Some information about integers

Let $n, d \in \mathbb{Z}$. We say d is a divisor of n if $n/d \in \mathbb{Z}$ (i.e. there exists some $k \in \mathbb{Z}$ for which $n = kd$).

Some information about integers

Let $n, d \in \mathbb{Z}$. We say d is a divisor of n if $n/d \in \mathbb{Z}$ (i.e. there exists some $k \in \mathbb{Z}$ for which $n = kd$). We say $p \in \mathbb{Z}$ is prime if for all $a, b \in \mathbb{Z}$, we have

if p is a divisor of ab, then p is a divisor of a or b.

"p prime $\equiv \forall a, b \in \mathbb{Z}\,(ab/p \in \mathbb{Z} \Rightarrow (a/p \in \mathbb{Z} \vee b/p \in \mathbb{Z}))$"

This is equivalent to the only divisors of p being $\pm p$, ± 1.

Some information about integers

Let $n, d \in \mathbb{Z}$. We say d is a divisor of n if $n/d \in \mathbb{Z}$ (i.e. there exists some $k \in \mathbb{Z}$ for which $n = kd$). We say $p \in \mathbb{Z}$ is prime if for all $a, b \in \mathbb{Z}$, we have

if p is a divisor of ab, then p is a divisor of a or b.

$$\text{“}p \text{ prime} \equiv \forall a, b \in \mathbb{Z}\,(ab/p \in \mathbb{Z} \Rightarrow (a/p \in \mathbb{Z} \vee b/p \in \mathbb{Z}))\text{”}$$

This is equivalent to the only divisors of p being $\pm p$, ± 1.
Ex. The integer divisors of 6 are $1, 2, 3, 6, -1, -2, -3$, and -6. So 6 is not prime.

Some information about integers

Let $n, d \in \mathbb{Z}$. We say d is a divisor of n if $n/d \in \mathbb{Z}$ (i.e. there exists some $k \in \mathbb{Z}$ for which $n = kd$). We say $p \in \mathbb{Z}$ is prime if for all $a, b \in \mathbb{Z}$, we have

$$\text{if } p \text{ is a divisor of } ab, \quad \text{then } p \text{ is a divisor of } a \text{ or } b.$$

$$\text{“}p \text{ prime} \equiv \forall a, b \in \mathbb{Z}\,(ab/p \in \mathbb{Z} \Rightarrow (a/p \in \mathbb{Z} \vee b/p \in \mathbb{Z}))\text{”}$$

This is equivalent to the only divisors of p being $\pm p$, ± 1.

Ex. The integer divisors of 6 are $1, 2, 3, 6, -1, -2, -3$, and -6. So 6 is not prime.

Ex. 5 is prime since its only divisors are $1, 5, -1$, and -5.

Some information about integers

Let $n, d \in \mathbb{Z}$. We say d is a divisor of n if $n/d \in \mathbb{Z}$ (i.e. there exists some $k \in \mathbb{Z}$ for which $n = kd$). We say $p \in \mathbb{Z}$ is prime if for all $a, b \in \mathbb{Z}$, we have

if p is a divisor of ab, then p is a divisor of a or b.

"p prime $\equiv \forall a, b \in \mathbb{Z}\, (ab/p \in \mathbb{Z} \Rightarrow (a/p \in \mathbb{Z} \vee b/p \in \mathbb{Z}))$"

This is equivalent to the only divisors of p being $\pm p$, ± 1.
Ex. The integer divisors of 6 are $1, 2, 3, 6, -1, -2, -3$, and -6. So 6 is not prime.
Ex. 5 is prime since its only divisors are $1, 5, -1$, and -5.

We say a is rational if there exists $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $n = a/p$.

Some information about integers

Let $n, d \in \mathbb{Z}$. We say d is a divisor of n if $n/d \in \mathbb{Z}$ (i.e. there exists some $k \in \mathbb{Z}$ for which $n = kd$). We say $p \in \mathbb{Z}$ is prime if for all $a, b \in \mathbb{Z}$, we have

if p is a divisor of ab, then p is a divisor of a or b.

$$\text{“}p \text{ prime} \equiv \forall a, b \in \mathbb{Z}\,(ab/p \in \mathbb{Z} \Rightarrow (a/p \in \mathbb{Z} \vee b/p \in \mathbb{Z}))\text{”}$$

This is equivalent to the only divisors of p being $\pm p$, ± 1.

Ex. The integer divisors of 6 are $1, 2, 3, 6, -1, -2, -3$, and -6. So 6 is not prime.

Ex. 5 is prime since its only divisors are $1, 5, -1$, and -5.

We say a is rational if there exists $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $n = a/p$. We say a/b is in lowest terms if a and b don't have any prime divisors in common.

Techniques of proof I: Direct method

Theorem

Suppose that $a \in \mathbb{Q}$ *and* $a^2 \in \mathbb{Z}$*. Then* $a \in \mathbb{Z}$*.*

Techniques of proof I: Direct method

Theorem

Suppose that $a \in \mathbb{Q}$ *and* $a^2 \in \mathbb{Z}$*. Then* $a \in \mathbb{Z}$*.*

Unpacking the problem:

Being rational means there are $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $a = m/n$. We might as well assume m/n is in lowest terms, so that m and n have no common prime divisors.

Being integral means that in lowest form, $m = \pm 1$.

Techniques of proof I: Direct method

Theorem

Suppose that $a \in \mathbb{Q}$ *and* $a^2 \in \mathbb{Z}$*. Then* $a \in \mathbb{Z}$*.*

Unpacking the problem:

Being rational means there are $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $a = m/n$. We might as well assume m/n is in lowest terms, so that m and n have no common prime divisors.

Being integral means that in lowest form, $m = \pm 1$.

Plan:

Start with "Let a be a rational number satisfying $a^2 \in \mathbb{Z}$."

