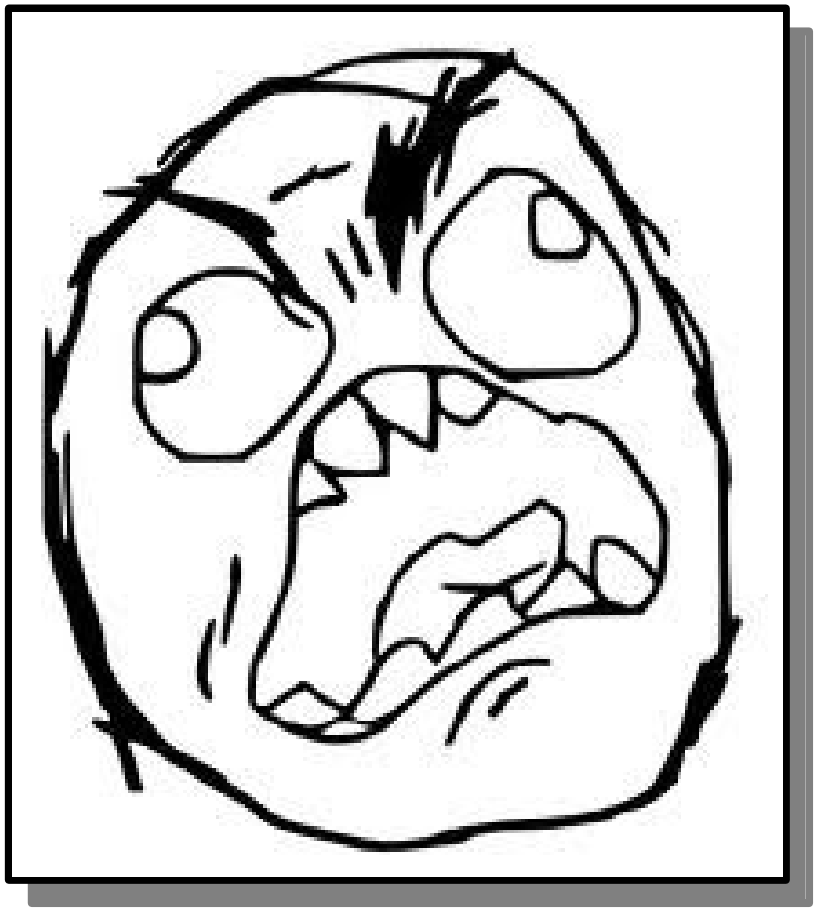
Introduction to Formal Proofs

Announcements

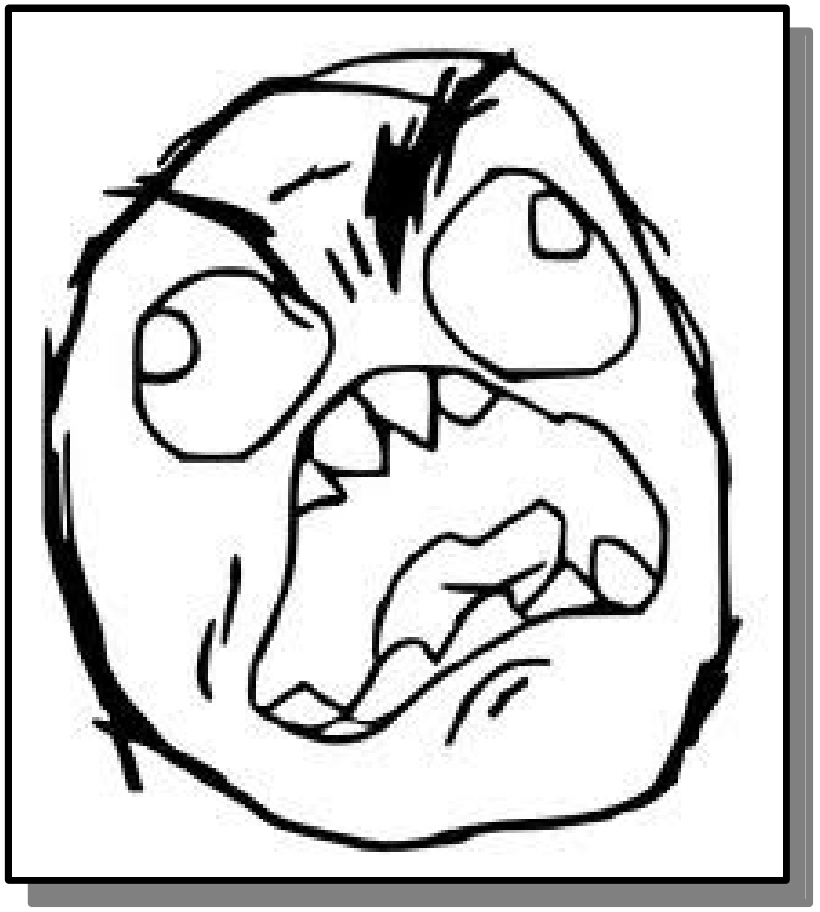
- Problem Set 1 out, due Friday, October 7 at 2:15PM (right before class).
  - **Start early!**
  - Later problems are harder than earlier ones; don't extrapolate from the first few problems.
  - Email us at **cs103@cs.stanford.edu** or stop by OH with questions.
- Office hours schedule is posted on the course website; Patrick is holding OH after class today (4:30PM – 6:30PM) in Gates B24A.

