# Math 127: Functions

Mary Radcliffe

## 1 Basics

We begin this discussion of functions with the basic definitions needed to talk about functions.

**Definition 1.** Let $X$ and $Y$ be sets. A *function* $f$ from $X$ to $Y$ is an object that, for each element $x \in X$, assigns an element $y \in Y$. We use the notation $f : X \to Y$ to denote a function as described. We write $f(x) = y$ or $f : x \mapsto y$ to denote that the element in $Y$ assigned to $x$ is $y$. We call $X$ the *domain* of $f$, and we call $Y$ the *codomain* of $f$. If $f(x) = y$, we say that $x$ *maps to* $y$ *under* $f$.

In general, we will often talk about functions from this perspective of "mapping;" we see the role of a function as taking things from $X$, and sending them over to $Y$, where the function $f$ is the map that explains where each element in $X$ is supposed to go. This is visualized in Figure 1.

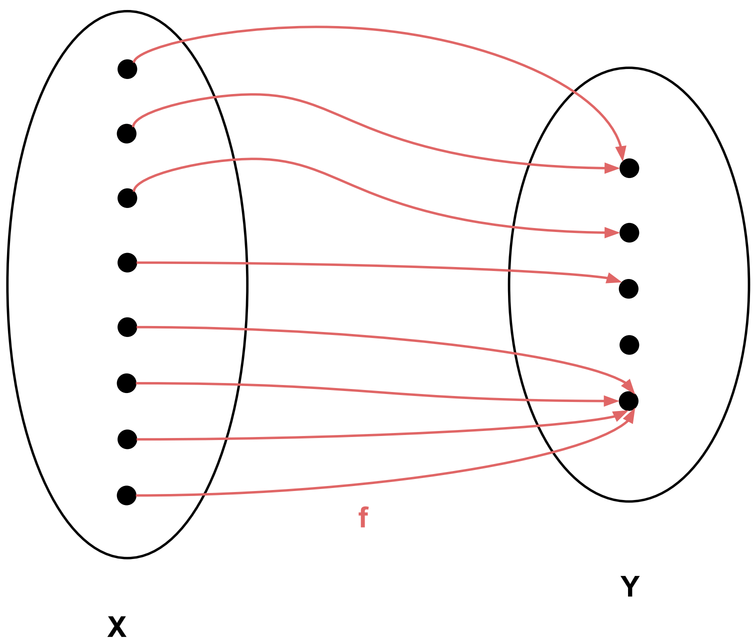



Figure 1: Imagine that the assignment of elements of $Y$ being done by the function $f$ is represented by the red arrows here, so that if $x \in X$ is assigned $y \in Y$, we have a red arrow from $x$ to $y$. Notice that it is permitted to have more than one element in $X$ map to the same $y \in Y$, and it is also permitted to have elements in $y$ that are not mapped to by any $x \in X$.

Let's think about this notion with a function we probably feel a little more comfortable with. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 2n$, as shown in Figure 2. Practically, what this function is asking us to do is map elements in $\mathbb{Z}$ over to new elements in $\mathbb{Z}$, where the directions on the map, described by the function, are to multiply something by 2. So if you ask the function "what do I do with the number

3?" the function will answer "Send it over to 6." In this way, the function provides us with a mechanism to transform the number 3 according to some rule, which is the definition of the function.

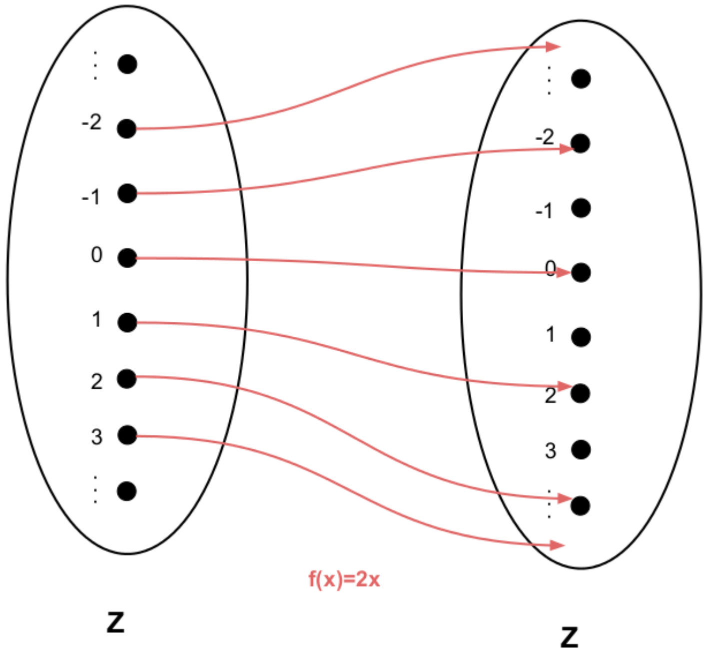



Figure 2: A representation of the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 2n$.

Now, in order for this map to make sense, there are a few basic properties that we need to ensure are satisfied. In particular, we want to make sure that every element of $X$ can be mapped to somewhere, and that the "somewhere" is appropriate. Together these properties constitute what is known as well-definedness.

**Definition 2.** An assignment of values $y$ to elements $x \in X$ is said to be a *well-defined* function $f : X \to Y$ if it satisfies the following three properties:

- Totality: For every $x \in X$, there exists $y$ such that $f(x) = y$.
- Existence: For every $x \in X$, $f(x) \in Y$.
- Uniqueness: For every $x \in X$, there is only one $y \in Y$ such that $f(x) = y$.

While these properties are trivially true in the definition of a function, it's useful to think about the failure cases to think about what kinds of assignments we might make that are in fact NOT functions. In general, if you are to define a function yourself, it's worth thinking about these things to ensure that the function you are creating is a well-defined function.

**Example 1.** Define $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = \frac{1}{x-1}$. This is NOT a well-defined function, because $g(1)$ is not an element of $\mathbb{R}$. There is no $y$ such that $g(1) = y$, and hence this function fails the totality property.

**Example 2.** Define $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = n - 1$. This is NOT a well-defined function, because $f(1) = 0$ is not an element of $\mathbb{N}$. This assignment of values fails the existence property.

**Example 3.** Define $f:(0,1)\to\{0,1,2,\ldots,9\}$ (where $(0,1)=\{x\in\mathbb{R}\mid 0<x<1\}$) by $f(x)=d$, where $d$ is the first digit after the decimal point in the base-10 expansion for $x$. This is NOT a well-defined function, because some numbers have more than one possible base-10 expansion. Indeed[a], $0.5=0.4999999\ldots$, and hence we have more than one $y\in\{0,1,\ldots,9\}$ with $f(\frac{1}{2})=y$. This assignment of values fails the uniqueness property.

[a]Just to be sure, let's prove that $0.9999\cdots=1$, which in turn clearly implies that $0.4999\cdots=0.5$. First, let $a=0.9999\ldots$, which is some real number. Then $10a=9.9999\ldots$, and hence $9a=10a-a=9.9999\cdots-0.9999\cdots=9$. Since $9a=9$, we therefore have that $a=1$. Thus, $1=a=0.99999$. QED.