Goal: Conclude $a \in \mathbb{Z}$.

Techniques of proof I: Direct method

Theorem

Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Unpacking the problem:

Being rational means there are $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $a = m/n$. We might as well assume m/n is in lowest terms, so that m and n have no common prime divisors.
Being integral means that in lowest form, $m = \pm 1$.

Plan:

Start with "Let a be a rational number satisfying $a^2 \in \mathbb{Z}$."
Goal: Conclude $a \in \mathbb{Z}$.
To try: Let $m/n \in \mathbb{Z}$ such that $a = m/n$ and m/n is in lowest form. Compute a^2 and use $a^2 \in \mathbb{Z}$.

Techniques of proof I: Direct method

Theorem

Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Unpacking the problem:

Being rational means there are $m, n \in \mathbb{Z}$ with $n \neq 0$ such that $a = m/n$. We might as well assume m/n is in lowest terms, so that m and n have no common prime divisors.
Being integral means that in lowest form, $m = \pm 1$.

Plan:

Start with "Let a be a rational number satisfying $a^2 \in \mathbb{Z}$."
Goal: Conclude $a \in \mathbb{Z}$.
To try: Let $m/n \in \mathbb{Z}$ such that $a = m/n$ and m/n is in lowest form. Compute a^2 and use $a^2 \in \mathbb{Z}$.

Proof. Let a be a rational number satisfying $a^2 \in \mathbb{Z}$. Since $a \in \mathbb{Q}$, there exists $m, n \in \mathbb{Z}$ (with $n \neq 0$) such that $a = m/n$. Assume, without loss of generality, that m/n is in lowest form (i.e. m and n have no common prime factors).

Techniques of proof I: Direct method

Theorem
Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Proof. Let a be a rational number satisfying $a^2 \in \mathbb{Z}$. Since $a \in \mathbb{Q}$, there exists $m, n \in \mathbb{Z}$ (with $n \neq 0$) such that $a = m/n$. Assume, without loss of generality, that m/n is in lowest form (i.e. m and n have no common prime factors). Thus

$$a^2 = (m/n)^2 = m^2/n^2.$$

Techniques of proof I: Direct method

Theorem
Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Proof. Let a be a rational number satisfying $a^2 \in \mathbb{Z}$. Since $a \in \mathbb{Q}$, there exists $m, n \in \mathbb{Z}$ (with $n \neq 0$) such that $a = m/n$. Assume, without loss of generality, that m/n is in lowest form (i.e. m and n have no common prime factors). Thus

$$a^2 = (m/n)^2 = m^2/n^2.$$

But since any prime factor of m^2 would also be a prime factor of m (and similarly for n^2 and n), we have m^2/n^2 is in lowest terms.

Techniques of proof I: Direct method

Theorem

Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Proof. Let a be a rational number satisfying $a^2 \in \mathbb{Z}$. Since $a \in \mathbb{Q}$, there exists $m, n \in \mathbb{Z}$ (with $n \neq 0$) such that $a = m/n$. Assume, without loss of generality, that m/n is in lowest form (i.e. m and n have no common prime factors). Thus

$$a^2 = (m/n)^2 = m^2/n^2.$$

But since any prime factor of m^2 would also be a prime factor of m (and similarly for n^2 and n), we have m^2/n^2 is in lowest terms. So since $m^2/n^2 \in \mathbb{Z}$, we have $n^2 = 1$.

Techniques of proof I: Direct method

Theorem

Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Proof. Let a be a rational number satisfying $a^2 \in \mathbb{Z}$. Since $a \in \mathbb{Q}$, there exists $m, n \in \mathbb{Z}$ (with $n \neq 0$) such that $a = m/n$. Assume, without loss of generality, that m/n is in lowest form (i.e. m and n have no common prime factors). Thus

$$a^2 = (m/n)^2 = m^2/n^2.$$

But since any prime factor of m^2 would also be a prime factor of m (and similarly for n^2 and n), we have m^2/n^2 is in lowest terms. So since $m^2/n^2 \in \mathbb{Z}$, we have $n^2 = 1$. So $n = \pm 1$.

Techniques of proof I: Direct method

Theorem
Suppose that $a \in \mathbb{Q}$ and $a^2 \in \mathbb{Z}$. Then $a \in \mathbb{Z}$.

Proof. Let a be a rational number satisfying $a^2 \in \mathbb{Z}$. Since $a \in \mathbb{Q}$, there exists $m, n \in \mathbb{Z}$ (with $n \neq 0$) such that $a = m/n$. Assume, without loss of generality, that m/n is in lowest form (i.e. m and n have no common prime factors). Thus

$$a^2 = (m/n)^2 = m^2/n^2.$$

But since any prime factor of m^2 would also be a prime factor of m (and similarly for n^2 and n), we have m^2/n^2 is in lowest terms. So since $m^2/n^2 \in \mathbb{Z}$, we have $n^2 = 1$. So $n = \pm 1$. And thus $a = m/n \in \mathbb{Z}$, as desired. $\square$

Techniques of proof I: Direct method

Theorem

Let x and y be positive real numbers. If $y > x$, then $\frac{x+1}{y+1} > \frac{x}{y}$.

Techniques of proof I: Direct method

Theorem

Let x and y be positive real numbers. If $y > x$, then $\frac{x+1}{y+1} > \frac{x}{y}$.

Plan:

Start with "Let x and y be positive real numbers with $y > x$."

Goal: Conclude $\frac{x+1}{y+1} > \frac{x}{y}$.

Techniques of proof I: Direct method

Theorem

Let x and y be positive real numbers. If $y > x$, then $\frac{x+1}{y+1} > \frac{x}{y}$.