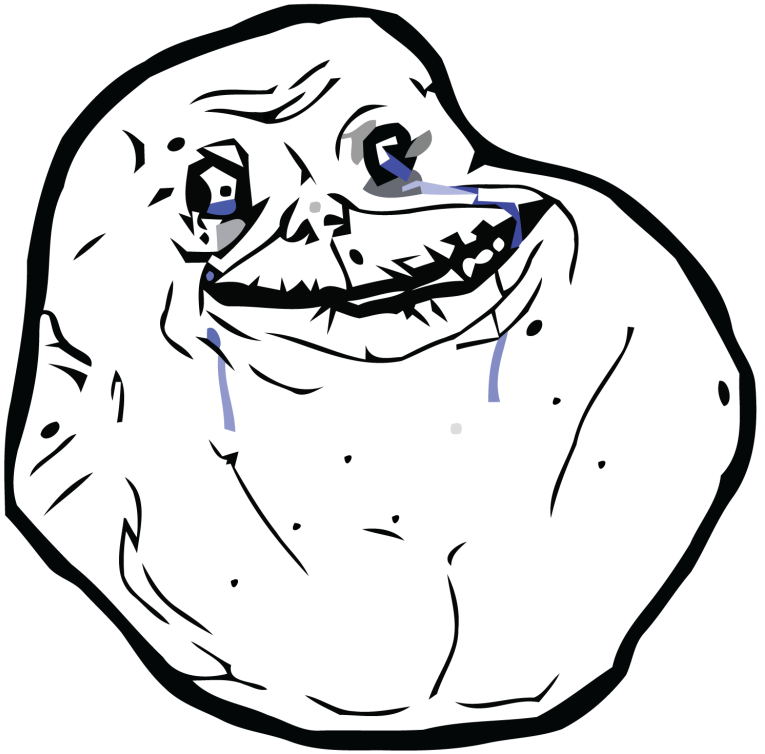
Office Hours

Office Hours

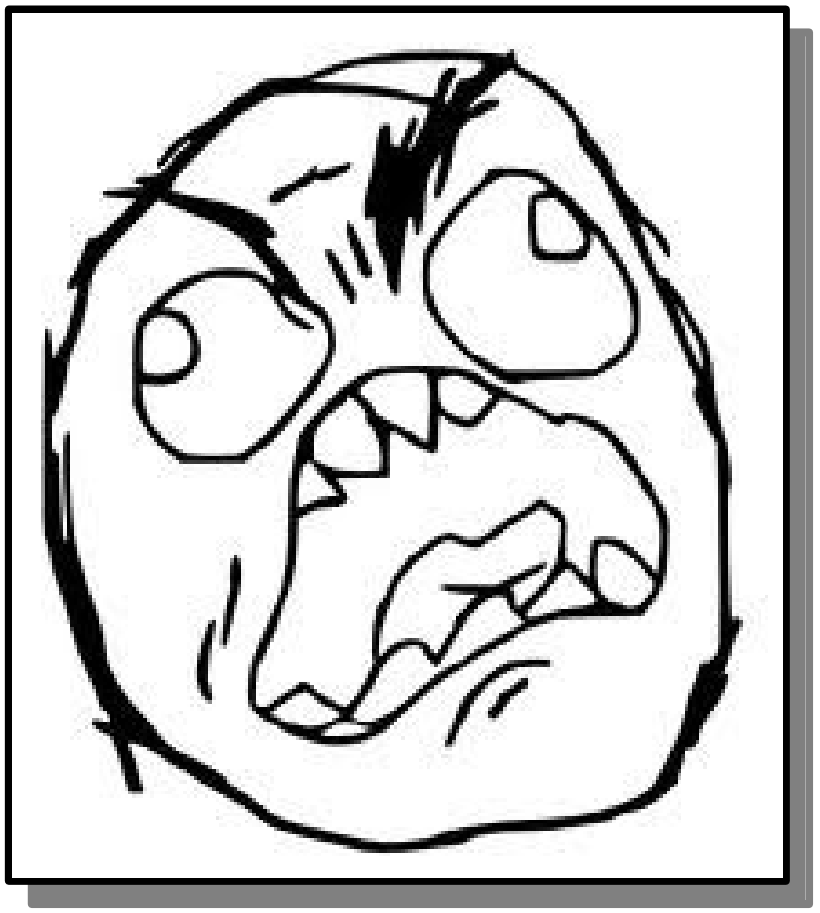


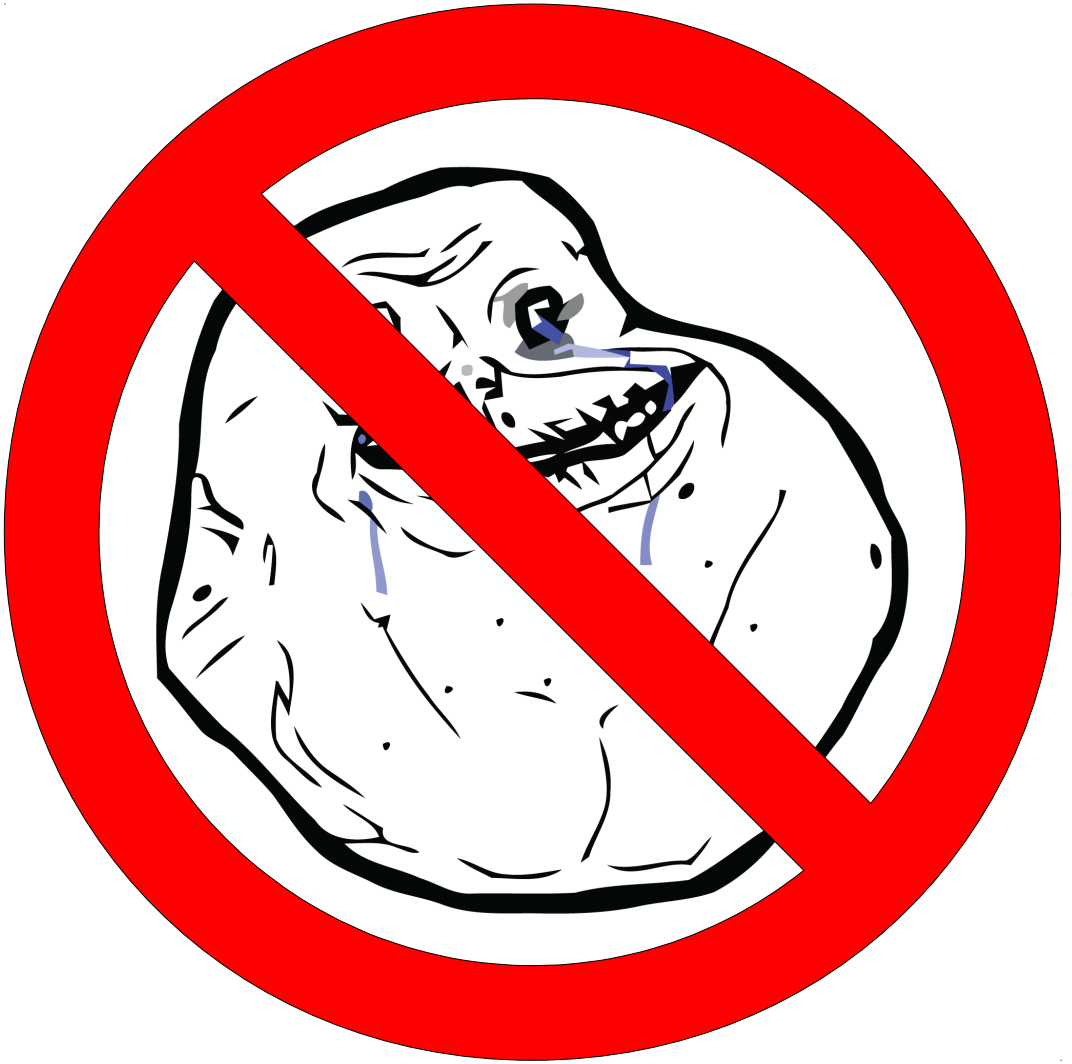
Office Hours





Office Hours





Office Hours

Friday Four Square

- Good snacks!
- Good company!
- Good game!
- Good fun!
- **Today at 4:15 in front of Gates.**

Friday Four Square

- Good snacks!
- Good company!
- Good game!
- Good fun!
- **Today at 4:15 in front of Gates.**

Mathematical Proofs

Structure of a Proof

- Begin with a set of initial assumptions (**hypotheses**).
- Through creativity, use logical reasoning to derive the final result (the **conclusion**) from the hypotheses.
- Assuming that all intermediary steps are sound logical reasoning, the conclusion **follows** from the hypotheses.

Proofs are Wonderful

- End up with **incontrovertible evidence** that your claim is correct.
- Develop a **better understanding** of the underlying structure of the problem.
  - Exploit interesting properties of the hypotheses to derive a final result.
  - See the connection between your proof and other similar proofs to arrive at a more general result.

Proofs are Hard

- A **single incorrect step** can render an entire proof invalid.
- Can't “**debug**” a proof as you would a program.
- Proofs are much harder to **synthesize** than to **follow**.

Looking Forward

- **Basic Proof Techniques** (Today/Monday)
  - What do proofs look like?
  - What strategies can be used to prove a result?
- **Proof by Induction** (Monday/Wednesday)
  - How do you prove properties of complex structures?
- **Application: Dijkstra's Algorithm** (Wednesday)
  - How do proofs help you better understand something?
- **Formal Logic** (Friday/Monday)
  - What are the formal laws governing proofs?

Direct Proofs

Direct Proofs

- A **direct proof** is the simplest type of proof.
- Starting with an initial set of hypotheses, apply simple logical steps to prove the conclusion.

Two Quick Definitions

- An integer is **even** if it can be written as 2k for some integer k.
- An integer is **odd** if it can be written as 2k + 1 for some integer k.
- Every integer is either even or odd.
- No integer is both even and odd.

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

If we let $m = 2k^2$, then $n^2 = 2m$.

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

If we let $m = 2k^2$, then $n^2 = 2m$.

So, by definition, n^2 is even.

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

If we let $m = 2k^2$, then $n^2 = 2m$.

So, by definition, n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

If we let $m = 2k^2$, then $n^2 = 2m$.

So, by definition, n^2 is even. ■

This symbol means "end of proof"

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

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

If we let m = 2k

So, by definitio

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

If we let $m = 2k^2$, then $n^2 = 2m$.

So, by definition, n^2 is even. ■

