Mathematical Proofs

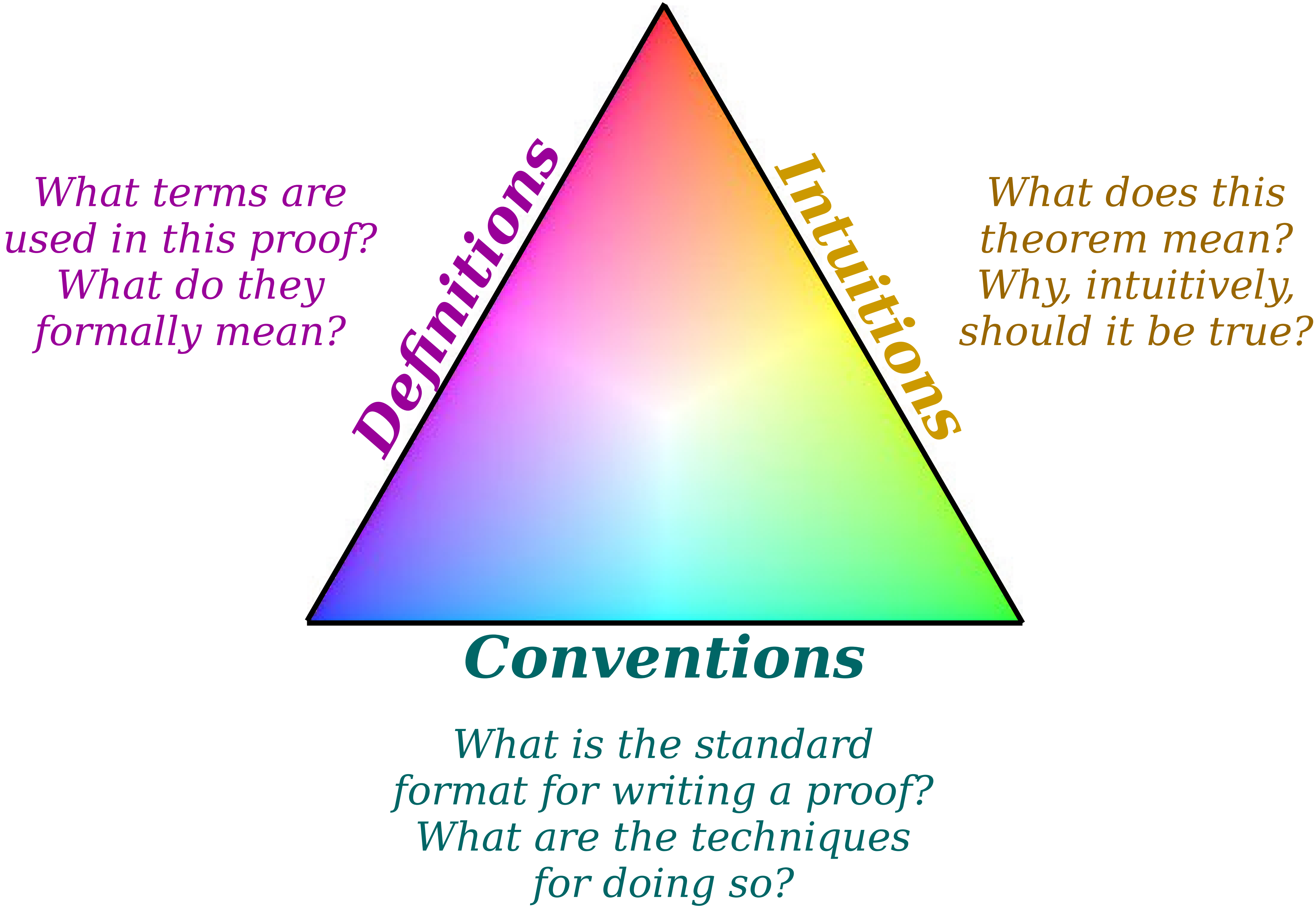
Outline for Today

- ***How to Write a Proof***
  - Synthesizing definitions, intuitions, and conventions.
- ***Proofs on Numbers***
  - Working with odd and even numbers.
- ***Universal and Existential Statements***
  - Two important classes of statements.
- ***Proofs on Sets***
  - From Venn diagrams to rigorous math.

What is a Proof?

A ***proof*** is an argument that demonstrates why a conclusion is true, subject to certain standards of truth.

A ***mathematical proof*** is an argument that demonstrates why a mathematical statement is true, following the rules of mathematics.

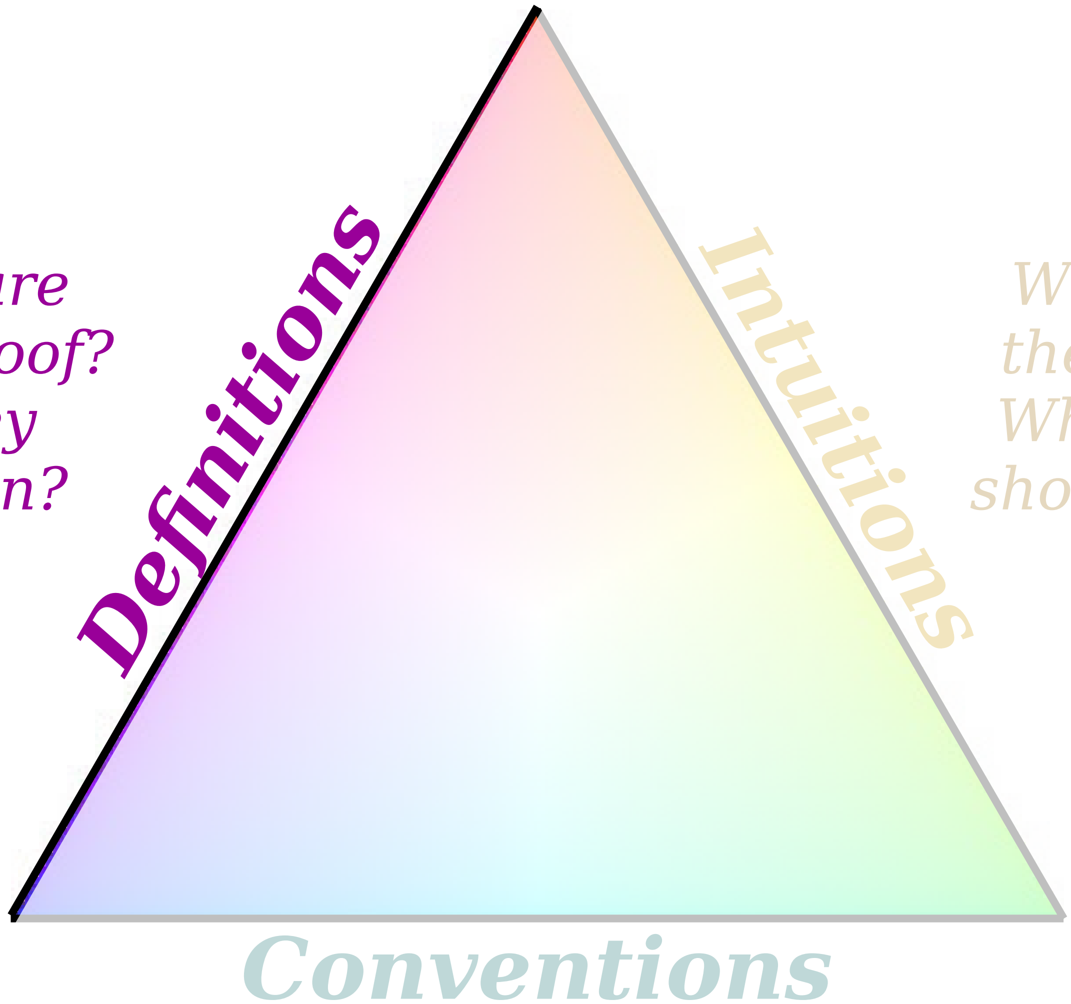


What terms are used in this proof? What do they formally mean?
Definitions
Intuitions
What does this theorem mean? Why, intuitively, should it be true?
Conventions
What is the standard format for writing a proof? What are the techniques for doing so?

Writing our First Proof

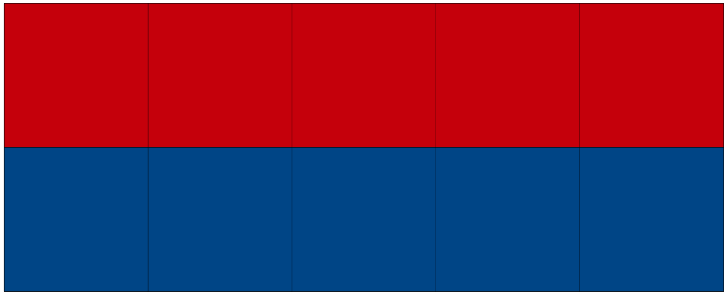
Theorem: If n is an even integer, then n^2 is even.

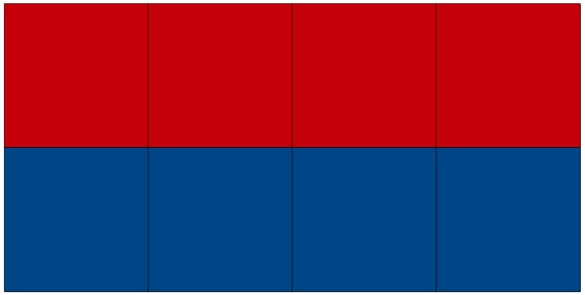
What terms are used in this proof? What do they formally mean?



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

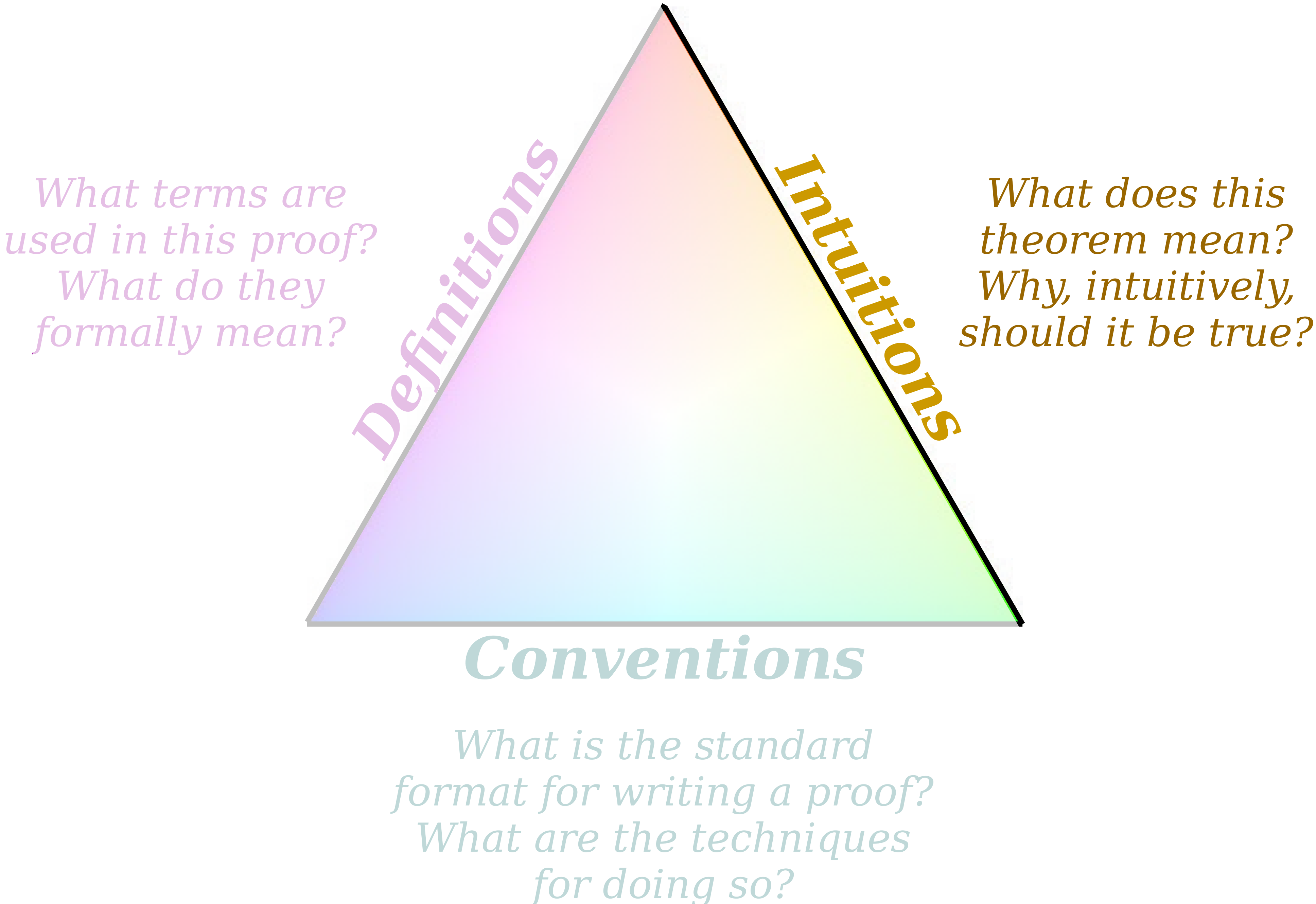
What is the standard format for writing a proof? What are the techniques for doing so?

10  $2 \cdot \mathbf{5}$

8  $2 \cdot \mathbf{4}$

0 $2 \cdot \mathbf{0}$

An integer n is called ***even*** if
there is an integer k where $n = 2k$.


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

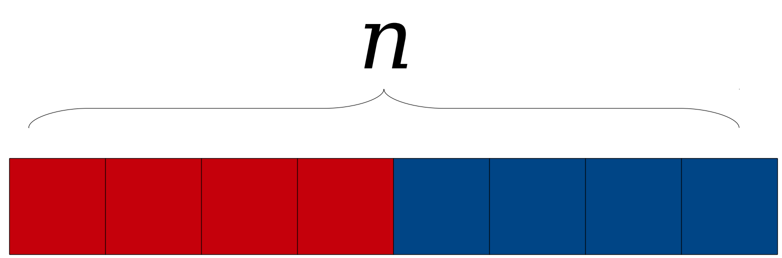
Let's Try Some Examples!

$$
\begin{aligned}
2^2 &= 4 &&= 2 \cdot \mathbf{2} \\
10^2 &= 100 &&= 2 \cdot \mathbf{50} \\
0^2 &= 0 &&= 2 \cdot \mathbf{0} \\
(-8)^2 &= 64 &&= 2 \cdot \mathbf{32} \\
n^2 & &&= 2 \cdot \mathbf{?}
\end{aligned}
$$

What's the pattern? How do we predict this?

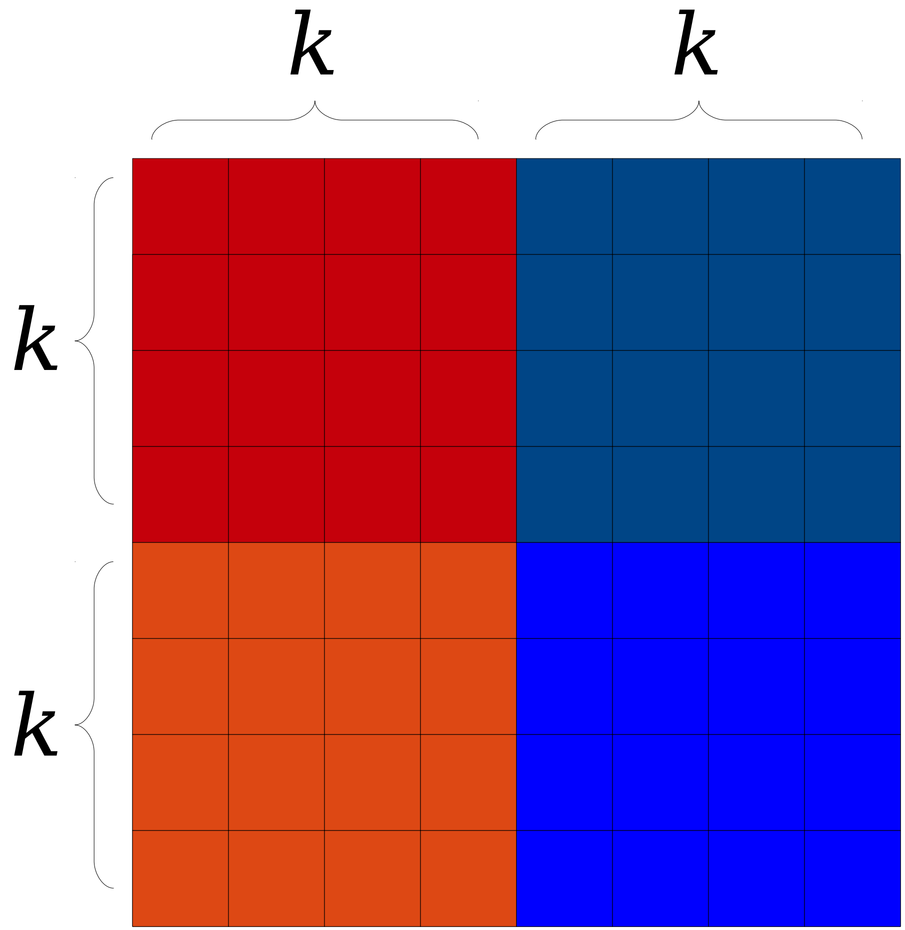
Theorem: If n is an even integer, then n^2 is even.

Let’s Draw Some Pictures!



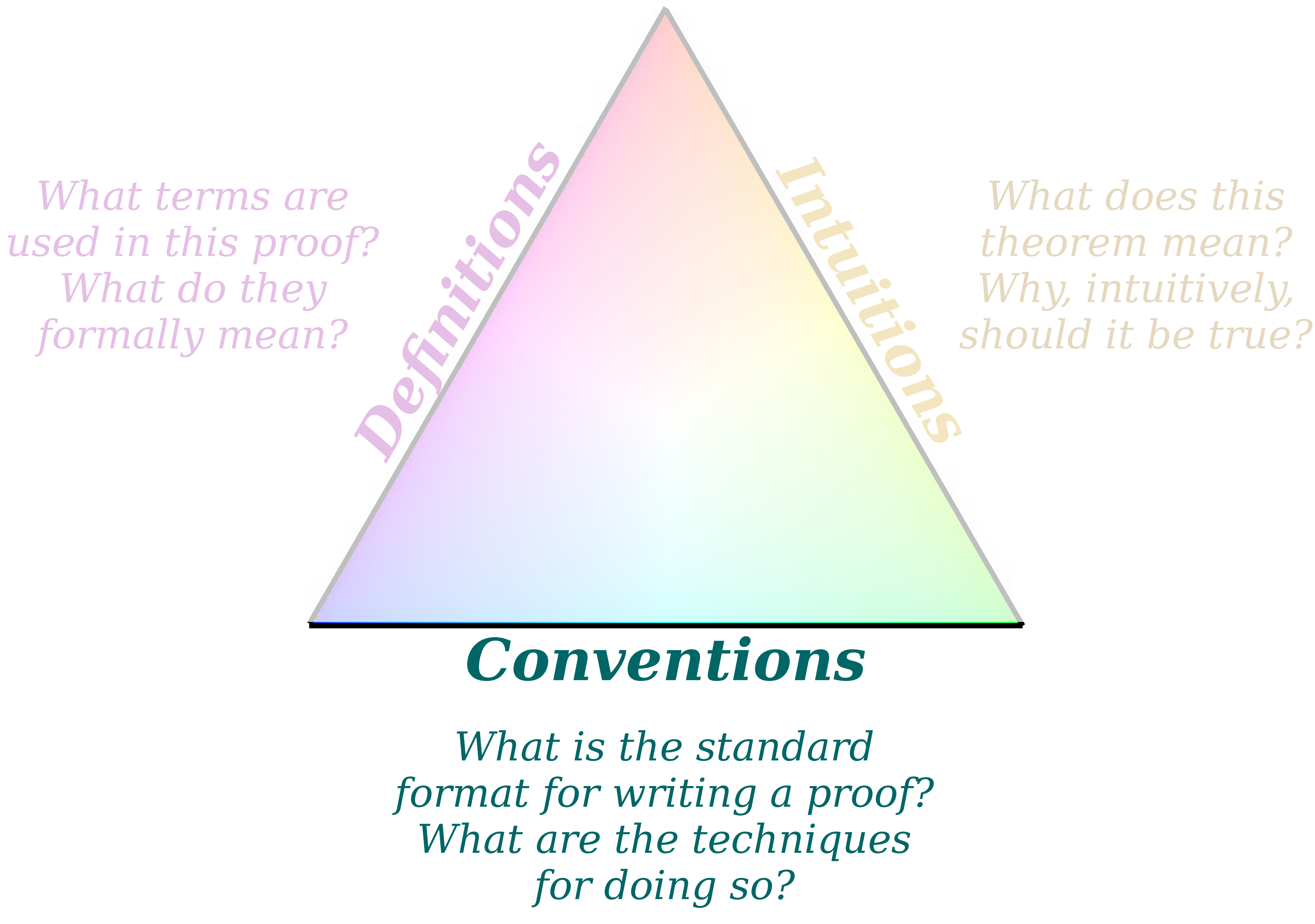
Theorem: If n is an even integer, then n^2 is even.

