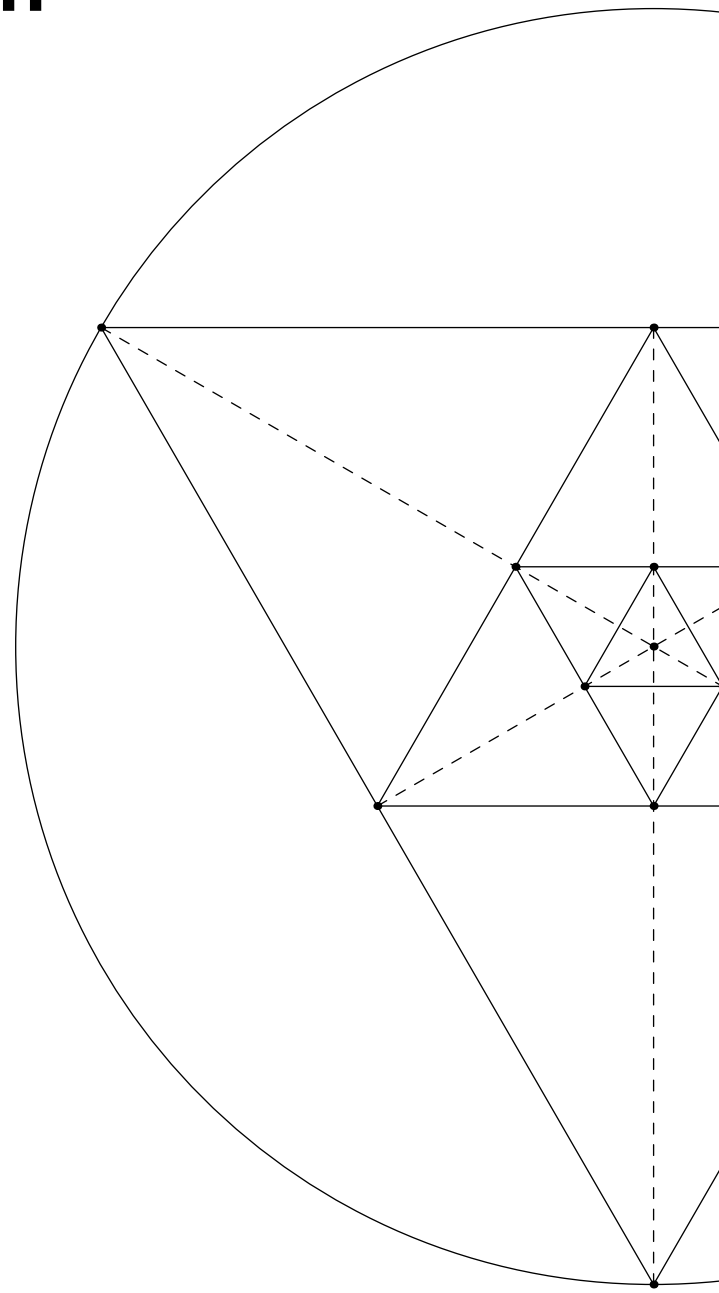
A Geometric Approach To Matrices

Answer Key

Timothy Herchen
Henry M. Gunn High School
Analysis Honors



Contents

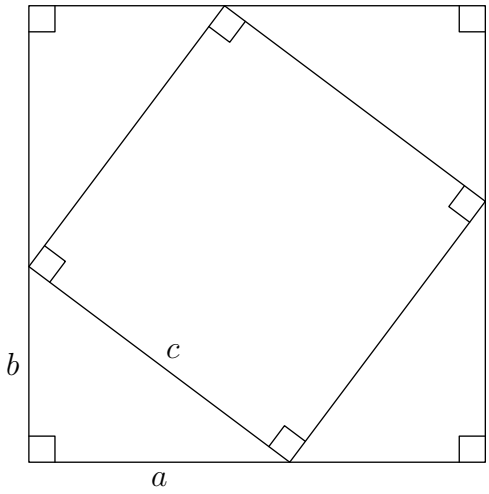


Figure 1: Scenario in Problem 1.

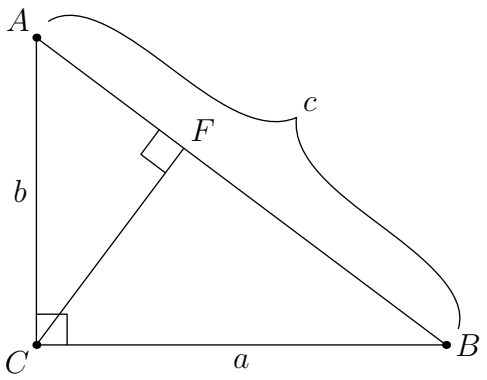


Figure 2: Scenario in Problem 2.

1 Trigonometry Review

1. Prove the Pythagorean theorem using "conservation of area." Start with Figure 1.

In Figure 1, the larger square has side length $a + b$. The smaller, nested square has side length c. Four copies of the right triangle with side lengths a, b, c are placed around the square. We have

$$\begin{aligned} A_{\text{triangles}} + A_{\text{small sq.}} &= A_{\text{big sq.}} && \text{[Conservation of area]} \\ 4A_{\text{triangle}} + A_{\text{small sq.}} &= A_{\text{big sq.}} \\ 4\left(\frac{1}{2}ab\right) + c^2 &= (a+b)^2 && \text{[Areas of triangle, square]} \\ 2ab + c^2 &= a^2 + 2ab + b^2 && \text{[Expanding]} \\ c^2 &= a^2 + b^2. && \text{Q.E.D.} \end{aligned}$$

2. Prove the Pythagorean theorem using a right triangle with an altitude drawn to its hypotenuse, making use of similar right triangles. This is shown in Figure 2.

Let $h = CF$, the length of the altitude to the hypotenuse. $\triangle ACF \sim \triangle ABC$ by AA Similarity because they share an angle and both have a right angle. Therefore, $\frac{AF}{AC} = \frac{AC}{AB}$. Substituting named variables for these lengths, we get

$$\frac{AF}{b} = \frac{b}{c} \implies AF = \frac{b^2}{c}.$$

Applying the same logic to $\triangle CFB$, we get $\triangle CFB \sim \triangle ABC$, so $\frac{BF}{BC} = \frac{BC}{AB}$. Substituting, we get

$$\frac{BF}{a} = \frac{a}{c} \implies BF = \frac{a^2}{c}.$$

Since F is between A and B, we have $AB = AF + FB$; substituting our found values for AF and FB, we get

$$\begin{aligned} c = AB &= AF + FB \\ c &= \frac{b^2}{c} + \frac{a^2}{c} \\ c^2 &= b^2 + a^2. && \text{Q.E.D.} \end{aligned}$$

3. Now you will prove the trig identities.

(a) Draw and label a right triangle and a unit circle, then write trig definitions for $\cos$, $\sin$, $\tan$, and $\sec$ in terms of your drawing.

The scenario is depicted in Figure 3. By the definition of sine and cosine, we have $\sin\theta = AP$ and $\cos\theta = OA$. Since $\triangle OAP \sim \triangle OPT$ by AA Similarity, we have $\frac{TP}{OP} = \frac{AP}{OA}$. Substituting known values, we get

$$\frac{TP}{1} = \frac{\sin\theta}{\cos\theta} \Longrightarrow TP = \tan\theta.$$

Also, $\triangle OAP \sim \triangle OKS$ by AA, so $\frac{OS}{OK} = \frac{1}{\cos\theta}$. Similarly, we have

$$\frac{OS}{1} = \frac{1}{\cos\theta} \Longrightarrow OS = \sec\theta.$$

Finally, as an alternate interpretation of $\tan$, we have $\frac{KS}{OK} = \frac{AP}{OA}$, so

$$\frac{KS}{1} = \frac{\sin\theta}{\cos\theta} \Longrightarrow KS = \tan\theta.$$

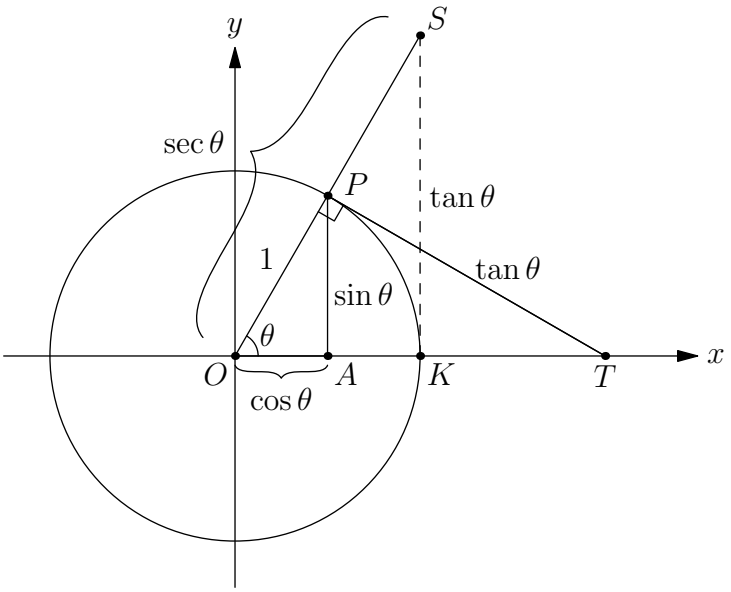


Figure 3: The right triangle and unit circle.

(b) Use a right triangle and the definitions of $\sin$ and $\cos$ to find and prove a value for $\sin^2\theta + \cos^2\theta$.

Referring back to Figure 3, focus on $\triangle OAP$. It is a right triangle with side lengths $a = \cos\theta$, $b = \sin\theta$, and $c = 1$. By the Pythagorean theorem, we have

$$\begin{aligned} OA^2 + AP^2 &= OP^2 && \text{[Pythagorean theorem]} \\ \cos^2\theta + \sin^2\theta &= 1^2 && \text{[Substitution]} \\ \sin^2\theta + \cos^2\theta &= 1 && \text{[Rearrange]} \end{aligned}$$

(c) Use the picture of the unit circle in Figure 4 to find and prove a value for $\cos(A - B)$. Note that D_1 and D_2 are the same length because they subtend the same size arc of the circle. Set them equal and work through the algebra, using the distance formula and part (b) of this problem.

We have $D_1 = D_2$, so

$$\begin{aligned} D_1^2 &= D_2^2 \\ (\cos A - \cos B)^2 + (\sin A - \sin B)^2 &= (\cos(A - B) - 1)^2 + \sin^2(A - B) \\ \cos^2 A - 2\cos A\cos B + \cos^2 B + \sin^2 A - 2\sin A\sin B + \sin^2 B &= \cos^2(A - B) - 2\cos(A - B) + \\ &\quad 1 + \sin^2(A - B) \end{aligned}$$

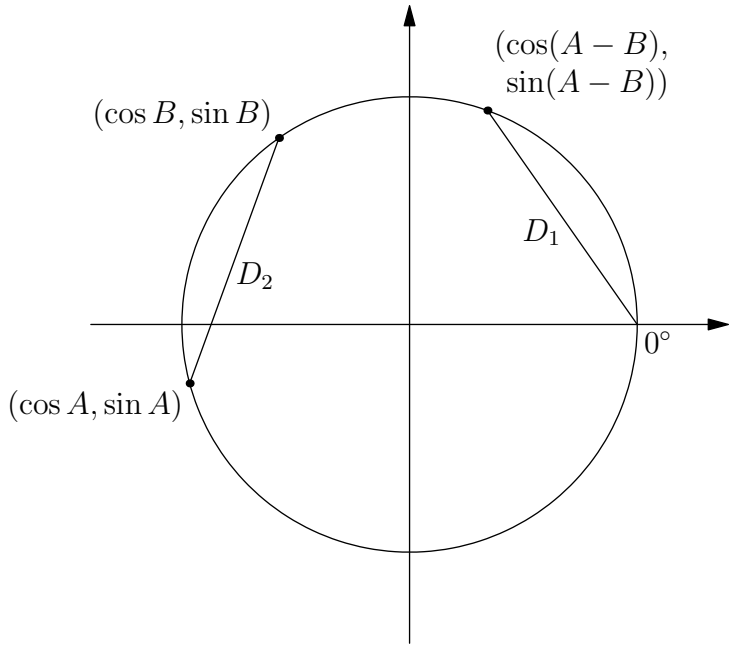


Figure 4: Scenario in Problem 3.

$$(\cos^2 A + \sin^2 A) + (\cos^2 B + \sin^2 A) - 2\sin A \sin B = (\cos^2(A-B) + \sin^2(A-B)) + 1 - 2\cos(A-B)$$

$$\cancelto{0}{1+1} - 2\sin A \sin B - 2\cos A \cos B = \cancelto{0}{1+1} - 2\cos(A-B)$$

$$2\sin A \sin B + 2\cos A \cos B = 2\cos(A-B)$$

$$\sin A \sin B + \cos A \cos B = \cos(A-B).$$ Q.E.D.

4. Write down as many trig identities as you can. There's no need to prove all of these right now.

$\sin(A+B) =$	$\sin(A-B) =$	$\cos(A+B) =$
$\tan(A+B) =$	$\tan(A-B) =$	$\sin(2A) =$
$\cos(2A) =$	$\tan(2A) =$	$\sin\left(\frac{A}{2}\right) =$
$\cos\left(\frac{A}{2}\right) =$	$\tan\left(\frac{A}{2}\right) =$	

You should probably memorize these for convenience.

$$\sin(A+B) = \sin A \cos B + \cos A \sin A$$
$$\sin(A-B) = \sin A \cos B - \cos A \sin B$$
$$\cos(A+B) = \cos A \cos B - \sin A \sin B$$
$$\tan(A+B) = \frac{\tan A + \tan B}{1 - \tan A \tan B}$$
$$\tan(A-B) = \frac{\tan A - \tan B}{1 + \tan A \tan B}$$
$$\sin(2A) = 2\sin A \cos A$$
$$\cos(2A) = 2\cos^2 A - 1 = 1 - 2\sin^2 A = \cos^2 A - \sin^2 A$$
$$\tan(2A) = \frac{2\tan A}{1 - \tan^2 A}$$
$$\sin\left(\frac{A}{2}\right) = \pm\sqrt{\frac{1-\cos A}{2}}$$
$$\cos\left(\frac{A}{2}\right) = \pm\sqrt{\frac{1+\cos A}{2}}$$

$$\tan\left(\frac{A}{2}\right) = \frac{\sin A}{1+\cos A} = \frac{1-\cos A}{\sin A}$$

5. Let's review complex numbers and DeMoivre's theorem.

(a) Recall that you can write a complex number both in Cartesian and polar forms. Let

$$a + bi = (a, b) = (r\cos\theta, r\sin\theta) = r\cos\theta + ir\sin\theta.$$

What is r in terms of a and b?

r is just the distance to the origin from $a + bi$. Draw a right triangle as shown in Figure 5. By the pythagorean theorem, $r = \sqrt{a^2 + b^2}$.

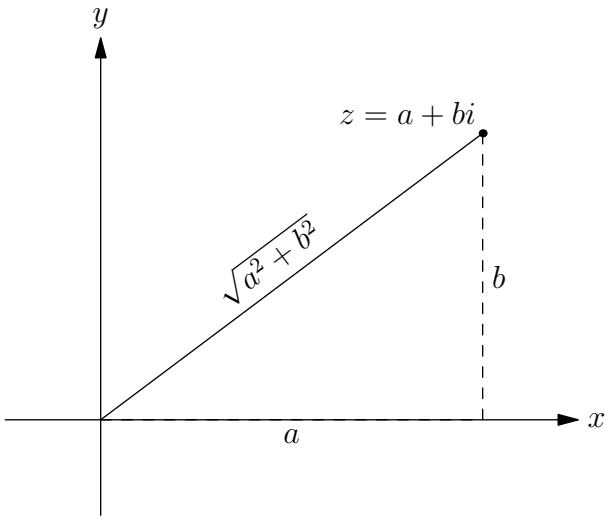


Figure 5: $a + bi$ in the complex plane.