A Simple Direct Proof

Theorem: If n is even, n^2 is even.

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

Then $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.

If we let $m = 2k^2$, then $n^2 = 2m$.

So, by definition, n^2 is even. ■

Proofs with Implications

- To prove a statement of the form “if P is true, Q is true:”
  - Assume that P is true.
  - Using P and other hypotheses, show that Q is true as well.
- In the previous proof, we **assumed** that n was even, then used that to prove that n^2 is even.

An Incorrect Proof

An Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

An Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well.

An Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well. Consider any arbitrary $x \in A \cap B$. This means that $x \in A$ and $x \in B$, so $x \in A$ as required. ■

An Incorrect Proof

Theorem: For any sets A and B, $A \subseteq A \cap B$.

Proof: We need to show that if $x \in A$, then $x \in A \cap B$ as well. **Consider any arbitrary $x \in A \cap B$.** This means that $x \in A$ and $x \in B$, so $x \in A$ as required. ■

An Incorrect Proof

Theorem: Fo

Proof: We ne A ∩ B as well. **Consi** s means that x ∈ A ar

If you want to prove that P implies Q, assume P and prove Q.

Don't assume Q and then prove P!

A More Elaborate Direct Proof

- Suppose that we have two equivalence relations $(A, =_A)$ and $(B, =_B)$.
- Define a new relation $(A \times B, =_{A \times B})$ as
  - $(a_1, b_1) =_{A \times B} (a_2, b_2)$ if $a_1 =_A a_2$ and $b_1 =_B b_2$.
- Examples:
  - Are two shapes the same color and size?
  - Did two Olympic teams earn the same number of gold and silver medals?
- **Prove**: $(A \times B, =_{A \times B})$ is an equivalence relation.

Recall

- An equivalence relation is a relation that is
  - **Reflexive**: For any a, aRa
  - **Symmetric**: If aRb, bRa.
  - **Transitive**: If aRb and bRc, aRc.
- Using the definition, let's prove that $=_{A \times B}$ is an equivalence relation.

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Proof: We show that $=_{A \times B}$ is reflexive, symmetric, and transitive.

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Proof: We show that $=_{A \times B}$ is reflexive, symmetric, and transitive.

To see that it is reflexive, note that for any $(a, b) \in A \times B$, $a =_A a$ and $b =_B b$ because $=_A$ and $=_B$ are reflexive. Thus $(a, b) =_{A \times B} (a, b)$.

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Proof: We show that $=_{A \times B}$ is reflexive, symmetric, and transitive.

To see that it is reflexive, note that for any $(a, b) \in A \times B$, $a =_A a$ and $b =_B b$ because $=_A$ and $=_B$ are reflexive. Thus $(a, b) =_{A \times B} (a, b)$.

To see that it is symmetric, note that if $(a_1, b_1) =_{A \times B} (a_2, b_2)$, then $a_1 =_A a_2$ and $b_1 =_B b_2$. Since $=_A$ and $=_B$ are symmetric, $a_2 =_A a_1$ and $b_2 =_B b_1$, so $(a_2, b_2) =_{A \times B} (a_1, b_1)$.