Let’s Draw Some Pictures!



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

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



Definitions
Intuitions
Conventions
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?

Our First Proof! 😃

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

This symbol means "end of proof"

Our First Proof! 😃

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

Since n i
such tha

This mea

From thi
m (name

Therefor

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

Our First Proof! 😃

Theorem: If n is an even integer, then n^2 is even.
Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means th … ^{2}).

From this, we … er
m (namely, $2k$ …

Therefore, n^2 …

This is the definition of an even integer. We need to use this definition to make this proof rigorous.

Our First Proof! 😃

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

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

Fr

m

Th

Notice how we use the value of $\boldsymbol{k}$ that we obtained above. Giving names to quantities, even if we aren't fully sure what they are, allows us to manipulate them. This is similar to variables in programs.

Our First Proof! 😃

Theorem: If n ... en.
Proof: Let n b...

Since n ...
such th...

Our ultimate goal is to prove that $\boldsymbol{n^2}$ is even. This means that we need to find some $\boldsymbol{m}$ such that $\boldsymbol{n^2 = 2m}$. Here, we're explicitly showing how we can do that.

This me... ^{2}).

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

Therefore, n^2 is even. ■

Our First Proof! 😃

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

Proof: Let n be an even integer.

Since n is even, there is some integer k such tha

This mea).

From thi r
m (name

Hey, that's what we were trying to show! We're done now.

Therefore, n^2 is even. ■

Our First Proof! 😃

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

Proof: Let n be an even integer.

Since n is even, there is some integer k such that $n = 2k$.

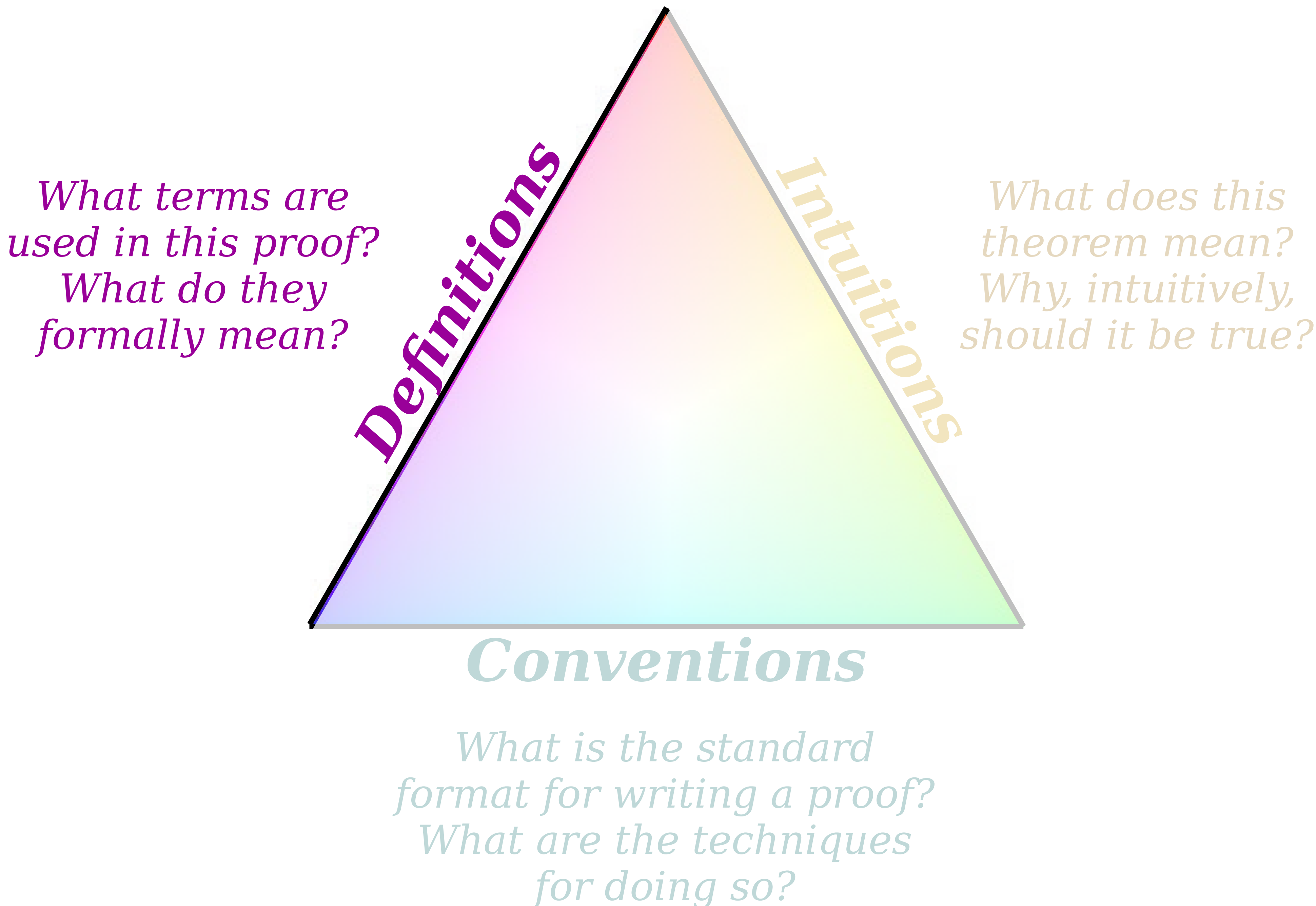
This means that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

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

Therefore, n^2 is even. ■

Our Next Proof

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

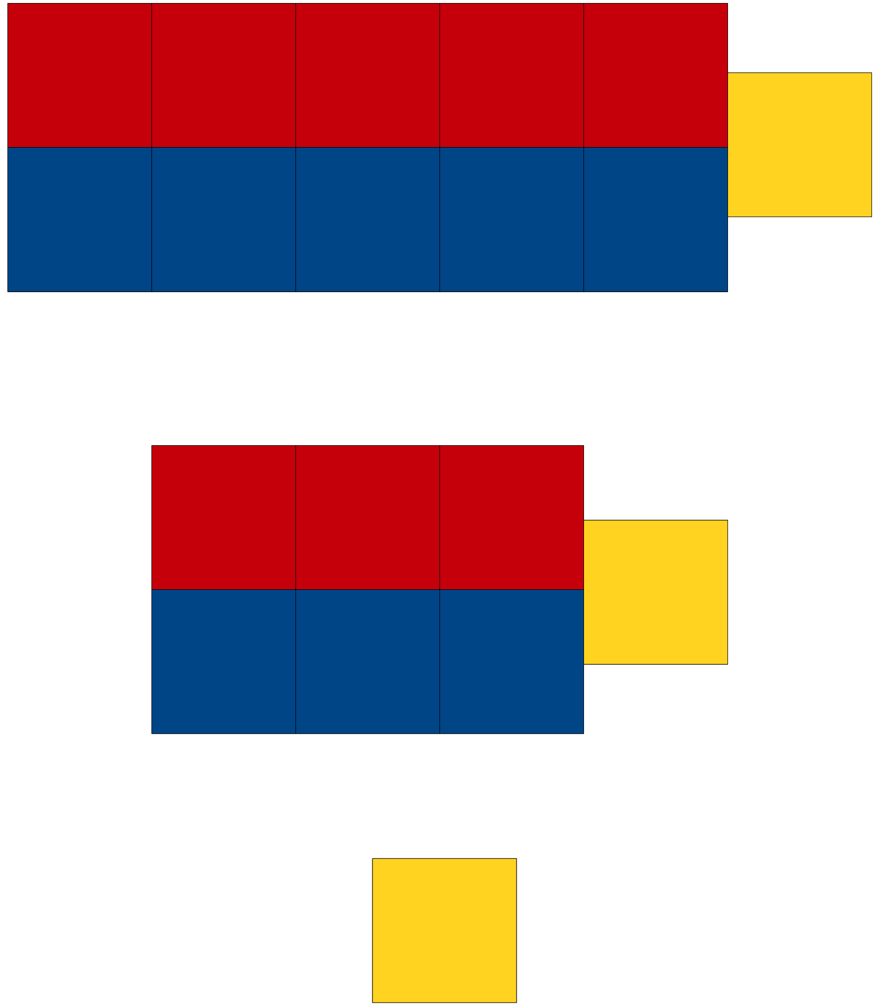


Definitions
Intuitions
Conventions
What terms are used in this proof? What do they formally mean?
What does this theorem mean? Why, intuitively, should it be true?
What is the standard format for writing a proof? What are the techniques for doing so?

11 $\quad 2 \cdot \mathbf{5} + \mathbf{1}$

7 $\quad 2 \cdot \mathbf{3} + \mathbf{1}$

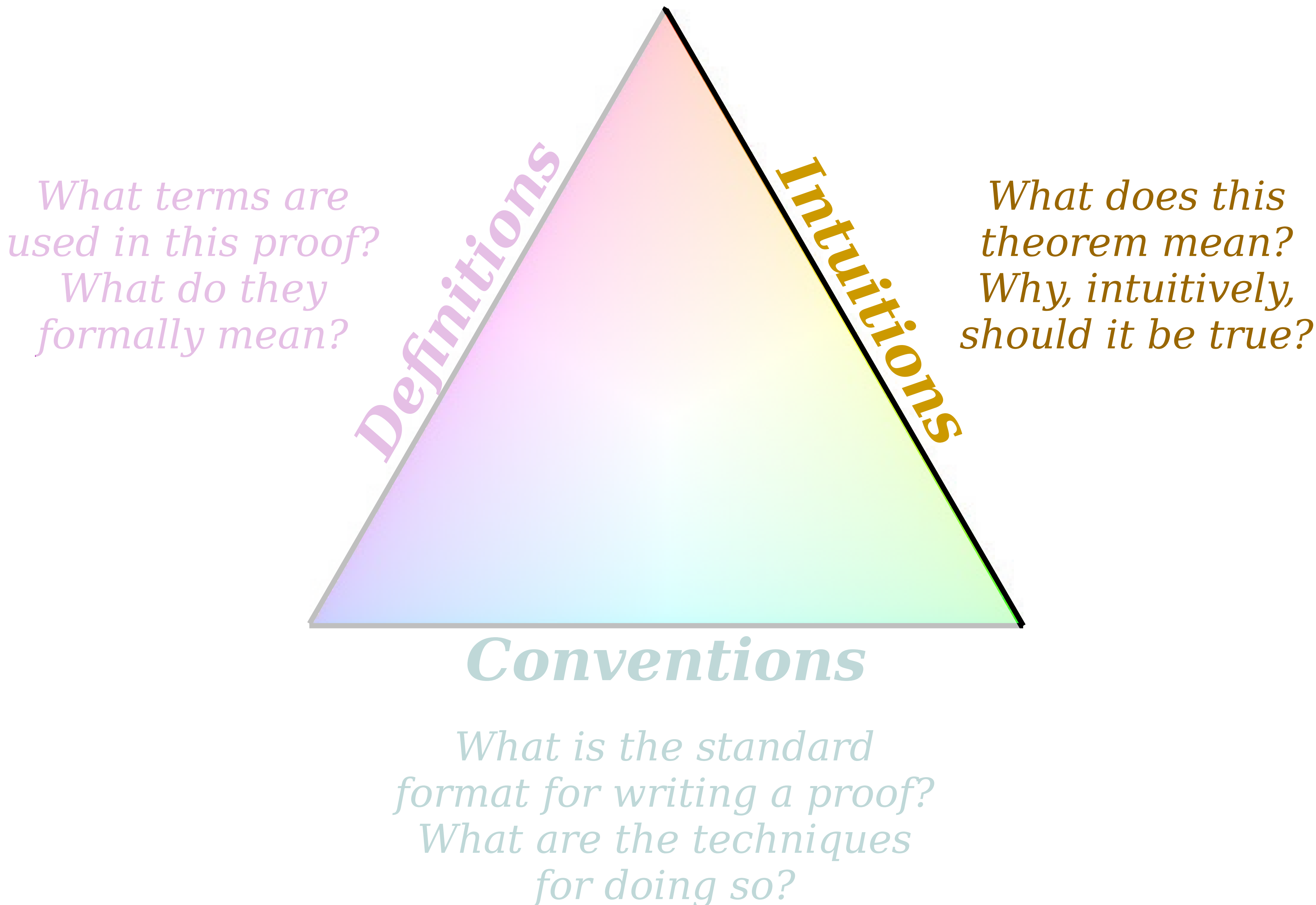
1 $\quad 2 \cdot \mathbf{0} + \mathbf{1}$



An integer n is called ***odd*** if there is an integer k where $n = 2k+1$.

Going forward, we'll assume the following:

1. Every integer is either even or odd.
2. No integer is both even and odd.


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

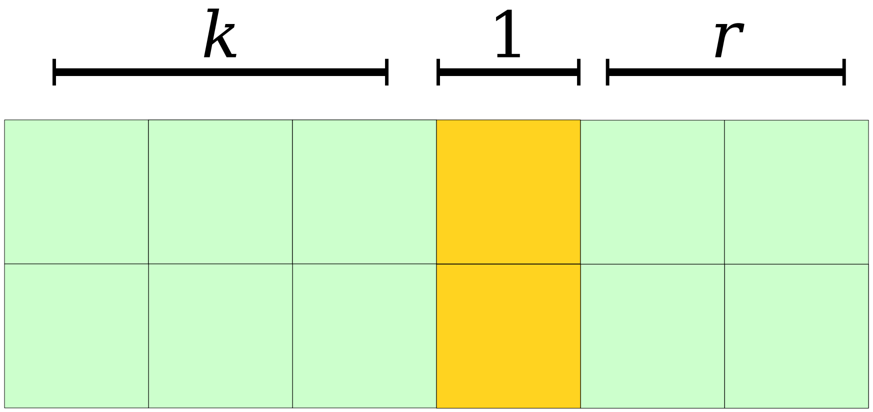
Let's Try Some Examples!

$$\begin{aligned} 1 + 1 &= 2 &&= 2 \cdot \mathbf{1} \\ 137 + 103 &= 240 &&= 2 \cdot \mathbf{120} \\ -5 + 5 &= 0 &&= 2 \cdot \mathbf{0} \\ m + n & &&= 2 \cdot \mathbf{?} \end{aligned}$$

What's the pattern? How do we predict this?

Theorem: For any integers m and n, if m and n are odd, then $m+n$ is even.

Let's Do Some Math!

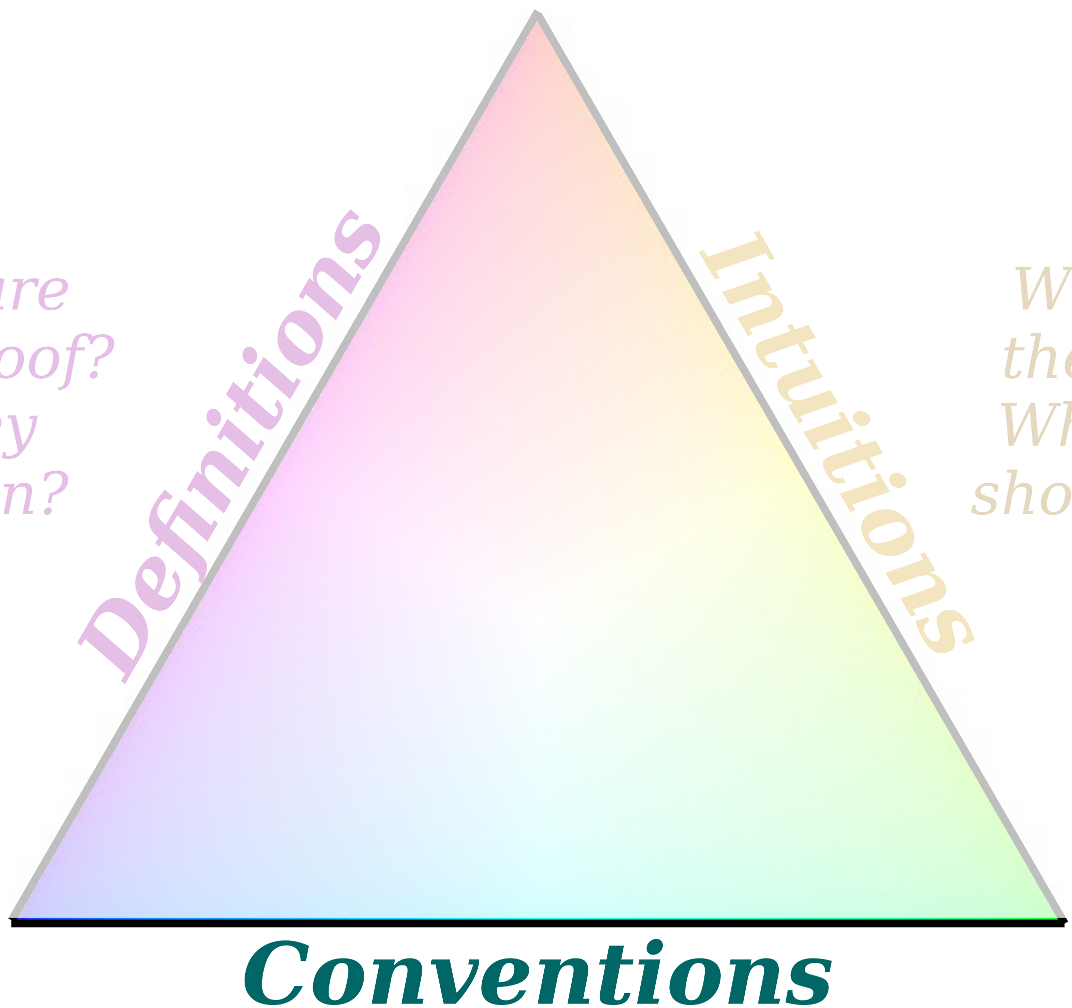


$2k+1$

$2r+1$

$$(2k+1) + (2r+1) = 2(k + r + 1)$$

Theorem: For any integers m and n,
if m and n are odd, then $m+n$ is even.



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: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

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

Similarly, because n is odd there must be some integer r such that

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

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

$$m = 2k + 1 \quad (1)$$

Similarl… such that

By addi…

Equatio… $+ r + 1)$ such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

This is called making arbitrary choices.
Rather than specifying what m and n are, we're signaling to the reader that they could, in principle, supply any choices of m and n that they'd like.

By picking m and n arbitrarily, anything we prove about m and n will generalize to all possible choices we could have made.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

)

Similarly, bec er r such that

To prove a statement of the form

"If *P*, then *Q*"

Assume that ***P*** is true, then show that ***Q*** must be true as well.

By adding eq

$$= 2k + 2r + 2$$

$$= 2(k + r + 1). \qquad (3)$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Numbering these equalities lets us refer back to them later on, making the flow of the proof a bit easier to understand.

The … d n are odd, then
m …

Proo … d n where m and n are
od … s an integer k where

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

Similarly, because n is odd there must be some integer r such that

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

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \qquad (3) \end{aligned}$$

Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

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

Similarly, because n is odd there must be some integer r such that

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

hat

1

(3)

er s (namely, $k + r + 1$)

hat $m + n$ is even, as

This is a complete sentence! Proofs are expected to be written in complete sentences, so you'll often use punctuation at the end of formulas.

We recommend using the "mugga mugga" test – if you read a proof and replace all the mathematical notation with "mugga mugga," what comes back should be a valid sentence.

Theorem: For any integers m and n, if m and n are odd, then $m + n$ is even.