Plan:

Start with "Let x and y be positive real numbers with $y > x$."
Goal: Conclude $\frac{x+1}{y+1} > \frac{x}{y}$.
To try: Start with $\frac{x+1}{y+1} > \frac{x}{y}$ and manipulate until I see how I can get there (scratch work). Best if steps are "if and only if".

Techniques of proof I: Direct method

Theorem

Let x and y be positive real numbers. If $y > x$, then $\frac{x+1}{y+1} > \frac{x}{y}$.

Plan:

Start with "Let x and y be positive real numbers with $y > x$."
Goal: Conclude $\frac{x+1}{y+1} > \frac{x}{y}$.
To try: Start with $\frac{x+1}{y+1} > \frac{x}{y}$ and manipulate until I see how I can get there (scratch work). Best if steps are "if and only if".

Proof. Since $y > x$, we have

$$(x+1)y = xy + y > xy + x = (y+1)x.$$

Techniques of proof I: Direct method

Theorem

Let x and y be positive real numbers. If $y > x$, then $\frac{x+1}{y+1} > \frac{x}{y}$.

Plan:

Start with "Let x and y be positive real numbers with $y > x$."

Goal: Conclude $\frac{x+1}{y+1} > \frac{x}{y}$.

To try: Start with $\frac{x+1}{y+1} > \frac{x}{y}$ and manipulate until I see how I can get there (scratch work). Best if steps are "if and only if".

Proof. Since $y > x$, we have

$$(x+1)y = xy + y > xy + x = (y+1)x.$$

Since $y > 0$, we have $y(y+1) > 0$.

Techniques of proof I: Direct method

Theorem

Let x and y be positive real numbers. If $y > x$, then $\frac{x+1}{y+1} > \frac{x}{y}$.

Plan:

Start with "Let x and y be positive real numbers with $y > x$."
Goal: Conclude $\frac{x+1}{y+1} > \frac{x}{y}$.
To try: Start with $\frac{x+1}{y+1} > \frac{x}{y}$ and manipulate until I see how I can get there (scratch work). Best if steps are "if and only if".

Proof. Since $y > x$, we have

$$(x+1)y = xy + y > xy + x = (y+1)x.$$

Since $y > 0$, we have $y(y+1) > 0$. Thus, dividing both sides by $y(y+1)$ gives

$$\frac{x+1}{y+1} > \frac{x}{y},$$

as desired. □

Techniques of proof I: Direct method

Theorem

Let x and y be positive real numbers. If $y > x$, then $\frac{x+1}{y+1} > \frac{x}{y}$.

Proof. Since $y > x$, we have

$$(x+1)y = xy + y > xy + x = (y+1)x.$$

Since $y > 0$, we have $y(y+1) > 0$. Thus, dividing both sides by $y(y+1)$ gives

$$\frac{x+1}{y+1} > \frac{x}{y},$$

as desired. □

> **Warning!** The book's proofs are occasionally more like first drafts, since they use a lot of symbols, and not enough words. Observe the difference between the "proof" of Thm 20.4 and this proof.

Proving "if and only if"

Recall that "A if and only if B" is equivalent to
$(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Proving "if and only if"

Recall that "A if and only if B" is equivalent to $(A \Rightarrow B) \wedge (B \Rightarrow A)$. We also have

$$((A \Leftrightarrow B) \wedge (B \Leftrightarrow C)) \Rightarrow (A \Leftrightarrow C)$$

(you can check the truth table). Namely, a string of equivalencies proves and equivalency.

Proving "if and only if"

Recall that "A if and only if B" is equivalent to $(A \Rightarrow B) \wedge (B \Rightarrow A)$. We also have

$$((A \Leftrightarrow B) \wedge (B \Leftrightarrow C)) \Rightarrow (A \Leftrightarrow C)$$

(you can check the truth table). Namely, a string of equivalencies proves and equivalency.

So to prove "A if and only if B", you can either...

1. prove $A \Rightarrow B$ and $B \Rightarrow A$ (or any of the logically equivalent implications); or
2. find a string of equivalent statements $C_1, C_2, \ldots, C_\ell$ such that

$$A \Leftrightarrow C_1 \Leftrightarrow C_2 \Leftrightarrow \cdots \Leftrightarrow C_\ell \Leftrightarrow B.$$

(We'll see examples of both of these.)

Proving "if and only if"

Recall that "A if and only if B" is equivalent to $(A \Rightarrow B) \wedge (B \Rightarrow A)$. We also have

$$((A \Leftrightarrow B) \wedge (B \Leftrightarrow C)) \Rightarrow (A \Leftrightarrow C)$$

(you can check the truth table). Namely, a string of equivalencies proves and equivalency.

So to prove "A if and only if B", you can either...

1. prove $A \Rightarrow B$ and $B \Rightarrow A$ (or any of the logically equivalent implications); or
2. find a string of equivalent statements $C_1, C_2, \ldots, C_\ell$ such that
$$A \Leftrightarrow C_1 \Leftrightarrow C_2 \Leftrightarrow \cdots \Leftrightarrow C_\ell \Leftrightarrow B.$$

(We'll see examples of both of these.)

Similarly, if you want to show two numbers a and b are equal, you can either...

1. prove $a \leqslant b$ and $b \leqslant a$; or
2. find a string of equivalent values $c_1, c_2, \ldots, c_\ell$ such that
$$a = c_1 = c_2 = \cdots = c_\ell = b.$$

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

$$\text{for all } x \in X, \text{ we have } x \in Y.$$

This is

$$\forall x \in X (x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

$$\text{for all } x \in X, \text{ we have } x \in Y.$$

This is

$$\forall x \in X (x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

To prove $X \subseteq Y \ldots$

Start with "let $x \in X$." Goal: conclude $x \in Y$.

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

$$\text{for all } x \in X, \text{ we have } x \in Y.$$

This is

$$\forall x \in X(x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

To prove $X \subseteq Y$...

