Functions

Let $f : X \to Y$ be a function. Recall, the image of f is

$$f(X) = \{y \in Y \mid f(x) = y \text{ for some } x \in X\}.$$

Further, f is...

- injective if at most one $x \in X$ maps to each $y \in Y$, i.e.

  $$\text{if } f(x_1) = f(x_2) \text{ then } x_1 = x_2.$$

  Ex. $f : \mathbb{R}_{>0} \to \mathbb{R}$ defined by $x \mapsto x^2$.

  Non-ex. $f : \mathbb{R} \to \mathbb{R}$ defined by $x \mapsto x^2$.

- surjective if every $y \in Y$ gets mapped to, i.e.

  $$\text{for all } y \in Y, \text{ there exists } x \in X \text{ such that } f(x) = y.$$

  Ex. $f : \mathbb{R} \to \mathbb{R}_{\geqslant 0}$ defined by $x \mapsto x^2$.

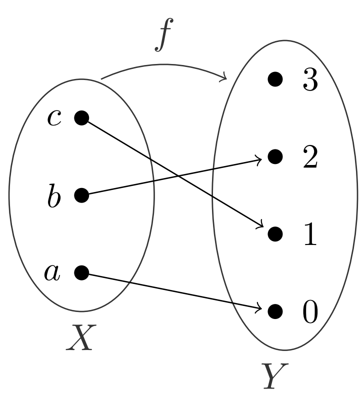
  Non-ex. $f : \mathbb{R} \to \mathbb{R}$ defined by $x \mapsto x^2$.

- bijective if it's both injective and surjective.

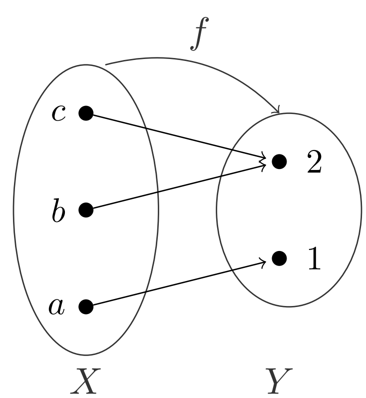
  Ex. $f : \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ defined by $x \mapsto x^2$.

  Non-ex. $f : \mathbb{R} \to \mathbb{R}$ defined by $x \mapsto x^2$.

Injective, not surjective:



Surjective, not injective:



To show $f : X \to Y$ is injective:

Start: *Suppose* $f(x_1) = f(x_2)\ldots$ Goal: *Show* $x_1 = x_2$.

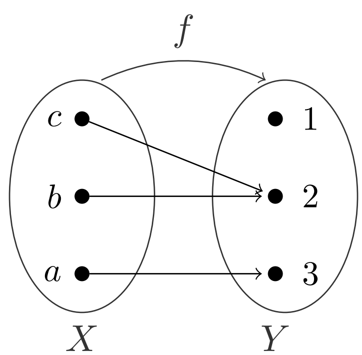
To show $f : X \to Y$ is surjective:

Start: *Let* $y \in Y\ldots$ Goal: *Find* $x \in X$ *such that* $f(x) = y$.

For a function $f : X \to Y$, and an element $y \in Y$, let

$$f^{-1}(y) = \{x \in X \mid f(x) = y\} \subset X,$$

called the inverse image or preimage of y. Note that this is abusing notation: we write f^{-1} whether or not f is invertible; and $f^{-1}(y)$ is a *set*, not an *element*.



$$f^{-1}(1) = \varnothing$$

$$f^{-1}(2) = \{b, c\}$$

$$f^{-1}(3) = \{a\}$$

We say f is invertible if for all $y \in Y$, $f^{-1}(y)$ has exactly one element (no more, no fewer).

Thm. For nonempty sets X and Y, a function $f : X \to Y$ is invertible if and only if it is bijective.

We say f is invertible if for all $y \in Y$, $f^{-1}(y)$ has exactly one element (no more, no fewer).

Thm. For nonempty sets X and Y, a function $f : X \to Y$ is invertible if and only if it is bijective.

Proof.

Suppose f is bijective. Since f is surjective, for all $y \in Y$, we have $|f^{-1}(y)| \geqslant 1$. And since f is injective, for any $x_1, x_2 \in f^{-1}(y)$, we have $x_1 = x_2$. So $|f^{-1}(y)| \leqslant 1$. Therefore, for all $y \in Y$, we have $|f^{-1}(y)| = 1$, so that f is invertible.

