Functions

Part Two

Outline for Today

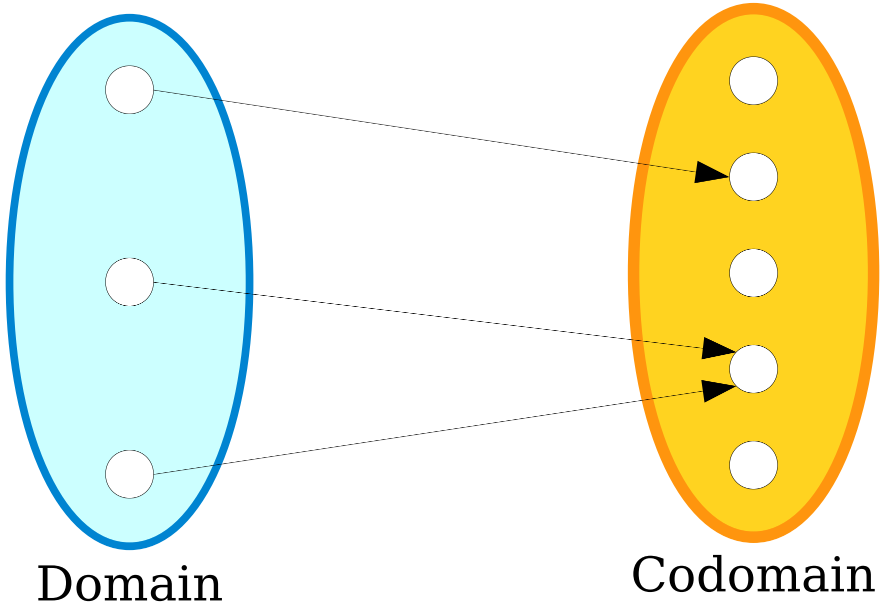
- ***Recap from Last Time***
  - Where are we, again?
- ***A Proof About Birds***
  - Trust me, it’s relevant. Ⅎ
- ***Assuming vs Proving***
  - Two different roles to watch for.
- ***Connecting Function Types***
  - Relating the topics from last time.
- ***Function Composition***
  - Sequencing functions together.

Recap from Last Time

Domains and Codomains

- Every function f has two sets associated with it: its ***domain*** and its ***codomain***.
- A function f can only be applied to elements of its domain. For any x in the domain, $f(x)$ belongs to the codomain.
- We write $\boldsymbol{f : A \rightarrow B}$ to indicate that f is a function whose domain is A and whose codomain is B.

The function must be defined for each element of its domain.



The output of the function must always be in the codomain, but not all elements of the codomain need to be covered.

Involutions

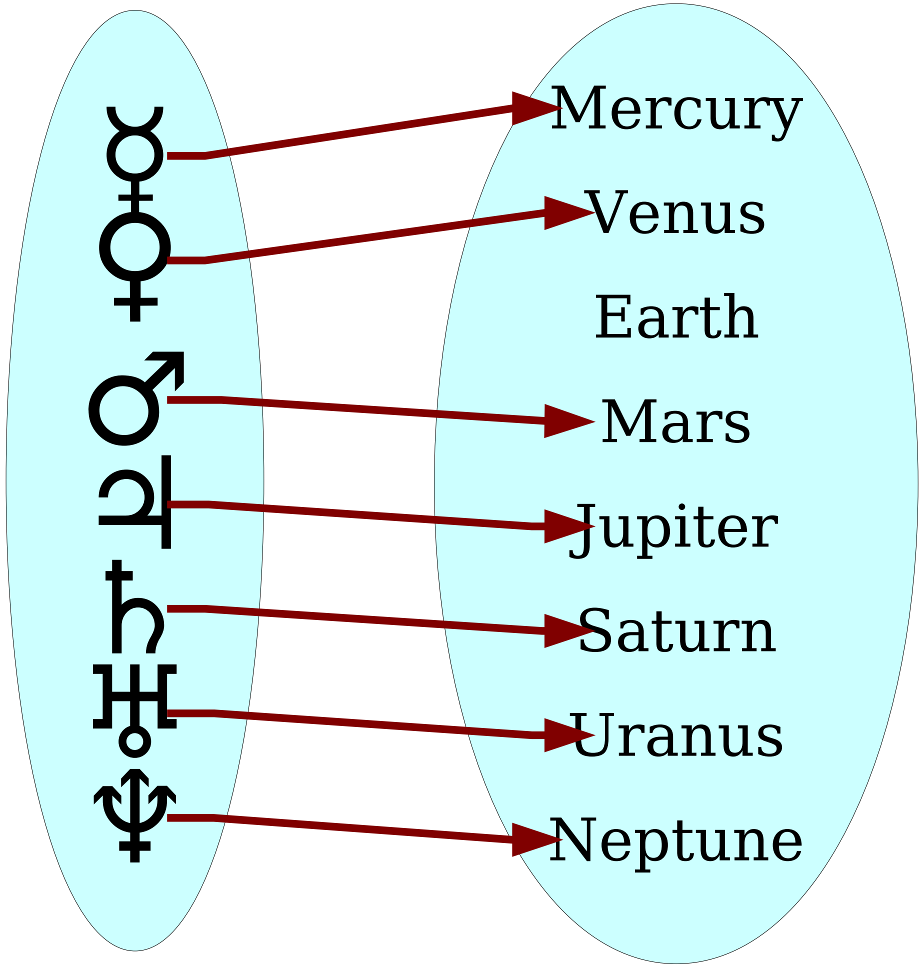
- A function $f : A \to A$ from a set back to itself is called an ***involution*** if the following first-order logic statement is true about f:

$$\forall x \in A.\ f(f(x)) = x.$$

("Applying f twice is equivalent to not applying f at all.")

Injective Functions

- $\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2))$
- $\forall a_1 \in A.\ \forall a_2 \in A.\ (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$



Review: Injective Functions

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$.
Then f is injective.

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$.
Then f is injective.

Proof:

What does it mean for the function f to be injective?

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$.
Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ f(n_1) = f(n_2) \to n_1 = n_2\ )$$

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ f(n_1) = f(n_2) \to n_1 = n_2\ )$$

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

Write two different sentences that could be the first sentence of a Direct Proof approach to this proof, one for each of the two definitions of injective–the "assume" step. *(remember that direct proof is for proving theorems that are implications–in this case that implication is in the definitions of injectivity.)*

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ f(n_1) = f(n_2) \to n_1 = n_2\ )$$

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

Write two different sentences that could be the **second** sentence of a **Direct Proof** approach to this proof, one for each of the two definitions of injective—the "want-to-show" step. *(remember that direct proof is for proving theorems that are implications—in this case that implication is in the definitions of injectivity.)*

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ f(n_1) = f(n_2) \to n_1 = n_2\ )$$

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ f(n_1) = f(n_2) \to n_1 = n_2\ )$$

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

Therefore, we'll pick arbitrary $n_1, n_2 \in \mathbb{N}$, assume $f(n_1) = f(n_2)$, then prove that $n_1 = n_2$.

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ f(n_1) = f(n_2) \to n_1 = n_2\ )$$

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

Therefore, we'll pick arbitrary $n_1, n_2 \in \mathbb{N}$, assume $f(n_1) = f(n_2)$, then prove that $n_1 = n_2$.

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ f(n_1) = f(n_2) \to n_1 = n_2\ )$$

$$\forall n_1 \in \mathbb{N}.\ \forall n_2 \in \mathbb{N}.\ (\ n_1 \neq n_2 \to f(n_1) \neq f(n_2)\ )$$

Therefore, we'll pick arbitrary $n_1, n_2 \in \mathbb{N}$, assume $f(n_1) = f(n_2)$, then prove that $n_1 = n_2$.

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof:

What does it mean for the function f to be injective?

$$\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. (f(n_1) = f(n_2) \to n_1 = n_2)$$

$$\forall n_1 \in \mathbb{N}. \forall n_2 \in \mathbb{N}. (n_1 \neq n_2 \to f(n_1) \neq f(n_2))$$

Therefore, we'll pick arbitrary $n_1, n_2 \in \mathbb{N}$, assume $f(n_1) = f(n_2)$, then prove that $n_1 = n_2$.

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof: Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof: Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof: Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$

This in turn means that

$$2n_1 = 2n_2$$

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof: Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$

This in turn means that

$$2n_1 = 2n_2,$$

so $n_1 = n_2$, as required.

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof: Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$

This in turn means that

$$2n_1 = 2n_2,$$

so $n_1 = n_2$, as required. ■

Good exercise: Repeat this proof using the other definition of injectivity!

Injective Functions

Theorem: Let $f : \mathbb{N} \to \mathbb{N}$ be defined as $f(n) = 2n + 7$. Then f is injective.

Proof: Consider any $n_1, n_2 \in \mathbb{N}$ where $f(n_1) = f(n_2)$. We will prove that $n_1 = n_2$.

