Abstract. We discuss how to structure a proof based on the statement being proved.

Writing proofs is typically not a straightforward, algorithmic process such as calculating
\[ \frac{d}{dx} [xe^{2x}] \quad \text{or} \quad \int_0^1 x^2 dx. \]
There is no sequence of steps one can always follow to give a complete proof of any mathematical truth. Indeed, there are many unsolved problems in mathematics, which amount to statements that people think are true, but do not know how to prove.

Nonetheless, there are general guidelines that we can follow which tell us the general structure that our proof should take. These guidelines will tell us how to get our proof started (what assumptions we should make, what kind of elements/sets we should consider), and also how our proof should end (what the “goal” is, that is the statement we are trying to prove.) For many “elementary” proofs (whatever that means...), figuring out this general structure amounts to about half the work in constructing the proof, and often suggests to us how the other half of the proof will go. In short, getting started really is the most important part in writing a proof, and fortunately, this is more of an algorithmic process such as calculating a derivative or an integral.

Our symbolic logic notation is as follows. The symbol \( \lor \) is used for disjunction (that is, “or” statements) so that \( P \lor Q \) means “\( P \) or \( Q \)” the symbol \( \land \) is for conjunction (“and” statements) so that \( P \land Q \) means “\( P \) and \( Q \)”. We use \( \neg P \) for the negation of the statement \( P \). Other notation such as for conditional statements and quantified statements is discussed below.

We shall first review the general methods we use to prove certain types of statements, namely conditional statements and quantified statements.

1. Proving Conditional Statements

Recall that given two statements \( P \) and \( Q \), the statement “If \( P \), then \( Q \)” is called a conditional statement, and is denoted \( P \Rightarrow Q \). Given a conditional statement \( P \Rightarrow Q \), the statement \( P \) is called the hypothesis and \( Q \) is called the conclusion. A very large portion of statements in mathematics that we want to prove are conditional statements. Thus, knowing how to prove a conditional statement is fundamental to everything we do. There are a few different ways to prove \( P \Rightarrow Q \).

1.1. Direct Proof. A direct proof of \( P \Rightarrow Q \) goes as follows: We assume the statement \( P \) is true, and then work to deduce that \( Q \) is true.
Once we realize that our goal is to prove $P \Rightarrow Q$, then the first thing we should do (if we want to proceed directly) is assume that the statement $P$ is true. Assuming $P$ is true is beneficial to us because it gives us something to work with.

We shall largely focus on direct proofs of conditionals in this document, but let’s review two other methods of proving conditionals first.

1.2. **Contrapositive (Indirect) Proof.** Recall that a conditional statement $P \Rightarrow Q$ is logically equivalent to its contrapositive $\neg Q \Rightarrow \neg P$. Thus, one strategy of proving a conditional statement is to prove its contrapositive instead. A contrapositive proof of $P \Rightarrow Q$ is a direct proof of the contrapositive $\neg Q \Rightarrow \neg P$. Thus in a contrapositive proof, we assume $\neg Q$, and then work to deduce that $\neg P$ follows. Contrapositive proofs can have a different flavor than direct proofs because one starts with very different assumptions in each. If you are struggling trying to prove something directly, one option would be to try a contrapositive proof.

1.3. **Proof by Contradiction.** In a proof by contradiction (which one can do with any statement, not just conditionals), one assumes the negation of the statement one is trying to prove, and then works to derive a contradiction. Recall that the negation of $P \Rightarrow Q$ is logically equivalent to $P \land \neg Q$. Thus, when one starts a proof by contradiction of $P \Rightarrow Q$, one gets to assume both $P$ and $\neg Q$. Having two assumptions to work with is definitely a perk of this approach. The downside is that it is less clear to identify the goal we are working towards. The proof is complete once we derive any contradiction. This could be that $0 = 1$, that $16$ is an odd number, or that the empty set contains an element. At the outset, we typically don’t know what the contradiction will be. We usually just have to explore the consequences of both $P$ and $\neg Q$ until we discover something fishy.

2. **Proving Quantified Statements**

Nearly every statement in mathematics that we prove involves quantifiers. To be successful at writing proofs, it is absolutely crucial that we understand how to work with quantifiers.

2.1. **Proving Universally Quantified Statements.** Recall the universal quantifier $\forall$ is used to mean “all” or “for every.” As an example, the statement “The square of every real number is nonnegative” is represented symbolically as

$$(\forall x \in \mathbb{R})(x^2 \geq 0).$$

Conversely, when presented with this symbolic statement, one reads it from left to right as “For every $x \in \mathbb{R}$, $x^2 \geq 0$.

Let’s discuss how to prove a general universally quantified statement

$$(\forall x \in X)P(x).$$

Here, $X$ could be any set, and $P$ is propositional function whose universal set (i.e. domain) is $X$. This means that for any $x \in X$, $P(x)$ is a statement about $x$. To relate it to the above example, $X$ could be $\mathbb{R}$ and $P(x)$ could be the statement “$x^2 \geq 0$”.

Suppose we want to prove the statement $(\forall x \in X)P(x)$. How do we do it? We need to prove $P(x)$ is a true statement for each individual $x \in X$. This is a pretty intimidating task. For example, if $X$ has infinitely many elements, we are being asked to prove infinitely many statements at once. The way this is done is not by
providing infinitely many proofs, but by providing one proof of the statement $P(x)$ which applies equally well to any particular element $x \in X$. You should imagine this: Someone presents you with a randomly chosen element $x$ from $X$, and you must explain why $P(x)$ is true. However, you don’t actually know which element $x$ you have, all you know is that it came from the set $X$ (the fact that $x \in X$ usually carries some mathematical content.)

The way this looks in practice is that one starts a proof of $(\forall x \in X)P(x)$ by saying “Let $x \in X$ be arbitrary.” “Arbitrary” means “arbitrarily chosen”. Other words that could be used here (but people traditionally don’t) could be “random”, “generic”, or “general”. Now that we have an arbitrarily chosen element $x \in X$, we must get to work and explain why $P(x)$ must be a true statement. Remember, we don’t actually know which element $x \in X$ we are dealing with. All we are allowed to use about $x$ at this point is the fact that $x \in X$. If we are successful in proving $P(x)$, then the end result is an argument that explains why $P(x)$ is true, which could be applied to any element $x \in X$. Thus we can conclude $(\forall x \in X)P(x)$ is a true statement.

Very often, the propositional function $P(x)$ is some sort of compound statement itself. For example, many statements take the form $(\forall x \in X)(P(x) \Rightarrow Q(x))$. To prove this, we must combine the methods we just discussed, along with the methods of proving conditional statements.

So, to prove $(\forall x \in X)(P(x) \Rightarrow Q(x))$, we should start with “Let $x \in X$ be arbitrary.” As discussed above, we must now prove the statement

$$P(x) \Rightarrow Q(x),$$

which is a conditional statement. [Proceeding by direct proof,] the next thing to do would be to assume that $P(x)$ is true, and then work to deduce that $Q(x)$ is true. If we successfully do this, we have proved the conditional statement

$$P(x) \Rightarrow Q(x).$$

Since we proved this for an arbitrary $x \in X$, we can triumphantly conclude that we have proved

$$(\forall x \in X)(P(x) \Rightarrow Q(x)).$$

### 2.2. Proving Existentially Quantified Statements.

Recall the existential quantifier $\exists$ is used to mean “there exists” or “for some.” The existential quantifier is used to assert the existence of objects with certain properties. When we say “there exists,” we mean “there exists at least one.” There could be several, or even infinitely many, but all the existential quantifier guarantees is that there is one.

