Welcome to CS103A!

Turn in:

• Homework Problems 3

Pick up:

• Practice Problems 3
Binary Relations + Functions
Where We Are Now

- Our dive into discrete structures covered the following topics:
  - Binary relations.
  - Graphs of relations
  - Properties of relations: reflexivity, symmetry, transitivity, irreflexivity, asymmetry
  - Equivalence relations
  - Equivalence classes
  - Strict orders
  - First-order definitions
  - Functions
  - Domains and codomains
  - Injections, surjections, and bijections
  - Function composition
Reflexivity

∀a ∈ A. aRa
(“Every element is related to itself.”)
Reflexivity

To prove that a relation is reflexive, we pick an arbitrary element $a$ from $A$

$$\forall a \in A. \ aRa$$

(“Every element is related to itself.”)
Reflexivity

To prove that a relation is reflexive, we pick an arbitrary element \(a\) from \(A\).

\[
\forall a \in A. \ aRa
\]

(“Every element is related to itself.”)

And then we prove that \(aRa\) is true.
Reflexivity

\[ \forall a \in A. \ aRa \]

("Every element is related to itself.")
Reflexivity

This relation is reflexive because every element has a self-loop.

∀a ∈ A. aRa
(“Every element is related to itself.”)
Reflexivity

∀a ∈ A. aRa
(“Every element is related to itself.”)

This relation is still reflexive - reflexivity says nothing about whether any two elements are related to each other.
Reflexivity

∀a ∈ A. aRa

(“Every element is related to itself.”)

This isn’t reflexive anymore because this blue person isn’t related to themselves.
Reflexivity

You can have a reflexive relation with just one element though!

\( \forall a \in A. \ aRa \)

(“Every element is related to itself.”)
Reflexivity

∀a ∈ A. aRa

(“Every element is related to itself.”)
Symmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)
(“If a is related to b, then b is related to a.”)
Symmetry

To prove that a relation is symmetric, we pick arbitrary elements $a$ and $b$ from $A$.

$\forall a \in A. \forall b \in A. (aRb \rightarrow bRa)$

("If $a$ is related to $b$, then $b$ is related to $a")."
Symmetry

And we assume that $aRb$ is true.

To prove that a relation is symmetric, we pick arbitrary elements $a$ and $b$ from $A$.

$\forall a \in A. \forall b \in A. \ (aRb \rightarrow bRa)$

("If $a$ is related to $b$, then $b$ is related to $a$.")
Symmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)
(“If a is related to b, then b is related to a.”)

And we **assume** that aRb is true

To prove that a relation is symmetric, we **pick** arbitrary elements a and b from A

And then we **prove** that bRa is true

And we **assume** that aRb is true
Symmetry

\[ \forall a \in A. \ \forall b \in A. \ (aRb \rightarrow bRa) \]

("If a is related to b, then b is related to a.")
Symmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)

("If a is related to b, then b is related to a.")
Symmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)
("If a is related to b, then b is related to a.")

This is also symmetric – self-loops don’t break symmetry, do you see why?
Symmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)  
("If a is related to b, then b is related to a.")
Symmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)

("If a is related to b, then b is related to a.")

I can’t have something like this though, because blue is related to yellow but yellow isn’t related to blue.
Transitivity

\( \forall a \in A. \forall b \in A. \forall c \in A. (aRb \land bRc \rightarrow aRc) \)

("Whenever \( a \) is related to \( b \) and \( b \) is related to \( c \), we know \( a \) is related to \( c \).")
Transitivity

To prove that a relation is transitive, we pick arbitrary elements \(a, b,\) and \(c\) from \(A\)

\[\forall a \in A. \forall b \in A. \forall c \in A. (aRb \land bRc \rightarrow aRc)\]

(“Whenever \(a\) is related to \(b\) and \(b\) is related to \(c\), we know \(a\) is related to \(c\).”)
Transitivity

\[ \forall a \in A. \forall b \in A. \forall c \in A. \ (aRb \land bRc \rightarrow aRc) \]

(“Whenever a is related to b and b is related to c, we know a is related to c.

To prove that a relation is transitive, we pick arbitrary elements a, b, and c from A.

And we assume that aRb and bRc are true.)
Transitivity

\[ \forall a \in A. \forall b \in A. \forall c \in A. (aRb \land bRc \rightarrow aRc) \]

("Whenever \(a\) is related to \(b\) and \(b\) is related to \(c\), we know \(a\) is related to \(c\).")

To prove that a relation is transitive, we pick arbitrary elements \(a\), \(b\), and \(c\) from \(A\).

And we assume that \(aRb\) and \(bRc\) are true.

And then we prove that \(aRc\) is true.