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Proof: We show that $=_{A \times B}$ is reflexive, symmetric, and transitive.

To see that it is reflexive, note that for any $(a, b) \in A \times B$, $a =_A a$ and $b =_B b$ because $=_A$ and $=_B$ are reflexive. Thus $(a, b) =_{A \times B} (a, b)$.

To see that it is symmetric, note that if $(a_1, b_1) =_{A \times B} (a_2, b_2)$, then $a_1 =_A a_2$ and $b_1 =_B b_2$. Since $=_A$ and $=_B$ are symmetric, $a_2 =_A a_1$ and $b_2 =_B b_1$, so $(a_2, b_2) =_{A \times B} (a_1, b_1)$.

To see that is is transitive, suppose that $(a_1, b_1) =_{AxB} (a_2, b_2)$ and that $(a_2, b_2) =_{A \times B} (a_3, b_3)$. Thus $a_1 =_A a_2$ and $a_2 =_A a_3$, and because $=_A$ is transitive, $a_1 =_A a_3$. Similarly, $b_1 =_B b_2$ and $b_2 =_B b_3$, and because $=_B$ is transitive, $b_1 =_B b_3$. Consequently, $(a_1, b_1) =_{AxB} (a_3, b_3)$ as required.

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Proof: We show that $=_{A \times B}$ is reflexive, symmetric, and transitive.

To see that it is reflexive, note that for any $(a, b) \in A \times B$, $a =_A a$ and $b =_B b$ because $=_A$ and $=_B$ are reflexive. Thus $(a, b) =_{A \times B} (a, b)$.

To see that it is symmetric, note that if $(a_1, b_1) =_{A \times B} (a_2, b_2)$, then $a_1 =_A a_2$ and $b_1 =_B b_2$. Since $=_A$ and $=_B$ are symmetric, $a_2 =_A a_1$ and $b_2 =_B b_1$, so $(a_2, b_2) =_{A \times B} (a_1, b_1)$.

To see that is is transitive, suppose that $(a_1, b_1) =_{AxB} (a_2, b_2)$ and that $(a_2, b_2) =_{A \times B} (a_3, b_3)$. Thus $a_1 =_A a_2$ and $a_2 =_A a_3$, and because $=_A$ is transitive, $a_1 =_A a_3$. Similarly, $b_1 =_B b_2$ and $b_2 =_B b_3$, and because $=_B$ is transitive, $b_1 =_B b_3$. Consequently, $(a_1, b_1) =_{AxB} (a_3, b_3)$ as required. ■

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Proof: We show that $=_{A \times B}$ is reflexive, symmetric, and transitive.

To see that it is reflexive, note that for any $(a, b) \in A \times B$, $a =_A a$ and $b =_B b$ because $=_A$ and $=_B$ are reflexive. Thus $(a, b) =_{A \times B} (a, b)$.

To see that it is symmetric, note that **if $(a_1, b_1) =_{A \times B} (a_2, b_2)$**, then $a_1 =_A a_2$ and $b_1 =_B b_2$. Since $=_A$ and $=_B$ are symmetric, $a_2 =_A a_1$ and $b_2 =_B b_1$, so $(a_2, b_2) =_{A \times B} (a_1, b_1)$.

To see that is is transitive, **suppose that $(a_1, b_1) =_{AxB} (a_2, b_2)$ and that $(a_2, b_2) =_{A \times B} (a_3, b_3)$**. Thus $a_1 =_A a_2$ and $a_2 =_A a_3$, and because $=_A$ is transitive, $a_1 =_A a_3$. Similarly, $b_1 =_B b_2$ and $b_2 =_B b_3$, and because $=_B$ is transitive, $b_1 =_B b_3$. Consequently, $(a_1, b_1) =_{AxB} (a_3, b_3)$ as required. ■

Theorem: If $(A, =_A)$ and $(B, =_B)$ are equivalence relations, $(A \times B, =_{A \times B})$ is an equivalence relation.

Proof: We show that $=_{A \times B}$ is reflexive, symmetric, and transitive.

To see that it is reflexive, note that **for any $(a, b) \in A \times B$**, $a =_A a$ and $b =_B b$ because $=_A$ and $=_B$ are reflexive. Thus $(a, b) =_{A \times B} (a, b)$.

To see that it is symmetric, note that if $(a_1, b_1) =_{A \times B} (a_2, b_2)$, then $a_1 =_A a_2$ and $b_1 =_B b_2$. Since $=_A$ and $=_B$ are symmetric, $a_2 =_A a_1$ and $b_2 =_B b_1$, so $(a_2, b_2) =_{A \times B} (a_1, b_1)$.

To see that is is transitive, suppose that $(a_1, b_1) =_{AxB} (a_2, b_2)$ and that $(a_2, b_2) =_{A \times B} (a_3, b_3)$. Thus $a_1 =_A a_2$ and $a_2 =_A a_3$, and because $=_A$ is transitive, $a_1 =_A a_3$. Similarly, $b_1 =_B b_2$ and $b_2 =_B b_3$, and because $=_B$ is transitive, $b_1 =_B b_3$. Consequently, $(a_1, b_1) =_{AxB} (a_3, b_3)$ as required. ■

Proofs with Quantifiers

- To prove a statement of the form “for any x, P(x)”:
  - Assign a name to some object representing an arbitrary choice of x.
  - This does **not** mean “choose an arbitrary x;” rather, the symbol x stands in for any choice of x that we could ever make.
  - Prove that P(x) is true under the assumption that x could be anything and the choice is out of your control.

Another Incorrect Proof

Theorem: For any integer n, if n is even, n has no odd divisors.

Another Incorrect Proof

Theorem: For any integer n, if n is even, n has no odd divisors.