Start with "let $x \in X$." Goal: conclude $x \in Y$.

Theorem

Let X and Y be sets. Then $X \cap Y \subseteq X \cup Y$.

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

$$\text{for all } x \in X, \text{ we have } x \in Y.$$

This is

$$\forall x \in X (x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

To prove $X \subseteq Y$...

Start with "let $x \in X$." Goal: conclude $x \in Y$.

Theorem

Let X and Y be sets. Then $X \cap Y \subseteq X \cup Y$.

Proof.

Let $x \in X \cap Y$.

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

$$\text{for all } x \in X, \text{ we have } x \in Y.$$

This is

$$\forall x \in X(x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

To prove $X \subseteq Y \ldots$

Start with "let $x \in X$." Goal: conclude $x \in Y$.

Theorem

Let X and Y be sets. Then $X \cap Y \subseteq X \cup Y$.

Proof.

Let $x \in X \cap Y$. Then, by the definition of $X \cap Y$, we have $x \in X$ and $x \in Y$.

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

$$\text{for all } x \in X, \text{ we have } x \in Y.$$

This is

$$\forall x \in X (x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

To prove $X \subseteq Y \ldots$

Start with "let $x \in X$." Goal: conclude $x \in Y$.

Theorem

Let X and Y be sets. Then $X \cap Y \subseteq X \cup Y$.

Proof.

Let $x \in X \cap Y$. Then, by the definition of $X \cap Y$, we have $x \in X$ and $x \in Y$. In particular, $x \in X$, so that $(x \in X) \vee (x \in Y)$ holds.

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

$$\text{for all } x \in X, \text{ we have } x \in Y.$$

This is

$$\forall x \in X (x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

To prove $X \subseteq Y$...

Start with "let $x \in X$." Goal: conclude $x \in Y$.

Theorem

Let X and Y be sets. Then $X \cap Y \subseteq X \cup Y$.

Proof.

Let $x \in X \cap Y$. Then, by the definition of $X \cap Y$, we have $x \in X$ and $x \in Y$. In particular, $x \in X$, so that $(x \in X) \vee (x \in Y)$ holds. Thus $x \in X \cup Y$.

Proving subsets

Defn. Let X and Y be sets. We say X is a subset of Y means

for all $x \in X$, we have $x \in Y$.

This is

$$\forall x \in X(x \in Y), \quad \text{or, equivalently,} \quad x \in X \Rightarrow x \in Y.$$

To prove $X \subseteq Y \ldots$

Start with "let $x \in X$." Goal: conclude $x \in Y$.

Theorem

Let X and Y be sets. Then $X \cap Y \subseteq X \cup Y$.

Proof.

Let $x \in X \cap Y$. Then, by the definition of $X \cap Y$, we have $x \in X$ and $x \in Y$. In particular, $x \in X$, so that $(x \in X) \vee (x \in Y)$ holds. Thus $x \in X \cup Y$. Therefore $X \cap Y \subseteq X \cup Y$, as desired.

□

Proving two sets are equal

Defn. Let X and Y be sets. We say X is equal to Y means

$$x \in X \text{ if and only if } x \in Y.$$

This is

$$x \in X \Leftrightarrow x \in Y.$$

Proving two sets are equal

Defn. Let X and Y be sets. We say X is equal to Y means

$$x \in X \text{ if and only if } x \in Y.$$

This is

$$x \in X \Leftrightarrow x \in Y.$$

Theorem

Let X, Y, and Z be sets. Then

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Proving two sets are equal

Defn. Let X and Y be sets. We say X is equal to Y means

$$x \in X \text{ if and only if } x \in Y.$$

This is

$$x \in X \Leftrightarrow x \in Y.$$

Theorem

Let X, Y, and Z be sets. Then

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Proof.

Let $a \in X \cap (Y \cup Z)$. This means

$$a \in X \quad \text{and} \quad (a \in Y) \vee (a \in Z).$$

We have shown that this is (logically) equivalent to

$$a \in X \wedge a \in Y \quad \text{or} \quad a \in X \wedge a \in Z.$$

Proving two sets are equal

Defn. Let X and Y be sets. We say X is equal to Y means

$$x \in X \text{ if and only if } x \in Y.$$

This is

$$x \in X \Leftrightarrow x \in Y.$$

Theorem

Let X, Y, and Z be sets. Then

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Proof.

Let $a \in X \cap (Y \cup Z)$. This means

$$a \in X \quad \text{and} \quad (a \in Y) \vee (a \in Z).$$

We have shown that this is (logically) equivalent to

$$a \in X \wedge a \in Y \quad \text{or} \quad a \in X \wedge a \in Z.$$

By definition, this is equivalent to $a \in (X \cap Y) \cup (X \cap Z)$.

Proving two sets are equal

Defn. Let X and Y be sets. We say X is equal to Y means

$$x \in X \text{ if and only if } x \in Y.$$

This is

$$x \in X \Leftrightarrow x \in Y.$$

Theorem

Let X, Y, and Z be sets. Then

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Proof.

Let $a \in X \cap (Y \cup Z)$. This means

$$a \in X \quad \text{and} \quad (a \in Y) \vee (a \in Z).$$

We have shown that this is (logically) equivalent to

$$a \in X \wedge a \in Y \quad \text{or} \quad a \in X \wedge a \in Z.$$

By definition, this is equivalent to $a \in (X \cap Y) \cup (X \cap Z)$. In other words, $a \in X \cap (Y \cup Z)$ if and only if $a \in (X \cap Y) \cup (X \cap Z)$.

Proving two sets are equal

Defn. Let X and Y be sets. We say X is equal to Y means

$$x \in X \text{ if and only if } x \in Y.$$

This is

$$x \in X \Leftrightarrow x \in Y.$$

Theorem

Let X, Y, and Z be sets. Then

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Proof.

