Indirect Proofs

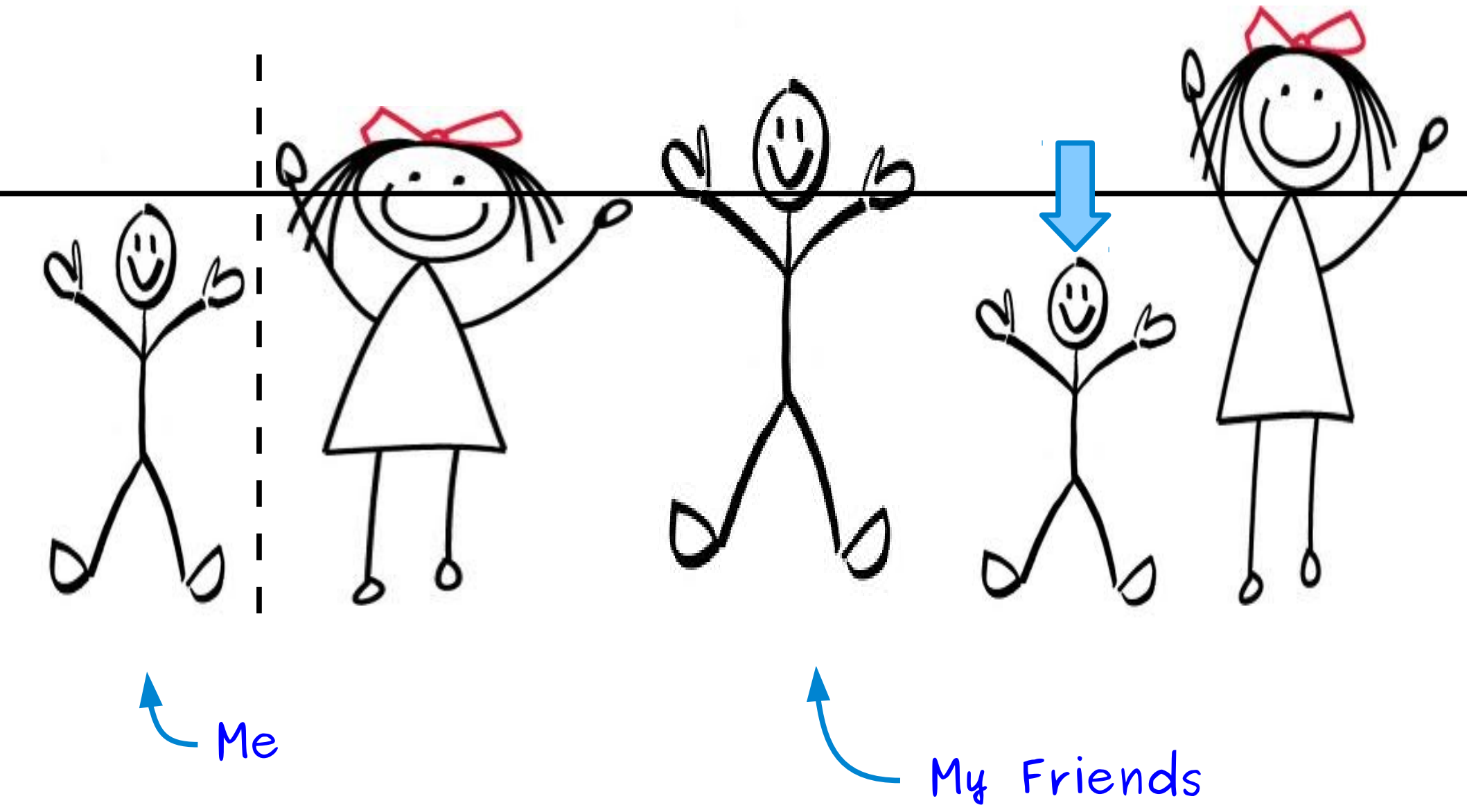
Logical Negation

Negations

- A ***proposition*** is a statement that is either true or false.
- Some examples:
  - If n is an even integer, then n^2 is an even integer.
  - $\varnothing = \mathbb{R}$.
- The ***negation*** of a proposition X is a proposition that is true when X is false and is false when X is true.
- For example, consider the proposition "it is snowing outside."
  - Its negation is "it is not snowing outside."
  - Its negation is *not* "it is sunny outside." ⚠

How do you find the negation of a statement?

“All My Friends Are Taller Than Me”



The negation of the ***universal*** statement

Every *P* is a *Q*

is the ***existential*** statement

There is a *P* that is not a *Q*.

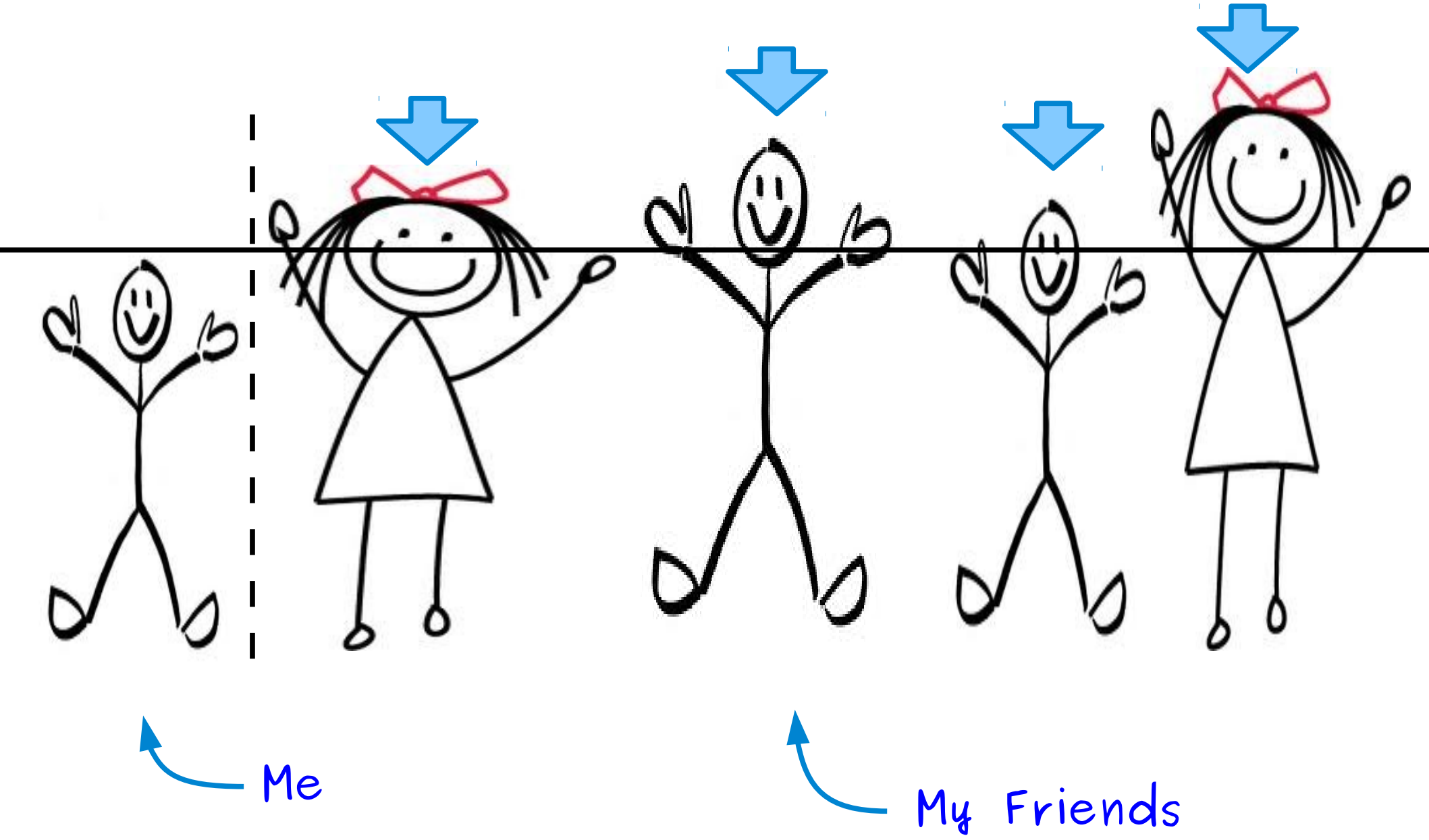
The negation of the ***universal*** statement

For all x, $P(x)$ is true.

is the ***existential*** statement

There exists an x where $P(x)$ is false.

“Some Friend Is Shorter Than Me”



The negation of the ***existential*** statement

There exists a *P* that is a *Q*

is the ***universal*** statement

Every *P* is not a *Q*.

The negation of the ***existential*** statement

There exists an x where $P(x)$ is true

is the ***universal*** statement

For all x, $P(x)$ is false.

Your Turn!

- What's the negation of the following statement?

"Every brown dog loves every orange cat."

Your Turn!

- What's the negation of the following statement?

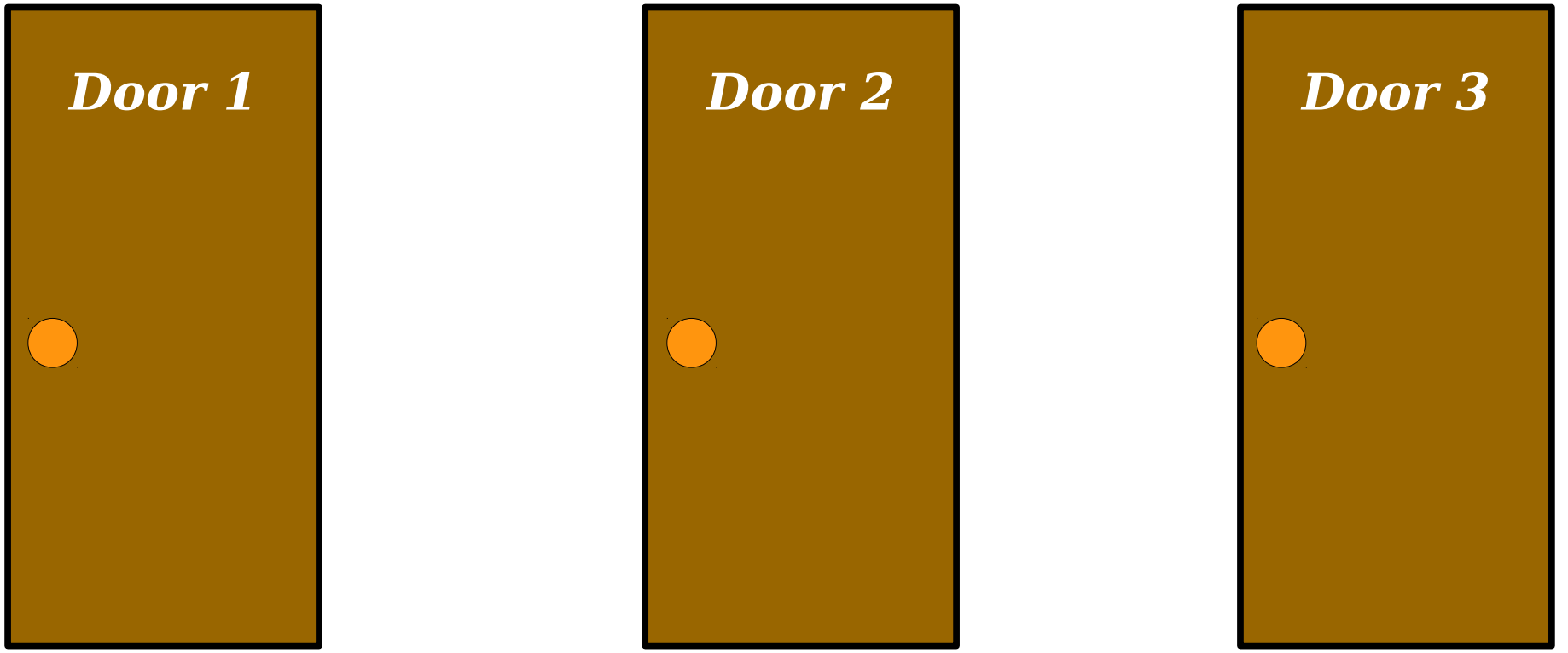
"Every brown dog loves every orange cat."

- Answer:

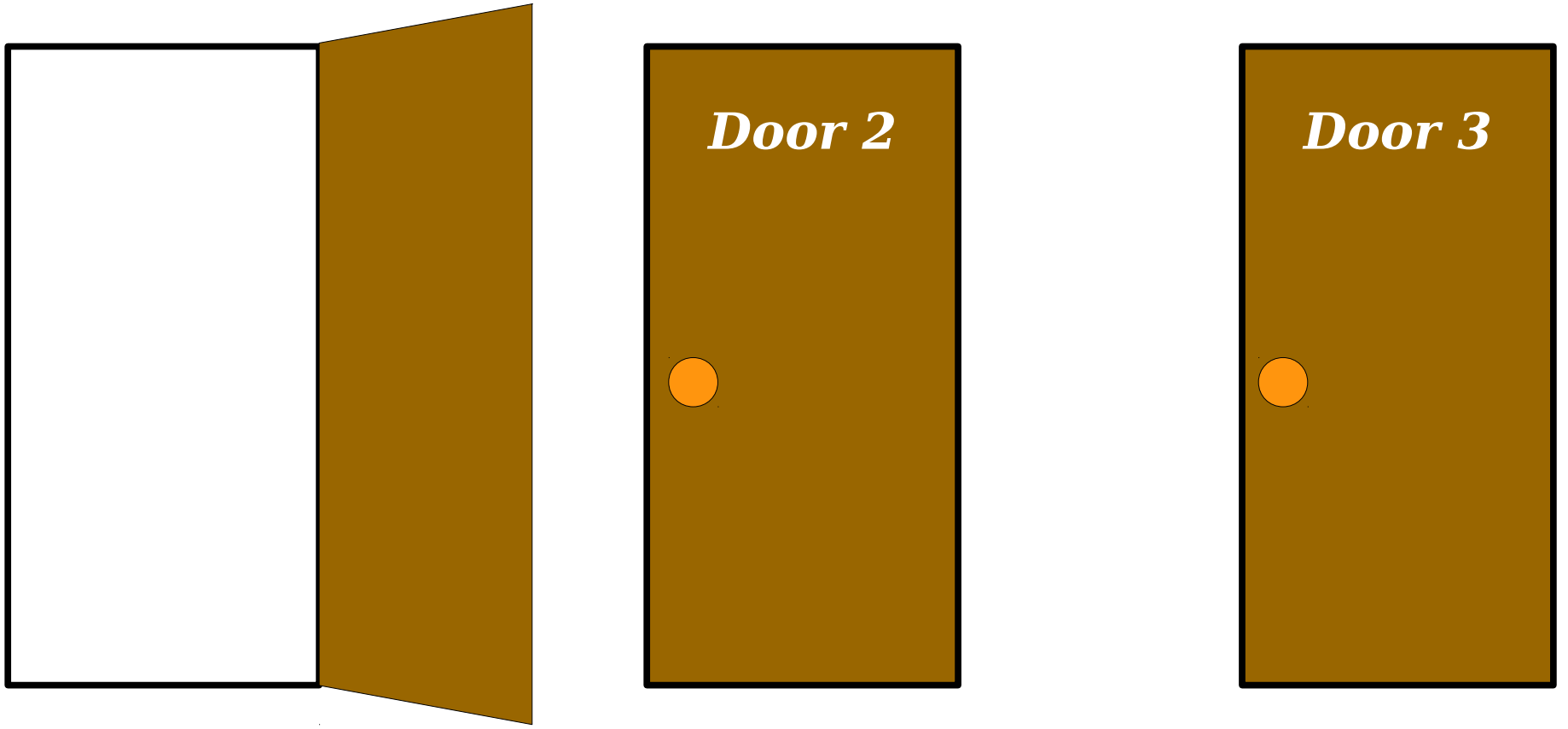
"There is a brown dog that doesn't love some orange cat"

Proof by Contradiction

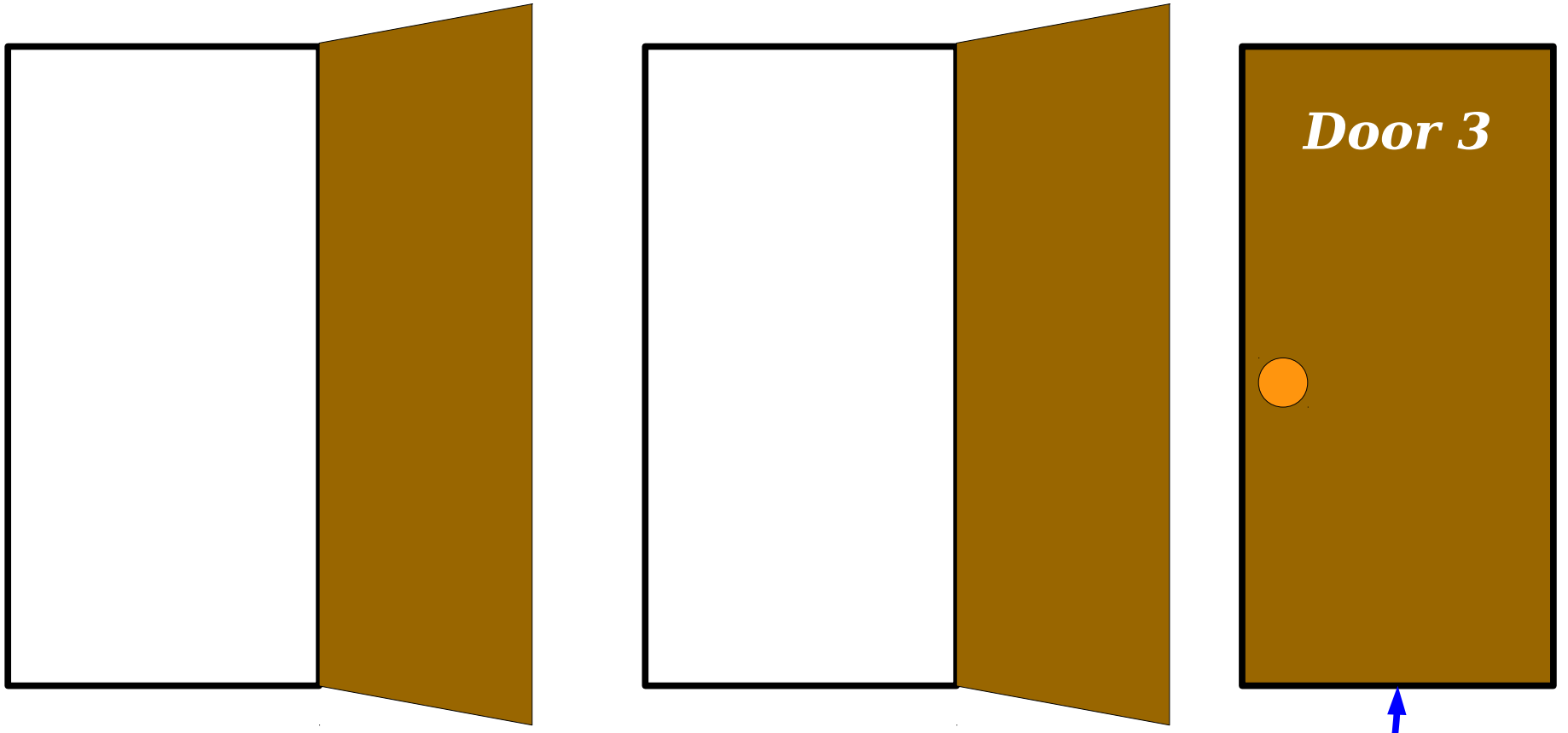
There's something hidden behind one of these doors. Which door is it hidden behind?



There's something hidden behind one of these doors. Which door is it hidden behind?

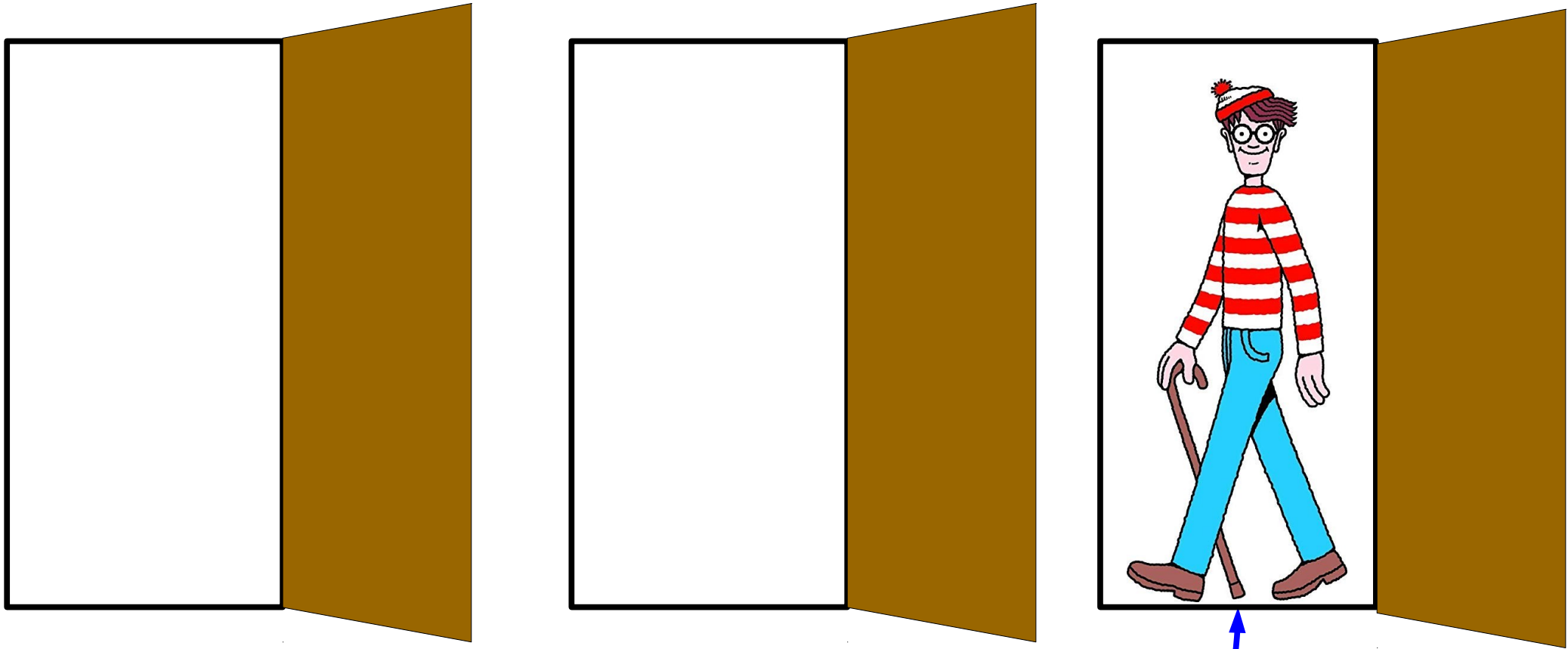


There's something hidden behind one of these doors. Which door is it hidden behind?