∀a ∈ A. ∀b ∈ A. ∀c ∈ A. (aRb ∧ bRc → aRc)
Transitivity

∀a ∈ A. ∀b ∈ A. ∀c ∈ A. (aRb ∧ bRc → aRc)

(“Whenever a is related to b and b is related to c, we know a is related to c.”)
Transitivity

∀a ∈ A. ∀b ∈ A. ∀c ∈ A. (aRb ∧ bRc → aRc)

(“Whenever a is related to b and b is related to c, we know a is related to c.”)
∀a ∈ A. ∀b ∈ A. ∀c ∈ A. (aRb ∧ bRc → aRc)

("Whenever a is related to b and b is related to c, we know a is related to c.
Self-loops are fine here too!

Transitivity
Transitivity

\[ \forall a \in A. \forall b \in A. \forall c \in A. (aRb \land bRc \rightarrow aRc) \]

(“Whenever \(a\) is related to \(b\) and \(b\) is related to \(c\), we know \(a\) is related to \(c\).”)

This also works!
Transitivity

∀a ∈ A. ∀b ∈ A. ∀c ∈ A. (aRb ∧ bRc → aRc)

("Whenever a is related to b and b is related to c, we know a is related to c.

This is not transitive though – pink is related to yellow and yellow is related to pink, so pink should be related to itself.

∀a ∈ A. ∀b ∈ A. ∀c ∈ A. (aRb ∧ bRc → aRc)
Transitivity

\( \forall a \in A. \forall b \in A. \forall c \in A. (aRb \land bRc \rightarrow aRc) \)

(“Whenever \( a \) is related to \( b \) and \( b \) is related to \( c \), we know \( a \) is related to \( c \).”)
Irreflexivity

\[ \forall a \in A. \ aR\neg a \]
(“No element is related to itself.”)
Irreflexivity

To prove that a relation is irreflexive, we pick an arbitrary element $a$ from $A$:

$$\forall a \in A. \ aRa$$

(“No element is related to itself.”)
Irreflexivity

To prove that a relation is irreflexive, we pick an arbitrary element $a$ from $A$

And then we prove that $aRa$ is true

$$\forall a \in A. \ aRa$$

(“No element is related to itself.”)
Irreflexivity

\( \forall a \in A. \ a R a \)  
(“No element is related to itself.”)
Irreflexivity

∀a ∈ A. aRa

(“No element is related to itself.”)
Irreflexivity

This is still irreflexive - irreflexivity says nothing about whether any two elements are related to each other.

∀a ∈ A. aR̸a
(“No element is related to itself.”)
Irreflexivity

∀a ∈ A. aRa

(“No element is related to itself.”)
Asymmetry

\[ \forall a \in A. \forall b \in A. (aRb \to bRa) \]

(“If a relates to b, then b does not relate to a.”)
To prove that a relation is asymmetric, we pick arbitrary elements $a$ and $b$ from $A$.

$$\forall a \in A. \forall b \in A. (aRb \rightarrow bRa)$$

(“If $a$ relates to $b$, then $b$ does not relate to $a$.”)
Asymmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)
("If a relates to b, then b does not relate to a.")

To prove that a relation is asymmetric, we pick arbitrary elements a and b from A.

And we assume that aRb is true
Asymmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)

("If a relates to b, then b does not relate to a.")
Asymmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)
("If a relates to b, then b does not relate to a.")
Asymmetry

\[ \forall a \in A. \forall b \in A. (aRb \rightarrow bRa) \]

(“If a relates to b, then b does not relate to a.”)
Asymmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)

("If a relates to b, then b does not relate to a.")
Asymmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)

("If a relates to b, then b does not relate to a.")
Asymmetry

∀a ∈ A. ∀b ∈ A. (aRb → bRa)

("If a relates to b, then b does not relate to a.")
Let’s do a practice problem together!
Let $R$ be a binary relation over a set $A$. We can define a new relation over $A$ called the *inverse relation of $R$*, denoted $R^{-1}$, as follows:

$$xR^{-1}y \quad \text{if} \quad yRx$$

Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$. 
Let $R$ be a binary relation over a set $A$. We can define a new relation over $A$ called the **inverse relation of $R$**, denoted $R^{-1}$, as follows:

$$xR^{-1}y \quad \text{if} \quad yRx$$

Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

Before we attempt the prove/disprove, it’s a good idea to **apply new definitions to a concrete example** and make sure we fully understand what the definition means.
Let $R$ be a binary relation over a set $A$. We can define a new relation over $A$ called the \textit{inverse relation of $R$}, denoted $R^{-1}$, as follows:

$$xR^{-1}y \quad \text{if} \quad yRx$$

Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

What is the inverse of the $<$ relation over $\mathbb{Z}$?