As an example, the statement “There is an even prime number” can be represented symbolically as

$$\exists p \in \mathbb{N}(p \text{ is even } \land p \text{ is prime}).$$

We know this statement is true because $p = 2$ is both even and prime. We also happen to know that 2 is the only even prime number, but that fact does not make a difference as to whether or not the statement is true or false.

Similarly, consider the statement “There is an odd prime number,” which is represented symbolically as

$$\exists p \in \mathbb{N}(p \text{ is odd } \land p \text{ is prime}).$$
This is certainly a true statement. There are many odd prime numbers, such as 3, 5, 7, 11, etc. In fact, every prime number except for 2 is odd. This implies that there are infinitely many odd prime numbers. However, this doesn’t make the original statement even more true, because such a notion makes no sense. In logic and mathematics, statements are either true or false – there are no varying degrees of truth.

Let’s consider a general existentially quantified statement

\[(\exists x \in X) P(x),\]

for some propositional function \(P(x)\). How do we prove such a statement? Well, the statement asserts the existence of an element \(x \in X\) with the special property that \(P(x)\) is true. Think of it this way: if you are trying to convince me that unicorns exist, I’m not going to believe you unless you show me a unicorn. There is no better way to prove something exists than to put it directly in front of someone’s face. Thus, to prove \((\exists x \in X) P(x)\), you need to provide an explicit example of an element \(x \in X\) with the property that \(P(x)\) is true. Thus, there are two steps in proving \((\exists x \in X) P(x)\).

(1) Present a candidate \(x \in X\), that is, an element for which you are claiming \(P(x)\) is true.

(2) Prove that \(P(x)\) is true for your candidate \(x\).

If you’ve carried out these two steps, then you are certain that at least one element of \(X\) has the property that \(P(x)\) is true. So you are entitled to conclude that \((\exists x \in X) P(x)\) is a true statement.

Regarding (1), you do not need to explain how you discovered your candidate \(x\) in your proof. Whatever inspired you to think of that particular \(x\) has nothing to do with the validity of your proof. In practice, step (1) can often be the more difficult step. You usually need to spend some time experimenting with different elements of \(X\) until you’ve found one. This is a process that should be done on scrap paper, not in your proof.

In presenting your candidate, be as specific and explicit as possible. Remember, you only need to prove one such element exists. If you’ve actually come up with a whole family of examples, resist the urge to present them and choose one specific one. Also, it is a good idea to choose the simplest one that you can. The reason is because you still have to carry out step (2). The more complicated an \(x\) you choose, the more complicated your proof of \(P(x)\) may have to be.

So, if we want to prove \((\exists p \in \mathbb{N})(p \text{ is even } \land p \text{ is prime})\), we should present \(p = 2\) as our candidate, and then prove that 2 is even and 2 is prime.

If we want to prove \((\exists p \in \mathbb{N})(p \text{ is odd } \land p \text{ is prime})\), we have many choices for a candidate. We should pick the simplest one. So we could present \(p = 3\) as our candidate and argue that 3 is both odd and prime. We could just as well present \(p = 15053\) as our candidate, but why make our lives more complicated than they need to be? Both 3 and 15053 are certainly odd, but it’s much, much simpler to prove 3 is prime than it is to prove 15053 is prime.

When proving \((\exists p \in \mathbb{N})(p \text{ is odd } \land p \text{ is prime})\), if you try to get to clever and say “Any prime number \(p\) that is not 2 is odd,” then you are opening up yourself to more work than you need to do in step (2). You would first need to explain why every prime that is not 2 is odd. You could argue this because if \(p\) is even, then \(p\) is divisible by 2. So \(p\) is composite, unless \(p = 2\). However, there’s another issue
here. You also need to explain why there are prime numbers besides 2. That is, your proof isn’t complete until you’ve proved the statement

\[(\exists p \in \mathbb{N})(p \text{ is prime } \land p \neq 2).\]

Do you see why? Now you are almost back to where you started. To prove this, you need to present a number \(p\) that is prime and not equal to 2. OK, you could say \(p = 3\) is such a number. But you really could have just done this in the first place. To summarize, I don’t recommend taking the approach of this paragraph. Just remember the acronym KISS (Keep it simple, student.)

2.3. Multiple Quantifiers.

2.3.1. Mixed Quantifiers. Quantifiers are at their deadliest when they are combined together. This happens quite frequently in mathematics, so it is something we have to learn to deal with. Consider the statement.

\[(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(y > x).\]

This is read, from left to right, as “For every \(x \in \mathbb{R}\), there is a \(y \in \mathbb{R}\) such that \(y > x\).” Translated further, this says “For every real number \(x\), there is another real number \(y\) such that \(y > x\).” Thus, the content of this statement is that whenever we have a real number \(x\), we can always find another real number \(y\) that is larger than \(x\). This is a true statement. Let’s prove it using the above guidelines.

First of all, multiple quantifiers like this should be viewed as layers. This statement is meant to be read as

\[\forall x \in \mathbb{R}\left(\exists y \in \mathbb{R}(y > x)\right).\]

On the outermost layer, this is a universally quantified statement. To prove it, we must follow the guidelines in section 2.1. That is, we must choose an arbitrary \(x \in \mathbb{R}\), and then prove the statement that follows the universal quantifier, which is

\[\exists y \in \mathbb{R}(y > x),\]

in this case. We’ve discovered the second layer of quantifiers. Now we see that our goal is to prove an existentially quantified statement, so we follow the guidelines in section 2.2. To prove this statement, we must construct a real number \(y\) that is larger than the arbitrarily chosen \(x\) which we started with. Since \(x\) is a fixed number at this point in the proof, we know that there are an awful lot of numbers bigger than \(x\). Thinking geometrically, anything to the right of \(x\) on the real number line will do. Remembering KISS, let’s choose our candidate to be \(y = x + 1\). To finish, we must prove that \(y > x\), that is \(x + 1 > x\). To see this, we start with the fact \(1 > 0\). Adding \(x\) to both sides of the inequality shows that \(x + 1 > x\). Thus, \(y > x\). This proves the statement

\[\exists y \in \mathbb{R}(y > x).\]

Now, we pass back the outermost layer where there was a universal quantifier. As discussed in section 2.1, since we proved the statement \(\exists y \in \mathbb{R}(y > x)\) for an arbitrary \(x \in \mathbb{R}\), we are now entitled to conclude

\[\forall x \in \mathbb{R}\left(\exists y \in \mathbb{R}(y > x)\right),\]

which was the statement we set out to prove.
Please be aware than the order of mixed quantifiers is very important. Consider the statement
\[(∃y ∈ \mathbb{R})(∀x ∈ \mathbb{R})(y > x).\]
As with the similar statement above, this should be read as
\[(∃y ∈ \mathbb{R})\left( (∀x ∈ \mathbb{R})(y > x) \right).\]
This statement asserts the existence of a real number \(y\) with the property that
\[(∀x ∈ \mathbb{R})(y > x).\]
In other words, it is saying that there is a real number \(y\) which is greater than all other real numbers. This is certainly a false statement (no, \(∞\) is not a real number.) If you want to prove it is false, you need the prove its negation is true.
The negation of
\[(∃y ∈ \mathbb{R})(∀x ∈ \mathbb{R})(y > x)\]
is logically equivalent to
\[(∀y ∈ \mathbb{R})(∃x ∈ \mathbb{R})(y ≤ x).\]
This statement can be proved in a similar fashion as how we proved
\[(∀x ∈ \mathbb{R})(∃y ∈ \mathbb{R})(y > x)\]
above.