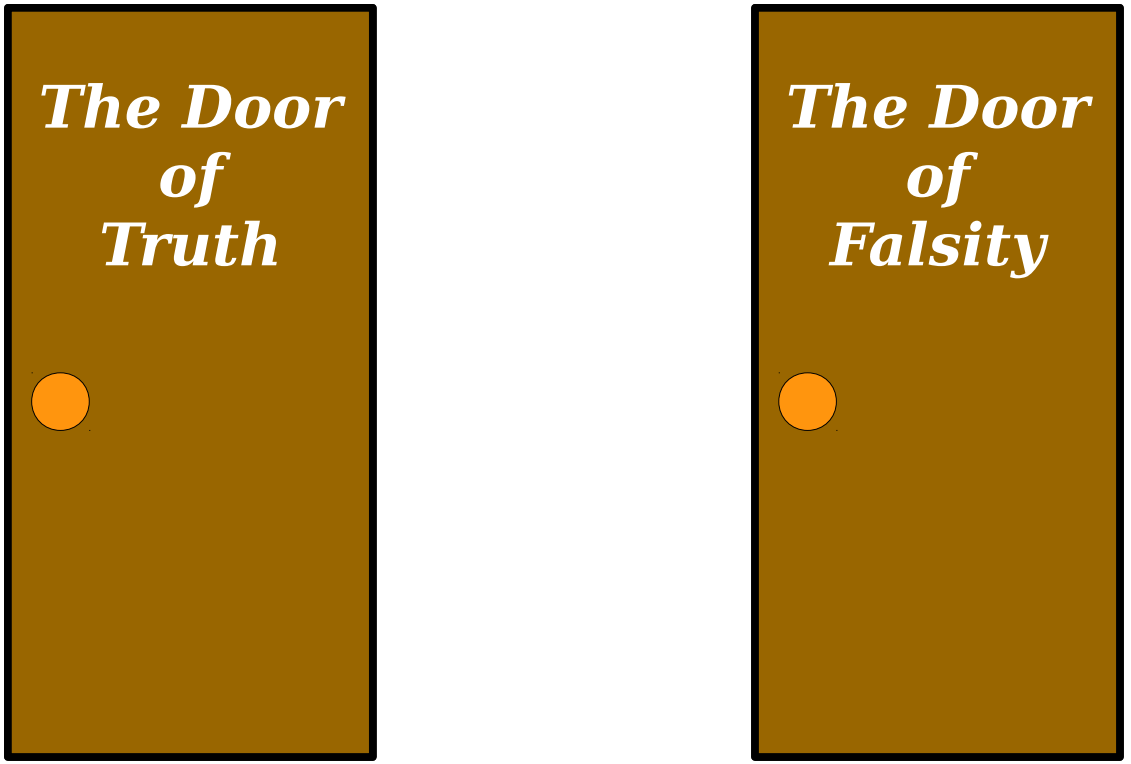
Even without opening this door, we know whatever is hidden has to be here.

There's something hidden behind one of these doors. Which door is it hidden behind?

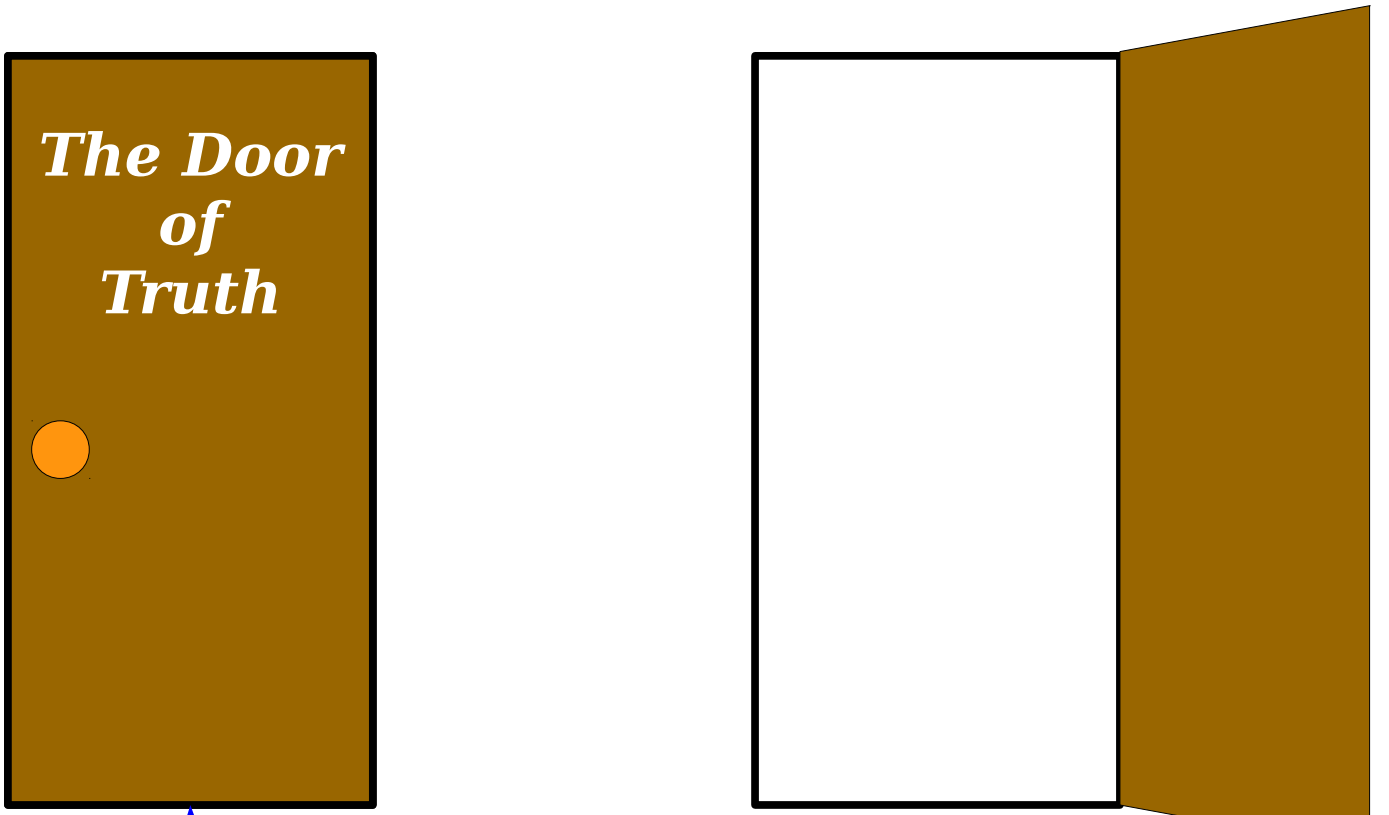


Even without opening this door, we know whatever is hidden has to be here.

Every statement in mathematics is either true or false.
*If statement P is **not false**, what does that tell you?*

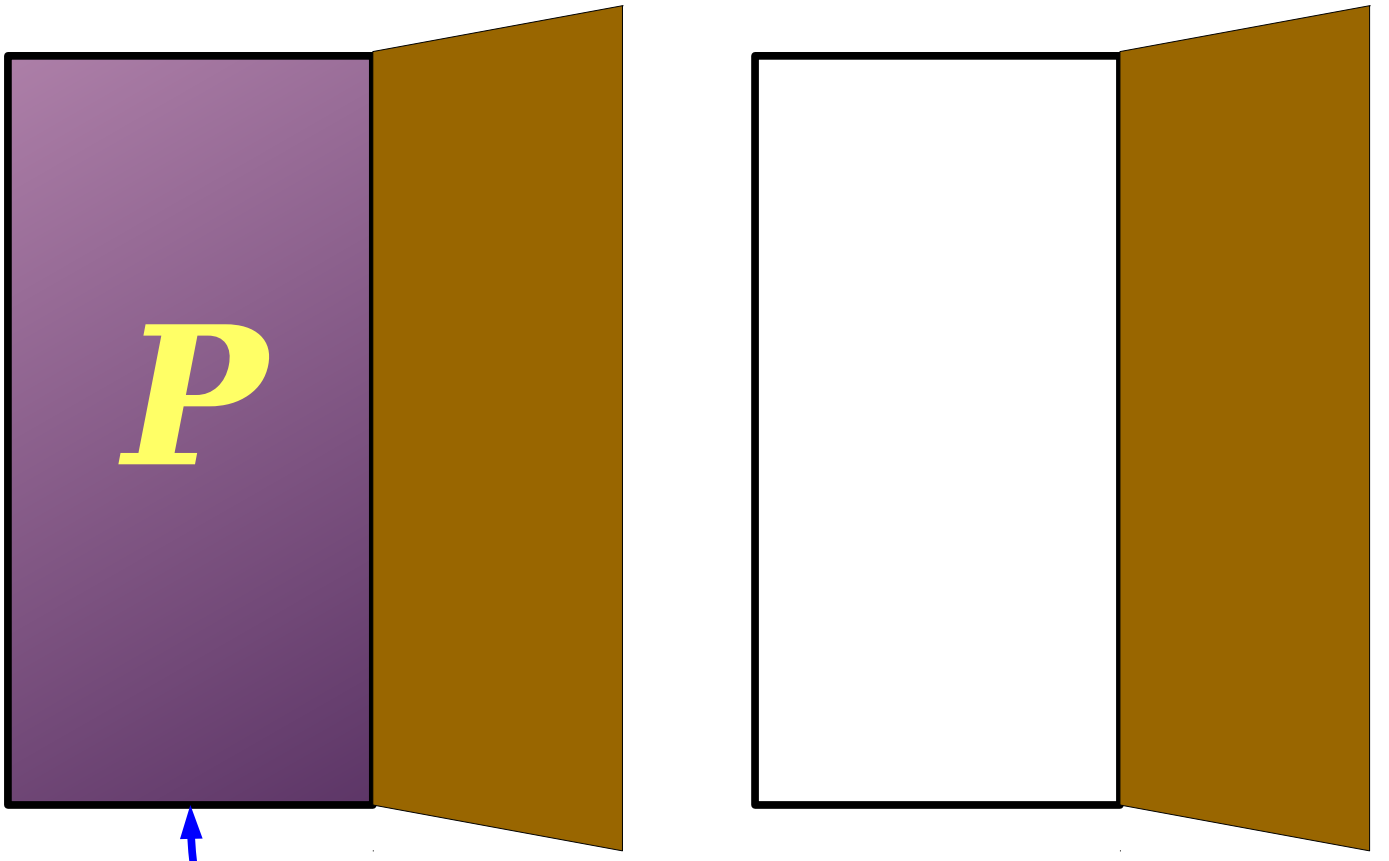


Every statement in mathematics is either true or false.
*If statement P is **not false**, what does that tell you?*



Even without opening this door, we know P has to be here.

Every statement in mathematics is either true or false.
*If statement P is **not false**, what does that tell you?*



Even without opening this door, we know P has to be here.

A ***proof by contradiction*** shows that some statement P is true by showing that P isn't false.

Proof by Contradiction

- ***Key Idea:*** Prove a statement P is true by showing that it isn't false.
- First, assume that P is false. The goal is to show that this assumption is silly.
- Next, show this leads to an impossible result.
  - For example, we might have that $1 = 0$, that $x \in S$ and $x \notin S$, that a number is both even and odd, etc.
- Finally, conclude that since P can't be false, we know that P must be true.

An Example: ***Set Cardinalities***

Set Cardinalities

- We've seen sets of many different cardinalities:
  - $|\varnothing| = 0$
  - $|\{1, 2, 3\}| = 3$
  - $|\{ n \in \mathbb{N} \mid n < 137 \}| = 137$
  - $|\mathbb{N}| = \aleph_0$.
  - $|\wp(\mathbb{N})| > |\mathbb{N}|$
- These span from the finite up through the infinite.
- ***Question:*** Is there a "largest" set? That is, is there a set that's bigger than every other set?

Theorem: There is no largest set.

Theorem: There is no largest set.

Proof:

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction, we're going to assume its negation.

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction, we're going to assume its negation.

What is the negation of the statement "there is no largest set?"

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction, we're going to assume its negation.

What is the negation of the statement "there is no largest set?"

One option: "there *is* a largest set."

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

To prove this statement by contradiction, we're going to assume its negation.

What is the negation of the statement "there is no largest set?"

One option: "there *is* a largest set."

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Notice that we're announcing

1. that this is a proof by contradiction, and
2. what, specifically, we're assuming.

This helps the reader understand where we're going. Remember – proofs are meant to be read by other people!

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

The three key pieces:

1. Say that the proof is by contradiction.
2. Say what you are assuming is the negation of the statement to prove.
3. Say you have reached a contradiction and what the contradiction means.

In CS103, please include all these steps in your proofs!

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Time-Out for Announcements!

Readings for Today

- On the course website we have some information you should look over.
- First is the ***Proofwriting Checklist***. It contains information about style expectations for proofs. We'll be using this when grading, so be sure to read it over.
- We've put together a ***Guide to Proofs*** and a ***Guide to Proofs on Sets*** that summarize the proofwriting techniques from Wednesday and today.
- Next is the ***Guide to Office Hours***, which talks about how our office hours work and how to make the most effective use of them.
- Finally is the ***Guide to LaTeX***, which explains how to use LaTeX to typeset your problem sets in a way that's so beautiful it will bring tears to your eyes.

Problem Set One

- Problem Set Zero was due at 4:00PM today.
- Problem Set One goes out today. It's due next Friday at 4:00PM.
  - Explore the language of set theory and better intuit how it works.
  - Learn more about the structure of mathematical proofs.
  - Write your first "freehand" proofs based on your experiences.
- As always, reach out if you have any questions!

Submitting Assignments

- All assignments should be submitted through GradeScope.
  - The programming portion of the assignment gets submitted separately from the written component.
  - The written component ***must*** be typed up; handwritten solutions don’t scan well and get mangled in GradeScope.
- Because submission times are recorded automatically, we're strict about the submission deadlines.
  - ***Very good idea:*** Leave at least two hours buffer time for your first assignment submission, just in case something goes wrong.
  - ***Very bad idea:*** Wait until the last minute to submit.
- However, we are pretty generous with how we grade. Your score on the problem sets is the square root of your raw score. So an 81% maps to a 90%, a 50% maps to a 71%, etc. This gives a huge boost even if you need to turn something in that isn’t done.

Getting Help

- It is ***completely normal*** in this class to need to get help from time to time.
- Feel free to ask clarifying and conceptual questions on EdStem.
- Need more structured help? We have office hours! Feel free to stop on by.
  - Check out the online “Guide to Office Hours” for more information about how our office hours system works.
  - The OH calendar is available on the course website.

Back to CS103!

If n is an even integer, then n^2 is an even integer.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If n is an even integer, then n^2 is an even integer.

This part of the implication is called the *antecedent*.

This part of the implication is called the *consequent*.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If n is an even integer, then n^2 is an even integer.

If m and n are odd integers, then $m+n$ is even.

If you like the way you look that much,
then you should go and love yourself.

An ***implication*** is a statement of the form
"If P is true, then Q is true."

What Implications Mean

“If there's a rainbow in the sky, then it's raining somewhere.”

- In mathematics, implication is directional.
  - The above statement doesn't mean that if it's raining somewhere, there has to be a rainbow.
- In mathematics, implications only say something about the consequent when the antecedent is true.
  - If there's no rainbow, it doesn't mean there's no rain.
- In mathematics, implication says nothing about causality.
  - Rainbows do not cause rain.

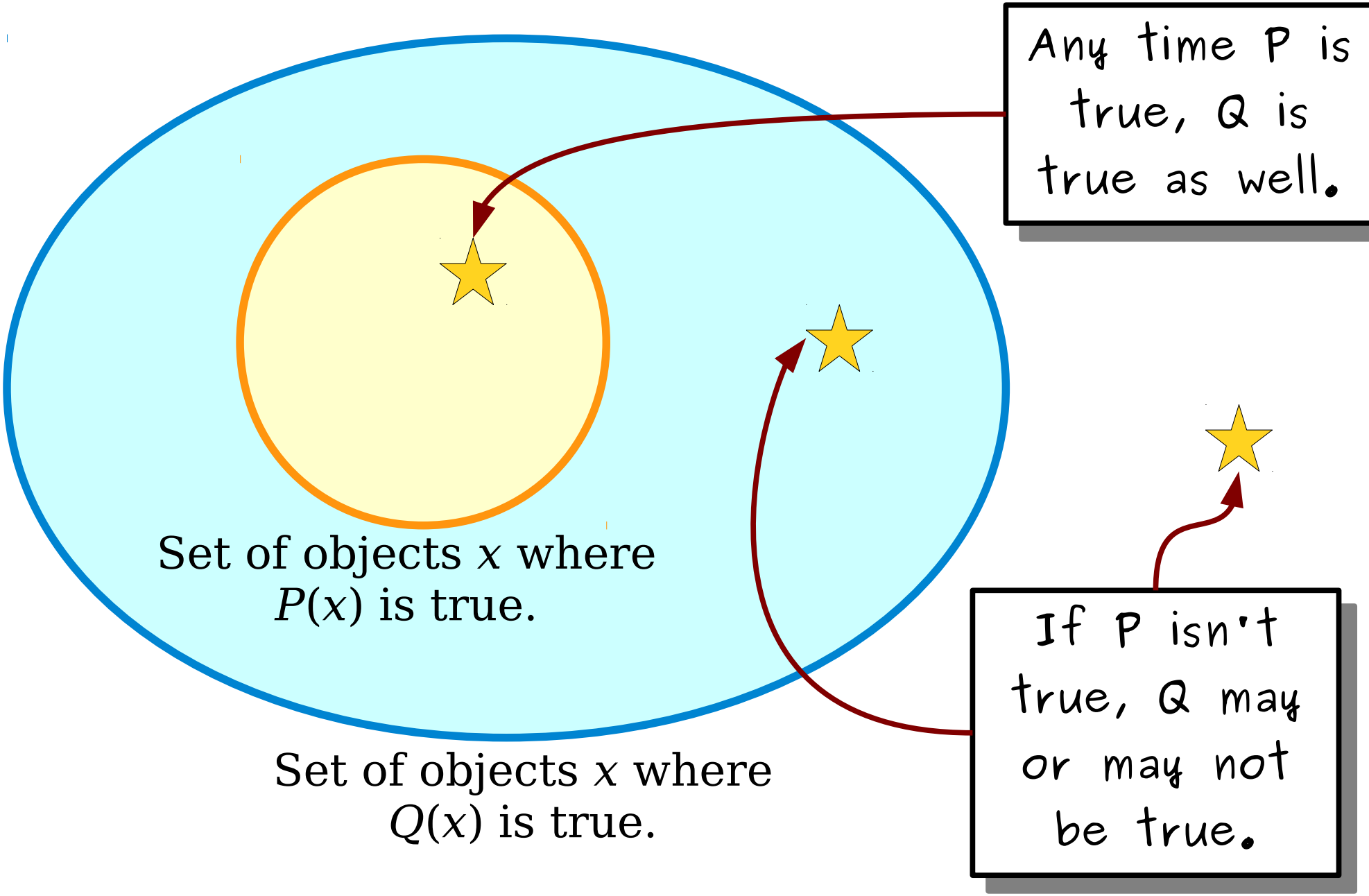
What Implications Mean

- In mathematics, a statement of the form

  For any x, if $P(x)$ is true, then $Q(x)$ is true

  means that any time you find an object x where $P(x)$ is true, you will see that $Q(x)$ is also true (for that same x).
- There is no discussion of causation here. It simply means that if you find that $P(x)$ is true, you'll find that $Q(x)$ is also true.

Implication, Diagrammatically

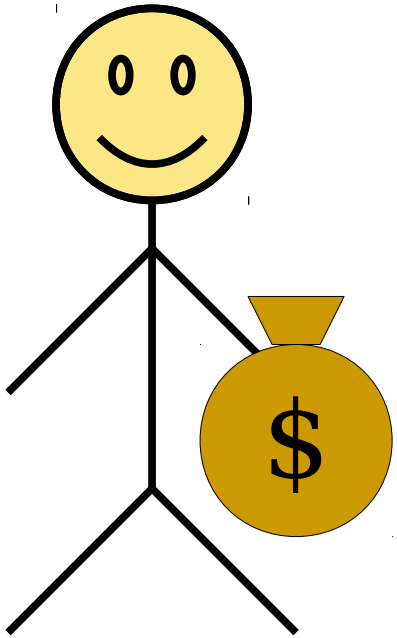


How do you negate an implication?

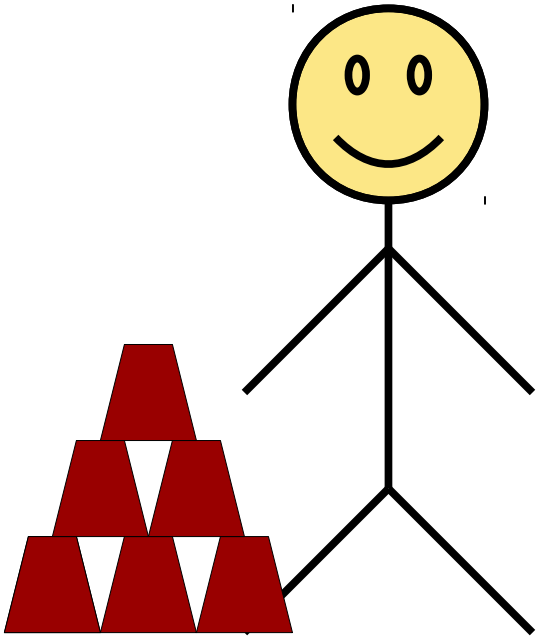

Story Time!

Ancient Contract:

If Nanni pays money to Ea-Nasir, then
Ea-Nasir will give Nanni quality copper ingots.



Nanni



Ea-Nasir

Question: What has to happen for this contract to be broken?