(b) Multiply $(a + bi)(c + di)$ out using FOIL.

$$\begin{aligned}(a+bi)(c+di) &= ac + adi + bci + (bi)(di)\\ &= ac + (ad+bc)i - bd\\ &= ac - bd + (ad+bc)i.\end{aligned}$$

(c) Convert the two multiplicands[1] to polar form, noting that the two lengths and angles are different numbers. Call them $r_1(\cos\theta + i\sin\theta)$ and $r_2(\cos\phi + i\sin\phi)$.

We have $r_1 = \sqrt{a^2+b^2}$ and $\theta = \tan^{-1}\left(\frac{b}{a}\right)$ [2]; similarly, $r_2 = \sqrt{c^2+d^2}$ and $\phi = \tan^{-1}\left(\frac{d}{c}\right)$.

(d) Multiply them, and use your results from Problems 3c and 3d to show that multiplying two complex numbers involves multiplying their lengths and adding their angles. This is DeMoivre's theorem!

$$\begin{aligned}r_1(\cos\theta + i\sin\theta)r_2(\cos\phi + i\sin\phi) &= r_1r_2(\cos\theta\cos\phi - \sin\theta\sin\phi + i(\sin\theta\cos\phi + \cos\theta\sin\phi))\\ &= r_1r_2(\cos(\theta+\phi) + i\sin(\theta+\phi)).\end{aligned}$$

(e) Use part (d) to simplify $(\sqrt{3} + i)^{18}$.

[1] This is the word for parts of a multiplication! So for example, if $a \cdot b = c$, then a and b are the multiplicands.
[2] You can get this from drawing a right triangle.

We have $\sqrt{3} + i = r(\cos\theta + i\sin\theta) = 2\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)$.

$$\begin{aligned}
(2\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right))^{18} &= 2^{18} \cdot \left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)^{18} \\
&= 2^{18} \cdot \underbrace{\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)\cdots\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)}_{18 \text{ copies}} \\
&= 2^{18} \cdot \left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)\underbrace{\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)\cdots\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right)}_{16 \text{ copies}} \\
&= \vdots \\
&= 2^{18} \cdot (\cos 3\pi + i\sin 3\pi) \\
&= 2^{18} \cdot -1 \\
&= -2^{18}.
\end{aligned}$$

6. Here is a review of 2D rotation.

(a) Remember that we can graph complex numbers as 2D ordered pairs in the complex plane. Now, consider the complex number $z = \cos\theta + i\sin\theta$, where θ is fixed. What is the magnitude of z?

We have

$$|z| = \sqrt{\cos^2\theta + \sin^2\theta} = \sqrt{1} = 1.$$

(b) Multiplying $z \cdot (x + yi)$ yields a rotation of the point (x, y) counterclockwise by the angle θ around the origin. What if we wanted to rotate clockwise by θ instead?

We can multiply by the conjugate of z, since

$$\overline{z} = \cos\theta - i\sin\theta = \cos -\theta + i\sin -\theta.$$

Thus, the operation is $\overline{z} \cdot (x + yi)$ to rotate clockwise by θ.

7. Rotate the following conics by (i) $30°$, (ii) $45°$, and (iii) θ:

(a) $x^2 - y^2 = 1$

i. $30°$

We make the substitution $x' = x\cos 30° - y\sin 30° = \frac{\sqrt{3}}{2}x - \frac{y}{2}$ and $y' = x\sin 30° + y\cos 30° = \frac{x}{2} + \frac{\sqrt{3}}{2}y$:

$$\begin{aligned}
x'^2 - y'^2 &= 1 \\
\left(\frac{\sqrt{3}}{2}x - \frac{y}{2}\right)^2 - \left(\frac{x}{2} + \frac{\sqrt{3}}{2}y\right)^2 &= 1 \\
x^2/2 - \sqrt{3}xy - y^2/2 &= 1
\end{aligned}$$

ii. $45°$

We make the substitution $x' = x\cos 45° - y\sin 45° = \frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y$ and $y' = x\sin 45° + y\cos 45° = \frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y$:

$$\begin{aligned}
x'^2 - y'^2 &= 1 \\
\left(\frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y\right)^2 - \left(\frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y\right)^2 &= 1 \\
-2xy &= 1.
\end{aligned}$$

iii. θ

We make the substitution $x' = x\cos\theta - y\sin\theta$ and $y' = x\sin\theta + y\cos\theta$:

$$\begin{aligned} x'^2 - y'^2 &= 1 \\ (x\cos\theta - y\sin\theta)^2 - (x\sin\theta + y\cos\theta)^2 &= 1. \end{aligned}$$

(b) $\frac{x^2}{16} - \frac{y^2}{9} = 1$.

i. 30°

We make the substitution $x' = x\cos 30^\circ - y\sin 30^\circ = \frac{\sqrt{3}}{2}x - \frac{y}{2}$ and $y' = x\sin 30^\circ + y\cos 30^\circ = \frac{x}{2} + \frac{\sqrt{3}}{2}y$:

$$\begin{aligned} \frac{x'^2}{16} - \frac{y'^2}{9} &= 1 \\ \frac{\left(\frac{\sqrt{3}}{2}x - \frac{y}{2}\right)^2}{16} - \frac{\left(\frac{x}{2} + \frac{\sqrt{3}}{2}y\right)^2}{9} &= 1 \\ \frac{1}{576}(11x^2 - 50\sqrt{3}xy - 39y^2) &= 1. \end{aligned}$$

ii. 45°

We make the substitution $x' = x\cos 45^\circ - y\sin 45^\circ = \frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y$ and $y' = x\sin 45^\circ + y\cos 45^\circ = \frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y$:

$$\begin{aligned} \frac{x'^2}{16} - \frac{y'^2}{9} &= 1 \\ \frac{\left(\frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y\right)^2}{16} - \frac{\left(\frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y\right)^2}{9} &= 1 \\ \frac{1}{288}(-x - 7y)(7x + y) &= 1 \end{aligned}$$

iii. θ

We make the substitution $x' = x\cos\theta - y\sin\theta$ and $y' = x\sin\theta + y\cos\theta$:

$$\begin{aligned} \frac{x'^2}{16} - \frac{y'^2}{9} &= 1 \\ \frac{(x\cos\theta - y\sin\theta)^2}{16} - \frac{(x\sin\theta + y\cos\theta)^2}{9} &= 1. \end{aligned}$$

(c) $y^2 = 4Cx$

i. 30°

We make the substitution $x' = x\cos 30^\circ - y\sin 30^\circ = \frac{\sqrt{3}}{2}x - \frac{y}{2}$ and $y' = x\sin 30^\circ + y\cos 30^\circ = \frac{x}{2} + \frac{\sqrt{3}}{2}y$:

$$\begin{aligned} y'^2 &= 4Cx' \\ \left(\frac{x}{2} + \frac{\sqrt{3}}{2}y\right)^2 &= 4C\left(\frac{\sqrt{3}}{2}x - \frac{y}{2}\right). \end{aligned}$$

ii. 45°

We make the substitution $x' = x\cos 45^\circ - y\sin 45^\circ = \frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y$ and $y' = x\sin 45^\circ + y\cos 45^\circ = \frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y$:

$$y'^2 = 4Cx'$$
$$\left(\frac{\sqrt{2}}{2}x + \frac{\sqrt{2}}{2}y\right)^2 = 4C\left(\frac{\sqrt{2}}{2}x - \frac{\sqrt{2}}{2}y\right)$$
$$\frac{1}{2}(x+y)^2 = 2C\sqrt{2}(x-y)$$

iii. θ

We make the substitution $x' = x\cos\theta - y\sin\theta$ and $y' = x\sin\theta + y\cos\theta$:

$$y'^2 = 4Cx'$$
$$(x\cos\theta - y\sin\theta)^2 = 4C\left(x\sin\theta + y\cos\theta\right).$$

$\bullet$	I	A	B	C	D	E
I						
A			E			
B						
C						
D						
E						

Figure 1: Unfilled 3-post snap group table.

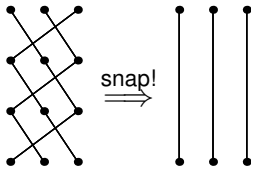


Figure 2: $E \bullet E \bullet E = I$; E has period 3.

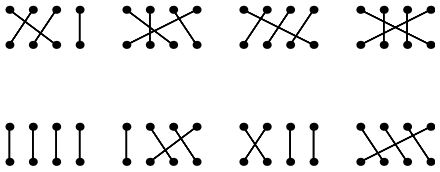


Figure 3: Some 4-post group elements.

2 It's a Snap

1. Fill out a 6×6 table like the one in Figure 1, showing the results of each of the 36 possible snaps, where $X \bullet Y$ is in X's row and Y's column. $A \bullet B = E$ is done for you.

$\bullet$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	E	D	C	B
B	B	D	I	E	A	C
C	C	E	D	I	B	A
D	D	B	C	A	E	I
E	E	C	A	B	I	D

2. Would this table look different if you wrote the elements A through E in a different order?

Yes; here's an example:

$\bullet$	I	E	A	D	B	C
I	I	E	A	D	B	C
E	E	D	C	I	A	B
A	A	B	I	C	E	D
D	D	I	B	E	C	A
B	B	C	D	A	I	E
C	C	A	E	B	D	I

3. Which of the elements is the **identity element** K, such that $X \bullet K = K \bullet X = X$ for all X?

The identity element is I, since $I \bullet A = A \bullet I = A$, $I \bullet B = B \bullet I = B$, and so forth.

4. Does every element have an inverse; can you get to the identity element from every element using only one snap?

Yes you can. The inverses are shown below.

$$I \leftrightarrow I$$
$$A \leftrightarrow A$$
$$B \leftrightarrow B$$
$$C \leftrightarrow C$$
$$D \leftrightarrow E$$

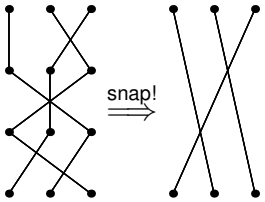


Figure 4: A 4×3 grid of posts has a unique result after the snap operation.

Note that the inverse of an element X is denoted X^{-1}.

5.

(a) Is the snap operation commutative (does $X \bullet Y = Y \bullet X$ for all X, Y)?

No, the snap operation is not commutative. For example, $A \bullet B = E$, but $B \bullet A = D$.

(b) Is the snap operation associative (does $(X \bullet Y) \bullet Z = X \bullet (Y \bullet Z)$ for all X, Y, Z)?'

Yes, the snap operation is associative. You can rationalize this as the fact that a 4×3 grid of posts is snapped to a single configuration, regardless of which middle row you remove first. This is shown in Figure 4.

6.

(a) For any elements X, Y, is there always an element Z so that $X \bullet Z = Y$?

Yes, there is always a way to get from one element to another in one snap. You can prove this by construction. If element X connects n_1 to n_1', n_2 to n_2', and n_3 to n_3', and element Y connects m_1 to m_1', m_2 to m_2', and m_3 to m_3', then the solution Z to $X \bullet Z = Y$ connects m_1 to $n_{m_1'}$, m_2 to $n_{m_2'}$, and m_3 to $n_{m_3'}$.

That's probably a bit hard to understand, but a more clever solution uses inverses. We multiply X by X^{-1}, then by Y:

$$X \bullet X^{-1} \bullet Y = Y.$$

But since every element has an inverse, and the snap operation is associative, we have

$$\begin{aligned} X \bullet (X^{-1} \bullet Y) &= Y \\ \implies Z &= X^{-1} \bullet Y. \end{aligned}$$

In this way, we have constructed the element Z.

(b) For (a), is Z always unique?

Yes. To show this, we use a proof by contradiction. Suppose we have two solutions Z_1 and Z_2 so that $Z_1 \neq Z_2$ and

$$\begin{aligned} X \bullet Z_1 &= Y \\ X \bullet Z_2 &= Y. \end{aligned}$$

We multiply to the left by Y^{-1}. Note that since the snap operation is not commutative, we need to multiply both sides on a specific side:

$$\begin{aligned} Y^{-1} \bullet X \bullet Z_1 &= Y^{-1} \bullet Y = I \\ Y^{-1} \bullet X \bullet Z_2 &= I \end{aligned}$$

So Z_1, Z_2 are the inverses of $Y^{-1} \bullet X$. But the inverse of an element is unique; we've showed this by listing them all out! Thus, $Z_1 = Z_2$, contradicting our assumption and proving that Z is unique in $X \bullet Z = Y$.

7. If you constructed a 5×5 table using only 5 of the snap elements, the table would not describe a group, because there would be entries in the table not in those 5. Therefore, a group must be **closed** under its operation; if $X, Y \in G$ ($\in$ means "is/are in"), then $X \bullet Y \in G$ for all X, Y. Some subsets, however, do happen to be closed.

   Write valid group tables using exactly 1, 2, and 3 elements from the snap group. These are known as **subgroups**.

Here are tables with 1, 2, and 3 elements:

$\bullet$	I
I	I

$\bullet$	I	A
I	I	A
A	A	I

$\bullet$	I	D	E
I	I	D	E
D	D	E	I
E	E	I	D

8. What do you guess is the complete definition of a mathematical group? (Hint: consider your answers to Problems 3–7.)

(Answers may vary.)

Definition of **group**: A group G is a set of elements together with a **binary operation** that meets the following criteria:

(a) Identity: There is an element $I \in G$ such that for all $X \in G$, $X \bullet I = I \bullet X = X$.

(b) Closure: If X, Y are elements of the group, then $X \bullet Y$ is also an element of the group.

(c) Invertibility: Each element X has an inverse X^{-1} such that $X \bullet X^{-1} = X^{-1} \bullet X = I$.

(d) Associativity: For all elements X, Y, and Z, $X \bullet (Y \bullet Z) = (X \bullet Y) \bullet Z$.

9. Notice that $E \bullet E \bullet E = I$. (See Figure 2.) This means that E has a **period** of 3 when acting upon itself. Which elements have a period of

(a) 1?

I is the only element with a period of 1, since $I = I$.

(b) 2?

A, B, and C have periods of 2, since for each $X \in A, B, C$ we have $X \bullet X = I$.

(c) 3?

D and E have periods of 3, since for each $Y \in D, E$ we have $Y \bullet Y \neq I$, but $Y \bullet Y \bullet Y = I$.

10. Answer the following with the 1, 2, and 4-post snap groups S_1, S_2 and S_4.

(a) How many elements would there be?

S_1 has $1! = 1$ elements. S_2 has $2! = 2$ elements. S_4 has $4! = 24$ elements.

(b) Systematically draw and name them.

Figure 5: Elements of S_1.

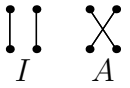


Figure 6: Elements of S_2.