2.3.2. Multiple Quantifiers of the Same Type. Multiple quantifiers are not as tough to deal with when they are of the same type. For example the set theoretic identity
\[A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\]
is something that is true for all sets \(A, B, C\). So this identity should be viewed as the universally quantified statement
\[(∀A)(∀B)(∀C)(A \cap (B \cup C) = (A \cap B) \cup (A \cap C)),\]
which is sometimes written as
\[(∀A, B, C)(A \cap (B \cup C) = (A \cap B) \cup (A \cap C))\]
for brevity. To prove this, we can deal with the three universal quantifiers all at once. A proof of this statement would start with “Let \(A, B,\) and \(C\) be arbitrary sets.” Then we would proceed to prove the equality of sets
\[A \cap (B \cup C) = (A \cap B) \cup (A \cap C).\]
After doing so, we are then entitled to say that we’ve proved
\[(∀A)(∀B)(∀C)(A \cap (B \cup C) = (A \cap B) \cup (A \cap C)).\]

Multiple existential quantifiers are dealt with simultaneously as well. For example, if \(f : X \to Y\) is a function, then the statement “\(f\) is not injective” is
\[(∃x_1 ∈ X)(∃x_2 ∈ X) \left[ (f(x_1) = f(x_2)) \land (x_1 ≠ x_2) \right].\]
In a more shorthand notation, this is written
\[(∃x_1, x_2 ∈ X) \left[ (f(x_1) = f(x_2)) \land (x_1 ≠ x_2) \right].\]
To prove this, we must explicitly construct two candidates \(x_1\) and \(x_2\), and then prove the statement
\[(f(x_1) = f(x_2)) \land (x_1 ≠ x_2).\]
It’s an “and” statement, so you just have to check that both \( f(x_1) = f(x_2) \) and \( x_1 \neq x_2 \) separately.

3. Definitions, definitions, definitions

Definitions are of the utmost importance in mathematics. Every term we use has a precise definition, so that there can never be any ambiguity over if object \( X \) really is of type \( A \). The defining condition is always a logical statement (often quantified) and thus is either true or false. It is never a matter of opinion.

A definition typically takes the form:

**Definition.** We’ll say that \( X \) is a \( ⟨ \text{term being defined} ⟩ \) if \( ⟨ \text{some logical statement about } X ⟩ \).

Some examples:

**Definition.** A number \( n \in \mathbb{Z} \) is even if \( (\exists k \in \mathbb{Z})(n = 2k) \).

**Definition.** A set \( A \) is a subset of a set \( B \) if
\[
(\forall x)(x \in A \Rightarrow x \in B).
\]

**Definition.** A function \( f : X \rightarrow Y \) is injective if
\[
(\forall x_1, x_2 \in X) [(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)].
\]

**Definition.** A function \( f : X \rightarrow Y \) is surjective if
\[
(\forall y \in Y)(\exists x \in X)(f(x) = y).
\]

**Definition.** Two sets \( A \) and \( B \) have the same cardinality if
\[
(\exists f : A \rightarrow B)(f \text{ is a bijection}).
\]

When people say “if” in a definition, they actually mean “if and only if.” For example, if an integer \( n \) is even, then we know that \( (\exists k \in \mathbb{Z})(n = 2k) \) is a true statement. Conversely, if \( n \) is an integer for which \( (\exists k \in \mathbb{Z})(n = 2k) \) is true, then we know that \( n \) is even. Practically speaking, these conditions are very important because they tell us what it is we need to prove to show that an object satisfies a certain definition (and conversely they tell us what we know about an object when we know it satisfies a certain definition.)

The definitions of various sets are also very important. Here, the logical condition which defines membership in the set is given in the description of the set in set-builder notation. Some examples:

**Definition.** The intersection of the sets \( A \) and \( B \) is the set
\[
A \cap B = \{ x : x \in A \land x \in B \}.
\]

**Definition.** The power set of a set \( A \) is the set
\[
\mathcal{P}(A) = \{ S : S \subseteq A \}.
\]

**Definition.** Given a function \( f : X \rightarrow Y \) and a subset \( A \subseteq X \), the image of \( A \) (under \( f \)) is the set
\[
f(A) = \{ y \in Y : (\exists x \in A)(f(x) = y) \}.
\]

**Definition.** Given a function \( f : X \rightarrow Y \) and a subset \( B \subseteq Y \), the preimage of \( B \) (under \( f \)) is the set
\[
f^{-1}(B) = \{ x \in X : f(x) \in B \}.
\]
So, for example, if you are trying to prove that $x \in A \cap B$, then you need to prove that $x \in A$ and $x \in B$ is a true statement. If you want to show $y \in f(A)$, you need to prove that $(\exists x \in A)(f(x) = y)$ is a true statement. If you want to show that $S \in \mathcal{P}(A)$, then you need to show that $S \subseteq A$ is true, which means you need to prove the statement $(\forall x)(x \in S \Rightarrow x \in A)$.

3.1. Specific Examples.

**Example 1.** Prove that $14$ is an even number.

*Proof.* By the definition of even, our goal is to prove that statement $(\exists k \in \mathbb{Z})(14 = 2k)$, which is an existentially quantified statement. Thus, all the remarks from section 2.2 apply. We need to provide our candidate $k \in \mathbb{Z}$ and prove that $14 = 2k$.

So, let $k = 7$, which is an integer (Remember, we don’t need to explain how we came up with the number $k = 7$.) Then $2k = 2 \cdot 7 = 14$.

Thus, we conclude that $(\exists k \in \mathbb{Z})(14 = 2k)$ is a true statement. So $14$ is even by definition of even. \qed

**Example 2.** For sets $A$ and $B$, prove that $A \cap B \subseteq A \cup B$.

*Proof (with thought process).* We must prove the statement $A \cap B \subseteq A \cup B$, which is the universally quantified statement $(\forall x)(x \in A \cap B \Rightarrow x \in A \cup B)$.

So we follow the guidelines of section 2.1. So, let's consider an arbitrary element $x$. Now, we must prove the statement $x \in A \cap B \Rightarrow x \in A \cup B$.

This is a conditional statement. So we follow the guidelines of section 1. Let’s attempt to prove it directly. Thus, we assume $x \in A \cap B$, and our goal is to show $x \in A \cup B$. (Notice that up to this point, we are mechanically following the guidelines discussed above.) The next thing to do is to see what our assumption gets us, and also better understand what we need to do to prove our “goal,” which is $x \in A \cup B$. For this, we consult our definitions. Since $x \in A \cap B$, then by definition of $A \cap B$, we know that $x \in A \land x \in B$. The goal is to show $x \in A \cup B$, which by definition of $A \cup B$ means $x \in A \lor x \in B$. (Notice we still haven’t really done anything substantial in this proof yet. All we did was set up the framework using the guidelines discussed above, and then translated our assumption and our “goal” into logical statements using definitions.) Now comes the mathematical content of the proof. We need to figure out how to deduce $x \in A \lor x \in B$ from the assumption $x \in A \land x \in B$. Since $x \in A \land x \in B$ is true, then $x \in A$ and $x \in B$ are both true statements. Thus, $x \in A \lor x \in B$ is true, by definition of disjunction. So $x \in A \cup B$. This completes the direct proof of $x \in A \cap B \Rightarrow x \in A \cup B$.

Since this was proved for an arbitrary $x$, we conclude $(\forall x)(x \in A \cap B \Rightarrow x \in A \cup B)$.

By definition of subset, this means $A \cap B \subseteq A \cup B$. \qed
Here is a condensed version of the proof, where we are not “thinking out loud.”