Ancient Contract:

If Nanni pays money to Ea-Nasir, then
Ea-Nasir will give Nanni quality copper ingots.

Question: What has to happen for this contract to be broken?
Answer: Nanni pays Ea-Nasir and doesn't get quality copper ingots.

The negation of the statement

"For any x, if $P(x)$ is true, then $Q(x)$ is true"

is the statement

"There is at least one x where $P(x)$ is true and $Q(x)$ is false."

The negation of an implication is not an implication!

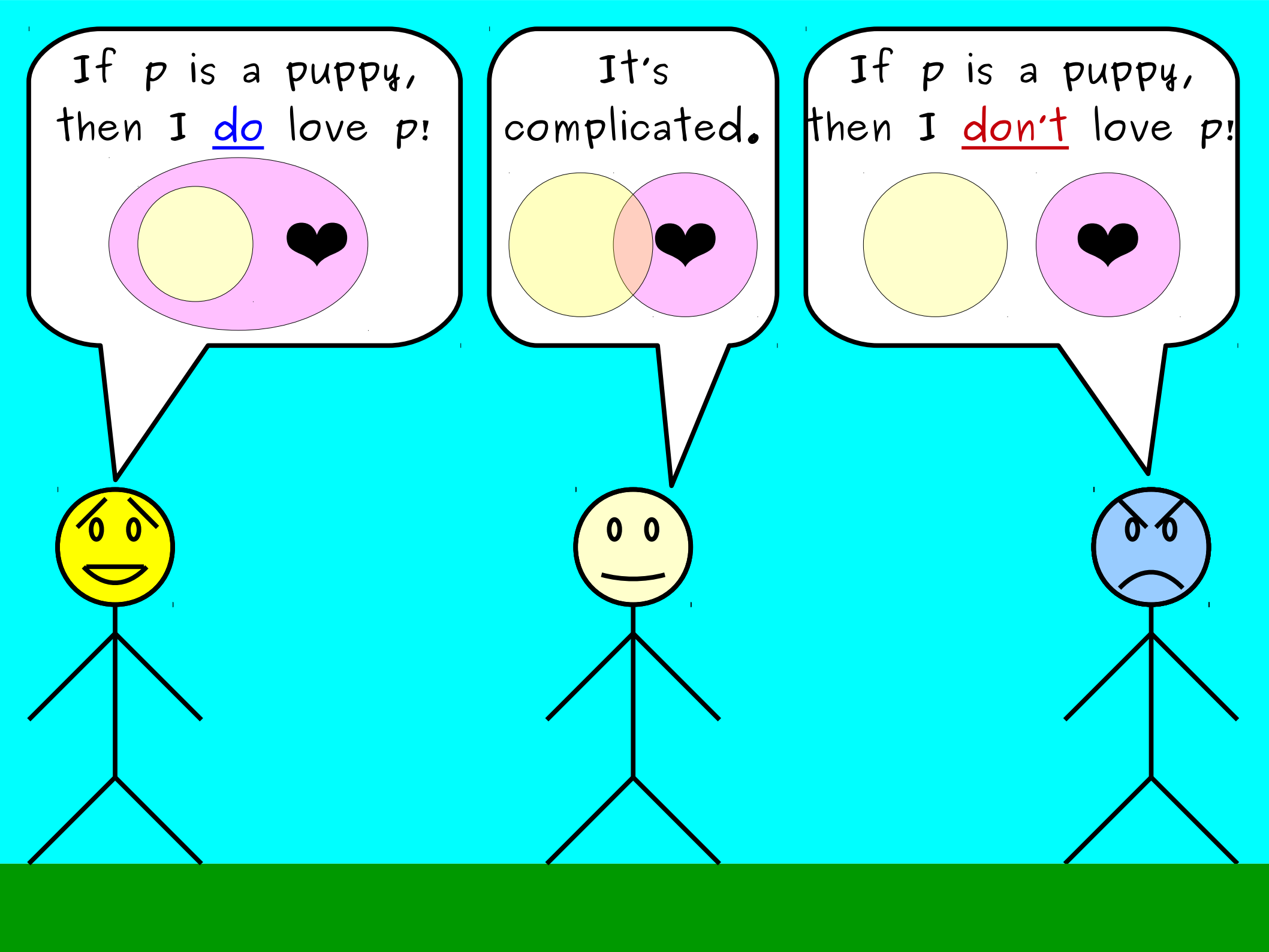
The negation of the statement

"For any x, if $P(x)$ is true, then $Q(x)$ is true"

is the statement

"There is at least one x where $P(x)$ is true and $Q(x)$ is false."

The negation of an implication is not an implication!


If p is a puppy, then I do love p!
It's complicated.
If p is a puppy, then I don't love p!

How to Negate Universal Statements:

"For all x, $P(x)$ is true"

becomes

"There is an x where $P(x)$ is false."

How to Negate Existential Statements:

"There exists an x where $P(x)$ is true"

becomes

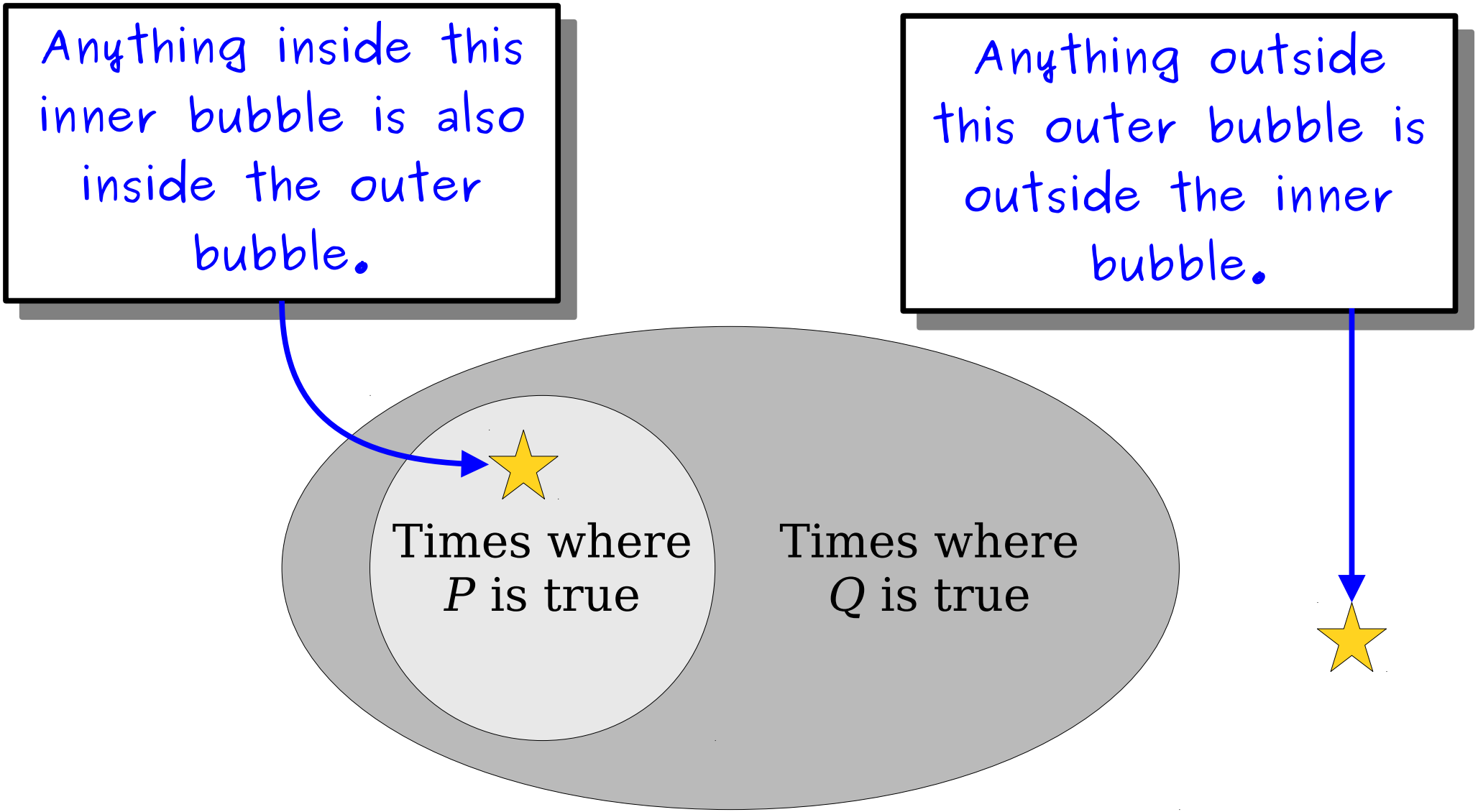
"For all x, $P(x)$ is false."

How to Negate Implications:

"For every x, if $P(x)$ is true, then $Q(x)$ is true"

becomes

"There is an x where $P(x)$ is true and $Q(x)$ is false."



If P is true, then Q is true.

If Q is false, then P is false.

The Contrapositive

- The ***contrapositive*** of the implication

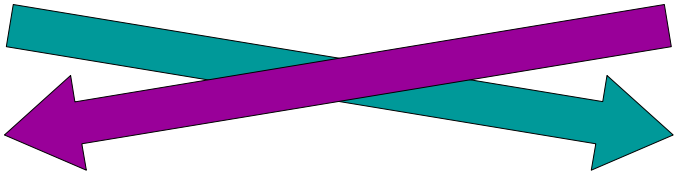
  If *P* is true, then *Q* is true

  is the implication

  If *Q* is false, then *P* is false.

- The contrapositive of an implication means exactly the same thing as the implication itself.

If it's a puppy, then I love it.



If I don't love it, then it's not a puppy.

The Contrapositive

- The ***contrapositive*** of the implication

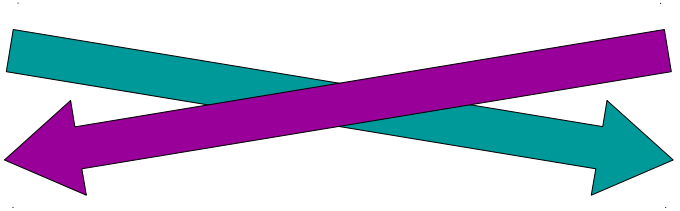
  If *P* is true, then *Q* is true

  is the implication

  If *Q* is false, then *P* is false.

- The contrapositive of an implication means exactly the same thing as the implication itself.

If I store cat food inside, then raccoons won't steal it.



If raccoons stole the cat food, then I didn't store it inside.

To prove the statement

“if *P* is true, then *Q* is true,”

you can choose to instead prove the equivalent statement

“if *Q* is false, then *P* is false,”

if that seems easier.

This is called a ***proof by contrapositive***.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

This is a courtesy to the reader and says "heads up! we're not going to do a regular old-fashioned direct proof here."

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

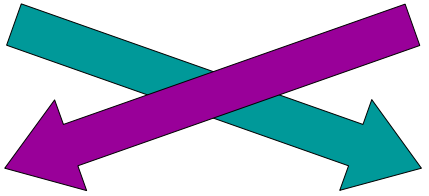
if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

if n^2 is even, then n is even.

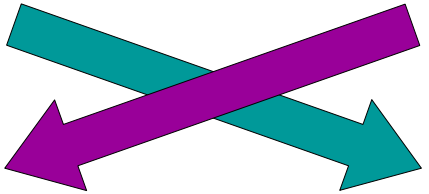


Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

if n^2 is even, then n is even.



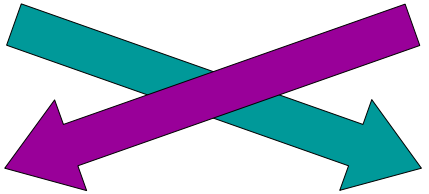
If n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd.

What is the contrapositive of this statement?

if n^2 is even, then n is even.



If n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd.

Here, we're explicitly writing out the contrapositive. This tells the reader what we're going to prove. It also acts as a sanity check by forcing us to write out what we think the contrapositive is.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd.

We've said that we're going to prove this new implication, so let's go do it! The rest of this proof will look a lot like a standard direct proof.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$n^2 = (2k + 1)^2$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. That means that n^2 is odd, which is what we needed to show.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. That means that n^2 is odd, which is what we needed to show. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd.

We know that there exists an integer k such that $n = 2k + 1$. This tells us that

From this, we see that $n^2 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer (namely, $k(k + 1)$), this means that n^2 is odd, as we needed to show. ■

The general pattern here is the following:

1. Start by announcing that we're going to use a proof by contrapositive so that the reader knows what to expect.

2. Explicitly state the contrapositive of what we want to prove.

3. Go prove the contrapositive.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. That means that n^2 is odd, which is what we needed to show. ■

Biconditionals

- The previous theorem, combined with what we saw on Wednesday, tells us the following:

  For any integer n, if n is even, then n^2 is even.

  For any integer n, if n^2 is even, then n is even.

- These are two different implications, each going the other way.
- We use the phrase ***if and only if*** to indicate that two statements imply one another.
- For example, we might combine the two above statements to say

  for any integer n: n is even if and only if n^2 is even.

Proving Biconditionals

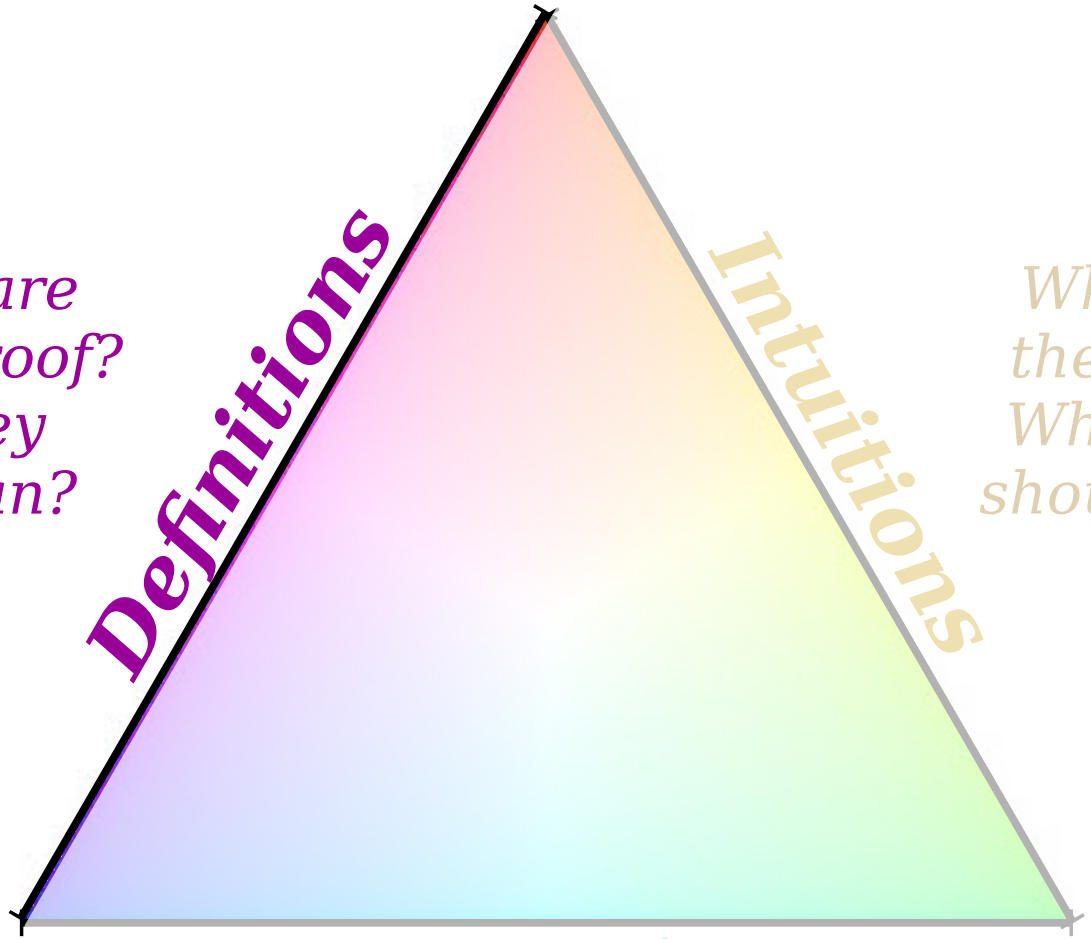
- To prove a theorem of the form

  _P_ if and only if _Q_,

  you need to prove two separate statements.
  - First, that if P is true, then Q is true.
  - Second, that if Q is true, then P is true.
- You can use any proof techniques you'd like to show each of these statements.
  - In our case, we used a direct proof for one and a proof by contrapositive for the other.

Proofs on Sets

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.



What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

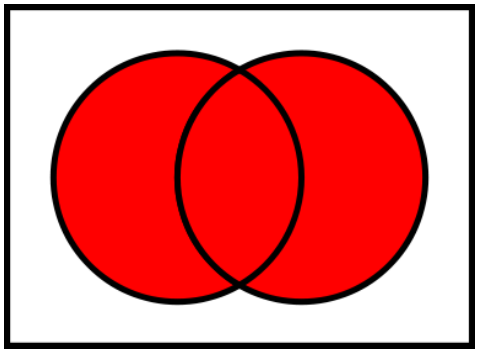
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

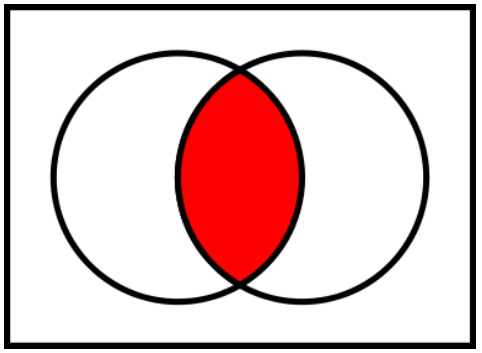
This is the ***element-of*** relation $\in$. It means that this object x is one of the items inside these sets.

Set Combinations

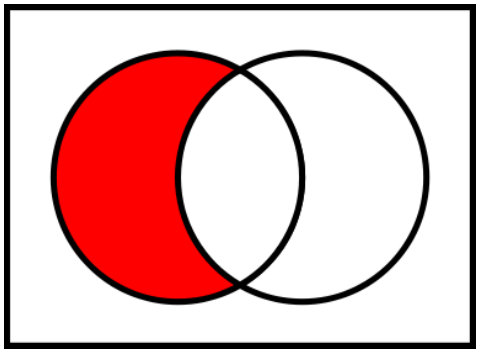
- So far, we've seen four ways of combining sets together.



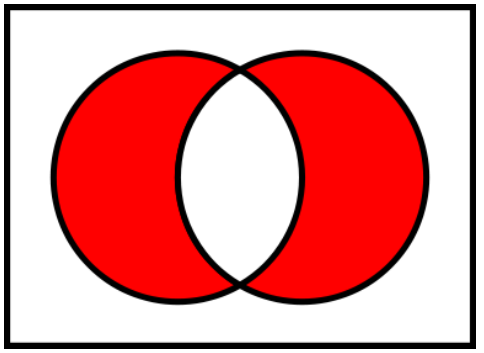
$S \cup T$



$S \cap T$



$S - T$



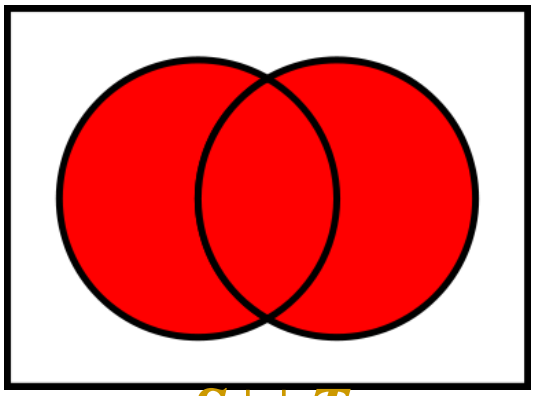
$S \Delta T$

- The above pictures give a holistic sense of how these operations work.
- However, mathematical proofs tend to work on sets in a different way.

Important Fact:

Proofs about sets *almost always* focus on individual elements of those sets. It's rare to talk about how collections relate to one another "in general."

Set Union



$S \cup T$

Definition: The set $S \cup T$ is the set where, for any x:

$$x \in S \cup T \quad \text{when} \quad x \in S \text{ or } x \in T$$

To prove that $x \in S \cup T$:

Prove either that $x \in S$ or that $x \in T$.

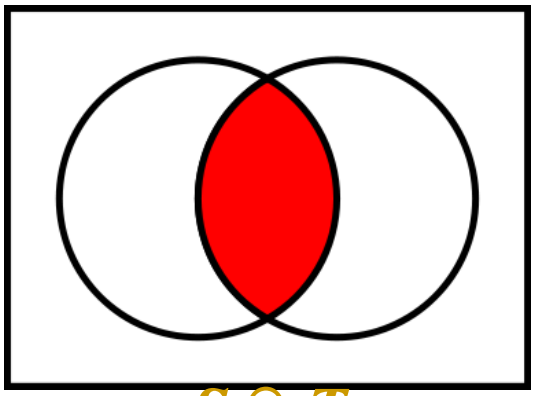
If you assume that $x \in S \cup T$:

Consider two cases:

Case 1: $x \in S$.

Case 2: $x \in T$.