Let $a \in X \cap (Y \cup Z)$. This means

$$a \in X \quad \text{and} \quad (a \in Y) \vee (a \in Z).$$

We have shown that this is (logically) equivalent to

$$a \in X \wedge a \in Y \quad \text{or} \quad a \in X \wedge a \in Z.$$

By definition, this is equivalent to $a \in (X \cap Y) \cup (X \cap Z)$. In other words, $a \in X \cap (Y \cup Z)$ if and only if $a \in (X \cap Y) \cup (X \cap Z)$. So $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$, as desired. □

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 1 (Using definitions and logical equivalencies).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 1 (Using definitions and logical equivalencies).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

But, by "if and only if", we mean

$$x \in X \Rightarrow x \in Y \text{ and } x \in X \Leftarrow x \in Y.$$

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 1 (Using definitions and logical equivalencies).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

But, by "if and only if", we mean

$$x \in X \Rightarrow x \in Y \text{ and } x \in X \Leftarrow x \in Y.$$

By the definition of $\subseteq$, this ie equivalent to

$$X \subseteq Y \quad \text{and} \quad X \supseteq Y,$$

as desired.

$\square$

Proving two sets are equal

Theorem
Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Proving two sets are equal

Theorem
Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).
Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Thus, if $x \in X$, then $x \in Y$, implying $X \subseteq Y$.

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Thus, if $x \in X$, then $x \in Y$, implying $X \subseteq Y$. Similarly, if $x \in Y$, then $x \in X$, implying $X \supseteq Y$.

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Thus, if $x \in X$, then $x \in Y$, implying $X \subseteq Y$. Similarly, if $x \in Y$, then $x \in X$, implying $X \supseteq Y$.

Conversely, suppose that $X \subseteq Y$ and $X \supseteq Y$.

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Thus, if $x \in X$, then $x \in Y$, implying $X \subseteq Y$. Similarly, if $x \in Y$, then $x \in X$, implying $X \supseteq Y$.

Conversely, suppose that $X \subseteq Y$ and $X \supseteq Y$. Then if $x \in X$, we have $x \in Y$; and if $x \in Y$, then $x \in X$.

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Thus, if $x \in X$, then $x \in Y$, implying $X \subseteq Y$. Similarly, if $x \in Y$, then $x \in X$, implying $X \supseteq Y$.

Conversely, suppose that $X \subseteq Y$ and $X \supseteq Y$. Then if $x \in X$, we have $x \in Y$; and if $x \in Y$, then $x \in X$. So $x \in X$ if and only if $x \in Y$. Namely, $X = Y$. □

Proving two sets are equal

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

Proof 2 (Prove one direction at a time).

Suppose $X = Y$. This means

$$x \in X \text{ if and only if } x \in Y.$$

Thus, if $x \in X$, then $x \in Y$, implying $X \subseteq Y$. Similarly, if $x \in Y$, then $x \in X$, implying $X \supseteq Y$.

Conversely, suppose that $X \subseteq Y$ and $X \supseteq Y$. Then if $x \in X$, we have $x \in Y$; and if $x \in Y$, then $x \in X$. So $x \in X$ if and only if $x \in Y$. Namely, $X = Y$. □

From now on, you can use this theorem to prove two sets are equal!

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

(We'll show that $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$ and $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.)

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

(We'll show that $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$ and $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.)

Proof. First, let $x \in \bigcap_{n=1}^{\infty} A_n$. Then since x is in every A_n, then in particular, $x \in A_1 = \{1\}$. So $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$.

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

(We'll show that $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$ and $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.)

Proof. First, let $x \in \bigcap_{n=1}^{\infty} A_n$. Then since x is in every A_n, then in particular, $x \in A_1 = \{1\}$. So $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$.

Conversely, let $x \in \{1\}$, so that $x = 1$.

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

(We'll show that $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$ and $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.)

Proof. First, let $x \in \bigcap_{n=1}^{\infty} A_n$. Then since x is in every A_n, then in particular, $x \in A_1 = \{1\}$. So $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$.

Conversely, let $x \in \{1\}$, so that $x = 1$. Thus $x \in \{1, \ldots, n\} = A_n$ for all $n \in \mathbb{Z}_{>0}$.

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

(We'll show that $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$ and $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.)

Proof. First, let $x \in \bigcap_{n=1}^{\infty} A_n$. Then since x is in every A_n, then in particular, $x \in A_1 = \{1\}$. So $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$.

Conversely, let $x \in \{1\}$, so that $x = 1$. Thus $x \in \{1, \ldots, n\} = A_n$ for all $n \in \mathbb{Z}_{>0}$. Therefore $x \in \bigcap_{n=1}^{\infty} A_n$.

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

(We'll show that $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$ and $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.)

Proof. First, let $x \in \bigcap_{n=1}^{\infty} A_n$. Then since x is in every A_n, then in particular, $x \in A_1 = \{1\}$. So $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$.

Conversely, let $x \in \{1\}$, so that $x = 1$. Thus $x \in \{1, \ldots, n\} = A_n$ for all $n \in \mathbb{Z}_{>0}$. Therefore $x \in \bigcap_{n=1}^{\infty} A_n$. So $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.

Theorem

Let X and Y be sets. Then $X = Y$ if and only if $X \subseteq Y$ and $X \supseteq Y$.

For each $n \in \mathbb{Z}_{>0}$, pick a subset $A_n \subseteq \mathbb{Z}$. Define

$$\bigcap_{n=1}^{\infty} A_n = A_1 \cap A_2 \cap \cdots = \{x \in \mathbb{Z} \mid x \in A_n \text{ for all } n \in \mathbb{Z}_{>0}\}.$$

Ex. Prove that if $A_n = \{1, 2, \ldots, n\}$, then

$$\bigcap_{n=1}^{\infty} A_n = \{1\}.$$

(We'll show that $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$ and $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.)