**Proof (shorter, without thought process).** Let \( x \) be arbitrary such that \( x \in A \cap B \). Then \( x \in A \) and \( x \in B \). It follows that \( x \in A \) or \( x \in B \), so that \( x \in A \cup B \). Since \( x \) was arbitrary, this proves \( A \cap B \subseteq A \cup B \).

**Example 3.** Prove that the function \( f : \mathbb{R} \to \mathbb{R} \) defined by \( f(x) = 5x - 2 \) is injective.

**Proof.** We must prove the statement

\[
(\forall x_1, x_2 \in \mathbb{R}) [(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)].
\]

Using the definition of \( f \), this is the statement

\[
(\forall x_1, x_2 \in \mathbb{R}) [(5x_1 - 2 = 5x_2 - 2) \Rightarrow (x_1 = x_2)].
\]

Following section 2.1, we know that we should take arbitrary elements \( x_1, x_2 \in \mathbb{R} \), and prove the statement

\[
(5x_1 - 2 = 5x_2 - 2) \Rightarrow (x_1 = x_2).
\]

Proceeding with a direct proof, as in section 1, we should assume

\[
5x_1 - 2 = 5x_2 - 2,
\]

and our goal is to show \( x_1 = x_2 \). This can be done using elementary algebra in this example: Adding 2 to both sides of the equation gives

\[
5x_1 = 5x_2.
\]

Dividing both sides by 5, we obtain

\[
x_1 = x_2,
\]

as desired. We have proved

\[
(5x_1 - 2 = 5x_2 - 2) \Rightarrow (x_1 = x_2).
\]

As \( x_1, x_2 \) were arbitrary, we have shown

\[
(\forall x_1, x_2 \in \mathbb{R}) [(5x_1 - 2 = 5x_2 - 2) \Rightarrow (x_1 = x_2)].
\]

By definition, the function \( f \) is injective.

**Example 4.** Prove that the function \( f : \mathbb{R} \to \mathbb{R} \) defined by

\[
f(x) = 2x^3 - 11
\]

is surjective.

**Proof.** We must prove the statement

\[
(\forall y \in \mathbb{R})(\exists x \in \mathbb{R})(f(x) = y).
\]

Remember that the nested quantifiers should be read as

\[
(\forall y \in \mathbb{R}) [(\exists x \in X)(f(x) = y)]
\]

This statement is universally quantified on the outermost layer, so we consider an arbitrary element \( y \in \mathbb{R} \), and we must prove the statement

\[
(\exists x \in \mathbb{R})(f(x) = y).
\]

Using the definition of \( f \), the statement to be proved is

\[
(\exists x \in \mathbb{R})(2x^3 - 11 = y).
\]
This is an existence statement, so it is on us to say what $x$ is. [At this point, you figure out what number $x$ satisfies the equation $2x^3 - 11 = y$ on your scrap paper, but don’t include your extra work in the proof.] Our proposed candidate is

$$x = \sqrt[3]{\frac{y + 11}{2}}.$$

Now we must show that $f(x)$ really does equal $y$. So we calculate

$$f(x) = f\left(\sqrt[3]{\frac{y + 11}{2}}\right)$$

$$= 2\left(\sqrt[3]{\frac{y + 11}{2}}\right)^3 - 11$$

$$= 2 \left(\frac{y + 11}{2}\right) - 11$$

$$= (y + 11) - 11$$

$$= y.$$

Voila! We have shown that $f(x) = y$ for our candidate $x$. We are entitled to conclude

$$(\exists x \in \mathbb{R})(f(x) = y).$$

Since this statement has been proved for an arbitrary $y \in \mathbb{R}$, it follows that

$$(\forall y \in \mathbb{R})(\exists x \in \mathbb{R})(f(x) = y).$$

By definition of surjective, we conclude that $f$ is surjective.

3.2. General Examples. Here, we shall review in general how one proves certain common statements. Compare the relevant examples in this section to the examples in the previous section.

**Example 5** (Subsets). To prove that $A \subseteq B$, we must prove the statement

$$(\forall x)(x \in A \Rightarrow x \in B).$$

Following our guidelines, we must let $x$ be arbitrary and prove the statement

$$x \in A \Rightarrow x \in B.$$

To prove this conditional statement directly, we assume $x \in A$ and must show that $x \in B$. Thus, a typical proof that $A \subseteq B$ will take the following form:

Let $x$ be arbitrary such that $x \in A$. (or: Let $x \in A$ be arbitrary.)

Therefore $x \in B$.

Since $x$ was arbitrary, we conclude $A \subseteq B$.

The statements that fill in the $\therefore$ will vary depending on what the sets $A$ and $B$ actually are. However, regardless of what $A$ and $B$ are, this is the general structure that a proof of $A \subseteq B$ should take.
Example 6 (Injective Functions). To prove that a function $f : X \to Y$ is injective, we must prove the statement

$$\forall x_1, x_2 \in X \left[ (f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2) \right].$$

Our guidelines dictate that we need to take arbitrary $x_1, x_2 \in X$, and prove the statement

$$\left(f(x_1) = f(x_2)\right) \Rightarrow \left(x_1 = x_2\right).$$

This is a conditional statement. Proceeding directly, we assume $f(x_1) = f(x_2)$ and our goal is to prove $x_1 = x_2$. So a typical proof of the injectivity of a function will take the form

Let $x_1, x_2 \in X$ be arbitrary such that $f(x_1) = f(x_2)$. 

\[ \vdots \]

Therefore $x_1 = x_2$.

Since $x_1$ and $x_2$ were arbitrary, we have proved that $f$ is injective.

Of course, the missing details will depend on what the function $f$ actually is. This is the general structure that a direct proof of injectivity takes.

Example 7 (Surjective Functions). To prove that a function $f : X \to Y$ is surjective, we must prove the statement

$$\forall y \in Y \left( \exists x \in X \left( f(x) = y \right) \right).$$

Notice these are nested quantifiers. This statement should be read as

$$\forall y \in Y \left( \exists x \in X \left( f(x) = y \right) \right).$$

To prove such a statement, we take an arbitrary $y \in Y$, and we must prove the statement

$$\exists x \in X \left( f(x) = y \right).$$

This is an existentially quantified statement. To prove it, we need to explicitly provide a candidate $x \in X$ and then prove $f(x) = y$. It is important to realize here that $y$ is a fixed object at the point in the proof. It has been arbitrarily (or randomly, if you like) chosen, but it is a fixed element of the set $Y$. What’s being suggested is that you shouldn’t think of it as some sort of variable quantity. So a typical proof of surjectivity looks like this:

Let $y \in Y$ be arbitrary.

Let $x = \langle$ insert candidate here $\rangle$.

Then $f(x) = \ldots = y$.

Thus there exists $x \in X$ for which $f(x) = y$.

Since $y$ was arbitrary, we conclude $f$ is surjective.

There are two parts that require extra work. One usually needs to do some work to figure out what the appropriate choice of the candidate $x$ is. Of course, this will depend on what the function $f$ is. As discussed in section 2.2, this work shouldn’t be part of the actual proof. It should be done on scrap paper. Of course, one also has to fill in the $\ldots$ above with an actual calculation which shows that $f(x) = y$.

Example 8 (Induction Step). A proof by induction involves two steps: proving the base case, and the induction step. Here, we just focus on the induction step. Recall that the induction step is a proof of the statement

$$\forall n \geq n_0 \left( P(n) \Rightarrow P(n+1) \right).$$
Following our guidelines, we should take an arbitrary $n \geq n_0$ and prove

$$P(n) \Rightarrow P(n + 1).$$

It’s a conditional statement, so we should assume $P(n)$, and our goal is to prove $P(n + 1)$. Recall that the statement $P(n)$ which is being assumed here is called the induction hypothesis. So, a typical induction step (not the whole proof by induction) takes the form:

Suppose $n \geq n_0$ is such that $P(n)$ is true.

\[ \vdots \]

Therefore $P(n + 1)$.