When you are defining a function, be on the lookout for these kinds of problems. Some things to think about:

- If you were handed a value of $x\in X$, would you always know what to do with it?
- If you're using a formula: can EVERY value of $x\in X$ be plugged in to your formula? If not, what are you doing with the other values?
- Can the formula ever give you numbers that live outside your codomain?
- Is there more than one way to represent elements in the domain? If so, do those representations give the same output under this function?

As with several of our previous topics, we have some special functions that will show up from time to time, and will be quite useful.

**Definition 3.** The *identity function* on a set $X$, denoted by $\iota_X$, is the function $\iota_X:X\to X$ such that $\forall x\in X,\ f(x)=x$.

The *empty function* is any function $f:\emptyset\to X$. Note that there is no need, in the empty function, to define any values for elements in the domain, as there are none!

Finally, we have to address the question of what it means for two functions to be the same.

**Definition 4.** Let $X,Y,A,B$ be sets, and let $f:X\to Y$ and $g:A\to B$ be functions. We say that $f$ is identically equal to $g$, denoted by $f\equiv g$, if the following conditions are met:

- $X=A$
- $Y=B$
- $\forall x\in X,\ f(x)=g(x)$.

There is a reason for distinguishing equality of functions with $\equiv$ rather than $=$. There are often times, for example, when it is important to find a specific choice of $x\in X$ for which $f(x)=g(x)$. However, this is quite different from $f(x)=g(x)$ for every single $x\in X$.

Moreover, we can have functions that are the same on all their common domain elements (that is, $f(x)=g(x)\ \forall x\in X\cap A$), but are not identically equal because perhaps they have different domains. An example might be as follows: define $f:\mathbb{N}\to\mathbb{N}$ by $f(x)=3x$, and for $A$ the set of even integers, define $g:A\to\mathbb{Z}$ by $g(a)=3a$. Then on any $x$ that is both a natural number and an even integer, $f$ and $g$ produce the same value. However, we cannot say that these are really the same function, because there are numbers that $f$ can map and $g$ cannot, and vice versa. Similar qualifications, of course, apply to the codomain.

For these reasons, we distinguish between identical equality of functions and equality on elements. This is similar to the use of $\equiv$ in the world of propositional logic: we use the symbol $\equiv$ to mean that the two objects are the same, all the time, regardless of how we set the corresponding parameters.

## 1.1 Functions and Subsets

We have, already, some language and notation to discuss things like the domain or codomain of a function. However, what if we wish to consider subsets of the domain or codomain? We need to develop concepts to deal with these structures.

**Definition 5.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. Given a set $U \subseteq X$, we define the *image* of $U$ in $Y$, denoted $f(U)$, to be the subset of $Y$ given by

$$f(U) = \{y \in Y \mid \exists x \in U \text{ with } f(x) = y\}.$$

If $U = X$, the image of $U$ in $Y$ is also called the *range* of $f$.

This is to say, if we are interested in a subset $U$ of $X$, we might want to ask ourselves: what values in $Y$ are assigned to elements in this subset? This is precisely what the image of $U$ is getting at.

**Example 4.** Define $f : \mathbb{Z} \to \mathbb{N}$ by $f(x) = |x| + 1$. To illustrate the concept of image, let's consider a few subsets of $\mathbb{Z}$ here.

- If $U = \{0, 1, 2\}$, then the image of $U$ is whatever function values are assigned to these 3 numbers. As
$$f(0) = 1, \quad f(1) = 2, \quad f(2) = 3,$$
we have that $f(U) = \{1, 2, 3\}$.

  Notice that as $U$ has 3 elements in it, we cannot have more than 3 elements in $f(U)$, due to the uniqueness property of well-defined functions.

- If $U = \{-2, -1, 0, 1, 2\}$, then the image of $U$ is whatever function values are assigned to these five numbers. Since
$$f(-2) = 3, \quad f(-1) = 2, \quad f(0) = 1, \quad f(1) = 2, \quad f(2) = 3,$$
we have that $f(U) = \{1, 2, 3\}$.

  Notice that despite the fact that $U$ has 5 elements in it, we still only have 3 elements in $f(U)$. This is due to the fact that some elements of $f(U)$ are assigned to more than one member of $U$.

- If we wish to consider the range of $f$, we think about $U = \mathbb{Z}$. In this case, we have that every element of $\mathbb{N}$ is a member of the range; if $n \in \mathbb{N}$, then by taking $z = n - 1$, we have $f(z) = n$. Hence, for every $n \in \mathbb{N}$, $\exists z \in \mathbb{Z}$ such that $f(z) = n$, so every $n \in \mathbb{N}$ is a member of the range of $f$.

- If $U = \{0\}$, then the image of $U$ is just $f(U) = \{1\}$. In general, this is true: for any function $f : X \to Y$, we have that $f(\{x\}) = \{f(x)\}$ for any $x \in X$; that is, the image of the set containing only one element $x$ is the set containing only one element, $f(x)$.

In the case of the function shown in Example 4, we have that the range of the function $f$ is precisely the same as the codomain of $f$. This is because for this function, every element in the codomain is the image of some element in the domain. Of course, this is not true for all functions; if we take $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(z) = 2z$, we clearly have that the codomain is all of $\mathbb{Z}$, but the range is just the even integers.

Of course, we may be interested in more than just what the function values are on a subset of $X$. Indeed, there are circumstances where we might wish only to consider a subset of $X$, and throw away superfluous elements. In that case, we can define a function on a subset of $X$ as follows.

**Definition 6.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. Given a set $U \subseteq X$, the *restriction of $f$ to $U$*, denoted as $f|_U$, is the function $f|_U : U \to Y$ defined by $f|_U(x) = f(x)$ for all $x \in U$.

The restriction of $f$ to a subset will occasionally appear as a useful tool.

Now, for the other side of the coin, suppose we have a subset of $Y$, and wish to think about what elements in $X$ might map to that subset. In that case, we can define a similar type of object to the image, called the preimage.

**Definition 7.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. Given a subset $V \subseteq Y$, we define the *preimage* of $V$ under $f$, denoted by $f^{-1}(V)$, to be the subset of $X$ given by

$$f^{-1}(V) = \{x \in X \mid f(x) \in V\}.$$

This is to say, the preimage of $V$ is the set of all elements in $X$ whose image is a member of $V$. To ensure we understand the concept, let's consider an example.

**Example 5.** Let $f : \mathbb{Z} \to \mathbb{Z}$ with $f(z) = |2z|$ for all $z \in \mathbb{Z}$. Let's consider the preimage of a few sets $V$.

- If $V = \{2\}$, then the preimage of $V$ is all those elements in $\mathbb{Z}$ that map to 2; that is, it is all choices of $z$ for which $f(z) = |2z| = 2$. There are two such elements, namely $\pm 1$. Hence $f^{-1}(V) = \{-1, 1\}$.
- If $V = \{1\}$, then the preimage of $V$ is all those elements in $\mathbb{Z}$ that map to 1; that is, it is all choices of $z$ for which $f(z) = |2z| = 1$. There are no such elements! Hence, $f^{-1}(V) = \emptyset$.
- If $V = \{0\}$, then the preimage of $V$ is all those elements of $\mathbb{Z}$ that map to 0, which is clearly just $z = 0$. Hence $f^{-1}(V) = \{0\}$.
- If $V = \{0, 1, 2, 3, 4\}$, then by repeating above ideas, we have that the elements in $\mathbb{Z}$ for which $f(z) \in V$ are exactly $f^{-1}(V) = \{-2, -1, 0, 1, 2\}$.
- If we take $V = \{x \in \mathbb{Z} \mid x \geq 0 \text{ and } x \text{ is even}\}$, then every element of $\mathbb{Z}$ has its image in $V$. Hence, we have $f^{-1}(V) = \mathbb{Z}$.