Proof. First, let $x \in \bigcap_{n=1}^{\infty} A_n$. Then since x is in every A_n, then in particular, $x \in A_1 = \{1\}$. So $\bigcap_{n=1}^{\infty} A_n \subseteq \{1\}$.

Conversely, let $x \in \{1\}$, so that $x = 1$. Thus $x \in \{1, \ldots, n\} = A_n$ for all $n \in \mathbb{Z}_{>0}$. Therefore $x \in \bigcap_{n=1}^{\infty} A_n$. So $\bigcap_{n=1}^{\infty} A_n \supseteq \{1\}$.

Therefore $\bigcap_{n=1}^{\infty} A_n = \{1\}$, as desired.

Summary of strategies

To prove "A **if and only if** B", you can either...

1. prove $A \Rightarrow B$ and $B \Rightarrow A$ (or any of the logically equivalent implications); or
2. find a string of equivalent statements $C_1, C_2, \ldots, C_\ell$ such that
$$A \Leftrightarrow C_1 \Leftrightarrow C_2 \Leftrightarrow \cdots \Leftrightarrow C_\ell \Leftrightarrow B.$$

To prove two **numbers** a **and** b **are equal**, you can either...

1. prove $a \leqslant b$ and $b \leqslant a$; or
2. find a string of equivalent values $c_1, c_2, \ldots, c_\ell$ such that
$$a = c_1 = c_2 = \cdots = c_\ell = b.$$

To prove two **sets** X **and** Y **are equal**, you can either...

1. prove $X \subseteq Y$ and $Y \subseteq X$; or
2. find a string sets $Z_1, Z_2, \ldots, Z_\ell$ such that
$$X = Z_1 = Z_2 = \cdots = Z_\ell = Y.$$

Common mistakes

1. Assuming your desired conclusion.
2. Taking square roots badly.
3. Dividing by zero.
4. Forgetting things might be negative.
5. Using examples to deduce “for all” statements.

Error 1: Assuming your desired conclusion.

Claim: $-1 = 1$

Error 1: Assuming your desired conclusion.

Claim: $-1 = 1$

Non-proof.

If $-1 = 1$, then

$$(-1)^2 = (1)^2$$

Error 1: Assuming your desired conclusion.

Claim: $-1 = 1$

Non-proof.

If $-1 = 1$, then

$$(-1)^2 = (1)^2, \qquad \text{so that} \qquad 1 = 1,$$

which is true. □

Error 1: Assuming your desired conclusion.

Claim: $-1 = 1$

Non-proof.

If $-1 = 1$, then

$$(-1)^2 = (1)^2, \qquad \text{so that} \qquad 1 = 1,$$

which is true. □

What went wrong:

We proved that

$$\text{“}-1 = 1 \Rightarrow 1 = 1\text{”},$$

which is true (F $\Rightarrow$ T is true)!

We **did not** show that $-1 = 1$.

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$a^2 + b^2 \geqslant 2ab \Rightarrow a^2 - 2ab + b^2 \geqslant 0$$

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$a^2 + b^2 \geqslant 2ab \Rightarrow a^2 - 2ab + b^2 \geqslant 0 \Rightarrow (a - b)^2 \geqslant 0.$$

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$a^2 + b^2 \geqslant 2ab \Rightarrow a^2 - 2ab + b^2 \geqslant 0 \Rightarrow (a-b)^2 \geqslant 0.$$

The last inequality is true, since the square of a number is always non-negative. So $a^2 + b^2 \geqslant 2ab$.

$\square$

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$\boxed{a^2 + b^2 \geqslant 2ab \Rightarrow} \; a^2 - 2ab + b^2 \geqslant 0 \Rightarrow (a-b)^2 \geqslant 0.$$

The last inequality is true, since the square of a number is always non-negative. So $a^2 + b^2 \geqslant 2ab$.

□

What went wrong:

We wanted to show

$$a, b \in \mathbb{R} \quad \Rightarrow \quad a^2 + b^2 \geqslant 2ab.$$

What we actually showed was

$$(a, b \in \mathbb{R}) \wedge (a^2 + b^2 \geqslant 2ab) \quad \Rightarrow \quad (a-b)^2 \geqslant 0.$$

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$\boxed{a^2 + b^2 \geqslant 2ab \Rightarrow} \; a^2 - 2ab + b^2 \geqslant 0 \Rightarrow (a-b)^2 \geqslant 0.$$

The last inequality is true, since the square of a number is always non-negative. So $a^2 + b^2 \geqslant 2ab$.

$\square$

What went wrong:

We wanted to show

$$a, b \in \mathbb{R} \quad \Rightarrow \quad a^2 + b^2 \geqslant 2ab.$$

What we actually showed was

$$(a, b \in \mathbb{R}) \wedge (a^2 + b^2 \geqslant 2ab) \quad \Rightarrow \quad (a-b)^2 \geqslant 0.$$

Fortunately, we can fix this!

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$a^2 + b^2 \geqslant 2ab \Rightarrow a^2 - 2ab + b^2 \geqslant 0 \Rightarrow (a-b)^2 \geqslant 0.$$

The last inequality is true, since the square of a number is always non-negative. So $a^2 + b^2 \geqslant 2ab$.

□

Proof.

Since the square of a number is always non-negative, we have

$$0 \leqslant (a-b)^2$$

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$a^2 + b^2 \geqslant 2ab \Rightarrow a^2 - 2ab + b^2 \geqslant 0 \Rightarrow (a-b)^2 \geqslant 0.$$

The last inequality is true, since the square of a number is always non-negative. So $a^2 + b^2 \geqslant 2ab$.

□

Proof.

Since the square of a number is always non-negative, we have

$$0 \leqslant (a-b)^2 = a^2 - 2ab + b^2.$$

Error 1: Assuming your desired conclusion.