Proof: Consider an arbitrary natural number, say, 16. 16 is even, and it has no odd divisors. Since our choice was arbitrary, for any arbitrary n, if n is even, n has no odd divisors. ■

Another Incorrect Proof

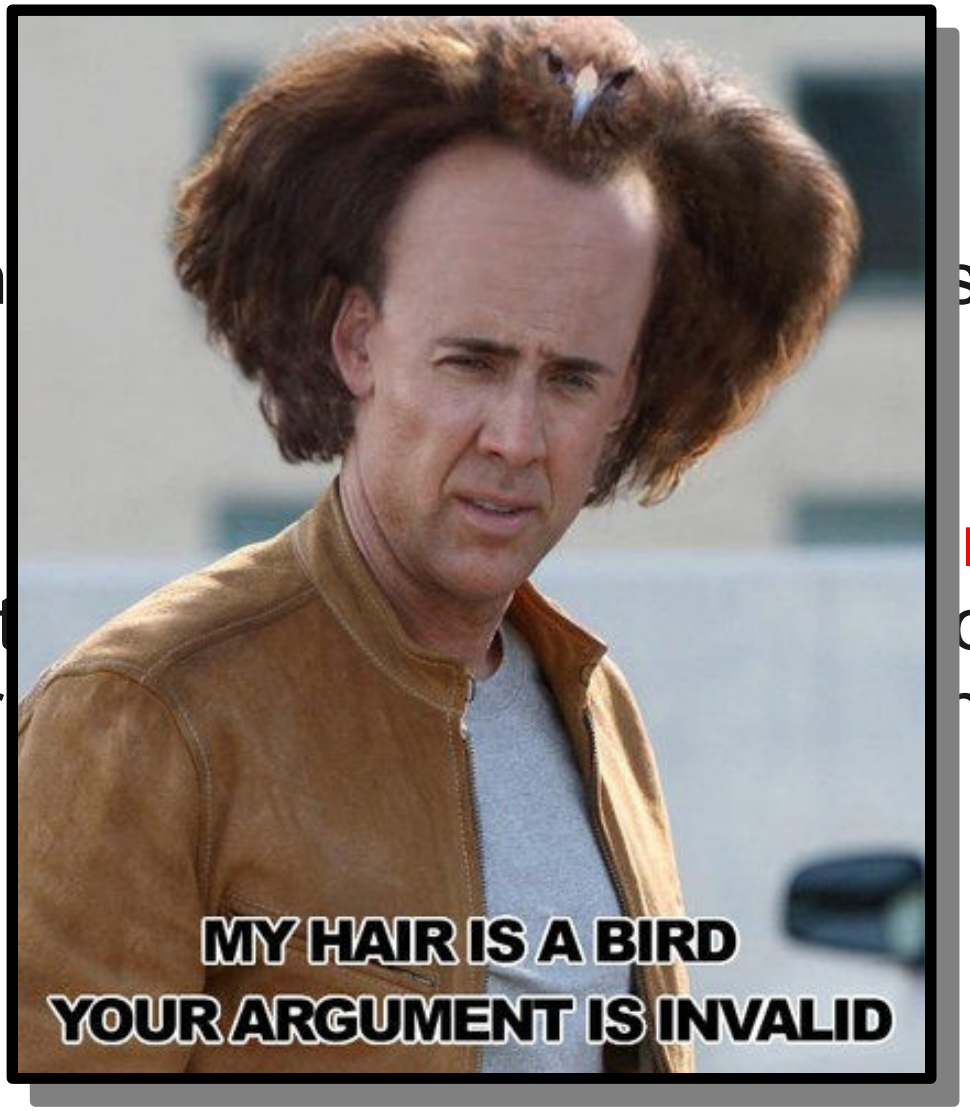
Theorem: For any integer n, if n is even, n has no odd divisors.

Proof: **Consider an arbitrary natural number, say, 16**. 16 is even, and it has no odd divisors. Since our choice was arbitrary, for any arbitrary n, if n is even, n has no odd divisors. ■

Another Incorrect Proof

Theorem: For an s no odd divisors.

Proof: **Consider r, say, 16**. 16 is even, and it our choice was arbitrary, for n has no odd divisors. ■



ar·bi·trar·y
adjective /ˈärbiˌtrerē/

1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value

Source: Google

ar·bi·trar·y
adjective /ˈärbiˌtrerē/

1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value

Source: Google

ar·bi·trar·y
adjective /ˈärbiˌtrerē/

Not this one!

1. Based on random choice or personal whim, rather than any reason or system - *“his mealtimes were entirely arbitrary”*

2. *(of power or a ruling body)* Unrestrained and autocratic in the use of authority - *“arbitrary rule by King and bishops has been made impossible”*

3. *(of a constant or other quantity)* Of unspecified value

Use this definition

Source: Google

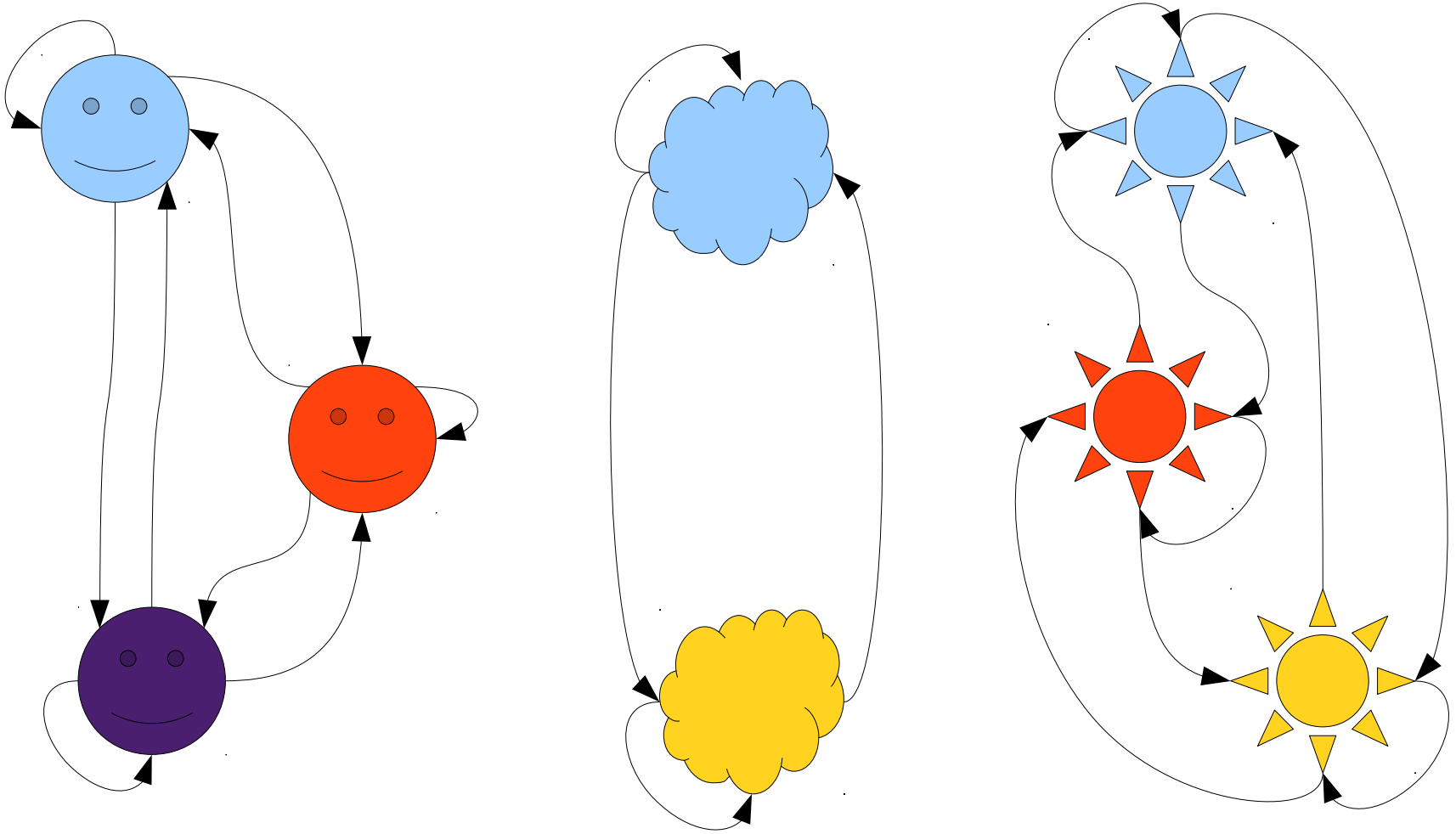
To prove something is true for all x, **do not** choose an x and base the proof off of your choice!