Unlike with the image, as we see above the number of elements in the preimage of a set $V$ is not necessarily tied to the number of elements in $V$. We can have empty preimages, which we cannot have with images, and we can have many elements that map to the same $y \in V$ contribute to the preimage.

In general, the preimage and image play well with unions and intersections of sets.

**Proposition 1.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function.

1. If $U_1, U_2 \subseteq X$, then $f(U_1 \cup U_2) = f(U_1) \cup f(U_2)$.
2. If $U_1, U_2 \subseteq X$, then $f(U_1 \cap U_2) \subseteq f(U_1) \cap f(U_2)$.
3. If $V_1, V_2 \subseteq Y$, then $f^{-1}(V_1 \cup V_2) = f^{-1}(V_1) \cup f^{-1}(V_2)$.
4. If $V_1, V_2 \subseteq Y$, then $f^{-1}(V_1 \cap V_2) = f^{-1}(V_1) \cap f^{-1}(V_2)$.

We shall not prove all these properties here; those that we do not prove will be left as an exercise. In particular, we shall prove items 2 and 3.

**Proof.** [Partial Proof.] Let $X, Y, f$ be as in the statement of Proposition 1.

2. Let $U_1, U_2 \subseteq X$. Suppose that $y \in f(U_1 \cap U_2)$. Then by definition, there exists $x \in U_1 \cap U_2$ having $f(x) = y$. Since $x \in U_1 \cap U_2$, we thus have that $x \in U_1$ and $x \in U_2$, so $y \in f(U_1)$ and $y \in f(U_2)$. But then $y \in f(U_1) \cap f(U_2)$, and thus $f(U_1 \cap U_2) \subseteq f(U_1) \cap f(U_2)$.

3. We prove the set equality by double containment.

   First, suppose that $x \in f^{-1}(V_1 \cup V_2)$. Then by definition, $f(x) \in V_1 \cup V_2$, so either $f(x) \in V_1$ or $f(x) \in V_2$. Wolog, suppose that $f(x) \in V_1$. Then we have $x \in f^{-1}(V_1)$, and hence $x \in f^{-1}(V_1) \cup f^{-1}(V_2)$.

   For the other direction, suppose that $x \in f^{-1}(V_1) \cup f^{-1}(V_2)$. Then we have $x \in f^{-1}(V_1)$ or $x \in f^{-1}(V_2)$; wolog suppose that $x \in f^{-1}(V_1)$. Then by definition, we have $f(x) \in V_1$, and thus $f(x) \in V_1 \cup V_2$. But then $x \in f^{-1}(V_1 \cup V_2)$.

   Therefore, we have that $f^{-1}(V_1 \cup V_2) = f^{-1}(V_1) \cup f^{-1}(V_2)$ by double containment.

□

In addition, we have similar properties for set complements.

**Proposition 2.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function.

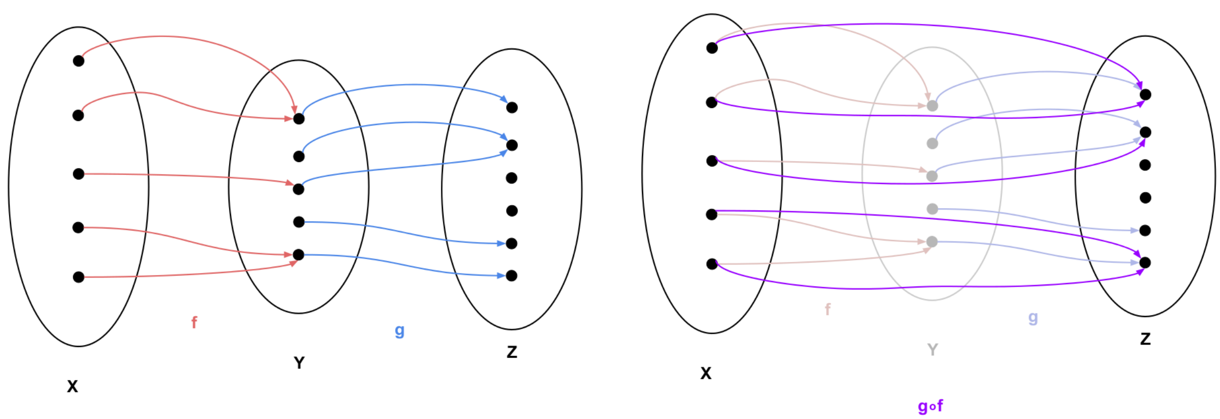
1. If $U \subseteq X$, then $f(X \backslash U) \supseteq f(X) \backslash f(U)$.
2. If $V \subseteq Y$, then $f^{-1}(Y \backslash V) = X \backslash f^{-1}(V)$

The proofs of these properties are left as an exercise.

## 1.2 Composition

**Definition 8.** Let $X, Y, Z$ be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions. We define the composition $g \circ f : X \to Z$ to be the function defined by $g \circ f(x) = g(f(x))$.

We can imagine a composition as follows. The function $f$ gives us a rule for how to map the set $X$ into the set $Y$, and the function $g$ gives us a rule for how to map the set $Y$ into the set $Z$. By chaining these rules together, first by doing the $f$ rule, then the $g$ rule, we can get from $X$ all the way to $Z$. This new function can disregard the set $Y$ completely, as shown in Figure 3. The notation for function composition is set up so that the first function you perform is closest to the $x$; $g \circ f$ indicates that $f$ has to be performed first, because when you put $x$ next to the function, $f$ is closest to it.




(a) (b)

Figure 3: To construct a composition of functions $f$ and $g$, we can imagine that we have two mappings, as shown in (a). To get the composite $g \circ f$, we start from $X$, and then follow both the red and blue arrows to get to $Z$, resulting in the purple arrows shown in (b). Once we have these purple arrows established, we can then disregard $Y$ and the original functions $f$ and $g$, and treat $g \circ f$ as its own function from $X$ to $Z$.

To ensure that we understand this, let's take a look at an example.

**Example 6.** Define $f : \mathbb{N} \to \mathbb{Z}$ by $f(x) = 2x$, and define $g : \mathbb{Z} \to \mathbb{Q}$ by $g(x) = \frac{x}{12}$. The composition $g \circ f$ is a function from $\mathbb{N}$ to $\mathbb{Q}$, that looks as follows: $g \circ f(x) = g(f(x)) = g(2x) = \frac{2x}{12} = \frac{x}{6}$. Once we have this expression of $g \circ f$, we can simply treat it as a function from $\mathbb{N}$ to $\mathbb{Q}$, ignoring anything that happened in the middle.