What is the inverse of the $=$ relation over $\mathbb{Z}$?

---

Discuss with your neighbors!
Let $R$ be a binary relation over a set $A$. We can define a new relation over $A$ called the **inverse relation of $R$**, denoted $R^{-1}$, as follows:

$$xR^{-1}y$$ if $$yRx$$

Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

What is the inverse of the $<$ relation over $\mathbb{Z}$?

*The inverse of the $<$ relation over $\mathbb{Z}$ is the $>$ relation over $\mathbb{Z}$. This is because $x < y$ happens precisely when $y > x$."

What is the inverse of the $=$ relation over $\mathbb{Z}$?

*The $=$ relation over $\mathbb{Z}$ is its own inverse. Note that $x = y$ happens precisely when $y = x$ happens.*
Let $R$ be a binary relation over a set $A$. We can define a new relation over $A$ called the inverse relation of $R$, denoted $R^{-1}$, as follows:

$$xR^{-1}y \quad \text{if} \quad yRx$$

Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

A good strategy for "prove or disprove" questions is to just try doing both a proof and a disproof.

If you find yourself having a hard time proving the claim, identifying why can often help you come up with a disproof and vice versa.
Let $R$ be a binary relation over a set $A$. We can define a new relation over $A$ called the \textit{inverse relation of $R$}, denoted $R^{-1}$, as follows:

$$xR^{-1}y \quad \text{if} \quad yRx$$

Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

How would you set up a proof of this claim?

How would you set up a disproof of this claim?

Discuss with your neighbors!
Let $R$ be a binary relation over a set $A$. We can define a new relation over $A$ called the **inverse relation of $R$**, denoted $R^{-1}$, as follows:

$$ xR^{-1}y \quad \text{if} \quad yRx $$

Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

How would you set up a proof of this claim?

*For an arbitrary relation $R$, assume that $R$ is an equivalence relation, then show that $R^{-1}$ also has to be an equivalence relation.*

How would you set up a disproof of this claim?

*Find a specific example of a relation $R$ such that $R$ is an equivalence relation but $R^{-1}$ is not.*
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

<table>
<thead>
<tr>
<th><strong>What We’re Assuming</strong></th>
<th><strong>What We Need To Show</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$ is an equivalence relation</td>
<td>$R^{-1}$ is an equivalence relation</td>
</tr>
</tbody>
</table>

**Relevant Definitions**

$xR^{-1}y$ if $yRx$
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

<table>
<thead>
<tr>
<th>What We’re Assuming</th>
<th>What We Need To Show</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R$ is an equivalence relation</td>
<td></td>
</tr>
<tr>
<td>- $R$ is reflexive</td>
<td></td>
</tr>
<tr>
<td>- $R$ is symmetric</td>
<td></td>
</tr>
<tr>
<td>- $R$ is transitive</td>
<td></td>
</tr>
<tr>
<td>$R^{-1}$ is an equivalence relation</td>
<td></td>
</tr>
<tr>
<td>- $R^{-1}$ is reflexive</td>
<td></td>
</tr>
<tr>
<td>- $R^{-1}$ is symmetric</td>
<td></td>
</tr>
<tr>
<td>- $R^{-1}$ is transitive</td>
<td></td>
</tr>
</tbody>
</table>

**Relevant Definitions**

$xR^{-1}y$ if $yRx$
Prove or disprove: if \( R \) is an equivalence relation over \( A \), then \( R^{-1} \) is an equivalence relation over \( A \).

A great proofwriting strategy is to **draw pictures** – it’s often easier to reason about concrete circles, lines, and arrows than abstract mathematical definitions.
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

We’ll use a red arrow to denote that $xRy$ and a blue arrow to denote that $xR^{-1}y$. 
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Assumptions:**

$R$ is reflexive

$\forall x \in A. \ xRx$

We can always draw a red self-loop
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Assumptions:**

$R$ is reflexive
\[ \forall x \in A. \ xRx \]

We can always draw a red self-loop

$R$ is symmetric
\[ \forall x \in A. \ \forall y \in A. \ (xRy \rightarrow yRx) \]

If there's a red arrow in one direction, we can draw one in the other direction
Prove or disprove: if \( R \) is an equivalence relation over \( A \), then \( R^{-1} \) is an equivalence relation over \( A \).

