

Discrete Algebraic Structures

WiSe 2025/2026

Prof. Dr. Antoine Wiehe
Research Group for Theoretical Computer Science



- Read the information sheet, many of your questions are answered there
- Sorry, it's not possible to make an exception "just for you"
- Starting this week: graded quiz in all the tutorials, the points count for the *Studienleistung*
- You don't submit solutions to the extra exercises given to you, this is only for practice.
But you can ask your tutor to have a look at your solution during the tutorial.

- Set: **unordered** bag of **distinct** things
- Notation: $\{1, 3, 4, 2\}$ is the set that contains 1, 3, 4, 2 and nothing else
- $x \in A$ means “ x is an element of A ”
- $B \subseteq A$ means “every element of B is an element of A ”
- Operations on sets:
 - $A \cup B$: **union**, set of elements contained in at least one of A or B
 - $A \cap B$: **intersection**, set of elements contained in both A and B
 - $A \setminus B$: **difference**, set of elements contained in A and not in B
 - $A \Delta B$: set of elements in exactly one of A and B
 - $A \times B$: set of **pairs** (a, b) with $a \in A$ and $b \in B$
 - $\mathcal{P}(A)$: set of **all subsets** of A

- Proof: sequence of basic instructions that shows how a **conclusion** follows from some **hypotheses**
- Writing a proof = writing a program
- Basic instruction:
 - applying a definition,
 - making a simple logical step (more on this next week),
 - applying a theorem (more on this later)
- A correct proof is a proof that is able to **convince**.
The best you can do for yourself: be **skeptical** of your own work (always ask “why?”)

Functions

Informally: a function from A to B is a recipe to transform an element of A into an element of B

```
def f(x: N) -> N:  
    y = 2*x+1  
    return y
```

```
def f2(x: N) -> Q:  
    y = x/2  
    return y
```

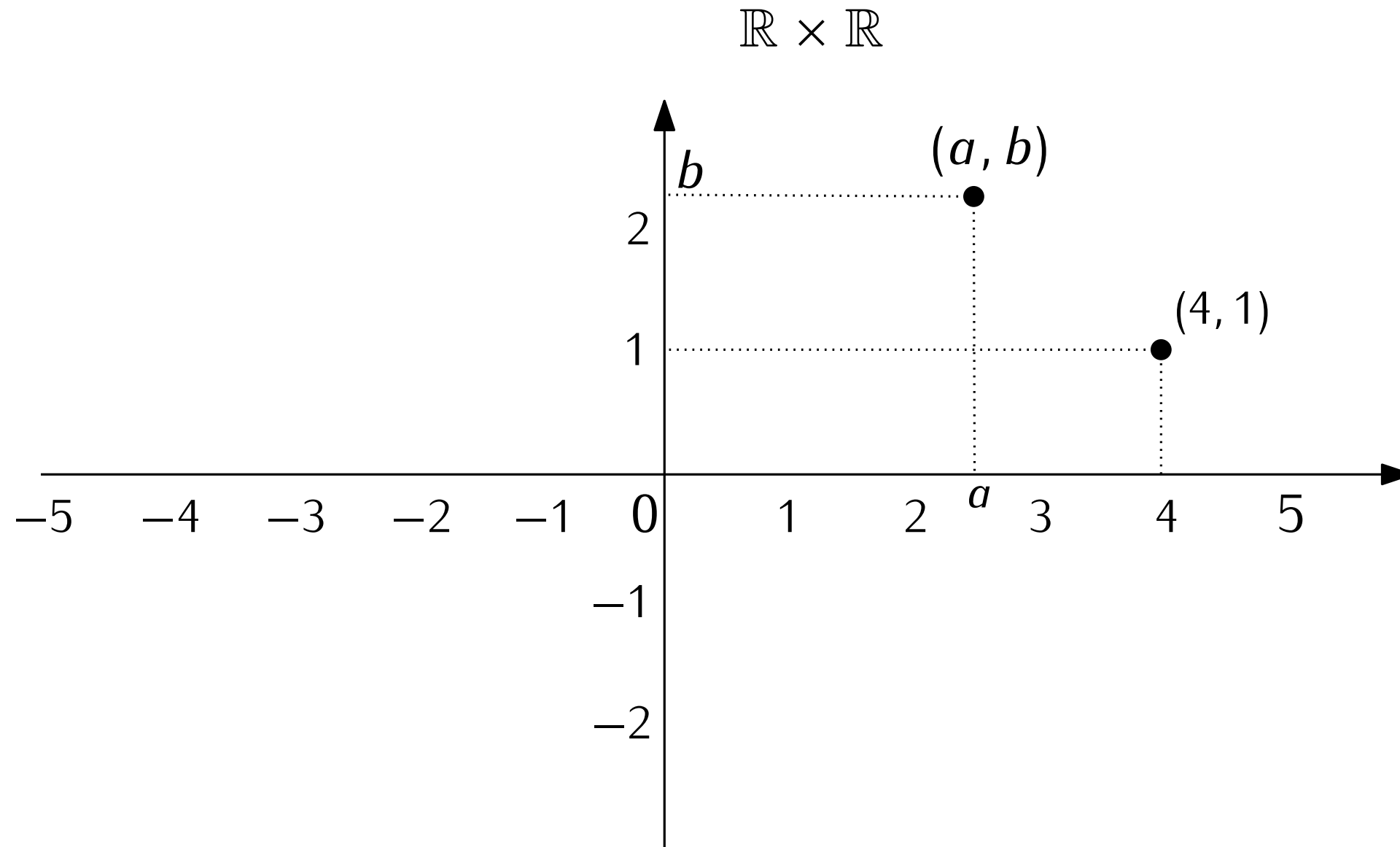
```
def g1(x: N) -> N:  
    y = 0  
    for i in {0,...,x}:  
        y = y + i  
    return y
```

```
def g2(x: N) -> N:  
    y = (x*(x+1))/2  
    return y
```

- Functions you already know from school (but not important here): $\cos$, $\sin$, $\exp$, ...
- The input set is called the **domain** of the function
- The output set is called the **codomain** of the function

