Week 6: Sets and Functions (2.1 - 2.3)

Goal: Revisit familiar concepts with more precision through the lens of logic and proof.

- These concepts will be the foundation for more complicated structures.
- These concepts are great testbeds for proof writing.

I) Sets   II) Functions

I) Sets

Defn: A set is an unordered collection of objects which are called its elements. A set contains its elements.

- $x \in A$ denotes that "x is an element of A"
- $x \notin A$ denotes that "x is not an element of A"

Ex: $A = \{1, 2, 3, \text{Erfan}\}$
$= \{1, \text{Erfan}, 3, 2\}$

$1 \in A$ $\quad$ $\text{Erfan} \in A$ $\quad$ $4 \notin A$

Ex: $\mathbb{Z}$ = Set of all integers
$\mathbb{R}$ = Set of real numbers
$\mathbb{Z}_{>0}$ = Set of positive integers

Q: Is $A = \{1, 1, 2, 3\}$ a set?

A: No. It's multiset. A set is merely defined by elements it contain.

Two Ways To Specify Sets

1) **Roster Notation:** Just list the elements

e.g., $B = \{apple, Orange\}$ $\quad C = \{1, 2, 3, \ldots, 10\}$

implicit Pattern

2) **Set-builder Notation:** Define sets with proposition function: $A = \{x : P(x)\}$ ← The Collection of all x such that $P(x)$

such that

$even(x): \exists k\,(k > 0 \land x = 2k)$

$E = \{x : even(x)\}$

Domain is implicit

$= \{x \in \mathbb{Z} : even(x)\}$

$odd(x):$

$O = \{x : odd(x)\}$

$= \{x \in \mathbb{Z} : odd(x)\}$

$C = \{x \in \mathbb{Z} : 1 \leq x \leq 10\}$

Remark: Sometimes you see set specifications of an infinite set by listing first few elements

e.g., $E = \{2, 4, 6, \dots\}$

You may see this type of specification a lot in future, but we/you avoid it for now.

Remark: We used the notion of object in definition of set without specifying what an object is. This is how Cantor described sets (i.e., based on intuitive understanding of objects). This naive definition leads to paradox.

Remark: In this course, naive definition is enough for us since all sets we consider can be treated consistently using Cantor's original theory.

In Case You Are Interested, This Is Russel's paradox

Consider the set $A = \{x : x \notin x\}$.

Q: Is $A \in A$?

- If $A \in A$. by defn of A, $A \in A$, which is a contradiction.

- If $A \notin A$, by defn of A, $A \in A$, which is a contradiction.

So $A \in A$ is neither true nor false, i.e., not a proposition. These inconsistencies can be avoided by building set theory beginning with axioms.

Axiomatic Set Theory.

Using Set Notation with Quantifiers

Now that you know proper set notation, you can use quantified statement with restricted domain (you can use it after the Term Test 1)

e.g., $\forall x \in S\,(P(x))$ denote the universal quantification of $P(x)$ over all elements in the set S.

$$\forall x \in S\,(P(x)) \equiv \forall x\,(x \in S \rightarrow P(x))$$

$$\exists x \in S\,(P(x)) \equiv \exists x\,(x \in S \wedge P(x))$$

Equality and Containment

Defn: Set A is equal to set B if they have the same elements

$$\forall A \forall B \left(A = B \longleftrightarrow \forall x\,(x \in A \longleftrightarrow x \in B)\right)$$

e.g., $\{x \in \mathbb{Z}_{>0} : \text{even}(x)\} = \{x \in \mathbb{Z}_{>0} : \neg\,\text{odd}(x)\}$

Defn: A set A is a subset of a set B if every element of A is an element of B

$$A \subseteq B \longleftrightarrow \forall x\,(x \in A \longrightarrow x \in B) \xrightarrow{\text{or}} \forall x \in A\,(x \in B)$$