**Assumptions:**

\( R \) is reflexive
\[ \forall x \in A. \; xRx \]

We can always draw a red self-loop

\( R \) is symmetric
\[ \forall x \in A. \; \forall y \in A. \; (xRy \rightarrow yRx) \]

If there's a red arrow in one direction, we can draw one in the other direction

\( R \) is transitive
\[ \forall x \in A. \; \forall y \in A. \; \forall z \in A. \; (xRy \land yRz \rightarrow xRz) \]

If you can get somewhere by following red arrows, you can draw a red arrow directly there
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

$x R^{-1} y$ if $y R x$

When can we draw a blue arrow?
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

$xR^{-1}y$ if $yRx$

When can we draw a blue arrow?

If there’s a red arrow going one way

Then we can draw a blue arrow going the other way
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is reflexive

$\forall x \in A. \; x R^{-1} x$

We want to always be able to draw a blue self-loop
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is reflexive
\[ \forall x \in A. \ xR^{-1}x \]

Since we assumed $R$ is reflexive, we can put in this red self loop

We want to always be able to draw a blue self-loop
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is reflexive

$\forall x \in A. \ xR^{-1}x$

Since we assumed $R$ is reflexive, we can put in this red self loop.

Since there’s a red arrow going from $x$ to $x$, we can draw a blue arrow going “the other way”, from $x$ to $x$. 
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

Goal:

$R^{-1}$ is symmetric
$\forall x \in A. \forall y \in A. (xR^{-1}y \rightarrow yR^{-1}x)$

We want to say that if there’s a blue arrow in one direction, we can draw one in the other direction.
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is symmetric

$\forall x \in A. \forall y \in A.
(x R^{-1} y \rightarrow y R^{-1} x)$

So we’ll assume this arrow exists

And prove that this arrow exists too
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is symmetric

$$\forall x \in A. \forall y \in A. (xR^{-1}y \rightarrow yR^{-1}x)$$

So we'll assume this arrow exists

And prove that this arrow exists too

Remember that you can apply this definition

$xR^{-1}y$ if $yRx$ in the other direction too
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is symmetric

$\forall x \in A. \forall y \in A. (xR^{-1}y \rightarrow yR^{-1}x)$

Since there's a blue arrow from $x$ to $y$, we can draw a red arrow going the other way, from $y$ to $x$.
Prove or disprove: if \( R \) is an equivalence relation over \( A \), then \( R^{-1} \) is an equivalence relation over \( A \).

**Goal:**

\( R^{-1} \) is symmetric
\[ \forall x \in A. \forall y \in A. \quad (xR^{-1}y \rightarrow yR^{-1}x) \]

Since \( R \) is symmetric, we can use this arrow to draw a red arrow from \( x \) to \( y \).
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$xR^{-1}y$ if $yRx$

Finally, since we have a red arrow from $x$ to $y$, we can apply the definition of $R^{-1}$ again to conclude that there's a blue arrow from $y$ to $x$
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

Goal:

$R^{-1}$ is transitive
\[ \forall x \in A. \forall y \in A. \forall z \in A. \quad (x R^{-1} y \land y R^{-1} z \rightarrow x R^{-1} z) \]

We want to say that if we can get from $x$ to $z$ through an intermediary $y$, then we can draw an arrow straight from $x$ to $z$. 

\[ \begin{array}{c}
\text{y} \\
\text{x} \\
\text{z}
\end{array} \] 

\[ R \quad R^{-1} \]
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is transitive

$\forall x \in A. \forall y \in A. \forall z \in A. (xR^{-1}y \land yR^{-1}z \rightarrow xR^{-1}z)$

So we'll assume that these arrows exist

And prove that this arrow exists too
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is transitive
$\forall x \in A. \forall y \in A. \forall z \in A. \ (xR^{-1}y \land yR^{-1}z \rightarrow xR^{-1}z)$

We can apply the definition of $R^{-1}$ to draw these two red arrows.

\[ R \quad R^{-1} \]
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Goal:**

$R^{-1}$ is transitive

$\forall x \in A. \forall y \in A. \forall z \in A.
(xR^{-1}y \land yR^{-1}z \rightarrow xR^{-1}z)$

Then since $R$ is transitive, we can draw this arrow
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

Goal:

$R^{-1}$ is transitive

$\forall x \in A. \forall y \in A. \forall z \in A. \ (xR^{-1}y \land yR^{-1}z \rightarrow xR^{-1}z)$

Applying the definition of $R^{-1}$ again gives us the arrow we desire!
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

$R^{-1}$ is reflexive

1. $xRx$  
   ($R$ is reflexive)

2. $xR^{-1}x$  
   (definition of $R^{-1}$)
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$. 