Since $f(n_1) = f(n_2)$, we see that

$$2n_1 + 7 = 2n_2 + 7.$$

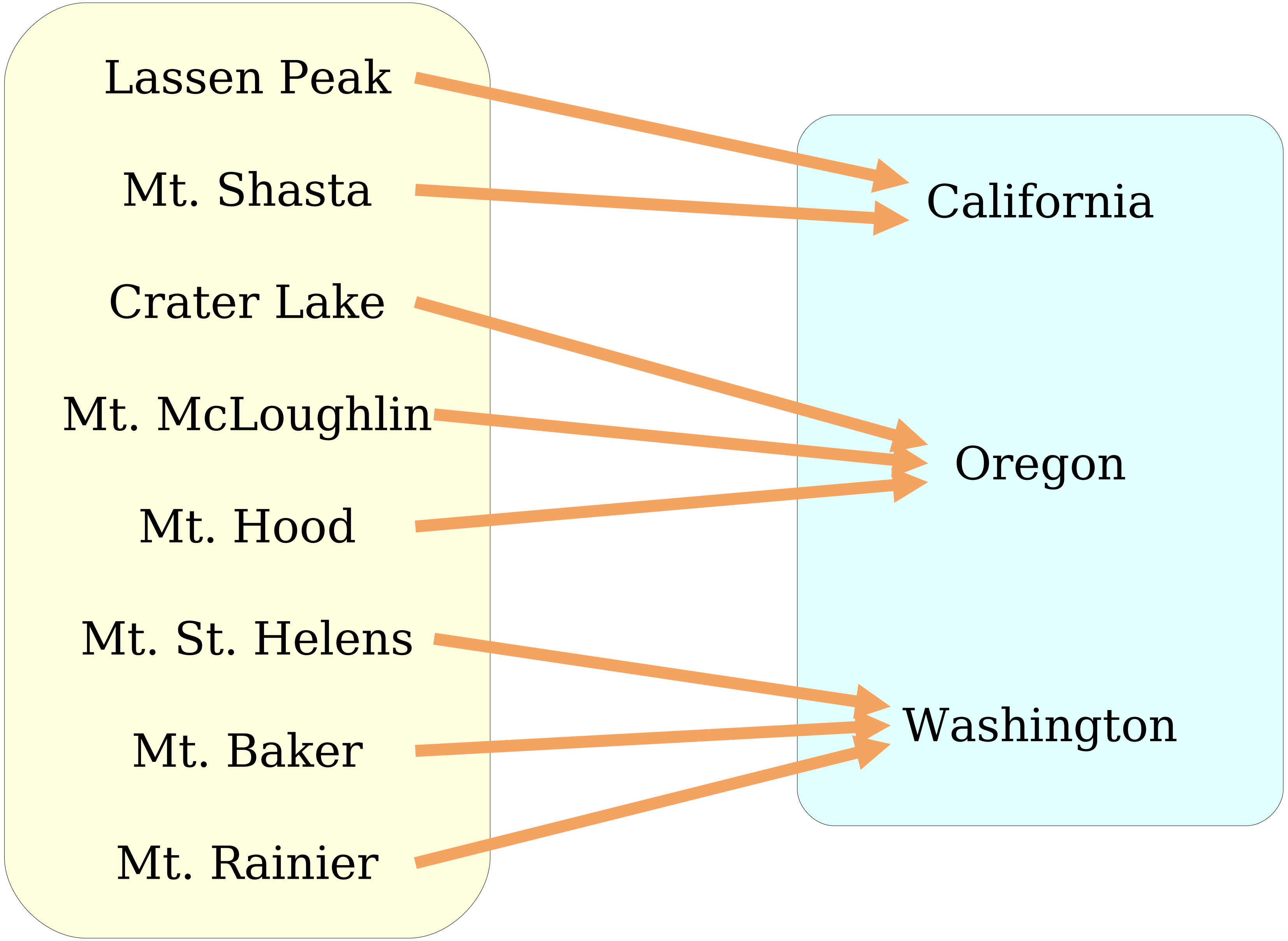
This in turn means that

$$2n_1 = 2n_2,$$

so $n_1 = n_2$, as required. ■

!! Important style rule !!
This proof contains <u>no first-order logic syntax</u> (quantifiers, connectives, etc.). It's written in plain English, just as usual.

Another Class of Functions


Lassen Peak
Mt. Shasta
Crater Lake
Mt. McLoughlin
Mt. Hood
Mt. St. Helens
Mt. Baker
Mt. Rainier
California
Oregon
Washington

Surjective Functions

- A function $f : A \to B$ is called ***surjective*** (or ***onto***) if this first-order logic statement is true about f:

$$\forall b \in B.\ \exists a \in A.\ f(a) = b$$

(*"For every output, there's an input that produces it."*)

- A function with this property is called a ***surjection***.
- How does this compare to our first rule of functions?

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof:

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof:

What does it mean for f to be surjective?

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

Therefore, we'll choose an arbitrary $y \in \mathbb{R}$, then prove that there is some $x \in \mathbb{R}$ where $f(x) = y$.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof:

What does it mean for f to be surjective?

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

Therefore, we'll choose an arbitrary $y \in \mathbb{R}$, then prove that there is some $x \in \mathbb{R}$ where $f(x) = y$.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof:

What does it mean for f to be surjective?

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

Therefore, we'll choose an arbitrary $y \in \mathbb{R}$, then prove that there is some $x \in \mathbb{R}$ where $f(x) = y$.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof:

What does it mean for f to be surjective?

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

Therefore, we'll choose an arbitrary $y \in \mathbb{R}$, then prove that there is some $x \in \mathbb{R}$ where $f(x) = y$.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof:

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2)$$

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2$$

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2 = y.$$

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2 = y.$$

So $f(x) = y$, as required.

Surjective Functions

Theorem: Let $f : \mathbb{R} \to \mathbb{R}$ be defined as $f(x) = 2x$. Then $f(x)$ is surjective.

Proof: Consider any $y \in \mathbb{R}$. We will prove that there is a choice of $x \in \mathbb{R}$ such that $f(x) = y$.

Let $x = y / 2$. Then we see that

$$f(x) = f(y / 2) = 2y / 2 = y.$$

So $f(x) = y$, as required. ■

!! Important style rule !!
This proof contains <u>no first-order logic syntax</u> (quantifiers, connectives, etc.). It's written in plain English, just as usual.

	To ***prove*** that this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.
$A \to B$	Assume A is true, then prove B is true.
$A \land B$	Prove A. Then prove B.
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.
$\neg A$	Simplify the negation, then consult this table on the result.

Pop Quiz!
Which row of this proof techniques table did we use for for that proof?

A Proof About Birds

Theorem: If all birds can fly,
then all herons can fly.

Theorem: If all birds can fly, then all herons can fly.

Given the predicates

$Bird(b)$, which says b is a bird;
$Heron(h)$, which says h is a heron; and
$CanFly(x)$, which says x can fly,

translate the theorem into first-order logic.

Go to
PollEv.com/cs103spr25

Theorem: If all birds can fly, then all herons can fly.

Given the predicates

> *Bird*(b), which says b is a bird;
> *Heron*(h), which says h is a heron; and
> *CanFly*(x), which says x can fly,

translate the theorem into first-order logic.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

	To ***prove*** that this is true…	
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	
$A \to B$	Assume A is true, then prove B is true.	
$A \land B$	Prove A. Then prove B.	
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	
$\neg A$	Simplify the negation, then consult this table on the result.	

	To ***prove*** that this is true…	
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	
$A \to B$	Assume A is true, then prove B is true.	
$A \land B$	Prove A. Then prove B.	
	Either prove $\neg A \to B$ or	

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

	To ***prove*** that this is true…	
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	
$A \to B$	Assume A is true, then prove B is true.	
$A \land B$	Prove A. Then prove B.	
	Either prove $\neg A \to B$ or	

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

$$\underbrace{(\forall b.\ (\mathit{Bird}(b) \to \mathit{CanFly}(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (\mathit{Heron}(h) \to \mathit{CanFly}(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Go to PollEv.com/cs103spr25

Which makes more sense as the next step in this proof?

1. Consider an arbitrary bird b.
2. Consider an arbitrary heron h.

$$(\forall b. (Bird(b) \to CanFly(b))) \to (\forall h. (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Which makes more sense as the next step in this proof?

1. Consider an arbitrary bird b.
2. Consider an arbitrary heron h.

$$(\forall b. (Bird(b) \to CanFly(b))) \to (\forall h. (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary bird b.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary bird b. Since b is a bird, b can fly.

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary bird b. Since b is a bird, b can fly. *[and now we're stuck! we are interested in herons, but b might not be one. It could be a hummingbird, for example!]*

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

All birds can fly — All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Which makes more sense as the next step in this proof?

1. Consider an arbitrary bird b.
2. Consider an arbitrary heron h.

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Which makes more sense as the next step in this proof?

1. Consider an arbitrary bird b.
2. Consider an arbitrary heron h.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

$$\underbrace{(\forall b.\ (Bird(b) \to CanFly(b)))}_{\text{All birds can fly}} \to \underbrace{(\forall h.\ (Heron(h) \to CanFly(h)))}_{\text{All herons can fly}}$$

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary heron h.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary heron h. We will show that h can fly.

$$(\forall b. (Bird(b) \to CanFly(b))) \to (\forall h. (Heron(h) \to CanFly(h)))$$

All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary heron h. We will show that h can fly. To do so, note that since h is a heron we know h is a bird.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

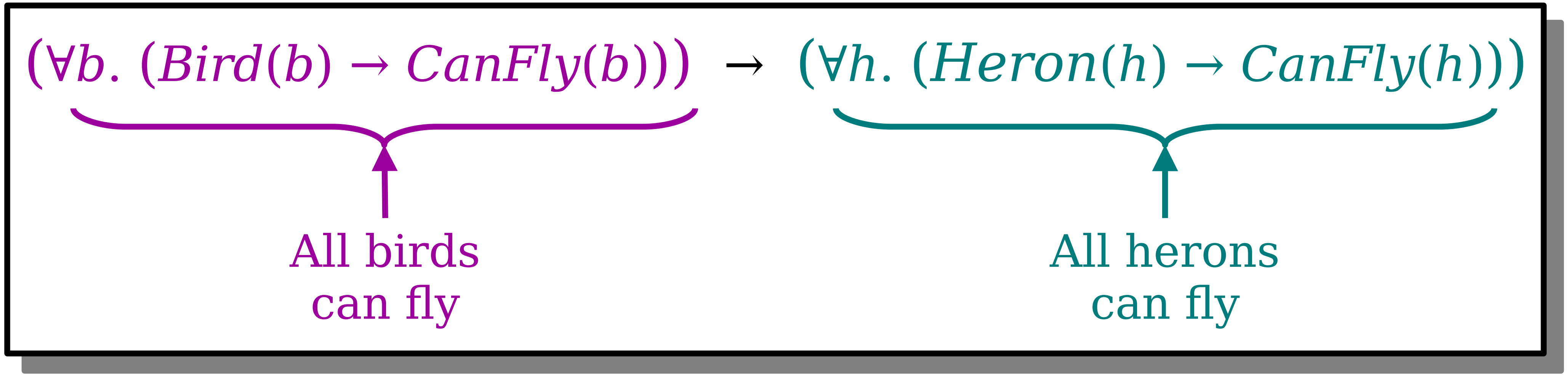
All birds can fly

All herons can fly

Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

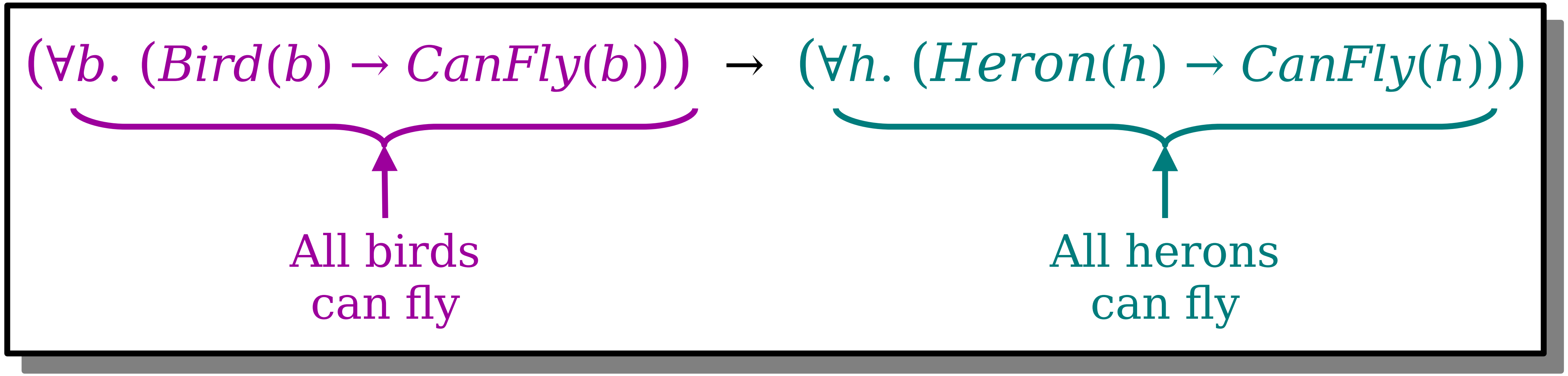
Consider an arbitrary heron h. We will show that h can fly. To do so, note that since h is a heron we know h is a bird. Therefore, by our earlier assumption, h can fly.



Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary heron h. We will show that h can fly. To do so, note that since h is a heron we know h is a bird. Therefore, by our earlier assumption, h can fly. ■



Theorem: If all birds can fly, then all herons can fly.

Proof: Assume that all birds can fly. We will show that all herons can fly.

Consider an arbitrary heron h. We will show that h can fly. To do so, note that since h is a heron we know h is a bird. Therefore, by our earlier assumption, h can fly. ■

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

We never introduce a variable b.

We introduce a variable h almost immediately.

Proving vs. Assuming

- In the context of a proof, you will need to assume some statements and prove others.
  - Here, we ***assumed*** all birds can fly.
  - Here, we ***proved*** all herons can fly.
- Statements behave differently based on whether you're assuming or proving them.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

We never introduce a variable *b*.

We introduce a variable *h* almost immediately.

Proving vs. Assuming

- To ***prove*** the universally-quantified statement

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

  we introduce a new variable x representing some arbitrarily-chosen value.

- Then, we prove that $P(x)$ is true for that variable x.
- That's why we introduced a variable h in this proof representing a heron.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \ \to\ (\forall h.\ (Heron(h) \to CanFly(h)))$$

We never introduce a variable b.

We introduce a variable h almost immediately.

Proving vs. Assuming

- If we ***assume*** the statement

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

  we ***do not*** introduce a variable x.

- Rather, if we find a relevant value z somewhere else in the proof, we can conclude that $P(z)$ is true.
- That's why we didn't introduce a variable b in our proof, and why we concluded that h, our heron, can fly.

$$(\forall b.\ (Bird(b) \to CanFly(b))) \to (\forall h.\ (Heron(h) \to CanFly(h)))$$

We never introduce a variable b.

We introduce a variable h almost immediately.

	To ***prove*** that this is true…	
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	
$A \to B$	Assume A is true, then prove B is true.	
$A \land B$	Prove A. Then prove B.	
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	
$\neg A$	Simplify the negation, then consult this table on the result.	

	To ***prove*** that this is true…	If you ***assume*** this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	
$A \to B$	Assume A is true, then prove B is true.	
$A \land B$	Prove A. Then prove B.	
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	
$\neg A$	Simplify the negation, then consult this table on the result.	

	To ***prove*** that this is true…	If you ***assume*** this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	Initially, ***do nothing***. Once you find a z through other means, you can state it has property A.
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	
$A \to B$	Assume A is true, then prove B is true.	Initially, ***do nothing***. Once you know A is true, you can conclude B is also true.
$A \land B$	Prove A. Then prove B.	
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	
$\neg A$	Simplify the negation, then consult this table on the result.	

	To ***prove*** that this is true…	If you ***assume*** this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	Initially, ***do nothing***. Once you find a z through other means, you can state it has property A.
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	Introduce a variable x into your proof that has property A.
$A \to B$	Assume A is true, then prove B is true.	Initially, ***do nothing***. Once you know A is true, you can conclude B is also true.
$A \land B$	Prove A. Then prove B.	Assume A. Then assume B.
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	
$\neg A$	Simplify the negation, then consult this table on the result.	

	To ***prove*** that this is true…	If you ***assume*** this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	Initially, ***do nothing***. Once you find a z through other means, you can state it has property A.
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	Introduce a variable x into your proof that has property A.
$A \to B$	Assume A is true, then prove B is true.	Initially, ***do nothing***. Once you know A is true, you can conclude B is also true.
$A \land B$	Prove A. Then prove B.	Assume A. Then assume B.
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	Consider two cases. Case 1: A is true. Case 2: B is true.
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	Assume $A \to B$ and $B \to A$.
$\neg A$	Simplify the negation, then consult this table on the result.	Simplify the negation, then consult this table on the result.

Connecting Function Types

Types of Functions

- We've seen three special types of functions:
  - ***involutions***, functions that undo themselves;
  - ***injections***, functions where different inputs go to different outputs; and
  - ***surjections***, functions that cover their whole codomain.
- ***Question:*** How do these three classes of functions relate to one another?

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{f \text{ is an involution.}} \quad \to \quad \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{f \text{ is surjective.}}$$

Theorem: For any function $f : A \to A$,
if f is an involution, then f is surjective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{\text{Assume this.}} \rightarrow \underbrace{(\forall b \in A.\ \exists a \in A.\ f(a) = b)}_{\text{Prove this.}}$$

Theorem: For any function $f : A \rightarrow A$,
if f is an involution, then f is surjective.

$$(\forall x \in A.\ f(f(x)) = x) \;\rightarrow\; (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

Assume this. Prove this.

$$(\forall b.\ (Bird(b) \rightarrow CanFly(b))) \;\rightarrow\; (\forall h.\ (Heron(h) \rightarrow CanFly(h)))$$

Assume this. Prove this.

Theorem: For any function $f : A \rightarrow A$,
if f is an involution, then f is surjective.

$$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

Assume this.

Prove this.

Since we're *assuming* this, we aren't going to pick a specific choice of x right now. Instead, we're going to keep an eye out for something to apply this fact to.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \rightarrow A$, if f is an involution, then f is surjective.

$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$

Ass

We've said that we need to prove this statement. How do we do that?

Prove this.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \rightarrow A$, if f is an involution, then f is surjective.

$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$

Prove this.

There's a universal quantifier up front. Since we're *proving* this, we'll pick an arbitrary $b \in A$.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \rightarrow A$, if f is an involution, then f is surjective.

$$(\forall x \in A.\ f(f(x)) = x) \to (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

Ass

There's a universal quantifier up front. Since we're *proving* this, we'll pick an arbitrary $b \in A$.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

$$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$$

Now, we hit an existential quantifier. Since we're *proving* this, we need to find a choice of $a \in A$ where this is true.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.

Theorem: For any function $f : A \rightarrow A$, if f is an involution, then f is surjective.

$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall b \in A.\ \exists a \in A.\ f(a) = b)$

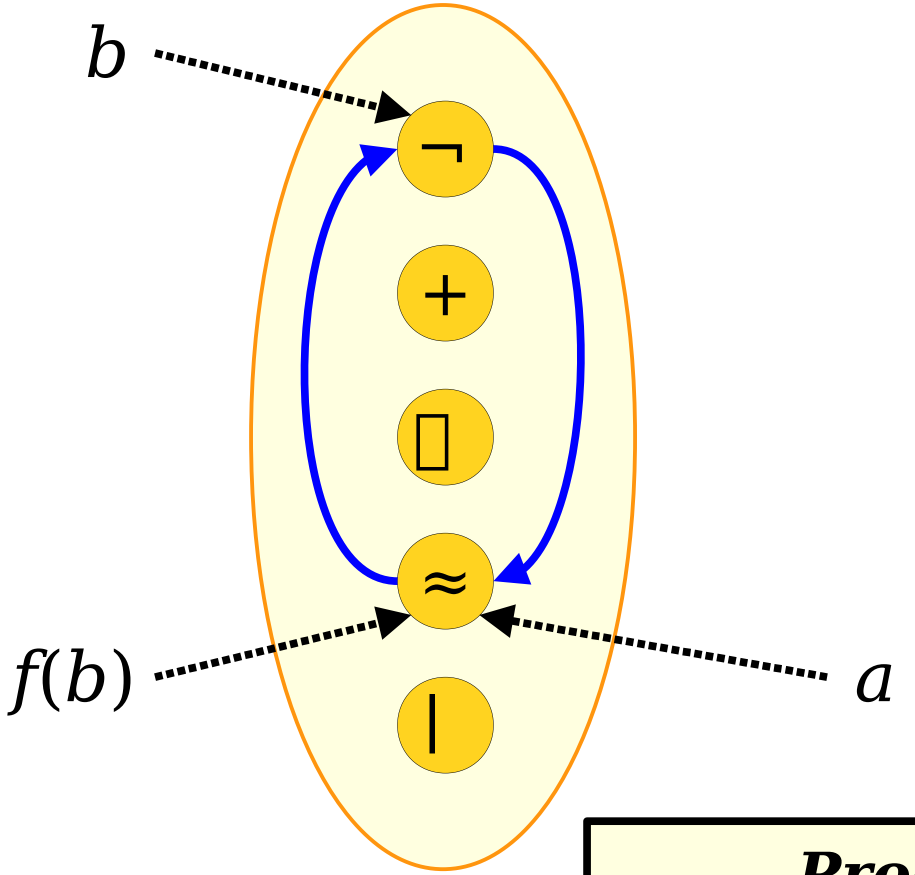
Now, we hit an existential quantifier. Since we're *proving* this, we need to find a choice of $a \in A$ where this is true.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \rightarrow A$, if f is an involution, then f is surjective.



Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof:

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$. We need to show that there is an $a \in A$ where $f(a) = b$.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$. We need to show that there is an $a \in A$ where $f(a) = b$.

Specifically, pick $a = f(b)$.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$. We need to show that there is an $a \in A$ where $f(a) = b$.

Specifically, pick $a = f(b)$. This means that $f(a) = f(f(b))$, and since f is an involution we know that $f(f(b)) = b$.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$. We need to show that there is an $a \in A$ where $f(a) = b$.

Specifically, pick $a = f(b)$. This means that $f(a) = f(f(b))$, and since f is an involution we know that $f(f(b)) = b$. Putting this together, we see that $f(a) = b$, which is what we needed to show.

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is surjective.

Proof: Pick any involution $f : A \to A$. We will prove that f is surjective. To do so, pick an arbitrary $b \in A$. We need to show that there is an $a \in A$ where $f(a) = b$.

Specifically, pick $a = f(b)$. This means that $f(a) = f(f(b))$, and since f is an involution we know that $f(f(b)) = b$. Putting this together, we see that $f(a) = b$, which is what we needed to show. ■

Proof Outline

1. Assume f is an involution.
2. Pick an arbitrary $b \in A$.
3. Give a choice of $a \in A$ where $f(a) = b$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$$\underbrace{(\forall x \in A.\ f(f(x)) = x)}_{f \text{ is an involution.}} \rightarrow \underbrace{(\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)))}_{f \text{ is injective.}}$$

Theorem: For any function $f : A \rightarrow A$,
if f is an involution, then f is injective.

$$(\forall x \in A.\ f(f(x)) = x) \to (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))$$

Assume this.

Prove this.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$$(\forall x \in A.\ f(f(x)) = x) \to (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))$$

Assume this.

Prove this.

$$(\forall b.\ (\mathit{Bird}(b) \to \mathit{CanFly}(b))) \to (\forall h.\ (\mathit{Heron}(h) \to \mathit{CanFly}(h)))$$

Assume this.

Prove this.

Theorem: For any function $f : A \to A$,
if f is an involution, then f is injective.

$$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)))$$

Assume this.