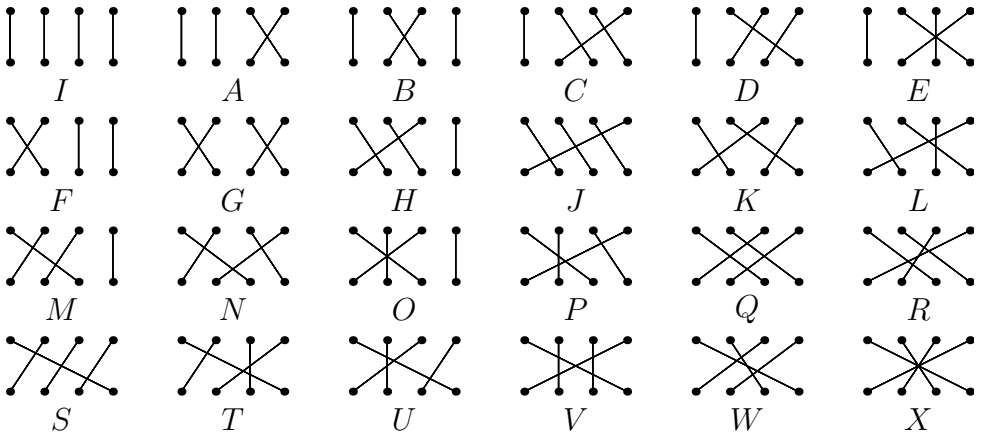


Figure 7: Elements of S_4.

(c) Make a group table of these elements. For 4 posts, instead of creating the massive table, give the number of entries that table would have.

Here are group tables for S_1 and S_2.

$\bullet$	I
I	I

Figure 8: Group table for S_1.

$\bullet$	I	A
I	I	A
A	A	I

Figure 9: Group table for S_2.

The table for S_4 is given at the end of the section in Figure 12 for the curious.

(d) What is the relationship between this new table and your original table?

Both S_1's and S_2's tables are subgroups of the original table for S_3. In turn, S_3 is a subgroup of S_4.

11. Can you think of an easier way to generate a snap group table without drawing all the possible configurations?

(Answers may vary.)

One way to do it is to treat each element as a list of indices. For example, I is the ordered triple $(1, 2, 3)$ because it takes column 1 to 1, 2 to 2, and 3 to 3. A is $(1, 3, 2)$, because it takes 1 to 1, 2 to 3, and 3 to 2.

This makes it a bit easier to calculate, because you can simply substitute indices for each configuration rather than make a drawing. It also makes it easy to write a program to calculate; this is actually how all the tables in this answer key were generated.

12.

(a) How many elements would there be in the 5-post snap group?

There would be $5! = 120$ elements in S_5.

(b) How many entries would its table have?

There would be $5!^2 = 14400$ entries in S_5's table.

(c) What possible periods would its elements have?

This is a more difficult question. We must ask what characteristics of an element determine its period.

If we observe the periodicity of an element with a pretty large period, say one from S_5 with a period of 6, you can see how a large period can arise. This is shown in Figure 11.

We can split up this element into two components: a component with period 3 and one with period 2. Let's call these components C_3 and C_2. After 2 steps, the C_3 has not completed one period, even though C_2. After 3 steps, C_3 has completed one period, but C_2 has gone through $\frac{3}{2}$. It takes $\mathrm{lcm}(2, 3) = 6$ steps before both components "line up!"

All elements can be split up into some number of these cyclic components, even if it doesn't look like it at first glance. For example, the element from S_8 shown in Figure 10 is actually two size 3 and size 2 components. It therefore has a period of $\mathrm{lcm}(2, 3, 3) = 6$. Note that it does *not* have a period of $2 \cdot 3 \cdot 3 = 18$!

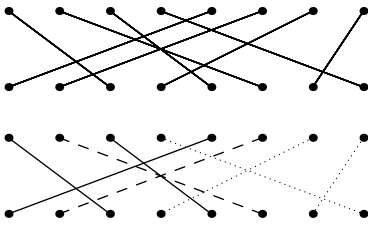


Figure 10: This element from S_8 has components of size $2, 3, 3$.

For S_5, we can split it up into components of size $1, 1, 1, 1, 1$, giving period 1; components of size $1, 1, 1, 2$, giving period 2; components of size $1, 1, 3$, giving period 3; components of size $1, 4$, giving period 4; a component of size 5, giving period 5; and component of size $1, 2, 3$, giving period 6. Thus, periods $1, 2, 3, 4, 5, 6$ are achievable.

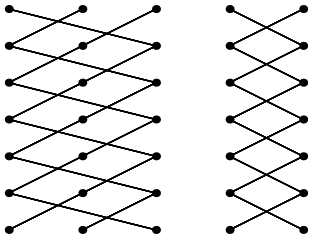


Figure 11: This element from S_5 has a period of 6.

(d) Extend your answers for a–c to M posts per row.

This is rather straightforward. There are (a) $M!$ elements in the M-post snap group, and thus (b) $M!^2$ elements in the corresponding group table. The possible periods are harder to calculate, but they can be generated like so:

Let integers $x_i > 0$ and $\sum_i x_i = M$. In other words, the sum of all x_i is M. Then $\operatorname{lcm}(x_1, x_2, \cdots, x_n)$ is a valid period; the least common multiple of all x_i is a possible period.

For fun: in set builder notation, we have the set of possible periods P_n for the n-post snap group as

$$P_n = \left\{ \operatorname{lcm}(x_1, x_2, \cdots, x_n) \;\middle|\; x_i \in \mathbb{Z}^+ \wedge \sum_i x_i = n \right\}.$$

The maximum such period (i.e. $\max P_n$) is actually known as Landau's function, $g(n)$.

13. As we learned, a **permutation** of some things is an order in which they can be arranged. What is the relationship between the set of permutations of m things and the m-post snap group?

We can make a pretty simple correspondence between a permutation of m things and an element of the m-post snap group. If we think back to the idea of treating each element of the group as a list of indices, the correspondence is obvious. For example, I is the ordered triple $(1, 2, 3)$ because it takes column 1 to 1, 2 to 2, and 3 to 3. A is $(1, 3, 2)$, because it takes 1 to 1, 2 to 3, and 3 to 2. But each ordered triple is a permutation of $1, 2, 3$! This extends to any m.

$\cdot$	I	A	B	C	D	E	F	G	H	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
I	I	A	B	C	D	E	F	G	H	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
A	A	I	D	E	B	C	G	F	K	L	H	J	S	T	U	V	W	X	M	N	O	P	Q	R
B	B	C	I	A	E	D	M	N	O	P	Q	R	F	G	H	J	K	L	T	S	W	X	U	V
C	C	B	E	D	I	A	N	M	Q	R	O	P	T	S	W	X	U	V	F	G	H	J	K	L
D	D	E	A	I	C	B	S	T	U	V	W	X	G	F	K	L	H	J	N	M	Q	R	O	P
E	E	D	C	B	A	I	T	S	W	X	U	V	N	M	Q	R	O	P	G	F	K	L	H	J
F	F	G	H	J	K	L	I	A	B	C	D	E	O	P	M	N	R	Q	U	V	S	T	X	W
G	G	F	K	L	H	J	A	I	D	E	B	C	U	V	S	T	X	W	O	P	M	N	R	Q
H	H	J	F	G	L	K	O	P	M	N	R	Q	I	A	B	C	D	E	V	U	X	W	S	T
J	J	H	L	K	F	G	P	O	R	Q	M	N	V	U	X	W	S	T	I	A	B	C	D	E
K	K	L	G	F	J	H	U	V	S	T	X	W	A	I	D	E	B	C	P	O	R	Q	M	N
L	L	K	J	H	G	F	V	U	X	W	S	T	P	O	R	Q	M	N	A	I	D	E	B	C
M	M	N	O	P	Q	R	B	C	I	A	E	D	H	J	F	G	L	K	W	X	T	S	V	U
N	N	M	Q	R	O	P	C	B	E	D	I	A	W	X	T	S	V	U	H	J	F	G	L	K
O	O	P	M	N	R	Q	H	J	F	G	L	K	B	C	I	A	E	D	X	W	V	U	T	S
P	P	O	R	Q	M	N	J	H	L	K	F	G	X	W	V	U	T	S	B	C	I	A	E	D
Q	Q	R	N	M	P	O	W	X	T	S	V	U	C	B	E	D	I	A	J	H	L	K	F	G
R	R	Q	P	O	N	M	X	W	V	U	T	S	J	H	L	K	F	G	C	B	E	D	I	A
S	S	T	U	V	W	X	D	E	A	I	C	B	K	L	G	F	J	H	Q	R	N	M	P	O
T	T	S	W	X	U	V	E	D	C	B	A	I	Q	R	N	M	P	O	K	L	G	F	J	H
U	U	V	S	T	X	W	K	L	G	F	J	H	D	E	A	I	C	B	R	Q	P	O	N	M
V	V	U	X	W	S	T	L	K	J	H	G	F	R	Q	P	O	N	M	D	E	A	I	C	B
W	W	X	T	S	V	U	Q	R	N	M	P	O	E	D	C	B	A	I	L	K	J	H	G	F
X	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	H	G	F	E	D	C	B	A	I

Figure 12: Group table for S_4.

3 From Snaps to Flips

1. The six "operations" are considered **isometries**. Isometries are ways of mapping the triangle to itself, preserving shape and location. Are there any others for this triangle?

There are no other isometries for this triangle; our list of operations is complete. To see why, note that the vertices must exchange places. At most there is $3! = 6$ ways to do this, so we have already achieved the maximum possible number of isometries.

$\cdot$	I	A	B	C	D	E
I						
A					B	
B						
C						
D						
E						

Figure 1: Unfilled D_3 group table.

2. As with the snap group, we can make a group table for the flip group. Fill out a table like the one in Figure 1 in your notebook. Like the snap group table, the top row indicates what operation is done first and the left column indicates what's done second, so that XY is in the X^{th} row and Y^{th} column. $AD = B$ is done for you.

The completed table is shown in Figure 2.

3. What is the relationship between the tables for the snap group S_3 and the flip group D_3?

D_3's table is S_3's table flipped over the top left–bottom right diagonal, and vice versa. Contrast D_3 from Figure 2 to S_3 in Figure 3. If these were matrices, one would be the transpose of the other: we'll get to that later.

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	D	E	B	C
B	B	E	I	D	C	A
C	C	D	E	I	A	B
D	D	C	A	B	E	I
E	E	B	C	A	I	D

Figure 2: Completed D_3 group table.

$\bullet$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	E	D	C	B
B	B	D	I	E	A	C
C	C	E	D	I	B	A
D	D	B	C	A	E	I
E	E	C	A	B	I	D

Figure 3: Completed S_3 group table from the last chapter.

4. Check your understanding by defining isomorphic in your own words.

(Answers may vary.)
Isomorphic means that two groups have the same structure. Isomorphic means that there is a correspondence between the elements of two groups so that the correspondence preserves the order. In the language of abstract algebra, an isomorphism between groups A and B exists if there is a homomorphism from A to B and from B to A.

5.

(a) Make a table for only the rotations of D_3, a subgroup of D_3.

The table is shown below. Note that the identity element I is a rotation of 0.

$\cdot$	I	D	E
I	I	D	E
D	D	E	I
E	E	I	D

Interestingly, this subgroup is a commutative group, also known as an abelian group.

(b) Which subgroup of the snap group S_3 is isomorphic to the subgroup in (a)?

The same elements (nominally) make the same subgroup:

$\bullet$	I	D	E
I	I	D	E
D	D	E	I
E	E	I	D

6. What shape's dihedral group is isomorphic to

(a) the two post snap group S_2?

The dihedral group of a line segment is isomorphic to S_2. After all, you can only reflect it over its midpoint, which is the other element of S_2 besides the identity. We can also think of this as permuting the two endpoints or vertices of a line segment.

(b) the one post snap group S_1?

The dihedral group of a point is isomorphic to S_1, because the only element is the identity element. This is permuting the one vertex of a point.

(c) the four post snap group S_4?

For this question we need to think 3 dimensions. There are four vertices to permute, but we can't do that on a square since diagonal points will remain on diagonals, as shown in Figure 4.

Instead, we choose the regular tetrahedron, so that there are no "diagonals"; every permutation is achievable. Note that rotations and reflections are now in 3 dimensional space, which is a bit difficult to visualize. A sample rotation is depicted in Figure 5.

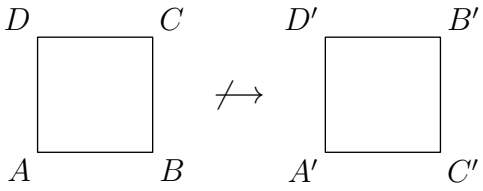


Figure 4: At right is a valid permutation of the vertices, but not a valid isometry of the square.

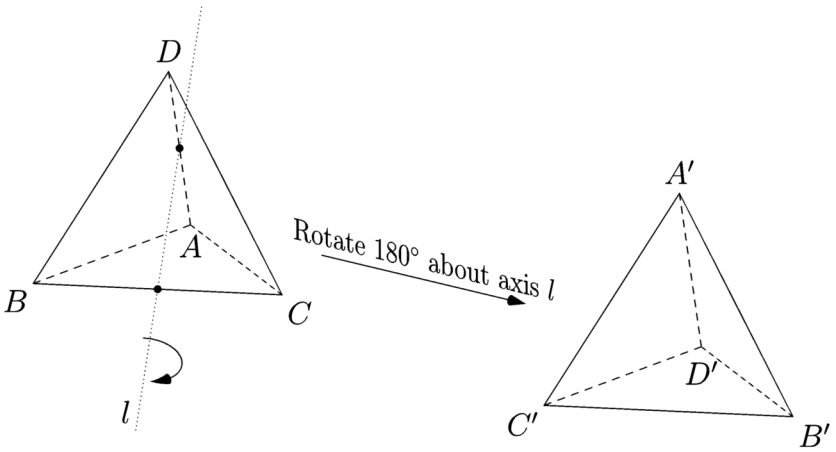


Figure 5: A rotation of the tetrahedron (orthographic view).

(d) the five post snap group S_5?

This is isomorphic to the dihedral group of the 4-dimensional equivalent of the tetrahedron, also known as the regular 4-simplex. A projection is shown in Figure 6, but it cannot be faithfully represented on this paper.

7. Find a combination of A and D that yields C.

8. We call A and D **generators** of the group because every element of the group is expressible as some combination of As and Ds. For convenience, let's call A "f" since it's a flip, and call D "r" meaning a $120°$ rotation counterclockwise. Then, for example, fr^2 is a rotation of $2 \cdot 120° = 240°$, followed by a flip across the A axis, equivalent to our original C. Make a new table using I, r, r^2, f, fr, and fr^2 as elements, like the one in Figure 7. *Note that the element order is different!*

$\cdot$	I	r	r^2	f	fr	fr^2
I						
r				fr^2		
r^2						
f						
fr						
fr^2						

Figure 7: Unfilled alternate D_3 table.

The filled table is shown in Figure 8 below.

$\cdot$	I	r	r^2	f	fr	fr^2
I	I	r	r^2	f	fr	fr^2
r	r	r^2	I	fr^2	f	fr
r^2	r^2	I	r	fr	fr^2	f
f	f	fr	fr^2	I	r	r^2
fr	fr	fr^2	f	r^2	I	r
fr^2	fr^2	f	fr	r	r^2	I

Figure 8: Completed alternate D_3 table.

