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 of the regular hexagon, also known as the cyclic group of order 6, C_6, 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 can generate 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. C_6 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?

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

(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 and a finite group be isomorphic?

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)

$$|Q| < |C|$$

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 $2\mathbb{N}$).[6]

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

(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.[7] 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 $[0, 1)^2$.

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

[7] Again, this uses the Cantor-Schröder-Bernstein theorem.

Step 3: An injection from $[0,1)$ into $[0,1)^2$ is straightforward:

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

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

(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 → 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. We start with the interval $[0,1]$, then split it into two intervals: $\left[0,\frac{1}{3}\right]$ and $\left[\frac{2}{3},1\right]$. This set, let's call it $\mathcal{C}_1$, has total length $\frac{2}{3}$. We split up each of $\mathcal{C}_1$'s intervals again, forming $\mathcal{C}_2 = \left[0,\frac{1}{9}\right] \cup \left[\frac{2}{9},\frac{1}{3}\right] \cup \left[\frac{2}{3},\frac{7}{9}\right] \left[\frac{8}{9},1\right]$. Note what happened here: the first interval in $\mathcal{C}_1$ had its middle third deleted, splitting it into our first two intervals; and the same with the second interval. $\mathcal{C}_2$ has total length $\frac{4}{9}$. We repeat this process to infinity, so that (informally speaking) $\mathcal{C}_\infty = \mathcal{C}$, the Cantor set. The set has total length 0, but it's not empty! 0, $\frac{1}{3}$, and $\frac{7}{9}$ are all members of $\mathcal{C}$, for example.
For a visual, the construction is shown in Figure 1.

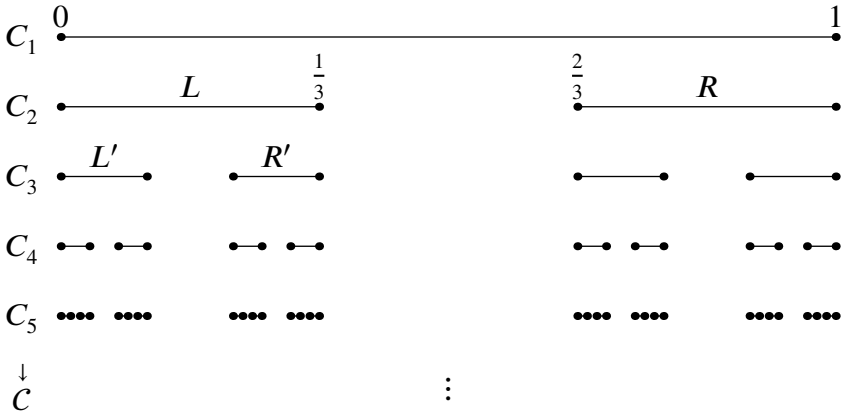

Figure 1: The construction of the Cantor set $\mathcal{C}$.

How do we attack this problem? It's not immediately clear how to tell whether a number x is in $\mathcal{C}$. It's not something as simple as $\frac{p}{3^n}$ for some integers p, n, because $\frac{4}{9}$ is in the deleted interval $\left[\frac{1}{3},\frac{2}{3}\right]$, and is not in $\mathcal{C}$. We should represent the set as something we know how to deal with, keeping in mind that answering our question of cardinality only involves making a one-to-one correspondence, not a complete description of the set.

Consider how we would choose a random point in $\mathcal{C}$. Starting at $\mathcal{C}_1$, we can either go to the left segment or the right segment (marked as L and R in Figure 1). If we choose L, which is $\left[0,\frac{1}{3}\right]$, then we once again have 2 choices: to go to L', which is $\left[0,\frac{1}{9}\right]$, or R', which is $\left[\frac{2}{9},\frac{1}{3}\right]$. This continues forever, and every element of $\mathcal{C}$ can be uniquely obtained this way. Thus, we can correspond each element $x \in \mathcal{C}$ with a binary number in the interval $[0,1]$.