Prove this.

Since we're *assuming* this, we aren't going to pick a specific choice of x right now. Instead, we're going to keep an eye out for something to apply this fact to.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$$(\forall x \in A.\ f(f(x)) = x) \rightarrow (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)))$$

We need to *prove* this part. What does that mean?

Prove this.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \rightarrow A$, if f is an involution, then f is injective.

$(\forall x \in A.\ f(f(x)) = x) \to (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2))$

Since we're *proving* something universally-quantified, we'll pick some values arbitrarily.

Prove this.

Proof Outline

1. Assume f is an involution.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$(\forall x \in A.\ f(f(x)) = x) \to (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2))$

Since we're *proving* something universally-quantified, we'll pick some values arbitrarily.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary a_1, $a_2 \in A$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$$(\forall x \in A.\ f(f(x)) = x) \to (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))$$

We now need to prove this implication. But we know how to do that! We assume the antecedent and prove the consequent.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary a_1, $a_2 \in A$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

$(\forall x \in A.\ f(f(x)) = x) \to (\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to f(a_1) \neq f(a_2)))$

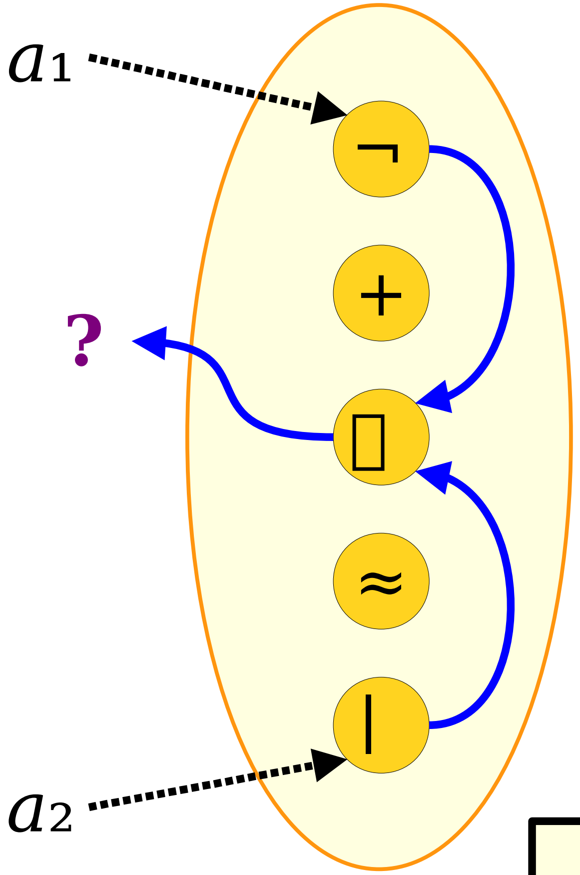
We now need to *prove* this implication. But we know how to do that! We assume the antecedent and prove the consequent.

Prove this.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.



Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof:

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

We'll proceed by contradiction.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

We'll proceed by contradiction. Suppose that $f(a_1) = f(a_2)$.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

We'll proceed by contradiction. Suppose that $f(a_1) = f(a_2)$. This means $f(f(a_1)) = f(f(a_2))$, which in turn tells us $a_1 = a_2$ because f is an involution.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

We'll proceed by contradiction. Suppose that $f(a_1) = f(a_2)$. This means $f(f(a_1)) = f(f(a_2))$, which in turn tells us $a_1 = a_2$ because f is an involution. But that's impossible, since $a_1 \neq a_2$.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

We'll proceed by contradiction. Suppose that $f(a_1) = f(a_2)$. This means $f(f(a_1)) = f(f(a_2))$, which in turn tells us $a_1 = a_2$ because f is an involution. But that's impossible, since $a_1 \neq a_2$.

We've reached a contradiction, so our assumption was wrong.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

We'll proceed by contradiction. Suppose that $f(a_1) = f(a_2)$. This means $f(f(a_1)) = f(f(a_2))$, which in turn tells us $a_1 = a_2$ because f is an involution. But that's impossible, since $a_1 \neq a_2$.

We've reached a contradiction, so our assumption was wrong. Therefore, we see that $f(a_1) \neq f(a_2)$, as required.

Proof Outline

1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Theorem: For any function $f : A \to A$, if f is an involution, then f is injective.

Proof: Consider any function $f : A \to A$ that's an involution. We will prove that f is injective. To do so, choose any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We need to show that $f(a_1) \neq f(a_2)$.

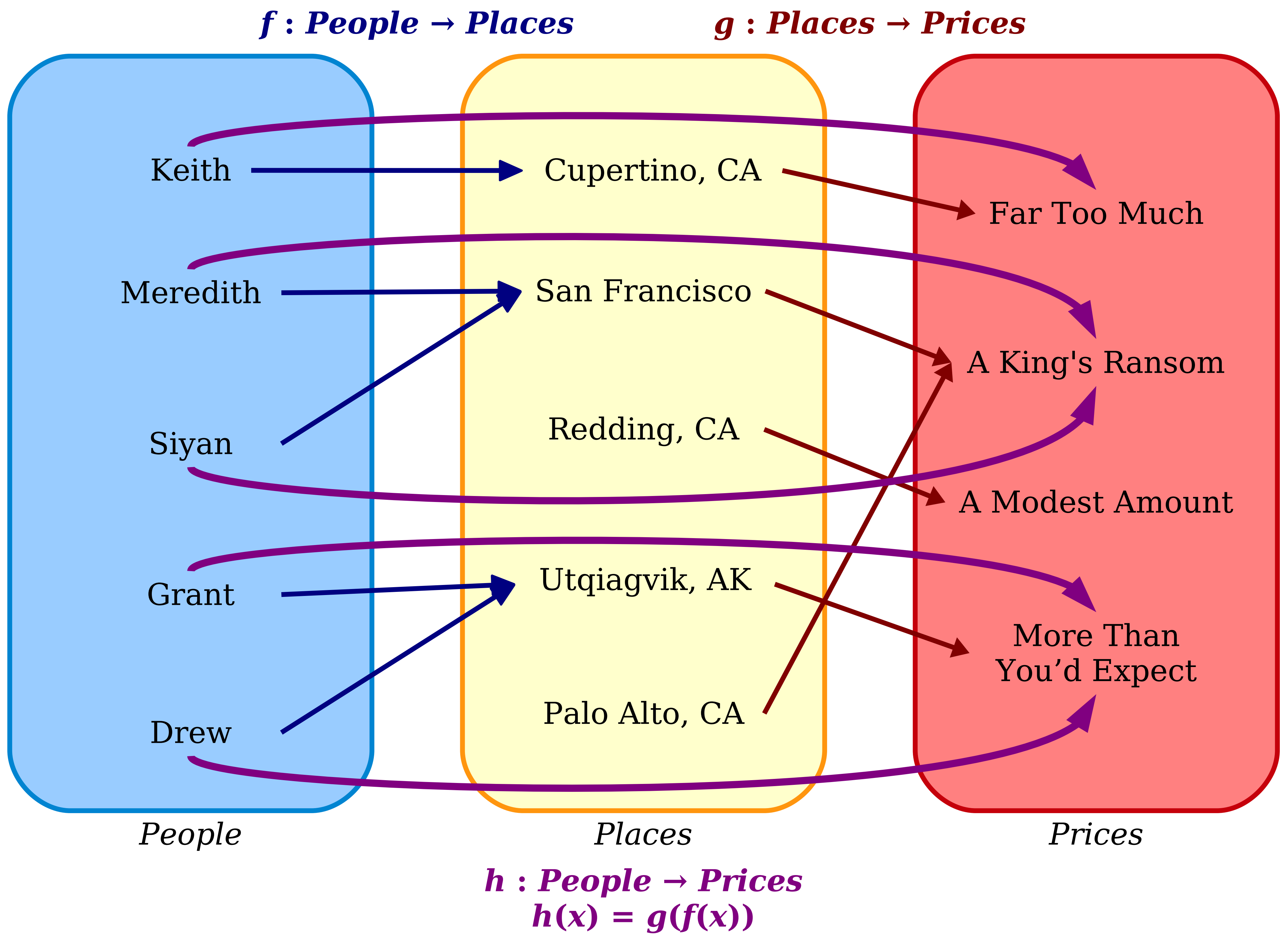
We'll proceed by contradiction. Suppose that $f(a_1) = f(a_2)$. This means $f(f(a_1)) = f(f(a_2))$, which in turn tells us $a_1 = a_2$ because f is an involution. But that's impossible, since $a_1 \neq a_2$.

We've reached a contradiction, so our assumption was wrong. Therefore, we see that $f(a_1) \neq f(a_2)$, as required. ■

Proof Outline

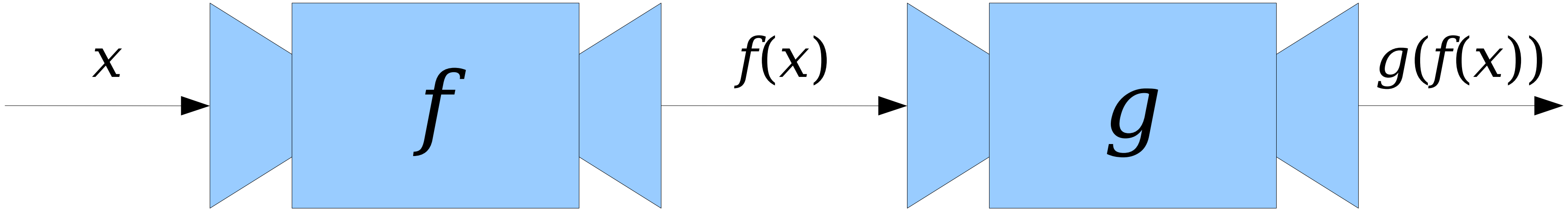
1. Assume f is an involution.
2. Pick arbitrary $a_1, a_2 \in A$ such that $a_1 \neq a_2$.
3. Prove $f(a_1) \neq f(a_2)$.

Function Composition


f : People → Places
g : Places → Prices
Keith
Meredith
Siyan
Grant
Drew
Cupertino, CA
San Francisco
Redding, CA
Utqiagvik, AK
Palo Alto, CA
Far Too Much
A King's Ransom
A Modest Amount
More Than You'd Expect
People
Places
Prices
h : People → Prices
h(x) = g(f(x))

Function Composition

- Suppose that we have two functions $f : A \to B$ and $g : B \to C$.
- Notice that the codomain of f is the domain of g. This means that we can use outputs from f as inputs to g.



Function Composition

- Suppose that we have two functions $f : A \to B$ and $g : B \to C$.
- The ***composition of f and g***, denoted $\boldsymbol{g \circ f}$, is a function where
  - $g \circ f : A \to C$, and
  - $(g \circ f)(x) = g(f(x))$.

> The name of the function is $g \circ f$. When we apply it to an input x, we write $(g \circ f)(x)$. I don't know why, but that's what we do.