The composition of functions operates in a way like a type of multiplication for functions. Indeed, it does satisfy some of the types of properties we like for multiplication. One such property that we shall frequently use is the following:

If $f : X \to Y$ is a function, then $f \equiv f \circ \iota_X \equiv \iota_Y \circ f$.

That is, composing a function with an identity doesn't change anything. This will show up as a useful tool in various proofs; the proof of this property itself is left as a (trivial) exercise.

Moreover, function composition is associative:

**Theorem 1.** *Let $W, X, Y, Z$ be sets, and let $f : W \to X$, $g : X \to Y$, and $h : Y \to Z$ be functions. Then $h \circ (g \circ f) \equiv (h \circ g) \circ f$.*

Before we prove this theorem, let's note the important caveat here about associativity. The theorem states that we can associate composition of functions, under the condition that the function composition makes sense. That is to say, we can perform this associativity, given that the sets involved allow function composition to take place, namely that the domain of each function is equal to the codomain of the preceding function.

**Proof.** [Proof of Theorem 1] To prove this theorem, we wish to show that $\forall w \in W$, we have that $h \circ (g \circ f)(w) = (h \circ g) \circ f(w)$.

Choose an arbitrary $w \in W$. Define the following variables:

- $x = f(w)$, so $x \in X$.
- $y = g(x)$, so $y \in Y$.
- $z = h(y)$, so $z \in Z$.

Note that by definition of composition, we have $g \circ f(w) = g(f(w)) = g(x) = y$. Then we have

$$\begin{aligned} h \circ (g \circ f)(w) &= h(g \circ f(w)) \quad \text{(by definition of composition)} \\ &= h(y) \quad \text{(by the above calculation)} \\ &= z. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} (h \circ g) \circ f(w) &= (h \circ g)(f(w)) \quad \text{(by definition of composition)} \\ &= h \circ g(x) \\ &= h(g(x)) \\ &= h(y) = z. \end{aligned}$$

Therefore, we have $h \circ (g \circ f)(w) = z = (h \circ g) \circ f(w)$. As $w$ is chosen arbitrarily from $W$, this equation is true $\forall w \in W$. Therefore, $h \circ (g \circ f) \equiv (h \circ g) \circ f$. $\square$

However, there are other types of multiplication properties that we do not see in the world of function composition. In particular, we do not get commutativity for function composition.

**Example 7.** Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = 2x$, and let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(x) = x^2$. Then we have, for any $x \in \mathbb{Z}$,

$$g \circ f(x) = g(f(x)) = g(2x) = (2x)^2 = 4x^2,$$

but on the other hand,

$$f \circ g(x) = f(g(x)) = f(x^2) = 2x^2.$$

Hence, $g \circ f \not\equiv f \circ g$.

Indeed, things can be substantially worse than this; we may not be able to switch the order at all. Consider:

**Example 8.** Let $f : \mathbb{N} \to \mathbb{R}$ be defined by $f(x) = \sqrt{x}$, and let $g : \mathbb{R} \to \mathbb{Z}$ be defined by $g(x) = \lfloor x \rfloor - 10$. Then $g \circ f$ is defined as $g(f(x)) = \lfloor \sqrt{x} \rfloor - 10$, an integer. However, we cannot consider $f \circ g$, since the codomain of $g$ is not equal to the domain of $f$. Indeed, if we take $x = 0$, then $g(x) = -10$, and we are unable to compute $f(g(x))$ since $f$ is only defined on positive integers.

# 2 Injectivity and Surjectivity

There are two important properties of functions that appear throughout mathematics, and we will pause a moment to consider them here.

## 2.1 Injectivity

**Definition 9.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. We say that $f$ is *injective* (sometimes called one-to-one) if $\forall x_1, x_2 \in X$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

This definition of injectivity is also often phrased in the contrapositive form: a function $f : X \to Y$ is injective if $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$. The idea here is that if we start from two different elements in the domain, we should land at two different elements in the domain. So the example shown in Figure 1, our first example of a function, is not injective. We can see this because the top two elements of $X$ both have the same image in $Y$. If we draw out a mapping for an injective function, it should be the case that every element in $Y$ has at most one arrow, as seen in Figure 4.

To demonstrate that a function is injective, one of two proof strategies is usually employed. First, one can suppose that $f(x_1) = f(x_2)$, and derive that $x_1 = x_2$; this is a direct proof following the definition of injectivity above. The other proof technique is to use a contradiction: suppose that $f(x_1) = f(x_2)$, but $x_1 \neq x_2$, and derive a contradiction. Let's take a look at some examples.

**Example 9.** Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$ is injective.

**Solution.** Suppose that $x_1, x_2 \in \mathbb{R}$, and that $f(x_1) = f(x_2)$. Then by definition of $f$, we have $2x_1 + 1 = 2x_2 + 1$, and thus $2x_1 = 2x_2$, and thus $x_1 = x_2$. Therefore $f$ is injective by definition.

This proof technique might remind you of showing that something is unique: first, you suppose there are two of it, and then show that those two must actually be the same. This is effectively the idea with injectivity: for each $y \in Y$, if there is an $x$ such that $f(x) = y$, then there is only one such $x$.

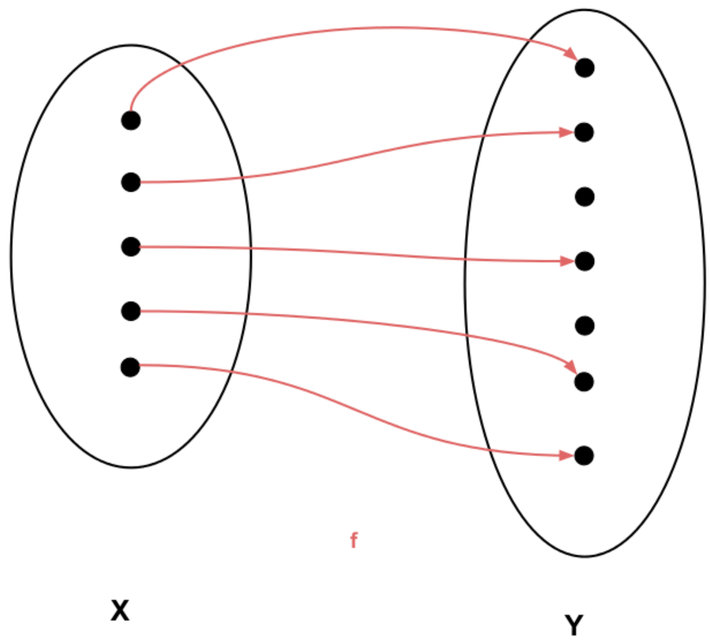



Figure 4: A basic picture of an injective function. Every element in the domain $X$ maps to a different element in the codomain $Y$; every element of the codomain $Y$ has at most one element of $X$ that maps to it.

**Example 10.** Let $n \in \mathbb{N}$. Show that the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^n - x$ is not injective.

**Solution.** Notice that when $x = 0$, we obtain $g(x) = 0^n - 0 = 0$, and when $x = 1$, we have $g(x) = 1^n - 1 = 0$. Therefore, as $g(0) = g(1)$, and $0 \neq 1$, we have that $g$ is not injective.