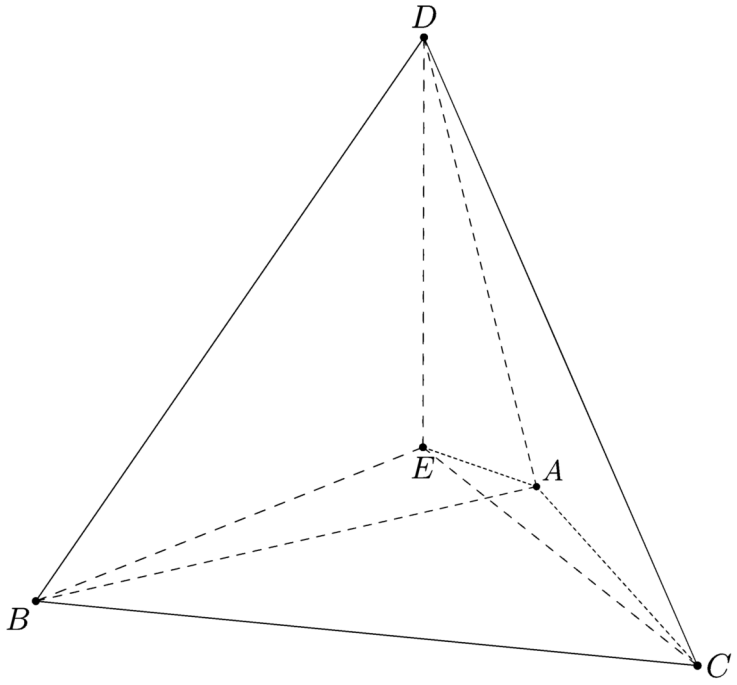


Figure 6: A 3D projection of the regular 4-simplex. In a true realization, every line segment here would be the same length.

Note that $I = I$, $A = f$, $B = fr$, $C = fr^2$, $D = r$, and $E = r^2$.

9. What other pairs of elements could you have used to generate the table?

You could also use any of the following pairs: $\{A, E\}$, $\{B, D\}$, $\{B, E\}$, $\{C, D\}$, $\{C, E\}$, $\{A, B\}$, $\{B, C\}$, $\{A, C\}$. In essence, you can generate it with any rotation element and any reflection element, or with any two reflection elements.

10. You should notice the 3×3 table of a group you've already described in the top-left corner of your table. What is it, and what are the two possible generators of this three-element group?

This is the cyclic group of order 3, C_3, also known as the rotation group of the equilateral triangle. The two possible generators are r and r^2.

11. Explain why each element of the flip group D_3 has the period it has.

I has a period of 1 because it is the identity. A, B, C have periods of 2 because they are reflections, so they are their own inverse transformation. D and E are rotations of a multiple of $1/3$ of a turn. Since 3 is a prime, they take 3 iterations to resolve, and thus have period 3.

12. Some pairs of elements of the flip group are two-element subgroups. Which pairs are they?

These would be the pairs I, A, I, B, and I, C, since $A \cdot A = B \cdot B = C \cdot C = I$ so the subgroup is closed. These are shown in Figure 9.

$\cdot$	I	A
I	I	A
A	A	I

$\cdot$	I	B
I	I	B
B	B	I

$\cdot$	I	C
I	I	C
C	C	I

Figure 9: The three two-element subgroups.

13. One of the elements forms a one-element subgroup. Which is it?

The element I forms the so-called trivial group, or the only group of order 1; this is shown in Figure 10. It is not very interesting.

$\cdot$	I
I	I

Figure 10: The trivial group.

14. Addition of two numbers is a binary operation, while addition of three numbers is not. In logic, $\wedge$ (and) and $\vee$ (or) are binary operations, but $\neg$ (not) is not. Define binary operation in your own words, and name some other binary operations.

(Answers may vary.)
A binary operation is an operation with two arguments.
Some binary operations:

1. multiplication
2. exponentiation
3. addition
4. subtraction
5. division
6. modulo operator
7. bitwise OR
8. bitwise AND
9. snap operation ($\bullet$)
10. function convolution

15. In your original flip group table, what is

(a) The identity element?

The identity element is I.

(b) The inverse of A?

The inverse of A is also A, since it is a reflection.

(c) The inverse of E?

The inverse of E is D, since $240^\circ + 120^\circ \equiv 0^\circ$.

4 Rotation and Reflection Groups

1. Notice that the original dihedral group had twice as many elements as the rotation group. Why?

(Answers may vary.)
There are a couple ways to think about this, but an intuitive way is to consider a "mirror world" of reflection and the "normal world" where the orientation in normal. Here, orientation is not absolute orientation, but the difference between clockwise and counterclockwise. For chemistry nerds, it is like chirality. Rotation preserves orientation, but reflection does not. Instead, it takes us between these two "worlds." Thus, it allows twice the number of elements.

2. Make and justify a conjecture extending this observation to the dihedral groups of other shapes like rectangles, squares, hexagons, cubes, etc.

(Answers may vary.)
Conjecture: The dihedral groups of a shape has twice the order of its rotation group.
Informal Justification: A shape can be flipped or not, and it can have whatever rotational isometries applied to it whether it's flipped or not. Thus, the dihedral group allows for twice the number of elements as the rotation group.

3. Let r be a 180° rotation, x be a reflection over the x-axis, and y be a reflection over the y-axis. Write a table for the dihedral group of the rectangle, recalling that the allowed isometries are reflections and rotations. How does this table differ from the dihedral group of the equilateral triangle?

$\cdot$	I	r	x	y
I	I	r	x	y
r	r	I	y	x
x	x	y	I	r
y	y	x	r	I

The table is shown above. The four elements are shown acting on a rectangle with "P" painted on it in Figure 1 to show the transformation a bit better.

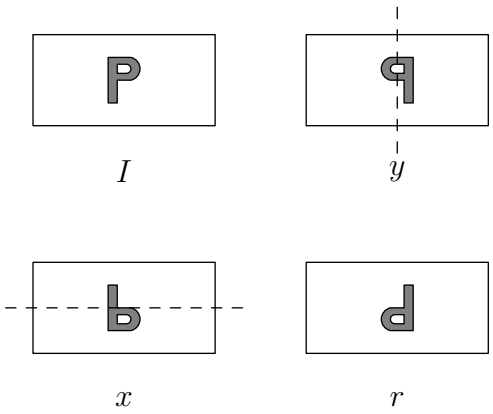


Figure 1: A rectangle AMBULATES and FLIPS around.

This differs from the dihedral group of the equilateral triangle, D_3, in several ways. The most obvious is that there are only 4 elements. Also, all elements besides I in this group have a period of 2, while D_3 has two elements with a period of 3.

4. Write a table for the rotation group of the square, with 4 elements and 16 entries. Compare this table to problem 3.

The elements are $I = r_0$, $r = r_{90}$, $r^2 = r_{180}$, and $r^3 = r_{270}$. The table is shown below.

$\cdot$	I	r	r^2	r^3
I	I	r	r^2	r^3
r	r	r^2	r^3	I
r^2	r^2	r^3	I	r
r^3	I	r	r^2	r^3

While this has the same order as the rectangle's dihedral group, it has a different structure. There are two elements with period 4 (r, r^3) and one element with period 2 (r^2).

For each of the following problems, find the following:

(a) Number of elements; this is known as the **order**

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

(c) A smallest possible **generating set**; in other words, the list of elements which generate a group[3]

(d) Whether the group is **commutative**; in other words, whether its operation $X \cdot Y$ doesn't care about the order of its operands (X and Y)

5. Rectangle under rotation

(a) Number of elements

This group has two elements, the identity and the rotation of $180°$.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

As stated, they are the identity I and the rotation r of $180°$, as shown in Figure 2.

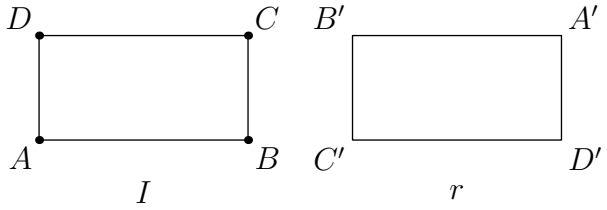


Figure 2: Rectangle under rotation.

(c) A smallest possible **generating set**

The smallest possible generating set is the singleton $\{r\}$.

(d) Whether the group is **commutative**

The group is commutative, since it's only comprised of rotations, which commute.

6. Rectangle under reflection

We already considered this in problem 3.

(a) Number of elements

There are 4 elements in this group.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

The elements are the identity I, rotation r by $180°$, reflection x over the x-axis, and reflection y over the y-axis.

(c) A smallest possible **generating set**

(Answers may vary.)
$\{r, x\}$, $\{r, y\}$, and $\{x, y\}$ all generate the group. No single element, however, can generate the group.

(d) Whether the group is **commutative**

This group is commutative.

7. Square under rotation

[3] There may be multiple generating sets of the same size.

Again, we have considered this group before.

(a) Number of elements

There are 4 elements.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

The elements are rotations $I = r_0$, $r = r_{90}$, $r^2 = r_{180}$, and $r^3 = r_{270}$.

(c) A smallest possible **generating set**

(Answers may vary.)
Both $\{r\}$ and $\{r^3\}$ generate the group, because $1, 3$ are coprime to 4.

(d) Whether the group is **commutative**

The group is commutative, since it consists of all rotations.

8. Square under reflection

(a) Number of elements

There are 8 elements in this group. We can quickly see this by noting that it is the dihedral group of the square, which has twice the order of the rotation group of the square. We just found that had 4 elements, and $2 \cdot 4 = 8$.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

The elements are as follows:
Rotations $I = r_0$, $r = r_{90}$, $r^2 = r_{180}$, and $r^3 = r_{270}$; reflections $f =$ flip over the x-axis, $fr = r$ then f, fr^2 and fr^3.
Recall that rotations can be generated by a sequence of two reflections.
Each of these elements is shown in Figure 3.

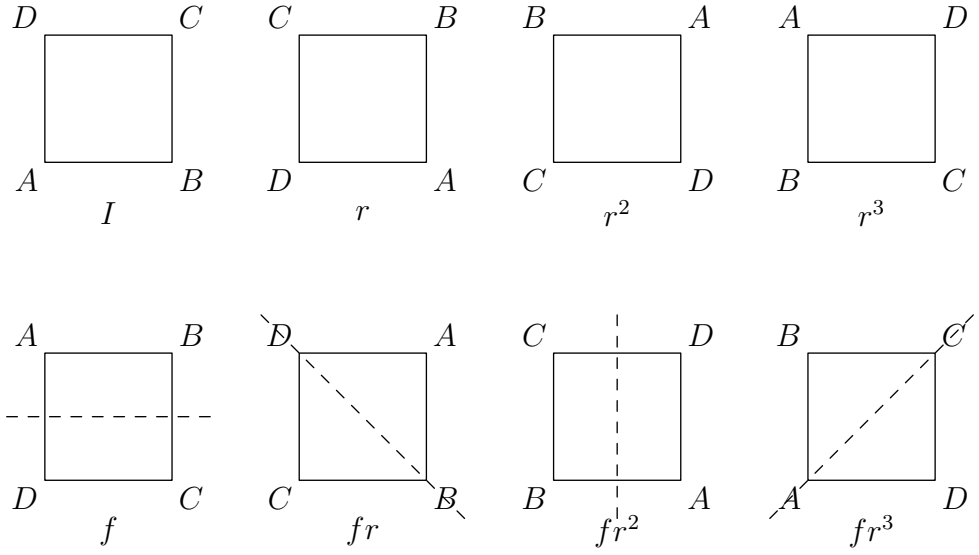


Figure 3: Reflections of a square.

(c) A smallest possible **generating set**

(Answers may vary.)
Any pair of a rotation and flip will generate the set, except for $\{r^2, fr^2\}$ and $\{r^2, f\}$; these will produce the rectangle group instead. Any pair of two flips, except for $\{f, fr^2\}$, will also work. As an example of both of these categories, both $\{r^2, fr^3\}$ and $\{f, fr\}$ will generate the group.

(d) Whether the group is **commutative**

This group is not commutative. For example, $fr = fr$, but $rf = fr^3$.

9. Square prism under rotation

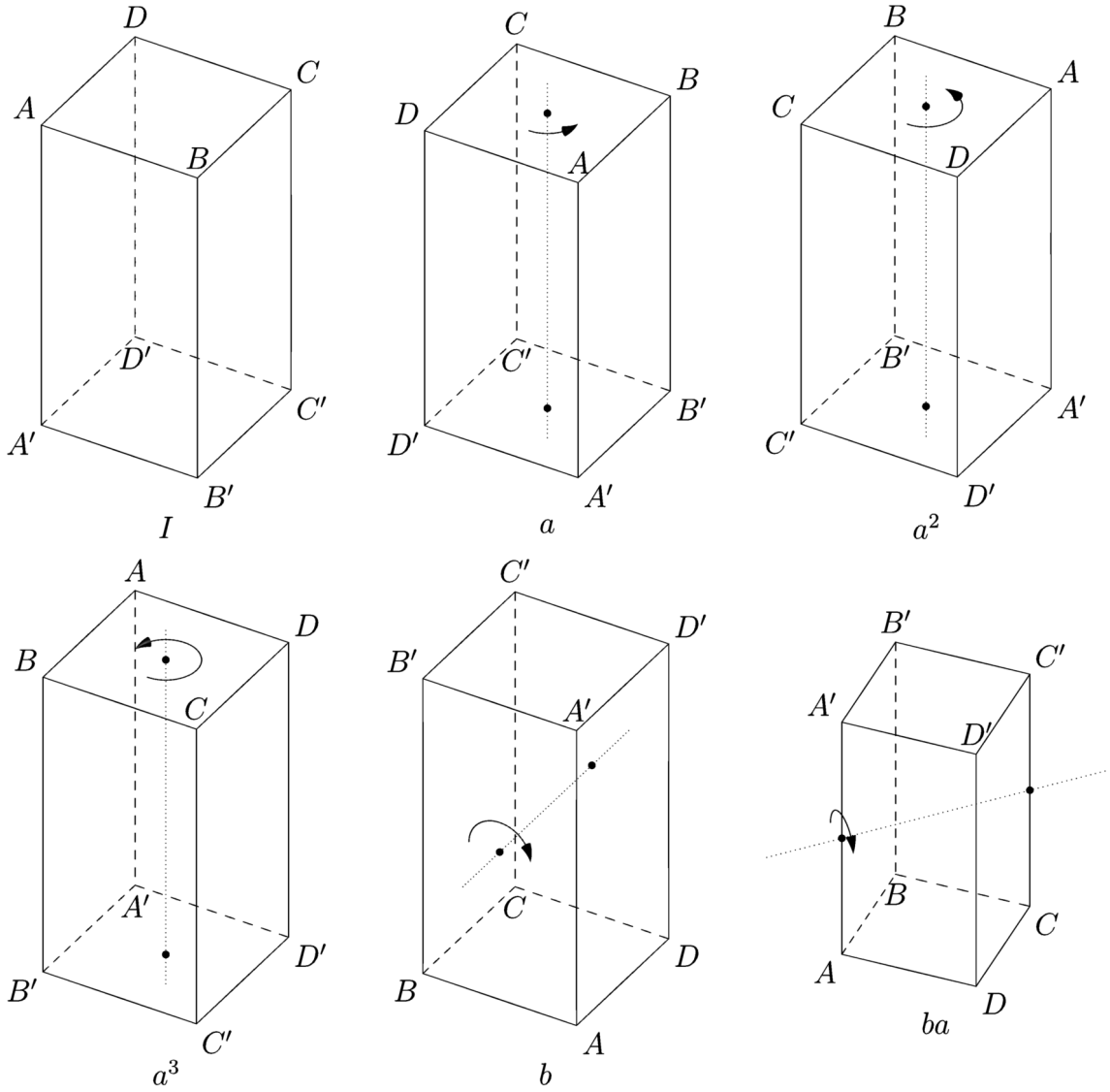
This group is isomorphic to the dihedral group of the square in Problem 8.