Claim: If a and b are real numbers, then $a^2 + b^2 \geqslant 2ab$.

Non-proof.

We have

$$a^2 + b^2 \geqslant 2ab \Rightarrow a^2 - 2ab + b^2 \geqslant 0 \Rightarrow (a - b)^2 \geqslant 0.$$

The last inequality is true, since the square of a number is always non-negative. So $a^2 + b^2 \geqslant 2ab$.

□

Proof.

Since the square of a number is always non-negative, we have

$$0 \leqslant (a - b)^2 = a^2 - 2ab + b^2.$$

So, subtracting $2ab$ from both sides, we get

$$a^2 + b^2 \geqslant 2ab.$$

as desired.

□

Error 1: Assuming your desired conclusion.

As a **problem-solving strategy**, it's effective to assume the thing you want to show, and work backwards.

This is your **scratch work**.

But when you actually go to write the proof, you have to make sure you can work forwards!

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root. Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x + 1$ are given by $x = 1$ and $x = -2$.

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x+1$ are given by $x = 1$ and $x = -2$.

Non-proof.

If $\sqrt{x+3} = x+1$, then squaring both sides gives

$$x + 3 = (x+1)^2$$

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x + 1$ are given by $x = 1$ and $x = -2$.

Non-proof.

If $\sqrt{x+3} = x + 1$, then squaring both sides gives

$$x + 3 = (x + 1)^2 = x^2 + 2x + 1.$$

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x+1$ are given by $x = 1$ and $x = -2$.

Non-proof.

If $\sqrt{x+3} = x+1$, then squaring both sides gives

$$x + 3 = (x+1)^2 = x^2 + 2x + 1.$$

So

$$0 = x^2 + x - 2$$

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x+1$ are given by $x = 1$ and $x = -2$.

Non-proof.
If $\sqrt{x+3} = x+1$, then squaring both sides gives

$$x + 3 = (x+1)^2 = x^2 + 2x + 1.$$

So

$$0 = x^2 + x - 2 = (x-1)(x+2).$$

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x+1$ are given by $x = 1$ and $x = -2$.

Non-proof.

If $\sqrt{x+3} = x+1$, then squaring both sides gives

$$x + 3 = (x+1)^2 = x^2 + 2x + 1.$$

So

$$0 = x^2 + x - 2 = (x-1)(x+2).$$

So $x = 1$ or $x = -2$. $\square$

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x + 1$ are given by $x = 1$ and $x = -2$.

Non-proof.

If $\sqrt{x+3} = x + 1$, then **squaring both sides** gives

$$x + 3 = (x + 1)^2 = x^2 + 2x + 1.$$

So

$$0 = x^2 + x - 2 = (x - 1)(x + 2).$$

So $x = 1$ or $x = -2$. □

What went wrong:

When we squared both sides, we threw in extra solutions!

Error 2: Taking square roots badly.

Our convention is to fix $\sqrt{x}$ to mean the *positive* root.
Namely, if $y^2 = x$, then $y = \pm\sqrt{x}$.

Claim. The solutions to $\sqrt{x+3} = x + 1$ are given by $x = 1$ and $x = -2$.

Non-proof.

If $\sqrt{x+3} = x + 1$, then **squaring both sides** gives

$$x + 3 = (x + 1)^2 = x^2 + 2x + 1.$$

So

$$0 = x^2 + x - 2 = (x - 1)(x + 2).$$

So $x = 1$ or $x = -2$. □

What went wrong:

When we squared both sides, we threw in extra solutions!
We actually found solutions to

$$\sqrt{x+3} = x + 1 \quad \text{and} \quad -\sqrt{x+3} = x + 1.$$

Error 3: Dividing by zero.

Claim. $1 = 2$.

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers.

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers. Then, multiplying both sides by a, we get

$$a^2 = ab.$$

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers. Then, multiplying both sides by a, we get

$$a^2 = ab.$$

Subtracting b^2 from both sides gives

$$ab - b^2 = a^2 - b^2$$

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers. Then, multiplying both sides by a, we get

$$a^2 = ab.$$

Subtracting b^2 from both sides gives

$$ab - b^2 = a^2 - b^2, \quad \text{so that} \quad b(a - b) = (a + b)(a - b).$$

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers. Then, multiplying both sides by a, we get

$$a^2 = ab.$$

Subtracting b^2 from both sides gives

$$ab - b^2 = a^2 - b^2, \quad \text{so that} \quad b(a-b) = (a+b)(a-b).$$

Cancelling $(a - b)$, we get

$$b = a + b.$$

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers. Then, multiplying both sides by a, we get

$$a^2 = ab.$$

Subtracting b^2 from both sides gives

$$ab - b^2 = a^2 - b^2, \quad \text{so that} \quad b(a-b) = (a+b)(a-b).$$

Cancelling $(a-b)$, we get

$$b = a + b.$$

Therefore, since $a = b$, we can substitute back in to get

$$b = a + b = b + b = 2b.$$

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers. Then, multiplying both sides by a, we get

$$a^2 = ab.$$

Subtracting b^2 from both sides gives

$$ab - b^2 = a^2 - b^2, \quad \text{so that} \quad b(a-b) = (a+b)(a-b).$$

Cancelling $(a - b)$, we get

$$b = a + b.$$

Therefore, since $a = b$, we can substitute back in to get

$$b = a + b = b + b = 2b. \quad \text{So, dividing by } b \text{ gives} \quad 1 = 2,$$

as desired. □

Error 3: Dividing by zero.

Claim. $1 = 2$.

Non-proof.