$\subseteq$: is a subset of

e.g., $\mathbb{Z}_{>0} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{R}$,

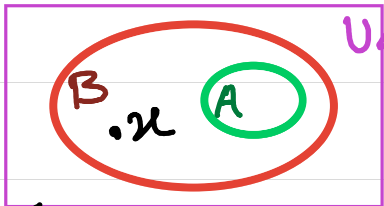
$\mathbb{R} \nsubseteq \mathbb{Z}$, since $\neg \forall x\,(x \in A \longrightarrow x \in B)$

$\equiv \exists x\,(x \in A \wedge x \notin B)$

$\nsubseteq$: is not a subset of

Consider $x = 1/2$. observe that $x \in A$ but $x \notin B$

Equality and Containment



universal set which contains all elements under consideration

Venn Diagram

In this Venn diagram,

$x \in B$, $x \notin A$

$A \subseteq B$; $B \not\subseteq A$

Remark: If A is a set, $A \subseteq A$

Remark: $A = B \longleftrightarrow A \subseteq B \wedge B \subseteq A$

Defn: The set with no element is called the *empty set* denoted by $\emptyset = \{\ \}$. $\{\emptyset\} \neq \emptyset$

Remark: For any set A, $\emptyset \subseteq A$ $\{\{\}\} \neq \{\ \}$

$\forall x\,(x \in \emptyset \to x \in A)$

Remark: $\subseteq$ is not the same as $\in$.

e.g., $2 \in \{1, 2, 3\}$ $\qquad$ $2 \not\subseteq \{1, 2, 3\}$ (2 is not even a set)

$\{2\} \notin \{1, 2, 3\}$ $\qquad$ $\{2\} \subseteq \{1, 2, 3\}$

$\{2\} \in \{1, 2, \{2\}, 3\}$ $\qquad$ $\{2\} \subseteq \{1, 2, \{2\}, 3\}$

Size of a finite Set

Defn: Let S be a set. If there are exactly n distinct elements in S where n is a non-negative integer, we say that S is a finite set an that n is the cardinality of S, denoted by $|S|$.

Defn: A set is said to be infinite if it's not finite.

e.g., $A = \{1, 2, 3\}$ $\quad |A| = 3 \qquad |\emptyset| = 0$

$\mathbb{Z}$ is an infinite set.

Power Set

Defn: The power set of set A is the set of all subset of A, denoted by

$$\mathcal{P}(A) = \{ S : S \subseteq A \}$$

e.g., $\mathcal{P}(\emptyset) = \{\emptyset\}$ $\qquad$ $\mathcal{P}(\{1,2\}) = \{\{1\}, \{2\}, \{1,2\}, \emptyset\}$

Remark: If A has n elements, $\mathcal{P}(A)$ has 2^n elements. (we will prove this later)

$$|\mathcal{P}(A)| = 2^n$$

Prop 1: For any set A and B, if $A=B$, then $\mathcal{P}(A)=\mathcal{P}(B)$

Proof: Assume arbitrary sets A and B.

Assume $A=B$. We will show that $\mathcal{P}(A)\subseteq\mathcal{P}(B)$ and $\mathcal{P}(A)\supseteq\mathcal{P}(B)$.

($\subseteq$): Consider arbitrary $x\in\mathcal{P}(A)$. Then, by definition, $x\subseteq A$. Since, $A=B$, we would have $x\subseteq B$. By definition, $x\in\mathcal{P}(B)$, as desired.

($\supseteq$): Identical proof, with roles of A and B reversed. $\square$

Prop 2: For any sets A and B, if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$.

Proof: Homework.

Cartesian Product

Defn: The Cartesian Product of sets A and B, denoted by $A \times B$, is the set of all ordered pairs (a,b), where $a \in A$ and $b \in B$.