Now suppose f is invertible. Thus for all $y \in Y$, we have $|f^{-1}(y)| = 1$. Therefore, for all $y \in Y$, $f(y) \neq \varnothing$, so that f is surjective. And for all $y \in Y$, since $f^{-1}(y)$ has exactly one element, it has at most one element. So f is injective. Therefore, f is bijective.

$\square$

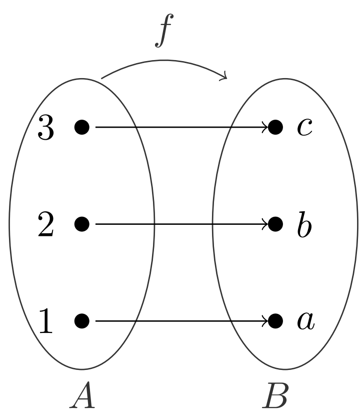
Cardinality of sets

Two sets A and B have the same size, or cardinality, if there is a bijection $f : A \to B$.

Example: We know that set $\{a, b, c\}$ has 3 elements because we can count them:

$$\begin{array}{rl} 1: & a \\ 2: & b \\ 3: & c \end{array}$$

But this is essentially the same as the bijection



Cardinality of sets

Definition:
Two sets A and B have the same size, or same cardinality, if and only if there is a bijection $f : A \to B$.

(This allows us to measure the relative sizes of sets, even if they happen to be infinite!)

Example: The sets $\mathbb{Z}_{\geqslant 0}$ and $\mathbb{Z}_{>0}$ have the same cardinality since

$$\begin{array}{rcl} f : \mathbb{Z}_{>0} & \to & \mathbb{Z}_{\geqslant 0} \\ x & \mapsto & x - 1 \end{array}$$

is a bijective map.

Countably infinite sets

A set is countable if it is either finite or the same cardinality as the natural numbers ($\mathbb{N} = \mathbb{Z}_{>0}$). If a set A is not finite but is countable, we say A is "countably infinite" and write $|A| = \aleph_0$ (pronounced "aleph naught" or "aleph null"). To show that $|A| = \aleph_0$: show A is not finite, and give a bijection $f : \mathbb{Z}_{\geqslant 0} \to A$.

Examples:

1. $\mathbb{Z}_{>0}$ is countably infinite:
   It is not finite, and $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ by $x \mapsto x$ is a bijection.
2. $\mathbb{Z}_{\geqslant 0}$ is countably infinite:
   It is not finite, and $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geqslant 0}$ by $x \mapsto x - 1$ is a bijection.
3. $\mathbb{Z}$ is countably infinite: Not finite, and $f : \mathbb{Z}_{>0} \to \mathbb{Z}$ by $x \mapsto (-1)^x \lfloor x/2 \rfloor$ is a bijection.

$$\begin{array}{rccccccccccc}
\mathbb{Z}_{>0}: & \cdots & 9 & 7 & 5 & 3 & 1 & 2 & 4 & 6 & 8 & \cdots \\
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathbb{Z}: & \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots
\end{array}$$

More on this last example, $|\mathbb{Z}| = \aleph_0$:

We started with the picture

$$\begin{array}{rccccccccccc}
\mathbb{Z}_{\geqslant 0}: & \cdots & 9 & 7 & 5 & 3 & 1 & 2 & 4 & 6 & 8 & \cdots \\
 & & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathbb{Z}: & \cdots & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \cdots
\end{array}$$

This at least gives us a "list" of integers,

$$1:0, \quad 2:1, \quad 3:-1, \quad 4:2, \quad 5:-2, \quad \ldots.$$

If I know that every integer appears on this list somewhere, then I know that the integers are countable. (Ok answer)
The next step in giving a more sophisticated, more robust, answer is to try to get the formula written down:

$$f : \mathbb{Z}_{>0} \to \mathbb{Z} \qquad x \mapsto \begin{cases} x/2 & \text{if } x \text{ is even,} \\ -(x-1)/2 & \text{if } x \text{ is odd.} \end{cases} \qquad \text{(Better answer)}$$

To be even more sophisticated, we used the floor function to get a closed form answer:

$$\begin{cases} x/2 & \text{if } x \text{ is even,} \\ -(x-1)/2 & \text{if } x \text{ is odd} \end{cases} = (-1)^x \lfloor x/2 \rfloor,$$

for $x \in \mathbb{Z}_{>0}$. (Best answer)

Recall that $|A| = |B|$ if and only if there is a bijection $f : A \to B$.

If we know that $|A| = \aleph_0$ and $f : A \to B$ is a bijection, then $|B| = |A| = \aleph_0$.