Of course, the details need to be filled in, and this depends on what the statement $P(n)$ is. The hallmark of an inductive proof is that the proof of the statement $P(n + 1)$ can somehow be proved using the simpler statement $P(n)$.

**Example 9** (Cardinality). To prove that the sets $A$ and $B$ have the same cardinality, we must prove the statement

$$\left( \exists f : A \rightarrow B \right) (f \text{ is a bijection}).$$

This is an existence statement, so we must explicitly provide such an $f$. After doing so, we must prove that $f$ is a bijection. A bijection is a function that is both an injective and a surjective. So we must prove that our $f$ has both of these properties, separately. Here is the structure of a typical proof:

Let $f : A \rightarrow B$ be defined by $f(x) = \ldots$

We shall first prove $f$ is injective.

Let $a_1, a_2 \in A$ be arbitrary such that $f(a_1) = f(a_2)$.

\[ \vdots \]

Therefore, $a_1 = a_2$. Thus, $f$ is injective.

We shall show $f$ is surjective.

Let $b \in B$ be arbitrary.

Consider $a = \langle \text{insert candidate here} \rangle$.

Then $f(a) = \ldots = b$.

Since $b \in B$ was arbitrary, $f$ is surjective.

This proves $f$ is a bijection.

We conclude $A$ has the same cardinality as $B$.

The missing details that need to be filled in will depend on what the actual sets $A$ and $B$ are, as well as what function $f$ we pick.

3.3. **Negative Examples.** Recall that to disprove a statement $P$ is to prove that $P$ is false. In other words, to disprove $P$ is to prove the statement $\neg P$. Thus, all the previous remarks in sections 1 and 2 apply when proving the statement $\neg P$. 
One must be comfortable with negating complicated logical expressions here involving quantifiers and the logical operations $\land, \lor, \Rightarrow$. Recall

$$
\neg(P \land Q) \equiv \neg P \lor \neg Q \\
\neg(P \lor Q) \equiv \neg P \land \neg Q \\
\neg(P \Rightarrow Q) \equiv P \land \neg Q \\
\neg(\forall x)P(x) \equiv (\exists x)(\neg P(x)) \\
\neg(\exists x)P(x) \equiv (\forall x)(\neg P(x))
$$

For example, to disprove the universal statement $(\forall x)P(x)$, we must prove $(\exists x)(\neg P(x))$. This is an existence statement, so we follow the guidelines of section 2.2, which state that we must produce an example of an $x$ for which the statement $\neg P(x)$ holds true (that is, $P(x)$ is false.) Such an $x$ that disproves a universal statement $(\forall x)P(x)$ is called a counterexample to the statement $(\forall x)P(x)$.

**Example 10** (Not a Subset). To show that $A$ is not a subset of $B$ is to prove the statement $\neg(A \subseteq B)$. That is, we must prove $\neg(\forall x)(x \in A \Rightarrow x \in B)$, which is logically equivalent to $$(\exists x)(x \in A \land x \notin B).$$

As this is an existence statement, it suffices to explicitly provide an element $x$ with the property that $x \in A$ and $x \notin B$.

Consider the following toy example: Let $A = \{1, 2\}$, $B = \{3, 4\}$, $C = \{1, 2, 3, 4\}$. Let’s prove that $C \times C$ is not a subset of $A \times B$. We must prove $\neg(C \times C \subseteq A \times B)$, which is equivalent to the statement $$(\exists(x, y))(x, y) \in C \times C \land (x, y) \notin A \times B).$$

Notice here that the types of elements in these sets are ordered pairs. So we write the quantified statement so the the quantified variable is an ordered pair. Let’s choose the ordered pair $(3, 4)$. To finish, we have to show $$(3, 4) \in C \times C \text{ and } (3, 4) \notin A \times B.$$ By definition of Cartesian Product, $(x, y) \in X \times Y$ if and only if $x \in X$ and $y \in Y$. This means that $(x, y) \notin X \times Y$ if and only if $x \notin X$ or $y \notin Y$, by De Morgan’s Laws. So it is clear that $(3, 4) \in C \times C$ because $3 \in C$ and $4 \in C$. However, $3 \notin A$, which implies that $3 \notin A$ or $4 \notin B$ is a true statement, even though $4 \notin B$ is true. Thus, $(3, 4) \notin A \times B$. We’ve shown that $C \times C$ is not a subset of $A \times B$.

\footnote{Recall that the \textit{Cartesian Product} of two sets $X$ and $Y$ is the set $X \times Y = \{(x, y) : x \in X \land y \in Y\}$.}
Example 11 (Not Equal Sets). Recall that two sets $A$ and $B$ are equal if
\[ A \subseteq B \text{ and } B \subseteq A. \]
Thus, to prove $A \neq B$, we must prove the statement
\[ A \nsubseteq B \text{ or } B \nsubseteq A. \]
So, you may have a choice here. You just need to prove one of the two “non-subset relations.” Carrying that out is the subject of the previous example. Depending the sets $A$ and $B$ you are dealing with, you may not actually have a choice. It may be the case that $A \subseteq B$ and $B \nsubseteq A$, in which case you will be quite unsuccessful if you try to prove $A \nsubseteq B$.

Example 12 (Not Injective Functions). To prove that a function $f : X \rightarrow Y$ is not injective, it to prove
\[ \neg (\forall x_1, x_2 \in X) [(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)], \]
which is logically equivalent to
\[ (\exists x_1, x_2 \in X) [(f(x_1) = f(x_2)) \land (x_1 \neq x_2)]. \]
This statement is the assertion that there exists two distinct elements of $X$ that have the same image under $f$. Our task is to prove an existence statement, so we follow section 2.2.

Let us consider a concrete example. Consider the function
\[ f : \mathbb{R} \rightarrow \mathbb{R}, \quad f(x) = x^2. \]
Let’s prove $f$ is not injective. This is just the statement that there exist two distinct real numbers that have the same square. We must produce an example of this. So let
\[ x_1 = 2, \quad x_2 = -2. \]
Clearly, $x_1 \neq x_2$. Moreover,
\[ f(x_1) = 2^2 = 4 \quad \text{and} \quad f(x_2) = (-2)^2 = 4, \]
which shows $f(x_1) = f(x_2)$. We have proved the statement
\[ (f(x_1) = f(x_2)) \land (x_1 \neq x_2) \]
for our choice of $x_1$ and $x_2$. Thus, we are entitled to conclude
\[ (\exists x_1, x_2 \in \mathbb{R}) [(f(x_1) = f(x_2)) \land (x_1 \neq x_2)] \]
is true. By definition, $f$ is not injective.

Example 13 (Not Surjective Functions). To prove that a function $f : X \rightarrow Y$ is not surjective is to prove the statement
\[ \neg (\forall y \in Y)(\exists x \in X)(f(x) = y). \]
This is equivalent to the statement
\[ (\exists y \in Y)(\forall x \in X)(f(x) \neq y). \]
This statement says that there is some $y \in Y$ which is not the image of any element $x \in X$ under $f$. In other words, there is $y \in Y$ which is not in the range of $f$. To prove this, we must first provide our candidate $y \in Y$, which we should choose to be something that we’re sure isn’t in the range. Then we must prove the statement
\[ (\forall x \in X)(f(x) \neq y) \]
for our candidate \( y \).