Instead, leave x unspecified and show that no matter what x is, the specified property must hold.

Making Arguments Readable

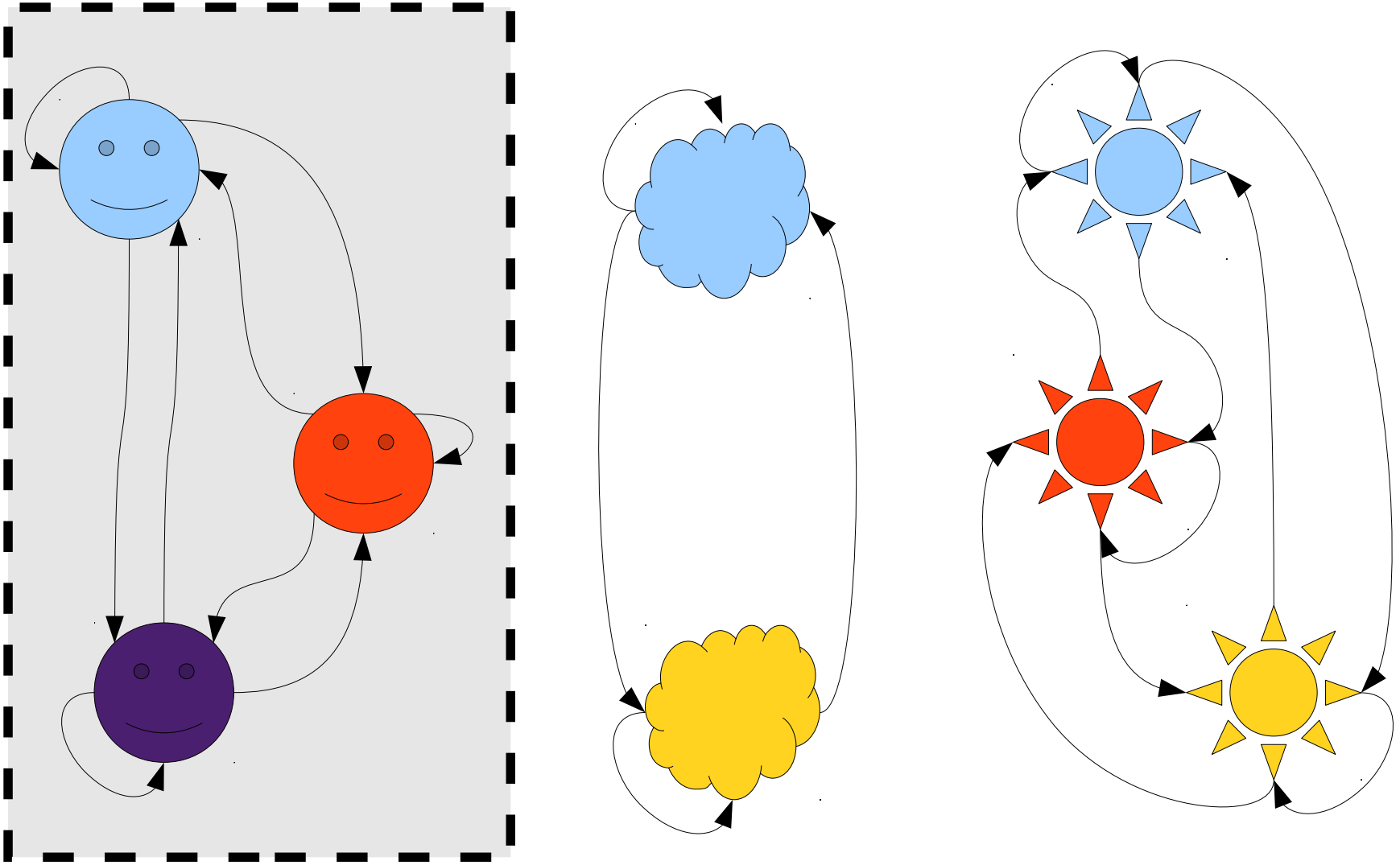
- Often, to prove some result, you must prove a weaker result first.
- From the weaker result, you then prove the final result.
- The weaker result is often called a **lemma**.
- Most lemmas are specific to a particular proof, though some lemmas are quite famous.
  - The **pumping lemma**.
  - **Schwarz's lemma** (no relation).