Example: To show that $2\mathbb{Z} = \{$ even integers $\}$ is countably infinite, we could construct a bijection like in the previous example. But it's a little more straightforward to note that

$$\begin{aligned} f : \mathbb{Z} &\to 2\mathbb{Z} \\ x &\mapsto 2x \end{aligned} \quad \text{is a bijection,}$$

so that $|2\mathbb{Z}| = |\mathbb{Z}| = \aleph_0$.

Examples: For each of the following, show that the set is countably infinite. (Define a bijective function to something that we know to be countably infinite if it's not too hard; otherwise, explain how to make the list.)

1. The set of negative integers ($\mathbb{Z}_{<0}$).
2. The set of integers less than 100 ($\mathbb{Z}_{<100}$).
3. The set of integers that are integer multiples of 3 ($3\mathbb{Z}$).
4. The set of integers that are not integer multiples of 3 ($\mathbb{Z} - 3\mathbb{Z}$).

The rational numbers

Claim: $\mathbb{Q}_{>0}$ is countably infinite. Make a table:

	1	2	3	4	5	$\cdots$
1	$1/1$ (1)	$2/1$ (2)	$3/1$ (5)	$4/1$ (6)	$5/1$ (11)	$\cdots$
2	$1/2$ (3)	$2/2$	$3/2$ (7)	$4/2$	$5/2$	
3	$1/3$ (4)	$2/3$ (8)	$3/3$	$4/3$	$5/3$	
4	$1/4$ (9)	$2/4$	$3/4$	$4/4$	$5/4$	
5	$1/5$ (10)	$2/5$	$3/5$	$4/5$	$5/5$	
$\vdots$						

(skip prev. counted fractions)

Then use the same alternating map that we did for $\mathbb{Z}_{>0} \to \mathbb{Z}$ to build a bijection $\mathbb{Q}_{>0} \to \mathbb{Q}$, yielding a bijection $\mathbb{Z}_{>0} \to \mathbb{Q}_{>0} \to \mathbb{Q}$.

Are there sets that are *not* countable?

Theorem. The set of real numbers in the interval $[0, 1)$ is not countable.

Proof outline: We will prove this by contradiction.
Suppose that the set $[0, 1)$ is countable, so that the real numbers in $[0, 1)$ can be listed.
Take one such list.

Goal: Show that the list isn't complete. Namely, algorithmically produce an element of $[0, 1)$ that isn't on any fixed list.

Take this is the supposedly complete list of real numbers in $[0, 1)$.

For example:

1. 0.**0**01240191057...
2. 0.1**2**3451234512...
3. 0.33**3**333333333...
4. 0.500**0**00000000...
5. 0.1212**1**2121212...
6. 0.55555**5**555555...
7. 0.141592**6**53589...
8. 0.0018500**0**0000...
9. 0.11111111**1**111...
10. 0.750000000**0**00...
11. 0.9487973624**7**1...

⋮

Algorithm for producing a number that is not on the list:
In the ith number in the list, highlight the ith digit.
Build a new number as follows:

i. If the highlighted digit of the ith number is a 0, then make the corresponding digit of the new number a 1.
ii. If the highlighted digit of the ith number is not a 0, then make the corresponding digit of the new number a 0.

Example:
0.10010001010...

In this way, this new number differs from every item in the list in at least one digit!

Theorem. The set of real numbers in the interval $[0,1)$ is not countable.

Proof outline: We will prove this by contradiction. Suppose that the set $[0,1)$ is countable, so that the real numbers in $[0,1)$ can be listed. Show that any list isn't complete. Namely, algorithmically produce an element of $[0,1)$ that isn't on any fixed list.

Proof. For $x \in [0,1)$, denote the ith digit of x by $x[i]$. Note that for $x, y \in [0,1)$, we have $x = y$ if and only if $x[i] = y[i]$ for all $i \in \mathbb{Z}_{>0}$.

Now, suppose $f : \mathbb{Z}_{>0} \to [0,1)$ is a bijection. Define $x_f \in [0,1)$ so that the ith digit of x_f is

$$x_f[i] = \begin{cases} 1 & \text{if } f(i)[i] = 0, \\ 0 & \text{if } f(i)[i] = 1. \end{cases}$$

Then, for all $i \in \mathbb{Z}_{>0}$, we have $f(i)[i] \neq x_f[i]$, so that $f(i) \neq x_f$. Therefore $x_f \notin f(\mathbb{Z}_{>0}$, so that f is not surjective. This contradicts f being bijective, so no such bijection exists. Therefore $[0,1)$ is not countable. □

Theorem. The set of real numbers in the interval $[0,1)$ is not countable.