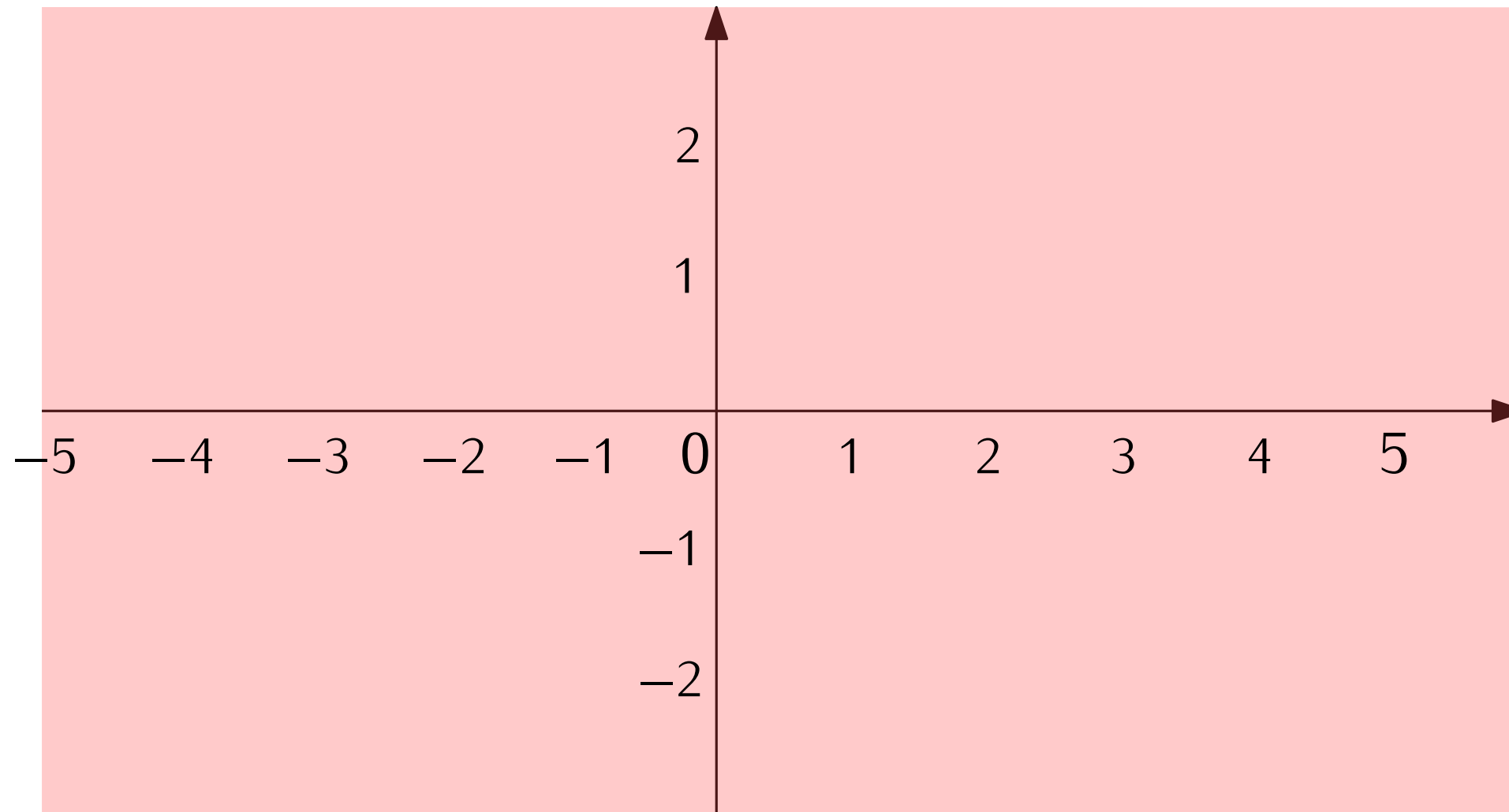
Notation. $f: A \rightarrow B$ means “ f is a function with domain A and codomain B ”.
 $f(a)$: output of the function on the input a

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.



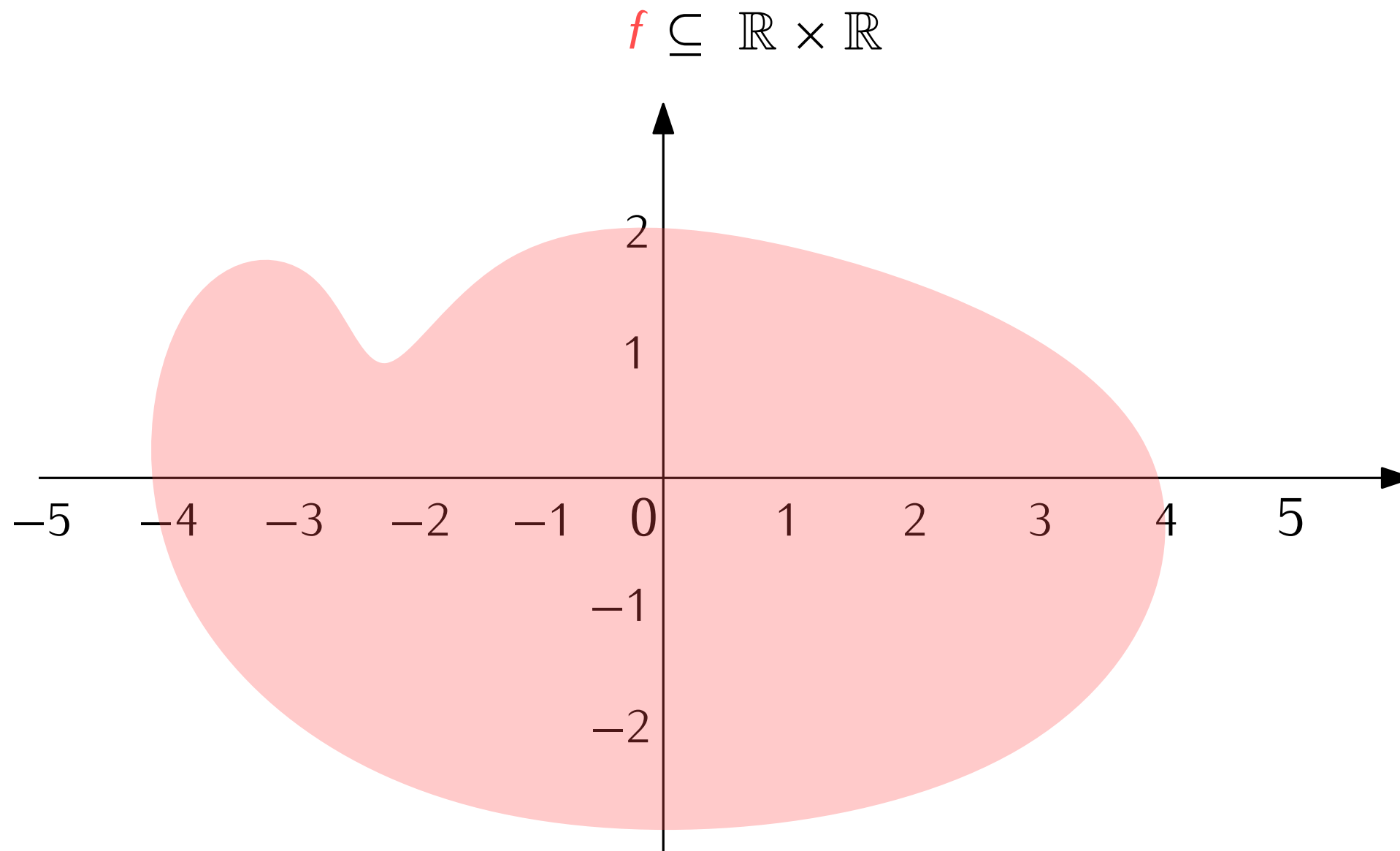
Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.