**$R^{-1}$ is reflexive**

1. $xRx$ \hspace{2cm} (definition of $R^{-1}$)
2. $xR^{-1}x$ \hspace{2cm} (by assumption)

**$R^{-1}$ is symmetric**

1. $xR^{-1}y$ \hspace{2cm} (by assumption)
2. $yRx$ \hspace{2cm} (definition of $R^{-1}$)
3. $xRy$ \hspace{2cm} (definition of $R^{-1}$)
4. $yR^{-1}x$ \hspace{2cm} (definition of $R^{-1}$)
Prove or disprove: if $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

$R^{-1}$ is reflexive

1. $xRx$ ($R$ is reflexive)
2. $xR^{-1}x$ (definition of $R^{-1}$)

$R^{-1}$ is symmetric

1. $xR^{-1}y$ (by assumption)
2. $yRx$ (definition of $R^{-1}$)
3. $xRy$ ($R$ is symmetric)
4. $yR^{-1}x$ (definition of $R^{-1}$)

$R^{-1}$ is transitive

1. $xR^{-1}y$ and $yR^{-1}z$ (by assumption)
2. $yRx$ and $zRy$ (definition of $R^{-1}$)
3. $zRx$ ($R$ is transitive)
4. $xR^{-1}z$ (definition of $R^{-1}$)
**Theorem:** If $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Proof:** Let $R$ be an equivalence relation over a set $A$. We will prove that $R^{-1}$ is also an equivalence relation over $A$ by proving that $R^{-1}$ is reflexive, symmetric, and transitive.
**Theorem:** If \( R \) is an equivalence relation over \( A \), then \( R^{-1} \) is an equivalence relation over \( A \).

**Proof:** Let \( R \) be an equivalence relation over a set \( A \). We will prove that \( R^{-1} \) is also an equivalence relation over \( A \) by proving that \( R^{-1} \) is reflexive, symmetric, and transitive.

To prove that \( R^{-1} \) is reflexive, consider any \( x \in A \). We need to prove that \( xR^{-1}x \). By definition, this means that we need to prove that \( xRx \). Since \( R \) is reflexive, we know that \( xRx \) holds.
**Theorem:** If $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Proof:** Let $R$ be an equivalence relation over a set $A$. We will prove that $R^{-1}$ is also an equivalence relation over $A$ by proving that $R^{-1}$ is reflexive, symmetric, and transitive.

To prove that $R^{-1}$ is reflexive, consider any $x \in A$. We need to prove that $xR^{-1}x$. By definition, this means that we need to prove that $xRx$. Since $R$ is reflexive, we know that $xRx$ holds.

To prove that $R^{-1}$ is symmetric, consider any $x, y \in A$ where $xR^{-1}y$. We need to prove that $yR^{-1}x$ holds. Since $xR^{-1}y$ holds, we know that $yRx$ holds. Since $R$ is symmetric and $yRx$ is true, we know that $xRy$ is true. Therefore by definition of $R^{-1}$, we know that $yR^{-1}x$ holds.
**Theorem**: If $R$ is an equivalence relation over $A$, then $R^{-1}$ is an equivalence relation over $A$.

**Proof**: Let $R$ be an equivalence relation over a set $A$. We will prove that $R^{-1}$ is also an equivalence relation over $A$ by proving that $R^{-1}$ is reflexive, symmetric, and transitive.

To prove that $R^{-1}$ is reflexive, consider any $x \in A$. We need to prove that $xR^{-1}x$. By definition, this means that we need to prove that $xRx$. Since $R$ is reflexive, we know that $xRx$ holds.

To prove that $R^{-1}$ is symmetric, consider any $x, y \in A$ where $xR^{-1}y$. We need to prove that $yR^{-1}x$ holds. Since $xR^{-1}y$ holds, we know that $yRx$ holds. Since $R$ is symmetric and $yRx$ is true, we know that $xRy$ is true. Therefore by definition of $R^{-1}$, we know that $yR^{-1}x$ holds.

Finally, to prove that $R^{-1}$ is transitive, consider any $x, y, z \in A$ where $xR^{-1}y$ and $yR^{-1}z$. We need to prove that $xR^{-1}z$. Since $xR^{-1}y$ and $yR^{-1}z$, we know that $yRx$ and that $zRy$. Since $zRy$ and $yRx$, by transitivity of $R$ we see that $zRx$. Thus by definition of $R^{-1}$, we know that $xR^{-1}z$ holds, as required. ■
Injectivity

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

(“If the inputs are different, the outputs are different.”)
Injectivity

To prove that a function is injective, we pick arbitrary \( a_1 \) and \( a_2 \) from \( A \)

\[
\forall a_1 \in A. \forall a_2 \in A. \ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2))
\]

(“If the inputs are different, the outputs are different.”)
Injectivity

To prove that a function is injective, we pick arbitrary \( a_1 \) and \( a_2 \) from \( A \).

And we assume that \( a_1 \neq a_2 \).