Set Intersection



$S \cap T$

Definition: The set $S \cap T$ is the set where, for any x:

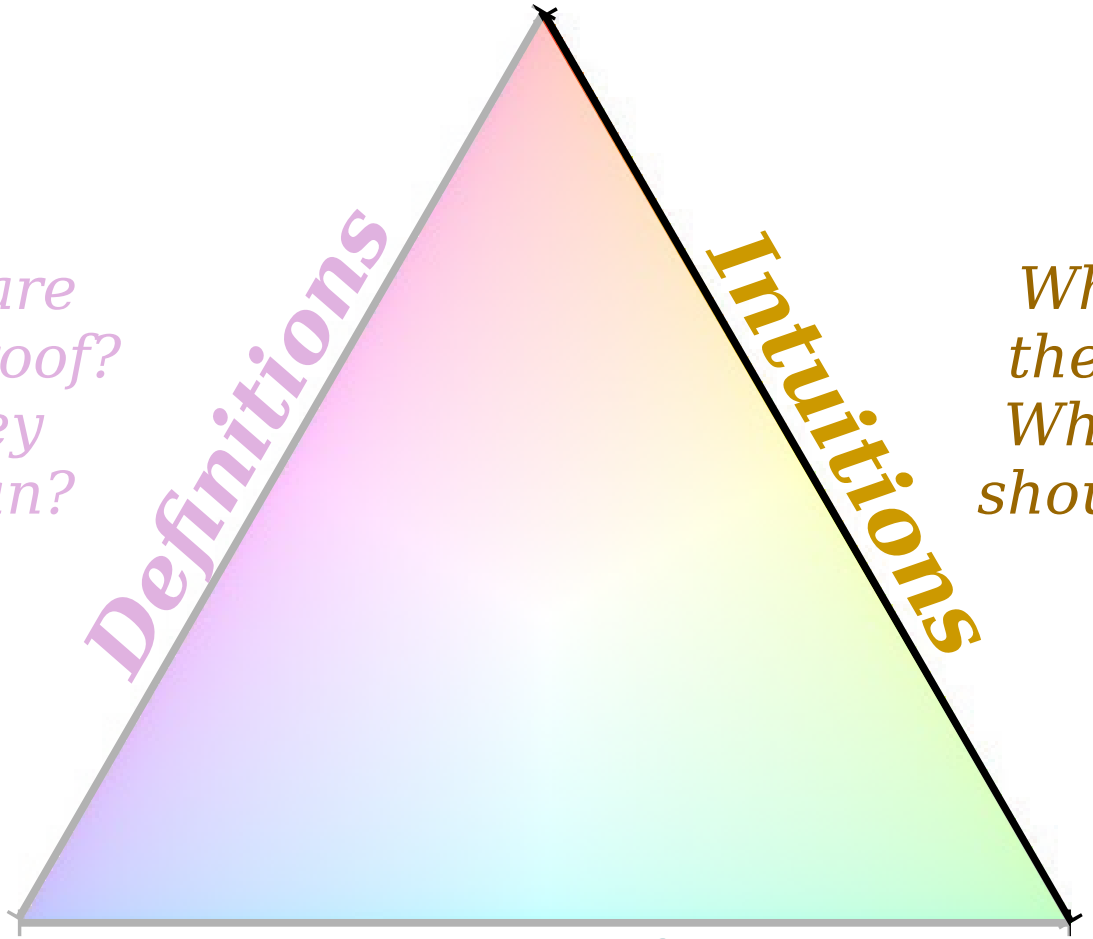
$$x \in S \cap T \quad \text{when} \quad x \in S \text{ and } x \in T$$

To prove that $x \in S \cap T$:

Prove both that $x \in S$ and that $x \in T$.

If you assume that $x \in S \cap T$:

Assume $x \in S$ and $x \in T$.



What terms are used in this proof? What do they formally mean?

What does this theorem mean? Why, intuitively, should it be true?

What is the standard format for writing a proof? What are the techniques for doing so?

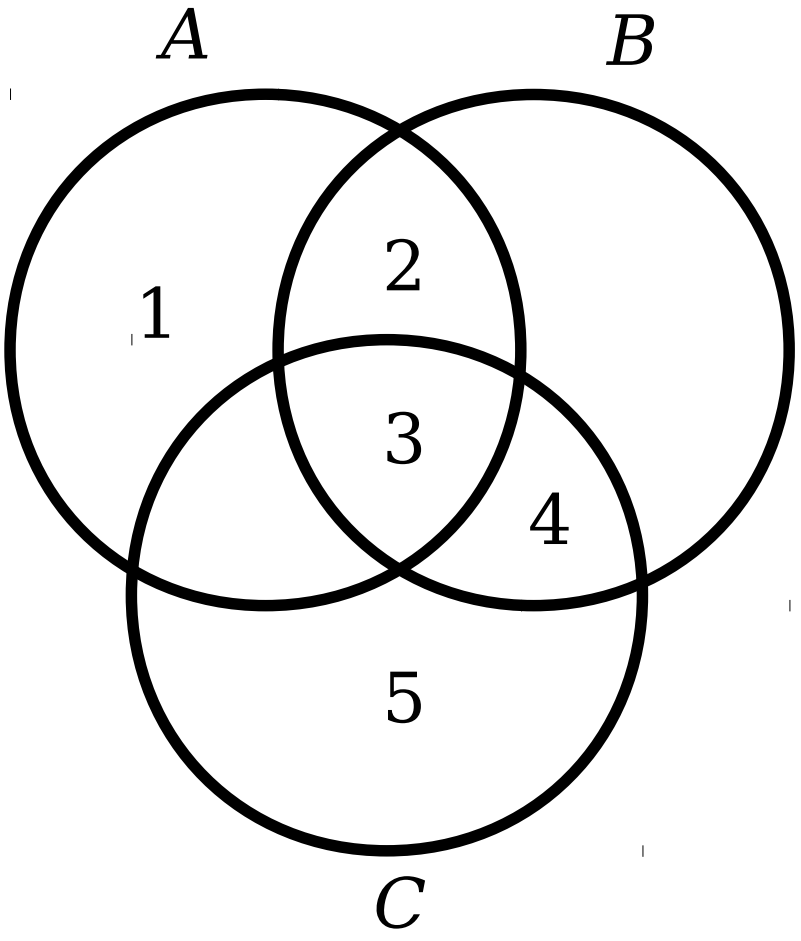
Let's Try Some Examples!

$A = \{1, 2, 3\}$
$B = \{2, 3, 4\}$
$C = \{3, 4, 5\}$

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Try Some Examples!

$A = \{1, 2, 3\}$
$B = \{2, 3, 4\}$
$C = \{3, 4, 5\}$



$x = 1$

✔ ✘ ✘

Is $x \in (A \cap B) \cup C$?

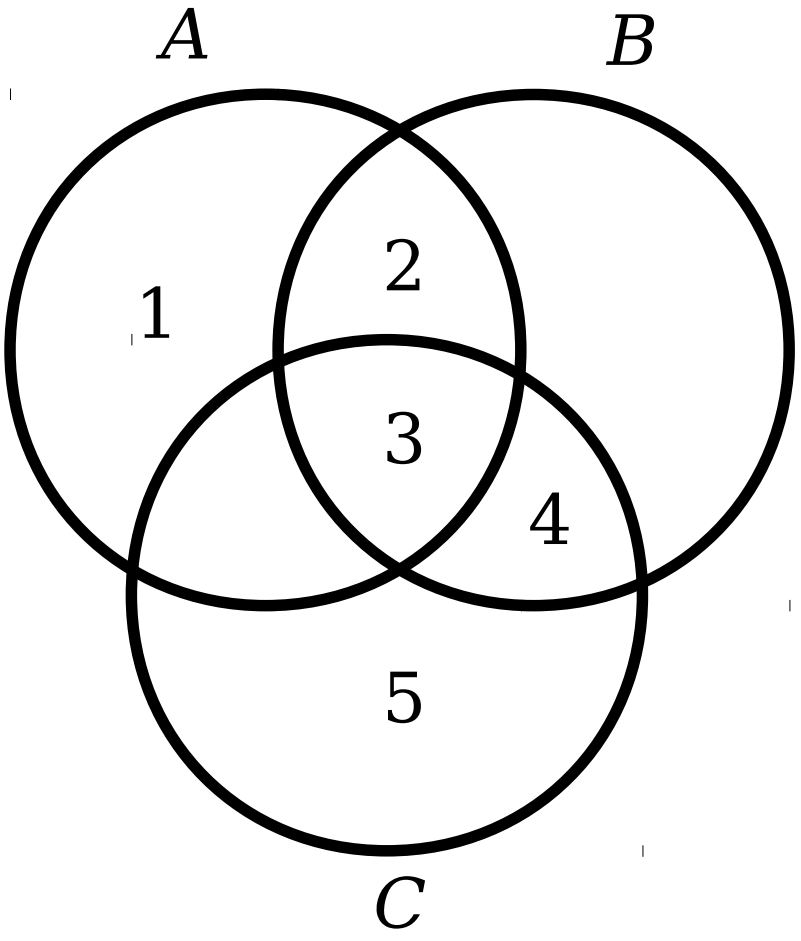
✔ ✘ ✘ ✘

Is $x \in (A \cup C) \cap (B \cup C)$?

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Try Some Examples!

$A = \{1, 2, 3\}$
$B = \{2, 3, 4\}$
$C = \{3, 4, 5\}$



$x = 2$

✔ ✔ ✘

Is $x \in (A \cap B) \cup C$?

✔ ✘ ✔ ✘

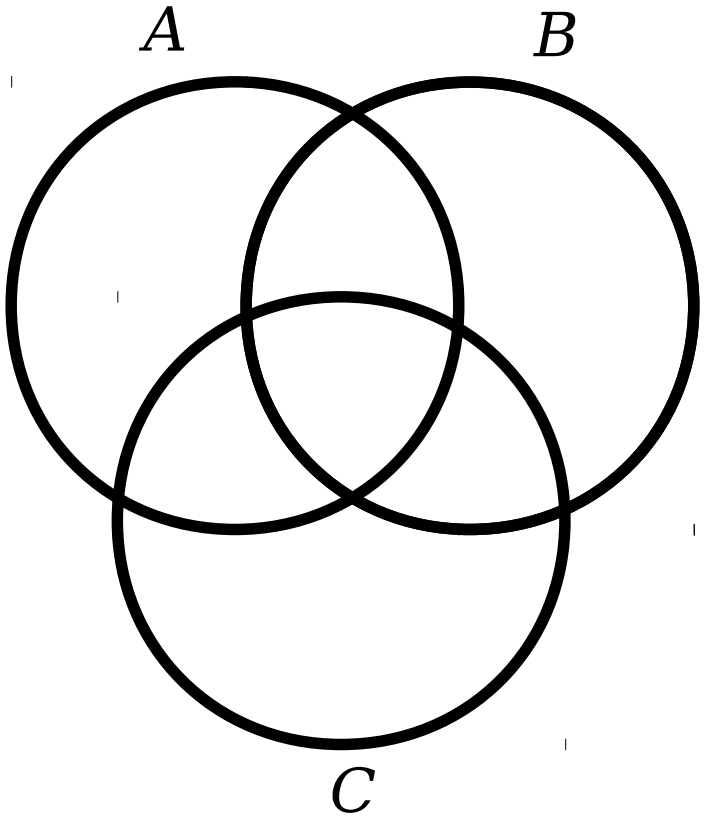
Is $x \in (A \cup C) \cap (B \cup C)$?

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!

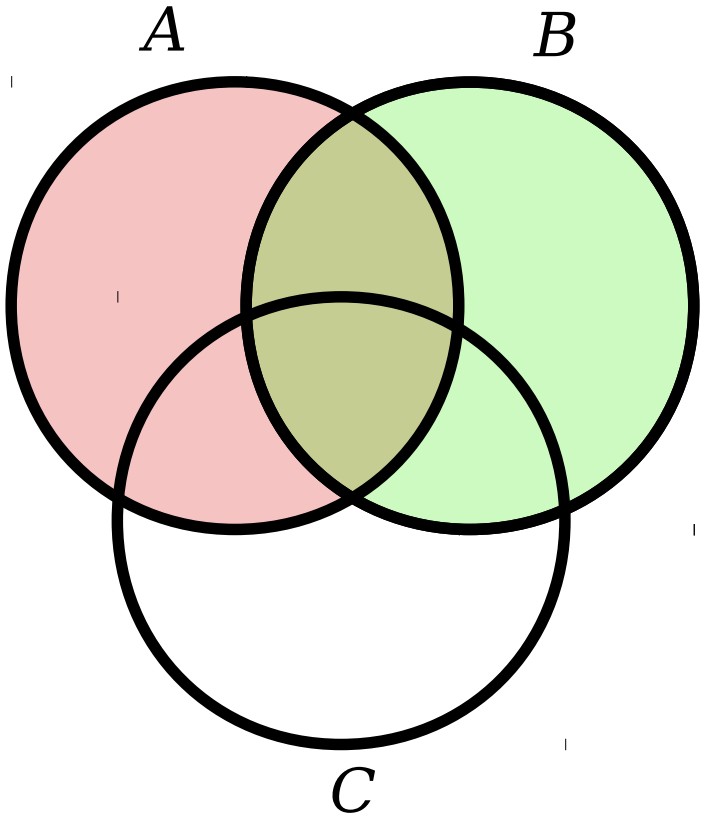
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



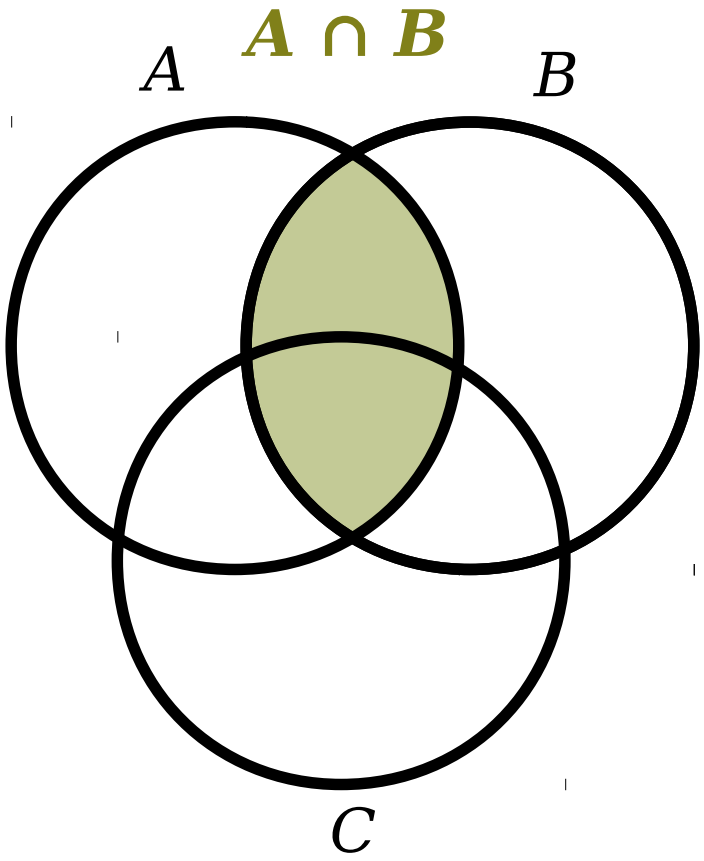
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



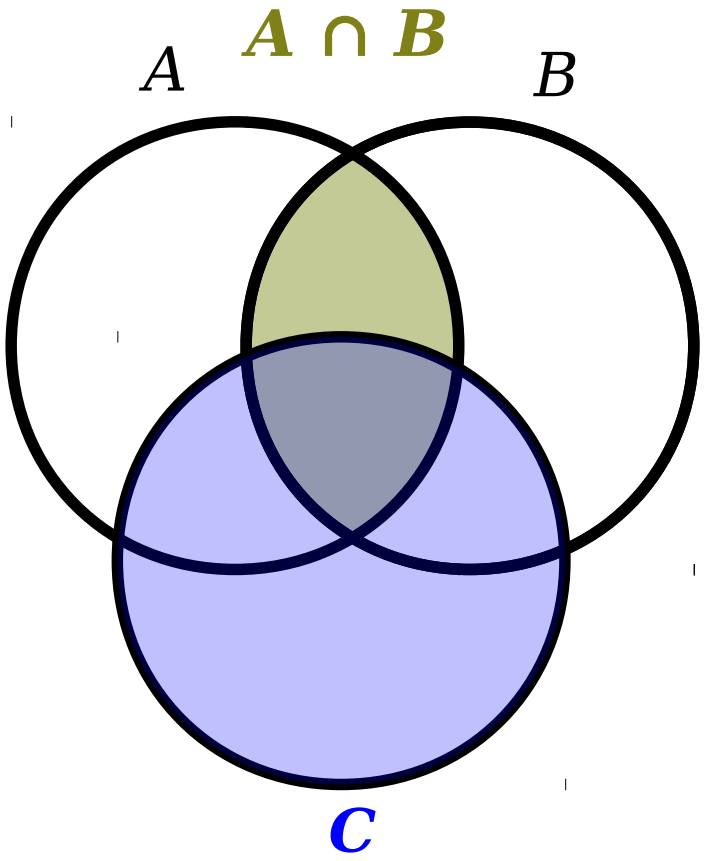
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



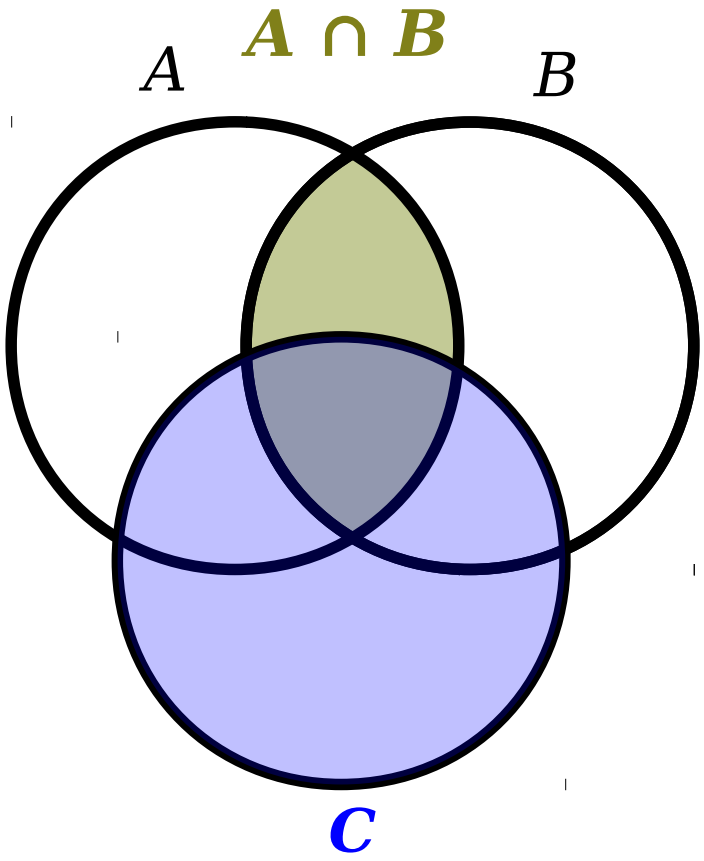
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

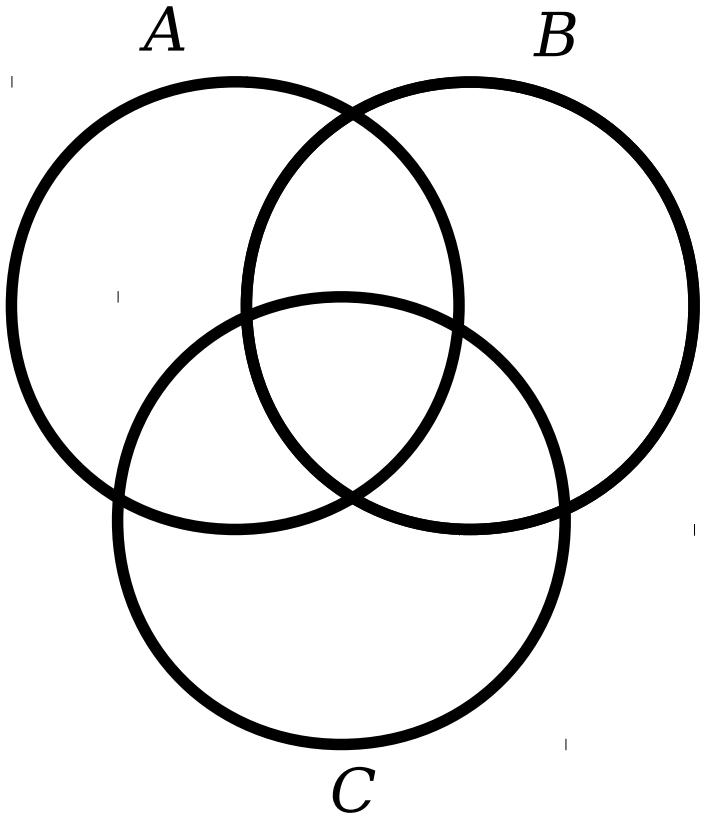
Let's Draw Some Pictures!



Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

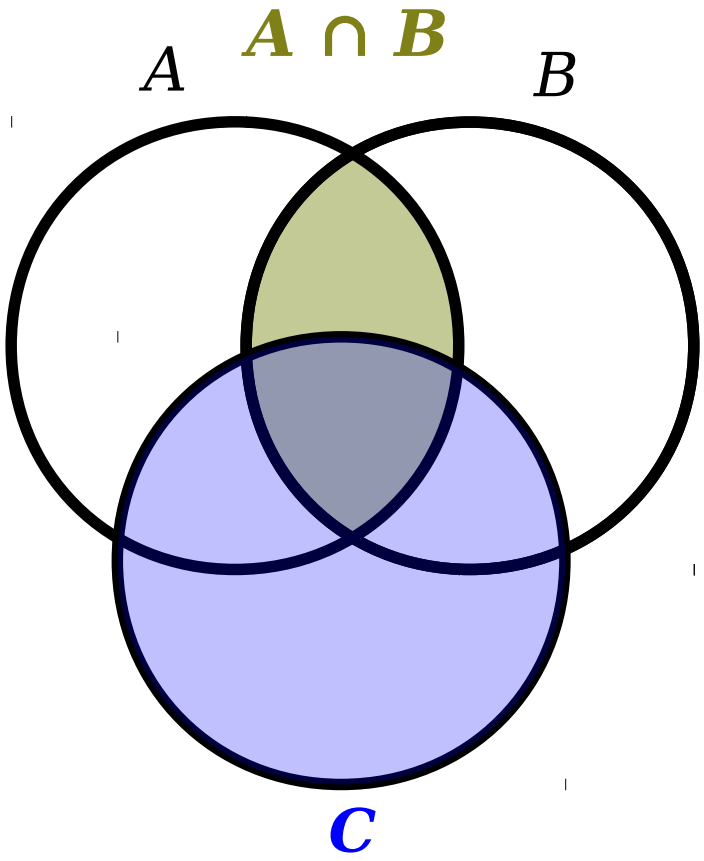
Let's Draw Some Pictures!