(a) Number of elements

This is a bit more difficult than the previous questions, because we need to understand what elements are possible. We can rotate the prism about its central axis, which an action analogous to just rotating a square: 4 elements. But we can also rotate the prism $180°$ on a axis through the middle (pictures are shown in the next subpart). This switches the top square face with the bottom face, giving another 4 elements. In total, we have 8 elements.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

The set of elements are shown in Figure 4 below. Let a be a rotation of $90°$ counterclockwise—as viewed from the top—around the central axis, going through the centers of both square faces; let b be a rotation of $180°$ around an axis going through the centers of faces $\square ABB'A'$ and $\square DCC'D'$.



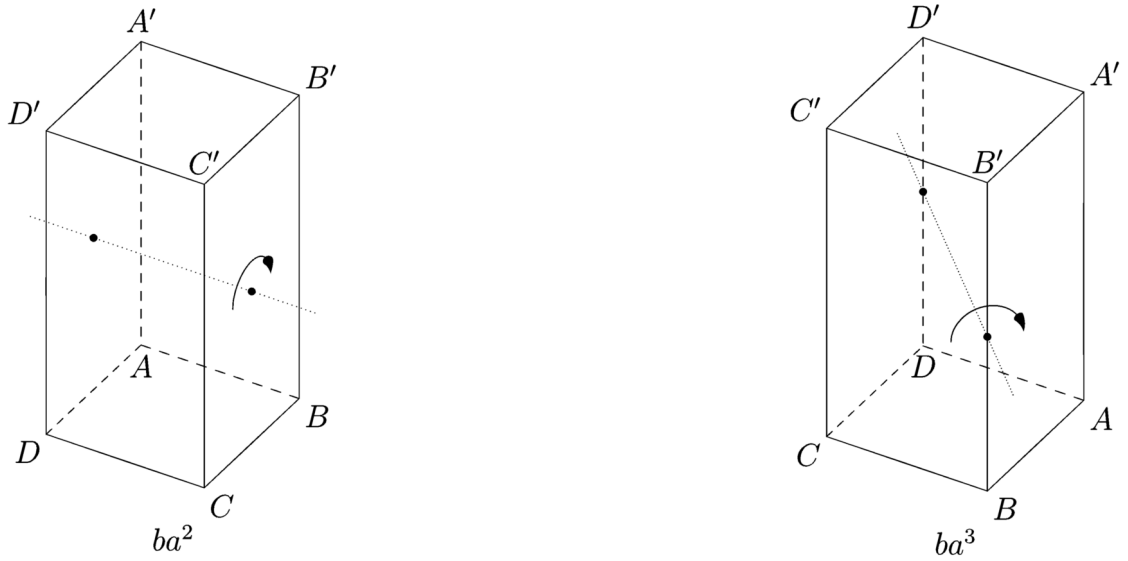


Figure 4: The elements of the rotation group of the rectangular prism.

(c) A smallest possible **generating set**

(Answers may vary.) The elements with b in their name are equivalent to the reflections in the dihedral group of the square. Thus, we need a "reflection" ba^n and a rotation a^m, or two separate reflections. All such pairs work except for $\{a^2, ba^2\}$, $\{a^2, b\}$ and $\{b, ba^2\}$. An example from each category: $\{a, b\}$, $\{b, ba\}$.

(d) Whether the group is **commutative**

This group is not commutative. For example, $ba = ba$, but $ab = ba^3$.

10. Square prism under reflection

(a) Number of elements

If the previous group—the rotation group of the square prism—had 8 elements, then this group should have 16 elements.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

We know the order because the previous group has 8 elements, and dihedral groups have twice the number of elements of the rotation group, this group has 16 elements.

(c) A smallest possible **generating set**

(Answers may vary significantly.)
Since we could generate the previous group with (most) pairs of $\{ba^n, a^m\}$, or (most) pairs of $\{a^n, a^m\}$, we could just add another element c which is a true geometric reflection about, say, the midplane P between $\square DCD'C'$ and $\square ABB'A$ as shown in Figure 5.

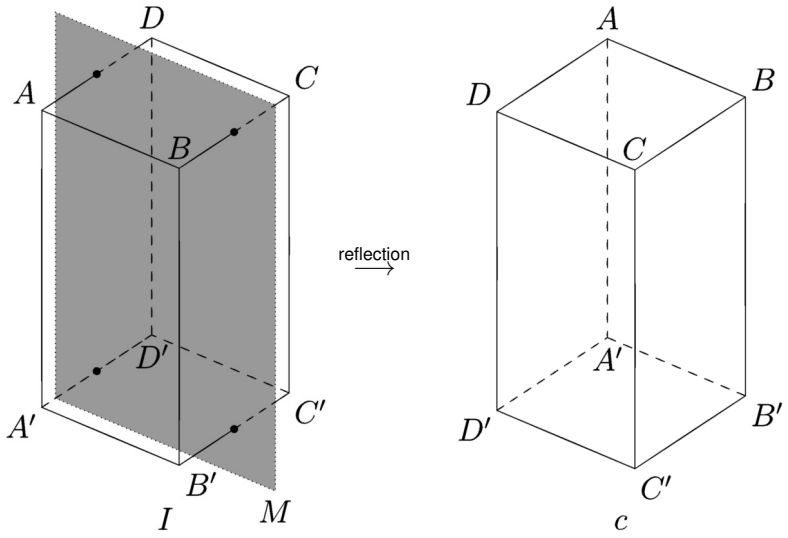


Figure 5: 3D reflection over the midplane M is c.

Thus, $\{a, b, c\}$ can generate the group. You can prove that two generators are impossible, but the proof either requires making the group table or some more sophisticated abstract algebra. I will give the latter for those who are well-versed in group theory already, but it will probably be inaccessible to most.

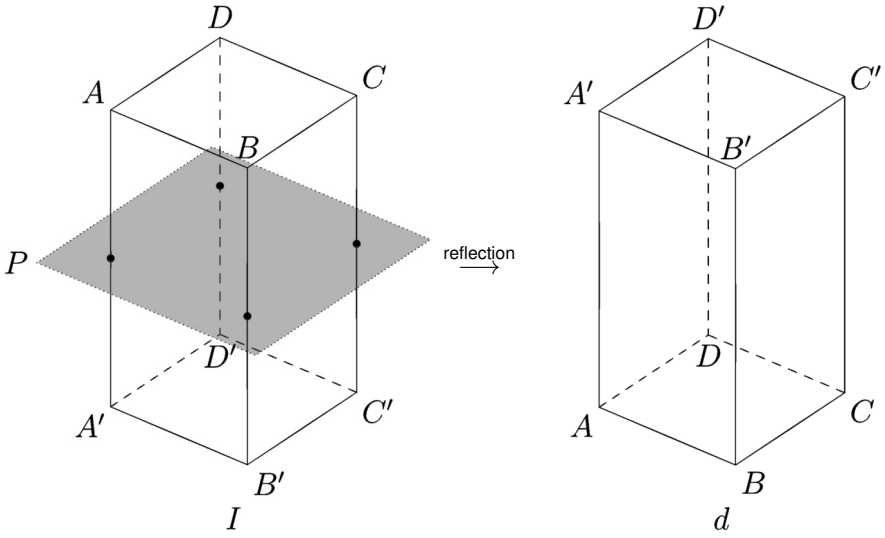


Figure 6: d is the reflection through midplane P.

The rotation group generated by $\{a, b\}$ is D_4. Define a new element d which is the reflection through the midplane P between the two square faces.[4] This is crudely shown in Figure 6; I couldn't be bothered to make a nicer figure. Then the reflection group generated by $\{d\}$ is Z_2. Furthermore, the operation sets $\{a, b\}$ and $\{d\}$ are separable, in that $a^x b^y d = d a^x b^y$ [5]. Thus, the group G described in this problem is (isomorphic to) the direct product:

$$G \cong D_4 \times Z_2.$$

We wish to show that $Z_2 \times Z_2 \times Z_2$ is a quotient of this group. That is, we wish to find a normal subgroup N such that

[4] For the curious, $d = cba^2$.

[5] This can be shown concretely by simply showing geometrically that $ad = da$ and $bd = db$.

$$G/N = Z_2 \times Z_2 \times Z_2.$$

If this is true, then the minimal generating set of G has at least cardinality 3. All that remains is to find N and G/N.

It suffices to show that $Z_2 \times Z_2 \triangleleft D_4$, since then $Z_2 \times Z_2 \times Z_2 \triangleleft D_4 \times Z_2$. We have $|Z_2 \times Z_2| = 2^2 = 4$, so we want $|D_4/N| = 4$. We know $|D_4| = 8$, so by Lagrange's theorem, $|N| = 2$.

A normal subgroup of D_4 is $N = \{1, a^2\}$. It is normal because for $x \in \{0, 1, 2, 3\}$ and $y \in \{0, 1\}$:

$$\begin{aligned}(b^x a^y)a^2(b^x a^y)^{-1} &= (b^x a^y)a^2(a^{-y}b^{-x}) \\ &= b^x a^{2+y-y} b^{-x} \\ &= b^x a^2 b^{-x} \\ &= b^x b^{-x} a^2 \\ &= a^2 \in \{1, a^2\}.\end{aligned}$$

The corresponding quotient group is

$$D_4/N = \{\{1, a^2\}, \{a, a^3\}, \{b, ba^2\}, \{ba, ba^3\}\}.$$

We have the isomorphism $\{b^x a^y, b^x a^{y+2}\} \leftrightarrow (x, y)$ under the operation of element-wise addition modulo 2. After all,

$$\{b^{x_1} a^{y_1}, b^{x_1} a^{y_1+2}\} \cdot \{b^{x_2} a^{y_2}, b^{x_1} a^{y_2+2}\} = \{b^{x_1+x_2} a^{y_1+y_2}, b^{x_1+x_2} a^{y_1+y_2+2}\}.$$

Therefore,

$$D_4/N \cong Z_2 \times Z_2,$$

so

$$Z_2 \times Z_2 \times Z_2 \triangleleft D_4 \times Z_2 = G.$$

Since the minimal generating set of $Z_2 \times Z_2 \times Z_2$ is 3, G's generating set is at least 3. But we've already found the set $\{a, b, c\}$ which generates G![6] Thus, it is minimal.

(d) Whether the group is **commutative**

As we found in the previous problem, the rotation group of the square prism is not commutative, and since that's a subgroup of this group, this group certainly isn't commutative.

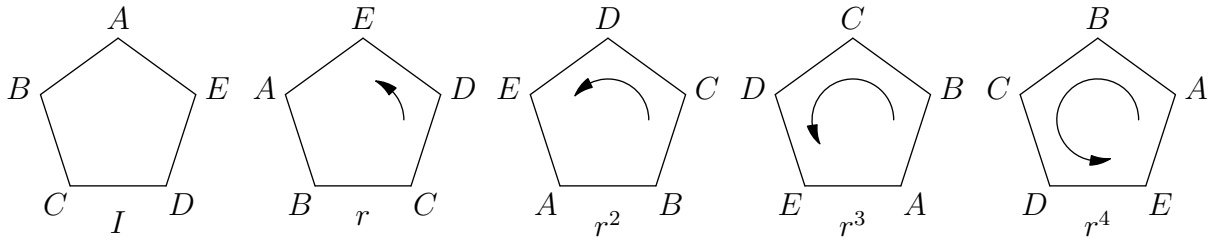
11. Pentagon under rotation

(a) Number of elements

This is just the cyclic group of order 5, so there are 5 elements.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

The elements are rotations of $I = r_0$, $r = r_{72}$, $r^2 = r_{144}$, $r^3 = r_{216}$, $r^4 = r_{288}$. They are shown below.



Pentagons should always wear helmets, lest they want to damage their vertices.

(c) A smallest possible **generating set**

[6] $\{a, b, d\}$ also generates G.

Any rotation by itself $\{r^n\}$ works, since 5 is a prime.

(d) Whether the group is **commutative**

The group is indeed commutative, since all operations are rotations.

12. Pentagon under reflection

(a) Number of elements

This is the dihedral group of the pentagon, which has $2 \cdots 5 = 10$ elements.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

We know the order because it should have twice the number of elements as the rotation group, which has 5 elements, giving 10 elements total.

(c) A smallest possible **generating set**

We can either do a rotation and a reflection or two reflections. Since 5 is prime, all pairs work (unlike for the square). Let f is a flip over the vertical axis. Examples of each are $\{r, f\}$ and $\{f, fr\}$.

(d) Whether the group is **commutative**

The group is not commutative. For example, $fr = fr$, but $rf = fr^4$.

13. Pentagonal prism under rotation

This is isomorphic to the dihedral group of the pentagon, which is Problem 12. The reason is the same as for Problem 9's dependence on 8, thus I will not explain it.

14. Pentagonal prism under reflection

This is akin to Problem 10.

(a) Number of elements

$2 \cdot 10 = 20$.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

We know the order because the rotation group of the pentagonal prism has 10 elements, so its dihedral group has 20 elements.

(c) A smallest possible **generating set**

If a is a rotation of 72° about the central axis, b is a rotation of 180° about a horizontal axis, and d is a reflection across the midplane between the two pentagonal faces, then $\{a, b, d\}$ generates the set, since $\{a, b\}$ generates all rotations and d turns them into their mirror images. But this isn't the right answer.

Are there any smaller generating sets? The previous trick asserting no using more advanced abstract algebra doesn't actually work[7]. We have $ad = da$ and $bd = db$ (you can verify this geometrically). So to have a two element subgroup we likely need something like $a^n d$ and ba^m for some integers n, m, so that we can potentially generate a, b and d.

Let's try ad and b. Taking successive powers of ad, we get

$$\begin{aligned}
ad &= ad \\
(ad)^2 &= a^2 \\
(ad)^3 &= a^3 d \\
(ad)^4 &= a^4 \\
(ad)^5 &= a^5 d = d \\
(ad)^6 &= a
\end{aligned}$$

[7] If you understand it, it's because $Z_2 \times Z_2 \times Z_2$ isn't a quotient of this group, since this group $D_5 \times Z_2$ has order 20 which is not divisible by 8.

We've just generated d and a from ad alone! Since we have b already, we have created $\{a, b, d\}$ from $\{ad, b\}$. Thus, the smallest generating set has size 2. (We can't have size 1 because then the group would be cyclic and thus commutative, which this group certainly isn't.)

This is a hard problem. Don't worry if you didn't get it.

(d) Whether the group is **commutative**

The dihedral group of the pentagon is a subgroup of this group, and is not commutative, so this group is not commutative.

15. Pentagonal pyramid under rotation

This is just isomorphic to the rotation group of the pentagon, or Problem 11.

16. Pentagonal pyramid under reflection

This is just isomorphic to the reflection group of the pentagon, or Problem 12.

17. Tetrahedron (triangular pyramid) under rotation

This is isomorphic to a subgroup of S_4, the snap group of order 24.

(a) Number of elements

The snap group includes reflections, but this does not: thus, this group has $\frac{4!}{2} = 12$ elements.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

We know the order because this is the rotation group of a tetrahedron, and the reflection group of a tetrahedron has 24 elements, so this must have half that.

(c) A smallest possible **generating set**

Another difficult problem!