Let’s consider the concrete example of the function

\[
f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2.
\]

Let’s show it is not surjective. We must first provide our candidate \( y \). Let’s choose \( y = -1 \). Now we must prove

\[
(\forall x \in \mathbb{R})(f(x) \neq -1).
\]

This is a universally quantified statement, so let’s follow section 2.1. Let \( x \in \mathbb{R} \) be arbitrary. Now we must prove that \( f(x) \neq -1 \). Here, we can use the fact that the square of any real number is nonnegative. Thus, we see

\[
f(x) = x^2 \geq 0 > -1.
\]

Since \( f(x) > -1 \), we see \( f(x) \neq -1 \). As \( x \in \mathbb{R} \) was arbitrary,

\[
(\forall x \in \mathbb{R})(f(x) \neq -1)
\]

is true. That is, we’ve proved

\[
(\forall x \in \mathbb{R})(f(x) \neq y)
\]

for our candidate \( y = -1 \). So we deduce

\[
(\exists y \in \mathbb{R})(\forall x \in \mathbb{R})(f(x) \neq y)
\]

is true. By definition, \( f \) is not surjective.

4. Constructing Proofs

The main point I’ve trying to make in this document is this:

**The logical structure of statement determines the general structure of its proof.**

Everything we prove is a statement, and so can be expressed in symbolic logic. Then, by looking at the type of statement we wish to prove, and using the guidelines in the previous sections, we will have a shell of a proof. This shell will tell us how to get started (what objects we should consider, what assumptions we should make), and it will tell us what the goal is that we are working toward (what we need to deduce to finish the proof.) Let’s consider some examples.

**Example 14.** Let \( f : X \to Y \) be a function and let \( A \subseteq X \) and \( B \subseteq Y \). Prove that

\[
\text{if } A \subseteq f^{-1}(B), \text{ then } f(A) \subseteq B.
\]

Here, the statement we are asked to prove is the conditional statement

\[
[A \subseteq f^{-1}(B)] \Rightarrow [f(A) \subseteq B].
\]

As in section 1, we should start by **assuming** \( A \subseteq f^{-1}(B) \). Then our goal is to prove the statement \( f(A) \subseteq B \). So our goal is to prove

\[
(\forall y)(y \in f(A) \Rightarrow y \in B).
\]

To prove such a statement, we must take an arbitrary \( y \in f(A) \), and then show that \( y \in B \). Doing so will prove \( f(A) \subseteq B \), which will complete our direct proof of

\[
[A \subseteq f^{-1}(B)] \Rightarrow [f(A) \subseteq B].
\]

In this mechanical way, we obtain a shell of a proof:

**Proof (Shell).**
Assume \( A \subseteq f^{-1}(B) \).
We will show that \( f(A) \subseteq B \).
Let \( y \in f(A) \) be arbitrary.

\[
\vdots
\]
Thus \( y \in B \).
Therefore, \( f(A) \subseteq B \).
We conclude that \( [A \subseteq f^{-1}(B)] \Rightarrow [f(A) \subseteq B] \).

\[\square\]

I can’t emphasize enough that we didn’t do anything clever yet. We followed a procedure which was almost algorithmic, based on the guidelines of the earlier sections. Now, we have to figure out how to fill in the missing details, which account for the actual mathematical content of this proof. We’ve already taken a huge step forward in this problem. We have two assumptions to work with: \( A \subseteq f^{-1}(B) \) and \( y \in f(A) \). We have also clearly identified our goal: to prove \( y \in B \). In order to use our assumptions, we must be clear about what they mean. That \( A \subseteq f^{-1}(B) \) means that
\[
(\forall x) (x \in A \Rightarrow x \in f^{-1}(B)).
\]
The only way we can use this is if we have an element of \( A \) in play. If we had such an element, we would be able to deduce it also is an element of \( f^{-1}(B) \). Since there are no elements of \( A \) in sight, let’s move on to our next assumption. We know that \( y \in f(A) \). This is where we need to know our definitions. Recall that
\[
f(A) = \{ z \in Y : (\exists x \in A) (f(x) = z) \}.
\]
(I used the letter \( z \) when recalling the definition of \( f(A) \) because \( y \) already has a meaning in our proof. Be careful not to use a symbol for two different purposes.) So knowing that \( y \in f(A) \) means that
\[
(\exists x \in A) (f(x) = y)
\]
is true. In our proof, we are entitled to deduce that \( y = f(x) \) for some element \( x \in A \). Now we have an element of \( A \) in our proof! So we can use our other assumption \( A \subseteq f^{-1}(B) \). Let’s see if it helps. Since \( x \in A \), we deduce that \( x \in f^{-1}(B) \). Let’s update our shell of a proof.

Proof (Shell after using assumptions).
Assume \( A \subseteq f^{-1}(B) \).
We will show that \( f(A) \subseteq B \).
Let \( y \in f(A) \) be arbitrary.
Then \( y = f(x) \) for some element \( x \in A \), by definition of \( f(A) \).
We see that \( x \in f^{-1}(B) \), because \( A \subseteq f^{-1}(B) \).

\[
\vdots
\]
Thus \( y \in B \).
Therefore, \( f(A) \subseteq B \).
We conclude that \( [A \subseteq f^{-1}(B)] \Rightarrow [f(A) \subseteq B] \).

\[\square\]

The last thing we figured out was that \( x \in f^{-1}(B) \). What does this get us? Recall the definition
\[
f^{-1}(B) = \{ w \in X : f(w) \in B \}.
\]
Since \( x \in f^{-1}(B) \), we can deduce that \( f(x) \in B \). Is this helpful? Well, our goal is to show that \( y \in B \). Yes, this is very helpful, because \( y = f(x) \). So we should be done! The elements \( y \) and \( f(x) \) are the same thing, so since \( f(x) \in B \) we know that \( y \in B \). Now we can update to a complete proof.

**Proof (Complete).**

Assume \( A \subseteq f^{-1}(B) \).

We will show that \( f(A) \subseteq B \).

Let \( y \in f(A) \) be arbitrary.

Then \( y = f(x) \) for some element \( x \in A \), by definition of \( f(A) \).

We see that \( x \in f^{-1}(B) \), because \( A \subseteq f^{-1}(B) \).

So \( f(x) \in B \), by definition of \( f^{-1}(B) \).

Thus \( y \in B \), because \( y = f(x) \).

Therefore, \( f(A) \subseteq B \).

We conclude that \([A \subseteq f^{-1}(B)] \Rightarrow [f(A) \subseteq B]\).

\[\square\]

To recap, we mechanically set up the general structure of our proof. Then we translated our assumptions using definitions until it became possible to connect our assumptions to our desired conclusion. You can really get a lot of mileage out of this basic approach. Once you get comfortable doing this, it may start to feel like the proof is writing itself!

**Exercise.** Follow a similar procedure to prove the converse statement. That is, suppose \( f : X \to Y \) is a function and \( A \subseteq X \), \( B \subseteq Y \). Prove

if \( f(A) \subseteq B \), then \( A \subseteq f^{-1}(B) \).

**Example 15.** Suppose \( A \) and \( B \) are sets. Prove that

if \( A \subseteq B \), then \( \mathcal{P}(A) \subseteq \mathcal{P}(B) \).

We are proving the conditional statement

\((A \subseteq B) \Rightarrow (\mathcal{P}(A) \subseteq \mathcal{P}(B))\).

So, to get started, we should assume \( A \subseteq B \). Our goal is to prove

\( \mathcal{P}(A) \subseteq \mathcal{P}(B) \),

which is the statement

\((\forall S)(S \in \mathcal{P}(A) \Rightarrow S \in \mathcal{P}(B))\).