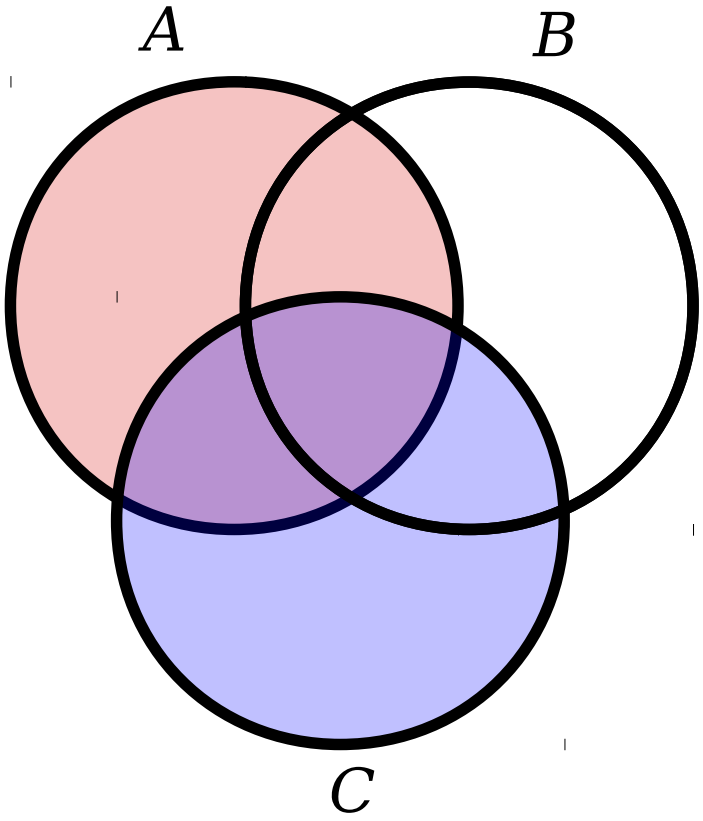




Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

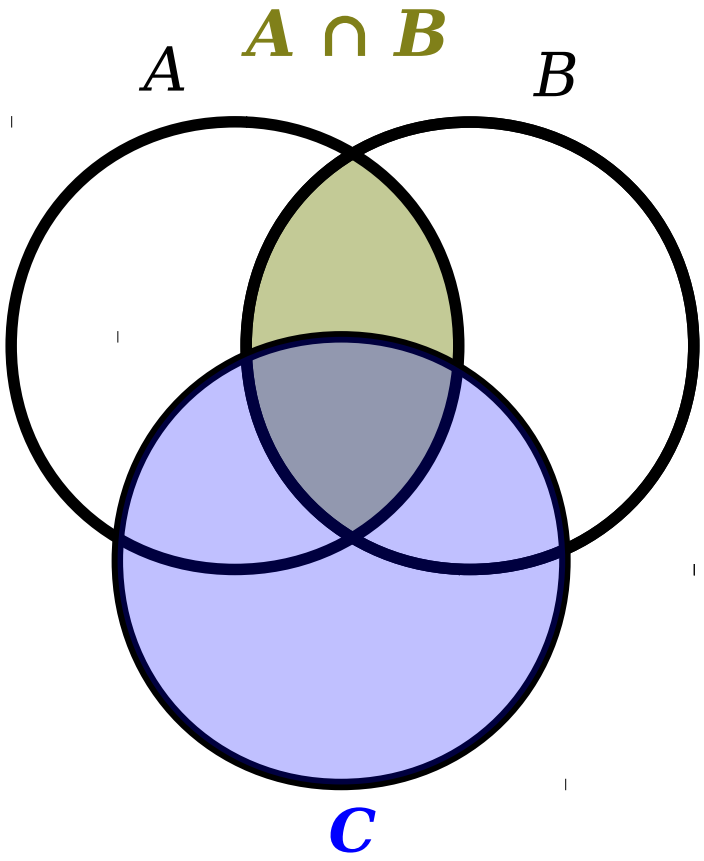
Let's Draw Some Pictures!

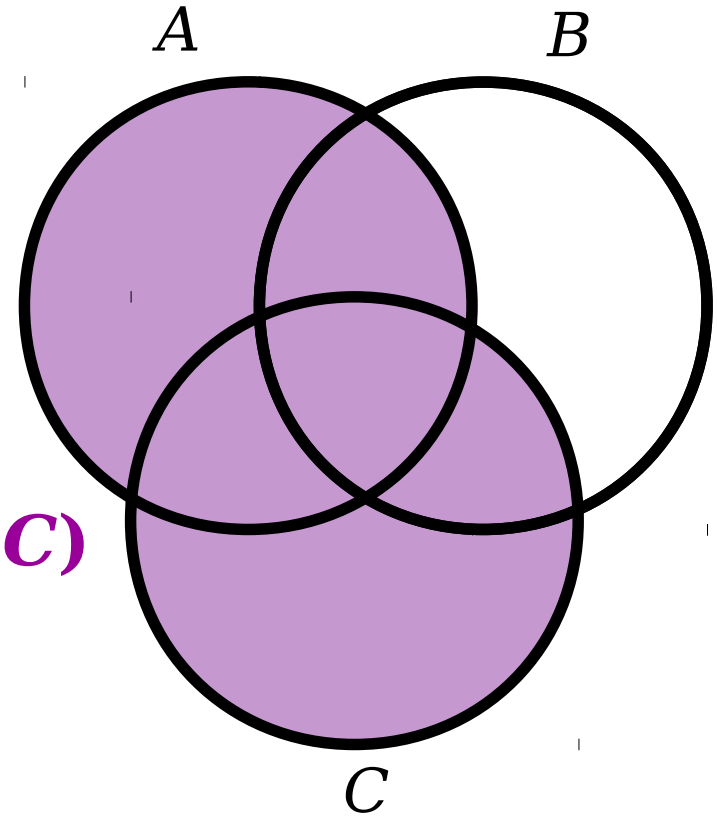




Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

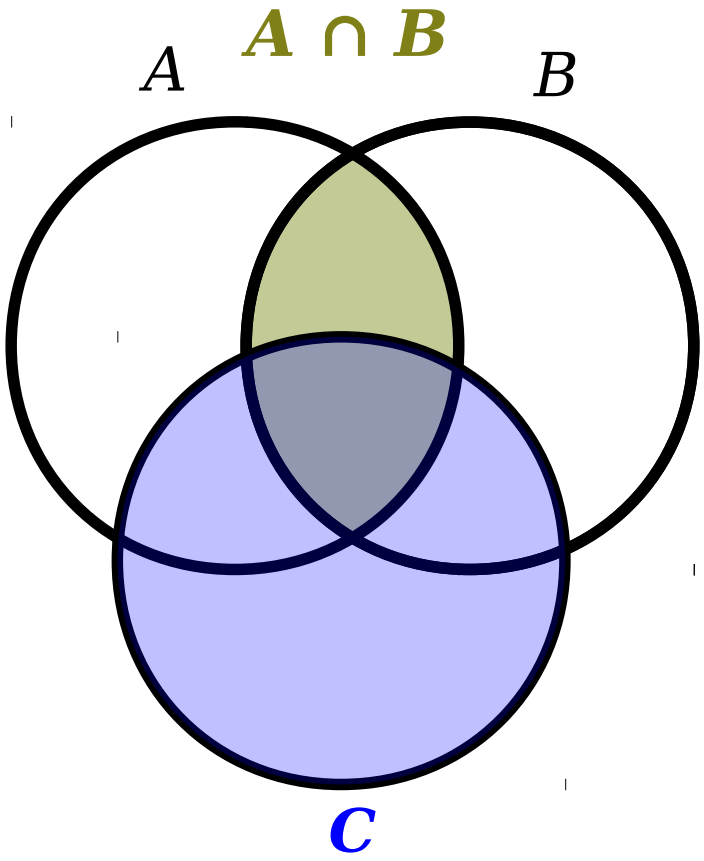
Let's Draw Some Pictures!

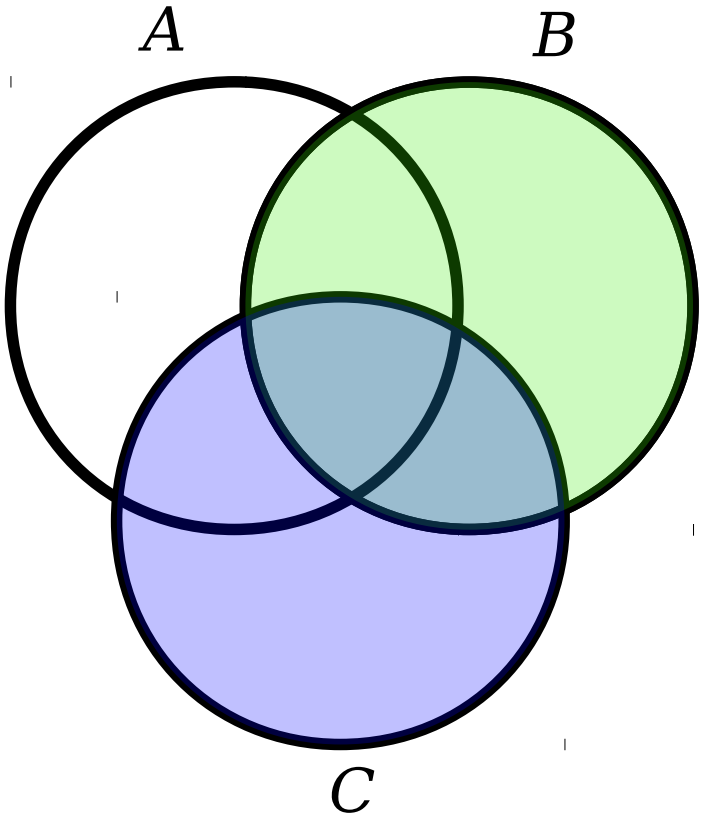




Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

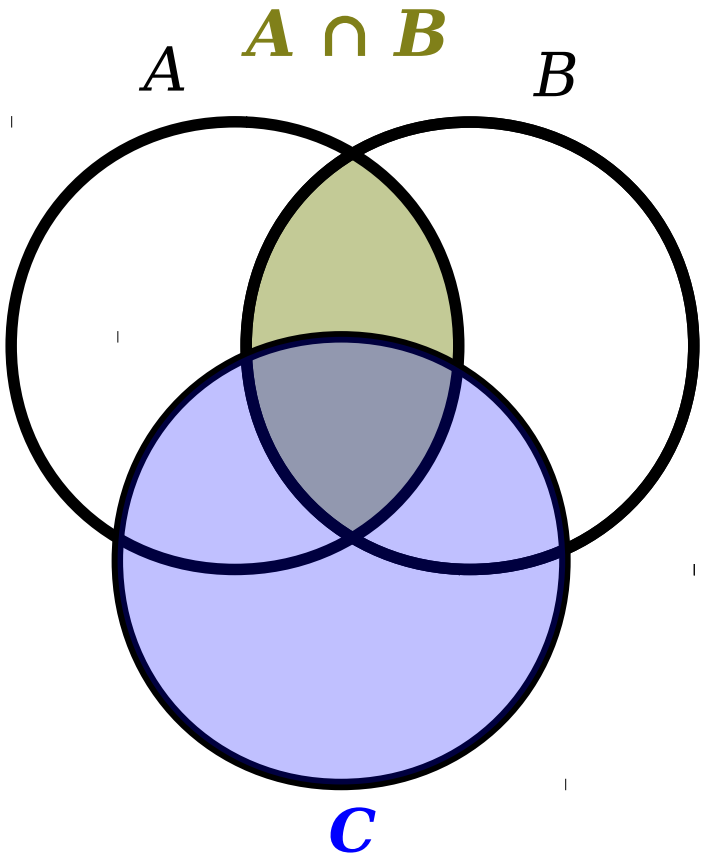
Let's Draw Some Pictures!

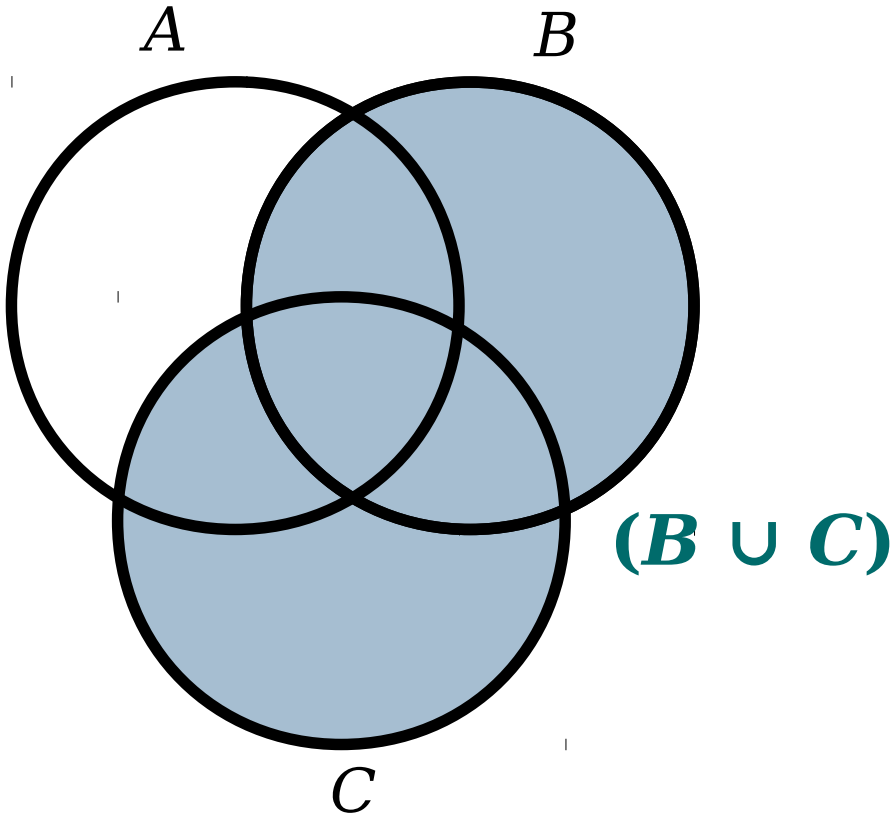




Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

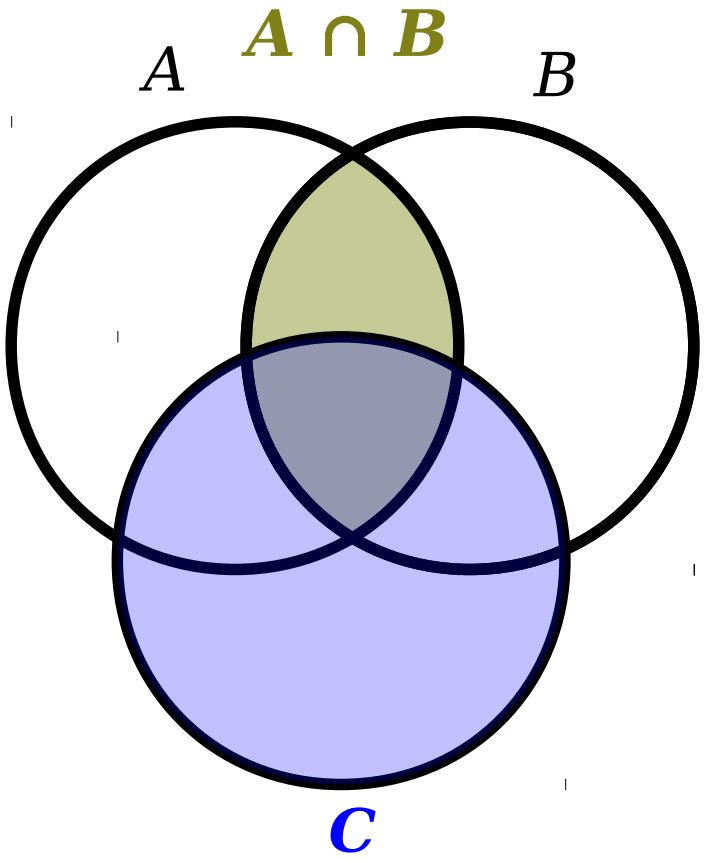
Let's Draw Some Pictures!

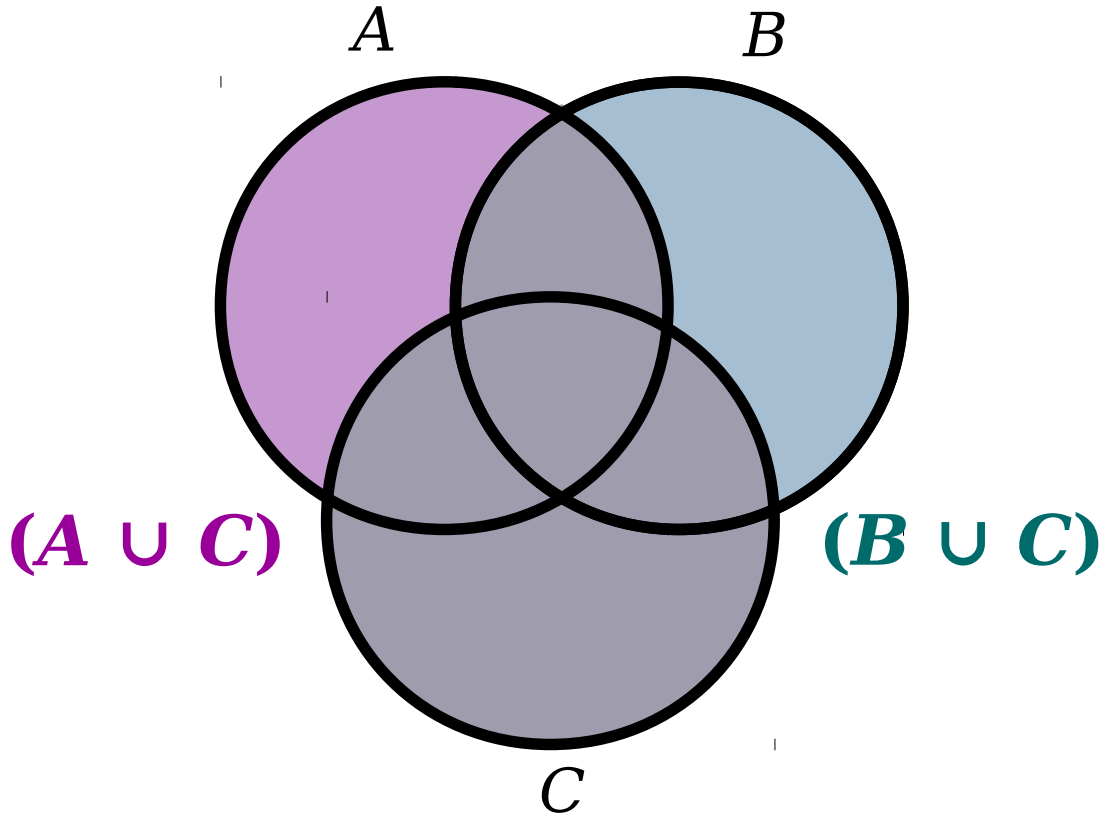




Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

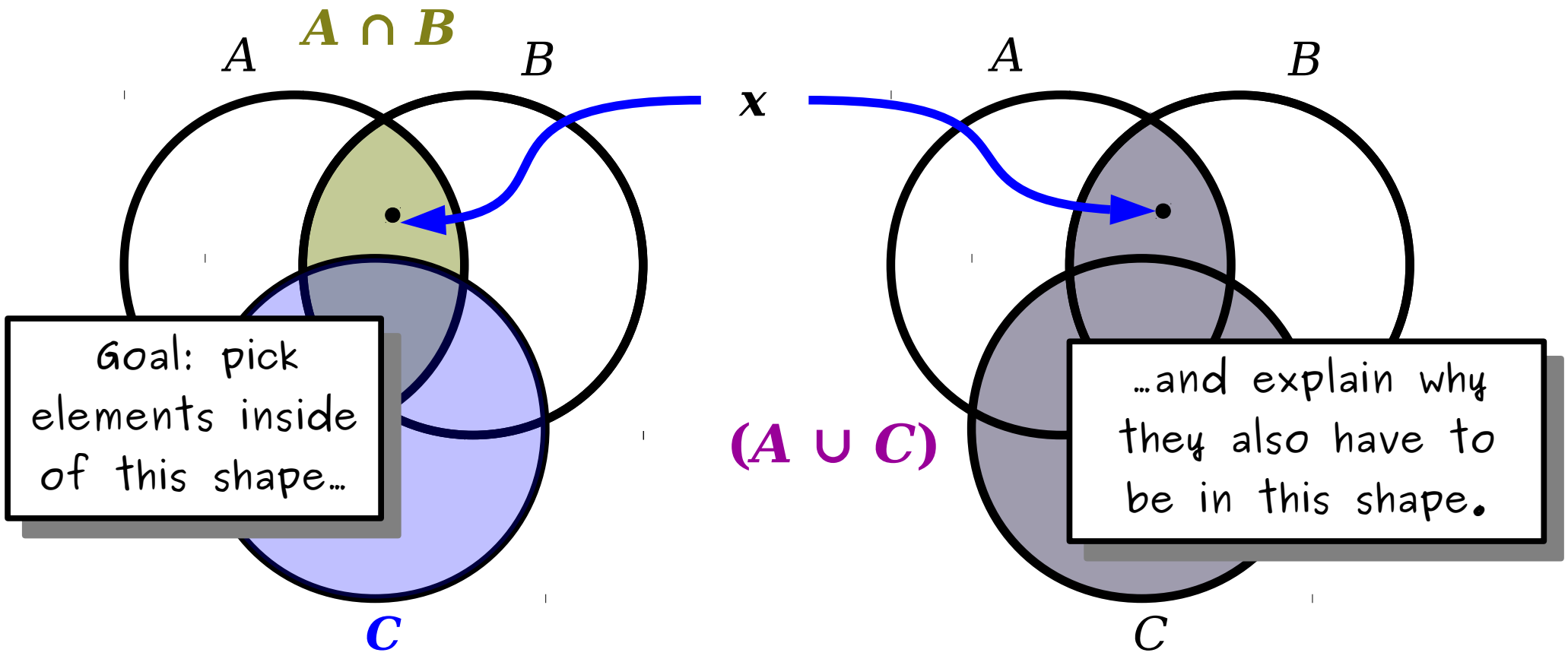
Let's Draw Some Pictures!