Let's figure out where the rotation axes actually are. There are 4 axes going through a vertex—let's call these *vertex* axes v_i. There are also 3 axes going through the midpoints of opposite edges: let's call these *edge* axes e_i. These axes are enumerated and shown in Figure 7.

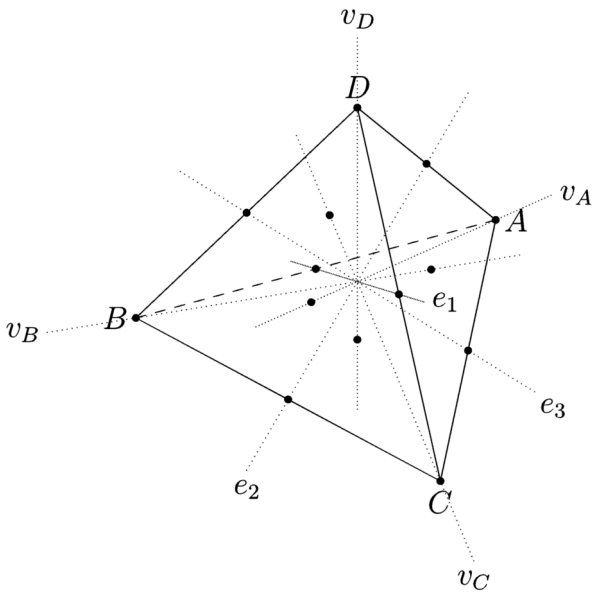


Figure 7: Regular tetrahedron's succulent rotation axes.

We can rotate by $120°$ or $240°$ (counterclockwise as viewed from the vertex) about any v_i, but only by $180°$ about any e_i. Along with the identity, this gives all $2 \cdot 4 + 3 + 1 = 12$ elements.

To make manipulating these elements easier, treat them as moving elements in a list. We name this list with indices as shown in Figure 8. Thus, the identity element I is (A, B, C, D). A rotation of $240°$ around v_A swaps vertices in positions $(3 \quad 4)$ then $(2 \quad 3)$, so $v_A = (A, D, B, C)$ as shown in Figure 9.

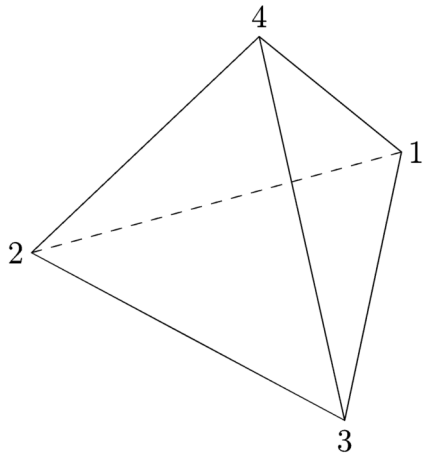


Figure 8: Regular tetrahedron's indices.

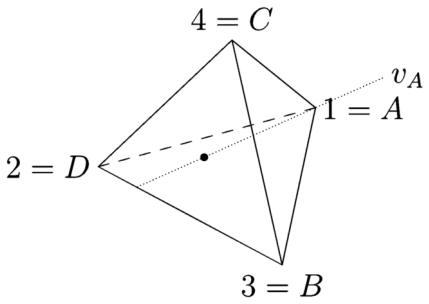


Figure 9: $v_A = (A, D, B, C)$.

If we take a look at an edge rotation, say e_1, you will see it also swaps two vertices: in this case, $(3 \quad 4)$ and $(1 \quad 2)$. In general, any edge rotation or vertex rotation will swap two vertices—you can see this by plain symmetry or if you want, working it out for each rotation.

We now have a more abstract representation of this group: namely, it is the group of *even permutations* of (A, B, C, D). Even permutations are permutations made by swapping two pairs at a time. For example, (B, A, D, C) is even, but (A, B, D, C) is not. The group operation is composing two permutations by chaining them together. Note that the identity, (A, B, C, D) is considered even, just as 0 is considered even.

One element is clearly not enough, because this group is not cyclic. Can we do it in two elements though?

Consider two vertex rotations, which cycle (without loss of generality) the first three vertices and the last three vertices. That is, $a = (3, 1, 2, 4)$ and $b = (1, 4, 2, 3)$. Can we get every even permutation with combinations of a and b? Let's try list them out:

$$
\begin{array}{llll}
a = (3,1,2,4), & a^2 = (2,3,1,4), & a^3 = I = (1,2,3,4), & b = (1,4,2,3), \\
b^2 = (1,3,4,2), & \cancel{b^3} = I = a^3, & ab = (2,1,4,3), & ab^2 = (4,1,3,2), \\
a^2b = (4,2,1,3), & a^2b^2 = (3,4,1,2), & \cancel{ba} = a^2b^2, & b^2a = (3,2,4,1), \\
ba^2 = (2,4,3,1), & \cancel{b^2a^2} = ab, & \cancel{bab} = a^2, & \cancel{b^2ab} = ba^2, \\
\cancel{bab^2} = a^2b, & b^2ab^2 = (4,3,2,1) = ba^2b &&
\end{array}
$$

We have successfully generated all 12 elements with the set $\{a, b\}$. Thus, a two element generating set is sufficient! Interestingly, this means you can turn a tetrahedron however you want by holding it at two corners and twisting it with each.

For the curious, this group is known as the alternating group A_4.

(d) Whether the group is **commutative**

The group is clearly not commutative, since $ab \neq ba$.

18. Tetrahedron under reflection

This is just the snap group of order 4, S_4.

(a) Number of elements

As we found in the first problem, S_4 has $4! = 24$ elements.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

As we found in the first problem, S_4 has $4! = 24$ elements.

(c) A smallest possible **generating set**

This is tricky.

The obvious thing to do is keep $\{a, b\}$ from the previous problem and add some reflection c. Then $\{a, b, c\}$ has all 24 elements, since $\{a, b\}$ makes 12 elements and c makes a copy of each "in the mirror world." This is not, however, the right answer.

A generating of 2 elements is actually possible! There are several ways to see this, but I find a permutation argument easiest to follow.

S_4 is not just the reflection group of the tetrahedron, but also the group of all permutations of $(1, 2, 3, 4)$. Consider the permutation $j = (4, 1, 2, 3)$, which cycles all the elements, and the permutation $k = (2, 1, 3, 4)$, which swaps the first elements. Then

$$j = (4, 1, 2, 3), \quad j^2 = (3, 4, 1, 2), \quad j^3 = (2, 3, 4, 1), \quad j^4 = I = (1, 2, 3, 4).$$

We can flip any two adjacent elements (as well as the first and last elements) by doing the following:

1. Cycle using powers of j until the two elements in question are the first two elements.
2. Swap them with an application of k.
3. Cycle back to the starting position with powers of j.

In more mathematical terms, we can swap indices i and $i + 1$, where $1 \le i \le 3$, with the following element.

$$j^{i-1} k j^{5-i}.$$

Intuitively, if you can swap any two adjacent elements, you can make any permutations. The proof of this is pretty standard and outside the scope of this answer key.

For fun, let's see what the elements j and k actually are, operating on the tetrahedron.

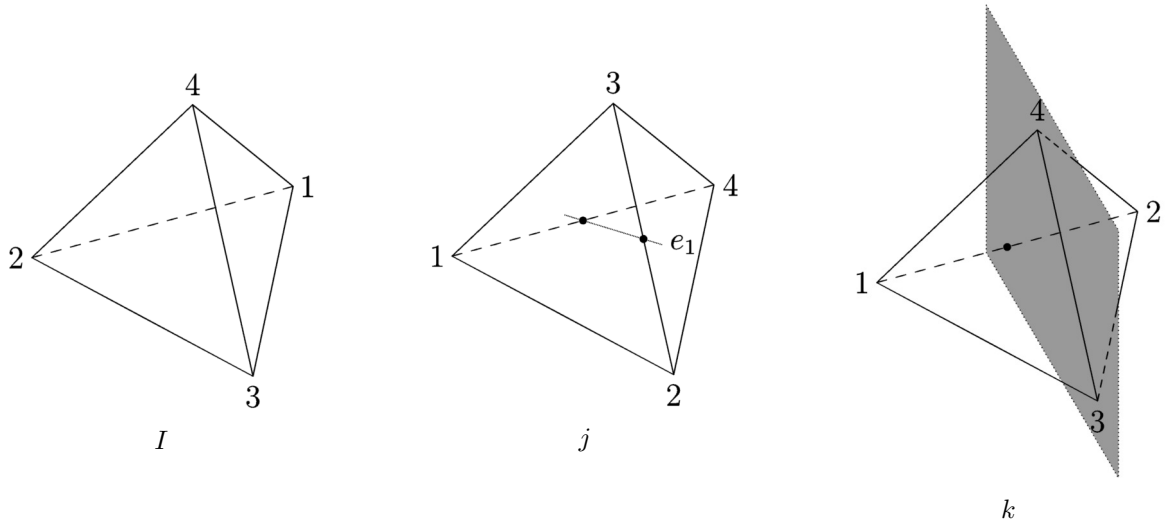


Figure 10: The two elements j and k generate the full symmetry group of the tetrahedron.

Thus, the true minimal generating set is $\{j, k\}$ as described.

(d) Whether the group is **commutative**

This group is certainly not commutative, since the previous group from Problem 17 was not commutative and is a subgroup of this group.

19. Cube under rotation

There are a couple ways to analyze this. My favorite one is to choose a face to make the top face, which can be done in 6 ways, then choose which rotation that face should be in, which can be done in 4 ways.

(a) Number of elements

Since we choose a front face in 6 ways, and its rotations in 4 ways, we have $6 \cdot 4 = 24$ total rotations.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

The order is found above.

(c) A smallest possible **generating set**

This is tough until you make a key observation. If we label space-diagonally opposite vertices (that is, vertices which don't share a face) with the same number, as shown in Figure 11, then we can easily enumerate valid rotations.

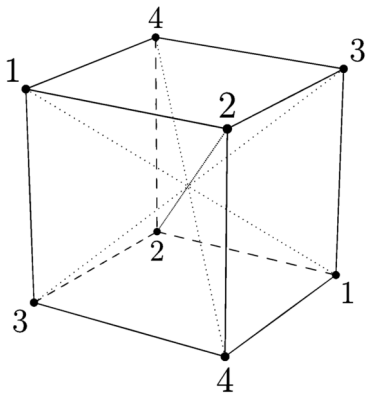


Figure 11: Marking opposite pairs of vertices.

The front face starts off saying "1,2,3,4." I claim that the $4!$ permutations of these four labels on the front face yields every rotation, and only rotations. This can be manually verified, but the higher-level argument isn't too bad.

First, note that you will always see the numbers "1,2,3,4" in *some order* on the front face; you cannot see two of one number because all numbers are placed on diagonals of each other, and never share a side.

Second, note that the list of four numbers on the front face uniquely determines the other labels, since each has exactly one pair on the back face. For example, if there is a 3 in the closest corner to the camera, then there *must* be a 3 in the furthest corner of the camera.

Third, we demonstrate that the permutation of labels can always be represented as a rotation. There are six fundamentally different types of label squares under rotation *rotation*, as shown in Figure 12. But all appear somewhere as a face on the cube, as shown in Figure 13.

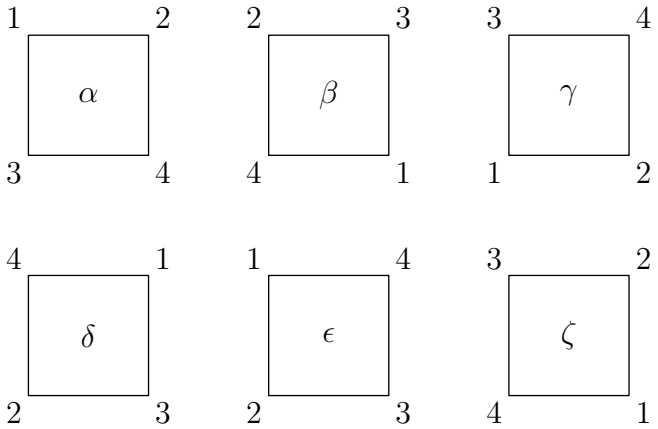


Figure 12: The six different labelings of a square.

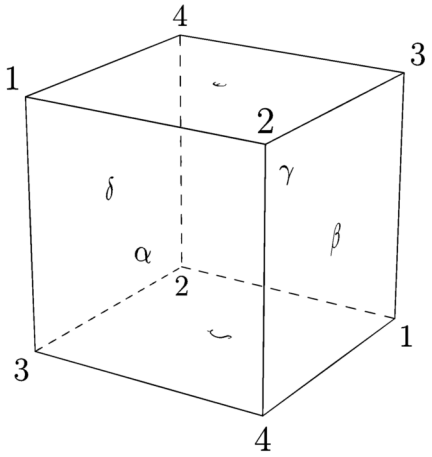


Figure 13: The six different labelings indeed appear on the cube!

We have demonstrated that every permutation of the front face labels 1. creates a unique orientation of the cube and 2. that orientation is a rotations. Since there are 24 unique permutations and 24 unique rotations, every rotation has exactly one corresponding permutation and vice versa. We can now construct an isomorphism! The set of label permutations under the operation of composing permutations (as we did

with the tetrahedron) and the set of rotations under the operation of composing rotations are *isomorphic*. In symbols, $S_4 \cong G$, our group.

So the group of rotations of a cube is actually S_4, the permutation group of 4 elements. I find this incredible.

Back to the main question: what is the minimal generating set? In the previous question, we found that the permutations $(4, 1, 2, 3)$–cycling all elements forward–and $(2, 1, 3, 4)$–swapping the first two elements–generating S_4. For the cube, those are two rotations a and b as shown in Figure 14.

Figure 14: The two rotations a and b.

(d) Whether the group is **commutative**

This group is not commutative, since S_4 is not commutative.

20. Cube under reflection

(a) Number of elements

There are 24 elements in the rotation group of the cube, so naturally there are 48 elements in the reflection group.

(b) If order < 10, the set of elements; otherwise, an explanation of how you know the order

For each of the 24 rotations of the cube, there is also a reflected version over some plane. This gives $2 \cdot 24 = 48$ total elements in this group.

(c) A smallest possible **generating set**

If c is a reflection about, say, the origin of the cube, then $\{a, b, c\}$ (where a, b are the rotations from before) would generate the whole group, since $\{a, b\}$ generates all rotations and $\{c\}$ generates their respective reflections. But can we do it in two?

As usual it seems, the answer is yes! The proof is not mine, because I couldn't figure it out, but due to math.SE user **verret**. It does require some more advanced concepts, so it is probably inaccessible to most.

The group we've been analyzing is $S_4 \times Z_2$. Let S_4 be permuting elements $\{1, 2, 3, 4\}$ and Z_2 be permuting elements $\{5, 6\}$ (note that $Z_2 = S_2$). Then given two elements $g = (4, 1, 2, 3, 5, 6)$ in our notation, meaning that indices $(1, 2, 3, 4)$ are cycled, and $h = (3, 1, 2, 4, 6, 5)$, meaning that indices $(1, 2, 3)$ and $(5, 6)$ are cycled, we can construct the group.

Note that $h^2 = (2, 3, 1, 5, 6)$ is in S_4, since it does not permute indices $5, 6$. It has a period of 3, and thus generates a subgroup of order 3. Furthermore, h^3 only permutes $(5, 6)$. Furthermore, g is an element in S_4 and has a period of 4. Thus, since $\gcd(3, 4) = 1$, by Lagrange's theorem we know that $\{h^2, g\}$ generates a subgroup of S_4 of at least order $3 \cdot 4 = 12$.