$$f \subseteq \mathbb{R} \times \mathbb{R}$$



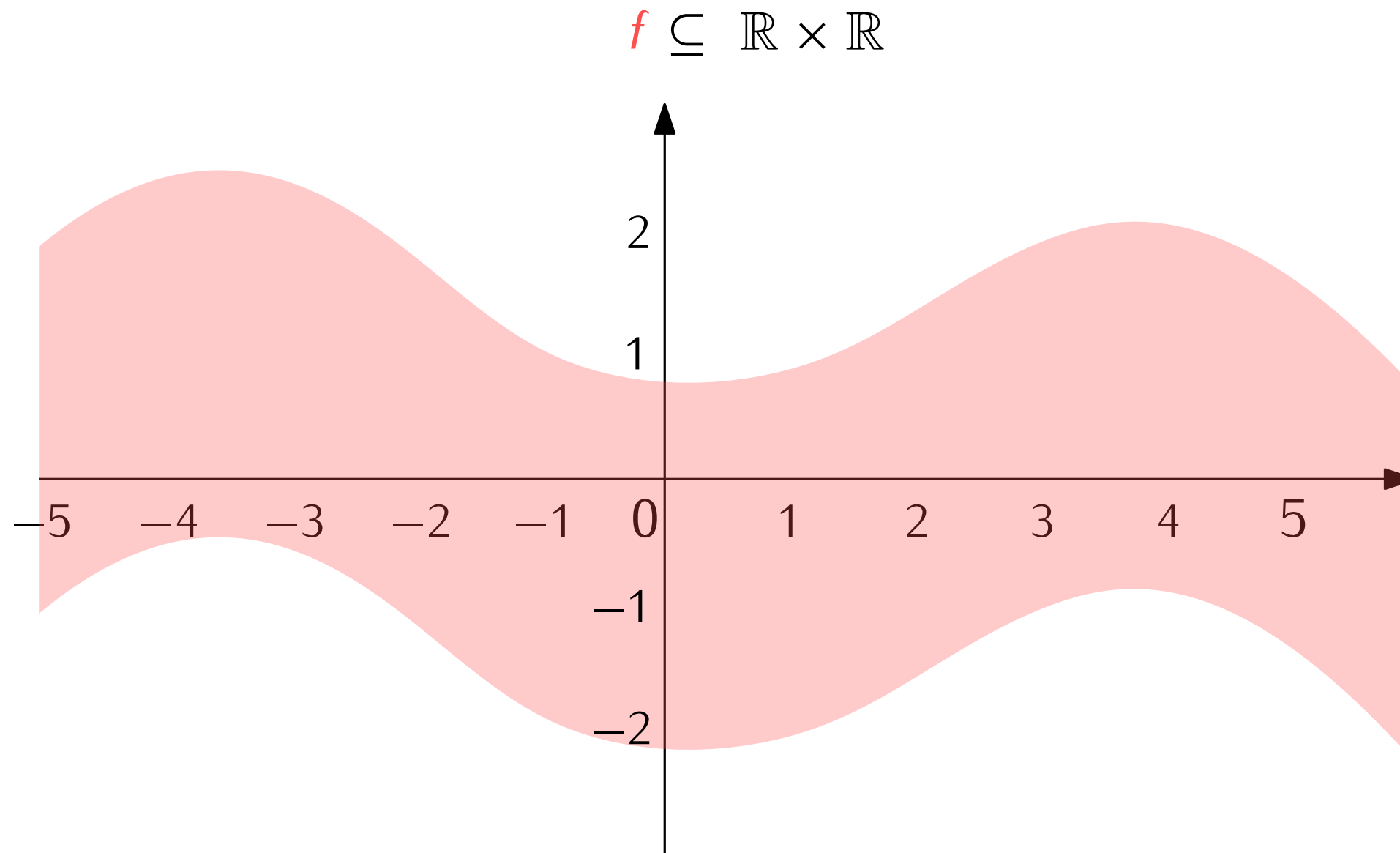
Question. Is this a function?

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.



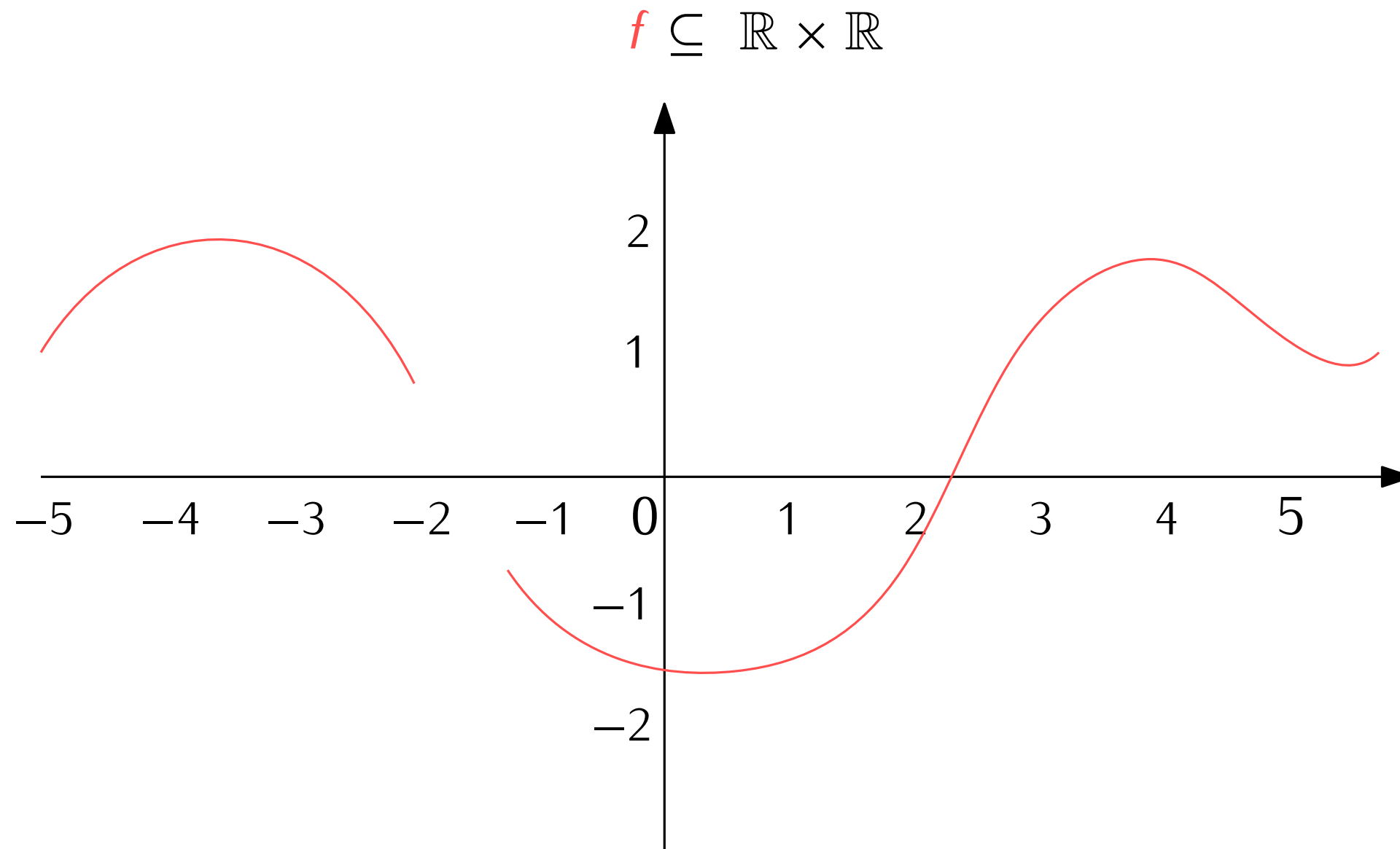
Question. Is this a function?

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.