To do so, we should consider an arbitrary \( S \) and prove the statement

\( S \in \mathcal{P}(A) \Rightarrow S \in \mathcal{P}(B) \).

This is another conditional statement. Proceeding directly, we should assume \( S \in \mathcal{P}(A) \), and our goal is to prove \( S \in \mathcal{P}(B) \). We have just come up with the general structure of our proof:

**Proof (Shell).**

Assume \( A \subseteq B \).

We will show that \( \mathcal{P}(A) \subseteq \mathcal{P}(B) \).

Let \( S \in \mathcal{P}(A) \) be arbitrary.

\( \vdots \)

Thus \( S \in \mathcal{P}(B) \).
Therefore, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

We conclude that $[A \subseteq B] \Rightarrow [\mathcal{P}(A) \subseteq \mathcal{P}(B)]$.

□

We have two assumptions: $A \subseteq B$ and $S \in \mathcal{P}(A)$. Our goal is to prove that $S \in \mathcal{P}(B)$. Since we are dealing with power sets, it would be helpful to recall the definition

$$\mathcal{P}(X) = \{T : T \subseteq X\}.$$ 

This helps us on both ends of our proof. Since $S \in \mathcal{P}(A)$, we know that $S \subseteq A$ by definition of power set. Our goal is to show that $S \in \mathcal{P}(B)$, so to do this, we must show $S \subseteq B$. Let’s update our proof.

Proof (Shell, update).

Assume $A \subseteq B$.

We will show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Let $S \in \mathcal{P}(A)$ be arbitrary.

Then $S \subseteq A$ by definition of $\mathcal{P}(A)$.

Thus, $S \subseteq B$.

This shows $S \in \mathcal{P}(B)$, by definition of $\mathcal{P}(B)$.

Therefore, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

We conclude that $[A \subseteq B] \Rightarrow [\mathcal{P}(A) \subseteq \mathcal{P}(B)]$.

□

Up until this point, we have just laid out the structure of the proof, following the guidelines of the earlier sections and using definitions. Now we must fill in the mathematical content of the proof. Here is where we stand: We know $A \subseteq B$ and we know $S \subseteq A$, and we are trying to prove $S \subseteq B$. Well, there basically nothing left to prove thanks to a basic result about subsets, which states that for any sets $X, Y, Z$,

$$[(X \subseteq Y) \land (Y \subseteq Z)] \Rightarrow (X \subseteq Z).$$

This is Proposition 3.1.4 in the text. Let’s finish the proof.

Proof (Complete).

Assume $A \subseteq B$.

We will show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Let $S \in \mathcal{P}(A)$ be arbitrary.

Then $S \subseteq A$ by definition of $\mathcal{P}(A)$.

Since $S \subseteq A$ and $A \subseteq B$, it follows that $S \subseteq B$. (Proposition 3.1.4)

This shows $S \in \mathcal{P}(B)$, by definition of $\mathcal{P}(B)$.

Therefore, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

We conclude that $[A \subseteq B] \Rightarrow [\mathcal{P}(A) \subseteq \mathcal{P}(B)]$.

□

Example 16. Show if $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ are injective, then $g \circ f : X \rightarrow Z$ is injective.

This statement is the conditional statement

$$[(f \text{ is injective}) \land (g \text{ is injective})] \Rightarrow g \circ f \text{ is injective}.$$
It is a conditional statement, so (proceeding directly) we should assume the statement
\((f \text{ is injective}) \land (g \text{ is injective})\),
and our goal is to prove \(g \circ f\) is injective. Let’s examine our goal a little further: we must prove
\[
(\forall x_1, x_2 \in X) \left[ ((g \circ f)(x_1) = (g \circ f)(x_2)) \Rightarrow (x_1 = x_2) \right].
\]
This is a universally quantified statement, so we should take arbitrary \(x_1, x_2 \in X\),
and prove the statement
\[
((g \circ f)(x_1) = (g \circ f)(x_2)) \Rightarrow (x_1 = x_2).
\]
Ah, it’s another conditional statement. To prove it, we should assume
\((g \circ f)(x_1) = (g \circ f)(x_2)\)
and our goal is to prove \(x_1 = x_2\). By unwinding this all, we have identified the structure that this proof should take.

\[\text{Proof (Shell).} \]
Assume that \(f : X \to Y\) and \(g : Y \to Z\) are injective.
We will show that \(g \circ f : X \to Z\) is injective.
Let \(x_1, x_2 \in X\) be arbitrary such that \((g \circ f)(x_1) = (g \circ f)(x_2)\).
Thus, \(x_1 = x_2\).
Since \(x_1, x_2\) were arbitrary, this shows \(g \circ f\) is injective.
We conclude that \([(f \text{ is injective}) \land (g \text{ is injective})] \Rightarrow g \circ f\) is injective.

Now, we should think a little bit about what our assumptions mean, and how we can use them to fill in the gap. We have three assumptions: \(f\) is injective, \(g\) is injective, and \((g \circ f)(x_1) = (g \circ f)(x_2)\). That \(f\) is injective is the statement
\[
(\forall w_1, w_2 \in X) \left[ (f(w_1) = f(w_2)) \Rightarrow (w_1 = w_2) \right],
\]
and that \(g\) is injective is the statement
\[
(\forall y_1, y_2 \in X) \left[ (g(y_1) = g(y_2)) \Rightarrow (y_1 = y_2) \right],
\]
In order to use the first assumption, we need to have two elements of \(X\) with the same image under \(f\). Similarly, to use the second, we need two elements of \(Y\) that have the same image under \(g\). Let’s look at our third assumption:
\((g \circ f)(x_1) = (g \circ f)(x_2)\).
By definition of composition, this means
\[g(f(x_1)) = g(f(x_2)).\]
Now we can start to connect these assumptions together. This equation asserts the equality of two images under \(g\). The elements that \(g\) is being applied to are \(f(x_1)\) and \(f(x_2)\). Injectivity of \(g\) implies that these two elements must be the same, that is
\[f(x_1) = f(x_2).\]
Now we are getting somewhere. Now we know that these two images under \(f\) are equal. Injectivity of \(f\) implies that \(x_1 = x_2\), and that is exactly what we wanted to prove. Let’s fill out the proof:
Proof (Complete).
Assume that \( f : X \to Y \) and \( g : Y \to Z \) are injective.
We will show that \( g \circ f : X \to Z \) is injective.
Let \( x_1, x_2 \in X \) be arbitrary such that \( (g \circ f)(x_1) = (g \circ f)(x_2) \).
Then \( g(f(x_1)) = g(f(x_2)) \) by definition of composition.
So \( f(x_1) = f(x_2) \) because \( g \) is injective.
Thus, \( x_1 = x_2 \) because \( f \) is injective.
Since \( x_1, x_2 \) were arbitrary, this shows \( g \circ f \) is injective.
We conclude that \([\text{\( f \) is injective}) \land (\text{\( g \) is injective})\] \( \Rightarrow \) \( g \circ f \) is injective.
\( \square \)

Example 17. Show if \( f : X \to Y \) and \( g : Y \to Z \) are surjective, then \( g \circ f : X \to Z \) is surjective.

The structure of this statement is similar to the last example. We must prove the conditional statement
\n\([\text{\( f \) is surjective}) \land (\text{\( g \) is surjective})\] \( \Rightarrow \) \( g \circ f \) is surjective.

Proceeding by direct proof, we should assume
\n\((\text{\( f \) is surjective}) \land (\text{\( g \) is surjective})\)

and our goal is to prove \( g \circ f \) is surjective. Thus, our goal is to prove
\n\((\forall z \in Z)(\exists x \in X)((g \circ f)(x) = z)\).