Proof outline: We will prove this by contradiction. Suppose that the set $[0,1)$ is countable, so that the real numbers in $[0,1)$ can be listed. Show that any list isn't complete. Namely, algorithmically produce an element of $[0,1)$ that isn't on any fixed list.

Proof. For $x \in [0,1)$, denote the ith digit of x by $x[i]$. Note that for $x, y \in [0,1)$, we have $x = y$ if and only if $x[i] = y[i]$ for all $i \in \mathbb{Z}_{>0}$.

Now, ~~suppose $f : \mathbb{Z}_{>0} \to [0,1)$ is a bijection~~ let $f : \mathbb{Z}_{>0} \to [0,1)$. Define $x_f \in [0,1)$ so that the ith digit of x_f is

$$x_f[i] = \begin{cases} 1 & \text{if } f(i)[i] = 0, \\ 0 & \text{if } f(i)[i] = 1. \end{cases}$$

Then, for all $i \in \mathbb{Z}_{>0}$, we have $f(i)[i] \neq x_f[i]$, so that $f(i) \neq x_f$. Therefore $x_f \notin f(\mathbb{Z}_{>0}$, so that f is not surjective. ~~This contradicts f being bijective, so no such bijection exists.~~ Thus, since no function $f : \mathbb{Z}_{>0} \to [0,1)$ can be surjective, no bijection between $\mathbb{Z}_{>0}$ and $[0,1)$ exists. Therefore $[0,1)$ is not countable. □

For sets X and Y, we say $|X| \leqslant |Y|$ if there exists an injective function $f : X \to Y$. And write $|X| < |Y|$ if $|X| \leqslant |Y|$ and $|X| \neq |Y|$.

Recall, the power set of as set A is the set of subsets of A, given by

$$\mathcal{P}(A) = \{S \mid S \subseteq A\}.$$

Theorem. $|A| < |\mathcal{P}(A)|$.

Outline:

1. Show $|A| \leqslant |\mathcal{P}(A)|$ by showing an injective map *exists* (give one example).
2. Show $|A| \neq |\mathcal{P}(A)|$ by showing that *any* map (not just the example from before) cannot be surjective.

   Hint. For any $f : A \to \mathcal{P}(A)$, show f is not surjective; i.e. construct a set $S \subseteq A$ such that $S \neq f(a)$ for all $a \in A$.

(Need for care: 1 is a "there exists" statement; 2 is a "for all" statement.)

Relations

A binary relation on a set A is a subset $R \subseteq A \times A$, where elements (a, b) are written as $a \sim b$.

Example: $A = \mathbb{Z}$ and $R = \{a \sim b \mid a < b\}$.
In words:

Let $\sim$ be the relation on $\mathbb{Z}$ given by $a \sim b$ if $a < b$.

(Note that we use language like in definitions, where "if" actually means "if and only if".)

Example: $A = \mathbb{R}$ and $R = \{a \sim b \mid a = b\}$.
In words:

Let $\sim$ be the relation on $\mathbb{R}$ given by $a \sim b$ if $a = b$.

Example: $A = \mathbb{Z}$ and $R = \{a \sim b \mid a \equiv b \pmod 3\}$.
In words:

Let $\sim$ be the relation on $\mathbb{Z}$ given by $a \sim b$ if $a \equiv b \pmod 3$.

More examples of (binary) relations:

1. For A a number system, let $a \sim b$ if $a = b$. R, S, T
2. For A a number system, let $a \sim b$ if $a < b$. not R, not S, T
3. For $A = \mathbb{R}$, let $a \sim b$ if $ab = 0$. not R, S, not T
4. For A a set of people, let $a \sim b$ if a is a (full) sibling of b. not R, S, T
5. For A a set of people, let $a \sim b$ if a and b speak a common language. R, S, not T

A binary relation on a set A is...

(R) reflexive if $a \sim a$ for all $a \in A$;

(S) symmetric if $a \sim b$ implies $b \sim a$;

(T) transitive if $a \sim b$ and $b \sim c$ implies $a \sim c$, i.e.

$$(a \sim b \wedge b \sim c) \Rightarrow a \sim c$$

An equivalence relation on a set A is a binary relation that is reflexive, symmetric, *and* transitive. (Only #1)

Fix $n \in \mathbb{Z}_{>0}$ and define the relation on $\mathbb{Z}$ given by

$$\text{“}a \sim b \quad \text{if } a \equiv b \pmod{n}.\text{”}$$

Is $\sim$ is an equivalence relation?