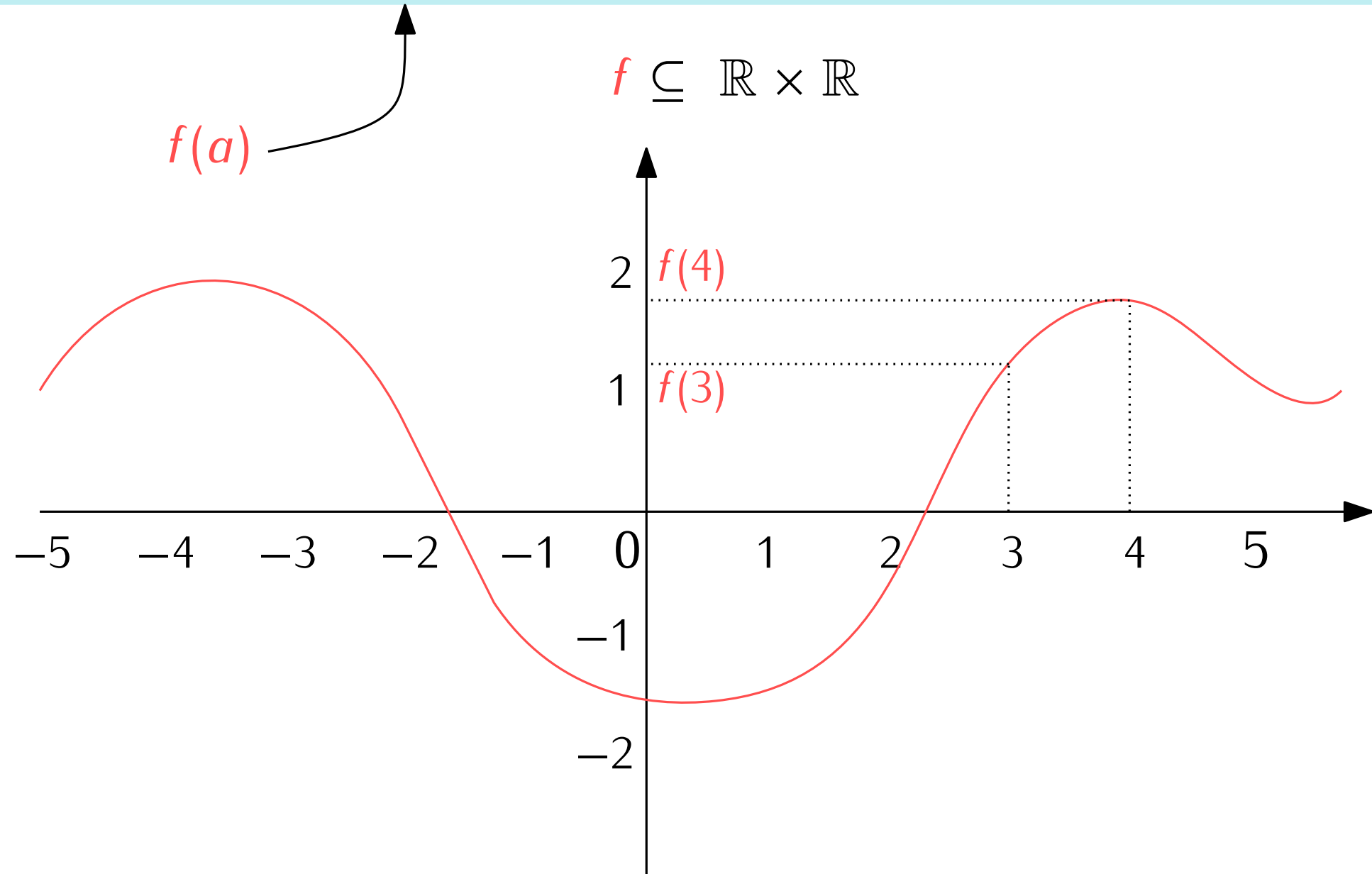
Question. Is this a function?

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.



Question. Is this a function?

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.

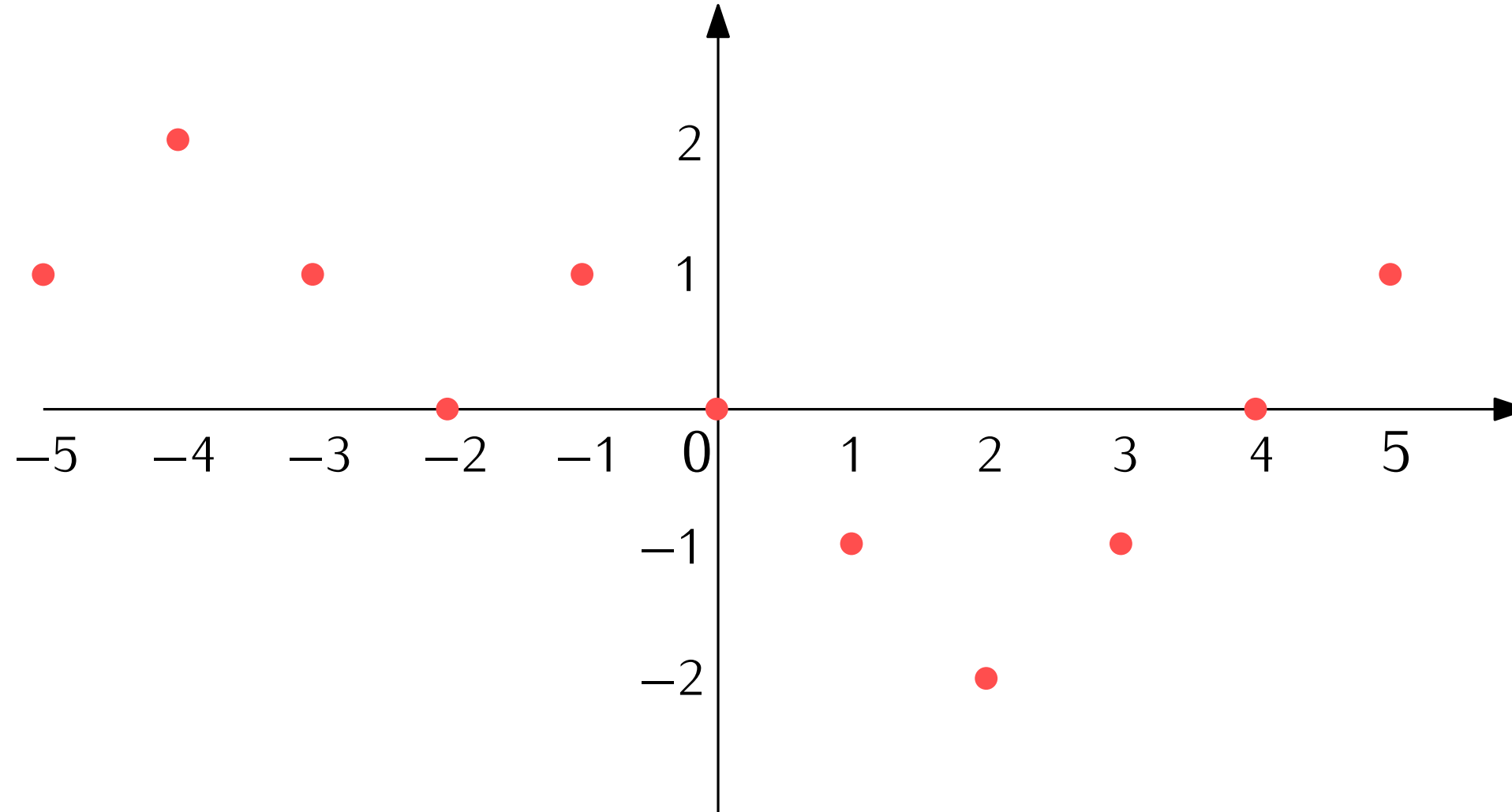


Question. Is this a function?

Remark. The definition corresponds to the idea of a “graph of a function”.

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.