The only such subgroup, besides S_4 itself, is the alternating group A_4. But g is outside of A_4, since it is an odd permutation:

$$(1, 2, \boxed{3, 4}) \to (1, \boxed{2, 4}, 3) \to (\boxed{1, 4}, 2, 3) \to (4, 1, 2, 3).$$

Thus, $\{h^2, g\}$ does not generate A_4, and must generate S_4. Adding h^3, the generator for Z_2, to this set gives the full S_4, Z_2. The minimal generating set is therefore $\{g, h\}$ as defined.

For the curious, using our vertex "labeling" convention as before, the elements g and h are shown in Figure 15.

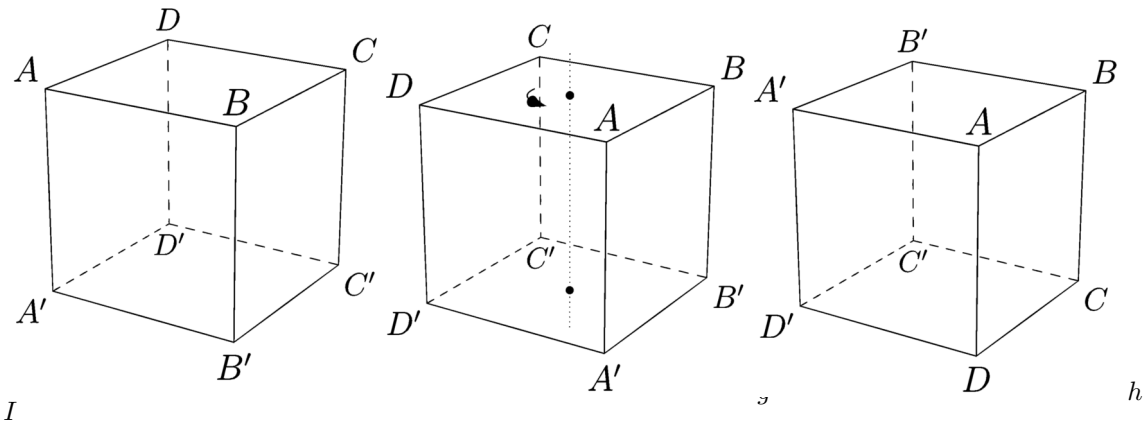


Figure 15: Elements g and h. Note that h is not solely a reflection about a mirror plane, but actually a combination of a rotation and reflection: a so-called rotoreflection!

(d) Whether the group is **commutative**

The subgroup of rotations of the cube, S_4, is not commutative, so this group is definitely not commutative.

5 Infinite Groups

Note: an **injection** f is a function taking A into B such that for all $a \in A$, $f(a) \in B$ and $f(a)$ is unique. In other words, there are no two $a_1, a_2 \in A$, $a_1 \neq a_2$ such that $f(a_1) = f(a_2)$.

1. Where have you come across the roots *iso-* and *-morphic* before?

(Answers may vary.)
Iso- is a root meaning equal. You might have seen it in isometry, isometric (paper), isomer, isosceles, isotonic, isotropy, and isotope. *Morph* means "form" or "shape." You might have seen it in metamorphosis, amorphous, anthropomorphism, or morpheme.

2. Can two groups be isomorphic if they have different orders?

No. Suppose we have groups A and B such that $|A| > |B|$ (A is bigger than B). Then we can't have a one-to-one correspondence between the elements of A and B, because there will always be elements in A without a "partner" in B. Thus, they cannot be isomorphic.

3. The rotation group for the hexagon H has six elements: the identity, and rotations of $\frac{\pi}{3}$, $\frac{2\pi}{3}$, π, $\frac{4\pi}{3}$, $\frac{5\pi}{3}$ radians. A rotation of $\frac{\pi}{3}$ generates the group.

(a) Which other rotation generates the group?

The other rotation which generates the group is $\frac{5\pi}{3}$, because 5 is coprime with 6. This is necessary because otherwise a subgroup of the full C_6 is formed. For example, $\frac{2\pi}{3}$ generates

$$\left\{0, \frac{2\pi}{3}, \frac{4\pi}{3}\right\},$$

which is merely C_3. Lame!

(b) What is the period of each element?

$$\begin{aligned} 0 \text{ or } I &: 1 \\ \frac{\pi}{3} &: 6 \\ \frac{2\pi}{3} &: 3 \\ \pi &: 2 \\ \frac{4\pi}{3} &: 3 \\ \frac{5\pi}{3} &: 6 \end{aligned}$$

4. H has the same number of elements as the dihedral group D_3.

(a) Are the two groups isomorphic? How do you know?

No, the two groups are not isomorphic, although they are the same size. An easy way to see this is that D_3 has three reflections, which have period 2, but H only has one element of period 2.

(b) What is the period of each element of D_3?

$$\begin{aligned} I \text{ or } I &: 1 \\ r &: 3 \\ r^2 &: 3 \\ f &: 2 \\ fr &: 2 \\ fr^2 &: 2 \end{aligned}$$

(c) What can you say if the sets of the periods of the elements of each group are not the same?

If the periods of each group can't be paired up, then the elements cannot be paired up either; after all, isomorphism is a structure-preserving operation. Thus, the two groups are not isomorphic.

(d) Which subgroups of the cyclic group C_6 and D_3 are isomorphic?

One is C_2, which is $\{0, \pi\}$ in C_6 and $\{I, \text{any reflection}\}$ in D_3. The other non-trivial one is C_3, which is $\left\{0, \frac{(3\pm1)\pi}{3}\right\}$ in C_6 and $\{I, \text{any rotation}\}$ in D_3. Both also have the trivial subgroup $\{I\}$ of just the identity element.

5. Could an infinite group be isomorphic to a finite group?

No, because their sizes are not the same; a one-to-one correspondence cannot be constructed.

6. Do you think all infinite groups are isomorphic to each other? Find a counterexample if you can.

Not all infinite groups are isomorphic. For example, the set of rotations about the origin has only one element of period 2, namely $r_{180°}$. But the set of reflections about the origin has infinitely many elements of period 2. Both, however, are infinite in size.

7. Make guesses to the relative sizes of the following pairs of sets. You may use shorthand like $|a| < |b|$, $|a| > |b|$, $|a| = |b|$. After you have made your guesses, we will analyze some of the cases and you can find out how good your intuition was.

(Answers may vary, but the "correct" answers are shown.)

(a) natural numbers, $\mathbb{N}$ vs. positive even numbers, $2\mathbb{N}$

$$|\mathbb{N}| = |2\mathbb{N}|$$

(b) natural numbers, $\mathbb{N}$ vs. positive rational numbers, $\mathbb{Q}^+$

$$|\mathbb{N}| = \left|\mathbb{Q}^+\right|$$

(c) natural numbers, $\mathbb{N}$ vs. real numbers between zero and one, $[0, 1)$

$$|\mathbb{N}| < |[0, 1)|$$

(d) real numbers, $\mathbb{R}$ vs. complex numbers, $\mathbb{C}$

$$|\mathbb{R}| = |\mathbb{C}|$$

(e) real numbers, $\mathbb{R}$ vs. points on a line

$$|\mathbb{R}| = |\text{points on a line}|$$

(f) points on a line vs. points on a line segment

$$|\text{points on a line}| = |\text{points on a line segment}|$$

(g) points on a line vs. points on a plane

$$|\text{points on a line}| = |\text{points on a plane}|$$

(h) rational numbers, $\mathbb{Q}$ vs. Cantor set (look this up or ask your teacher)

$$|Q| < |\mathcal{C}|$$

8. Now, please return to problem 7 and revise your answers. Justify each answer by producing a one-to-one correspondence, or showing the impossibility of doing so. Part (h) is an optional challenge.

(a) natural numbers, $\mathbb{N}$ vs. positive even numbers, $2\mathbb{N}$

This one is pretty straightforward. We have the following injection from $\mathbb{N}$ to $2\mathbb{N}$:

$$s \in \mathbb{N} \to 2s \in 2\mathbb{N}.$$

We have the following injection from $2\mathbb{N}$ to $\mathbb{N}$:

$$s \in \mathbb{N} \to \frac{s}{2} \in \mathbb{N}.$$

Since we can go both ways, we have $|\mathbb{N}| = |2\mathbb{N}|$, even though $\mathbb{N} \subset 2\mathbb{N}$ ($\mathbb{N}$ is a subset of $2\mathbb{N}$).[8]

(b) natural numbers, $\mathbb{N}$ vs. positive rational numbers, $\mathbb{Q}^+$

Surprisingly, we can make a one-to-one correspondence. If we list out the positive rationals in reduced form ($\frac{p}{q}$ with p, q coprime), ordered by increasing denominator, we can create the correspondence:

$$\begin{array}{cccccccccccc} \mathbb{Q}^+ & \frac{0}{1} & \frac{1}{1} & \frac{1}{2} & \frac{2}{1} & \frac{1}{3} & \frac{3}{1} & \frac{1}{4} & \frac{2}{3} & \frac{3}{2} & \frac{4}{1} & \cdots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\ \mathbb{N} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \end{array}$$

More details of this construction are given later in the textbook chapter. In any case, $|\mathbb{Q}^+| = |\mathbb{N}|$.

(c) natural numbers, $\mathbb{N}$ vs. real numbers between zero and one, $[0, 1)$

A one-to-one correspondence cannot exist between these two sets, so $|\mathbb{N}| < |[0, 1)|$. The classic proof of this is Cantor's diagonal argument, which is given in the textbook.

(d) real numbers, $\mathbb{R}$ vs. complex numbers, $\mathbb{C}$

This is a pretty tough problem to do in a logically sound way. The key is to represent complex numbers $a + bi$ as the ordered pair (a, b) where $a, b \in \mathbb{R}$. The set of all (a, b) is denoted $\mathbb{R}^2$.
Here is the route we will take:

1. Construct a one-to-one correspondence between the interval $[0, 1)$ and $\mathbb{R}$.
2. Use (1) to construct a similar correspondence between $[0, 1)^2$ and $\mathbb{R}^2$. That is, we will construct a correspondence between ordered pairs of reals in $[0, 1)$ and ordered pairs of any reals.
3. We find an injection from $[0, 1)$ into $[0, 1)^2$.
4. We find an injection from $[0, 1)^2$ into $[0, 1)$. This shows there is a one-to-one correspondence between $[0, 1)$ and $[0, 1)^2$.
5. We "chain" the correspondences together:

$$\mathbb{R} \leftrightarrow [0, 1) \leftrightarrow [0, 1)^2 \leftrightarrow \mathbb{R}^2.$$

Step 1: The most straight forward way to do this is to show there is an injection from $[0, 1)$ into $\mathbb{R}$, and vice versa.[9] We have $f(x) = x$ as a straightforward injection from $[0, 1)$ into $\mathbb{R}$, and

$$g(x) = \frac{1}{1 + e^{-x}}$$

as an injection $g : \mathbb{R} \to [0, 1)$. Thus, there exists a one-to-one correspondence H between $\mathbb{R}$ and $[0, 1)$.
Step 2: If H is the function from Step 1, we have

$$J(a, b) = (H(a), H(b))$$

as a one-to-one correspondence between $\mathbb{R}^2$ and $[0, 1)^2$.
Step 3: An injection from $[0, 1)$ into $[0, 1)^2$ is straightforward:

[8] We didn't explicitly state it because it's pretty intuitive, but this is using the Cantor-Schröder-Bernstein theorem (CSB).
[9] Again, this uses the Cantor-Schröder-Bernstein theorem.

$$k_1(x) = (x, 0).$$

Step 4: An injection from $[0, 1)^2$ into $[0, 1)$ is the more challenging portion. The basic idea is to interleave digits like so:

$$(0.123456789..., 0.314159265) \overset{k_2}{\to} 0.132134415569728695...$$

The main issue with this construction is that $0.5 = 0.4999...$ gives two different outputs, so this mapping isn't even a function:

$$(0.5, 0.0) \to 0.50$$

$$(0.499..., 0.0) \to 0.409090... \neq 0.50.$$

The easiest thing to do here is arbitrarily choose one of these mappings. In particular, we represent a number with an infinite sequence of trailing zeroes $0.a_1a_2 \cdots a_n00000...$ with the numerically equivalent

$$0.a_1a_2 \cdots (a_n - 1)9999....$$

Now, our function k_2 is a true injection, since $k(a, b) \in [0, 1)$ for all $(a, b) \in [0, 1)^2$ and $k(a_1, b_1) \neq k(a_2, b_2)$ for $(a_1, b_1) \neq (a_2, b_2)$.

Step 5: We have constructed an injection k_1 from $[0, 1) \to [0, 1)^2$ and an injection k_2 from $[0, 1)^2 \to [0, 1)$. Thus, there exists a one-to-one correspondence K between $[0, 1)$ and $[0, 1)^2$.

We chain the correspondences, finally proving that there exists a one-to-one correspondence between $\mathbb{R}$ and $\mathbb{R}^2$:

$$\mathbb{R} \overset{H}{\leftrightarrow} [0, 1) \overset{K}{\leftrightarrow} [0, 1)^2 \overset{J}{\leftrightarrow} \mathbb{R}^2.$$

Thus, $|mathbbR| = \left|\mathbb{R}^2\right|$.

(e) real numbers, $\mathbb{R}$ vs. points on a line

This is pretty straightforward if you think of points on a line as points on a number line. We arbitrarily choose a point on the line for 0 and a point for 1. In this regime, each point on the line corresponds with a unique real number. Thus, $|\mathbb{R}| = |$points on a line$|$.

(f) points on a line vs. points on a line segment

The simplest way to do this is, once again, to show there is an injection going both ways. We can go from segment $\to$ line by observing that a segment is just a subset of a line. We can go from line to segment by representing each point as a real number $\mathbb{R}$ as we already did, then taking the function

$$f(x) = \frac{1}{1 + e^{-x}}$$

which turns that point into a real number in the interval $(0, 1)$. This can be mapped onto the line segment by simply choosing one endpoint to be 0 and the other to be 1.

$|$points on a line segment$| = |$points on a line$|$

(g) points on a line vs. points on a plane

We can represent points on a line, as usual, with $\mathbb{R}$. We can represent points on a plane by arbitrarily choosing non-collinear points for $(0, 0)$, $(1, 0)$ and $(0, 1)$ and letting this be a coordinate space where points (a, b) are expressed as

$$a < 1, 0 > +b < 0, 1 > .$$

Note that the two vectors don't have to be perpendicular. This shows that we can represent points on a plane by $\mathbb{R}^2$. But we've already proved $\left|\mathbb{R}^2\right| = |\mathbb{R}|$! Thus,

$$|\text{points on a plane}| = |\text{points on a line}|.$$

(h) rational numbers, $\mathbb{Q}$ vs. Cantor set (look this up or ask your teacher)

The Cantor set $\mathcal{C}$ is formed by iteratively deleting the open middle third of segments, starting with the unit segment. Formally, we can construct this like so[10]:

$$C_1 = [0, 1]$$

$$C_n = \frac{1}{3}C_{n-1} \cup \left(\frac{1}{3}C_{n-1} + \frac{2}{3}\right) \quad \text{for } n \geq 2$$

$$\mathcal{C} = \bigcap_{n=1}^{\infty} C_n. \quad \text{(Intersection of all intervals } C_n\text{.)}$$

More intuitively, the construction is shown in Figure 1.