Let $a = b$ be real numbers. Then, multiplying both sides by a, we get

$$a^2 = ab.$$

Subtracting b^2 from both sides gives

$$ab - b^2 = a^2 - b^2, \quad \text{so that} \quad b(a-b) = (a+b)(a-b).$$

Cancelling $(a-b)$, we get

$$b = a + b.$$

Therefore, since $a = b$, we can substitute back in to get

$$b = a + b = b + b = 2b. \quad \text{So, dividing by } b \text{ gives} \quad 1 = 2,$$

as desired. □

Error 4: Forgetting things might be negative

Claim. $-1 > 1$.

Error 4: Forgetting things might be negative

Claim. $-1 > 1$.

Non-proof.

Let $x = -1$.

Error 4: Forgetting things might be negative

Claim. $-1 > 1$.

Non-proof.

Let $x = -1$. Then $x < 1$.

Error 4: Forgetting things might be negative

Claim. $-1 > 1$.

Non-proof.

Let $x = -1$. Then $x < 1$. So, since $a > b$ implies $1/a < 1/b$, we get

$$1/x > 1/1 = 1.$$

Error 4: Forgetting things might be negative

Claim. $-1 > 1$.

Non-proof.

Let $x = -1$. Then $x < 1$. So, since $a > b$ implies $1/a < 1/b$, we get

$$1/x > 1/1 = 1.$$

But since $1/x = 1/-1 = -1$, we have $-1 > 1$. $\square$

Error 4: Forgetting things might be negative

Claim. $-1 > 1$.

Non-proof.

Let $x = -1$. Then $x < 1$. So, since $a > b$ **implies** $1/a < 1/b$, we get

$$1/x > 1/1 = 1.$$

But since $1/x = 1/-1 = -1$, we have $-1 > 1$. □

Error 4: Forgetting things might be negative

Claim. $-1 > 1$.

Non-proof.

Let $x = -1$. Then $x < 1$. So, since $a > b$ **implies** $1/a < 1/b$, we get

$$1/x > 1/1 = 1.$$

But since $1/x = 1/-1 = -1$, we have $-1 > 1$. $\square$

Lesson: When doing algebraic manipulation, be careful not to assume things are positive (unless that's part of the assumptions). In particular, it's possible for $-x$ to be positive (if x was negative).

Error 5: Using examples badly

JUST WHEN YOU THOUGHT
YOU UNDERSTOOD THE PATTERN

$$\int_0^\infty \frac{\sin t}{t}\,dt = \frac{\pi}{2}$$

$$\int_0^\infty \frac{\sin t}{t}\,\frac{\sin(t/101)}{t/101}\,dt = \frac{\pi}{2}$$

$$\int_0^\infty \frac{\sin t}{t}\,\frac{\sin(t/101)}{t/101}\,\frac{\sin(t/201)}{t/201}\,dt = \frac{\pi}{2}$$

$$\int_0^\infty \frac{\sin t}{t}\,\frac{\sin(t/101)}{t/101}\,\frac{\sin(t/201)}{t/201}\,\frac{\sin(t/301)}{t/301}\,dt = \frac{\pi}{2}$$

and so on... but not forever! The formula

$$\int_0^\infty \frac{\sin t}{t}\,\frac{\sin(t/101)}{t/101}\,\frac{\sin(t/201)}{t/201}\cdots\frac{\sin(t/(100n+1))}{t/(100n+1)}\,dt = \frac{\pi}{2}$$

holds whenever $n < 9.8 \cdot 10^{42}$. But it eventually fails! It's *false* for all $n > 7.4 \cdot 10^{43}$.

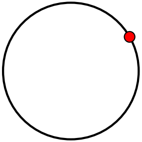
See link to "Patterns that eventually fail" on course website.

Claim: Draw n unique points on the circle, such that when you connect them with line segments, no more than two lines cross at any point. Then this will divide the circle into 2^{n-1} regions.

Claim: Draw n unique points on the circle, such that when you connect them with line segments, no more than two lines cross at any point. Then this will divide the circle into 2^{n-1} regions.

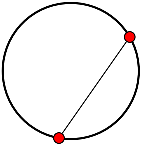
Non-proof. Let's do some examples:

$n = 1$:



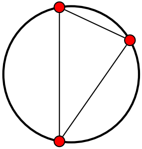
1 region

$n = 2$:



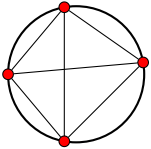
2 regions

$n = 3$:



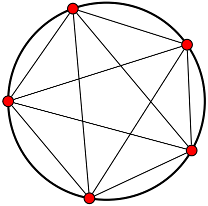
4 regions

$n = 4$:



8 regions

$n = 5$:



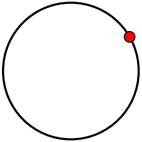
16 regions

Since this works for $n = 1, 2, 3, 4$, and 5, it must be true! □

Claim: Draw n unique points on the circle, such that when you connect them with line segments, no more than two lines cross at any point. Then this will divide the circle into 2^{n-1} regions.

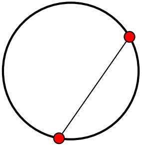
Non-proof. Let's do some examples:

$n = 1$:



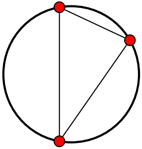
1 region

$n = 2$:



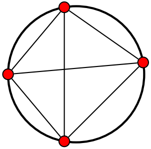
2 regions

$n = 3$:



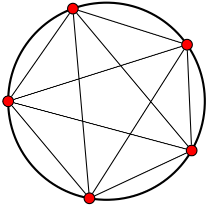
4 regions

$n = 4$:



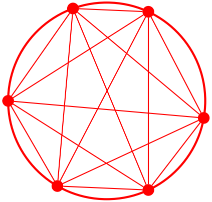
8 regions

$n = 5$:



16 regions

$n = 6$:



31 regions!

Since this works for $n = 1, 2, 3, 4$, and 5, it must be true! □