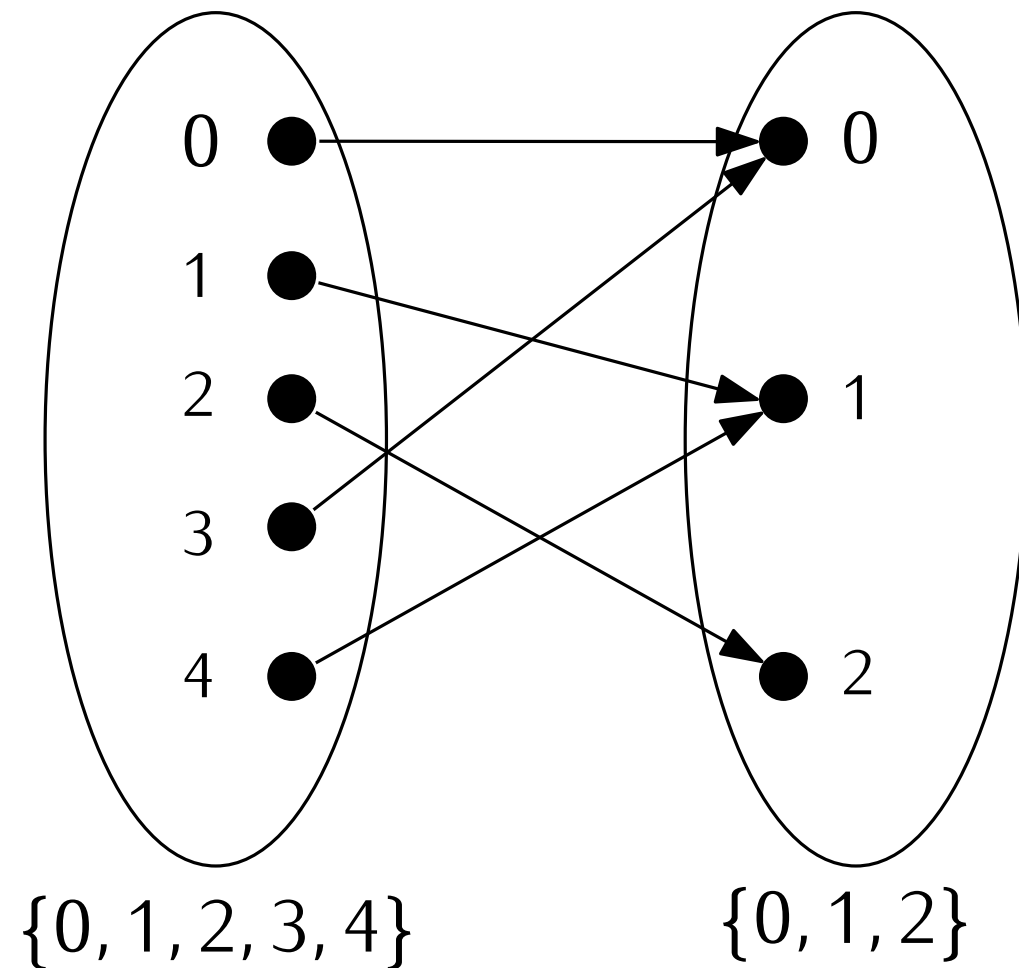
In discrete maths, we don't talk about $\mathbb{R}$! But sets like $\mathbb{N}, \mathbb{Z}, \{0, 2, 4\}, \dots$
How do we draw functions with such sets?



A function $f: \mathbb{Z} \rightarrow \{-2, -1, 0, 1, 2\}$

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.

In discrete maths, we don't talk about $\mathbb{R}$! But sets like $\mathbb{N}, \mathbb{Z}, \{0, 2, 4\}, \dots$
How do we draw functions with such sets?



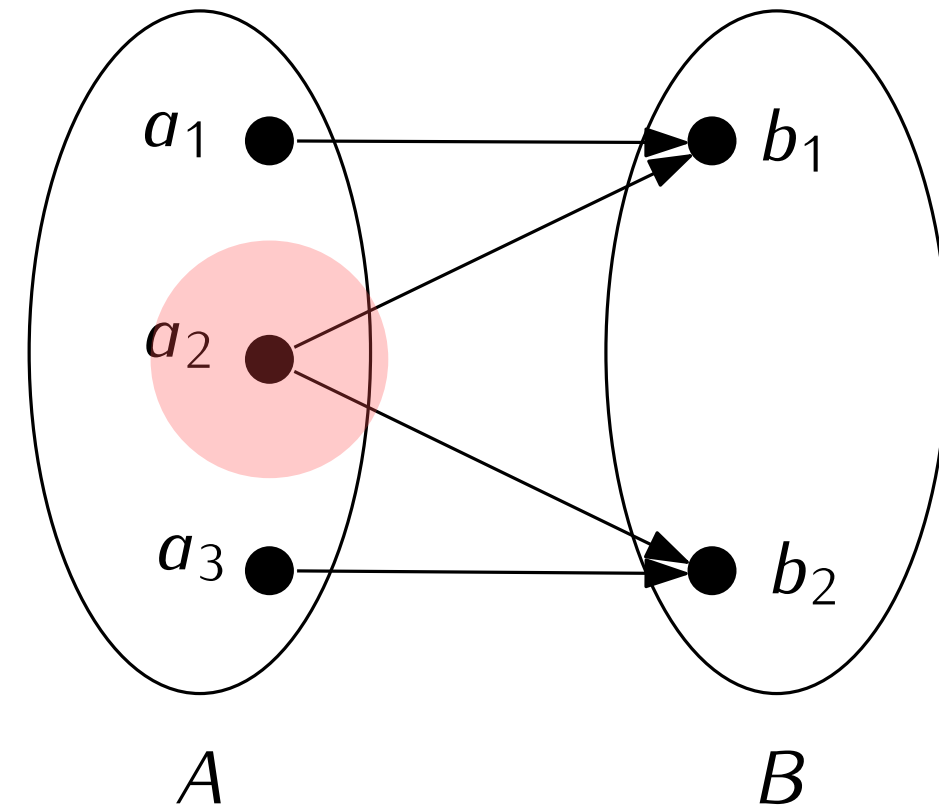
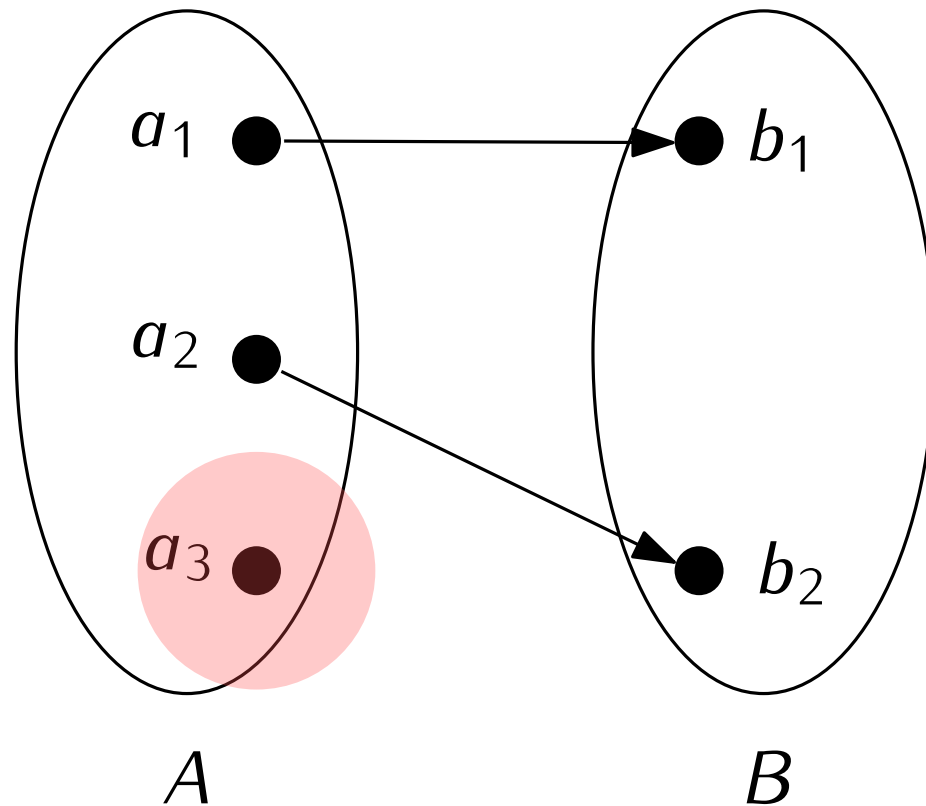
This represents the function

$$f = \{(0, 0), (1, 1), (2, 1), (3, 0), (4, 2)\}$$

Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.