On the outermost layer, this is universally quantified, so we should consider an arbitrary \( z \in Z \), and then prove
\n\((\exists x \in X)((g \circ f)(x) = z)\).

As this is an existential statement, we will have to produce an element \( x \in X \) with the property that \( (g \circ f)(x) = z \). Using the definition of composition, this means we will have to show that \( g(f(x)) = z \). We can assemble a shell of a proof:

Proof (Shell).
Assume that \( f : X \to Y \) and \( g : Y \to Z \) are surjective.
We will show that \( g \circ f : X \to Z \) is surjective.
Let \( z \in Z \) be arbitrary.
\begin{align*}
    & \vdots \\
    & \text{Let } x = \ldots \\
    & \vdots \\
    & \text{Thus, } g(f(x)) = z. \\
\end{align*}
So there exists \( x \in X \) such that \( (g \circ f)(x) = z \).
Since \( z \) was arbitrary, this shows \( g \circ f \) is surjective.
We conclude that \([\text{\( f \) is surjective}) \land (\text{\( g \) is surjective})\] \( \Rightarrow \) \( g \circ f \) is surjective.
\( \square \)

Now, let’s explore our assumptions to try to figure out how to fill in the details.
We have an element \( z \in Z \) and two assumptions: \( f \) is surjective and \( g \) is surjective.
Surjectivity of \( f \) says that every element of \( Y \) has a preimage under \( f \). It appears we cannot use this yet, because we have no elements of \( Y \) in sight. However, surjectivity of \( g \) says that every element of \( Z \) has a preimage under \( g \). We have an element \( z \in Z \), so let’s use the fact that \( g \) is surjective to produce an element \( y \in Y \).
such that \( g(y) = z \). The definition of surjectivity guarantees that such a \( y \) exists. Now we have something new: an element of \( Y \). We can now use the surjectivity of \( f \) to produce an element \( x \in X \) with the property that \( f(x) = y \). Now, we’ve got our hands on something in \( X \). If we are lucky enough, perhaps this \( x \) is the type of \( x \) we are looking for. Let’s fill out the details.

**Proof (Complete).**

Assume that \( f : X \to Y \) and \( g : Y \to Z \) are surjective.

We will show that \( g \circ f : X \to Z \) is surjective.

Let \( z \in Z \) be arbitrary.

There is \( y \in Y \) such that \( g(y) = z \) because \( g \) is surjective.

Then \( f(x) = y \). Proceeding directly, we should assume this large hypothesis, and work to prove that \( f \) is not injective. So we should assume there is a \( b \in Y \) and two ordered pairs \((x_1, y_1), (x_2, y_2) \in L_b \cap \text{graph}(f)\) such that \( (x_1, y_1) \neq (x_2, y_2) \). This is a lot of information. Before we break it down, keep in mind that our goal is to prove \( f \) is not injective, which is to prove the statement

\[
(\exists w_1, w_2 \in X) \left[ (f(w_1) = f(w_2)) \land (w_1 \neq w_2) \right].
\]

I used the names \( w_1 \) and \( w_2 \) here rather than \( x_1, x_2 \), because \( x_1, x_2 \) already have a meaning in this problem. We have no reason yet to believe that they are the same (although it will turn out that they are in this case.) Following the guidelines of section 2.2, we will have to identify two elements \( w_1, w_2 \in X \) and prove that

\[
(f(w_1) = f(w_2)) \land (w_1 \neq w_2).
\]

Let’s put together a rough outline of a proof.

**Proof (Shell).**
Suppose there is \( b \in Y \) and distinct ordered pairs \((x_1, y_1), (x_2, y_2)\) which are both elements of \( L_b \cap \text{graph}(f) \). We will show that \( f \) is not injective.

Let \( w_1 = \ldots \) and \( w_2 = \ldots \).

Thus, \( f(w_1) = f(w_2) \) and \( w_1 \neq w_2 \).
We conclude that \( f \) is not injective.

\[ \square \]

Let’s start to investigate all of the assumptions. First, we know that \((x_1, y_1) \in L_b \cap \text{graph}(f)\).

This is an intersection, so we can deduce that \((x_1, y_1) \in L_b \) and \((x_1, y_1) \in \text{graph}(f)\).

Let’s see what these two facts bring us by using definitions. The set \( L_b \) is the set of all ordered pairs whose second element is \( b \). Thus, since \((x_1, y_1) \in L_b\), we see that \( y_1 = b \). By definition of \( \text{graph}(f) \), we see that \( f(x_1) = y_1 \) because \((x_1, y_1) \in \text{graph}(f)\). If we put these two pieces together, we have \( f(x_1) = y_1 = b \).

This is what we’ve learned about \( x_1 \) and \( y_1 \) using the fact that \((x_1, y_1) \in L_b \cap \text{graph}(f)\). Similarly, since \((x_2, y_2) \in L_b \cap \text{graph}(f)\), we get \( f(x_2) = y_2 = b \).

So the images of \( x_1 \) and \( x_2 \) under \( f \) are both \( b \). This should make us think of injectivity. (So we will actually want \( w_1 = x_1 \) and \( w_2 = x_2 \) in the above outline.) However, we haven’t quite finished. We need to be certain that \( x_1 \neq x_2 \). We know \((x_1, y_1) \neq (x_2, y_2)\), which doesn’t give this to us immediately. That \((x_1, y_1) \neq (x_2, y_2)\) is the statement
\[ \neg[(x_1 = x_2) \land (y_1 = y_2)], \]

which is equivalent to
\[ (x_1 \neq x_2) \lor (y_1 \neq y_2) \]
by De Morgan’s Laws. We can only deduce \( x_1 \neq x_2 \) if we know that \( y_1 = y_2 \) (so that \( y_1 \neq y_2 \) is false.) However, we’ve actually shown this already, because
\[ y_1 = b = y_2. \]

It seems we’ve connected all the dots for a complete proof. Let’s fill in the details, and get rid of the superfluous notation \( w_1 \) and \( w_2 \).

Proof (Complete).

Suppose there is \( b \in Y \) and distinct ordered pairs \((x_1, y_1), (x_2, y_2)\) which are both elements of \( L_b \cap \text{graph}(f) \). We will show that \( f \) is not injective by showing that \( f(x_1) = f(x_2) \) and \( x_1 \neq x_2 \).

Since \((x_1, y_1) \in L_b \cap \text{graph}(f)\), we see \((x_1, y_1) \in L_b \) and \((x_1, y_1) \in \text{graph}(f)\). Then \( y_1 = b \) because \((x_1, y_1) \in L_b \).
Also, $f(x_1) = y_1$ because $(x_1, y_1) \in \text{graph}(f)$.
Similarly, $y_2 = b$ and $f(x_2) = y_2$ because $y_2 \in L_b \cap \text{graph}(f)$.
So $f(x_1) = y_1 = b = y_2 = f(x_2)$.
This shows $f(x_1) = f(x_2)$.
Since $(x_1, y_1) \neq (x_2, y_2)$, it follows that $x_1 \neq x_2$ or $y_1 \neq y_2$.
So $x_1 \neq x_2$, because $y_1 = y_2$ was shown above.
Thus, $f(x_1) = f(x_2)$ and $x_1 \neq x_2$.
We conclude that $f$ is not injective.

Exercise. Prove the converse to the above statement: If $f$ is not injective, then there exists $b \in Y$ such that $L_b \cap \text{graph}(f)$ contains at least two distinct points.
(The corresponding “if and only if” statement is usually called “The Horizontal Line Test.”)