Proof: Consider any arbitrary integers m and n where m and n are odd. Since m is odd, we know that there is an integer k where

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

Similarly, because n is odd there must be some integer r such that

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

By adding equations (1) and (2) we learn that

$$\begin{aligned} m + n &= 2k + 1 + 2r + 1 \\ &= 2k + 2r + 2 \\ &= 2(k + r + 1). \end{aligned} \tag{3}$$

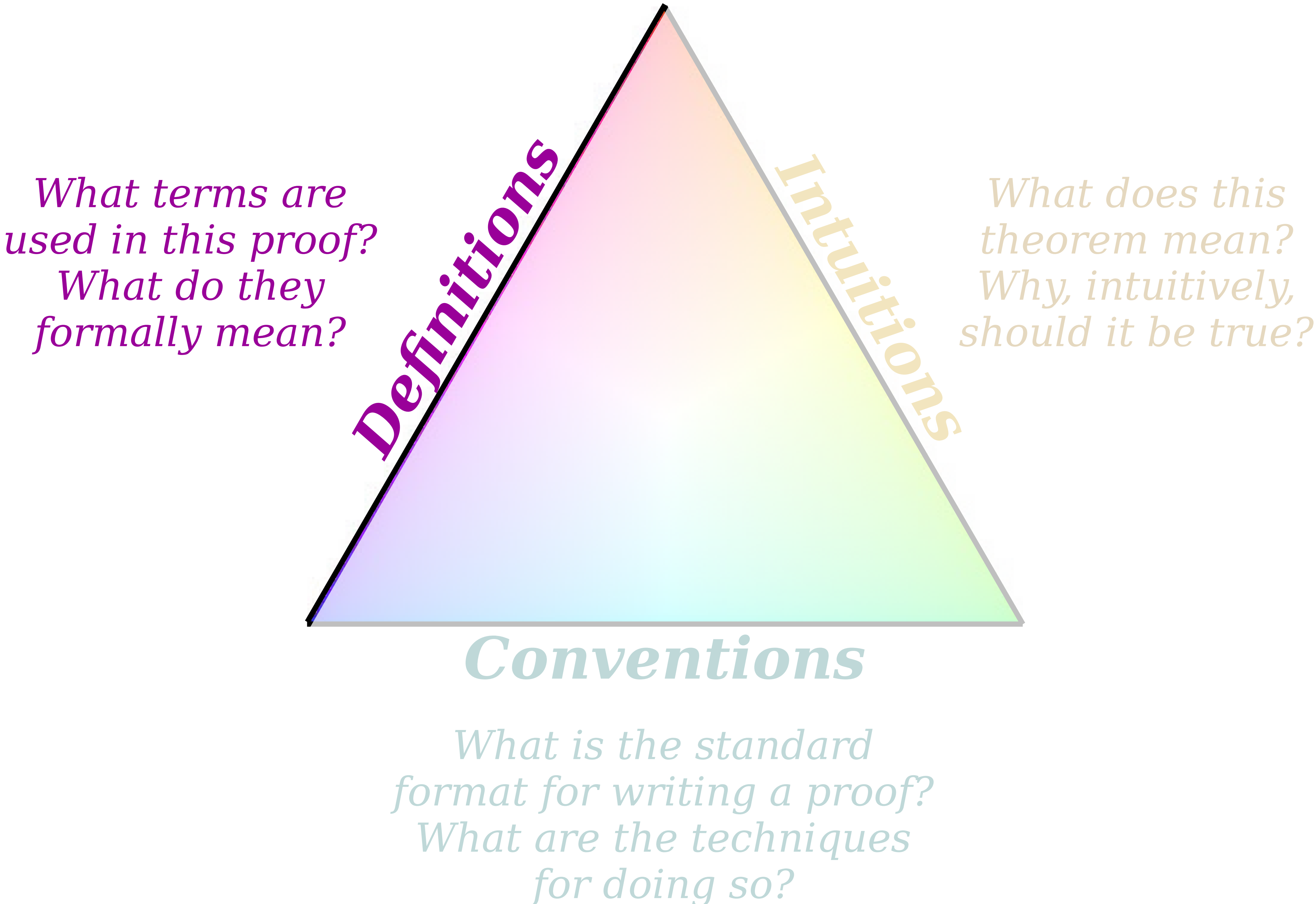
Equation (3) tells us that there is an integer s (namely, $k + r + 1$) such that $m + n = 2s$. Therefore, we see that $m + n$ is even, as required. ■

Some Little Exercises

- Here's a list of other theorems that are true about odd and even numbers:
  - ***Theorem:*** The sum and difference of any two even numbers is even.
  - ***Theorem:*** The sum and difference of an odd number and an even number is odd.
  - ***Theorem:*** The product of any integer and an even number is even.
  - ***Theorem:*** The product of any two odd numbers is odd.
- Going forward, we'll just take these results for granted. Feel free to use them in the problem sets.
- If you'd like to practice the techniques from today, try your hand at proving these results!

Universal and Existential Statements

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.


What terms are
used in this proof?
What do they
formally mean?
Definitions
Intuitions
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: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

This result is true for every possible choice of odd integer n. It'll work for $n = 1$, $n = 137$, $n = 103$, etc.

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

We aren't saying this is true for every choice of r and s. Rather, we're saying that *somewhere out there* are choices of r and s where this works.

Universal vs. Existential Statements

- A ***universal statement*** is a statement of the form

For all *x*, `[some-property]` holds for *x*.

- We've seen how to prove these statements.
- An ***existential statement*** is a statement of the form

There is some *x* where `[some-property]` holds for *x*.

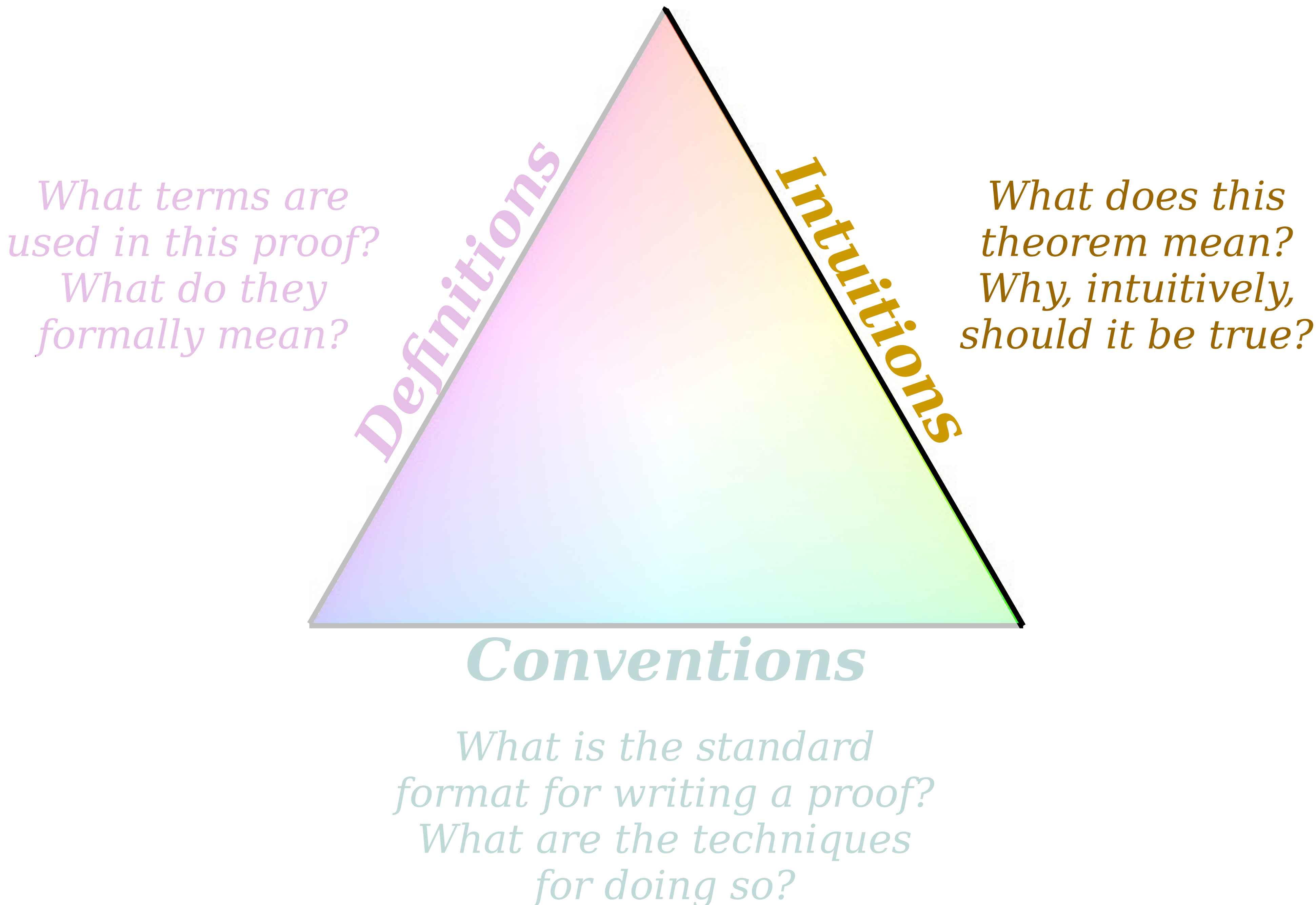
- How do you prove an existential statement?

Proving an Existential Statement

- Over the course of the quarter, we will see several different ways to prove an existential statement of the form

  There is an *x* where `[some-property]` holds for *x*.

- ***Simplest approach:*** Search far and wide, find an *x* that has the right property, then show why your choice is correct.


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

Let’s Try Some Examples!

$$1 = \mathbf{1}^2 - \mathbf{0}^2$$

$$3 = \mathbf{2}^2 - \mathbf{1}^2$$

$$5 = \mathbf{3}^2 - \mathbf{2}^2$$

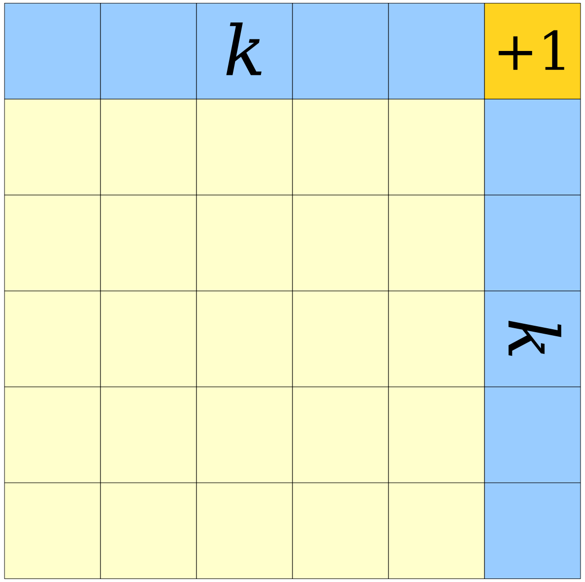
$$7 = \mathbf{4}^2 - \mathbf{3}^2$$

$$9 = \mathbf{5}^2 - \mathbf{4}^2$$

We’ve got a pattern – but why does this work?

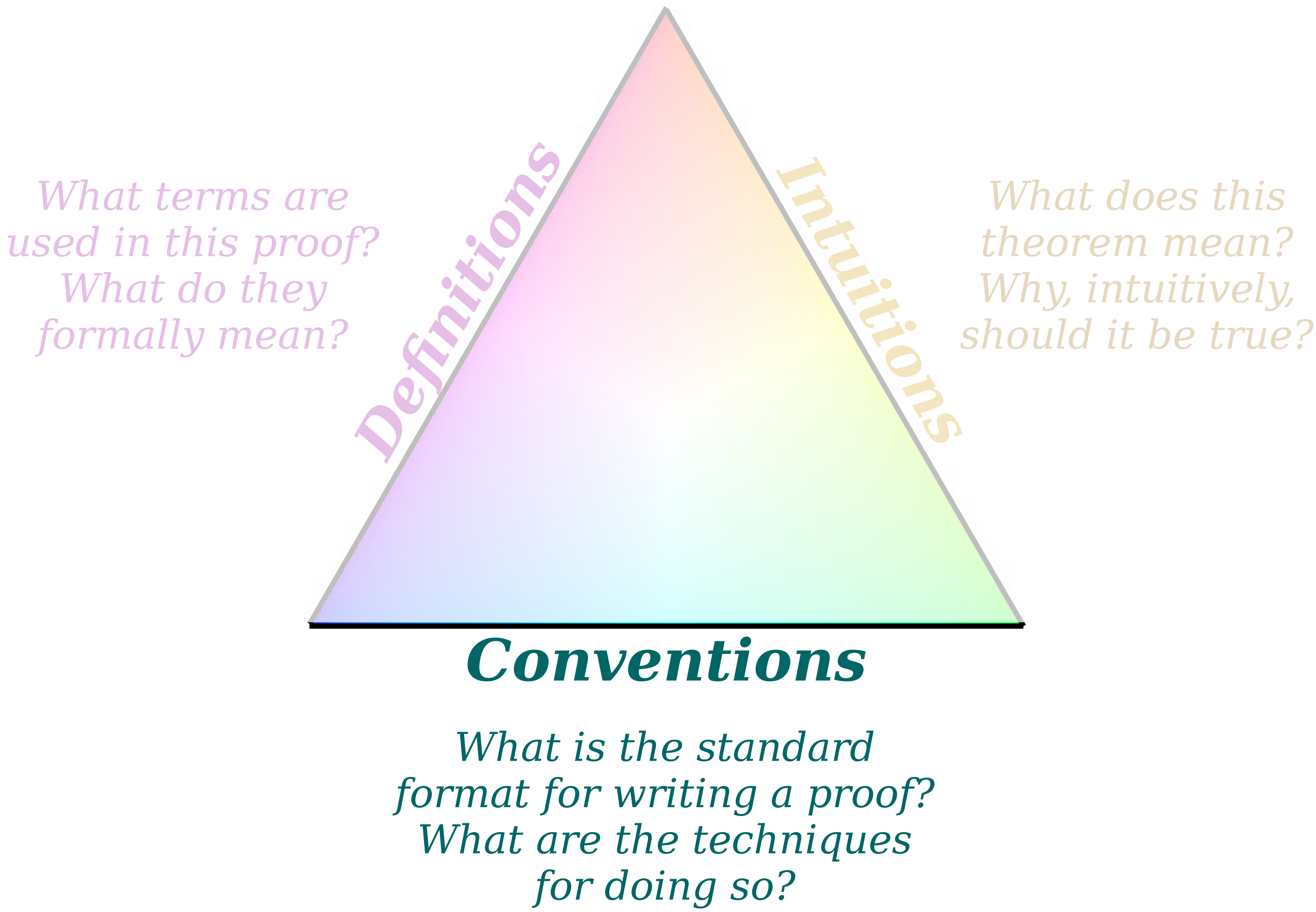
Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Let's Draw Some Pictures!



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

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.


Definitions
Intuitions
Conventions
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: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

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

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, l

We make an *arbitrary choice*. Rather than specifying what n is, we're signaling to the reader that they could, in principle, supply any choice n that they'd like.

$$= \quad 2k + 1$$

$$= \quad n.$$

This means that $r^2 - s^2 = n$, which is what we needed to show. ■

Theorem: For any odd integer n, there exist integers r and s where $r^2 - s^2 = n$.

Proof: Pick any odd integer n. Since n is odd, we know there is some integer k where $n = 2k + 1$.

Now, let $r = k+1$ and $s = k$. Then we see that

$$r^2 - s^2 = (k+1)^2 - k^2$$

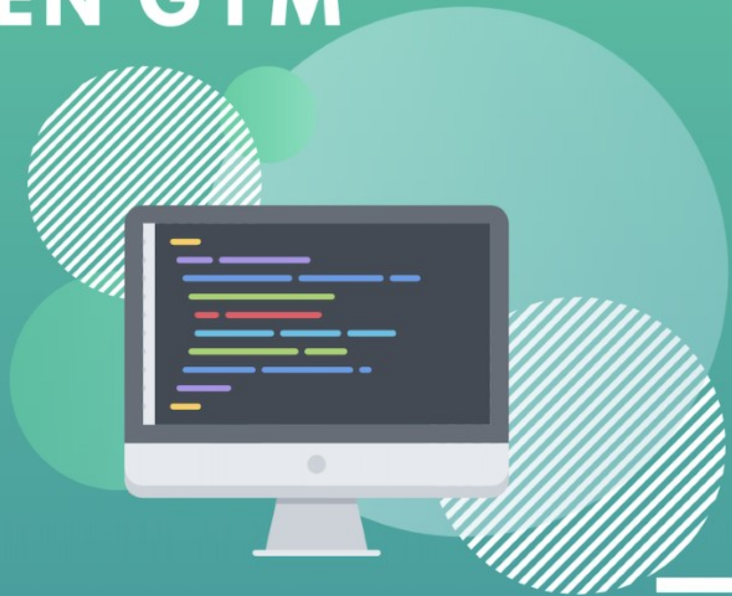
We're trying to prove an existential statement. The easiest way to do that is to just give concrete choices of the objects being sought out.

This mean ... e needed to show. ■

Time-Out for Announcements!

Black in CS & Women in CS

TECHNICAL INTERVIEW OPEN GYM



Learn interview techniques and run mock interviews with peers who worked at top tech companies.

September 25 | 6PM- 8PM
Gates 415

JUST BRING YOURSELF (AND A FRIEND)
FOR MORE INFORMATION EMAIL
MEKHI@ OR PANZALDO@

CURIS Poster Session

- There’s a CURIS poster session showcasing work from the summer going on from 3PM – 5PM Friday on the Packard lawn. Feel free to stop on by!
- Interested in seeing what research projects are open right now? Visit https://curis.stanford.edu.
- Have questions about research or how CURIS works?
  - Email PhD students and CURIS mentors Griffin Dietz and Kexin Rong at curis-mentors@cs.stanford.edu.
  - Email CURIS admin Nan Aoki at nanaoki@cs.stanford.edu.
  - Email Phil Levis, the professor who runs CURIS, at pal@cs.stanford.edu.

Piazza

- We have a Piazza site for CS103.
- Sign in to www.piazza.com and search for the course CS103 to sign in.
- Feel free to ask us questions!
- ***Use the site to find a partner for the problem sets!***

Qt Creator Help Session

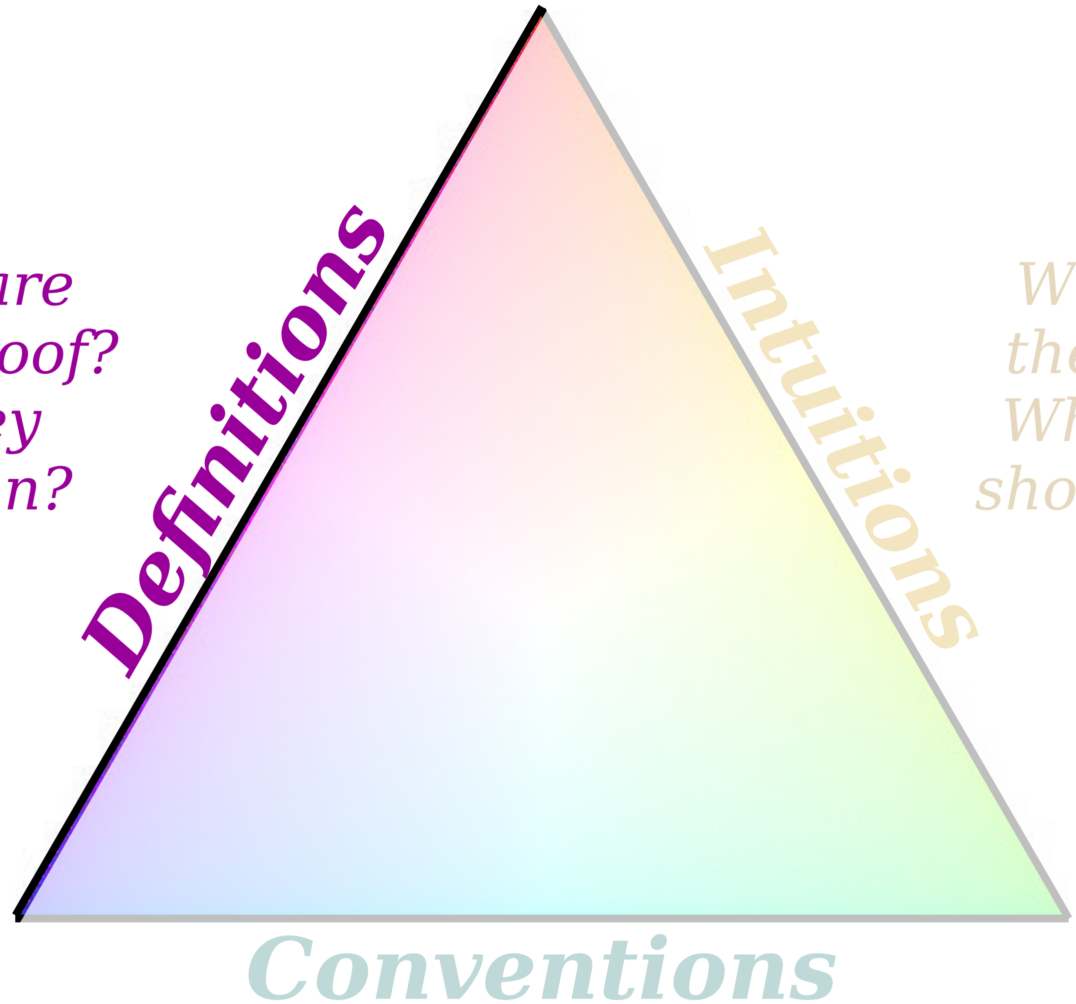
- The lovely CS106B/X folks have invited all y'all to join them for a Qt Creator Help Session this evening if you're having trouble getting Qt Creator up and running on your system.
- Runs ***7:30PM – 9:30PM*** in the Tresidder first floor lounge.
- SCPD students – please reach out to us if you need help setting things up. We'll do our best to help out.

Back to CS103!

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 $x \in (A \cup C) \cap (B \cup C)$.

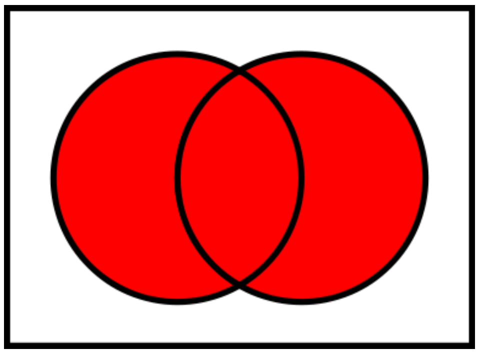
This is the ***element-of*** relation $\in$. It means that this object x is one of the items inside these sets.