- A few things to notice:
  - The domain of $g \circ f$ is the domain of f. Its codomain is the codomain of g.
  - Even though the composition is written $g \circ f$, when evaluating $(g \circ f)(x)$, the function f is evaluated first.

Properties of Composition

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

Organizing Our Thoughts

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming	***What We Need to Prove***
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$	

We need to *prove* this universally-quantified statement. So let's introduce arbitrarily-chosen values.

We're *assuming* these universally-quantified statements, so we won't introduce any variables for what's here.

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming	***What We Need to Prove***
$f : A \to B$ is an injection. $\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$ $g : B \to C$ is an injection. $\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$ $a_1 \in A$ is arbitrarily-chosen. $a_2 \in A$ is arbitrarily-chosen.	$g \circ f$ is an injection. $\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$ We need to prove this universally-quantified statement. So let's introduce arbitrarily-chosen values.

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming	***What We Need to Prove***
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	
$a_1 \neq a_2$	

Now we're looking at an implication. Let's *assume* the antecedent and *prove* the consequent.

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming

$f : A \to B$ is an injection.

$\forall x \in A.\ \forall y \in A.\ (x \neq y \to$
$f(x) \neq f(y)$
$)$

$g : B \to C$ is an injection.

$\forall x \in B.\ \forall y \in B.\ (x \neq y \to$
$g(x) \neq g(y)$
$)$

$a_1 \in A$ is arbitrarily-chosen.

$a_2 \in A$ is arbitrarily-chosen.

$a_1 \neq a_2$

What We Need to Prove

$g \circ f$ is an injection.

$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to$
$(g \circ f)(a_1) \neq (g \circ f)(a_2)$
$)$

Let's write this out separately and simplify things a bit.

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

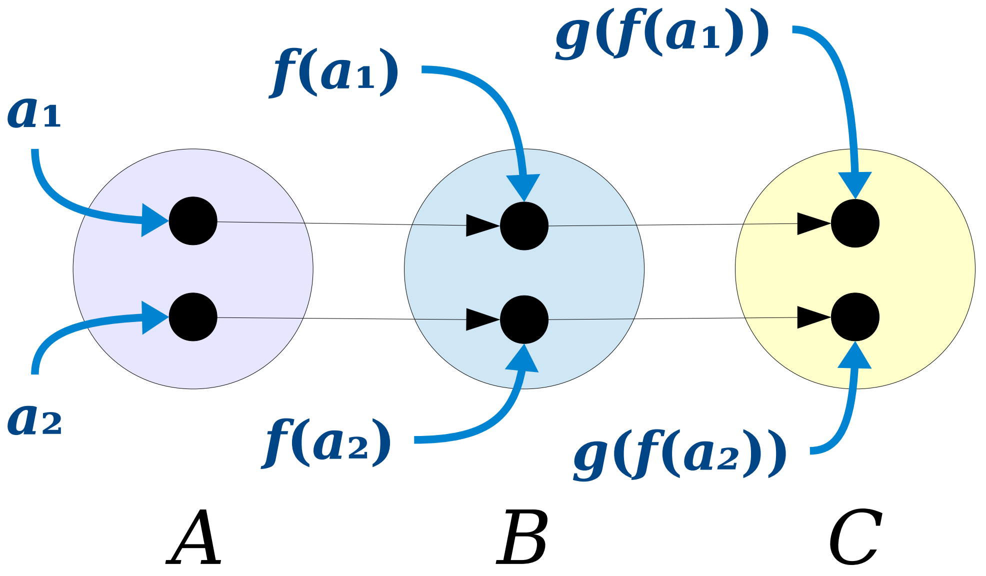
What We're Assuming	**What We Need to Prove**
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	$(g \circ f)(a_1) \neq (g \circ f)(a_2)$
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	
$a_1 \neq a_2$	

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

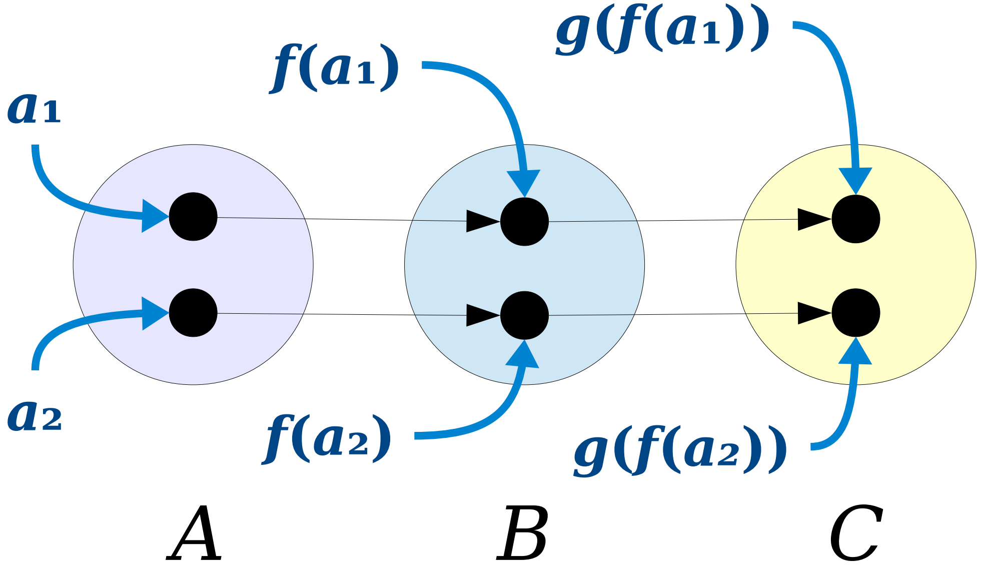
What We're Assuming	What We Need to Prove
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	$g(f(a_1)) \neq g(f(a_2))$
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	
$a_1 \neq a_2$	

Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is an injection.

What We're Assuming	What We Need to Prove
$f : A \to B$ is an injection.	$g \circ f$ is an injection.
$\forall x \in A.\ \forall y \in A.\ (x \neq y \to f(x) \neq f(y))$	$\forall a_1 \in A.\ \forall a_2 \in A.\ (a_1 \neq a_2 \to (g \circ f)(a_1) \neq (g \circ f)(a_2))$
$g : B \to C$ is an injection.	$g(f(a_1)) \neq g(f(a_2))$
$\forall x \in B.\ \forall y \in B.\ (x \neq y \to g(x) \neq g(y))$	
$a_1 \in A$ is arbitrarily-chosen.	
$a_2 \in A$ is arbitrarily-chosen.	
$a_1 \neq a_2$	

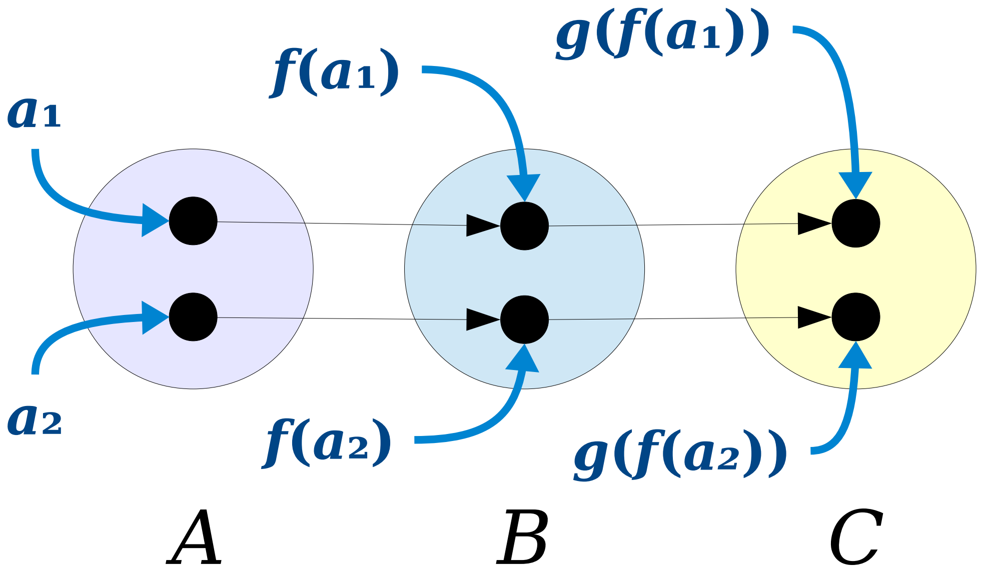


Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.



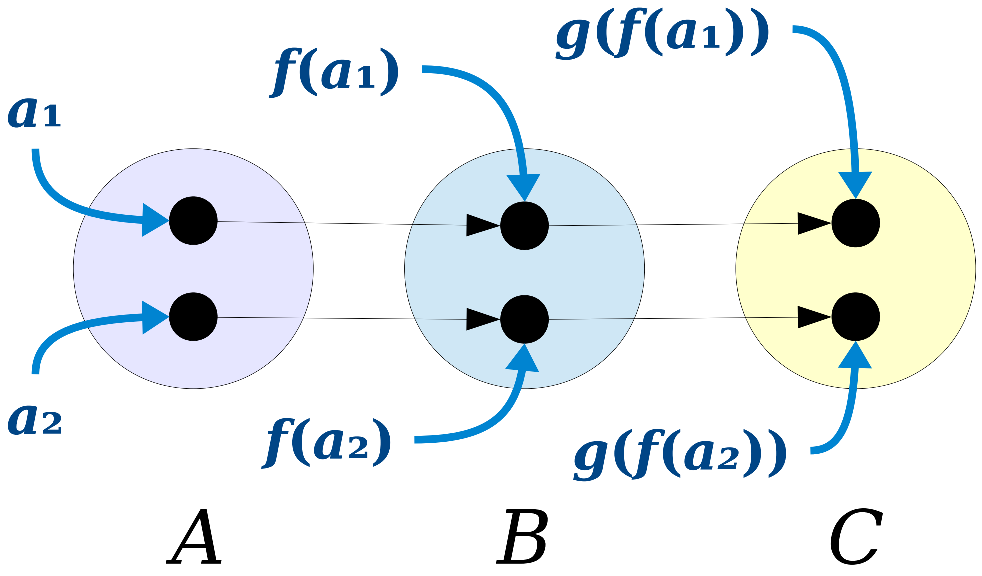
Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof:



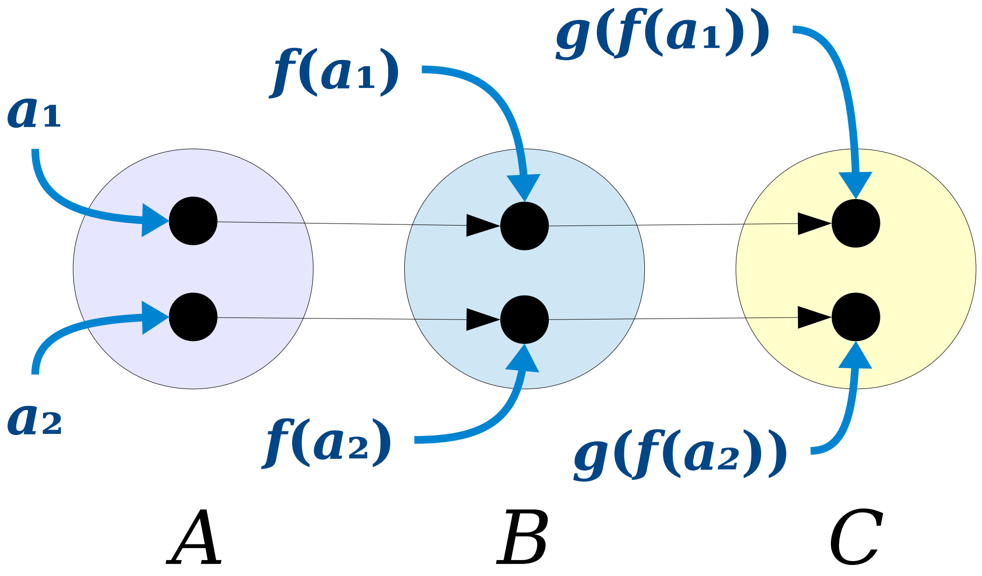
Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections.