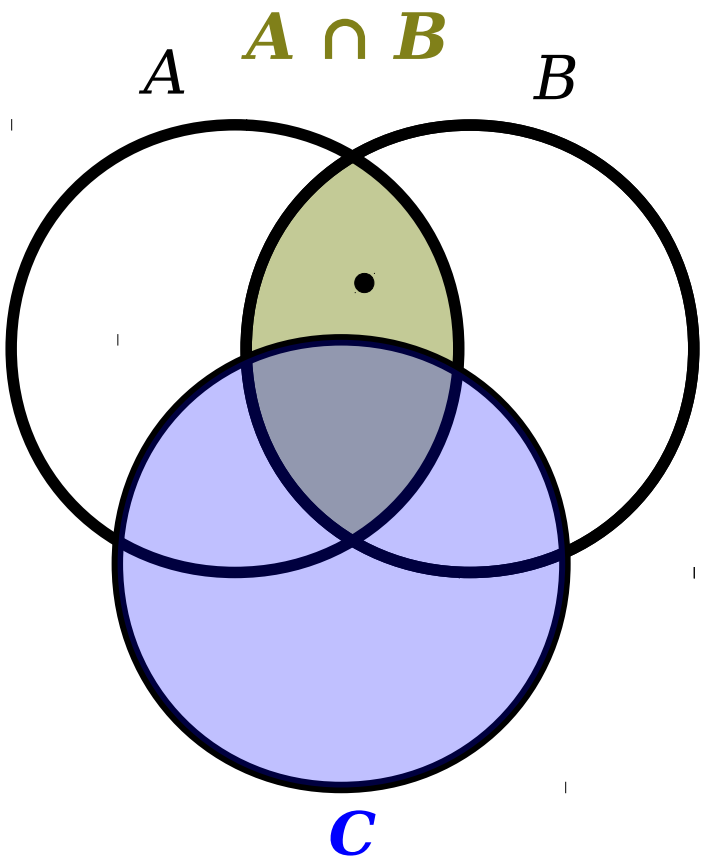
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!

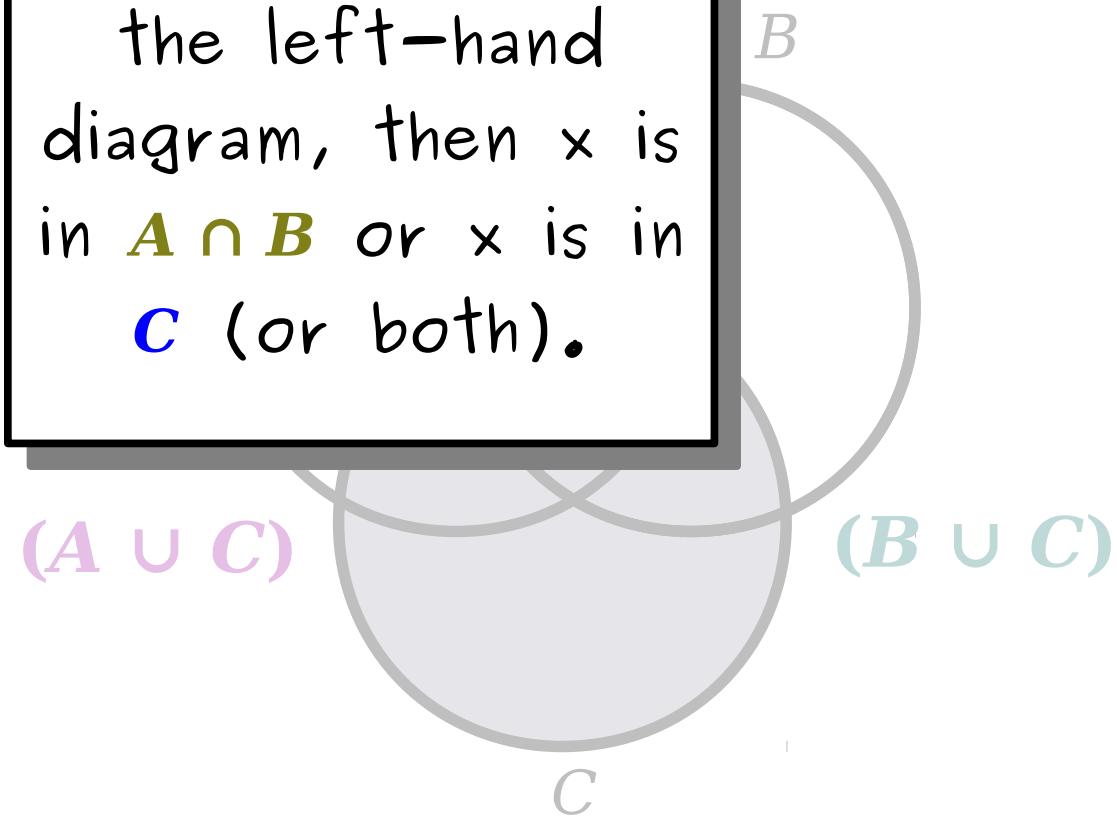


Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!

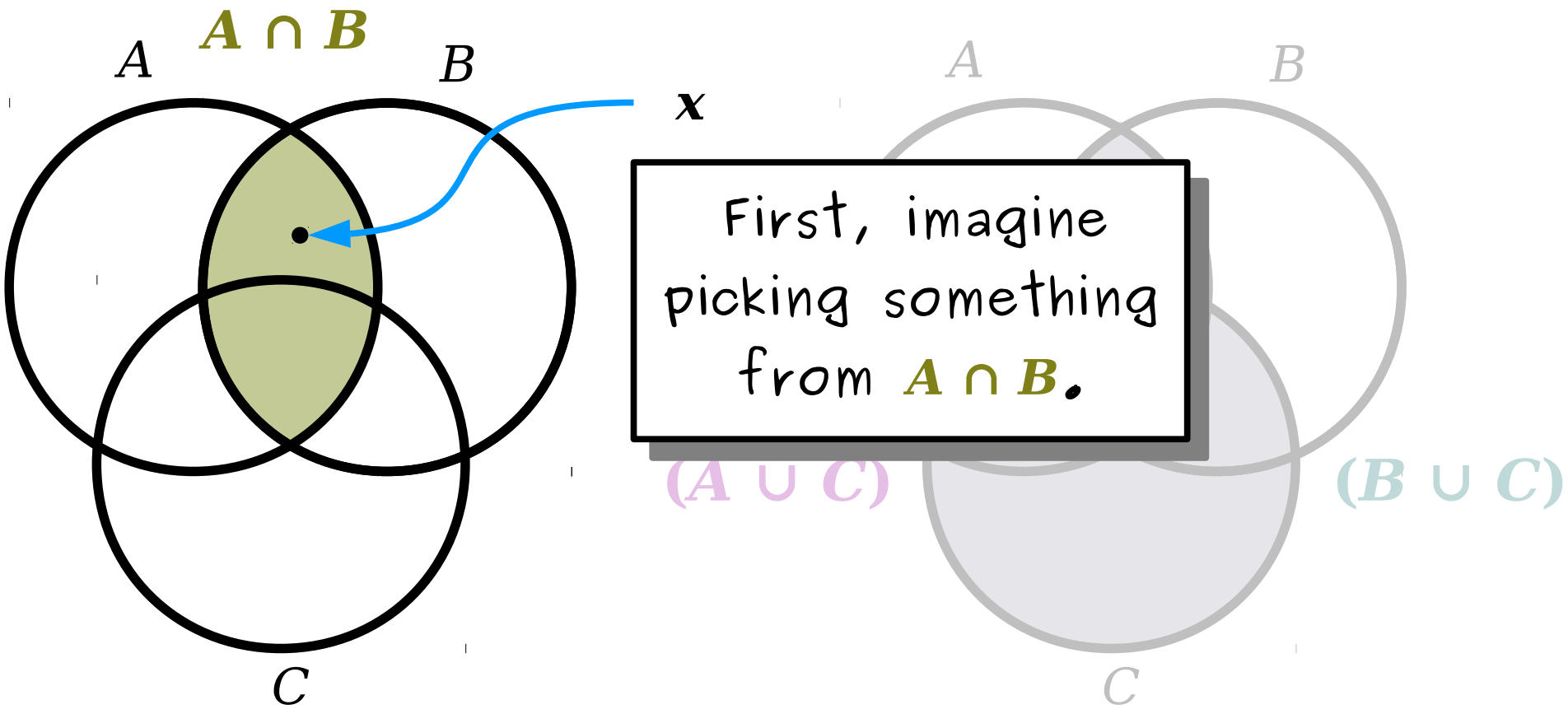


If we pick x from the left-hand diagram, then x is in $A \cap B$ or x is in C (or both).



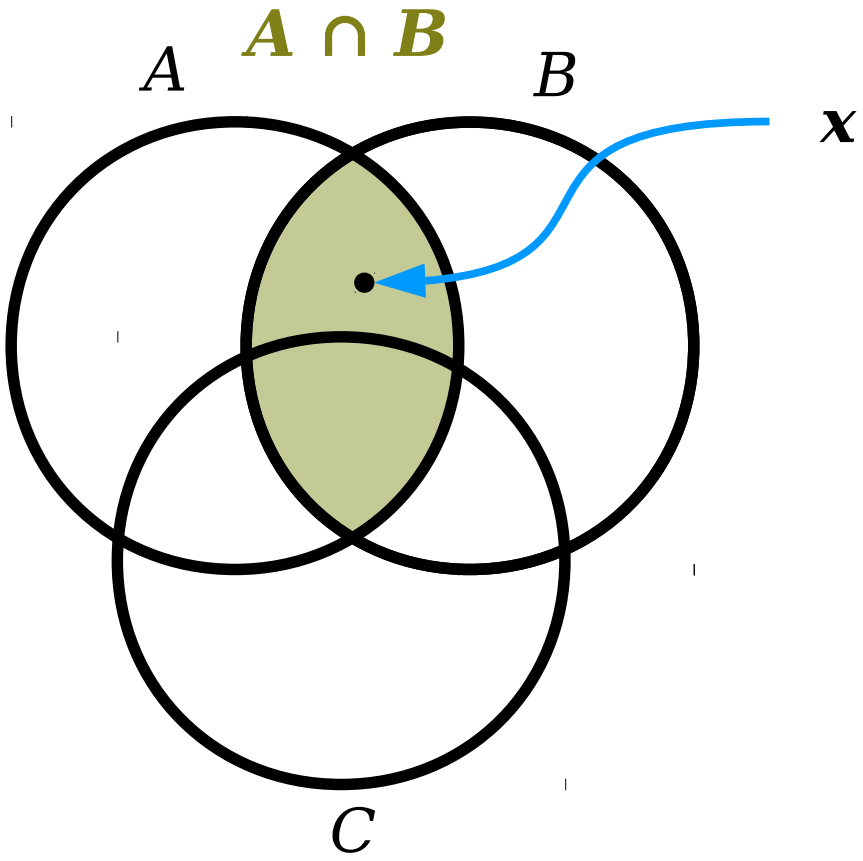
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

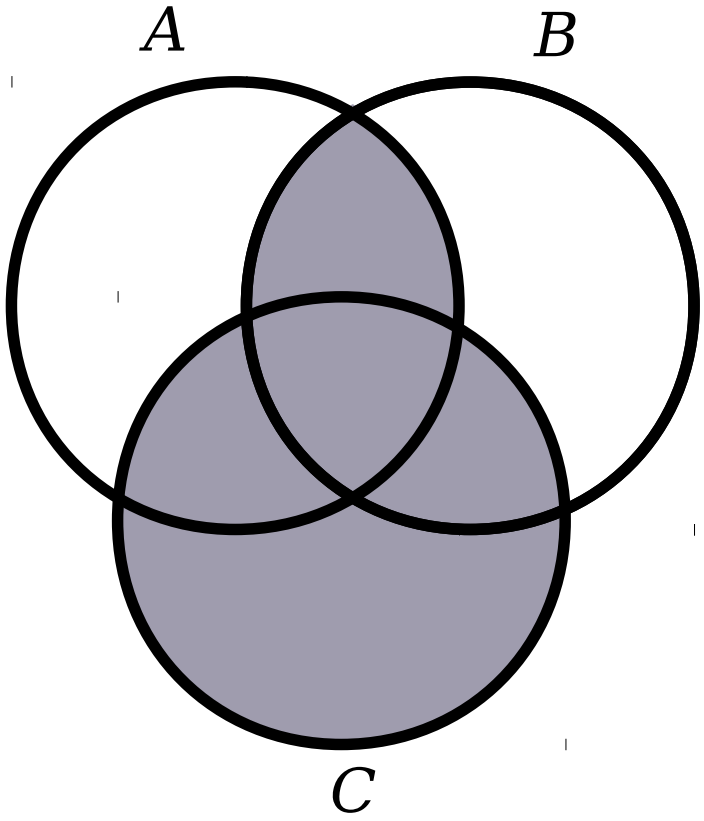
Let's Draw Some Pictures!



Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

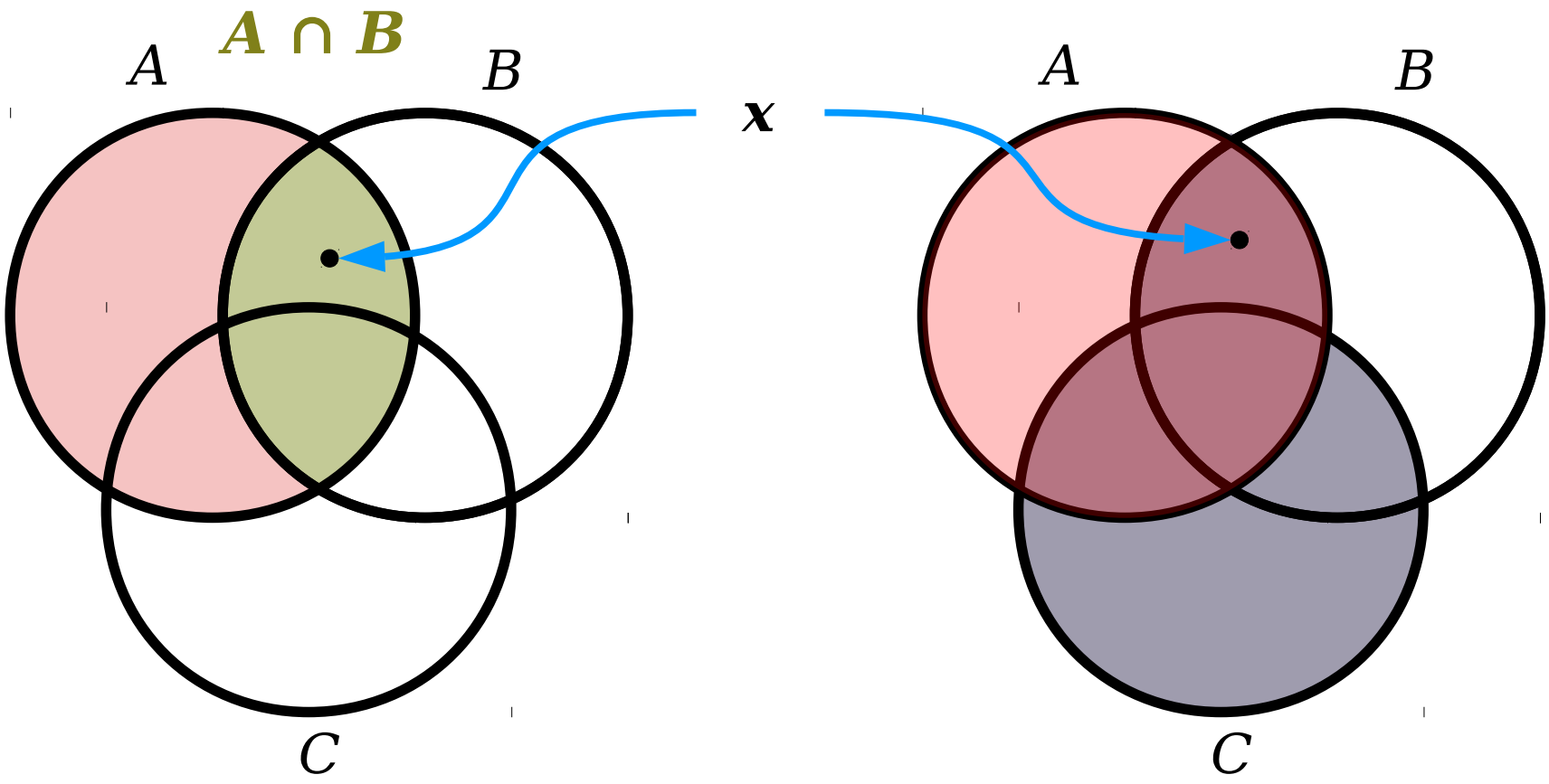
Let's Draw Some Pictures!





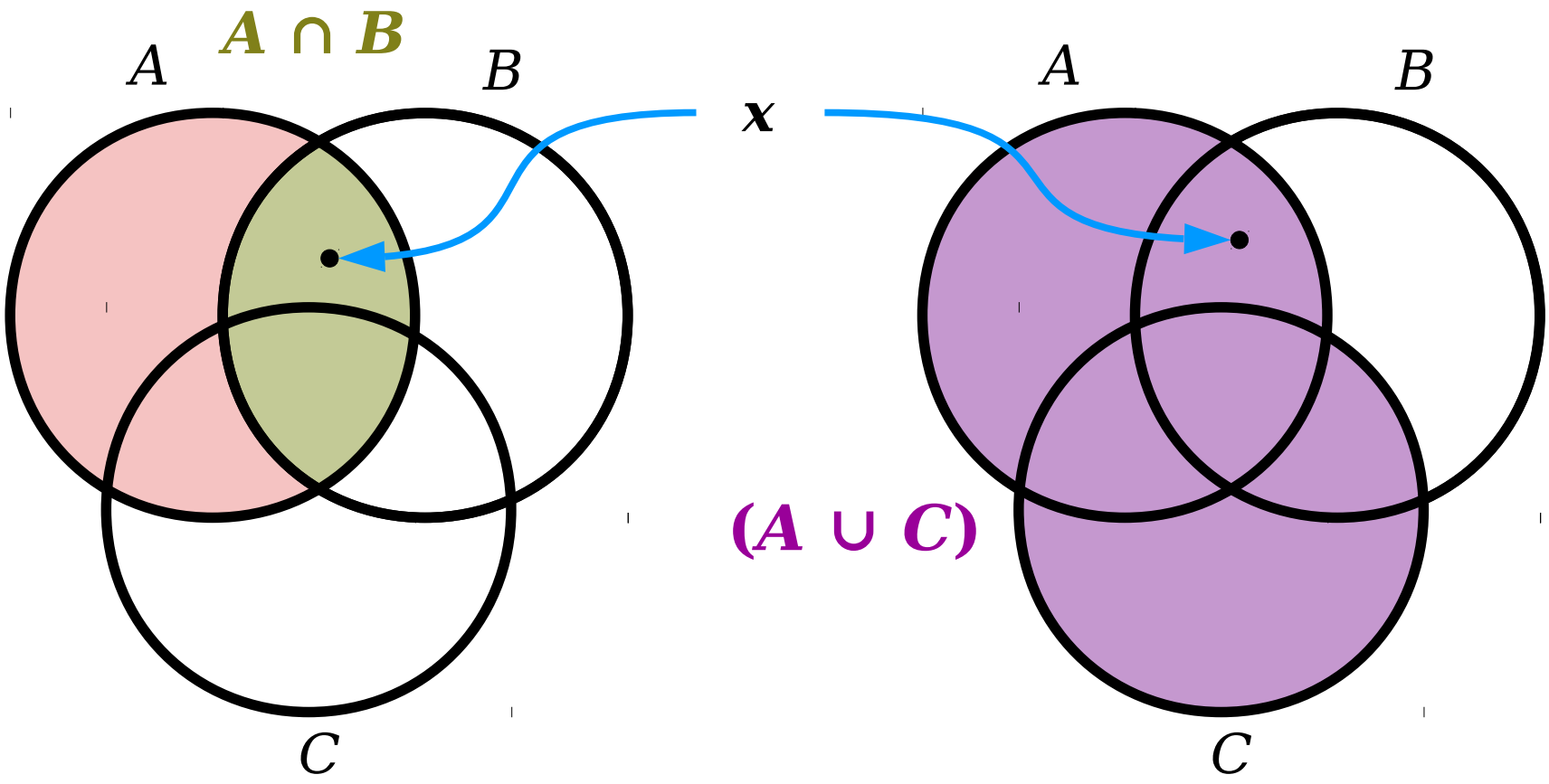
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



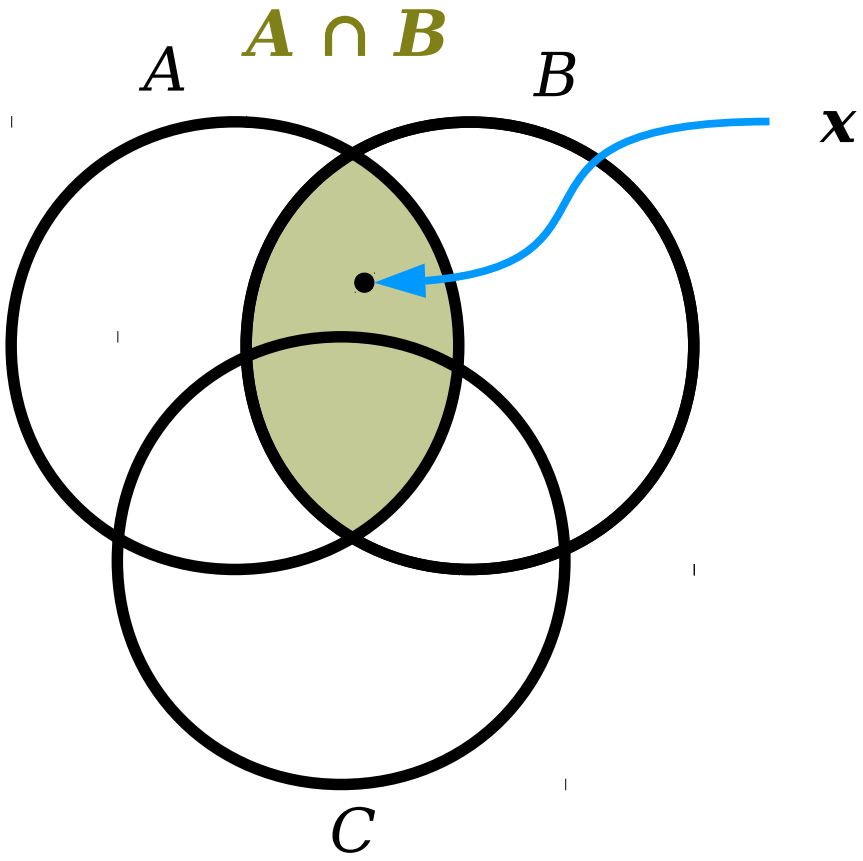
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

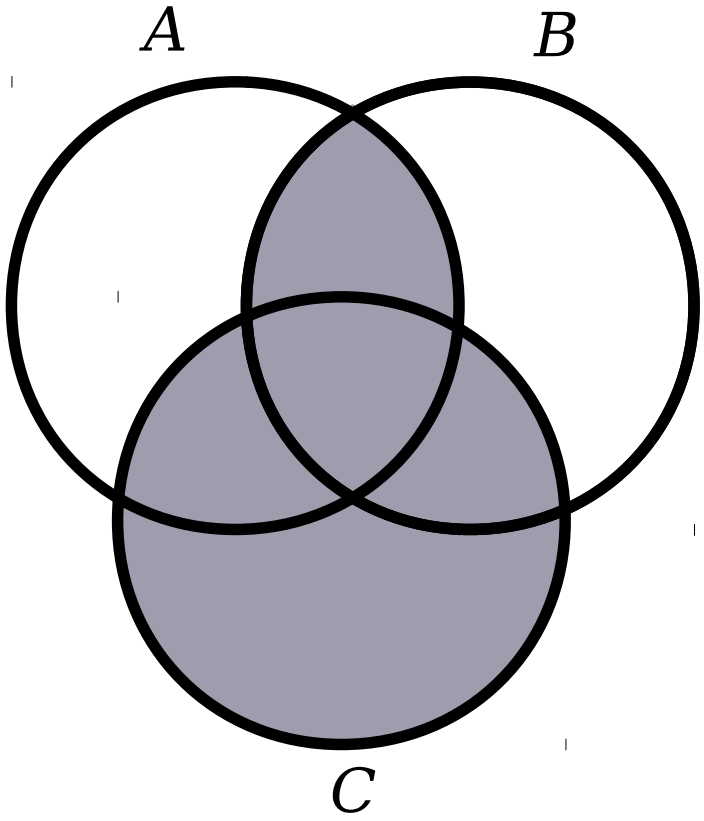
Let's Draw Some Pictures!



Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

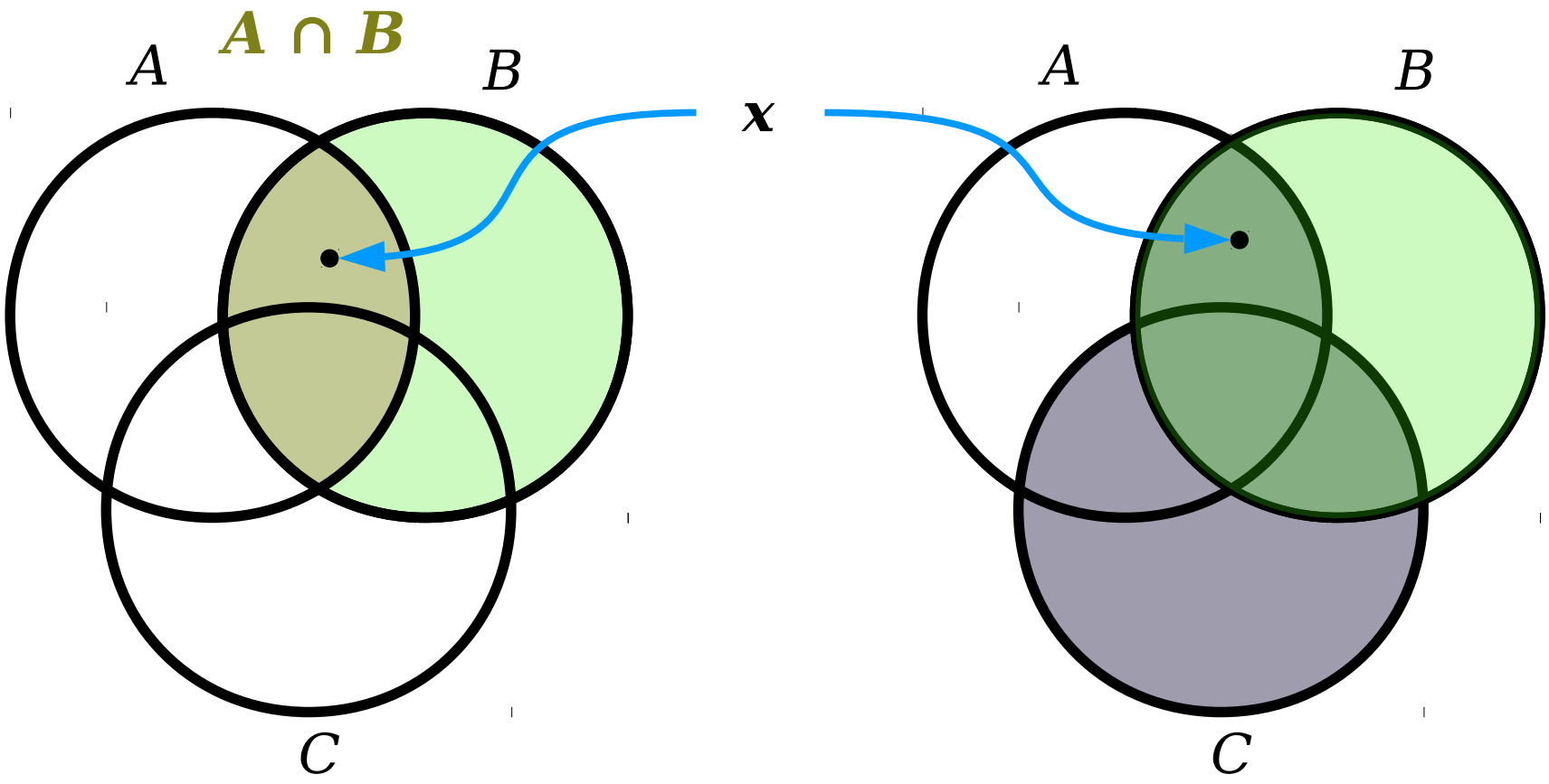
Let's Draw Some Pictures!





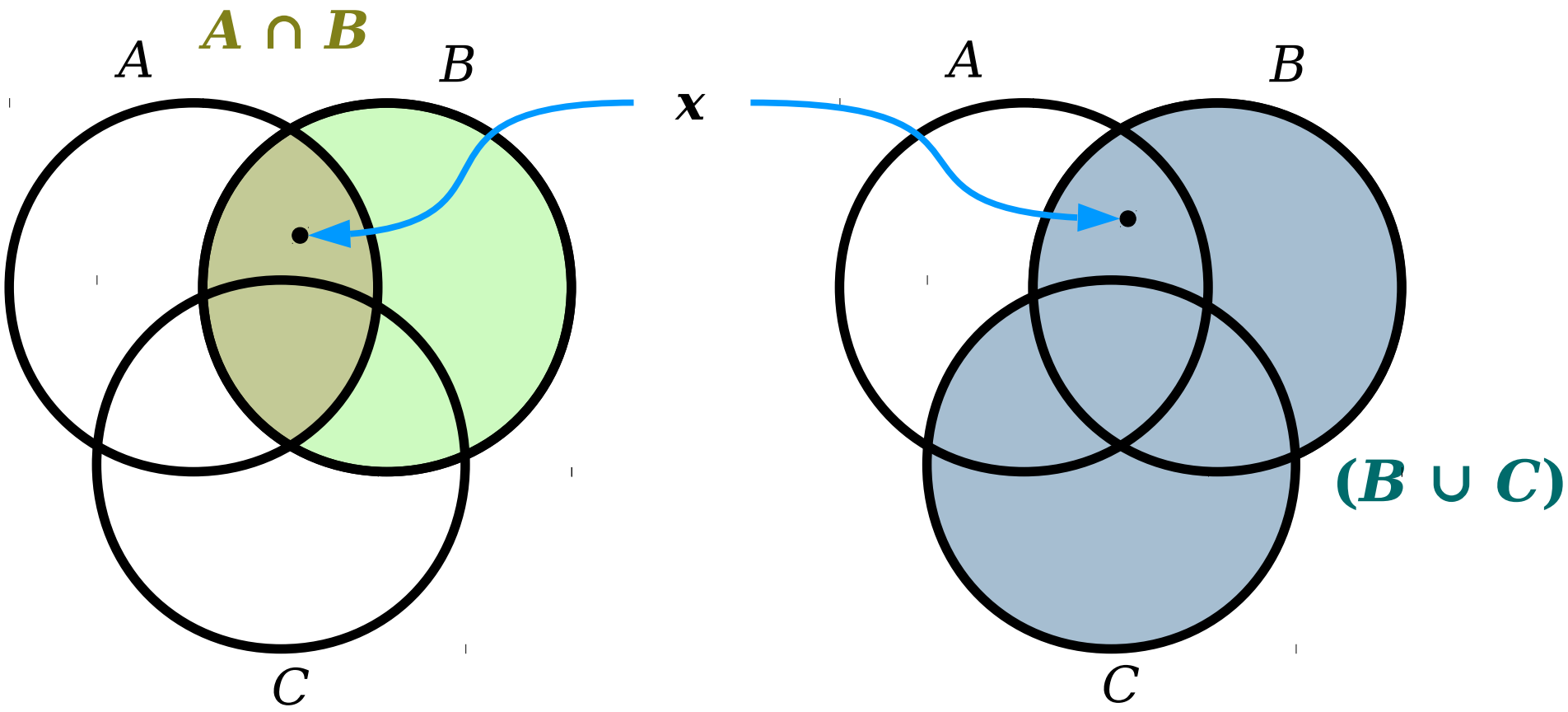
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



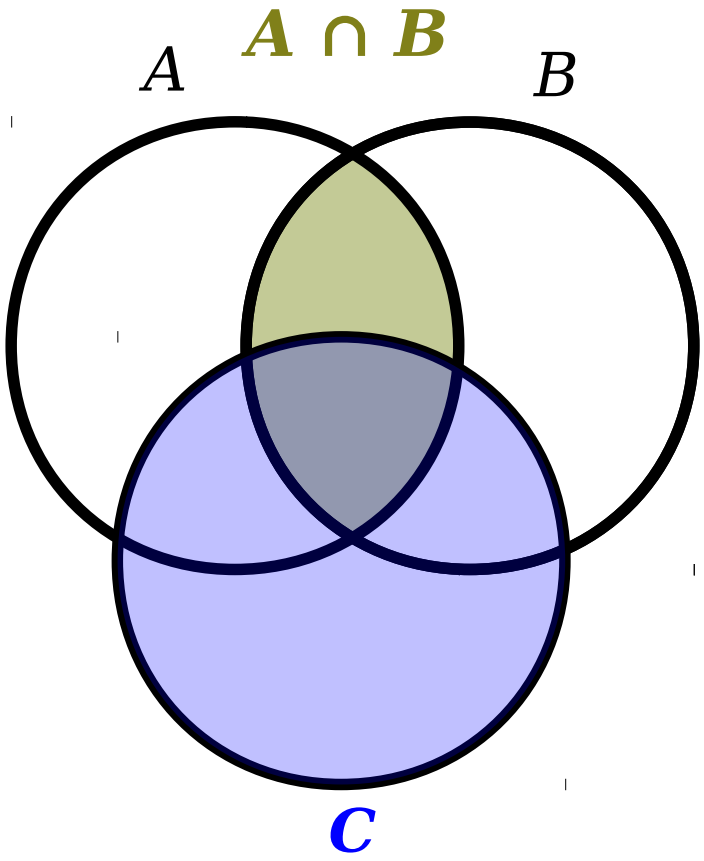
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

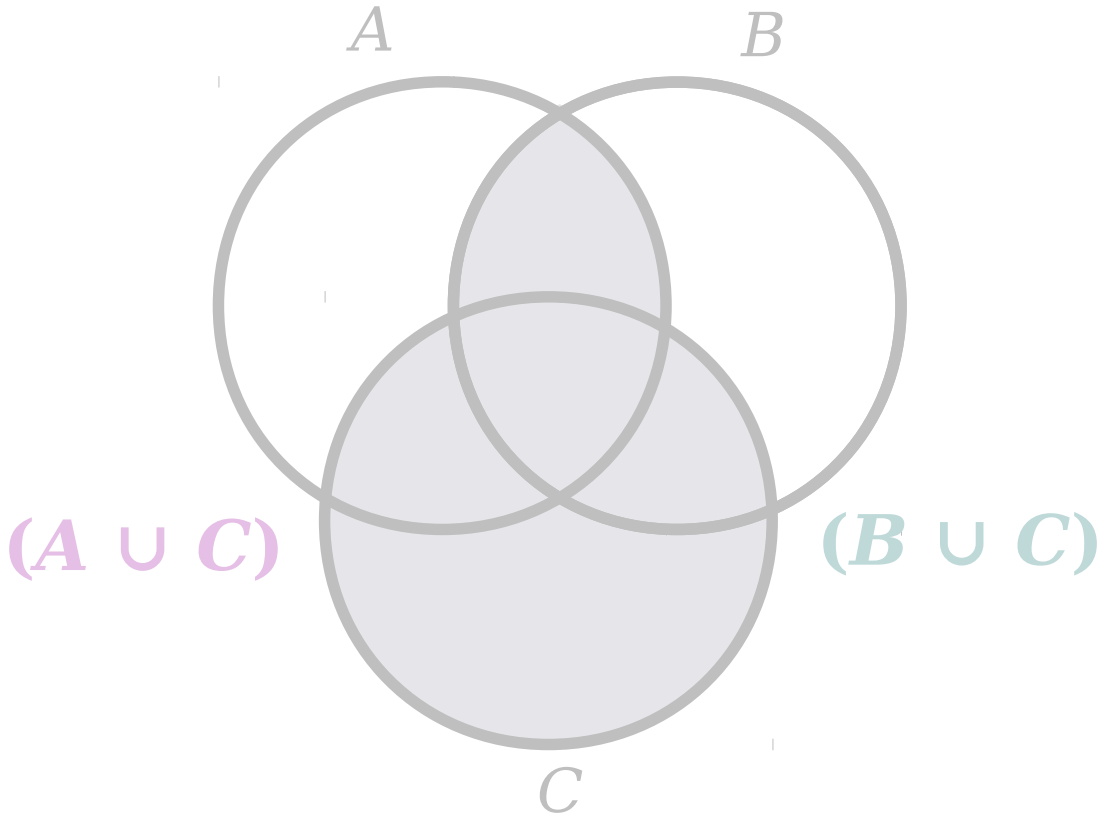
Let's Draw Some Pictures!



Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

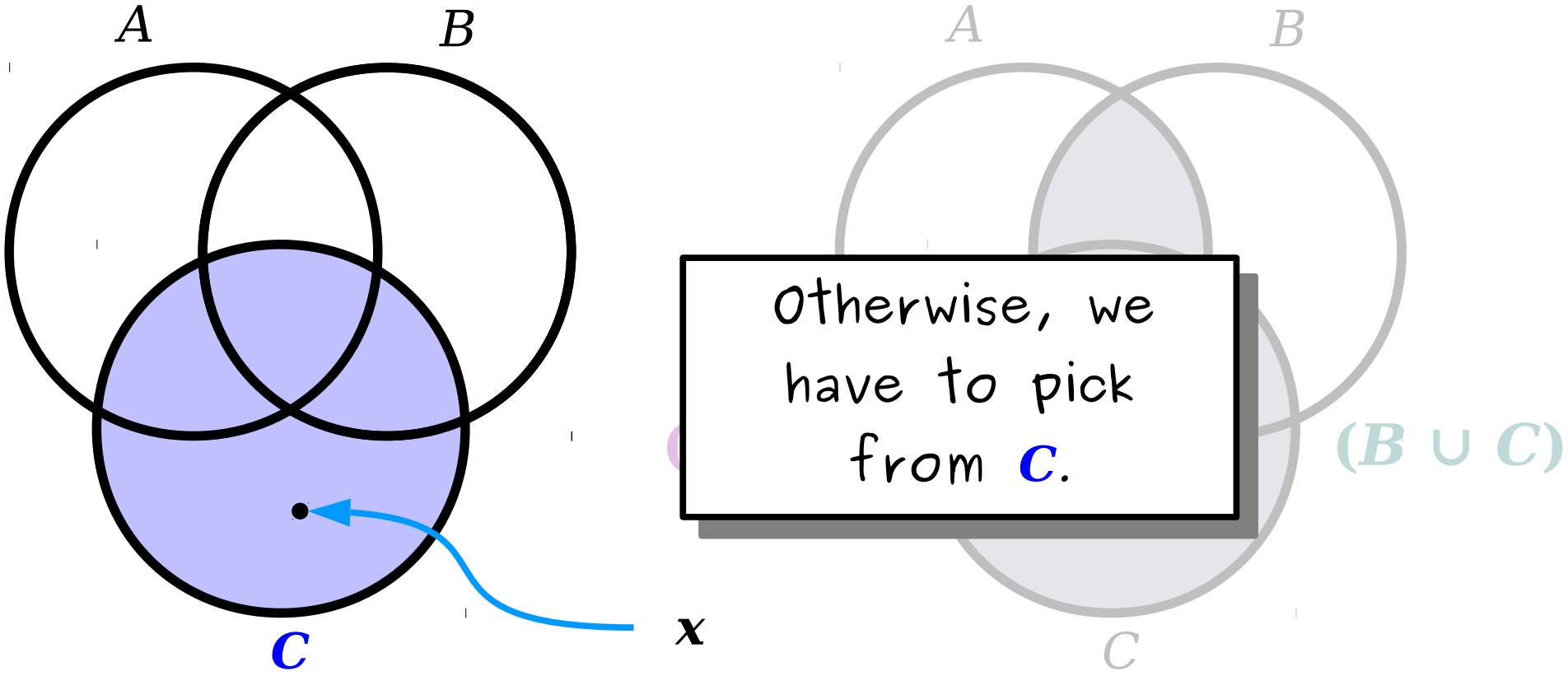
Let's Draw Some Pictures!





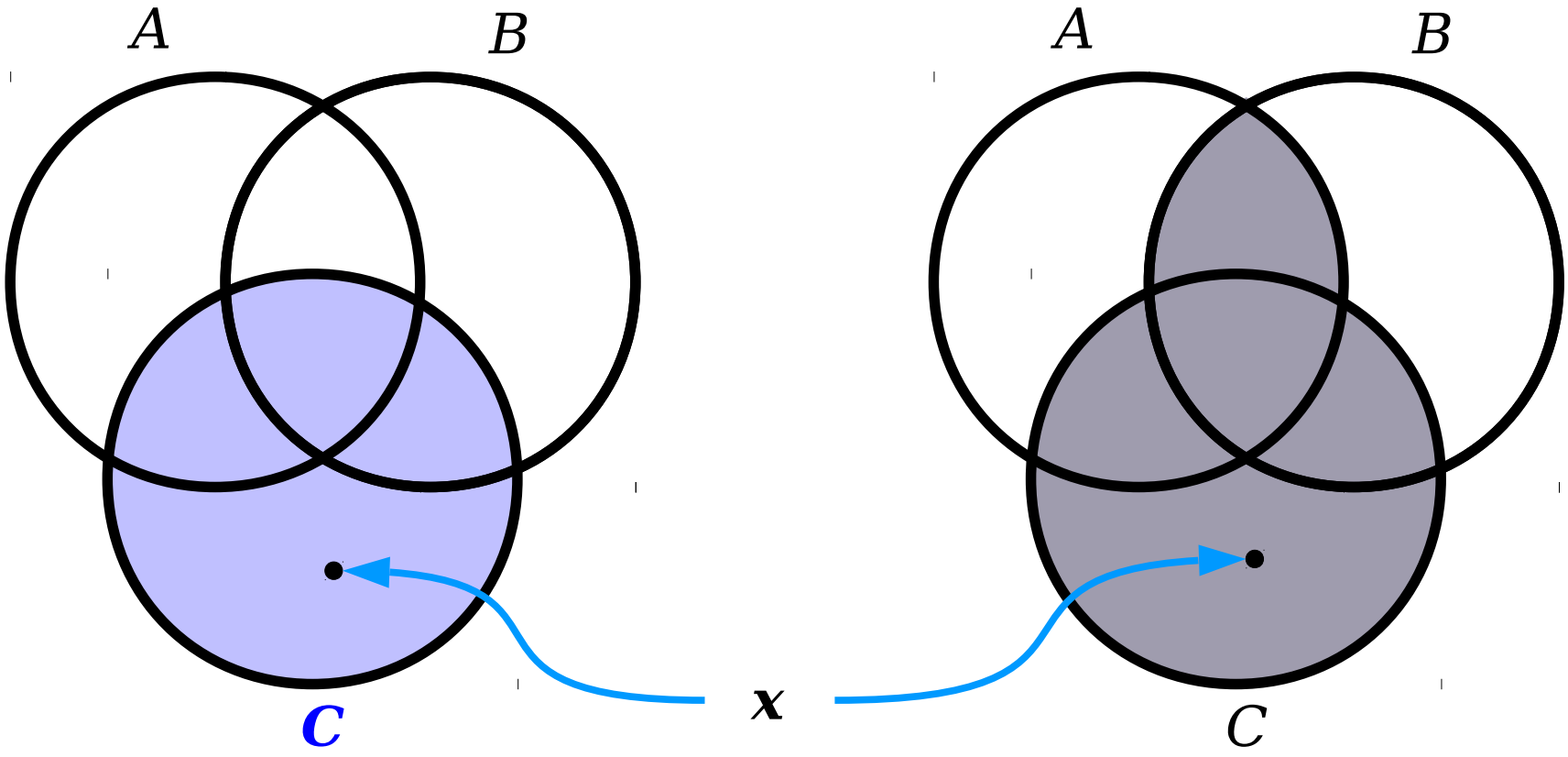
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