$(a,b) \neq (b,a)$

$$A \times B = \{(a,b) : a \in A \wedge b \in B\}$$

e.g., $A = \{1,2,3\}$ $B = \{a,b\}$ $A \times B = \{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}$

$$\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$$

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a,b) : a \in \mathbb{R} \wedge b \in \mathbb{R}\}$$

$$\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R} = \{(a_1,\ldots,a_n) : a_1 \in \mathbb{R} \wedge \cdots \wedge a_n \in \mathbb{R}\}$$

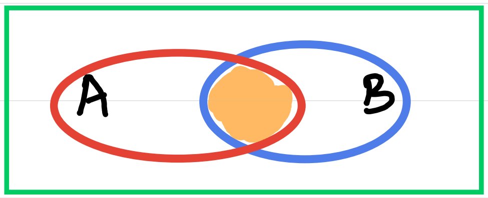
A = students in A67 B = Rock albums

$A \times B = \{(a,b) : a \in A \wedge b \in B\}$ $W = \{(a,b) \in A \times B : \text{"}a \text{ has listened } b\text{"}\}$

Operators on Sets (Corresponding to $\wedge, \vee, \neg$)

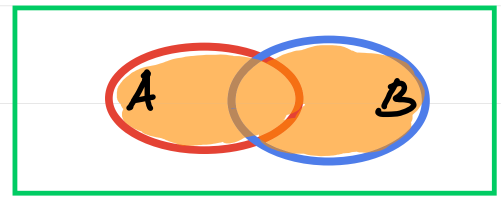
1) Intersection:

$$A \cap B = \{x : x \in A \wedge x \in B\}$$



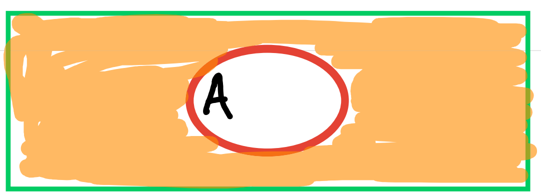
2) Union:

$$A \cup B = \{x : x \in A \vee x \in B\}$$



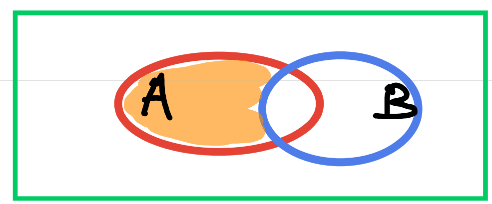
3) Complement (with respect to the universe V):

$$\overline{A} = \{x \in V : x \notin A\}$$



4) Set difference:

$$A - B = \{x \in A : x \notin B\}$$



Set Identities: Relation between sets that always hold.

e.g.,

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

$$A - B = A \cap \overline{B}$$

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Follow from deMorgan's Laws

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$$

Set Identities

Textbook, ch 2.2

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

as with equivalency laws and rules of inference, you don't need to remember the name of the Set Identities, But you shold know the identities themselves.

How to Prove That Two Sets are equal?

- by showing that each set is a subset of the other one. (we have seen examples of this method)

e.g., prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof: Assume arbitrary sets A and B. We prove the equality by showing that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ and $\overline{A \cap B} \supseteq \overline{A} \cup \overline{B}$.

($\subseteq$): Assume arbitrary object x. Assume $x \in \overline{A \cap B}$. By definition, $x \notin A \cap B$. By definition, $\neg(x \in A \wedge x \in B)$. By deMorgan's law, $\neg(x \in A) \vee \neg(x \in B)$. By definition, $(x \notin A) \vee (x \notin B)$. By definition, $(x \in \overline{A}) \vee (x \in \overline{B})$. By definition, $x \in (\overline{A} \cup \overline{B})$, as desired. Now you prove ($\supseteq$)

How to Prove That Two Sets are equal?

- by showing that each set is a subset of the other one. (We have seen examples of this method)

e.g., prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

We can do it more succinctly with set builder notation.

Proof: $\overline{A \cap B} = \{x : x \in \overline{A \cap B}\} = \{x : x \notin A \cap B\}$

$= \{x : \neg (x \in A \wedge x \in B)\} = \{x : \neg (x \in A) \vee \neg (x \in B)\}$

$= \{x : x \notin A \vee x \notin B\} = \{x : x \in \overline{A} \vee x \in \overline{B}\}$

$= \{x : x \in \overline{A} \cup \overline{B}\} = \overline{A} \cup \overline{B}.$ $\square$

How to Prove That Two Sets are equal?