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

(“If the inputs are different, the outputs are different.”)
Injectivity

To prove that a function is injective, we pick arbitrary $a_1$ and $a_2$ from $A$.

And we assume that $a_1 \neq a_2$.

And then we prove that $f(a_1) \neq f(a_2)$.

\[ \forall a_1 \in A. \forall a_2 \in A. \ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)) \]

("If the inputs are different, the outputs are different.")
Injectivity

\[\forall a_1 \in A. \forall a_2 \in A. (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2))\]

(“If the inputs are different, the outputs are different.”)
Injectivity

∀a₁ ∈ A. ∀a₂ ∈ A. (a₁ ≠ a₂ → f(a₁) ≠ f(a₂))
(“If the inputs are different, the outputs are different.”)

∀a₁ ∈ A. ∀a₂ ∈ A. (f(a₁) = f(a₂) → a₁ = a₂)
(“If the outputs are the same, the inputs are the same.”)
Injectivity

∀a₁ ∈ A. ∀a₂ ∈ A. (a₁ ≠ a₂ → f(a₁) ≠ f(a₂))

(“If the inputs are different, the outputs are different.”)

You can also pick arbitrary a₁ and a₂ from A

∀a₁ ∈ A. ∀a₂ ∈ A. (f(a₁) = f(a₂) → a₁ = a₂)

(“If the outputs are the same, the inputs are the same.”)
Injectivity

\[ \forall a_1 \in A. \forall a_2 \in A. (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)) \]

(“If the inputs are different, the outputs are different.”)

You can also pick arbitrary \(a_1\) and \(a_2\) from \(A\)

And assume that \(f(a_1) = f(a_2)\)

\[ \forall a_1 \in A. \forall a_2 \in A. (f(a_1) = f(a_2) \rightarrow a_1 = a_2) \]

(“If the outputs are the same, the inputs are the same.”)
Injectivity

\[ \forall a_1 \in A. \forall a_2 \in A. \ (a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)) \]

(“If the inputs are different, the outputs are different.”)

You can also pick arbitrary \( a_1 \) and \( a_2 \) from \( A \)

And assume that \( f(a_1) = f(a_2) \)

And then prove that \( a_1 = a_2 \)

\[ \forall a_1 \in A. \forall a_2 \in A. \ (f(a_1) = f(a_2) \rightarrow a_1 = a_2) \]

(“If the outputs are the same, the inputs are the same.”)
Injectivity

\[ \forall a_1 \in A. \forall a_2 \in A. \ (f(a_1) = f(a_2) \rightarrow a_1 = a_2) \]

(“If the outputs are the same, the inputs are the same.”)
Injectivity

\[ \forall a_1 \in A. \forall a_2 \in A. (f(a_1) = f(a_2) \rightarrow a_1 = a_2) \]

("If the outputs are the same, the inputs are the same.")

This function is not injective because there are two different inputs that map to the same output.
Injectivity

This function is injective because different inputs map to different outputs.

∀a₁ ∈ A. ∀a₂ ∈ A. (f(a₁) = f(a₂) → a₁ = a₂)

("If the outputs are the same, the inputs are the same.")
Injectivity

This is not a function, because you cannot have the same input mapping to more than one output.

∀a₁ ∈ A. ∀a₂ ∈ A. (f(a₁) = f(a₂) → a₁ = a₂)

(“If the outputs are the same, the inputs are the same.”)
Surjective Functions

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

("For every possible output, there's at least one possible input that produces it")
Surjective Functions

To prove that a function is injective, we pick arbitrary $b$ from $B$.

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

(“For every possible output, there's at least one possible input that produces it”)
Surjective Functions

To prove that a function is injective, we pick arbitrary b from B.

And then prove that there exists and a in A such that f(a) = b.

∀b ∈ B. ∃a ∈ A. f(a) = b

(“For every possible output, there's at least one possible input that produces it”)
Surjective Functions

∀b ∈ B. ∃a ∈ A. f(a) = b

(“For every possible output, there's at least one possible input that produces it”)
Surjective Functions

This function is surjective because every output is covered by some input.

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

(“For every possible output, there's at least one possible input that produces it”)
Surjective Functions

∀b ∈ B. ∃a ∈ A. f(a) = b

(“For every possible output, there's at least one possible input that produces it”)

This function is not surjective because there is an output that is not mapped to by any input.
Surjective Functions

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

("For every possible output, there's at least one possible input that produces it")

This is not a function because there is an input that does not map to any output.
Let’s do another practice problem together!
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

Let’s **apply new definitions to a concrete example** again to make sure we fully understand what the definition means.
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

Give three different examples of involutions from $\mathbb{Z}$ to $\mathbb{Z}$.

