (hence $|\mathcal{O}| = |H|$).*
2. *Deduce* Lagrange's Theorem*: if G is finite and $H \leq G$ then $|H|$ divides $|G|$.*

. . . .

Intuition. The orbit $\mathcal{O}$ is exactly the left coset $Hx = \{hx : h \in H\}$. The map $h \mapsto hx$ is just "evaluate the coset representative." Left cancellation in groups forces injectivity; the definition of the orbit gives surjectivity. All distinct orbits are disjoint (Exercise 18), so G is a disjoint union of orbits, each of size $|H|$—hence $|H| \mid |G|$.

. . . .

Proof. **(1) φ is a bijection.** Let $\varphi : H \to \mathcal{O}$ be $\varphi(h) = hx$. If $\varphi(h) = \varphi(k)$ then $hx = kx$, and left cancellation gives $h = k$; hence φ is injective. Conversely, by definition of the orbit $\mathcal{O}$, each $y \in \mathcal{O}$ has the form $y = hx$ for some $h \in H$, so φ is surjective. Therefore φ is a bijection and $|\mathcal{O}| = |H|$.

(2) Lagrange's Theorem. By Exercise 18 the orbits of H on G form a partition of G. From (1), every orbit has cardinality $|H|$. If there are m orbits, then

$$|G| \;=\; \sum_{i=1}^{m} |\mathcal{O}_i| \;=\; \sum_{i=1}^{m} |H| \;=\; m\,|H|.$$

Thus $|H|$ divides $|G|$. □

Remarks. (1) For any (possibly infinite) G, (1) shows $|\mathcal{O}| = |H|$ as cardinals; finiteness is only used to conclude divisibility.
(2) Identifying $\mathcal{O}$ with Hx makes the bijection $h \mapsto hx$ tautological.

Conclusion.

$$\boxed{\text{The orbit } H \cdot x \text{ has size } |H| \text{ and } |H| \mid |G| \text{ (Lagrange).}}$$

Recall cue (one-liner). *"Orbit = left coset; cancel on the left; sum orbit sizes ⇒ Lagrange."*

Exercise 135 (D&F §1.7, Ex. 20)**.** *Show that the group G of rigid motions of a tetrahedron is isomorphic to a subgroup of S_4.*

. . . .

Intuition. A rigid motion permutes the four vertices. Label them $\{1, 2, 3, 4\}$. Send each motion α to the permutation $\sigma_\alpha \in S_4$ describing how it relabels vertices. Different motions yield different permutations (the only motion fixing all four vertices is the identity), so this gives an injective homomorphism $G \hookrightarrow S_4$.

. . . .

Proof. Let the vertices of a (regular) tetrahedron be labeled $A = \{1, 2, 3, 4\}$. Each rigid motion α maps the solid to itself and induces a permutation σ_α of A by

$$\sigma_\alpha(i) = \text{the label of the vertex to which } \alpha \text{ sends vertex } i.$$

Define $\varphi : G \to S_4$ by $\varphi(\alpha) = \sigma_\alpha$.
Homomorphism. For $\alpha, \beta \in G$ and $i \in A$,

$$\begin{aligned} &\varphi(\alpha\beta)(i) \\ &\qquad = \sigma_{\alpha\beta}(i) \\ &\qquad = \text{vertex reached by } (\alpha\beta) \text{ from } i \\ &\qquad = \sigma_\alpha(\sigma_\beta(i)) \\ &\qquad = \big(\sigma_\alpha \circ \sigma_\beta\big)(i) \\ &\qquad = \big(\varphi(\alpha)\varphi(\beta)\big)(i), \end{aligned}$$

so $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.
Injective. If $\varphi(\alpha) = \mathrm{id}$, then α fixes each vertex. A Euclidean isometry fixing four noncoplanar points must be the identity; hence $\alpha = \mathrm{id}$. Therefore $\ker \varphi = \{1\}$ and φ is injective.

Thus φ is an injective homomorphism, so $G \cong \varphi(G) \leq S_4$. □

Remarks. (1) In fact, the full symmetry group of a regular tetrahedron has order 24 and is isomorphic to S_4; the rotation (orientation-preserving) subgroup has order 12 and is isomorphic to A_4.
(2) The key step is faithfulness: no nontrivial rigid motion can fix all four vertices.

Conclusion.

$$\boxed{\text{Rigid motions of a tetrahedron embed into } S_4 \text{ (indeed, are } S_4 \text{ itself).}}$$

Recall cue (one-liner). *"Move the solid, permute the four corners; fixing all four $\Rightarrow$ identity."*

Exercise 136 (D&F §1.7, Ex. 21)**.** *Show that the group G of rigid motions of a cube is isomorphic to S_4.*

. . . .

Intuition. A cube has four *pairs of opposite vertices* (equivalently, four *space diagonals*). Every rigid motion permutes these four objects. This gives a homomorphism

$$\varphi : G \longrightarrow S_4.$$

It is injective (no nontrivial motion fixes all four pairs), and $|G| = 24$ (from earlier counting of cube rotations), so φ must be an isomorphism onto all of S_4.

. . . .

Proof. Label the four pairs of opposite vertices by $A = \{1, 2, 3, 4\}$ (each i stands for one pair). Every rigid motion $\alpha \in G$ permutes these pairs, so define

$$\varphi : G \to S_4, \qquad \varphi(\alpha)(i) = \alpha \cdot i.$$

Homomorphism. For $\alpha, \beta \in G$ and any $i \in A$,

$$\varphi(\alpha\beta)(i) = (\alpha\beta) \cdot i = \alpha \cdot (\beta \cdot i) = (\varphi(\alpha) \circ \varphi(\beta))(i),$$

so $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

Injective. If $\varphi(\alpha) = \mathrm{id}$, then α fixes each pair of opposite vertices, hence fixes each space diagonal as a set. A nontrivial rigid motion of a cube cannot fix all four body diagonals simultaneously; the only Euclidean isometry doing so is the identity. Thus $\ker \varphi = \{1\}$ and φ is injective.