- by using membership table. We consider each combination of the atomic sets. To indicate that an element is in a set, 1 is used, otherwise we use 0.

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

TABLE 2 A Membership Table for the Distributive Property.

A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

the two columns are the same

How to Prove That Two Sets are equal?

- by using the set identities to prove new ones.

Claim: $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$

Proof:

$$\overline{A \cup (B \cap C)} \underset{\text{by deMorgan}}{=} \overline{A} \cap \overline{(B \cap C)} \overset{\text{by demorgan}}{=} \overline{A} \cap (\overline{B} \cup \overline{C})$$

$$\overset{\text{by commutative}}{=} (\overline{B} \cup \overline{C}) \cap \overline{A}$$

$$\overset{\text{by commutative}}{=} (\overline{C} \cup \overline{B}) \cap \overline{A}$$

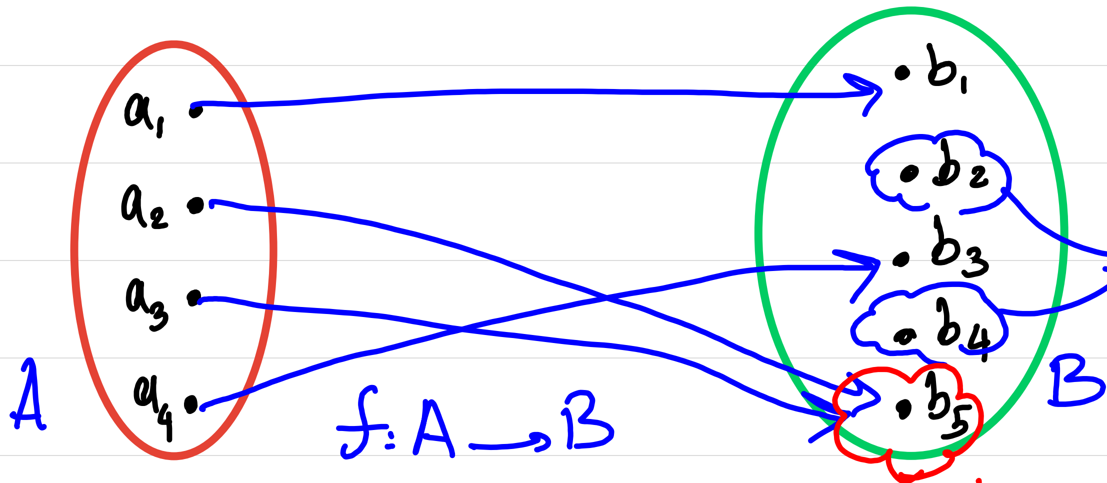
II) Functions

Defn: If A and B are sets, a function f from A to B is a role that assigns exactly one element of B to every element of A. The assignment is denoted by $f(a) = b$ for $a \in A$, $b \in B$.

f is written as $f: A \longrightarrow B$

domain "inputs"

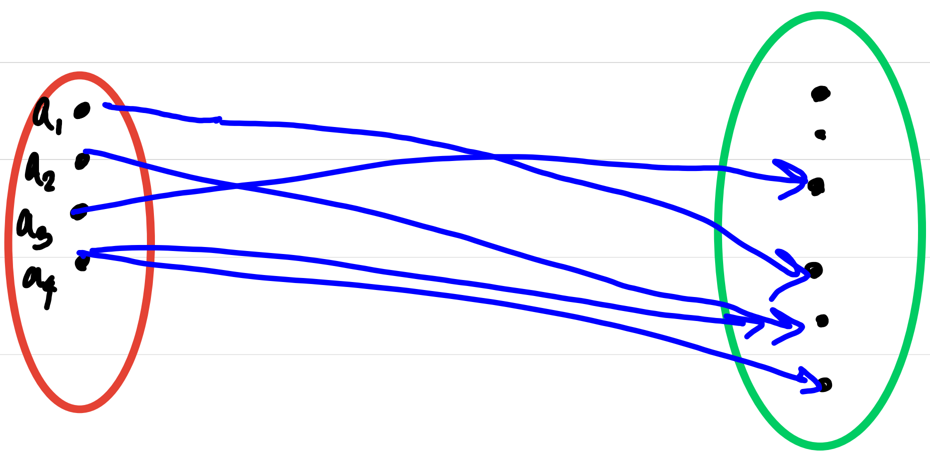
Co-domain "possible outputs"