Check: we have $a \equiv b \pmod{n}$ if and only if $a - b = kn$ for some $k \in \mathbb{Z}$.

reflexivity: $a - a = 0 = 0 \cdot n$ ✓

symmetry: If $a - b = kn$, then $b - a = -kn = (-k)n$. ✓

transitivity: If $a - b = kn$ and $b - c = \ell n$, then

$$a - c = (a - b) + (b - c) = kn + \ell n = (k + \ell)n. ✓$$

Yes! This is an equivalence relation!

Let A be a set. Consider the relation on $\mathcal{P}(A)$ by

$$S \sim T \qquad \text{if} \qquad S \subseteq T$$

Is $\sim$ is an equivalence relation?

Check: This is reflexive and transitive, but not symmetric.
So no, it is not an equivalence relation.

Is

$$S \sim T \qquad \text{if} \qquad S \subseteq T \text{ or } S \subseteq T$$

an equivalence relation on $\mathcal{P}(A)$?

Check: This is reflexive and symmetric, but not transitive.
So still no, it is not an equivalence relation.

Is

$$S \sim T \qquad \text{if} \qquad |S| = |T|$$

an equivalence relation on $\mathcal{P}(A)$?

Read: Why reflexivity doesn't follow from symmetry and transitivity.

Let $\sim$ be an equivalence relation on a set A, and let $a \in A$. The set of all elements $b \in A$ such that $a \sim b$ is called the equivalence class of a, denoted by $[a]$.

Example: Consider the equivalence relation on $A = \{a, b, c\}$ given by

$$a \sim a, \quad b \sim b, \quad c \sim c, \quad a \sim c, \quad \text{and} \quad c \sim a.$$

Then

$$[a] = \{a, c\} = [c], \quad \text{and}$$
$$[b] = \{b\}$$

are the two equivalence classes in A (with respect to this relation).

(We say there are two, *not three*, since "the equivalence classes" refers to the sets themselves, not to the elements that generate them.)

Let $\sim$ be an equivalence relation on a set A, and let $a \in A$. The set of all elements $b \in A$ such that $a \sim b$ is called the equivalence class of a, denoted by $[a]$.

Example: We showed that

$$\text{“}a \sim b \quad \text{if } a \equiv b \pmod 5\text{”}$$

is an equivalence relation on $\mathbb{Z}$. Then

$$[0] = \{5n \mid n \in \mathbb{Z}\} = 5\mathbb{Z} \qquad [1] = \{5n+1 \mid n \in \mathbb{Z}\} = 5\mathbb{Z}+1$$

$$[2] = \{5n+2 \mid n \in \mathbb{Z}\} = 5\mathbb{Z}+2 \qquad [3] = \{5n+3 \mid n \in \mathbb{Z}\} = 5\mathbb{Z}+3$$

$$[4] = \{5n+4 \mid n \in \mathbb{Z}\} = 5\mathbb{Z}+4$$

$$[5] = \{5n+5 \mid n \in \mathbb{Z}\} = \{5m \mid m \in \mathbb{Z}\} = [0] = [-5] = [10] = \cdots$$

$$[6] = \{5n+6 \mid n \in \mathbb{Z}\} = \{5m+1 \mid m \in \mathbb{Z}\} = [1] = [-4] = [11] = \cdots$$

$$\vdots$$

In general, if $x \in [y]$, that means $y \sim x$.
So $x \sim y$. So $y \in [x]$.
Claim: $x \in [y]$ if and only if $[x] = [y]$.

We call any element a of a class C representative of C (since we can write $C = [a]$ for any $a \in C$).

Theorem. The equivalence classes of A partition A into subsets, meaning

1. the equivalence classes are subsets of A:
$$[a] \subseteq A \text{ for all } a \in A;$$
2. any two equivalence classes are either equal or disjoint:
for all $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \varnothing$; and
3. the union of all the equivalence classes is all of A:
$$A = \bigcup_{a \in A} [a].$$

We say that A is the disjoint union of equivalency classes, written

$$A = \bigsqcup_{a \in A} [a], \qquad \text{LaTeX: \textbackslash bigsqcup, \textbackslash sqcup}$$

For example, in our last example, there are exactly 5 equivalence classes: $[0]$, $[1]$, $[2]$, $[3]$, and $[4]$. Any other seemingly different class is actually one of these (for example, $[5] = [0]$). And

$$[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}.$$

So $\boxed{\mathbb{Z} = [0] \sqcup [1] \sqcup [2] \sqcup [3] \sqcup [4]}$.