In general, when considering proving if a function is injective or not, the following procedures can be employed:

**To prove a function $f : X \to Y$ is injective:**

- Let $x_1, x_2 \in X$ be such that $f(x_1) = f(x_2)$.
- Follow any proof technique to conclude that $x_1 = x_2$.
- Conclude that $f$ is injective.

**To prove a function $f : X \to Y$ is NOT injective:**

- Find a specific choice of $x_1, x_2 \in X$, such that $x_1 \neq x_2$, and $f(x_1) = f(x_2)$.
- Conclude that $f$ is not injective.

Let's consider how injectivity plays with function composition.

**Theorem 2.** *Let $X, Y, Z$ be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions. If $g$ and $f$ are both injective, then $g \circ f$ is injective.*

Before we formally prove this theorem, let's think about what it is saying, and why the converse is false. If both $f$ and $g$ are injective, then when we start from two elements in $X$, we map, via $f$, to distinct elements in $Y$. Then these in turn map, via $g$, to distinct elements in $Z$. Since each stage of the mapping yields distinct elements, the images of the two original points in $X$ must be distinct.

On the other hand, we don't necessarily have the converse. Imagine that $g \circ f$ is injective. This means that if we pick two elements in $X$, they map to distinct elements in $Z$ under the composition $g \circ f$. But if the function $f$ misses a lot of elements in $Y$, then we could have that $g$ isn't injective, just that it maps to distinct elements on the image of $f$. Consider the following example:

**Example 11.** Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = 2x$, and let $g : \mathbb{N} \to \mathbb{N}$ be defined by $g(x) = \left\lceil \frac{x}{2} \right\rceil$. This is illustrated in Figure 5. Notice that $g$ is not injective, since $g(1) = \left\lceil \frac{1}{2} \right\rceil = 1 = \left\lceil \frac{2}{2} \right\rceil = g(2)$. However, if we consider the composition $g \circ f$, we have $g \circ f(x) = g(2x) = \left\lceil \frac{2x}{2} \right\rceil = x$, which is certainly injective. Thus, even though $g \circ f$ is injective, we do not have to have that $g$ and $f$ are both injective.

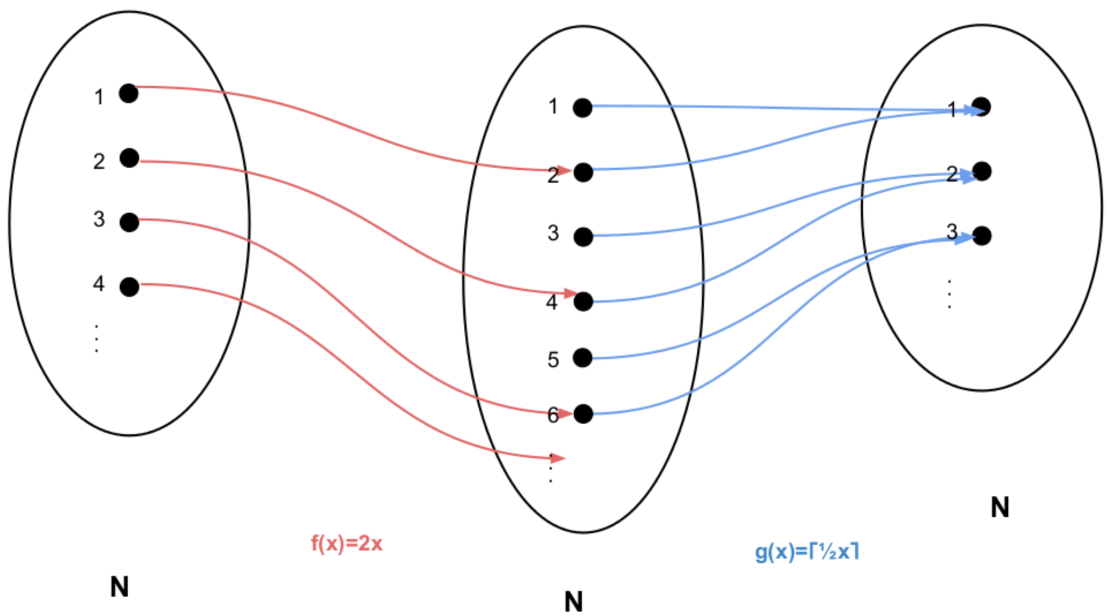



Figure 5: The functions $f$ and $g$ as defined in Example 11. We can see that the composition is injective, even as $g$ is not.

In general, however, we do have a partial converse, the proof of which is left as an exercise:

**Proposition 3.** Let $X, Y, Z$ be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions. If $g \circ f$ is injective, then $f$ is injective.

Now, let us prove the original theorem.

**Proof.** [Proof of Theorem 2] Let $f, g$ be as in the statement of the theorem, and suppose that both $f$ and $g$ are injective. We wish to prove that $g \circ f$ is also injective.

Let $x_1, x_2 \in X$, having $g \circ f(x_1) = g \circ f(x_2)$. By definition, then $g(f(x_1)) = g(f(x_2))$. Since $g$ is injective, this implies that $f(x_1) = f(x_2)$. Since $f$ is injective, this implies that $x_1 = x_2$. Therefore, by definition, $g \circ f$ is injective. $\square$

## 2.2 Surjectivity

**Definition 10.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. We say that $f$ is *surjective* if $\forall y \in Y$, $\exists x \in X$ such that $f(x) = y$.

For surjectivity, we want a function to have its range actually equal to its codomain. That is to say, every element in the codomain is mapped to by some element in the domain. Pictorially, we can imagine this as saying that when we draw the function, every element in $Y$ gets at least one arrow pointed at it. So, for example, if you look at Figure 5, the function $g : \mathbb{N} \to \mathbb{N}$ with $g(x) = \left\lceil \frac{x}{2} \right\rceil$ is surjective, since every element of the codomain has a blue arrowhead, but the function $f : \mathbb{N} \to \mathbb{N}$ with $f(x) = 2x$ is not surjective, since there are some elements of $\mathbb{N}$ in the center that do not have a red arrowhead.

A proof that a function is surjective is effectively an existence proof; given an arbitrary element of the codomain, we need only demonstrate the existence of one element in the domain that maps to it. Let's see an example.

**Example 12.** Define $\mathbb{Q}^+$ to be the set of positive rational numbers. Given $q \in \mathbb{Q}^+$, define $a_q = \min\{m \in \mathbb{N} \mid \exists n \in \mathbb{N} \text{ with } nq = m\}$. Note that this function is well defined, since if $q \in \mathbb{Q}^+$ there exist positive integers $a, b$ having $q = \frac{a}{b}$, so $bq \in \mathbb{N}$ and thus $\{m \in \mathbb{N} \mid \exists n \in \mathbb{N} \text{ with } nq = m\}$ is nonempty[a]. Let $f : \mathbb{Q}^+ \to \mathbb{Z}$ be defined by $f(q) = a_q$. Prove that $f$ is surjective.