There are two reasons for some $f \subseteq A \times B$ to **not** be a function $A \rightarrow B$:

- It could be that for some $a \in A$, there are **no** $b \in B$ such that $(a, b) \in f$
- It could be that for some $a \in A$, there are **at least two** $b, b' \in B$ such that $(a, b) \in f$ and $(a, b') \in f$



Definition. A function $f: A \rightarrow B$ is a set $f \subseteq A \times B$ such that **for every** $a \in A$, there exists a **unique** $b \in B$ such that $(a, b) \in f$.

There are two reasons for some $f \subseteq A \times B$ to **not** be a function $A \rightarrow B$:

- It could be that for some $a \in A$, there are **no** $b \in B$ such that $(a, b) \in f$
- It could be that for some $a \in A$, there are **at least two** $b, b' \in B$ such that $(a, b) \in f$ and $(a, b') \in f$

Which of the following sets are functions $\{1, 2, 3\} \rightarrow \{1, 2\}$?

- $\{(1, 1), (1, 2), (2, 1), (3, 2)\}$
- $\{(1, 1), (2, 1), (3, 2)\}$
- $\{(1, 1), (2, 1)\}$
- $\{(1, 2), (2, 1), (3, 2)\}$

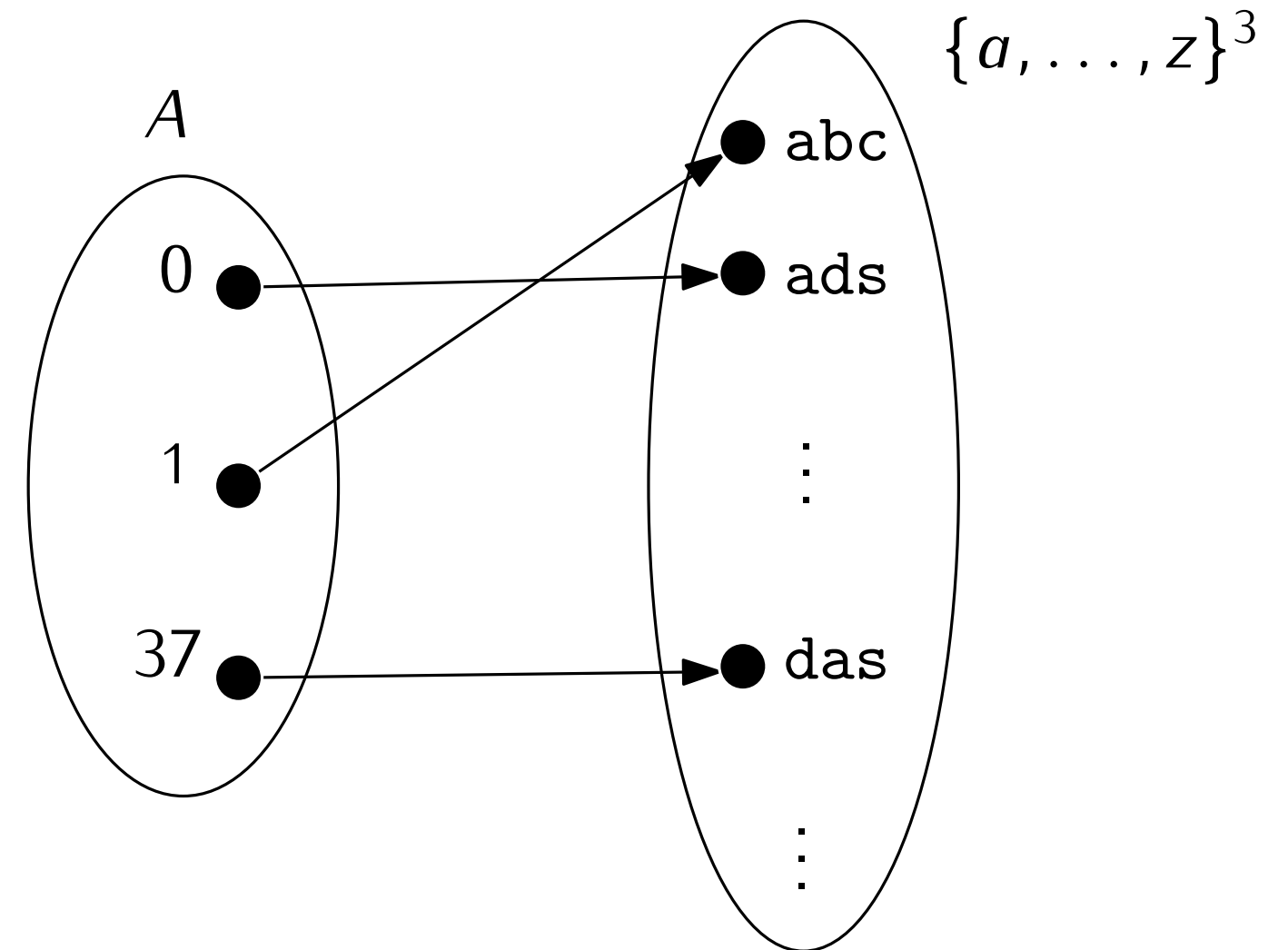


- Functions in programming languages:

```
def Collatz(x: int) -> int:
    if x%2 == 0:
        return x/2
    else:
        return 3*x+1
```

- Dictionaries (in programming languages):

```
f = {0: 'ads', 1: 'abc', 37: 'das'}
print(f.keys()) # {0,1,37}
print(f.values()) # {'ads','abc','das'}
```



- Functions in programming languages:

```
def Collatz(x: int) -> int:
    if x%2 == 0:
        return x/2
    else:
        return 3*x+1
```

- Dictionaries (in programming languages):

```
f = {0: 'ads', 1: 'abc', 37: 'das'}
print(f.keys()) # {0,1,37}
print(f.values()) # {'ads', 'abc', 'das'}
```