Equivalence Classes



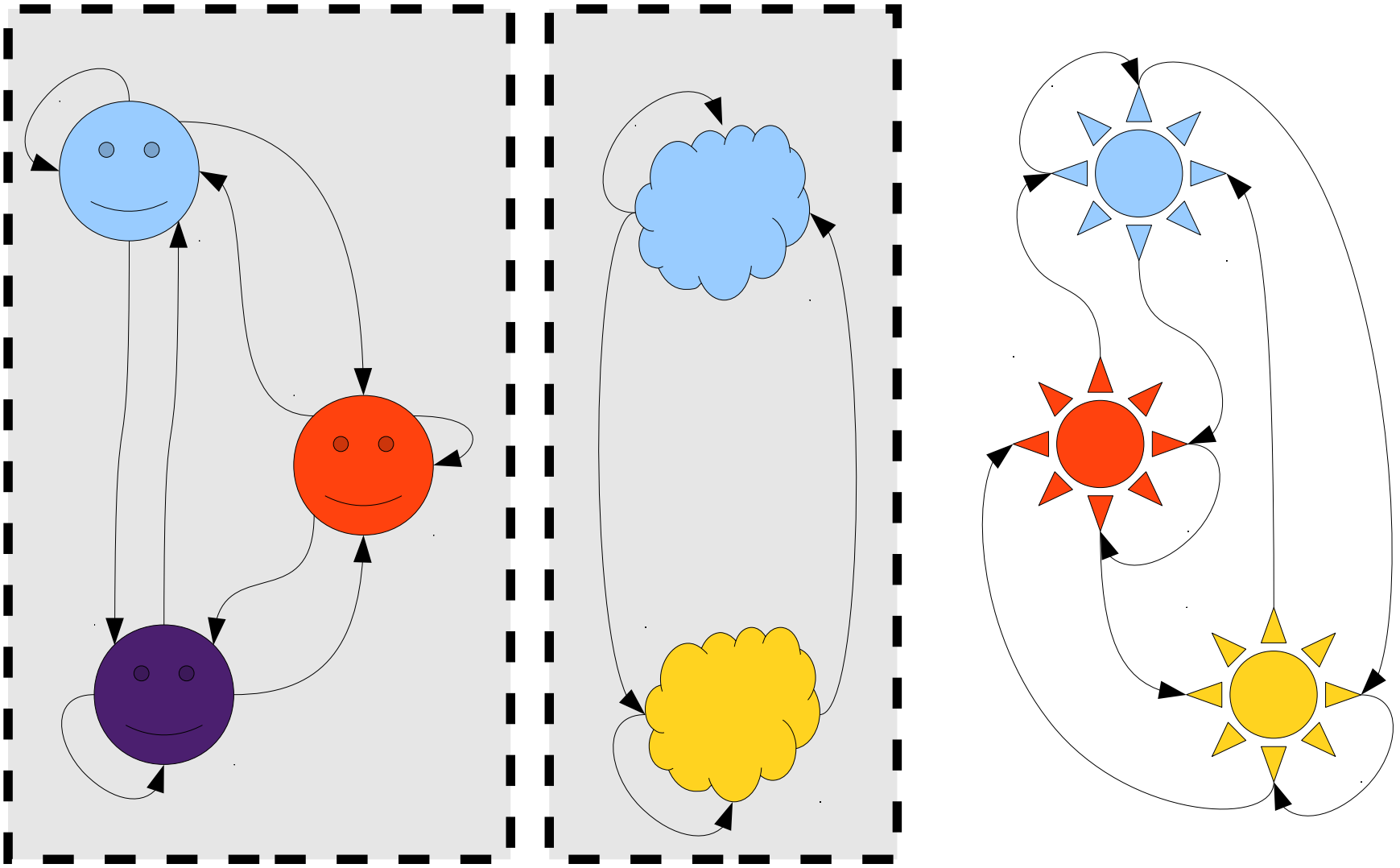
xRy ≡ x and y are the same shape.

Equivalence Classes



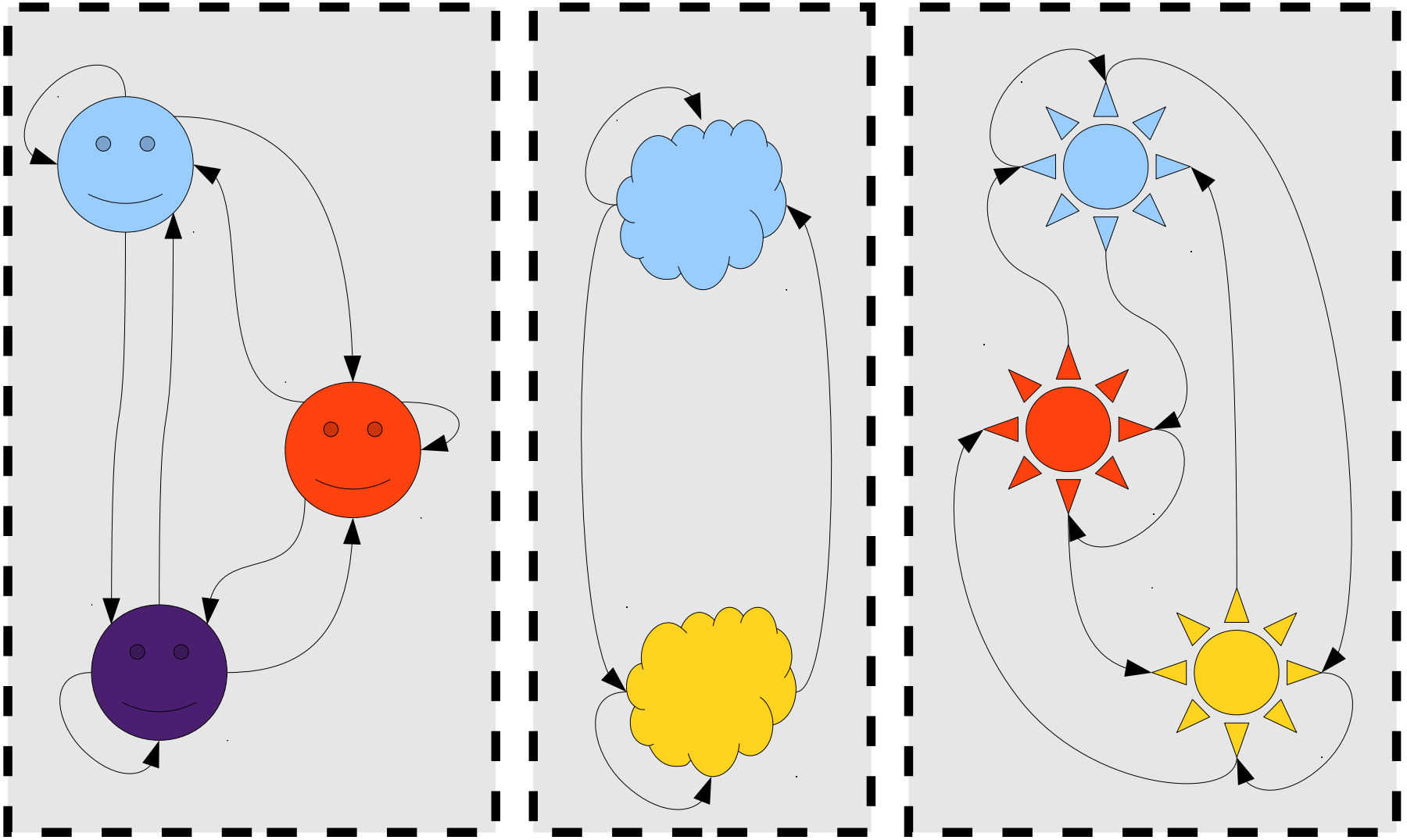
xRy ≡ x and y are the same shape.