**Proof.** Given $a \in \mathbb{N}$, we need only demonstrate the existence of some $q \in \mathbb{Q}^+$ such that $f(q) = a$. Suppose $a \in \mathbb{N}$. Let $q = a$. Note, then that $1q = a$, and hence $a \in \{m \in \mathbb{N} \mid \exists n \in \mathbb{N} \text{ with } nq = m\}$, by taking $n = 1$. Moreover, if $n \geq 1$, then $na \geq a$, and hence if $b \in \{m \in \mathbb{N} \mid \exists n \in \mathbb{N} \text{ with } nq = m\}$, then $b \geq a$. Therefore, as $a$ is both a member of this set and is a lower bound for this set, it is the minimum of this set. Thus, $f(a) = a$.
Since every $a \in \mathbb{N}$ has some $q \in \mathbb{Q}^+$ with $f(q) = a$, we therefore have that $f$ is surjective. □

[a]Another way to think of this function is to imagine that $a_q$ is the smallest possible numerator for $q$.

Likewise, to show that something is not surjective, it suffices to show an example of a number in the codomain that is not in the range of the function.

**Example 13.** Let $f : \mathbb{Z} \to \mathbb{N}$ be defined by $f(z) = |z| + 2$. Prove that $f$ is not surjective.

**Proof.** Notice that for any $z \in \mathbb{Z}$, we have that $f(z) \geq 2$. Therefore, if $y = 1$, there is no $z \in Z$ such that $f(z) = y$. Hence, $f$ is not surjective. □

In general, when considering proving if a function is surjective or not, the following procedures can be employed:

**To prove a function $f : X \to Y$ is surjective:**

- Let $y \in Y$ be an arbitrary element of the codomain.
- Give an example of $x \in X$ having $f(x) = y$. Usually the choice of $x$ will depend on $y$ in some meaningful way.
- Conclude that $f$ is surjective.

**To prove a function $f : X \to Y$ is NOT surjective:**

- Find a specific choice of $y \in Y$ for which there is no $x \in X$ having $f(x) = y$.
- Conclude that $f$ is not surjective.

As with injectivity, we have a theorem about surjectivity and composition.

**Theorem 3.** *Let $X, Y, Z$ be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions. If $f$ and $g$ are surjective, then $g \circ f$ is also surjective.*

Let us stop to consider this result for a moment. Essentially we have this: if we have any element in $Z$, we know that if $g$ is surjective, there is some element of $Y$ that maps to it. Moreover, if $f$ is surjective, there is some element of $X$ that maps to that. So we can trace any element of $Z$ back to some element of $X$. This is the value of surjectivity; given an element in the codomain, we can trace it back to some (not necessarily unique) corresponding element in the domain.

Of course, as with Theorem 2, the converse here is false, and the example from Example 11 and shown in Figure 5 can prove it.

**Example 14.** Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(x) = 2x$, and let $g : \mathbb{N} \to \mathbb{N}$ be defined by $g(x) = \left\lceil \frac{x}{2} \right\rceil$, as defined in Example 11. This is illustrated in Figure 5. Then $g \circ f$ is surjective, but $f$ is not surjective.
Notice that $f$ is not surjective, since there is no $x \in \mathbb{N}$ having $f(x) = 1$. But as noted in Example 11, $g \circ f(x) = x$ for all $x \in \mathbb{N}$, which is clearly surjective.

As with Theorem 2, we have a partial converse, the proof of which is left as an exercise:

**Proposition 4.** Let $X, Y, Z$ be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions. If $g \circ f$ is surjective, then $g$ is surjective.

Now, let us prove Theorem 3.

**Proof.** [Proof of Theorem 3 Let $f, g$ be as in the statement of the theorem, and suppose that $f$ and $g$ are surjective.

Given $z \in Z$, there exists some $y \in Y$ such that $g(y) = z$, since $g$ is surjective. Moreover, since $f$ is surjective, there exists some $x \in X$ such that $f(x) = y$. We therefore have that $g \circ f(x) = g(f(x)) = g(y) = z$, and hence, for any $z \in Z$, there exists some $x \in X$ such that $g \circ f(x) = z$. Therefore, $g \circ f$ is surjective. $\square$

# 3 Bijectivity and Inverses

Now, let's consider the situation with injectivity and surjectivity pictorially. When we say a function is injective, what we mean is that if we look at the codomain, every element has at most one arrowhead touching it. When we say a function is surjective, what we mean is that if we look at the codomain, every element has at least one arrowhead touching it. But what happens if we have both? Well, then every element in the codomain would have at most and at least one arrowhead touching it.... that means EXACTLY one arrowhead. This is really convenient, since it gives us an obvious way to go back to the domain; just reverse every arrow! Because every element has exactly one arrowhead, this will yield a well-defined function (commonly called the inverse). Let's formalize some of these ideas.

**Definition 11.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. We say that $f$ is *bijective* if $f$ is both injective and surjective.

Another way of seeing this is that every element has exactly one preimage under $f$, as discussed above. To express that, we introduce the unique existential quantifier, hitherto unseen:

**Definition 12.** Let $p(x)$ be a proposition with range $X$. The proposition $\exists! x \in X, p(x)$ is true if $\exists x \in X, p(x)$ is true, and $\forall x_1, x_2 \in X$, $x_1 \neq x_2 \Rightarrow \neg(p(x_1) \wedge p(x_2))$. That is to say, $p(x)$ cannot be true for two different values of $x$, so there is only one choice of $x \in X$ for which $p(x)$ is true. The symbol $\exists!$ is called the *unique existential quantifier*.

**Proposition 5.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. Then $f$ is bijective if and only if $\forall y \in Y, \exists! x \in X$ such that $f(x) = y$.

The proof of this proposition is left as an exercise, but the two pieces of the unique existential quantifier appear due to the two properties we have. The fact of existence is given to us by surjectivity; the fact of uniqueness is given by injectivity. Without both, the statement falls apart.

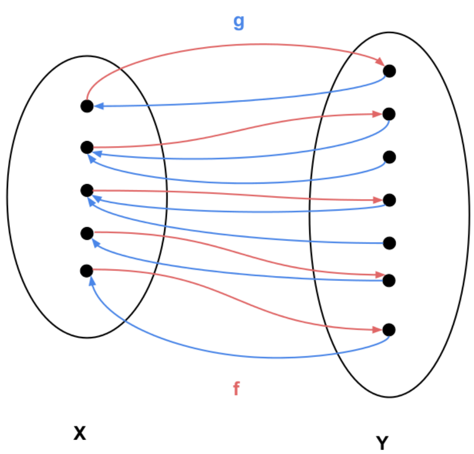
By taking Theorems 2 and 3 together, we immediately have the following theorem:

**Theorem 4.** *Let $X, Y, Z$ be sets, and let $f : X \to Y$ and $g : Y \to Z$ be functions. If $f$ and $g$ are bijective, then $g \circ f$ is bijective.*

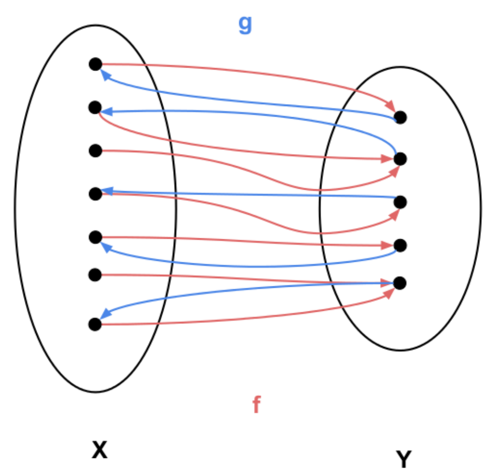
Of course, the converse is false, as the example seen in Examples 11 and 14 shows. In that case, we have that $g \circ f$ is both injective and surjective (hence bijective) even though neither $f$ nor $g$ is bijective.