- Encoding: ASCIIencoding: $\text{ASCII} \rightarrow \{0,1\}^8$

ASCIIencoding('a') = 01100001

ASCIIencoding('=') = 00111101

UTF8encoding: $\text{UTF8} \rightarrow \{0,1\}^{48}$

bit-strings of length 48
6 **bytes**



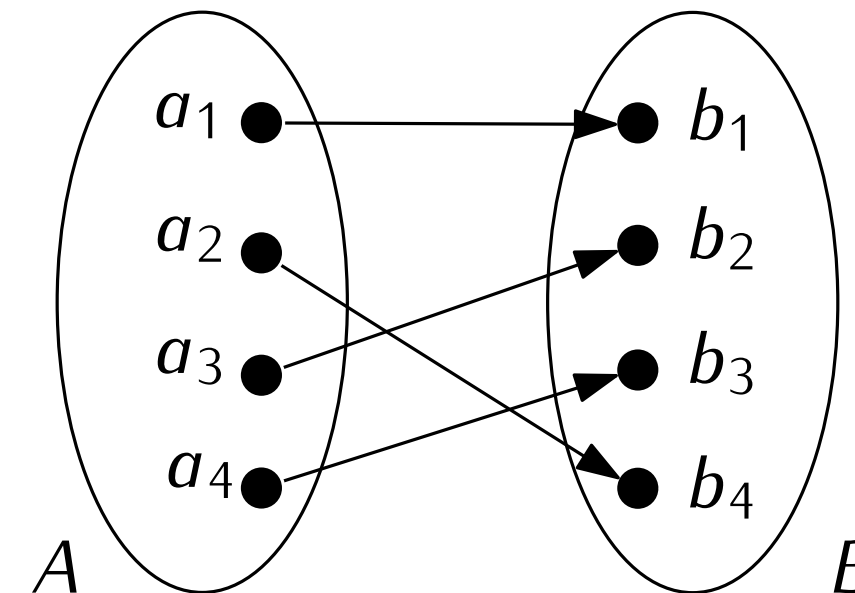
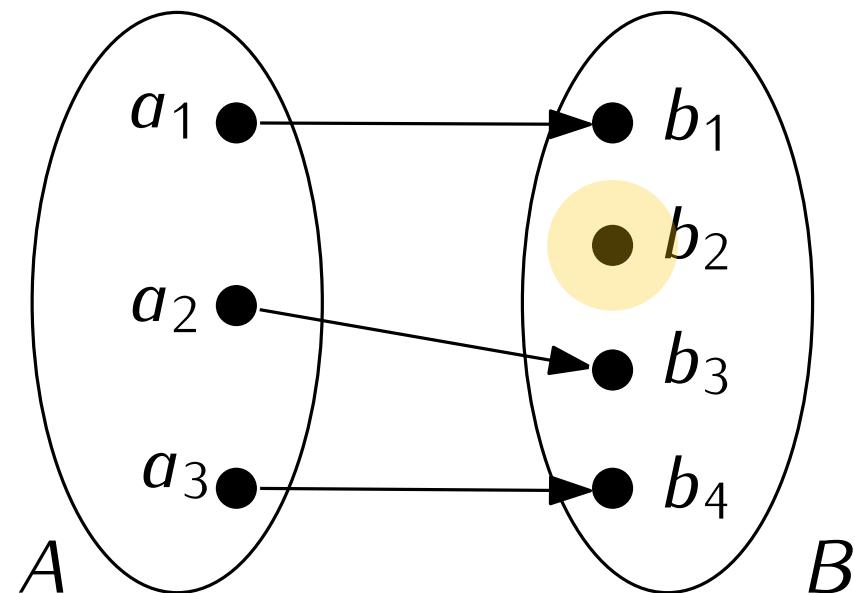
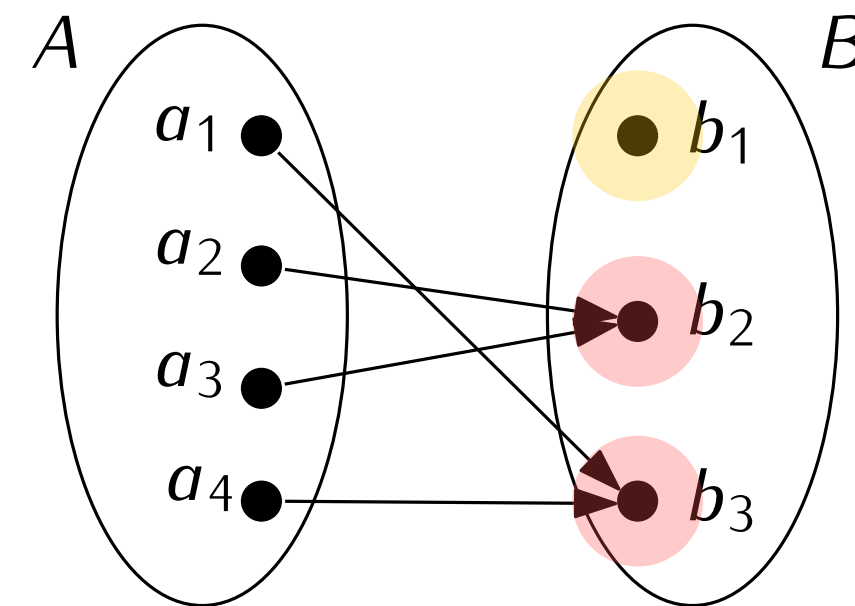
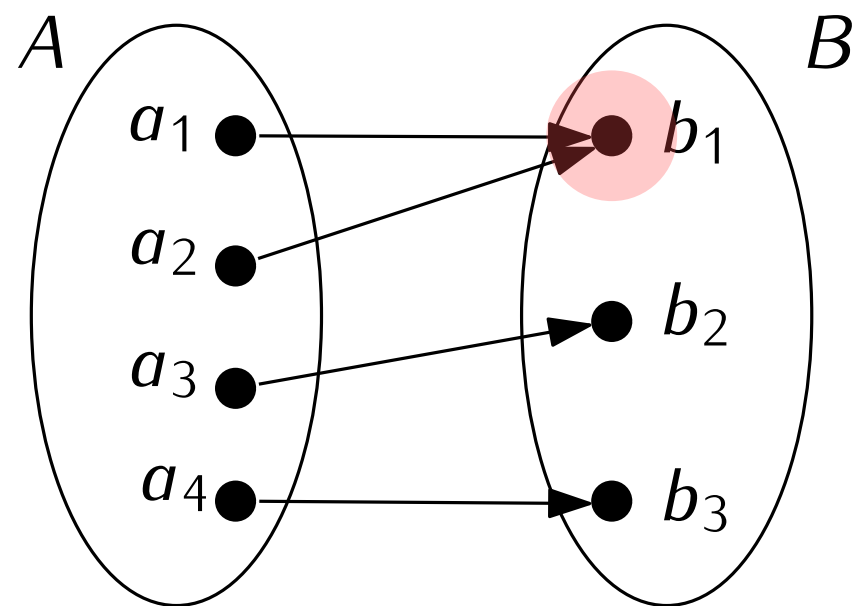
- Encryption: EncryptionScheme: $\text{ClearText} \rightarrow \text{EncryptedText}$
- Hash functions: MD5, SHA-1, SHA-256,...
- Transformers: $\text{Tokens} \rightarrow \mathbb{Q}^{4096}$

- Definition; be able to determine if a given set $f \subseteq A \times B$ is a function or not
- Properties of functions: injectivity, surjectivity, bijectivity
- Composition of functions
- Identity function
- Inverses