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

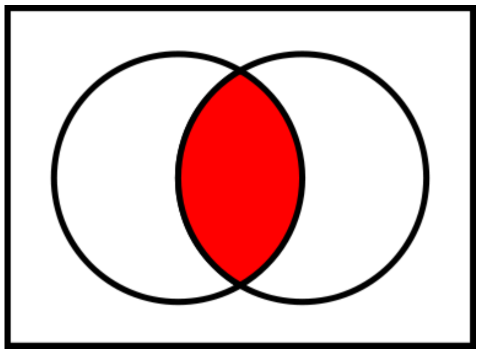
What are these, again?

Set Combinations

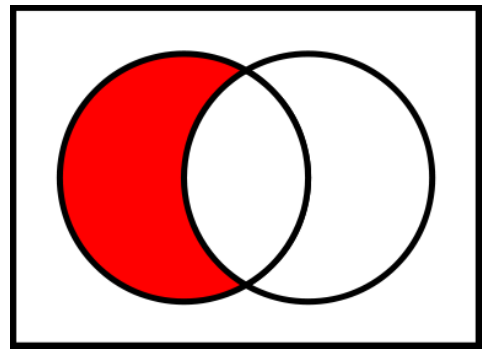
- In our last lecture, we saw four ways of combining sets together.



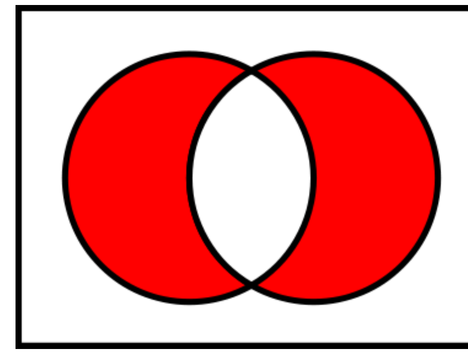
$S \cup T$



$S \cap T$



$S - T$



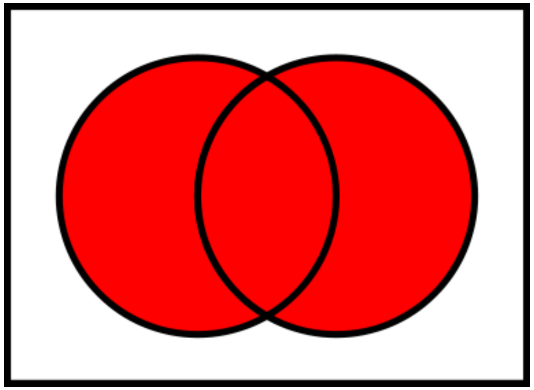
$S \Delta T$

- 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:

$x \in S \cup T$ when $x \in S$ or $x \in T$ (or both)

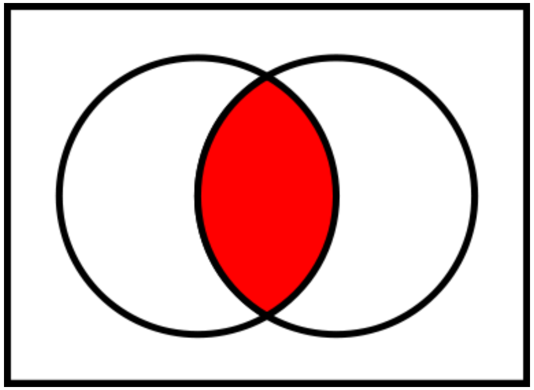
If you know that $x \in S \cup T$:

You can conclude that $x \in S$ or that $x \in T$ (or both).

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

Prove either that $x \in S$ or that $x \in T$ (or both).

Set Intersection



$S \cap T$

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

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

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

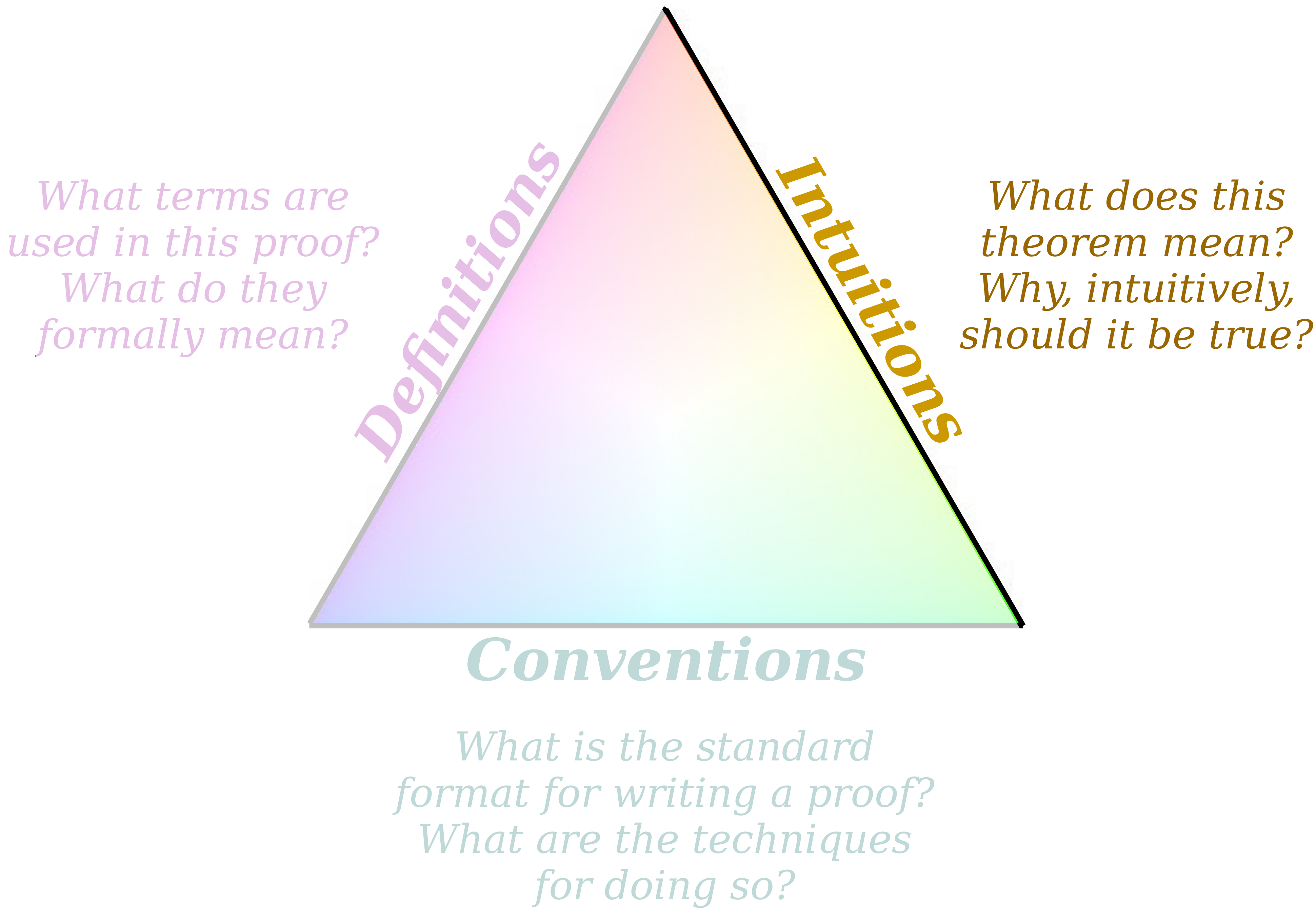
You can conclude both that $x \in S$ and that $x \in T$.

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

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

There are similar rules for
$S - T$ and $S \Delta T$.

Check the ***Guide to Set Theory Proofs***
for more details!


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

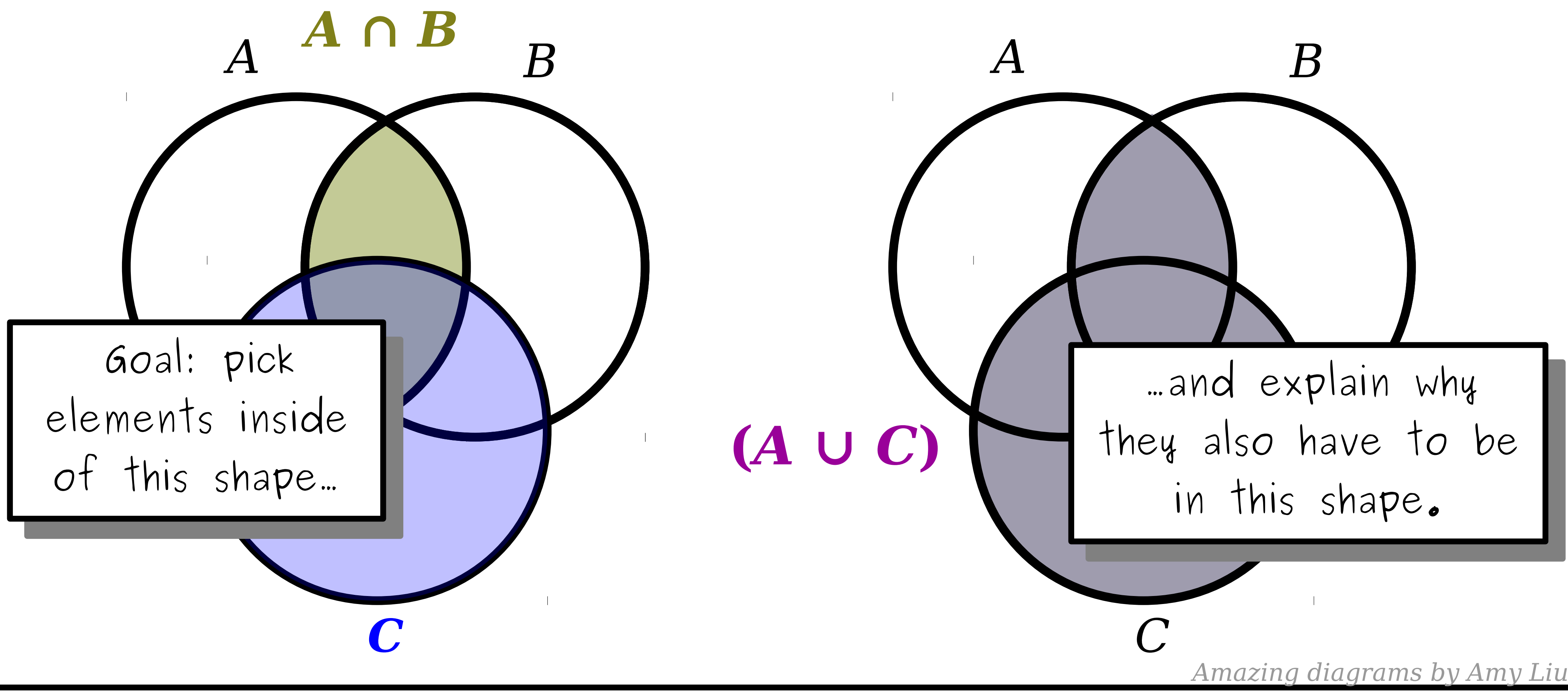
Let's Try Some Examples!

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

$$x = 1?$$
$$x = 2?$$
$$x = 3?$$

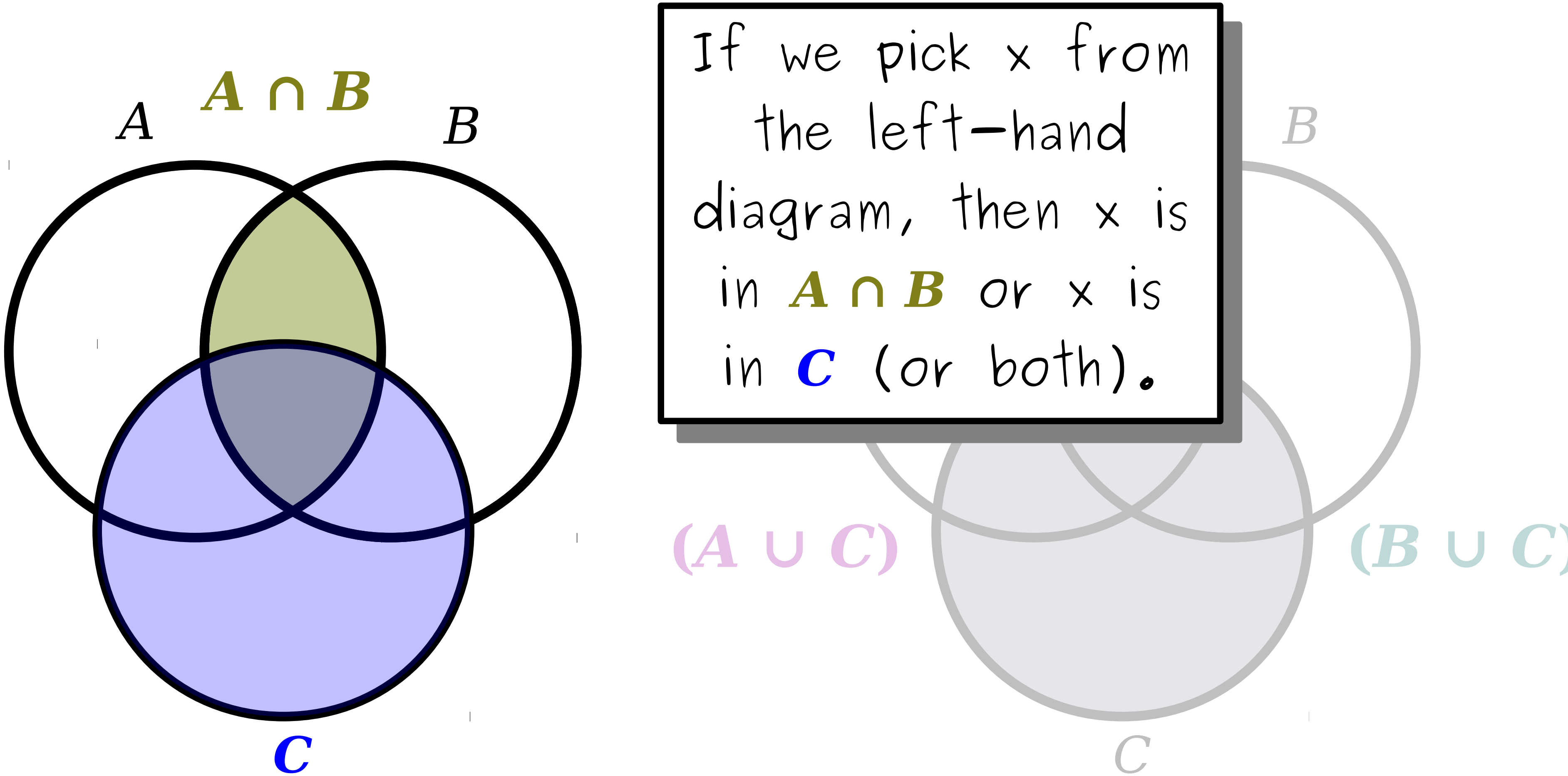
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

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 $x \in (A \cup C) \cap (B \cup C)$.

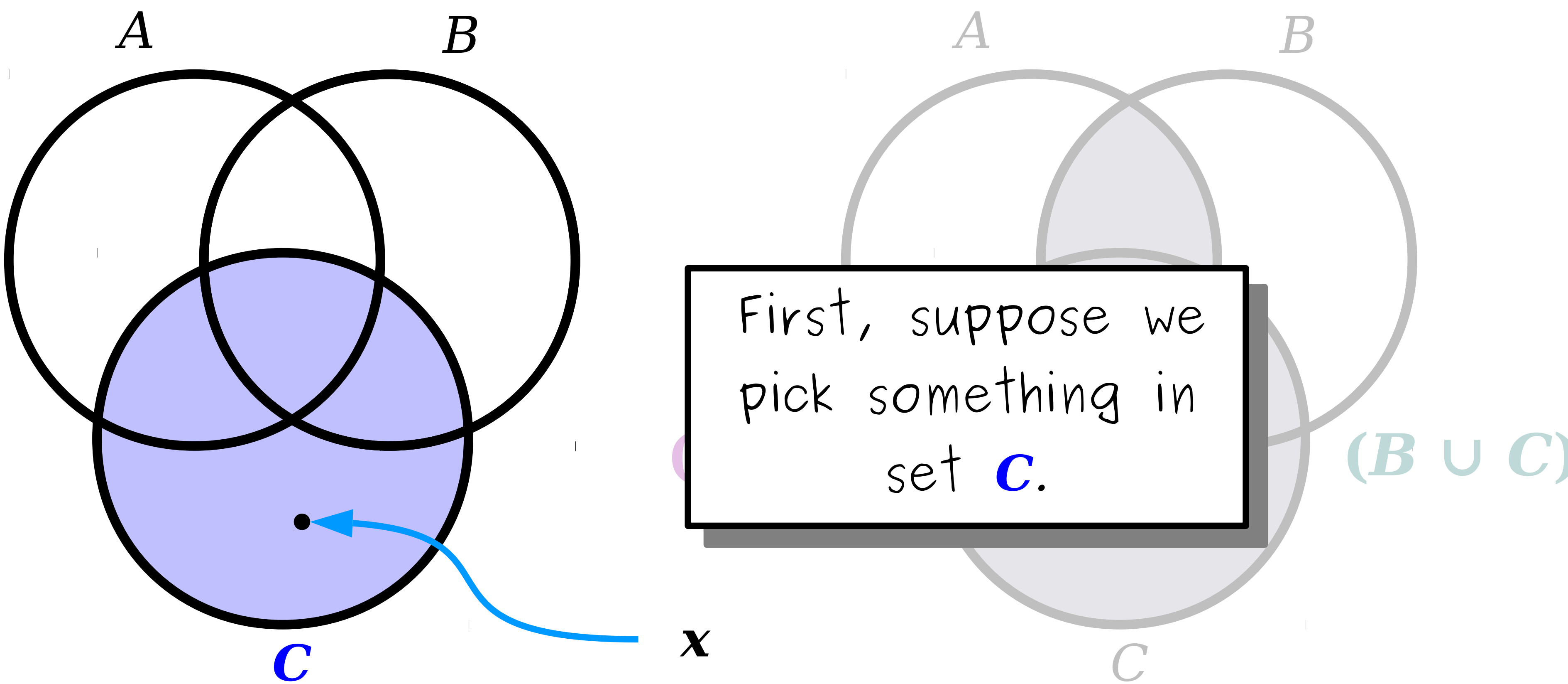
Let’s Draw Some Pictures!



Amazing diagrams by Amy Liu.

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

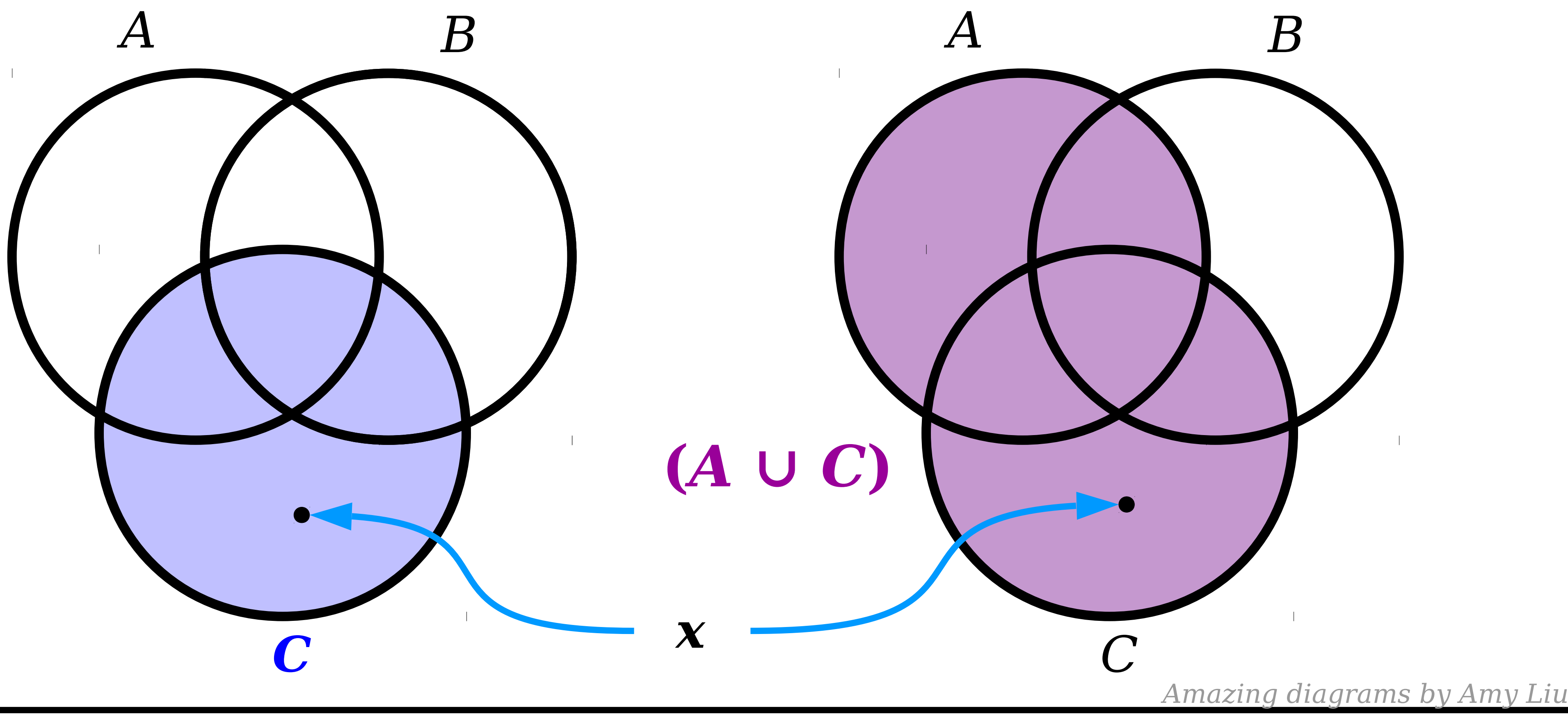
Let's Draw Some Pictures!