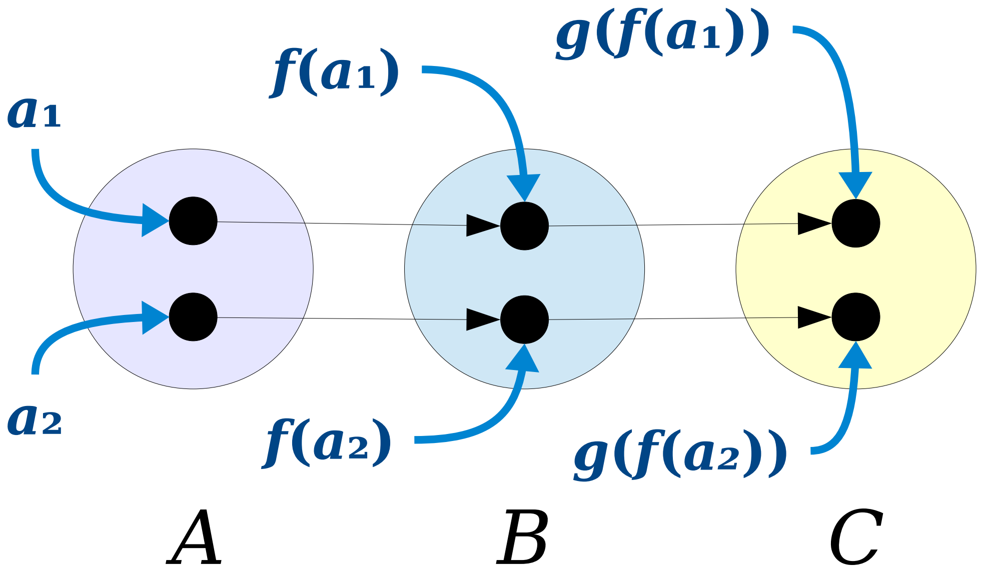
Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective.



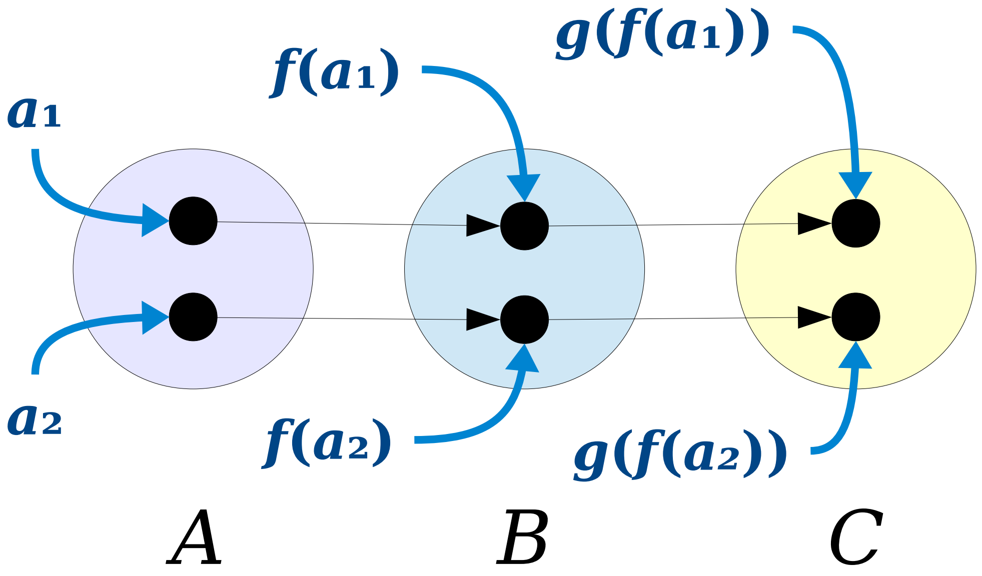
Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$.



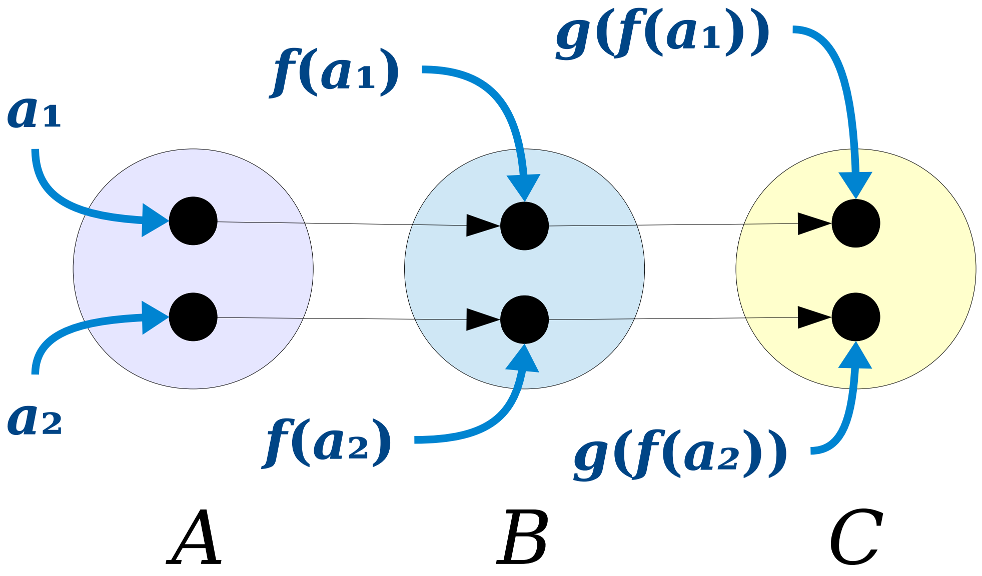
Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$.



Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

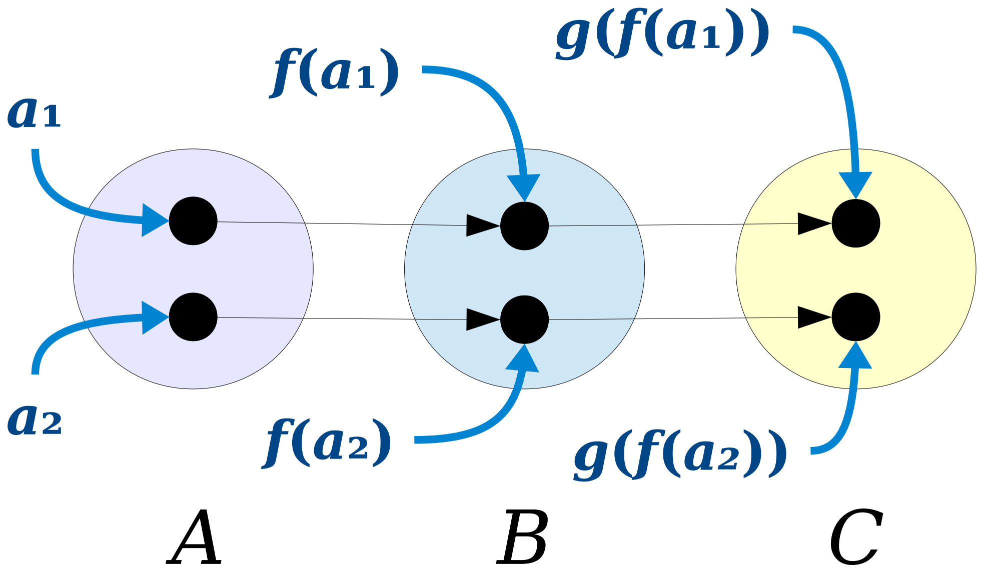
Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Equivalently, we need to show that $g(f(a_1)) \neq g(f(a_2))$.



Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Equivalently, we need to show that $g(f(a_1)) \neq g(f(a_2))$.

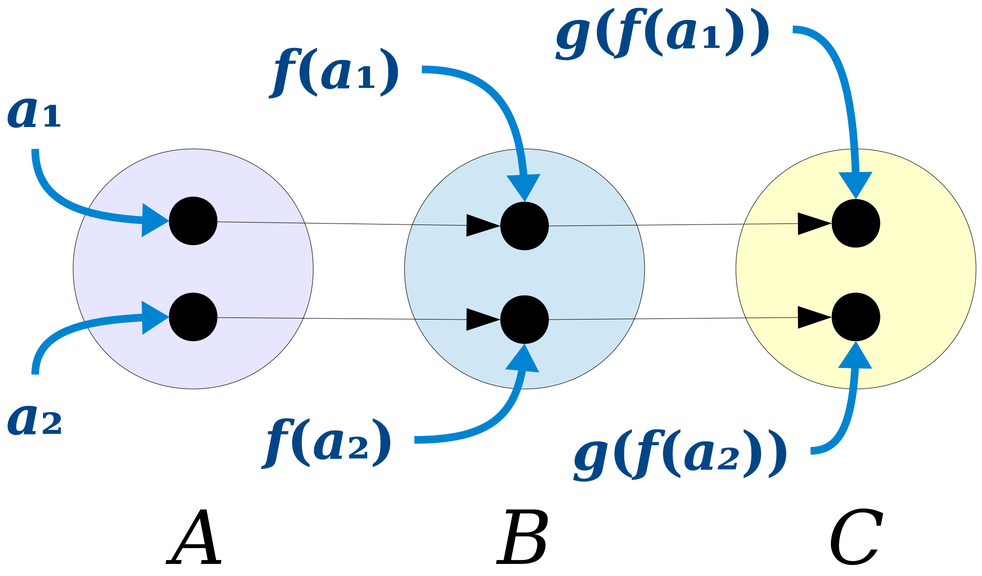
Since f is injective and $a_1 \neq a_2$, we see that $f(a_1) \neq f(a_2)$.



Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Equivalently, we need to show that $g(f(a_1)) \neq g(f(a_2))$.