Cardinality and surjectivity. From the standard count of cube rotations, $|G| = 24$. Since φ is an injective homomorphism into S_4 (also of size 24), its image is a subgroup of S_4 of order 24, hence equals S_4. Therefore φ is an isomorphism $G \cong S_4$. □

Remarks. (1) One can equivalently act on the set of four *space diagonals*; the same argument applies.
(2) Orientation-preserving motions already account for all rigid motions of the cube's rotational symmetry group, which has order 24.

Conclusion.

$$\boxed{\text{The group of rigid motions of a cube is isomorphic to } S_4.}$$

Recall cue (one-liner). *"Permute the four body diagonals; size* 24 *in,* 24 *out* $\Rightarrow S_4$*.*

Exercise 137 (D&F §1.7, Ex. 22)**.** *Show that the group G of rigid motions of an octahedron is isomorphic to S_4. Deduce that the groups of rigid motions of a cube and an octahedron are isomorphic.*

. . . .

Intuition. An octahedron has *four* pairs of opposite faces. Every rigid motion permutes these four objects, giving a natural homomorphism to S_4. Injectivity follows because fixing all four pairs forces the identity. Counting shows $|G| = 24$, so the image must be all of S_4.

. . . .

Proof. Label the four pairs of opposite faces by $A = \{1, 2, 3, 4\}$. Each rigid motion $\alpha \in G$ sends each pair to a pair, so it induces a permutation $\sigma_\alpha \in S_4$. Define

$$\varphi : G \to S_4, \qquad \varphi(\alpha) = \sigma_\alpha.$$

Homomorphism. For $\alpha, \beta \in G$ and $i \in A$, $\varphi(\alpha\beta)(i) = \alpha \cdot (\beta \cdot i) = (\varphi(\alpha) \circ \varphi(\beta))(i)$, hence $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

Injective. If $\varphi(\alpha) = \text{id}$ then α fixes each pair of opposite faces, hence fixes their supporting lines through the center; the only such rigid motion is the identity. Thus $\ker \varphi = \{1\}$.

Cardinality and surjectivity. It is standard (or from earlier counting) that $|G| = 24$ (all rotational symmetries of the octahedron). Since φ is an injective homomorphism into S_4 (also of order 24), we have $\varphi(G) = S_4$, so $G \cong S_4$.

Deduction about the cube. By Exercise 21 the cube's rigid-motion group is also isomorphic to S_4, hence the two groups are isomorphic to each other. □

Remarks. (1) Acting on the four *pairs of opposite faces* mirrors the cube case (acting on four pairs of opposite vertices / space diagonals).

(2) Duality viewpoint: cube and octahedron are dual polyhedra, which explains the isomorphism of their rotation groups.

Conclusion.

$$\boxed{\text{Rigid motions of an octahedron } \cong S_4 \cong \text{ rigid motions of a cube.}}$$

Recall cue (one-liner). *"Four opposite-face pairs $\Rightarrow S_4$; dual to the cube, so same group."*

Exercise 138 (D&F §1.7, Ex. 23)**.** *Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.*

. . . .

Intuition. There are only 3 pairs of opposite faces, so the action factors through a subgroup of S_3 (size 6), but the cube's rotation group has size 24. An injective homomorphism $G \hookrightarrow S_3$ is impossible, so the action has a nontrivial kernel. The motions that survive in the kernel are precisely the 180° half–turns about the three axes through the centers of opposite faces (plus the identity): each flips two faces within a pair, so each pair is fixed as a set.

. . . .

Proof. Let G be the (rotational) rigid-motion group of the cube; $|G| = 24$. Let X be the set of the three pairs of opposite faces. The action of G on X gives a homomorphism

$$\varphi : G \longrightarrow \mathrm{Sym}(X) \cong S_3, \qquad |\,\mathrm{Sym}(X)| = 6.$$

Since $|G| > |S_3|$, φ cannot be injective; hence the action is not faithful.

To determine $\ker\varphi$, note that $\alpha \in \ker\varphi$ iff α fixes each *pair* of opposite faces setwise. A rotation about the line orthogonal to a chosen face and its opposite by 180° swaps those two faces and also swaps each of the other two pairs, hence fixes all three pairs as sets. There are exactly three such half–turns (one for each axis through opposite faces), and together with the identity they form a normal Klein four subgroup

$$\ker\varphi = \{1,\ \rho_x,\ \rho_y,\ \rho_z\} \ \cong\ V_4,$$

where ρ_* denotes the 180° rotation about the corresponding face-axis.

Conversely, no other nontrivial rotation fixes all three pairs setwise:

- 90° or 270° turns about a face-axis cycle the three pairs, so they are not in the kernel;

- rotations about body-diagonals or edge-axes permute the pairs nontrivially.

Hence the kernel is exactly $\{1, \rho_x, \rho_y, \rho_z\}$. □

Conclusion.

$$\boxed{\text{The action is not faithful; } \ker = \{1\} \cup \{\text{three } 180^\circ \text{ face-axis rotations}\} \ \cong\ V_4.}$$

Recall cue (one-liner). *"Three pairs $\Rightarrow S_3$ image; kernel $=$ the three face half–turns (plus 1)."*