Amazing diagrams by Amy Liu.

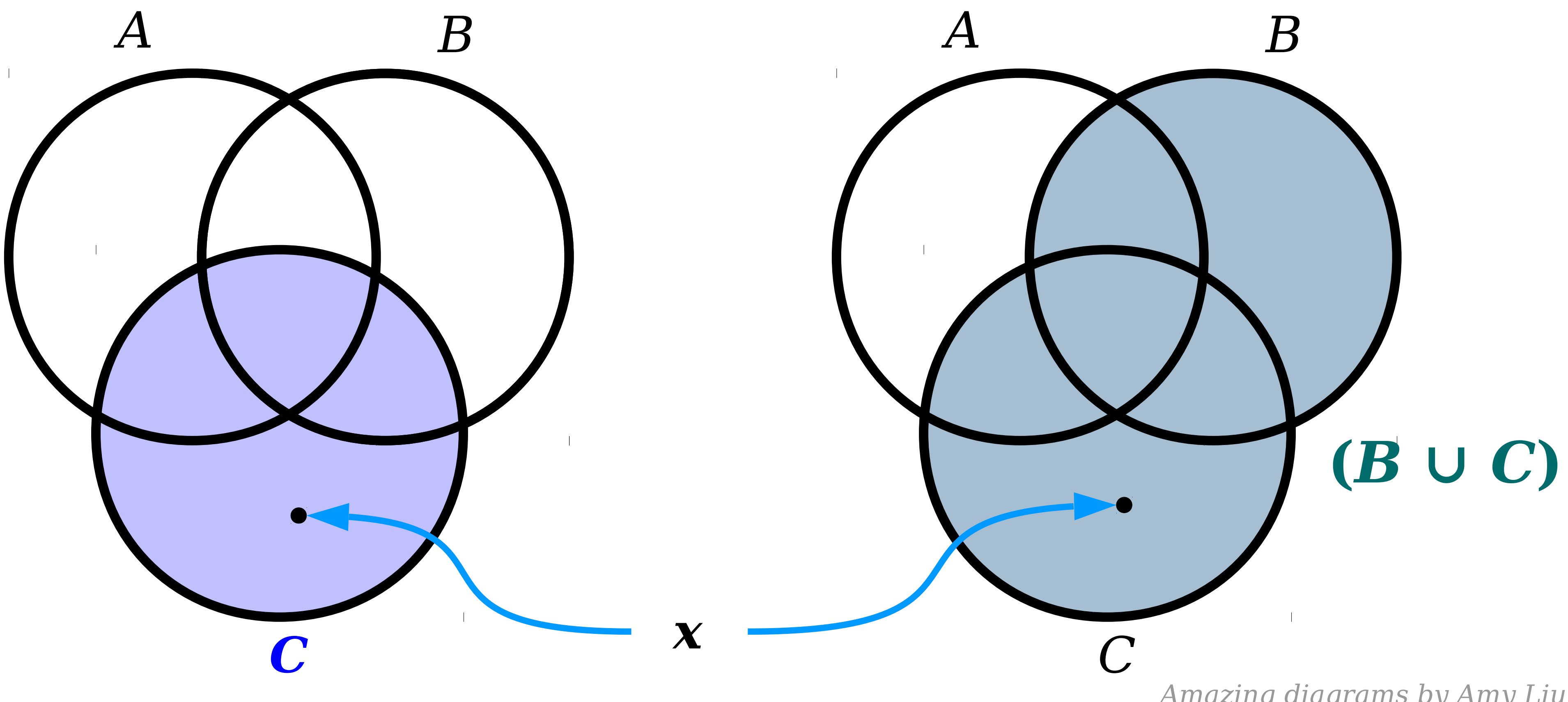
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



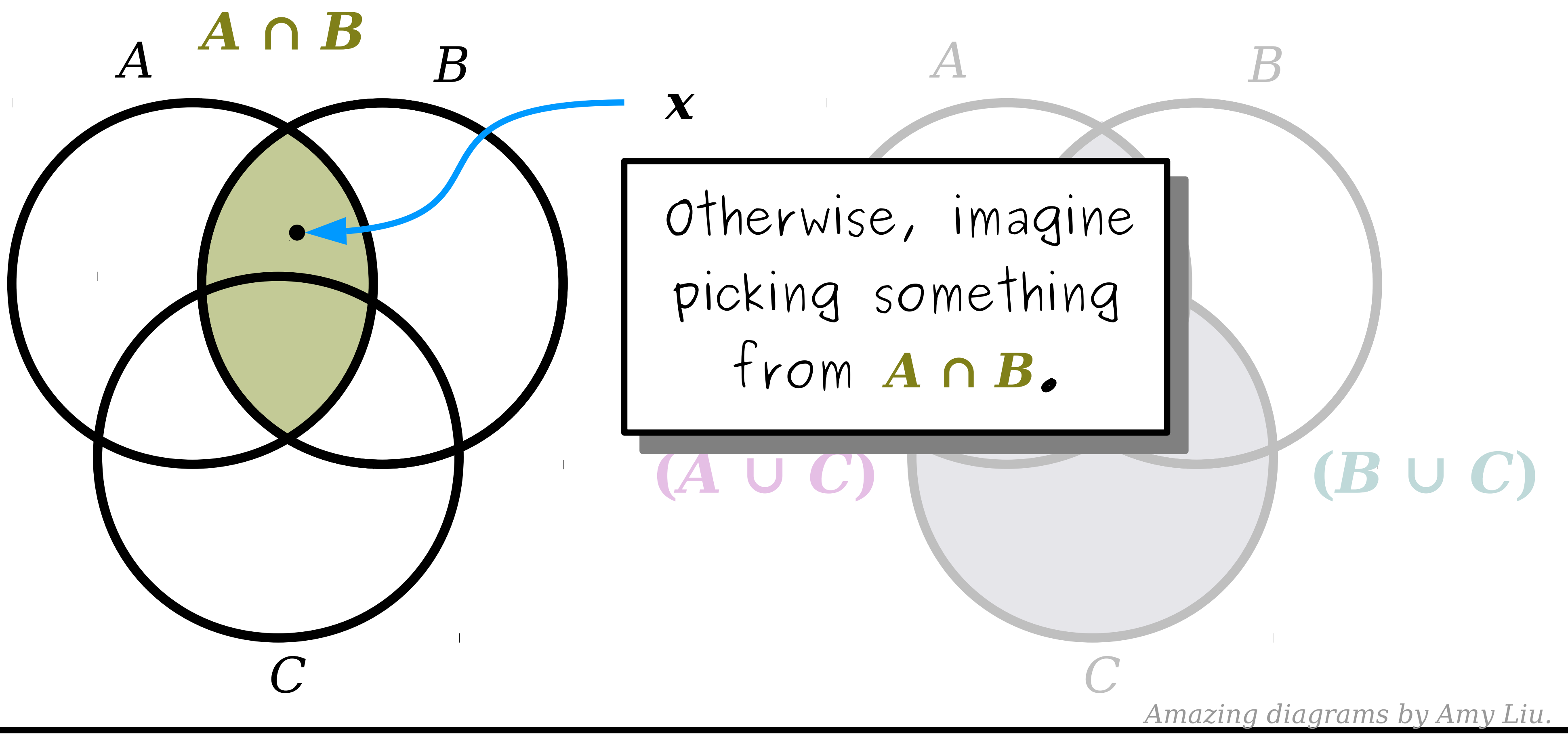
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



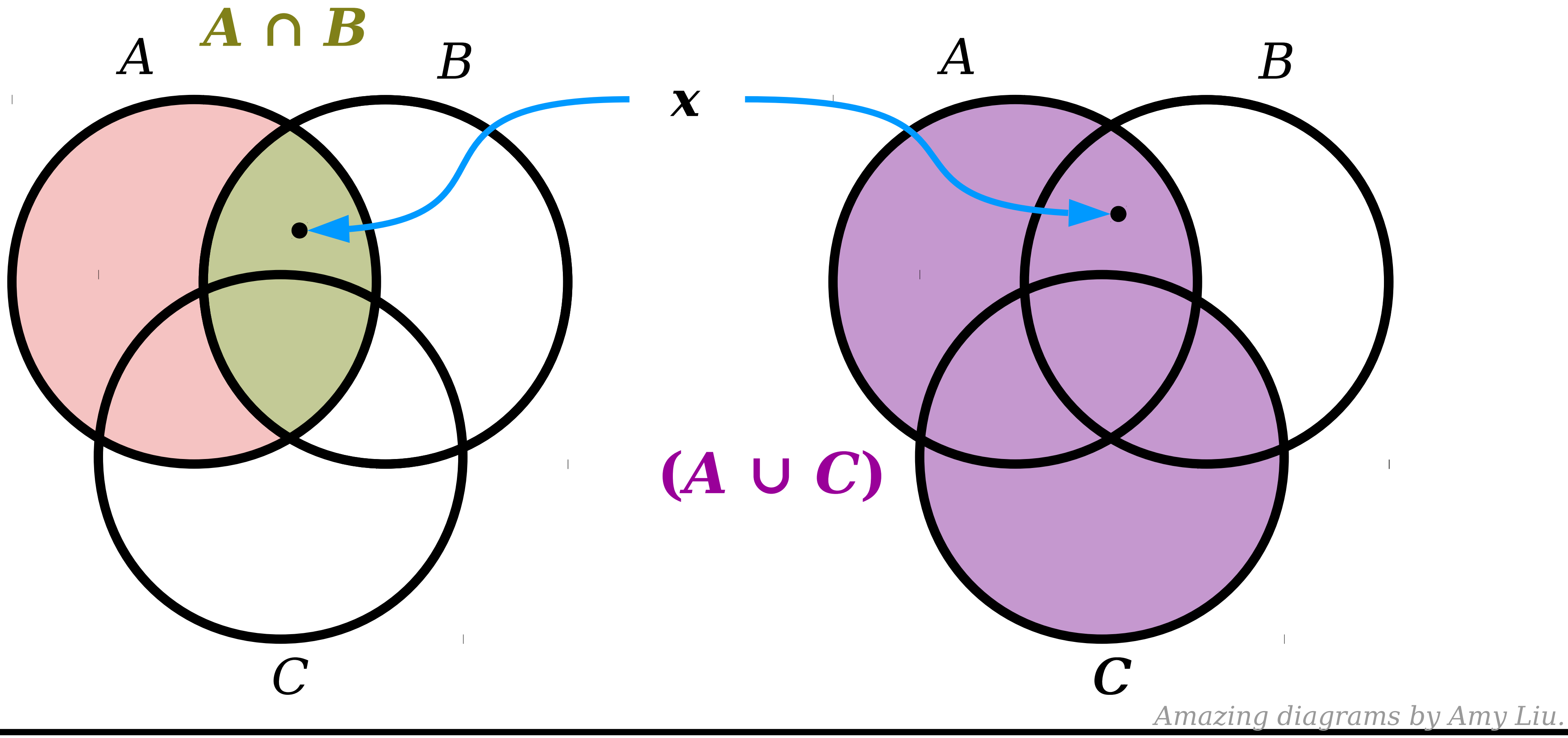
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



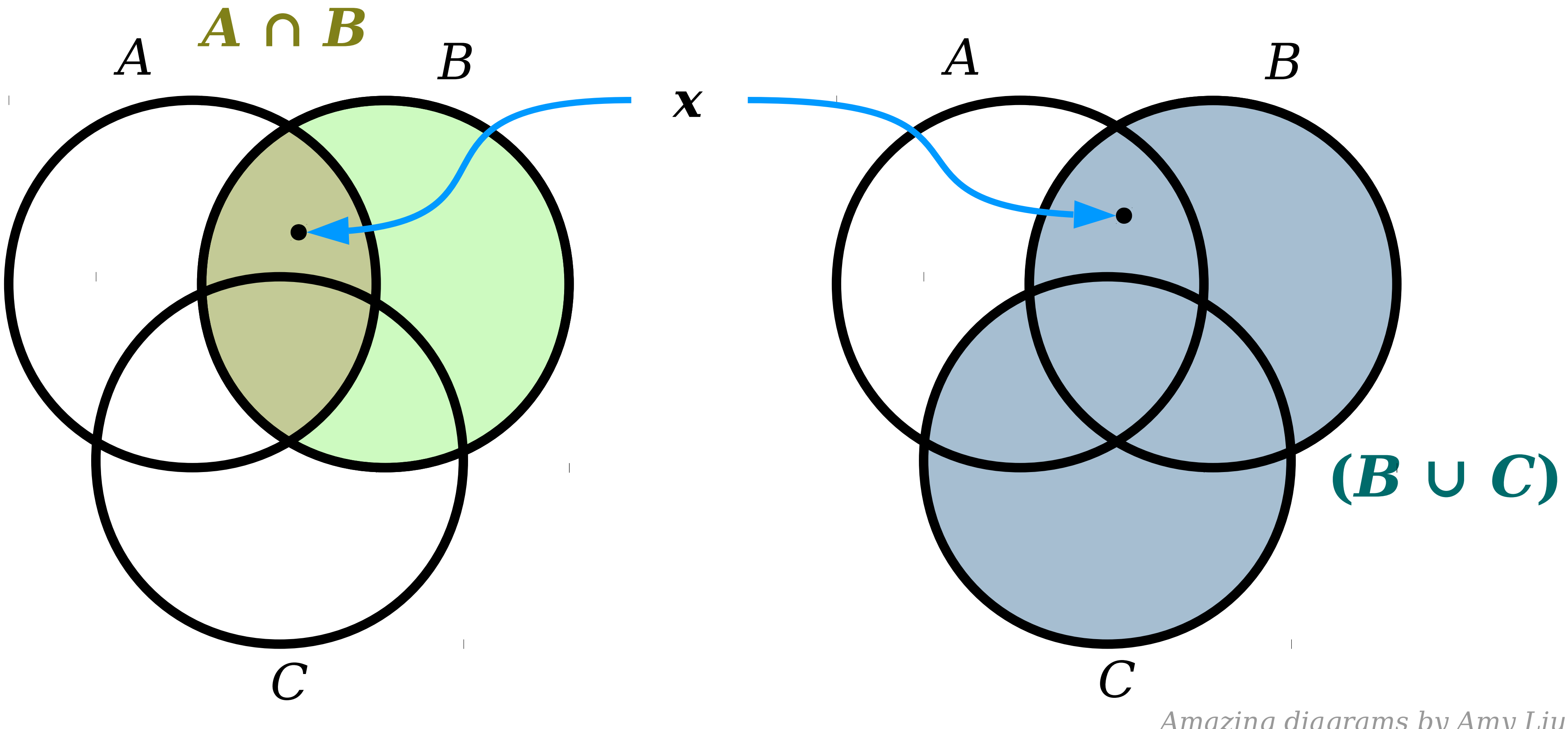
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



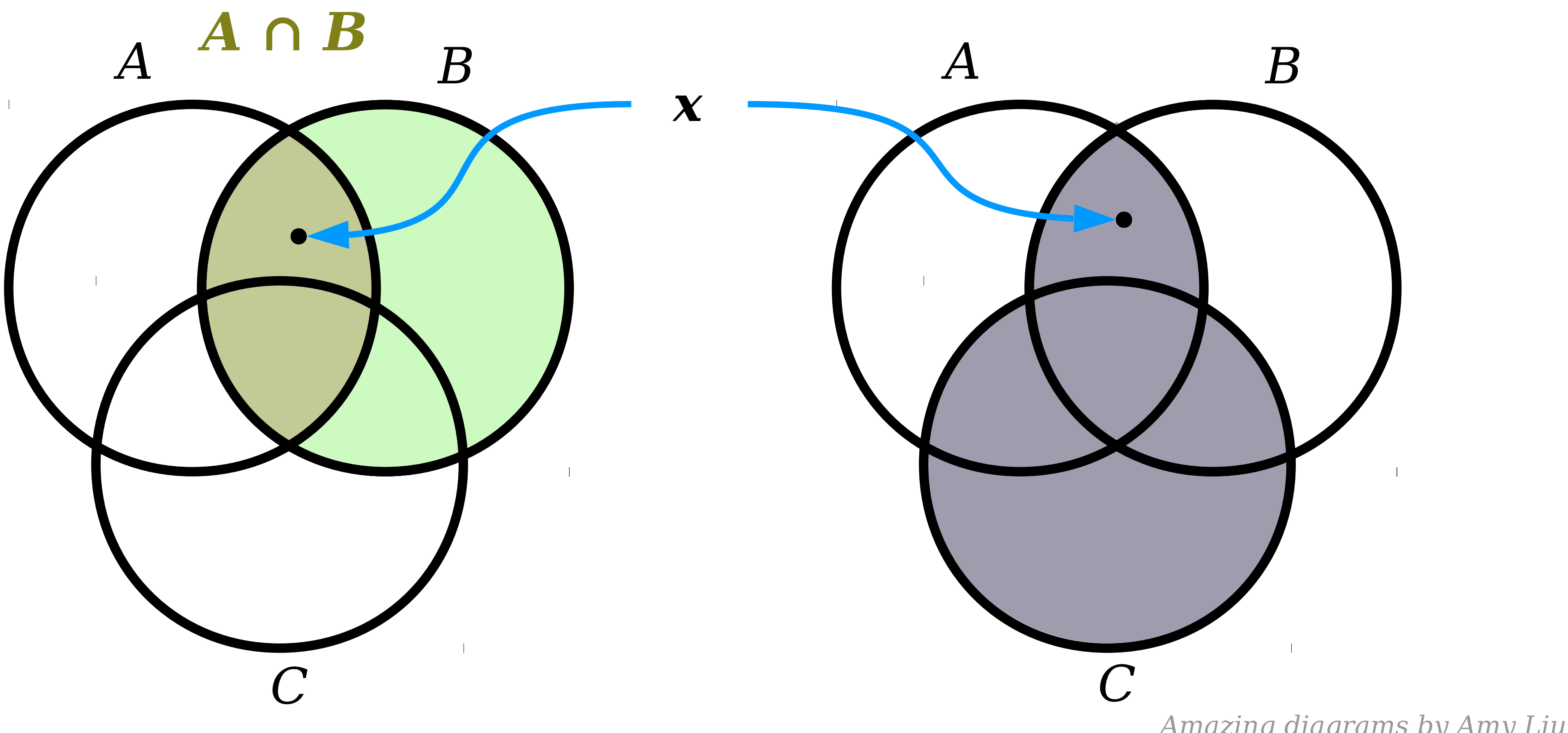
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

Let's Draw Some Pictures!