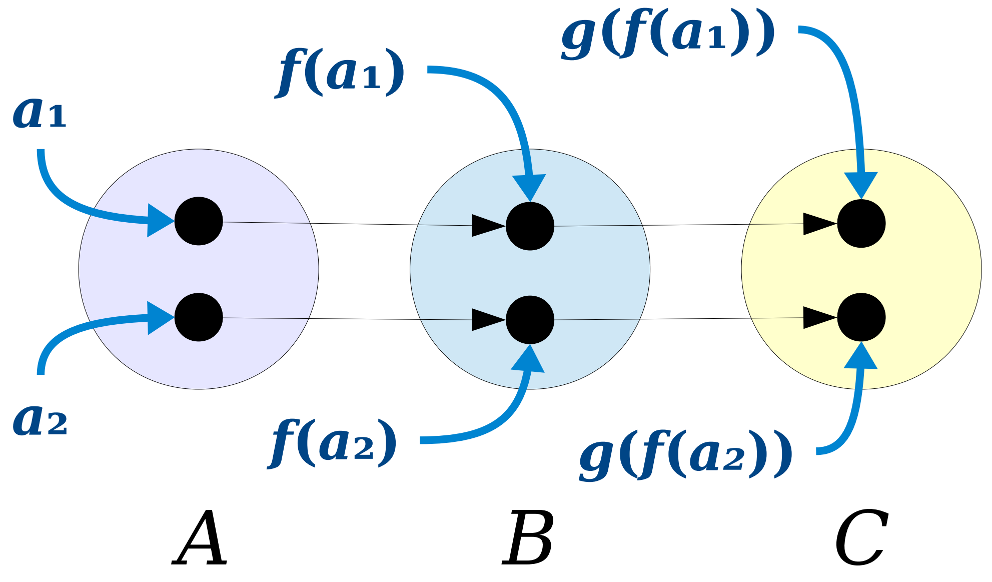
Since f is injective and $a_1 \neq a_2$, we see that $f(a_1) \neq f(a_2)$. Then, since g is injective and $f(a_1) \neq f(a_2)$, we see that $g(f(a_1)) \neq g(f(a_2))$, as required.



Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Equivalently, we need to show that $g(f(a_1)) \neq g(f(a_2))$.

Since f is injective and $a_1 \neq a_2$, we see that $f(a_1) \neq f(a_2)$. Then, since g is injective and $f(a_1) \neq f(a_2)$, we see that $g(f(a_1)) \neq g(f(a_2))$, as required. ■

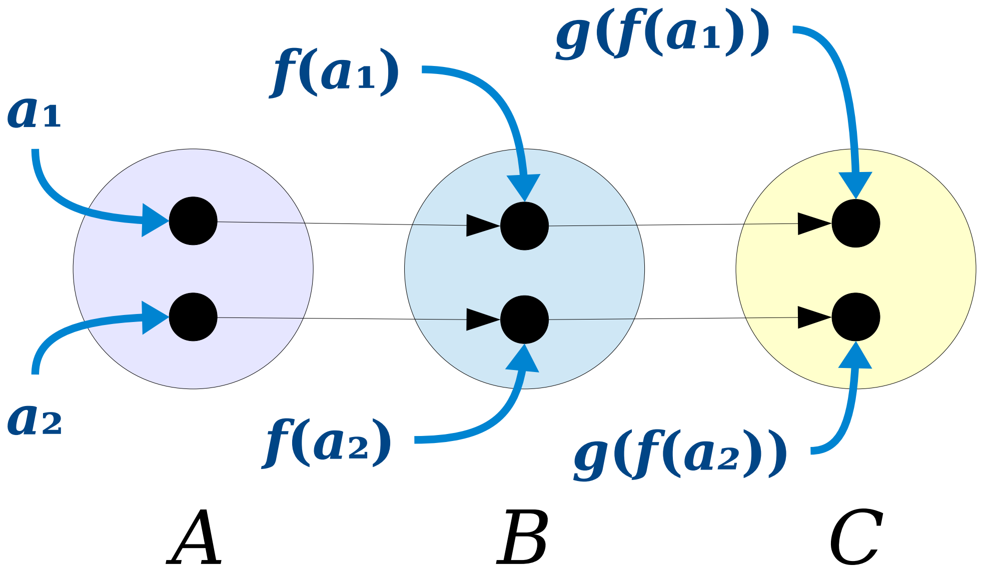


Theorem: If $f : A \to B$ is an injection and $g : B \to C$ is an injection, then the function $g \circ f : A \to C$ is also an injection.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary injections. We will prove that the function $g \circ f : A \to C$ is also injective. To do so, consider any $a_1, a_2 \in A$ where $a_1 \neq a_2$. We will prove that $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Equivalently, we need to show that $g(f(a_1)) \neq g(f(a_2))$.

Since f is injective and $a_1 \neq a_2$, we see that $f(a_1) \neq f(a_2)$. Then, since g is injective and $f(a_1) \neq f(a_2)$, we see that $g(f(a_1)) \neq g(f(a_2))$, as required. ■

Great exercise: Repeat this proof using the other definition of injectivity.



Major Ideas From Today

- Statements behave differently based on whether you're ***assuming*** or ***proving*** them.
- When you ***assume*** a universally-quantified statement, initially, do nothing. Instead, keep an eye out for a place to apply the statement more specifically.
- When you ***prove*** a universally-quantified statement, pick an arbitrary value and try to prove it has the needed property.
- As always: try concrete examples, draw pictures, etc. before you dive into writing a proof.

	To ***prove*** that this is true…	If you ***assume*** this is true…
$\forall x.\ A$	Have the reader pick an arbitrary x. We then prove A is true for that choice of x.	Initially, ***do nothing***. Once you find a z through other means, you can state it has property A.
$\exists x.\ A$	Find an x where A is true. Then prove that A is true for that specific choice of x.	Introduce a variable x into your proof that has property A.
$A \to B$	Assume A is true, then prove B is true.	Initially, ***do nothing***. Once you know A is true, you can conclude B is also true.
$A \land B$	Prove A. Then prove B.	Assume A. Then assume B.
$A \lor B$	Either prove $\neg A \to B$ or prove $\neg B \to A$. *(Why does this work?)*	Consider two cases. Case 1: A is true. Case 2: B is true.
$A \leftrightarrow B$	Prove $A \to B$ and $B \to A$.	Assume $A \to B$ and $B \to A$.
$\neg A$	Simplify the negation, then consult this table on the result.	Simplify the negation, then consult this table on the result.

Next Time

- ***Cardinality Revisited***
  - Formalizing our definitions.
- ***The Nature of Infinity***
  - Infinity is more interesting than it looks!
- ***Cantor's Theorem Revisited***
  - Formally proving a major result.

Extra Slides

(The following is a proof of a theorem just like the one we just did with injection, but with surjection.)

Theorem: If $f : A \to B$ is a surjection and $g : B \to C$ is a surjection, then the function $g \circ f : A \to C$ is a surjection.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof:

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective.

What does it mean for $g \circ f : A \to C$ to be surjective?

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective.

What does it mean for $g \circ f : A \to C$ to be surjective?

$$\forall c \in C.\ \exists a \in A.\ (g \circ f)(a) = c$$

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective.

What does it mean for $g \circ f : A \to C$ to be surjective?

$$\forall c \in C.\ \exists a \in A.\ (g \circ f)(a) = c$$

Therefore, we'll choose an arbitrary $c \in C$ and prove that there is some $a \in A$ such that $(g \circ f)(a) = c$.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective.

What does it mean for $g \circ f : A \to C$ to be surjective?

$$\forall c \in C.\ \exists a \in A.\ (g \circ f)(a) = c$$

Therefore, we'll choose an arbitrary $c \in C$ and prove that there is some $a \in A$ such that $(g \circ f)(a) = c$.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective.

What does it mean for $g \circ f : A \to C$ to be surjective?

$$\forall c \in C.\ \exists a \in A.\ (g \circ f)(a) = c$$

Therefore, we'll choose an arbitrary $c \in C$ and prove that there is some $a \in A$ such that $(g \circ f)(a) = c$.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective.

What does it mean for $g \circ f : A \to C$ to be surjective?

$$\forall c \in C.\ \exists a \in A.\ (g \circ f)(a) = c$$

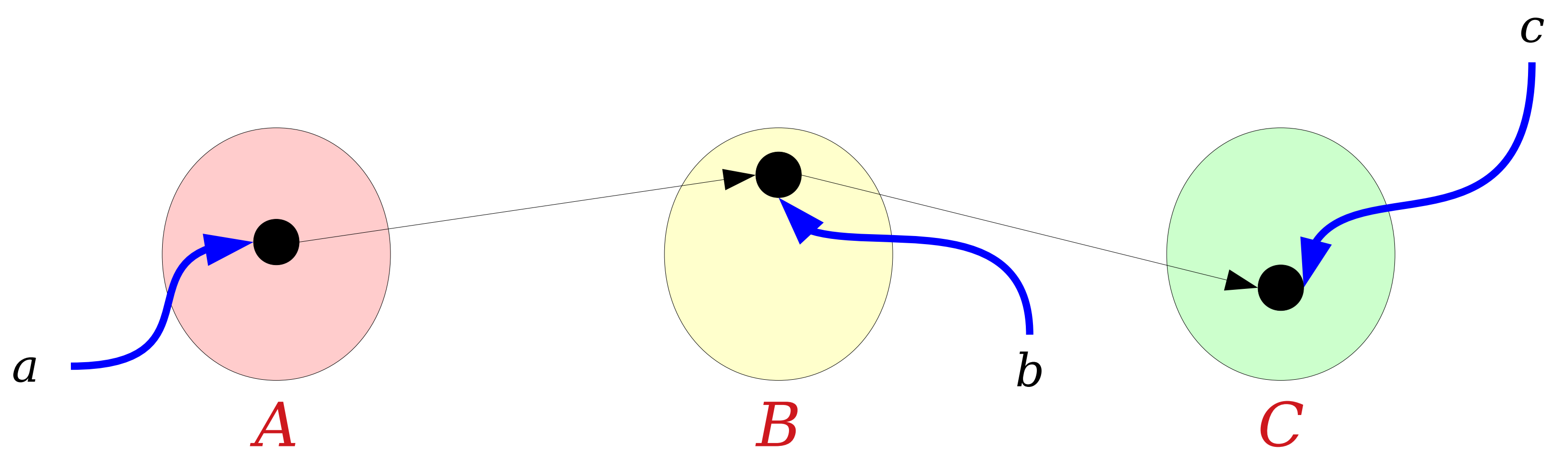
Therefore, we'll choose an arbitrary $c \in C$ and prove that there is some $a \in A$ such that $(g \circ f)(a) = c$.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$.

Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

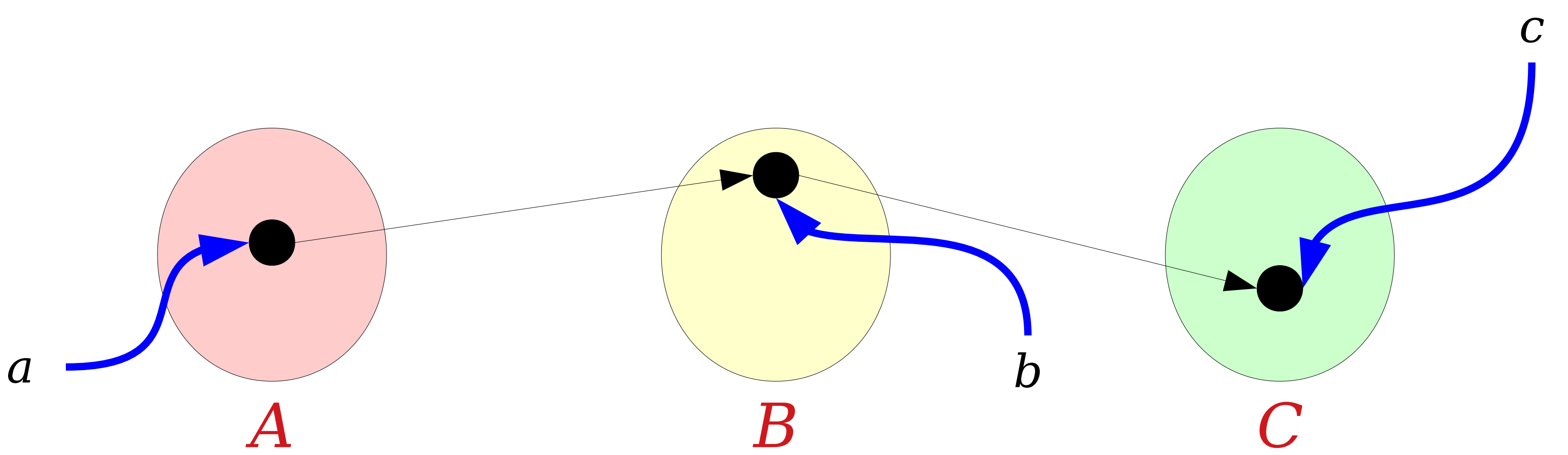
Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$. Equivalently, we will prove that for any $c \in C$, there is some $a \in A$ such that $g(f(a)) = c$.



Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$. Equivalently, we will prove that for any $c \in C$, there is some $a \in A$ such that $g(f(a)) = c$.

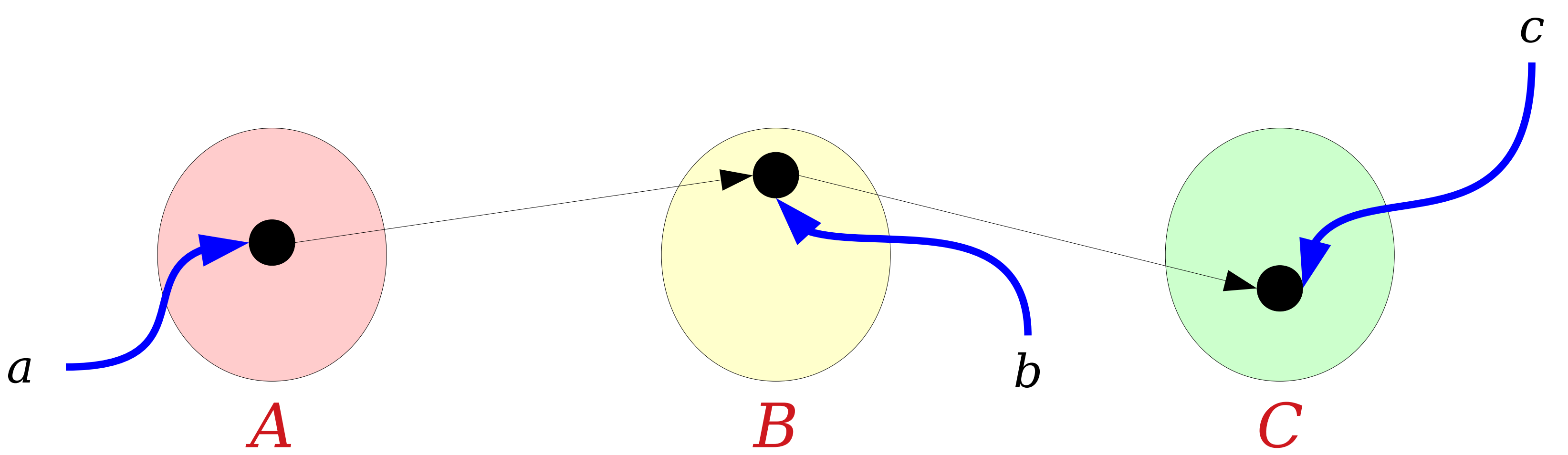
Consider any $c \in C$.



Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$. Equivalently, we will prove that for any $c \in C$, there is some $a \in A$ such that $g(f(a)) = c$.

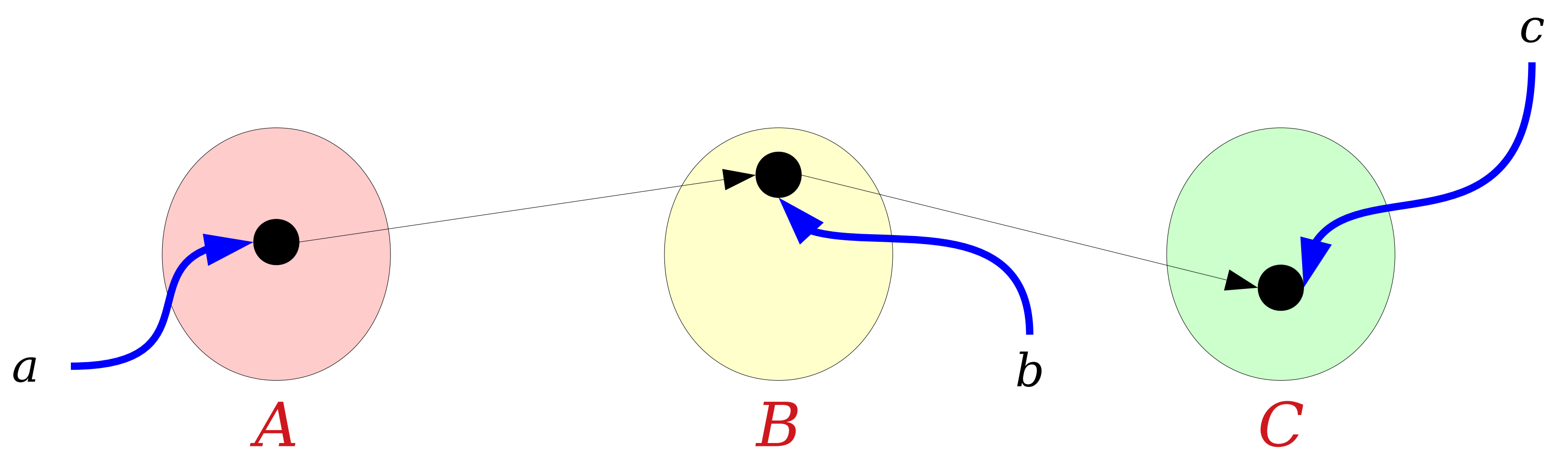
Consider any $c \in C$. Since $g : B \to C$ is surjective, there is some $b \in B$ such that $g(b) = c$.



Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$. Equivalently, we will prove that for any $c \in C$, there is some $a \in A$ such that $g(f(a)) = c$.

Consider any $c \in C$. Since $g : B \to C$ is surjective, there is some $b \in B$ such that $g(b) = c$. Similarly, since $f : A \to B$ is surjective, there is some $a \in A$ such that $f(a) = b$.



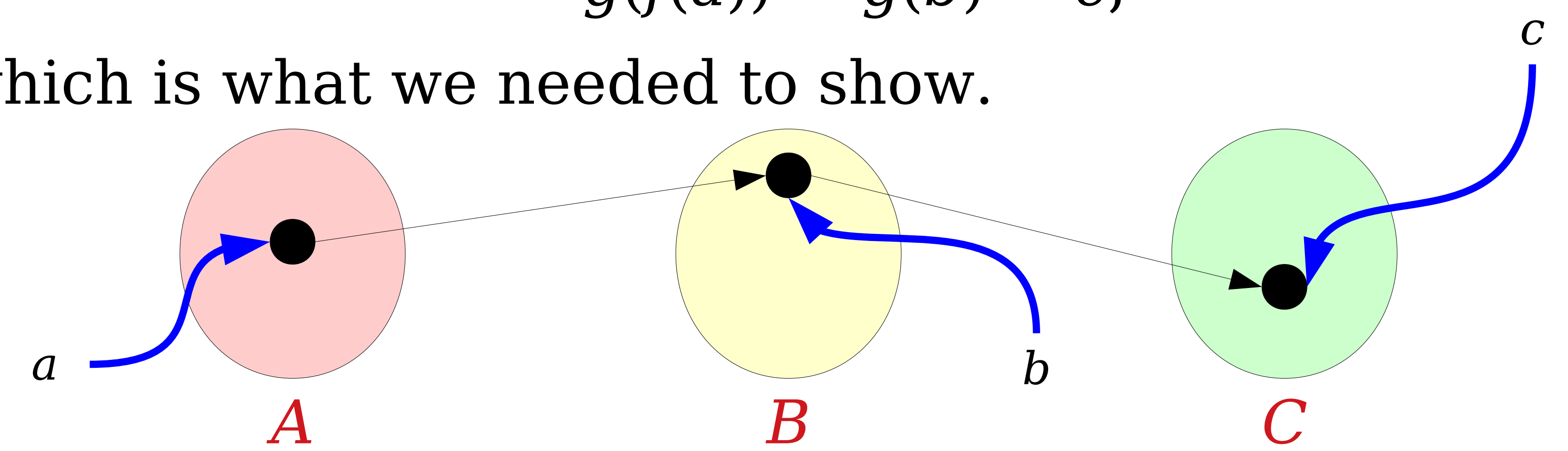
Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$. Equivalently, we will prove that for any $c \in C$, there is some $a \in A$ such that $g(f(a)) = c$.

Consider any $c \in C$. Since $g : B \to C$ is surjective, there is some $b \in B$ such that $g(b) = c$. Similarly, since $f : A \to B$ is surjective, there is some $a \in A$ such that $f(a) = b$. Then we see that

$$g(f(a)) = g(b) = c,$$

which is what we needed to show.



Theorem: If $f : A \to B$ is surjective and $g : B \to C$ is surjective, then $g \circ f : A \to C$ is also surjective.

Proof: Let $f : A \to B$ and $g : B \to C$ be arbitrary surjections. We will prove that the function $g \circ f : A \to C$ is also surjective. To do so, we will prove that for any $c \in C$, there is some $a \in A$ such that $(g \circ f)(a) = c$. Equivalently, we will prove that for any $c \in C$, there is some $a \in A$ such that $g(f(a)) = c$.

Consider any $c \in C$. Since $g : B \to C$ is surjective, there is some $b \in B$ such that $g(b) = c$. Similarly, since $f : A \to B$ is surjective, there is some $a \in A$ such that $f(a) = b$. Then we see that

$$g(f(a)) = g(b) = c,$$

which is what we needed to show. ■