Discuss with your neighbors!
A function \( f : A \to A \) is called an **involution** if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.

Give three different examples of involutions from \( \mathbb{Z} \) to \( \mathbb{Z} \).

*Here are three involutions from \( \mathbb{Z} \) to \( \mathbb{Z} \):*

1. \( f(x) = x \). Then \( f(f(x)) = f(x) = x \)
2. \( f(x) = -x \). Then \( f(f(x)) = f(-x) = -(-x) = x \)
3. \( f(x) = \begin{cases} 
  x+1 & \text{if } x \text{ is even} \\
  x-1 & \text{if } x \text{ is odd}
\end{cases} \)
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

Now let's **draw some pictures** to try and develop an intuitive feel for why this result is true.
A function \( f : A \rightarrow A \) is called an \textbf{involution} if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.

This function is defined from some set \( A \) to itself, so we can draw that like this.
A function \( f : A \to A \) is called an **involution** if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

This function is defined from some set $A$ to itself, so we can draw that like this.

![Diagram of a function from set A to itself]
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

This definition says: if we take some element $x$, apply $f$, and then apply $f$ again, we should get back $x$. 

**Domain**

**Codomain**
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**This definition says:** if we take some element $x$, apply $f$, and then apply $f$ again, we should get back $x$. 

**Domain**

**Codomain**
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

This definition says: if we take some element $x$, apply $f$, and then apply $f$ again, we should get back $x$. 

![Diagram showing an involution function](image)
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

This definition says: if we take some element $x$, apply $f$, and then apply $f$ again, we should get back $x$. 

\[ f(x) \]
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

Now we need to explain why a function with this property must necessarily be a bijection. What do we need to show?
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 1: Injectivity**

\[
\forall a_1 \in A. \forall a_2 \in A. \ (f(a_1) = f(a_2) \rightarrow a_1 = a_2)
\]

(“If the outputs are the same, the inputs are the same.”)
A function \( f : A \to A \) is called an **involution** if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a **bijection**.

**Part 1: Injectivity**

Pick arbitrary \( a_1 \) and \( a_2 \) from the domain.

\[
\forall a_1 \in A. \forall a_2 \in A. (f(a_1) = f(a_2) \rightarrow a_1 = a_2)
\]

("If the outputs are the same, the inputs are the same.")
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 1: Injectivity**

Pick arbitrary $a_1$ and $a_2$ from the domain $A$.

Assume that $f(a_1) = f(a_2)$.

\[ \forall a_1 \in A. \forall a_2 \in A. \ (f(a_1) = f(a_2) \rightarrow a_1 = a_2) \]

(“If the outputs are the same, the inputs are the same.”)
A function \( f : A \to A \) is called an **involution** if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.

**Part 1: Injectivity**

Pick arbitrary \( a_1 \) and \( a_2 \) from the domain

Prove that \( a_1 = a_2 \)

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

(“If the outputs are the same, the inputs are the same.”)
A function \( f : A \to A \) is called an \textit{involution} if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a \textit{bijection}.

\begin{center}
\textbf{Part 1: Injectivity}
\end{center}

\[
\forall a_1 \in A. \ \forall a_2 \in A. \ (f(a_1) = f(a_2) \to a_1 = a_2)
\]

(“If the outputs are the same, the inputs are the same.”)
A function $f : A \to A$ is called an involutio**n**n if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 1: Injectivity**

\[ \forall a_1 \in A. \forall a_2 \in A. (f(a_1) = f(a_2) \rightarrow a_1 = a_2) \]

(“If the outputs are the same, the inputs are the same.”)
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 1: Injectivity**

What happens when we apply $f$ to this input?

\[ \forall a_1 \in A. \forall a_2 \in A. \ (f(a_1) = f(a_2) \to a_1 = a_2) \]

("If the outputs are the same, the inputs are the same.")
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 1: Injectivity**

\[ \forall a_1 \in A. \forall a_2 \in A. (f(a_1) = f(a_2) \rightarrow a_1 = a_2) \]

("If the outputs are the same, the inputs are the same.")
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a **bijection**.

**Part 1: Injectivity**

What happens when we apply $f$ to this input?

∀$a_1 \in A$. ∀$a_2 \in A$. ($f(a_1) = f(a_2) \rightarrow a_1 = a_2$)

(“If the outputs are the same, the inputs are the same.”)
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 1: Injectivity**

Let $a_1, a_2 \in A$. If $f(a_1) = f(a_2)$, then $a_1 = a_2$.

(“If the outputs are the same, the inputs are the same.”)
A function \( f : A \to A \) is called an \textit{involution} if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.