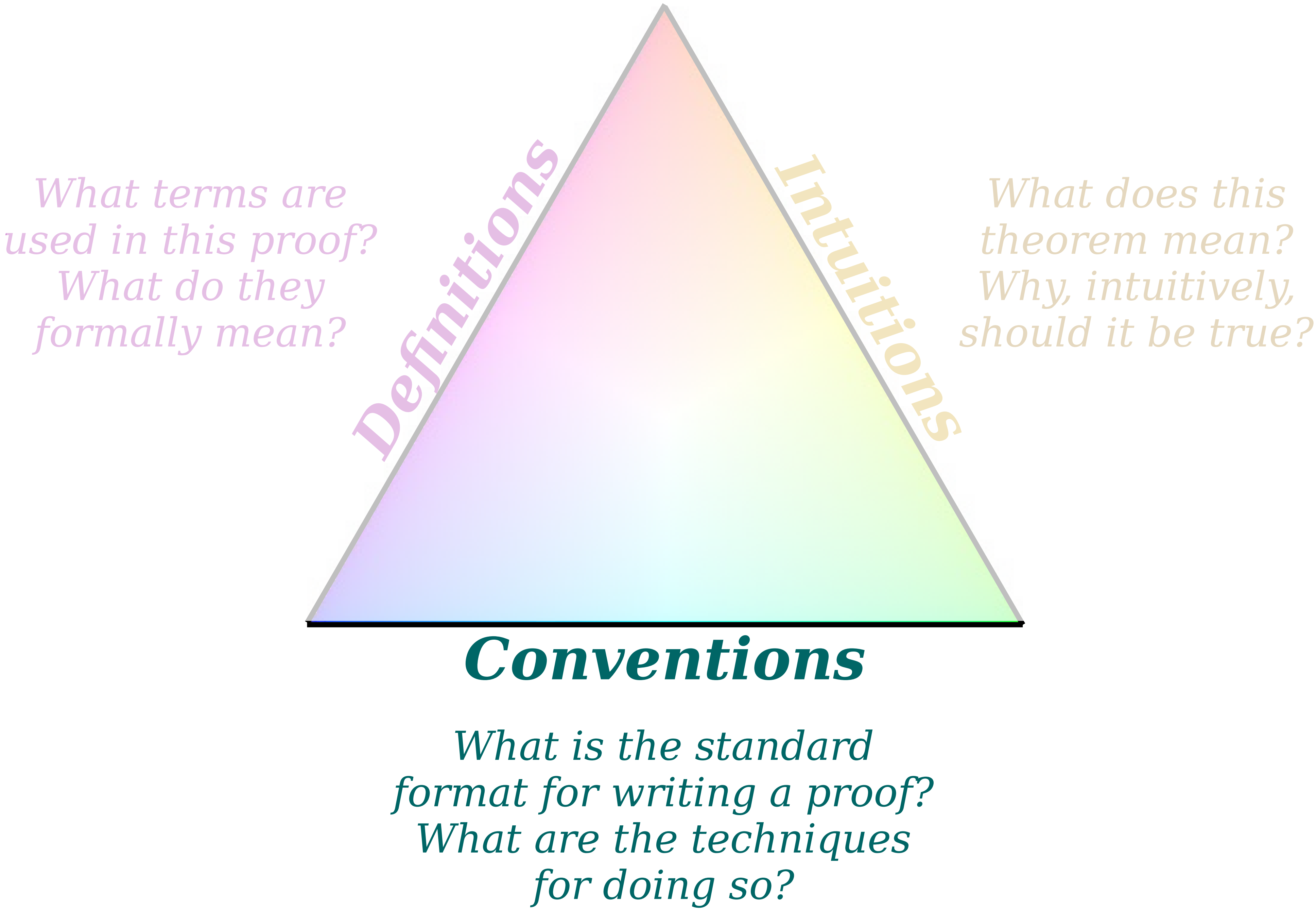
Theorem: If A, B, and C are sets, then for any $x \in (A \cap B) \cup C$, we have $x \in (A \cup C) \cap (B \cup C)$.

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 $x \in (A \cup C) \cap (B \cup C)$.


Definitions
What terms are used in this proof? What do they formally mean?
Intuitions
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 $x \in (A \cup C) \cap (B \cup C)$.

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 … at $x \in C$.
We cons …

Case … and
tha …

Case … at
$x \in$ …
$x \in A \cup C$ and that $x \in B \cup C$.

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.

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

$x \in A \cup C$ and th

In either case, we lear

establishes that $x \in (A$

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…

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.

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

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: $\boldsymbol{x \in C}$. This in turn means that $x \in A \cup C$ and that $x \in B \cup C$.

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

In eit

estab

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

You can conclude that $x \in S$ or that $x \in T$ (or both).

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

You can conclude both that $x \in S$ and that $x \in T$.

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 $x \in T$.

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 $x \in (A \cup C) \cap (B \cup C)$.

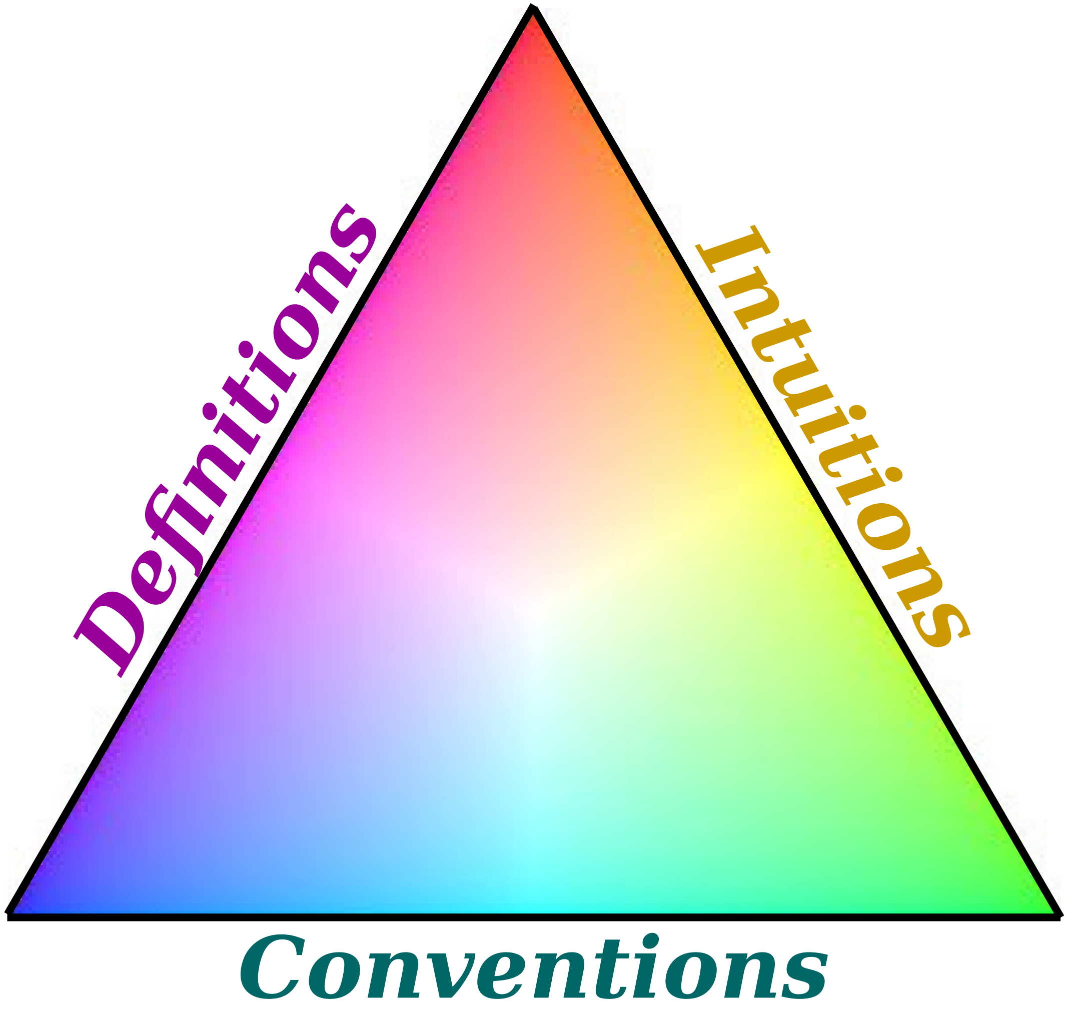
Since $x \in (A \cap B) \cup C$, we know that $x \in A \cap B$ or that $x \in C$. We consider each case separately.

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. ■

To Recap



Writing a good proof requires a blend of definitions, intuitions, and conventions.

An integer n is ***even*** if there is an integer k where $n = 2k$.

An integer n is ***odd*** if there is an integer k where $n = 2k+1$.

$\boldsymbol{S \cup T}$ is the set where, for any x:
$x \in S \cup T$ when $x \in S$ or $x \in T$ (or both).

$\boldsymbol{S \cap T}$ is the set where, for any x:
$x \in S \cap T$ when both $x \in S$ and $x \in T$.

$\boldsymbol{S \subseteq T}$ when for any $x \in S$, we have $x \in T$.

$\boldsymbol{S = T}$ when $S \subseteq T$ and $T \subseteq S$.

Definitions tell us what we need to do in a proof.
Many proofs directly reference these definitions.

Let's Draw Some Pictures!

Let's Do Some Math!

Let's Try Some Examples!

Building intuition for results requires creativity, trial, and error.

- Prove universal statements by making arbitrary choices.
- Prove existential statements by making concrete choices.
- Prove "If P, then Q" by assuming P and proving Q.
- Write in complete sentences.
- Number sub-formulas when referring to them.
- Summarize what was shown in proofs by cases.
- Articulate your start and end points.

Mathematical proofs have established conventions that increase rigor and readability.

Your Action Items

- ***Read "How to Succeed in CS103."***
  - There's a lot of valuable advice in there – take it to heart!
- ***Read "Guide to Proofs on Set Theory."***
  - This picks up where we left off in today's lecture. Pay particular attention to what we didn't cover: proofs on differences, symmetric differences, and power sets.
- ***Read "Guide to ∈ and ⊆."***
  - You'll want to have a handle on how these concepts are related, and on how they differ.
- ***Finish and submit Problem Set 0.***
  - Don't put this off until the last minute!

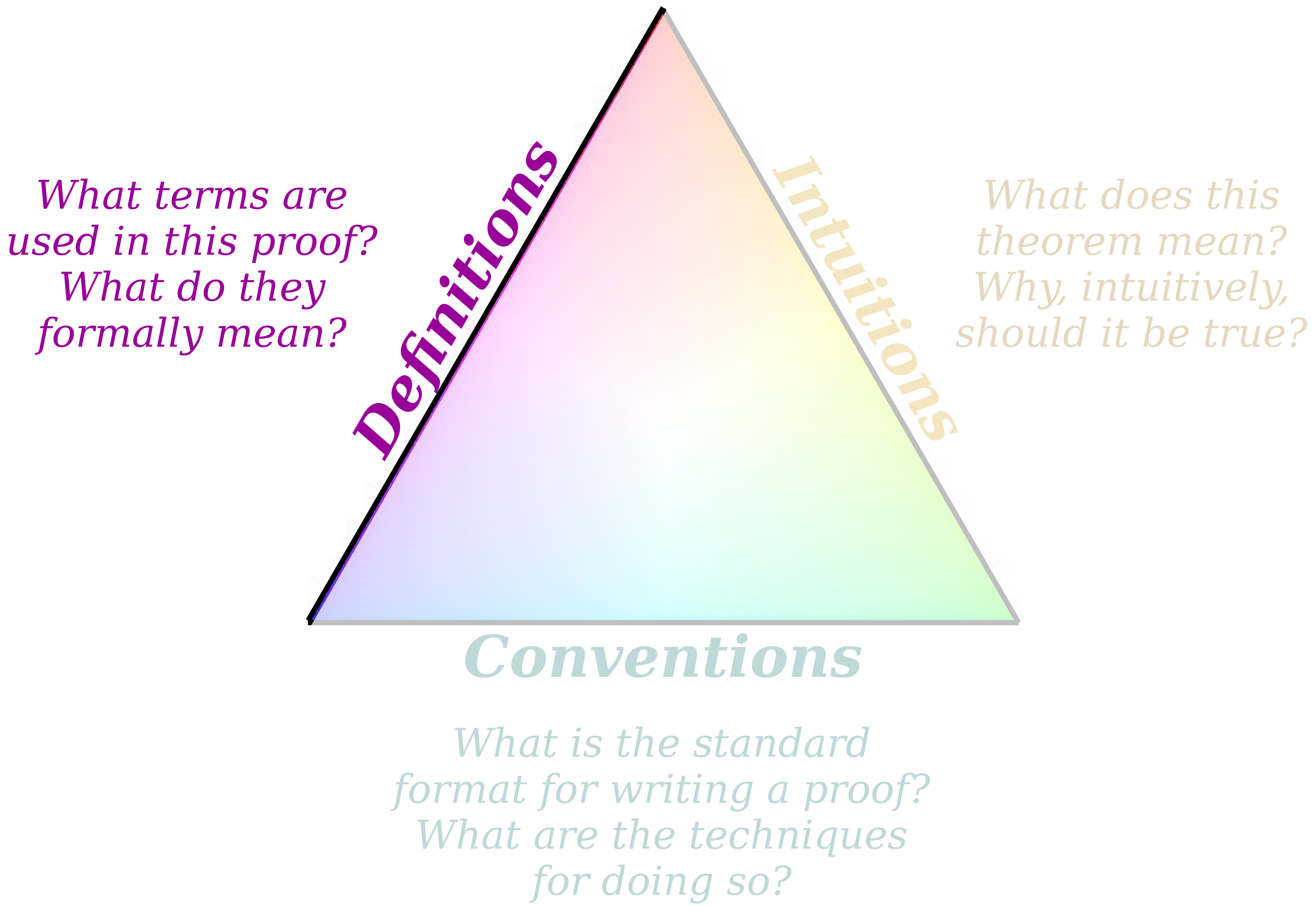
Next Time

- ***Indirect Proofs***
  - How do you prove something without actually proving it?
- ***Mathematical Implications***
  - What exactly does "if P, then Q" mean?
- ***Proof by Contrapositive***
  - A helpful technique for proving implications.
- ***Proof by Contradiction***
  - Proving something is true by showing it can't be false.

Appendix: More Proofs on Sets

Proofs on Subsets

Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.



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

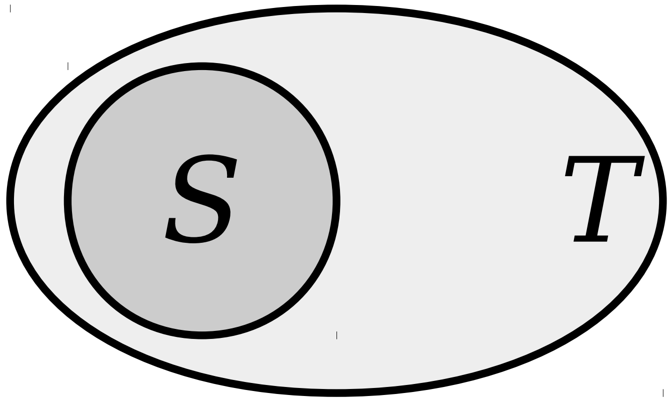
Set Theory Review

- Recall from last time that we write $x \in S$ if x is an element of set S and $x \notin S$ if x is not an element of set S.
- If S and T are sets, we say that S is a subset of T (denoted $S \subseteq T$) if the following statement is true:

For every *x*, if $x \in S$, then $x \in T$.

- What does this mean for proofs?

Subsets

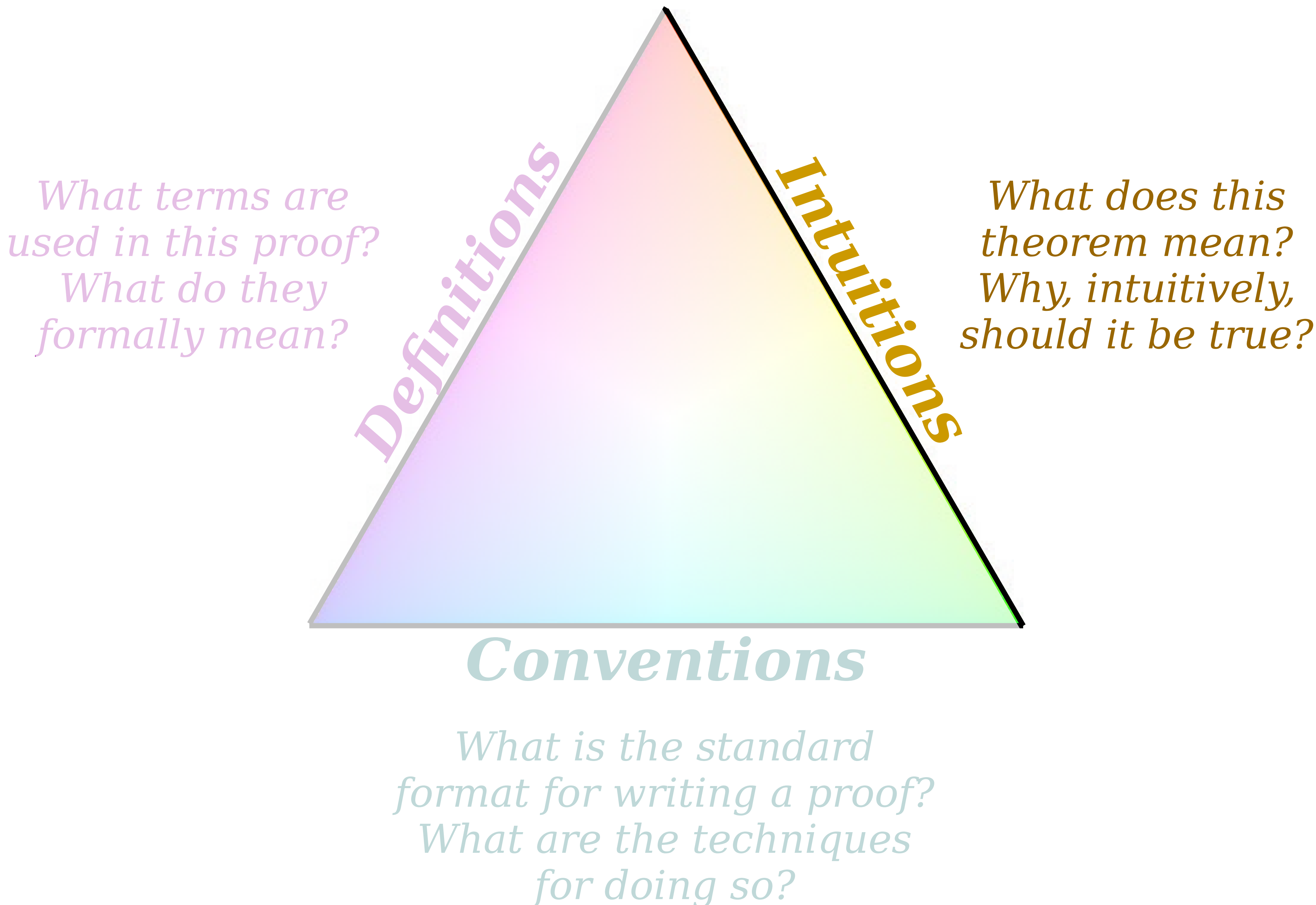


$S \subseteq T$

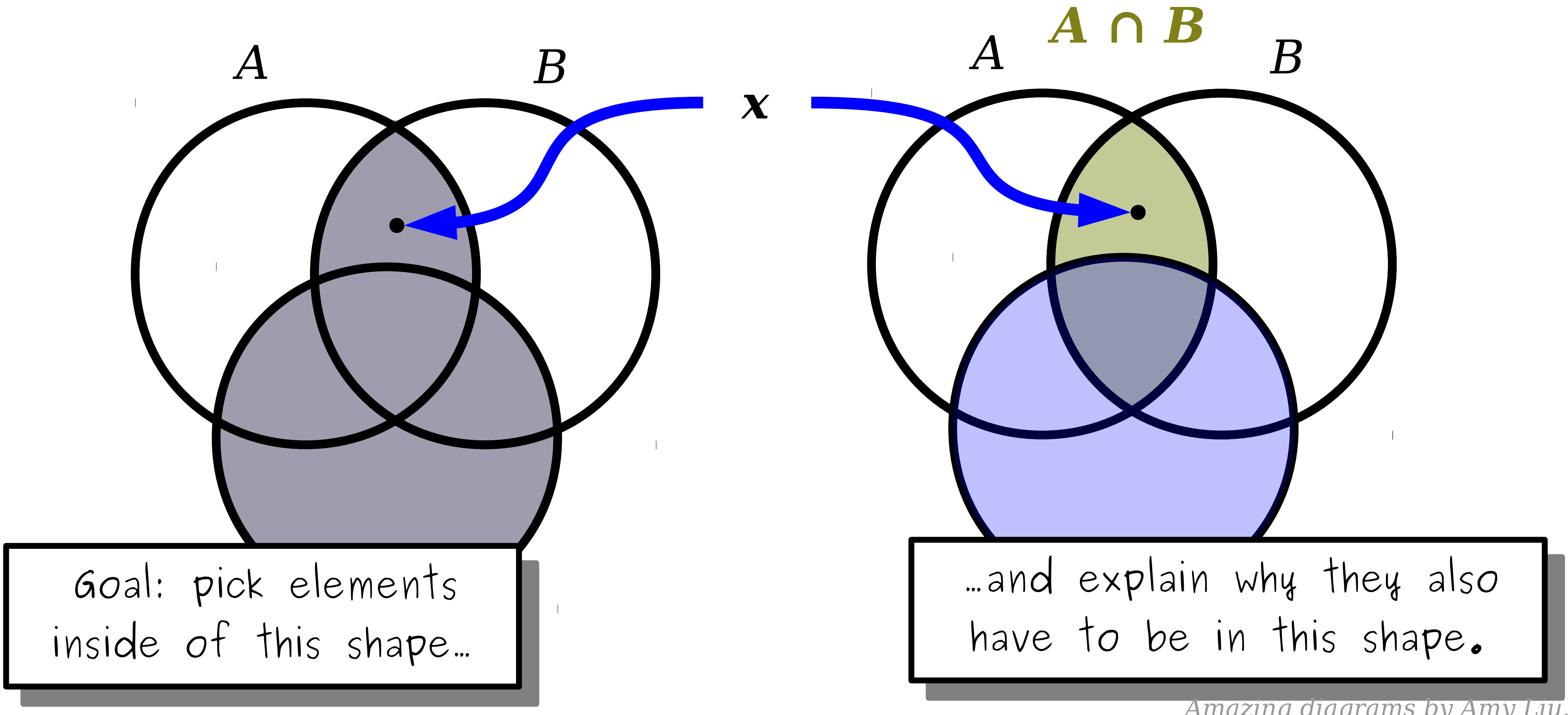
Definition: If S and T are sets, then $S \subseteq T$ when for every $x \in S$, we have $x \in T$.