$f(a_2) = b_5$

are not assigned to any element in A, and it's Completely fine.

b_5 is assigned to a_2 and a_3 and its perfectly fine.



NOT A Function!

e.g., $f: \mathbb{Z} \longrightarrow \mathbb{Z}$
by $f(x) = x^2$

e.g., $g: \mathbb{R} \longrightarrow \mathbb{R}_{\geq 0}$
by $g(x) = x^2$

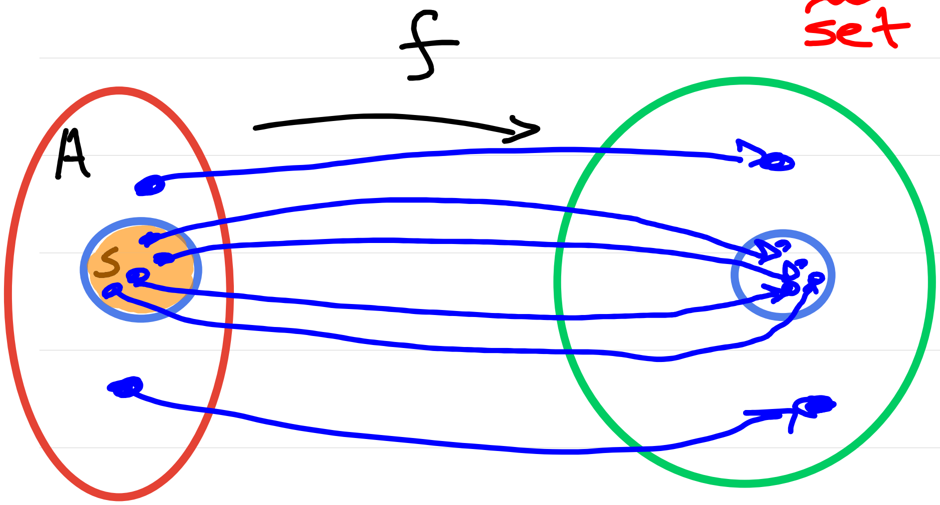
e.g., $h: \mathbb{R} \longrightarrow \mathbb{R}$
by $h(x) = e^x$

e.g., $v: A \longrightarrow \mathcal{P}(A)$
by $v(a) = \{a\}$

e.g., $m: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$
$m(a, b) = ab$

Defn: $f: A \to B$ is ==onto / Surjective== if
$\forall b \in B\ (\exists a \in A\ (f(a) = b))$

Defn: If $S \subseteq A$, the ==image of S== under f is defined as $f(\underbrace{S}_{\text{set}}) = \{ b \in B : \exists a \in S\ (f(a) = b)\}$
$= \{ f(a) : a \in S \}$



Note that $f(a) \neq f(\{a\})$

(f is onto iff $f(A) = B$)