Now, as we hinted at the beginning of this section, our goal is really to construct a notion of inverse; we'd like to be able to reverse the direction of our arrows. Formally speaking, given a function $f$, we would like to be able to construct a function $g$ so that when we perform $f$ and then $g$ (aka $g \circ f$), we get back to where we started.

**Definition 13.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function. A function $g : Y \to X$ is called a *left inverse* to $f$ if $g \circ f \equiv \iota_X$. A function $h : Y \to X$ is called a *right inverse* to $f$ if $f \circ h \equiv \iota_Y$. A function from $Y$ to $X$ is called a *two-sided inverse*, or sometimes just *inverse*, to $f$ if it is both a left and right inverse.




(a) Here, $g$ is a left inverse to $f$. We can imagine that if we performed the red function, and then the blue, we would end up back where we started from. This is equivalent to the composition $g \circ f$. Hence, $g \circ f \equiv \iota_X$, meeting the definition of left inverse.




(b) Here, $g$ is a right inverse to $f$. We can imagine that if we performed the blue function, and then the red, we would end up back where we started from. This is equivalent to the composition $f \circ g$. Hence, $f \circ g \equiv \iota_Y$, meeting the definition of right inverse.

Figure 6

**Example 15.** Let $f : \mathbb{N} \to \mathbb{N}$ be the function $f(x) = 3x$. Then $f$ has a left inverse.

**Proof.** We wish to find a function $g$ so that $g \circ f \equiv \iota_{\mathbb{N}}$. Since $f$ maps any $x$ to $3x$, we would like that $g$ maps any $y$ that is divisible by 3 to $\frac{y}{3}$. So we construct $g$ as follows:

$$g(y) = \begin{cases} \frac{y}{3} & \text{if } 3|y \\ 1 & \text{if } 3 \not| y \end{cases}$$

Notice, then, that for any $x \in \mathbb{N}$, we have $g \circ f(x) = g(f(x)) = g(3x) = x$, so $g \circ f \equiv \iota_{\mathbb{N}}$. Therefore, $g$ is a left inverse to $f$. □

Note that here, all we need to prove that a left inverse exists is to demonstrate it. Moreover, it's clear that this left inverse is not a right inverse: if we think about $f \circ g(4)$, we have that $g(4) = 1$, since 4 is not divisible by 3, so $f \circ g(4) = f(1) = 3 \neq 4$. Thus, $f \circ g \not\equiv \iota_{\mathbb{N}}$.

The approach for constructing a right inverse is similar; given a function $f : X \to Y$, we can construct a right inverse $g : Y \to X$ by trying to assign $g(y) = x$ in such a way that $f(x) = y$, that is, $g(y) \in f^{-1}(y)$.

The difference between a left and right inverse is illustrated in Figure 6. Notice the distinction: for a left inverse to exist, we can have extra points in $Y$ that $f$ does not interact with, so long as every point in the image of $f$ has the correct preimage. Notice also that we can't have more than one point in $X$ have the same image; if $f(x_1) = f(x_2) = y$, then how can we choose $g(y)$ to yield both $x_1$ and $x_2$? That is to say, in order that a left inverse exists, clearly we require that $f$ is an injective function.

In the same way, for the right inverse to exist, we want to be able to construct some $g$ so that $f \circ g \equiv \iota_Y$. In order that this is possible, we must have that all of $Y$ is part of the image of $f$, so that we can get to everywhere upon performing the composition. That is to say, in order that a right inverse exists, we clearly require that $f$ is a surjective function.

Both of these characterizations are biconditional, and we have the following lemma:

**Lemma 1.** *Let $X, Y$ be nonempty sets, and let $f : X \to Y$ be a function. Then*

1. *$f$ has a left inverse if and only if $f$ is injective*
2. *$f$ has a right inverse if and only if $f$ is surjective.*

**Proof.** Let $X, Y, f$ be as described. We prove the two properties separately.

1. As this is a biconditional, we consider each direction.

   For the forward direction, suppose that $f$ has a left inverse $g$. Let $x_1, x_2 \in X$ such that $f(x_1) = f(x_2) = y$. Let $x = g(y)$. Since $g$ is a left inverse to $f$, we have that $g \circ f \equiv \iota_X$, and hence $g \circ f(x_1) = x_1$, and $g \circ f(x_2) = x_2$. On the other hand, $g \circ f(x_1) = g(f(x_1)) = g(y)$, and $g \circ f(x_2) = g(f(x_2)) = g(y)$. Hence $x_1 = g \circ f(x_1) = g(y) = g \circ f(x_2) = x_2$. Therefore, by definition, $f$ is injective.

   For the backward direction, suppose that $f$ is injective. Let $x_0 \in X$ be any point; note that some such $x_0$ exists since $X$ is presumed to be nonempty. Define a function $g : Y \to X$ as follows: for all $y \in Y$, if there exists $x \in X$ such that $f(x) = y$, then $g(y) = x$. If no such $x$ exists, then $g(y) = x_0$.

   We first verify that $g$ is a well-defined function. Note that for all $y \in Y$, either there exists $x \in X$ with $f(x) = y$, or there does not; hence $g$ is totally defined. Since $g(y)$ is a member of $X$ for each $y$ by definition, we satisfy the existence property. Finally, since $f$ is injective, for each $y$ there is at most one choice of $x$ for which $f(x) = y$, and thus $g$ satisfies the uniqueness property. Therefore, $g$ is a well-defined function.

   Moreover, $\forall x \in X,\ g \circ f(x) = g(f(x)) = x$, by definition of $g$, so $g \circ f \equiv \iota_X$. Therefore, $g$ is a left inverse to $f$, so a left inverse therefore exists.

   As both directions hold, we therefore have that $f$ has a left inverse if and only if $f$ is injective.

2. As with part 1, we consider the two directions.

   For the forward direction, suppose that $f$ has a right inverse $g$. Let $y \in Y$, and let $x = g(y)$. Then we have $f(x) = f(g(y)) = f \circ g(y) = \iota_Y(y) = y$, and hence for every $y \in Y$ there is an $x \in X$ with $f(x) = y$. Therefore, $f$ is surjective.

   For the backward direction[1], suppose that $f$ is surjective. Define a function $g : Y \to X$ as follows. For any $y \in Y$, define $g(y)$ to be any member of $f^{-1}(y)$. Again, we verify the well-definedness of $g$.

   Since for each $y \in Y$, there is at least one $x \in X$ having $f(x) = y$, we have that for every $y \in Y$, $f^{-1}(y)$ is nonempty, and hence there is a point in $f^{-1}(y)$ that can be chosen as the image of $y$ under $g$. Hence, $g$ is totally defined, and existence is also verified. Since we explicitly choose one such point, uniqueness is implied by definition (that is not to say this functio is the only possible right inverse, but it is to say that once we choose the image of $y$ under $g$, it is uniquely chosen).