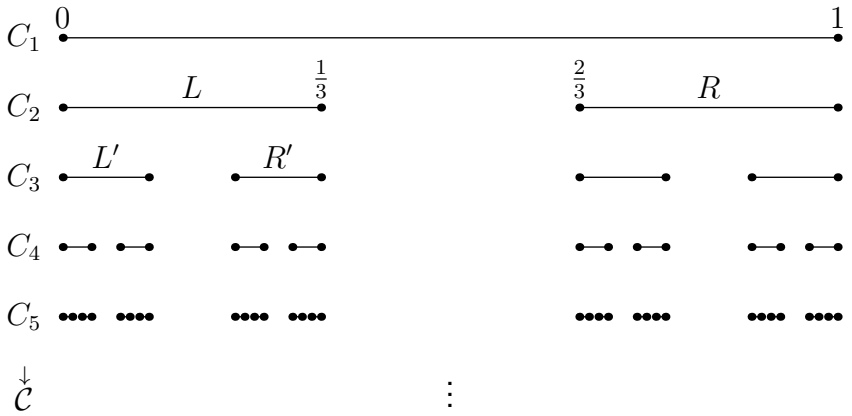


Figure 1: The construction of the Cantor set $\mathcal{C}$.

How do we attack this problem? It's not immediately clear how to tell whether a number x is in $\mathcal{C}$.[11] We should turn it into something we know how to deal with.

Consider how we would choose a random point in $\mathcal{C}$. Starting at C_1, we can either go to the left segment or the right segment (marked as L and R in Figure 1). If we choose L, then we once again have 2 choices: to go to L' or R'. This continues ad infinitum. Thus, we can correspond each element $x \in \mathcal{C}$ with a binary number in the interval $[0, 1]$.[12]

As an example, suppose we choose segments in the sequence $LRRLLLRLLL...$. Then the corresponding binary number is

$$0.01100010\overline{0}_2 = \frac{39}{128} \in [0, 1].$$

Thus, we have a one-to-one correspondence between the elements of $\mathcal{C}$ and $[0, 1]$. The question is asking the relative sizes of $\mathbb{Q}$ and $\mathcal{C}$. We already know (by Cantor's diagonal argument or otherwise) that $|\mathbb{Q}| < |[0, 1]|$. Therefore, we have

$$|\mathbb{Q}| < |[0, 1]| = |\mathcal{C}| \implies |\mathbb{Q}| < |\mathcal{C}|.$$

9. Here's a list of infinite sets, each with an operation. For each pair, answer: i. Does it form a group? ii. Which previous group(s) is it isomorphic to?

(a) natural numbers, addition

i. Does it form a group?

Nope! It cannot satisfy the identity, since for $x + I = I + x = I$ to be true for all x we need $I = 0$. If you're a fan of the standard ISO 80000, and include $0 \in \mathbb{N}$, then it still doesn't form a group, since it can't satisfy the invertibility property. For example, the inverse of 1 should be -1 so that $1 + (-1) = 0$, but $-1 \notin \mathbb{N}$.

[10] This construction, taken literally, is actually scaling the set down by $\frac{1}{3}$ and copying it at each step. The net result, however, is equivalent.

[11] A number x is in $\mathcal{C}$ if and only if it has a ternary (base-3) representation consisting of only 0s and 2s. For example, $1/27$ is in the Cantor set because $1/27 = 0.001_3 = 0.000\overline{2}_3$.

[12] Note it is inclusive because $0.1111...2 = 1$ and $0.0000...2 = 0$.

ii. Which previous group(s) is it isomorphic to?

oof

(b) integers, addition

i. Does it form a group?

It does form a group. The identity element is 0, and it satisfies all necessary properties:
Identity: $x + 0 = 0 + x = x$.
Closure: If $x, y \in \mathbb{Z}$, then $x + y \in \mathbb{Z}$.
Associativity: We have $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{Z}$.
Inverse: The inverse of x is $-x$, since $x + (-x) = (-x) + x = 0$.

ii. Which previous group(s) is it isomorphic to?

None, I wonder why.

(c) even integers, addition

i. Does it form a group?

It does form a group. The identity element is 0, and it satisfies all necessary properties:
Identity: $x + 0 = 0 + x = x$.
Closure: If $x, y \in 2\mathbb{Z}$, then $x + y = 2s + 2t = 2(s + t) \in 2\mathbb{Z}$.
Associativity: We have $x + (y + z) = (x + y) + z$ for all $x, y, z \in 2\mathbb{Z}$.
Inverse: The inverse of x is $-x$, since $x + (-x) = (-x) + x = 0$.

ii. Which previous group(s) is it isomorphic to?

It is isomorphic to integers under addition, because we can simply correspond $2n \in 2\mathbb{Z}$ with $n \in \mathbb{Z}$. All the group structure is preserved, since $2m + 2n \in 2\mathbb{Z}$ corresponds with $m + n \in \mathbb{Z}$.

(d) odd integers, addition

i. Does it form a group?

This does not form a group, since it cannot satisfy the identity property. There is no odd integer I such that $x + I = I + x = x$.

ii. Which previous group(s) is it isomorphic to?

oof

(e) rational numbers, addition

i. Does it form a group?

Yes, this forms a group with identity element 0. It satisfies all necessary properties:
Identity: $\frac{p}{q} + 0 = 0 + \frac{p}{q} = \frac{p}{q}$.
Closure: If $\frac{p_1}{q_1}, \frac{p_2}{q_2} \in \mathbb{Q}$, then

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2} \in \mathbb{Q}.$$

Associativity: We have $x + (y + z) = (x + y) + z$ for all $x, y, z \in 2\mathbb{Z}$.
Inverse: The inverse of $\frac{p}{q}$ is $-\frac{p}{q}$, since

$$\frac{p}{q} + \left(-\frac{p}{q}\right) = \left(-\frac{p}{q}\right) + \frac{p}{q} = 0.$$

ii. Which previous group(s) is it isomorphic to?

None. It's not isomorphic to integers under addition because for each element $x \in \mathbb{Q}$, there exists an element $y = \frac{x}{2} \in \mathbb{Q}$ such that

$$y + y = x.$$

This is impossible for any odd integers (analogously, for the group of even integers under addition, impossible for any elements not divisible by 4).

(f) real numbers, addition

i. Does it form a group?

Yes, this forms a group with identity element 0. It satisfies all necessary properties:
Identity: $x + 0 = 0 + x = x$.
Closure: If $x, y \in \mathbb{R}$, then $x + y \in \mathbb{R}$.
Associativity: We have $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{R}$.
Inverse: The inverse of x is $-x$, since $x + (-x) = (-x) + x = 0$.

ii. Which previous group(s) is it isomorphic to?

None. After all, $\mathbb{R}$ is uncountable, while the groups we've seen so far are countable.

(g) complex numbers, addition

i. Does it form a group?

Yes, this forms a group with identity element $0 = 0 + 0i$. It satisfies all necessary properties:
Identity: $x + 0 = 0 + x = x$.
Closure: If $x, y \in \mathbb{C}$, then $x + y \in \mathbb{C}$.
Associativity: We have $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{C}$.
Inverse: The inverse of x is $-x$, since $x + (-x) = (-x) + x = 0$.

ii. Which previous group(s) is it isomorphic to?

Assuming the axiom of choice[13], it is actually isomorphic to $\mathbb{R}$ under addition. Since $\mathbb{C}$ is uncountable, this is the only candidate.

Proving they are isomorphic is tough[14] without the introduction of vector spaces (specifically, $\mathbb{Q}$-vector spaces). I was originally going to put it in, but I couldn't get it under a satisfactory length. If you're really curious, check out https://math.stackexchange.com/a/1511685/677124 for a mildly accessible view of the subject... if you already understand the basics of vector spaces. In summary, both $\mathbb{R}$ and $\mathbb{R}^2$ are vector spaces over the rational numbers $\mathbb{Q}$, and since $|\mathbb{R}| = |\mathbb{R}^2|$ they are isomorphic as vector spaces. This also implies that they are isomorphic as additive groups.

(h) integers, multiplication

i. Does it form a group?

No, this does not form a group. The identity element would be 1, so that $1 \cdot x = x \cdot 1 = x$, but $1 \cdot 0 = 0 \neq 1$, so it cannot satisfy invertibility. Even if we removed 0, for any $p \neq \pm 1$ there is no integer q such that $pq = 1$.

ii. Which previous group(s) is it isomorphic to?

oof

(i) integer powers of 2, multiplication

i. Does it form a group?

[13] The axiom of choice states that for every indexed family of sets $(S_i)_{i \in I}$, where $S_i \neq \emptyset$, there exists an indexed family of elements $(x_i)_{i \in I}$ such that $x_i \in S_i$ for all $i \in I$. Intuitively, this means that given a list of non-empty sets, you can select exactly one item from each set.

[14] In fact, it is impossible to construct an "explicit" isomorphism because $\mathbb{R} \ncong \mathbb{C}$ is consistent with the axiom of choice.

Yes! Let the group be called $\in = \{2^x : x \in \mathbb{Z}\}$ for fun. The identity element is $2^0 = 1$. The group properties are satisfied:
Identity: $2^x \cdot 1 = 1 \cdot 2^x = 2^x$.
Closure: $2^x \cdot 2^y = 2^{x+y} \in \in$.
Associativity: We have $2^x(2^y \cdot 2^z) = (2^x \cdot 2^y)2^z = 2^{x+y+z}$ for all $x, y, z \in \mathbb{Z}$.
Inverse: The inverse of 2^x is 2^{-x}, since $2^x 2^{-x} = 2^{-x}2^x = 2^0 = 1$.

ii. Which previous group(s) is it isomorphic to?

It is isomorphic to integers under addition. $2^n \in \in$ corresponds with $n \in \mathbb{Z}$, since we have

$$2^m \cdot 2^n = 2^{m+n} \leftrightarrow m + n.$$

(j) rational numbers, multiplication

i. Does it form a group?

The rational numbers under multiplication do not form a group, because if the identity element is 1, then $1 \cdot 0 = 0 \neq 1$, so it cannot satisfy invertibility.

ii. Which previous group(s) is it isomorphic to?

oof

(k) rational numbers excluding 0, multiplication

i. Does it form a group?

Yes! The rational numbers excluding 0, written $\mathbb{Q}\backslash 0$, form a group under multiplication with identity element 1. The group properties are satisfied:
Identity: $x \cdot 1 = 1 \cdot x = x$.
Closure: If $x, y \in \mathbb{Q} \setminus 0$, then $x + y \in \mathbb{Q} \setminus 0$; the product of two nonzero rational numbers is rational and nonzero.
Associativity: We have $x(yz) = (xy)z$ for all $x, y, z \in \mathbb{Q} \setminus 0$.
Inverse: The inverse of $x \in \mathbb{Q} \setminus 0$ is $\frac{1}{x}$, since $x\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)x = 1$ and $x \neq 0$.

ii. Which previous group(s) is it isomorphic to?

It is not isomorphic to any. The only candidates are other groups with countably infinite order, aka addition of rational numbers and addition of integers.
It cannot be addition of rational numbers, because for every element $k = \frac{p}{q}$ there exists an element $r = \frac{p}{2q}$ such that $k = 2r$. This property is not true for rational numbers under multiplication, because the corresponding r would be $\sqrt{\frac{p}{q}}$, which is only valid for perfect (rational) squares $\frac{p}{q}$. For the same reason, it cannot be addition of integers, since odd integers also cannot have this property.

(l) complex numbers, multiplication

i. Does it form a group?

No, because 0 prevents the group from satisfying invertibility.

ii. Which previous group(s) is it isomorphic to?

oof

(m) rotation by a rational number of degrees

i. Does it form a group?

Yes! The identity is 0 and it can simply by thought of adding rationals modulo 360. The group properties are satisfied:
Identity: $x \cdot 1 = 1 \cdot x = x$.
Closure: If $x, y \in \mathbb{Q}$ then $x + y \in \mathbb{Q}$ and it
Associativity: We have $x(yz) = (xy)z$ for all $x, y, z \in \mathbb{Q} \setminus 0$.
Inverse: The inverse of $x \in \mathbb{Q} \setminus 0$ is $\frac{1}{x}$, since $x\left(\frac{1}{x}\right) = \left(\frac{1}{x}\right)x = 1$ and $x \neq 0$.

ii. Which previous group(s) is it isomorphic to?

None. The easiest way to see this is that the element $\frac{360}{n}^\circ$, where n is an integer, has period n, so we can construct elements of arbitrary periods. No previous groups have elements of arbitrary periods.

(n) rotation by a rational number of radians

i. Does it form a group?

Yes! The identity element is 0 and it is totally equivalent to the rational numbers under addition. That's because for any rational radian rotations r_{p_1/q_1} and r_{p_2/q_2}, where $p_1, q_1, p_2, q_2 \in \mathbb{Z}$, $q_1, q_2 \neq 0$ and $p_1/q_1 \neq p_2/q_2$, we have $r_{p_1/q_1} \ncong r_{p_2/q_2}$. The easiest way to understand this is that for two such rotations to be equal, there must be some integer k such that

$$\frac{p_1}{q_1} = \frac{p_2}{q_2} + 2\pi k.$$

There are two cases to consider: $k = 0$ and $k \neq 0$. If $k = 0$, then $\frac{p_1}{q_1} = \frac{p_2}{q_2}$, which violates our assumption. If $k \neq 0$, then since π is irrational, the RHS is irrational while the LHS is rational. Since an irrational and rational cannot be equal, such an integer k cannot exist and $r_{p_1/q_1} \ncong r_{p_2/q_2}$.

The group properties are straightforward and identical to the rationals under addition.

ii. Which previous group(s) is it isomorphic to?

As explained, it is isomorphic to the rational numbers under addition.

(o) rotation by an integer number of radians

i. Does it form a group?

Yes. The identity element is 0 and it is equivalent to the integers under addition. We proceed in a similar method to the previous problem: consider two integer radian rotations r_a and r_b where $a, b \in \mathbb{Z}$ and $a \neq b$.

Suppose $r_a \cong r_b$. Then there is some integer k such that

$$a = b + 2\pi k.$$

If $k = 0$, then $a = b$, contradicting our assumption that $a \neq b$. If $k \neq 0$, then the RHS is irrational while the LHS is rational. This is impossible to satisfy, so k does not exist and $r_a \ncong r_b$.

The group properties are straightforward and identical to the integers under addition.

ii. Which previous group(s) is it isomorphic to?

As explained, it is isomorphic to the integers under addition.

10. Can an irrational number taken to an irrational power ever be rational? Consider the potential example $a = \sqrt{2}^{\sqrt{2}}$. To help you answer this question, let $b = a^{\sqrt{2}}$. Simplify b, and explain why we don't need to know whether a is rational or irrational.

We have

$$b = a^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2.$$

We know $\sqrt{2}$ is irrational. Suppose a is rational. Then we have an example of an irrational number raised to an irrational power which *is* rational! But if a is not rational, then must be irrational, so b is an example of an irrational number (a) raised to an irrational power ($\sqrt{2}$) which is rational! Thus, no matter the case, there exists an irrational number raised to an irrational power which is rational. Interestingly, we don't know whether a is rational or irrational, only that one of a, b satisfies the problem.

Logically, let $A = a$ is rational and $C =$ there exists an irrational number raised to an irrational power which is rational. Then $A \to C$ and $\neg A \to C$. Since $A \vee \neg A$, we know that $C \vee C$, so C is true.

As an aside, a is the irrational one (and is in fact transcendental) by the Gelfond-Schneider theorem. Proving this theorem requires some pretty advanced analysis, yet we are able to derive related results with simple logic.