If you know that $S \subseteq T$:
If you have an $x \in S$, you can conclude $x \in T$.

To prove that $S \subseteq T$:
Pick an arbitrary $x \in S$, then prove $x \in T$.

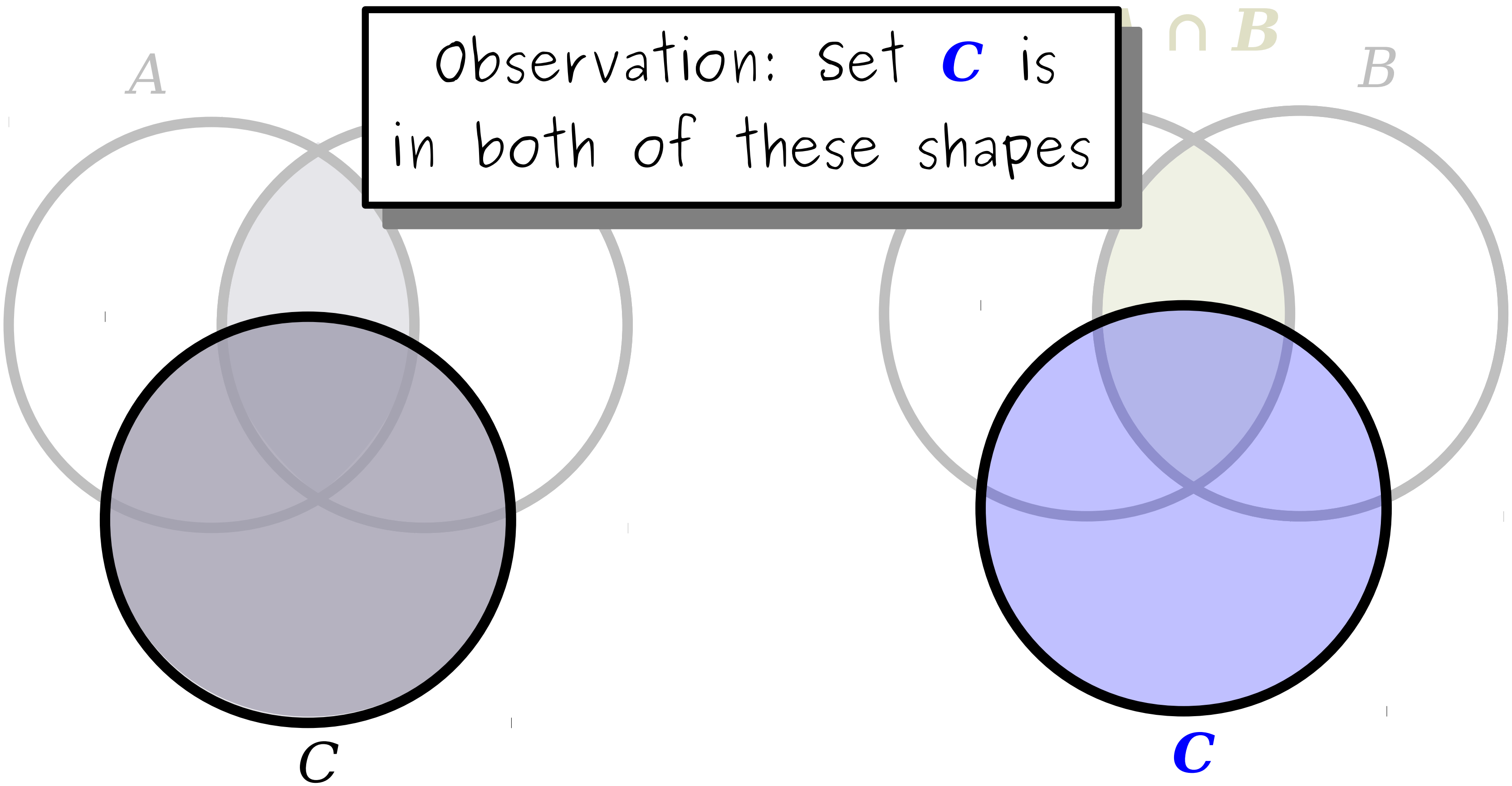

What terms are used in this proof? What do they formally mean?
Definitions
Intuitions
What does this theorem mean? Why, intuitively, should it be true?
Conventions
What is the standard format for writing a proof? What are the techniques for doing so?

Let's Draw Some Pictures!



Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Let's Draw Some Pictures!

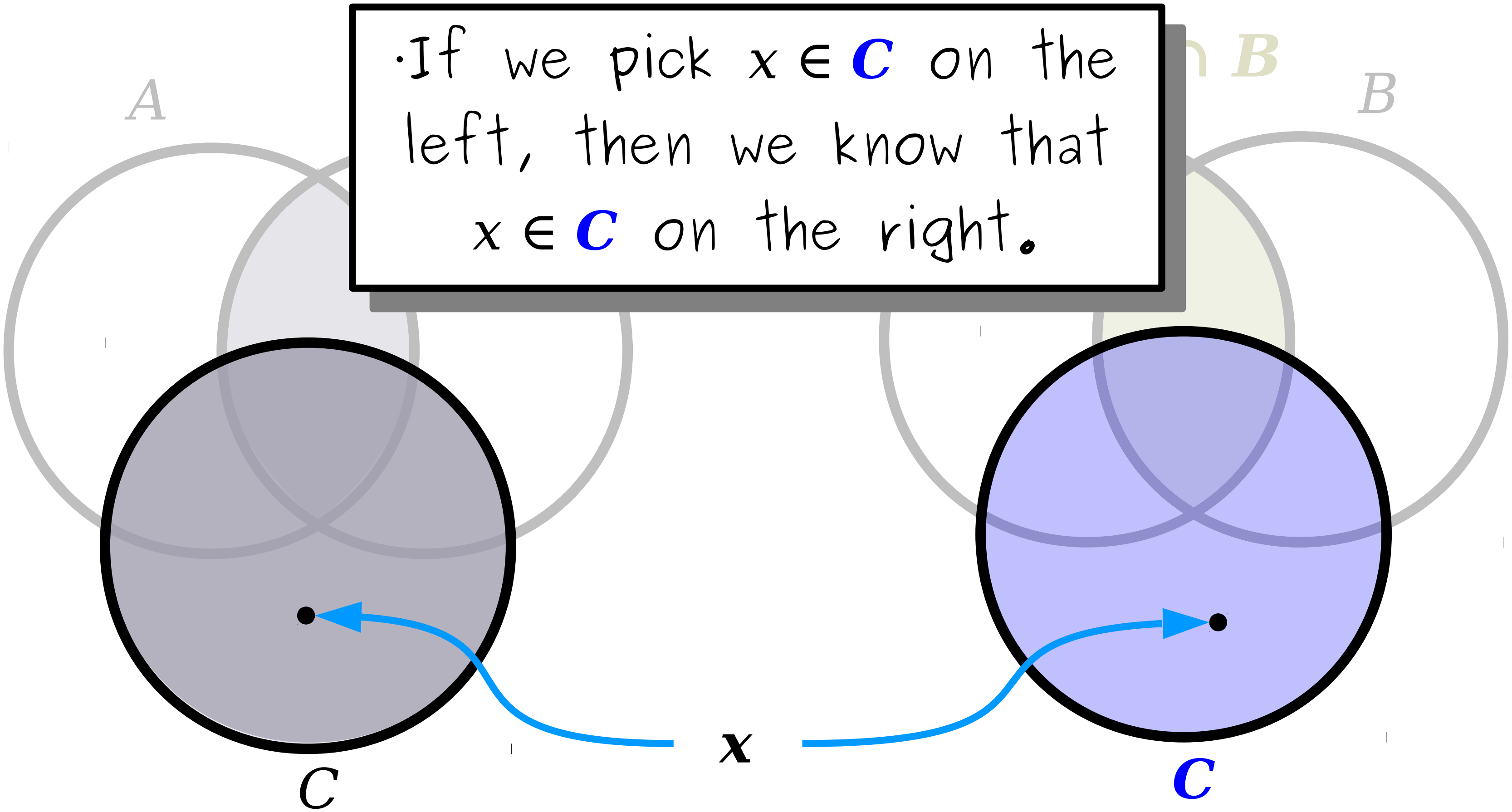


Observation: Set C is in both of these shapes

Amazing diagrams by Amy Liu.

Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

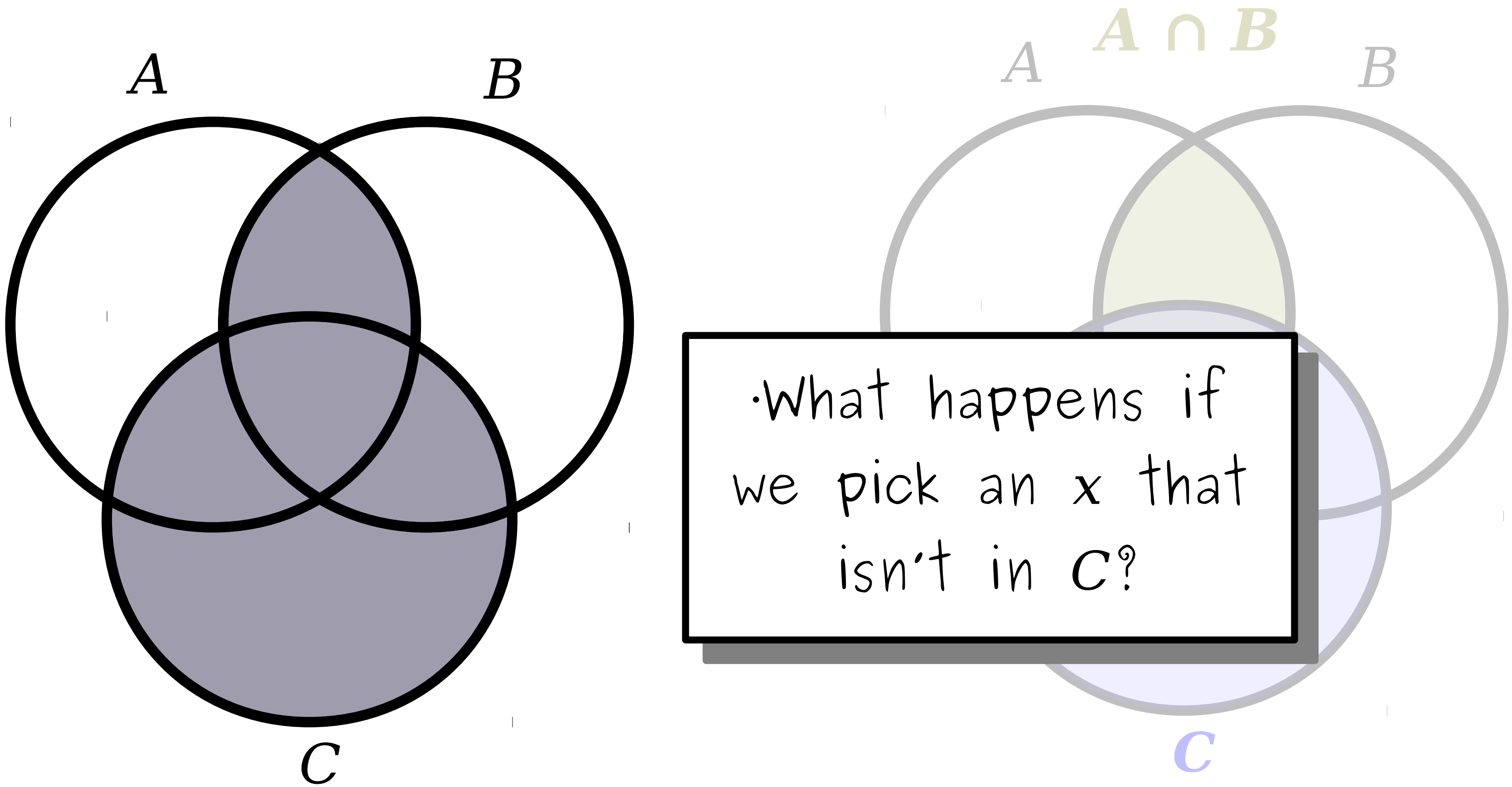
Let's Draw Some Pictures!



Amazing diagrams by Amy Liu.

Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

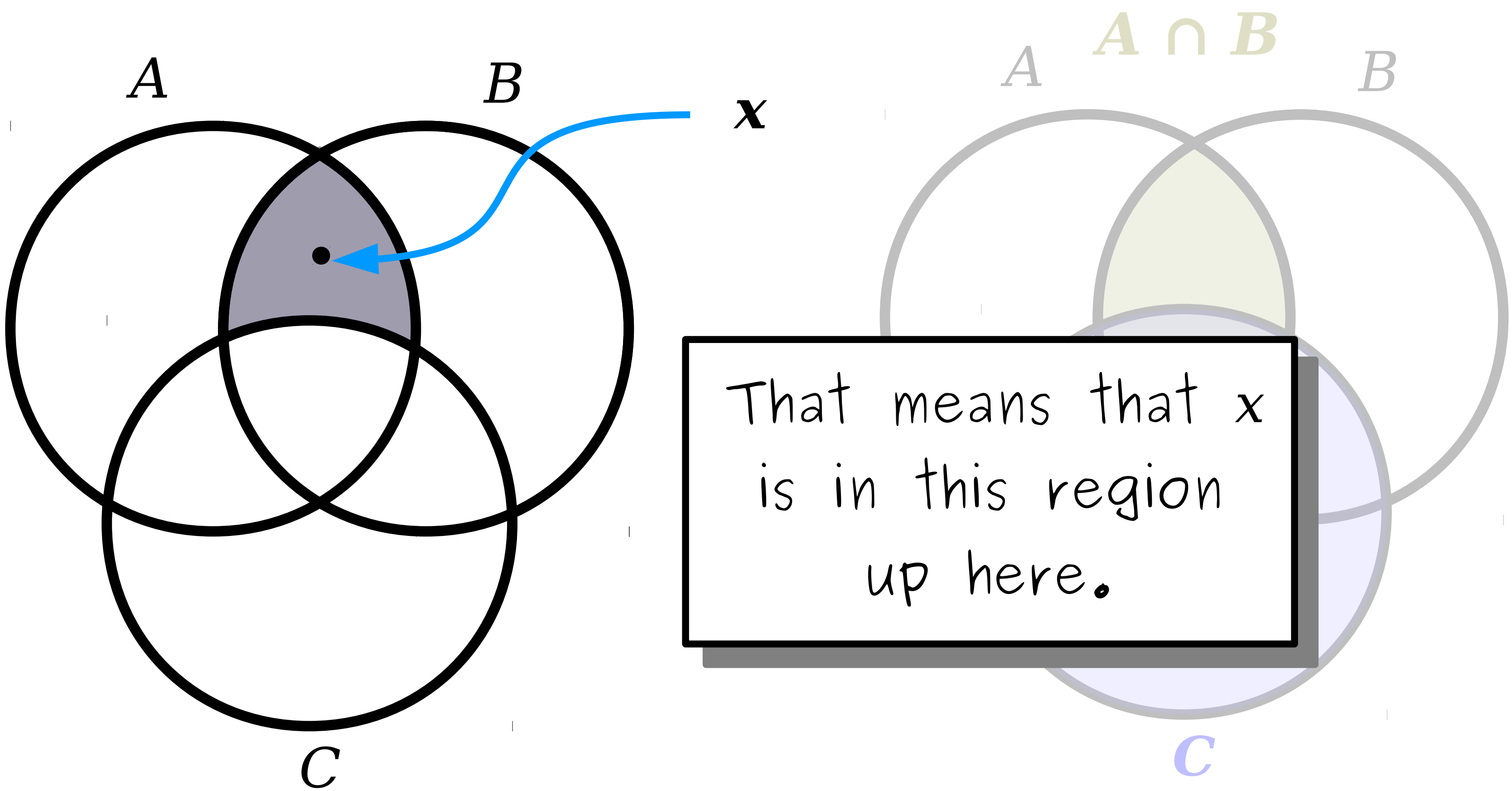
Let's Draw Some Pictures!



Amazing diagrams by Amy Liu.

Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

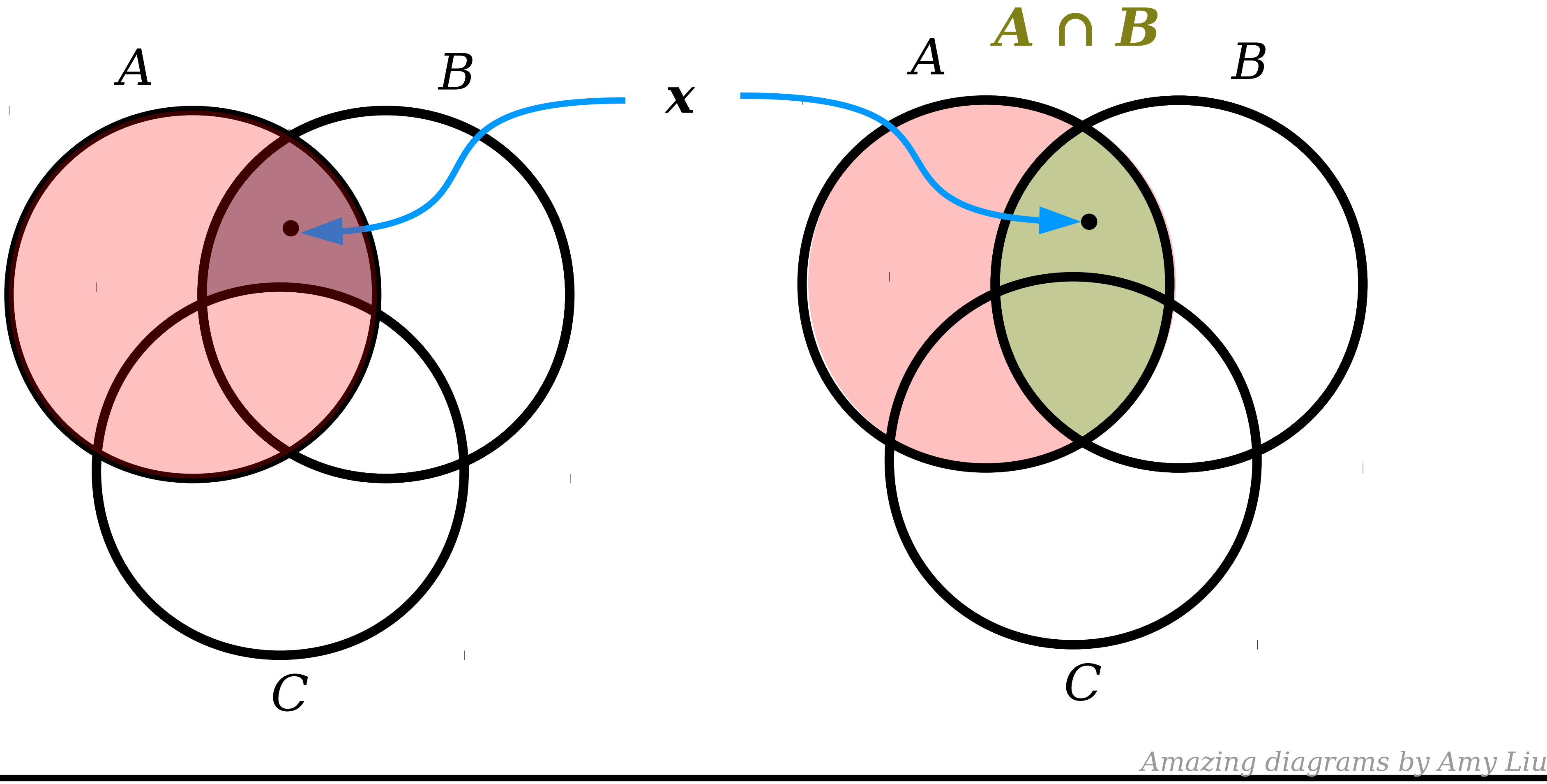
Let's Draw Some Pictures!



Amazing diagrams by Amy Liu.