As an example, suppose we choose segments in the sequence $LRRLLLRLLLLLLLL...$ with infinite trailing L's. 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 $[0,1]$.[8] 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

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

This might be counterintuitive, that a set with "length" 0 is still bigger than all the rational numbers on the great big number line. Frankly, without some formal language (particularly from topology), it's hard to describe this set with any rigor. The Wikipedia article on the Cantor set may guide you further!

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

[8] Note it is inclusive because $0.\overline{1}_2 = 1$ and $0.\overline{0}_2 = 0$.

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 $-1 \notin \mathbb{N}$.

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

Not a group, 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?

Not a group, 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[9], 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[10] 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?

Not a group, oof.

(i) integer powers of 2, multiplication

i. Does it form a group?

[9] 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.

[10] 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 $\mathcal{W} = \{2^x \ : \ x \in \mathbb{Z}\}$ 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: $2^x \cdot 2^y = 2^{x+y} \in \mathcal{W}$.

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. $2^n \in \mathcal{W}$ 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; the identity element must be 1, but then 0 would not have an inverse since nothing times 0 is 1.

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

Not a group, oof.

(k) rational numbers excluding 0, multiplication

i. Does it form a group?

Yes! The rational numbers excluding 0, written $\mathbb{Q} \setminus 0$, 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 $x \cdot y \in \mathbb{Q} \setminus 0$; 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. Let this group be $\mathcal{M}$. The only candidates are other groups with countably infinite order, aka addition of rational numbers ($\mathcal{R}$) and addition of integers ($\mathcal{J}$). $\mathcal{M}$ can't be isomorphic to $\mathcal{R}$, because all elements of $\mathcal{R}$ have a "half," while the elements of $\mathcal{M}$ don't all have an analogous square root. To be more explicit, all elements $k' = \frac{p}{q}$ in $\mathcal{R}$ have a corresponding element j' such that $j' + j' = k'$. But not all elements k in $\mathcal{R}$ have a corresponding element j such that $j \cdot j = k$, since, for example, no element q of $\mathcal{M}$ satisfies $q \cdot q = -\frac{1}{2}$.

Thinking about $j' + j' = k'$ and $j \cdot j = k$ also helps us prove that $\mathcal{M}$ can't be isomorphic to $\mathcal{J}$. Take the element $k = 4$ in $\mathcal{M}$, for example. Then $j = 2$ and $j = -2$ both square to k. In contrast, no element k' of $\mathcal{J}$ has the property that there are *two different values of* j' which satisfy $j' + j' = k'$, since either is no solution or the unique solution $j' = k'/2$.

(l) real numbers excluding 0, multiplication

i. Does it form a group?

Yes! The real numbers excluding 0, written $\mathbb{R} \setminus 0$, form a group under multiplication with identity element 1. The group properties are satisfied:

Identity: $x \cdot 1 = 1 \cdot x = x$.

Closure: If $x, y \in \mathbb{R} \setminus 0$, then $x + y \in \mathbb{R} \setminus 0$; the product of two nonzero rational numbers is rational and nonzero.

Associativity: We have $x(yz) = (xy)z$ for all $x, y, z \in \mathbb{R} \setminus 0$.

Inverse: The inverse of $x \in \mathbb{R} \setminus 0$ 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 of the previous groups.

(m) 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?

Not a group, oof.

(n) 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.

(o) 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 $r_{p_1/q_1} \cong r_{p_2/q_2}$. 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.

(p) 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

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

Let's write out the facts we know.

1. We know that $\sqrt{2}$ is irrational.

2. By (1), we know that a is the result of an irrational number to an irrational power.

3. We know that 2 is the result of a to an irrational power.

Suppose a is rational. Then $a = \sqrt{2}^{\sqrt{2}}$ is our desired example, by (2)! So, suppose a is irrational. Then by (3), 2 is the result of an irrational number (namely, a) to an irrational power (namely, $\sqrt{2}$). So then $2 = a^{\sqrt{2}}$ is our desired example! a has to be irrational or rational; it can't be something else. But in either case, we can produce a number which satisfies the requirements. Thus, we can answer in the affirmative, but we can't give an explicit example!

In fact, a is the irrational one by the Gelfond-Schneider theorem. Proving this theorem requires some pretty advanced analysis, yet we are able to derive related results with simple logic! Exciting.