   Hence, $g$ is a well-defined function. Moreover, for any $y \in Y$, we have that $f \circ g(y) = y$, since $g(y) \in f^{-1}(y)$. Therefore, $g$ is a right inverse to $f$, so a right inverse therefore exists.

   As both directions hold, we therefore have that $f$ has a right inverse if and only if $f$ is surjective.

□

Using this lemma, we have two options for showing if something has a left or right inverse. We could work as in Example 15, and demonstrate the actual left/right inverse. Or, we could simply check if the function is injective or surjective, respectively, and conclude from the lemma that it is sufficient to guarantee the existence of a left/right inverse, without actually demonstrating what the inverse might look like. Consider the following example.

**Example 16.** Let $h : \mathbb{Q} \to \mathbb{Q}$ be defined by $h(q) = 2q$. Then $h$ has a left inverse and a right inverse.

**Proof.** First, for the left inverse, we consider injectivity of $h$. Suppose that $q_1, q_2 \in \mathbb{Q}$ with $h(q_1) = h(q_2)$. Then $2q_1 = 2q_2 \Rightarrow q_1 = q_2$, and hence $h$ is injective. By Lemma 1, then, $h$ has a left inverse.
Second, for the right inverse, we consider surjectivity of $h$. Suppose that $r \in \mathbb{Q}$. Then $h(\frac{r}{2}) = r$, and hence $h$ is surjective. Therefore, by Lemma 1, $h$ has a right inverse. □

By using injectivity and surjectivity, we can verify that the left and right inverse exist, without having to explicitly construct them. This can be very useful, as sometimes explicit constructions of inverses are hard.

Now, what we'd truly like is a two-sided inverse: a function $g$ so that $g \circ f \equiv \iota_X$ and $f \circ g \equiv \iota_Y$. Then we could go back and forth between $X$ and $Y$ willy-nilly. Lemma 1 tells us that in order that $f$ has both a left and right inverse, we need that $f$ is both injective and surjective; that is, we need that $f$ is bijective. Indeed, we have the following theorem:

**Theorem 5.** *Let $X$ and $Y$ be sets, and let $f : X \to Y$ be a function. Then $f$ has a two-sided inverse if and only if $f$ is bijective.*

Lemma 1 is almost enough to give us this theorem, but we need one more piece of information. In order to have an inverse, we must have that the left and right inverse are the same; that is, we need the SAME function to work as both a left and right inverse. Lemma 1 only tells us that there are functions for each side, so we will also require the following lemma, that these two functions are in fact the same.

**Lemma 2.** *Let $X, Y$ be sets, and let $f : X \to Y$ be a function. If $f$ has a left inverse $g$ and a right inverse $h$, then $g \equiv h$.*

[1] WARNING! The following argument relies on the Axiom of Choice. In fact, the statement we claim here cannot be proven without the Axiom of Choice. At some point, I will go into the details about this, probably, but that point is not here and now.

**Proof.** Suppose that $f$ has a left inverse $g$ and a right inverse $h$. Then we have

$$\begin{aligned} g &\equiv g \circ \iota_Y \\ &\equiv g \circ (f \circ h) \quad \text{(since } h \text{ is a right inverse to } f\text{, so } f \circ h \equiv \iota_Y) \\ &\equiv (g \circ f) \circ h \quad \text{(by Theorem 1)} \\ &\equiv \iota_X \circ h \quad \text{(since } g \text{ is a left inverse to } f\text{, so } g \circ f \equiv \iota_X) \\ &\equiv h. \end{aligned}$$

□

We are now ready to combine these properties to prove Theorem 5.

**Proof.** [Proof of Theorem 5] Let $X$ and $Y$ be sets, and let $f : X \to Y$ be a function. We consider each direction.

First, suppose that $f$ is bijective. Then by definition, $f$ is both injective and surjective, so by Lemma 1, we have that $f$ has a left inverse $g$ and $f$ has a right inverse $h$. By Lemma 2, we have that $g \equiv h$, and hence $g$ is both a left and right inverse to $f$. But then, by definition, $f$ has a two-sided inverse.

On the other hand, suppose that $f$ has a two-sided inverse $g$. But then by definition, $g$ is both a left and right inverse, and hence by Lemma 1, we have that $f$ is both injective and surjective. Therefore, $f$ is bijective. □

Now, to determine if a function $f$ has an inverse, we have two options. We can either explicitly demonstrate an inverse $g$, and show that both $f \circ g$ and $g \circ f$ are equivalent to identity functions, or we can show that $f$ is bijective.

**Example 17.** Show that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = (x-2)^3$ has an inverse.
We shall show this in two ways, as described above.

**Proof.** [Proof 1] Define $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = \sqrt[3]{x} + 2$. Recalling that the cube root of any real number is both defined and unique, we have that $g$ is a well-defined function. Moreover, $g \circ f(x) = g((x-2)^3) = \sqrt[3]{(x-2)^3} + 2 = x$, so $g \circ f \equiv \iota_{\mathbb{R}}$. Also, $f \circ g(x) = f(\sqrt[3]{x} + 2) = (\sqrt[3]{x} + 2 - 2)^3 = x$, so $f \circ g \equiv \iota_{\mathbb{R}}$.
Therefore, since $g$ is an inverse to $f$, we must have that $f$ has an inverse. □

**Proof.** [Proof 2] We prove that $f$ is invertible by demonstrating that $f$ is bijective.
For injectivity, suppose that $x_1, x_2 \in \mathbb{R}$ and $f(x_1) = f(x_2)$. Then $(x_1 - 2)^3 = (x_2 - 2)^3$. Since the cube root of any real number is defined and unique, we can take a cube root on both sides of this equation to conclude $x_1 - 2 = x_2 - 2$, and hence $x_1 = x_2$. Therefore, $f$ is injective.
For surjectivity, suppose that $y \in \mathbb{R}$. Let $x = \sqrt[3]{y} + 2$. Then $f(x) = y$, and hence $f$ is surjective.
As $f$ is both injective and surjective, it has an inverse. □

Finally, a bit more notation.

**Definition 14.** Let $X, Y$ be sets, and let $f : X \to Y$ be a function having an inverse. We say that $f$ is *invertible*, and we use the notation $f^{-1}$ to denote the inverse of $f$.

We note that in order to define "the" inverse of $f$, we should be careful that there is only one such number. This is a corollary of Lemma 2; if $f$ has two different inverses, we can show they are the same by treating one of them as a left inverse and the other as a right inverse.

**Corollary 1.** *Let $f : X \to Y$ be an invertible function. If $g, h$ are both inverses of $f$, then $g \equiv h$.*

Lastly, just a word about notation. It is true that we use the same notation to denote the inverse function of $f$ and the inverse image of subsets of $Y$. This is, of course, awful. From context, though, the two should be distinguishable; one of them takes only sets as input, and the other takes only elements as input. The reason that the notation repeats is that these two things look very similar on singleton sets (if the inverse exists). Indeed, if $f : X \to Y$ is an invertible function, then we have that $\forall y \in Y$, $f^{-1}(\{y\}) = \{f^{-1}(y)\}$; that is, the preimage on the singleton set $\{y\}$ is the set containing the single element which is $f^{-1}(y)$. Note the distinction on the inputs as well; when we mean to take a preimage, we input a set into $f^{-1}$. When we mean to take it as a function, we input an element.