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

(“For every possible output, there's at least one possible input that produces it”)

Part 2: Surjectivity
A function \( f : A \rightarrow A \) is called an **involution** if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.

**Part 2: Surjectivity**

Pick arbitrary \( b \) from the codomain

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

(“For every possible output, there’s at least one possible input that produces it”)

\[
\text{Pick arbitrary } b \text{ from the codomain}
\]

\[
\forall b \in B. \exists a \in A. f(a) = b
\]
A function $f : A \rightarrow A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 2: Surjectivity**

Pick arbitrary $b$ from the codomain

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

(“For every possible output, there's at least one possible input that produces it”)

Prove that there exists an $a$ in the domain that maps to $b$
A function \( f : A \to A \) is called an **involution** if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.

**Part 2: Surjectivity**

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

(“For every possible output, there's at least one possible input that produces it”)
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 2: Surjectivity**

For every possible output, there's at least one possible input that produces it.
A function \( f : A \to A \) is called an **involution** if \( f(f(x)) = x \) for all \( x \in A \). Prove that if \( f \) is an involution, then \( f \) is a bijection.

**Part 2: Surjectivity**

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

(“For every possible output, there's at least one possible input that produces it”)
A function $f : A \to A$ is called an **involution** if $f(f(x)) = x$ for all $x \in A$. Prove that if $f$ is an involution, then $f$ is a bijection.

**Part 2: Surjectivity**

For every possible output, there's at least one possible input that produces it.

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

(“For every possible output, there's at least one possible input that produces it”)

- What happens when we apply $f$ to this input?
- What happens when we apply $f$ to this input?
Theorem: If $f : A \to A$ is an involution, then $f$ is a bijection.
**Theorem:** If if $f : A \to A$ is an involution, then $f$ is a bijection.

**Proof:** Let $f : A \to A$ be an involution. We will prove that $f$ is a bijection by proving that it's both injective and surjective.
**Theorem:** If if $f : A \rightarrow A$ is an involution, then $f$ is a bijection.

**Proof:** Let $f : A \rightarrow A$ be an involution. We will prove that $f$ is a bijection by proving that it's both injective and surjective.

To prove that $f$ is injective, consider any arbitrary $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$. We will prove that $a_1 = a_2$. To see this, start with $f(a_1) = f(a_2)$ and apply $f$ to both sides of this equality. This tells us that $f(f(a_1)) = f(f(a_2))$. Since $f$ is an involution, we know that $f(f(a_1)) = a_1$ and also that $f(f(a_2)) = a_2$, so we conclude that $a_1 = a_2$, as required.
**Theorem:** If if $f : A \to A$ is an involution, then $f$ is a bijection.

**Proof:** Let $f : A \to A$ be an involution. We will prove that $f$ is a bijection by proving that it's both injective and surjective.

To prove that $f$ is injective, consider any arbitrary $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$. We will prove that $a_1 = a_2$. To see this, start with $f(a_1) = f(a_2)$ and apply $f$ to both sides of this equality. This tells us that $f(f(a_1)) = f(f(a_2))$. Since $f$ is an involution, we know that $f(f(a_1)) = a_1$ and also that $f(f(a_2)) = a_2$, so we conclude that $a_1 = a_2$, as required.

To prove that $f$ is surjective, consider any $b \in A$. We need to show that there is some $a \in A$ such that $f(a) = b$. To do so, let $a = f(b)$. Then, since $f$ is an involution, we see that $f(a) = f(f(b)) = b$, as required. ■
**Theorem:** If $f : A \rightarrow A$ is an involution, then $f$ is a bijection.

**Proof:** Let $f : A \rightarrow A$ be an involution. We will prove that $f$ is a bijection by proving that it's both injective and surjective.

To prove that $f$ is injective, consider any arbitrary $a_1, a_2 \in A$ where $f(a_1) = f(a_2)$. We will prove that $a_1 = a_2$. To see this, start with $f(a_1) = f(a_2)$ and apply $f$ to both sides of this equality. This tells us that $f(f(a_1)) = f(f(a_2))$. Since $f$ is an involution, we know that $f(f(a_1)) = a_1$ and also that $f(f(a_2)) = a_2$, so we conclude that $a_1 = a_2$, as required.

To prove that $f$ is surjective, consider any $b \in A$. We need to show that there is some $a \in A$ such that $f(a) = b$. To do so, let $a = f(b)$. Then, since $f$ is an involution, we see that $f(a) = f(f(b)) = b$, as required. ■

Which parts of this proof don't work if $f$ is not an involution?
Before You Leave...

Turn in:

• Attendance Problems 3

Pick up:

• Homework Problems 4
• Attendance Problems 4
• Solutions to Practice Problems 3