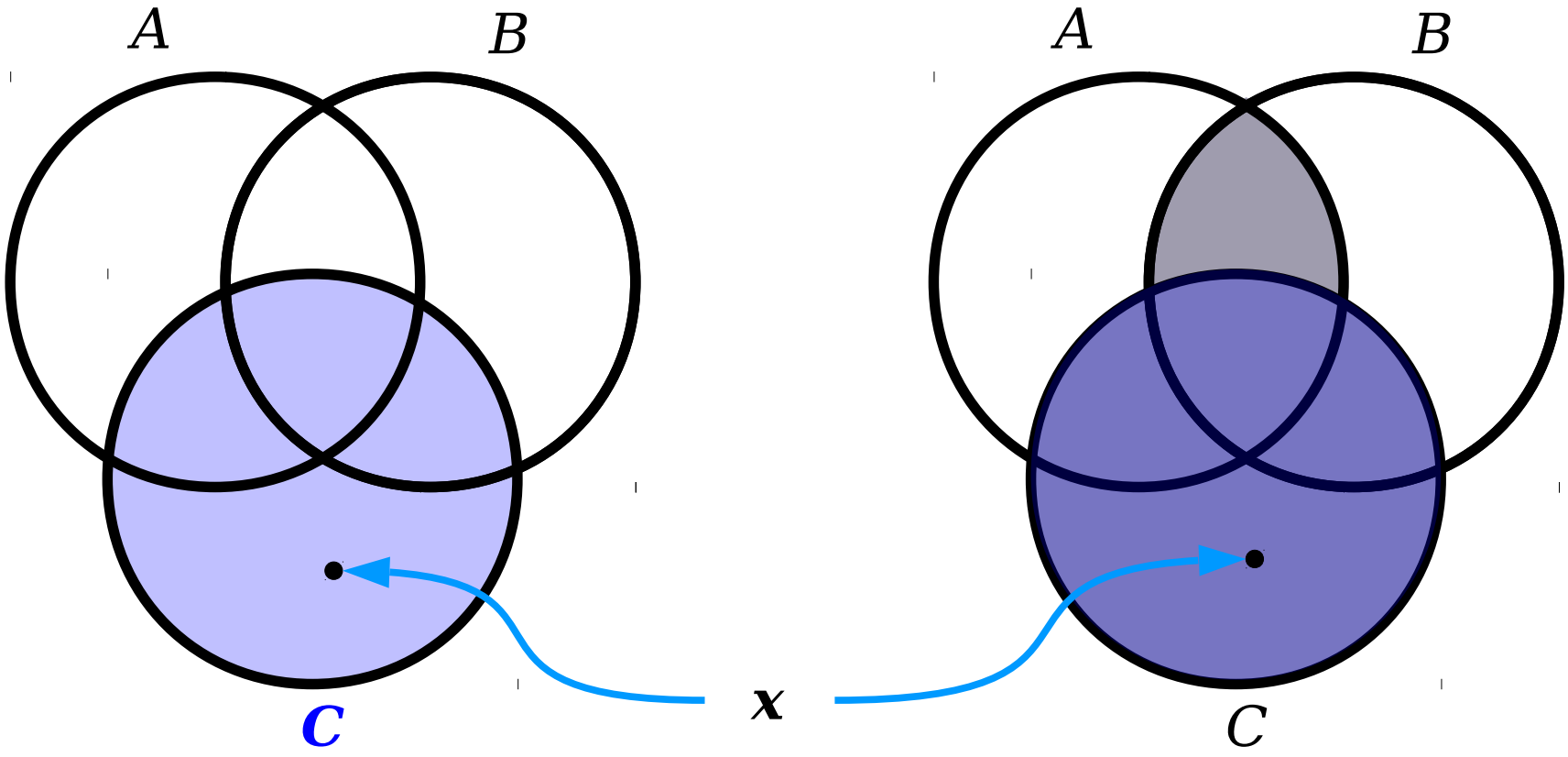
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



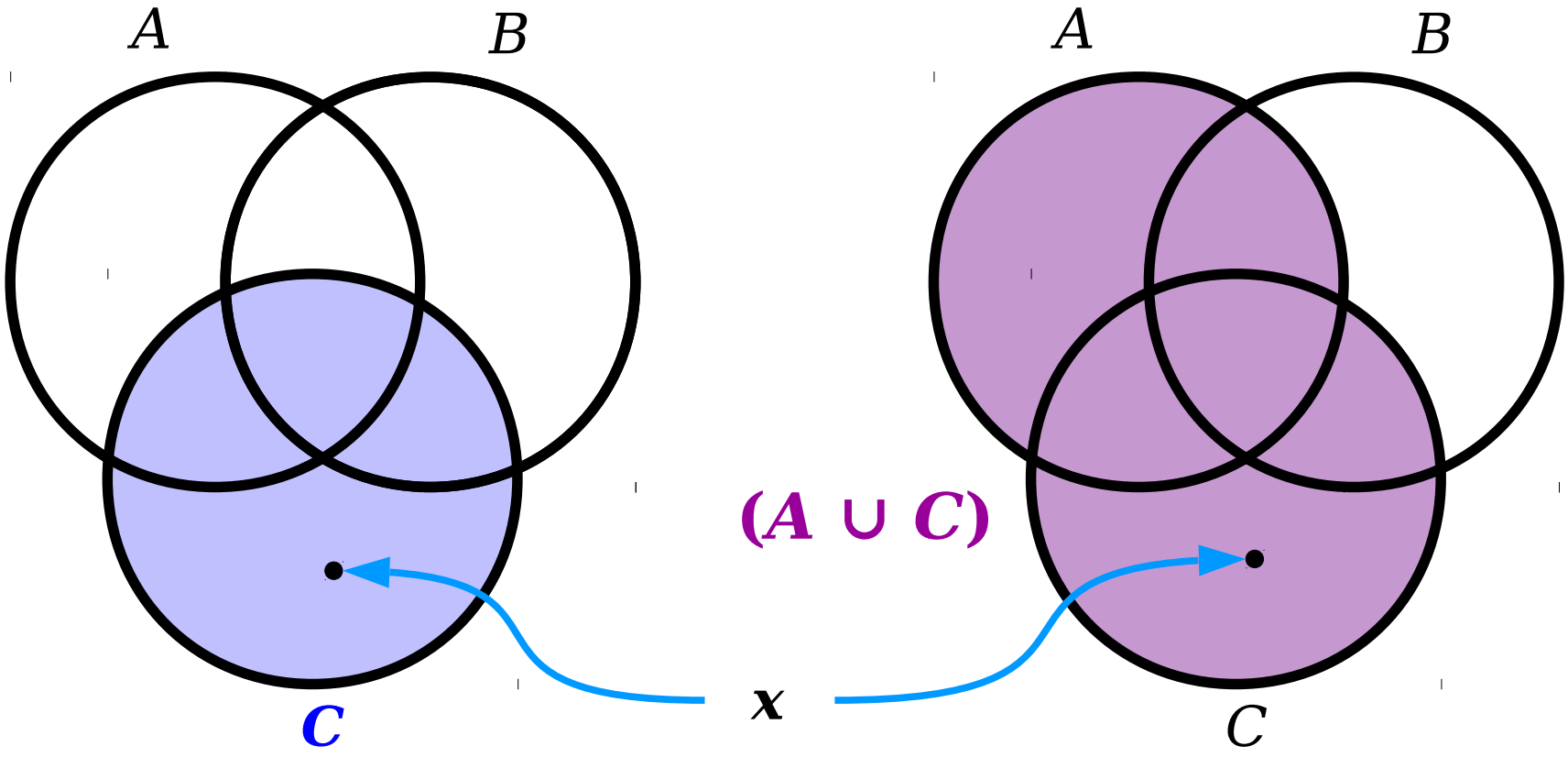
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



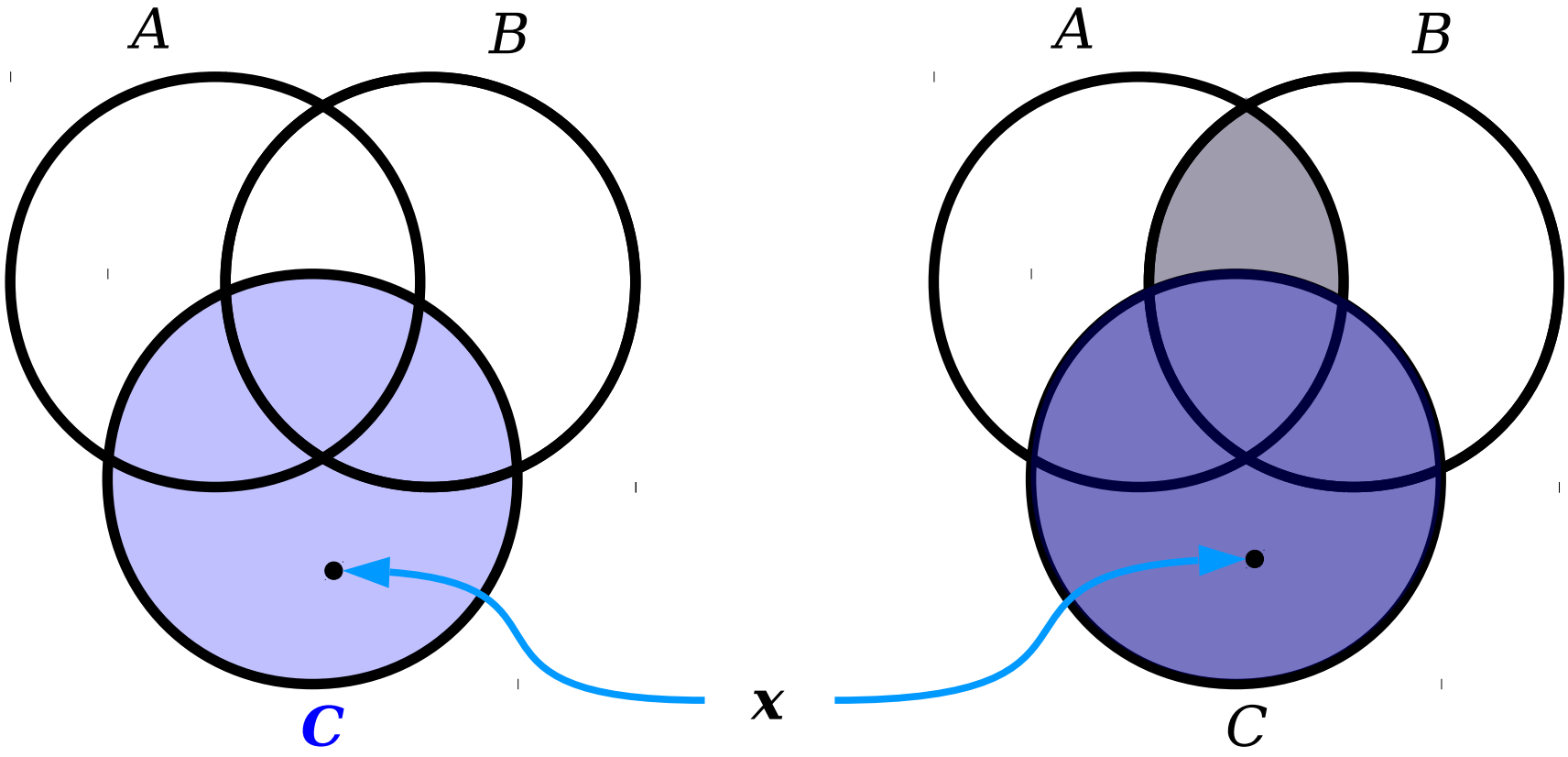
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



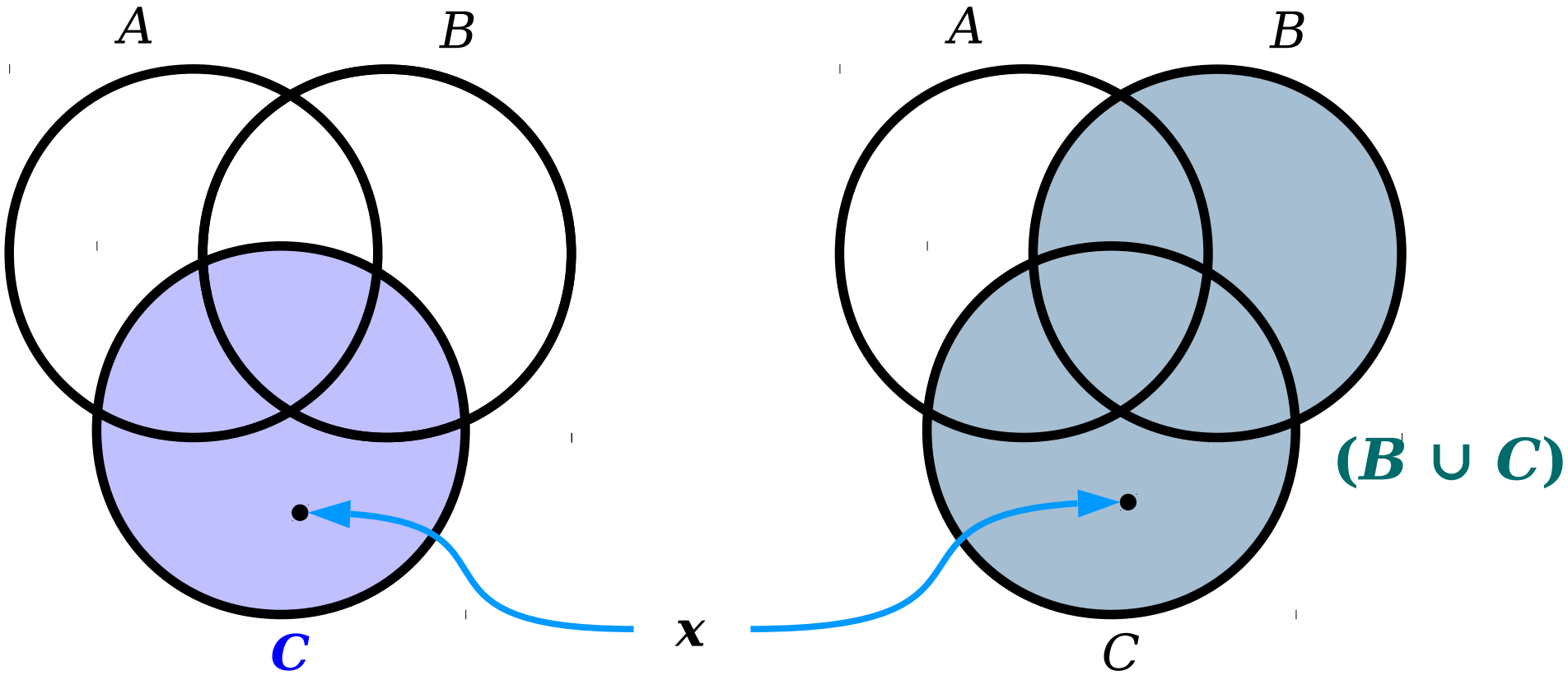
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

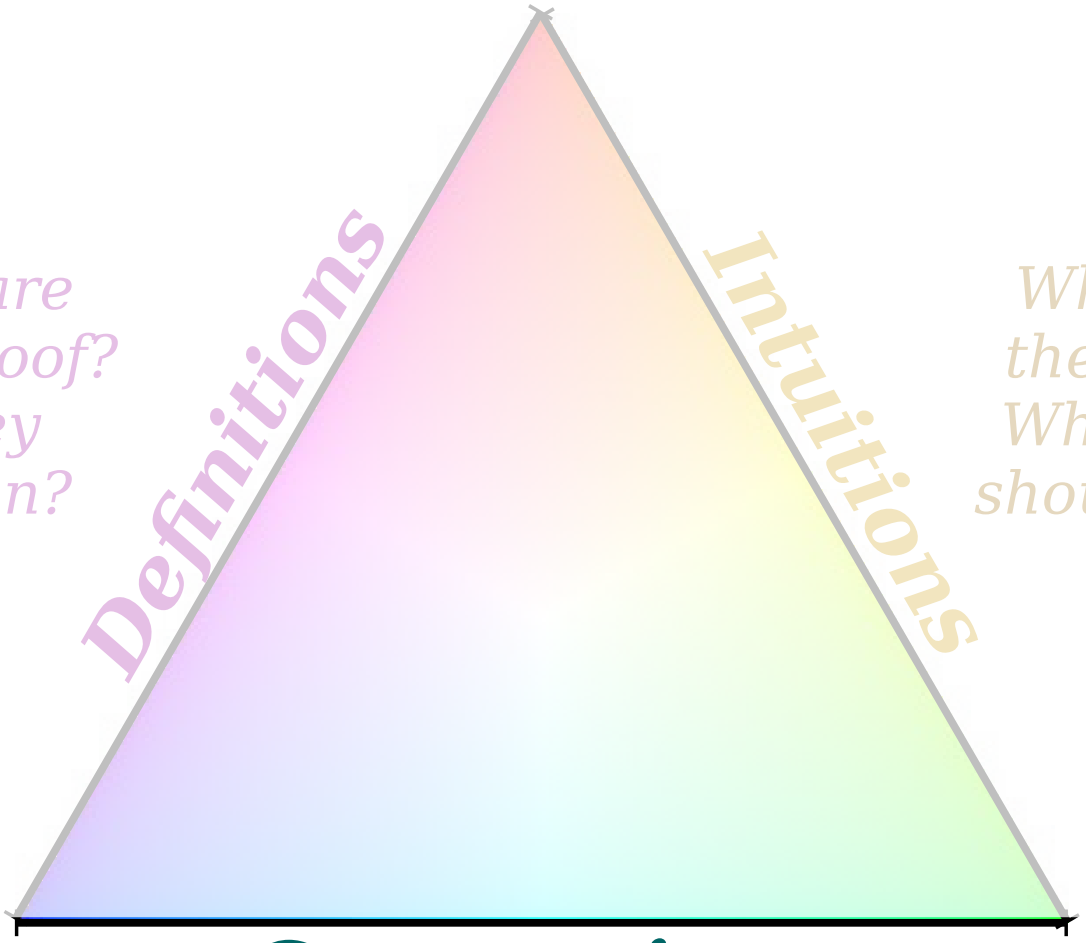
Let's Draw Some Pictures!



Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

What terms are used in this proof? What do they formally mean?



What does this theorem mean? Why, intuitively, should it be true?

Conventions

What is the standard format for writing a proof? What are the techniques for doing so?

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof:

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$.

Case 2: $x \in A \cap B$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$. This establishes that $x \in (A \cup C) \cap (B \cup C)$, as required.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$. This establishes that $x \in (A \cup C) \cap (B \cup C)$, as required. ■

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$. This establishes that $x \in (A \cup C) \cap (B \cup C)$, as required. ■

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since x [illegible] that $x \in C$. We cons[illegible]

Case [illegible] and tha[illegible]

Case [illegible] $x \in$ [illegible]

$x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$. This establishes that $x \in (A \cup C) \cap (B \cup C)$, as required. ■

These are *arbitrary choices*. Rather than specifying what ***A***, ***B***, ***C***, and ***x*** are, we're signaling to the reader that they could, in principle, supply any choices of ***A***, ***B***, ***C***, and ***x*** that they'd like.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that

If you assume that $x \in S \cup T$:

Consider two cases: Case 1: $x \in S$. Case 2: $x \in T$.

If you assume that $x \in S \cap T$:

Assume $x \in S$ and $x \in T$.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$,

To prove that $x \in S \cup T$:
Prove either that $x \in S$ or that $x \in T$ (or both).

To prove that $x \in S \cap T$:
Prove both that $x \in S$ and that $x \in T$.

Case 1: ***$x \in C$***. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: ***$x \in A \cap B$***. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$. This establishes that $x \in (A \cup C) \cap (B \cup C)$, as required. ■

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that x [illegible] $x \in A \cup C$ and th[illegible]

In either case, we lear[illegible] establishes that $x \in (A$[illegible]

This is called a proof by cases (alternatively, a proof by exhaustion) and works by showing that the theorem is true regardless of what specific outcome arises.

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary … y $x \in (A \cap B) \cup C$. We w…

Since $x \in (A \cap B) \cup C$, … $\in C$. We consider each case…

> After splitting into cases, it's a good idea to summarize what you just did so that the reader knows what to take away from it.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$. This establishes that $x \in (A \cup C) \cap (B \cup C)$, as required. ■

Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Proof: Consider arbitrary sets A, B, and C, then choose any $x \in (A \cap B) \cup C$. We will prove $x \in (A \cup C) \cap (B \cup C)$.

Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

Case 1: $x \in C$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

Case 2: $x \in A \cap B$. From $x \in A \cap B$, we learn that $x \in A$ and that $x \in B$. Therefore, we know that $x \in A \cup C$ and that $x \in B \cup C$.

In either case, we learn that $x \in A \cup C$ and $x \in B \cup C$. This establishes that $x \in (A \cup C) \cap (B \cup C)$, as required. ■

	Is defined as…	To ***prove*** that this is true…	If you ***assume*** this is true…
$x \in S \cap T$	$x \in S$ and $x \in T$	Prove $x \in A$. Then prove $x \in B$.	Assume $x \in A$. Then assume $x \in B$.
$x \in S \cup T$	$x \in S$ or $x \in T$	Prove either $x \in S$ or that $x \in T$.	Consider two cases: Case 1: $x \in$ S. Case 2: $x \in T$.
$S \subseteq T$	For every $x \in S$, we have $x \in T$	Pick an arbitrary $x \in S$. Prove $x \in T$.	Initially, ***do nothing***. Once you find some $x \in S$, conclude $x \in T$.
$S = T$	$S \subseteq T$ and $T \subseteq S$	Prove $S \subseteq T$. Then prove $T \subseteq S$.	Assume $S \subseteq T$ and $T \subseteq S$.
$X \in \wp(A)$	$X \subseteq A$.	Prove $X \subseteq A$.	Assume $X \subseteq A$.

For more details, see the Guide to Proofs on Sets.

Next Time

- ***Mathematical Logic***
  - How do we formalize the reasoning from our proofs?
- ***Propositional Logic***
  - Reasoning about simple statements.
- ***Propositional Equivalences***
  - Simplifying complex statements.

Appendix: Proving Implications by Contradiction

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***
  - ***Proof by Contrapositive.***
  - ***Proof by Contradiction.***

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P* is true**, then prove ***Q* is true**.
  - ***Proof by Contrapositive.***
  - ***Proof by Contradiction.***

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P* is true**, then prove ***Q* is true**.
  - ***Proof by Contrapositive.***

    Assume ***Q* is false**, then prove that ***P* is false**.
  - ***Proof by Contradiction.***

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P* is true**, then prove ***Q* is true**.
  - ***Proof by Contrapositive.***

    Assume ***Q* is false**, then prove that ***P* is false**.
  - ***Proof by Contradiction.***

    … what does this look like?

Theorem: For any integer n, if n^2 is even, then n is even.

Theorem: For any integer n, if n^2 is even, then n is even.

What is the negation of our theorem?

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$n^2 = (2k + 1)^2$$

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned} \tag{2}$$

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect.

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well.

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned} \tag{2}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such

The three key pieces:

1. Say that the proof is by contradiction.
2. Say what the negation of the original statement is.
3. Say you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned} \tag{2}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P* is true**, then prove ***Q* is true**.
  - ***Proof by Contrapositive.***

    Assume ***Q* is false**, then prove that ***P* is false**.
  - ***Proof by Contradiction.***

    Assume ***P is true*** and ***Q is false***,
    then derive a contradiction.