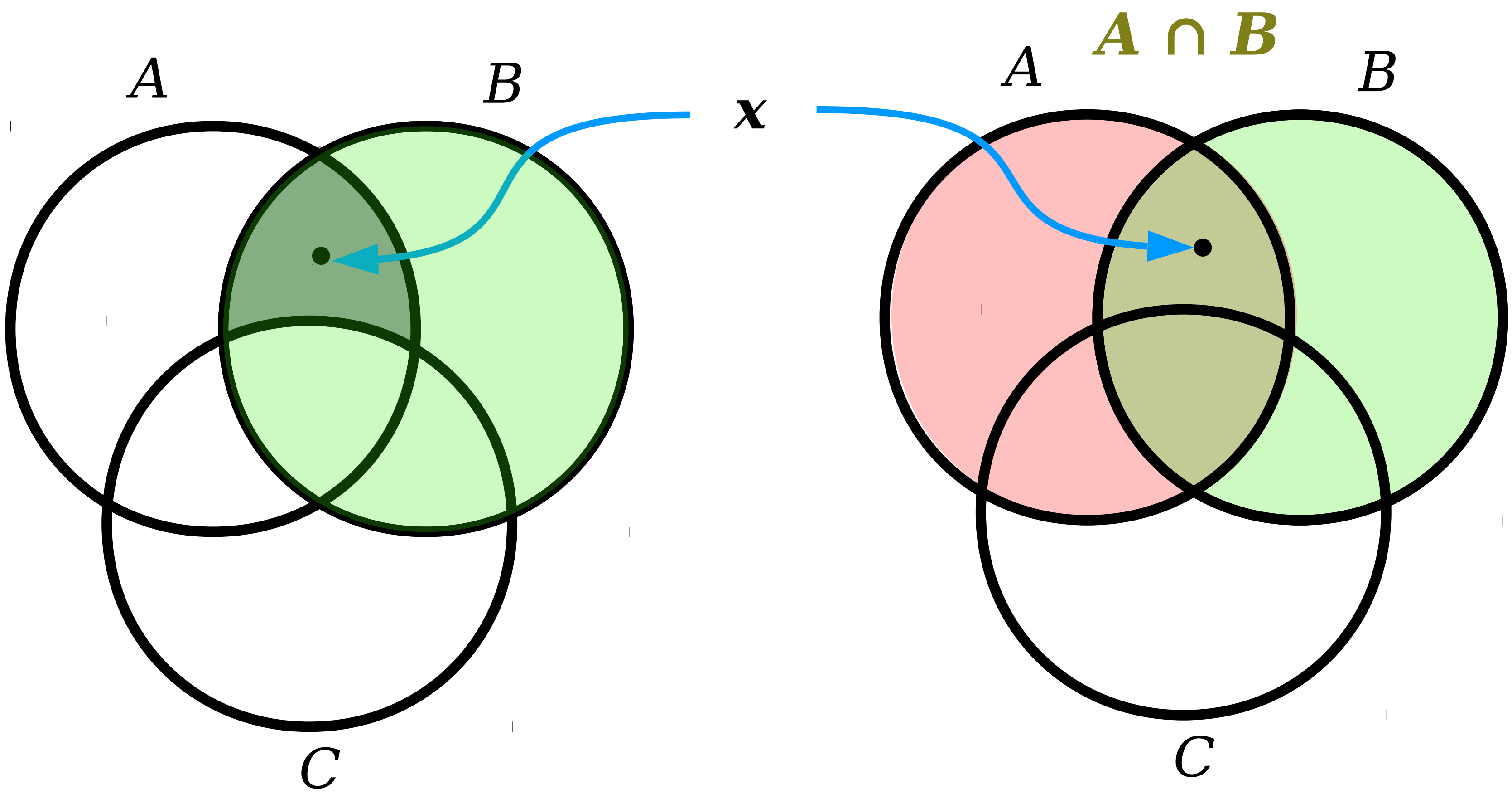
Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Let's Draw Some Pictures!



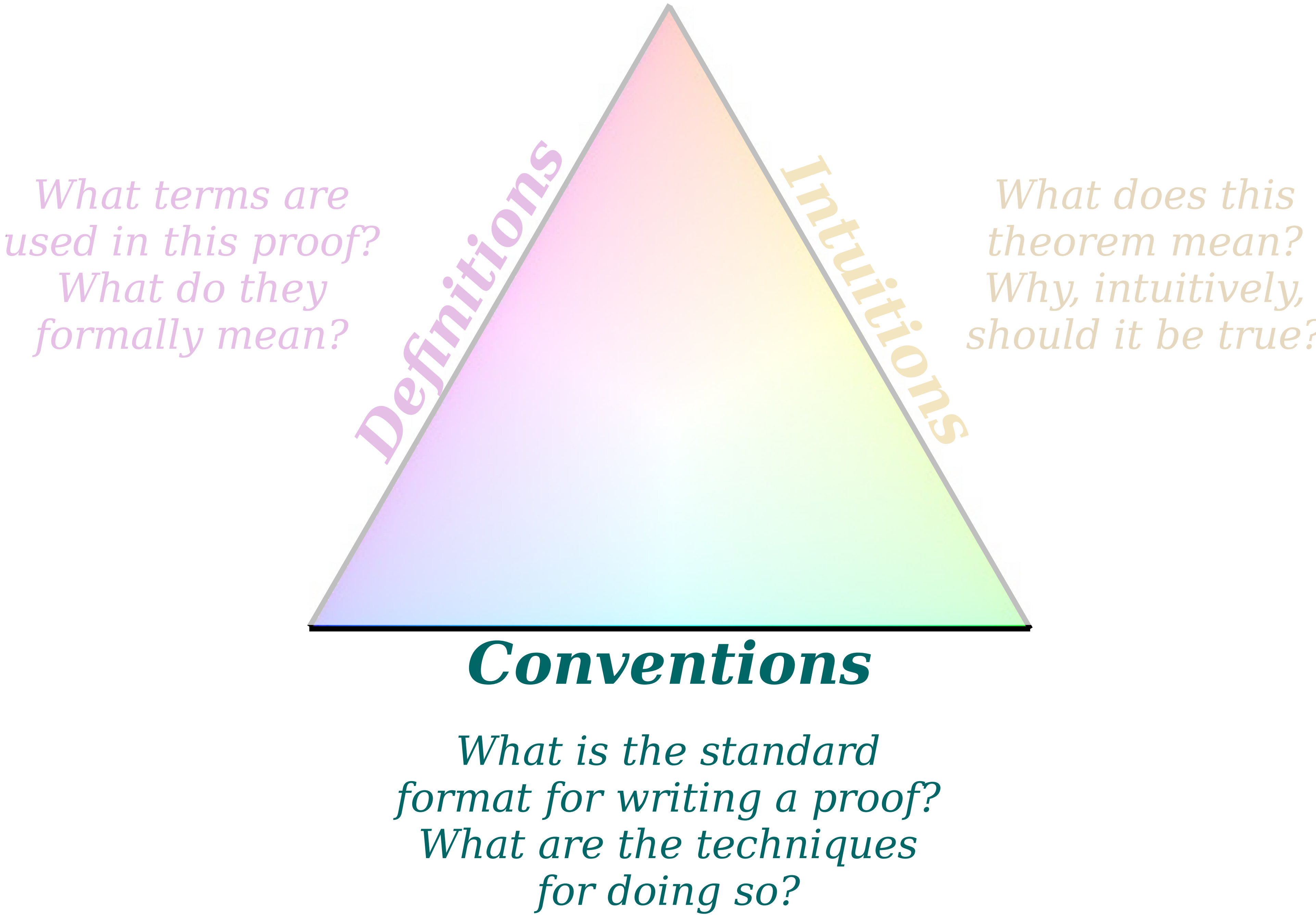
Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Let's Draw Some Pictures!



Amazing diagrams by Amy Liu.

Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.


What terms are used in this proof? What do they formally mean?
Definitions
Intuitions
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
$(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Proof: Pick any sets A, B, and C. Then, choose any element $x \in (A \cup C) \cap (B \cup C)$. We will prove that $x \in (A \cap B) \cup C$.

Since $x \in (A \cup C) \cap (B \cup C)$, we know that $x \in A \cup C$ and that $x \in B \cup C$. We now consider two cases.

Case 1: $x \in C$. This means $x \in (A \cap B) \cup C$ as well.

Case 2: $x \notin C$. Because $x \in A \cup C$, we know that $x \in A$ or that $x \in C$. However, since we have $x \notin C$, we're left with $x \in A$. By similar reasoning, from $x \in B \cup C$ we learn that $x \in B$.

Collectively, we've shown that $x \in A$ and that $x \in B$, so we see that $x \in A \cap B$. This means $x \in (A \cap B) \cup C$.

In either case, we see that $x \in (A \cap B) \cup C$, which is what we needed to show. ■

Theorem: If A, B, and C are sets, then

$(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Proof: Pick any sets A, B, and C. Then, choose any element $x \in (A \cup C) \cap (B \cup C)$. We will prove that $x \in (A \cap B) \cup C$.

Since $x \in (A \cup C) \cap (B \cup C)$, we know that $x \in A \cup C$ and that $x \in B \cup C$. We now consider two cases.

Case … ll.

Case … $x \in A$ or … we're lef… $B \cup C$ we…

These are <u>*arbitrary choices*</u>. Rather than specifying what $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{C}$ are, we're signaling to the reader that they could, in principle, supply any choices of $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{C}$ that they'd like.

Collectively, we've shown that $x \in A$ and that $x \in B$, so we see that $x \in A \cap B$. This means $x \in (A \cap B) \cup C$.

In either case, we see that $x \in (A \cap B) \cup C$, which is what we needed to show. ■

Theorem: If A, B, and C are sets, then
$(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Proof: Pick any sets A, B, and C. Then, choose any element $x \in (A \cup C) \cap (B \cup C)$. We will prove that $x \in (A \cap B) \cup C$.

Since x …
that $x \in$ …

Case 1: $x \in C$. This means $x \in (A \cap B) \cup C$ as well.

Case …

To prove that S ⊆ T:
Pick an arbitrary $x \in S$, then prove $x \in T$.

Notice that the statement of the theorem doesn't include any variable named x. We introduced this variable because that's what the definition says to do.

This is common in proofwriting. Always call back to the definition to make sure you're proving the right thing!

In eithe…
we need…

Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Proof: Pick any set
$x \in (A \cup C) \cap (B$.

Since $x \in (A \cup C$
that $x \in B \cup C$. W

As before, it's good to summarize what we established when splitting into cases.

Case 1: $x \in C$. This means $x \in (A \cap B) \cup C$ as well.

Case 2: $x \notin C$. Because $x \in A \cup C$, we know that $x \in A$ or that $x \in C$. However, since we have $x \notin C$, we're left with $x \in A$. By similar reasoning, from $x \in B \cup C$ we learn that $x \in B$.

Collectively, we've shown that $x \in A$ and that $x \in B$, so we see that $x \in A \cap B$. This means $x \in (A \cap B) \cup C$.

In either case, we see that $x \in (A \cap B) \cup C$, which is what we needed to show. ■

Theorem: If A, B, and C are sets, then
$(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$.

Proof: Pick any sets A, B, and C. Then, choose any element $x \in (A \cup C) \cap (B \cup C)$. We will prove that $x \in (A \cap B) \cup C$.

Since $x \in (A \cup C) \cap (B \cup C)$, we know that $x \in A \cup C$ and that $x \in B \cup C$. We now consider two cases.

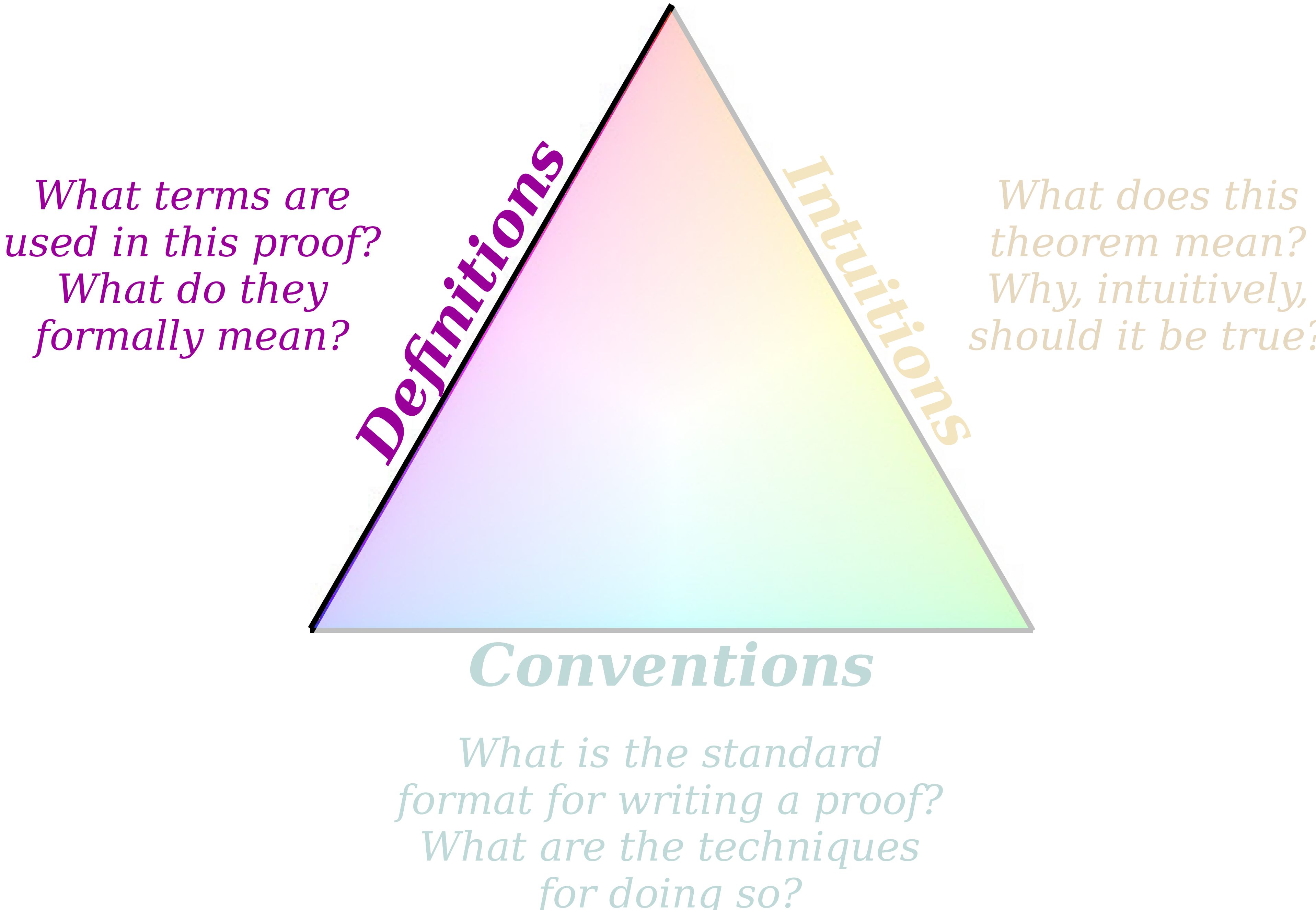
Case 1: $x \in C$. This means $x \in (A \cap B) \cup C$ as well.

Case 2: $x \notin C$. Because $x \in A \cup C$, we know that $x \in A$ or that $x \in C$. However, since we have $x \notin C$, we're left with $x \in A$. By similar reasoning, from $x \in B \cup C$ we learn that $x \in B$.

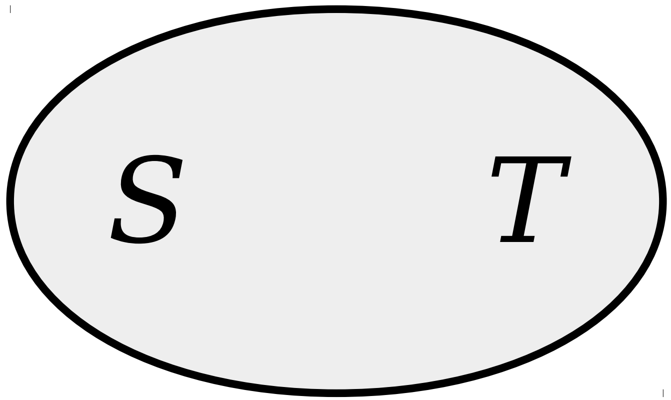
Collectively, we've shown that $x \in A$ and that $x \in B$, so we see that $x \in A \cap B$. This means $x \in (A \cap B) \cup C$.

In either case, we see that $x \in (A \cap B) \cup C$, which is what we needed to show. ■

Theorem: If A, B, and C are sets, then $(A \cup C) \cap (B \cup C) = (A \cap B) \cup C$.


Definitions
Intuitions
Conventions
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?

Set Equality



$S = T$

Definition: If S and T are sets, then $S = T$ if

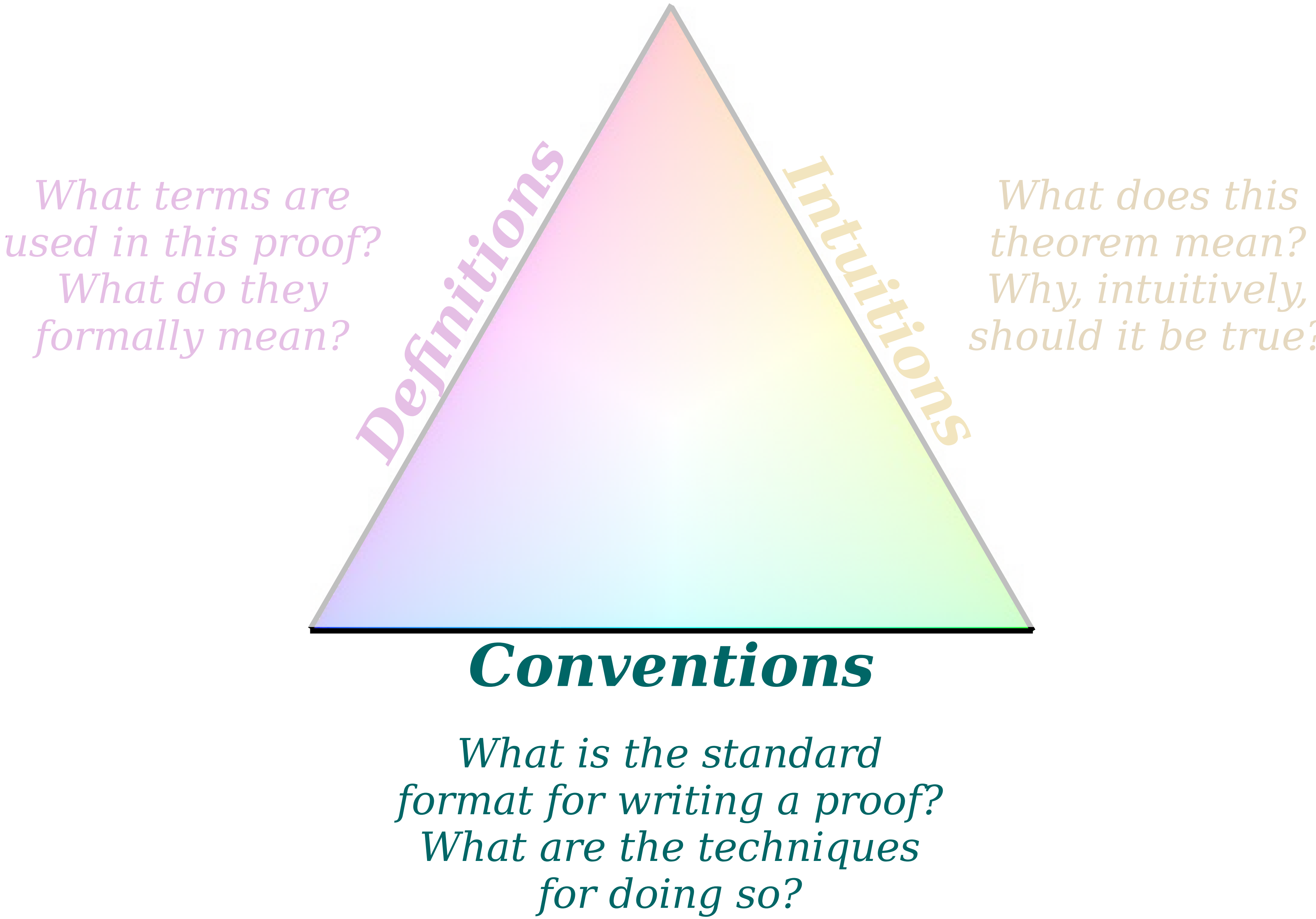
$$S \subseteq T \quad \text{and} \quad T \subseteq S.$$

If you know that $S = T$:

If you have an $x \in S$, you can conclude $x \in T$.
If you have an $x \in T$, you can conclude $x \in S$.

To prove that $S = T$:

Prove that $S \subseteq T$ and $T \subseteq S$.


Definitions
What terms are used in this proof? What do they formally mean?
Intuitions
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 $(A \cup C) \cap (B \cup C) = (A \cap B) \cup C$.

Proof: Fix any sets A, B, and C. We need to show that

$$(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C \tag{1}$$

and that

$$(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C). \tag{2}$$

We've already proved that (1) holds, so we just need to show (2). To do so, pick any $x \in (A \cap B) \cup C$. We need to prove that $x \in (A \cup C) \cap (B \cup C)$. But this is something we already know – we proved this earlier.

Since both (1) and (2) hold, we know that each of these two sets are subsets of one another, and therefore that the sets are equal. ■

Theorem: If A, B, and C are sets, then

$$(A \cup C) \cap (B \cup C) =$$

Proof: Fix any sets A, B

$$(A \cup C) \cap (B \cup$$

and that

It is common for proofs in math to build on one another. That's how we make progress and make new discoveries!

$$(A \cap B) \cup C \quad \subseteq \quad (A \cup C) \cap (B \cup C). \qquad (2)$$

We've already proved that (1) holds, so we just need to show (2). To do so, pick any $x \in (A \cap B) \cup C$. We need to prove that $x \in (A \cup C) \cap (B \cup C)$. But this is something we already know – we proved this earlier.

Since both (1) and (2) hold, we know that each of these two sets are subsets of one another, and therefore that the sets are equal. ■