Equivalence Classes



xRy ≡ x and y are the same shape.

Equivalence Classes



xRy ≡ x and y are the same shape.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

(Recall:

$$[a]_R = \{ x \mid aRx \}$$

that is, the set of elements equal to a)

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Pro tip: This is a standard technique for proving two sets are equal. You can use this result without having to prove it yourself.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy. Since R is symmetric, yRa.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy. Since R is symmetric, yRa. Since $x \in [a]_R$, aRx.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy. Since R is symmetric, yRa. Since $x \in [a]_R$, aRx. By transitivity, yRa and aRx gives yRx.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy. Since R is symmetric, yRa. Since $x \in [a]_R$, aRx. By transitivity, yRa and aRx gives yRx. Now, since $x \in [b]_R$, bRx and by symmetry, xRb.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy. Since R is symmetric, yRa. Since $x \in [a]_R$, aRx. By transitivity, yRa and aRx gives yRx. Now, since $x \in [b]_R$, bRx and by symmetry, xRb. yRx and xRb gives yRb by transitivity, which yields bRy by symmetry, and so by definition $y \in [b]_R$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy. Since R is symmetric, yRa. Since $x \in [a]_R$, aRx. By transitivity, yRa and aRx gives yRx. Now, since $x \in [b]_R$, bRx and by symmetry, xRb. yRx and xRb gives yRb by transitivity, which yields bRy by symmetry, and so by definition $y \in [b]_R$.

Proof: By Lemma 2, $[a]_R \subseteq [b]_R$ and $[b]_R \subseteq [a]_R$. By Lemma 1, this means that $[a]_R = [b]_R$.

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any sets S, T, if $S \subseteq T$ and $T \subseteq S$, then $S = T$.
Proof: By definition, $S = T$ if every $x \in S$ satisfies $x \in T$ and every $x \in T$ satisfies $x \in S$. Since $S \subseteq T$, for any $x \in S$, $x \in T$. Since $T \subseteq S$, for any $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.
Proof: Consider any $y \in [a]_R$. Then by definition, aRy. Since R is symmetric, yRa. Since $x \in [a]_R$, aRx. By transitivity, yRa and aRx gives yRx. Now, since $x \in [b]_R$, bRx and by symmetry, xRb. yRx and xRb gives yRb by transitivity, which yields bRy by symmetry, and so by definition $y \in [b]_R$.

Proof: By Lemma 2, $[a]_R \subseteq [b]_R$ and $[b]_R \subseteq [a]_R$. By Lemma 1, this means that $[a]_R = [b]_R$. ■

Proofs With Lemmas

Theorem: Let R be an equivalence relation over A. Then if $x \in [a]_R$ and $x \in [b]_R$, then $[a]_R = [b]_R$.

Lemma 1: For any

Proof: By definitio

very $x \in T$ satisfies $x \in S$. Since $S \subseteq$

y $x \in T$, $x \in S$. Thus $S = T$.

Lemma 2: Let R b

$\in [a]_R$ and $x \in [b]_R$, then $[a]_R \subseteq [b]_R$.

Proof: Consider a

R is symmetric, yRa. Since $x \in [a$

Rx. Now, since $x \in [b]_R$, bRx and

by transitivity, which yields bRy by symmetry, and so by definition $y \in [b]_R$.

Proof: By Lemma 2, $[a]_R \subseteq [b]_R$ and $[b]_R \subseteq [a]_R$. By Lemma 1, this means that $[a]_R = [b]_R$. ■

Proof by Contradiction

“When you have eliminated all which is impossible, then whatever remains, however improbable, must be the truth.”

- Sir Arthur Conan Doyle, *The Adventure of the Blanched Soldier*

Proof by Contradiction

- A **proof by contradiction** is a proof that works as follows:
  - To prove that P is true, assume that P is not true.
  - Based on the assumption that P is not true, conclude something impossible.
  - Assuming the logic is sound, the only option is that the assumption that P is not true is incorrect.
  - Conclude, therefore, that P is true.

A Simple Proof by Contradiction

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

A Simple Proof by Contradiction

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

Proof: By contradiction; assume that n^2 is even but that n is odd.

A Simple Proof by Contradiction

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

Proof: By contradiction; assume that n^2 is even but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

A Simple Proof by Contradiction

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

Proof: By contradiction; assume that n^2 is even but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

A Simple Proof by Contradiction

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

Proof: By contradiction; assume that n^2 is even but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is clearly impossible, since n^2 is even.

A Simple Proof by Contradiction

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

Proof: By contradiction; assume that n^2 is even but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is clearly impossible, since n^2 is even.

We have reached a contradiction, so our assumption was false. Thus if n^2 is even, n is even as well.

A Simple Proof by Contradiction

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

Proof: By contradiction; assume that n^2 is even but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is clearly impossible, since n^2 is even.

We have reached a contradiction, so our assumption was false. Thus if n^2 is even, n is even as well. ■

A Simple Proof by Contradiction

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

Proof: By contradiction; assume that n^2 is even but that n is odd.

Since n is odd, $n = 2k + 1$ for some integer k.

Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Now, let $m = 2k^2 + 2k$. Then $n^2 = 2m + 1$, so by definition n^2 is odd. But this is clearly impossible, since n^2 is even.

We have reached a contradiction, so our assumption was false. Thus if n^2 is even, n is even as well. ■