Defn: Consider a function $f: A \to B$. $f(A)$ is called the range of f.
(f is onto iff range$(f) = B$)

e.g., $f: \mathbb{Z} \to \mathbb{Z}$ by $f(x) = x^2$

Surjective? NO

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

$\equiv \exists b \in B (\forall a \in A\ f(a) \neq b)$

Consider $b = -1$. Observe that for any $a \in \mathbb{Z}$, $a^2 \geq 0$ and cannot be equal to -1. $\square$

e.g., $g: \mathbb{R} \to \mathbb{R}_{\geq 0}$ by $g(x) = x^2$

Surjective? Yes

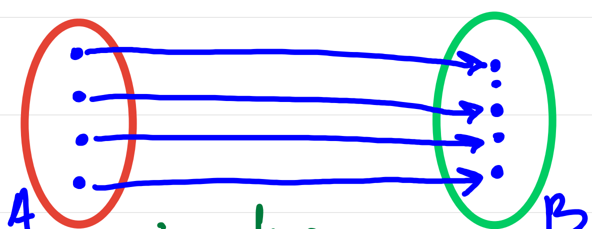
Assume arbitrary $b \in \mathbb{R}_{\geq 0}$. Choose $a = \sqrt{b}$. Observe that $\sqrt{b}$ is well defined for non-negative real numbers and $\sqrt{b} \in \mathbb{R}$. Observe that $(\sqrt{b})^2 = b$. $\square$

e.g., $h: \mathbb{R} \to \mathbb{R}$ by $h(x) = e^x$

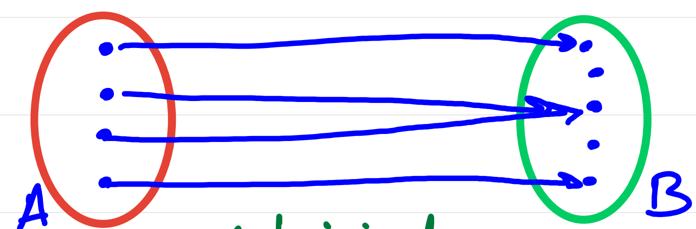
e.g., $v: A \to \mathcal{P}(A)$ by $v(a) = \{a\}$

e.g., $m: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ $m(a,b) = ab$

Defn: A function $f: A \to B$ is **one-to-one/injective** if $\forall a_1, a_2 \in A \ (f(a_1) = f(a_2) \longrightarrow a_1 = a_2)$ or equivalently $\forall a_1, a_2 \in A \ (a_1 \neq a_2 \longrightarrow f(a_1) \neq f(a_2))$



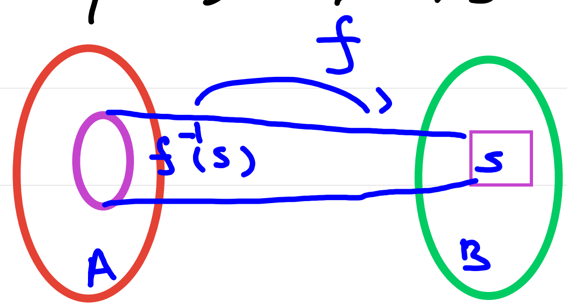
injective



Not injective

Defn: If $f: A \to B$ is a function an $S \subseteq B$, then the inverse image of S, denoted by $f^{-1}(S)$ is

$$f^{-1}(S) = \{a \in A : f(a) \in S\}$$



Remark: A function is onto if $f^{-1}(\{b\})$ has at least one element. (i.e., $f^{-1}(\{b\}) \neq \phi$)

Remark: A function is one-to-one if $f^{-1}(\{b\})$ has at most one element. (i.e., $|f^{-1}(\{b\})| \leq 1$)

e.g., $f: \mathbb{Z} \to \mathbb{Z}$
by $f(x) = x^2$

e.g., $g: \mathbb{R} \to \mathbb{R}_{\geq 0}$
by $g(x) = x^2$

e.g., $m: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$m(a,b) = ab$

e.g., $v: A \to \mathcal{P}(A)$
by $v(a) = \{a\}$

one-to-one? yes

e.g., $h: \mathbb{R} \to \mathbb{R}$
by $h(x) = e^x$

one-to-one. Yes.

Assume arbitrary $a_1 \in \mathbb{R}$ and $a_2 \in \mathbb{R}$. Assume $e^{a_1} = e^{a_2}$. Observe that

$$e^{a_1} = e^{a_2} \to \ln(e^{a_1}) = \ln(e^{a_2})$$
$$\to a_1 = a_2. \quad \square$$