} coming up

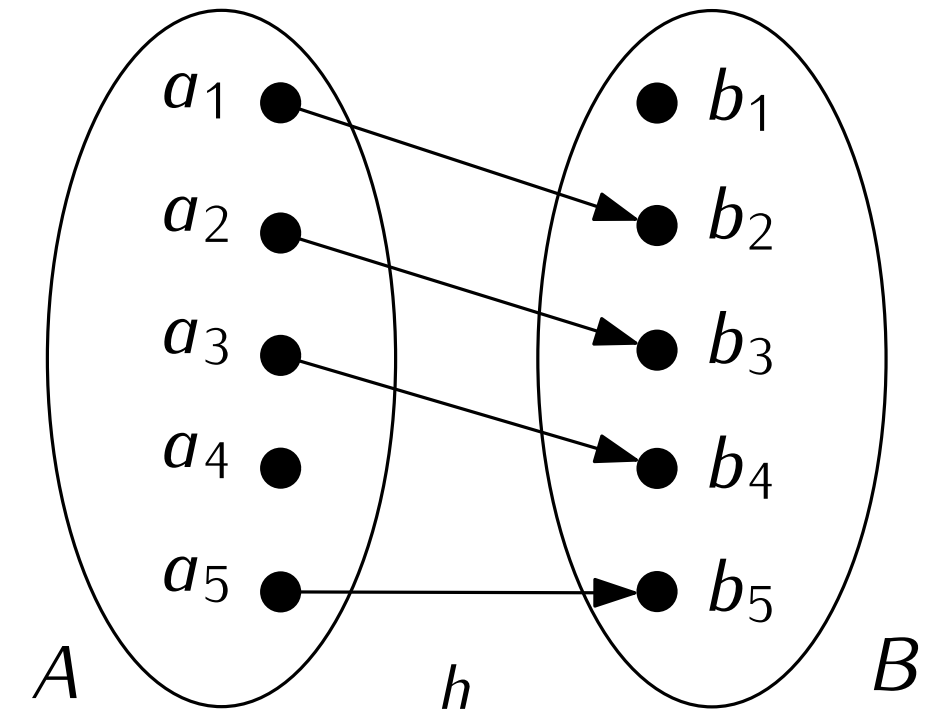
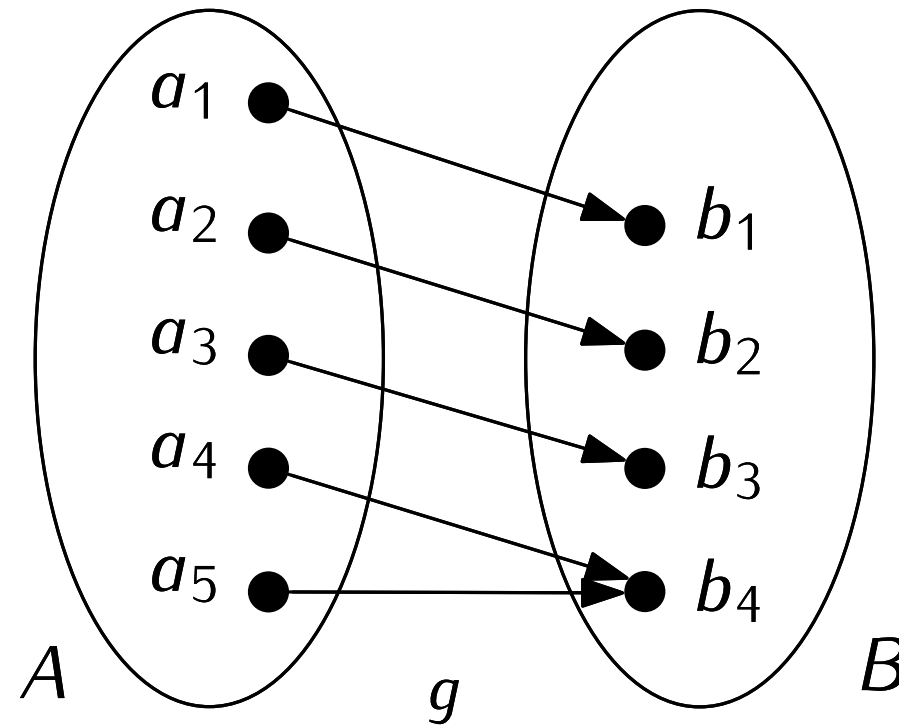
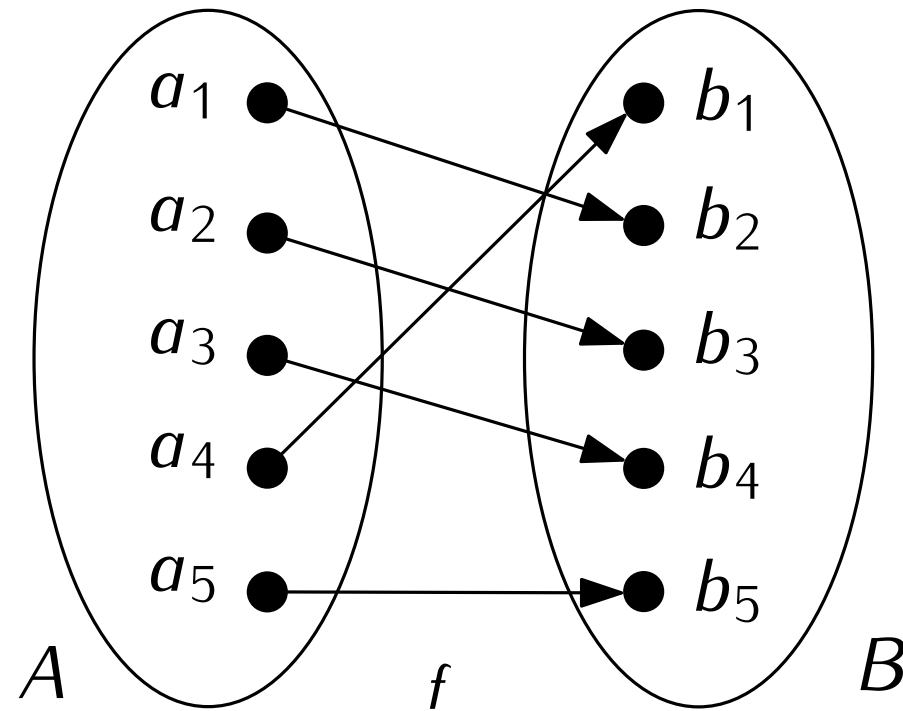
Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.



Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.



True/False?

- f is injective
- f is surjective
- g is injective
- g is surjective
- h is a function



Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.

Checking injectivity/surjectivity is “easy” if we can draw the function completely.

How to check if a function is injective/surjective if the sets are infinite/big?

- To check f is injective: **prove** that if $f(a) = f(a')$, then $a = a'$.

Theorem. The function $f: \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.

Hypothesis 1: $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 2x + 1$

Goal: f is injective

Proof.

Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.

Checking injectivity/surjectivity is “easy” if we can draw the function completely.

How to check if a function is injective/surjective if the sets are infinite/big?

- To check f is injective: **prove** that if $f(a) = f(a')$, then $a = a'$.

Theorem. The function $f: \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.

Hypothesis 1: $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 2x + 1$

Goal: if $f(a) = f(a')$, then $a = a'$.

Proof.

1. By definition of injectivity, we need to check that if $f(a) = f(a')$, then $a = a'$.

Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.

Checking injectivity/surjectivity is “easy” if we can draw the function completely.

How to check if a function is injective/surjective if the sets are infinite/big?

- To check f is injective: **prove** that if $f(a) = f(a')$, then $a = a'$.

Theorem. The function $f: \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.

Hypothesis 1: $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 2x + 1$

Hypothesis 2: $f(a) = f(a')$

Goal: $a = a'$.

Proof.

1. By definition of injectivity, we need to check that if $f(a) = f(a')$, then $a = a'$.
2. So let a, a' be such that $f(a) = f(a')$.

Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.

Checking injectivity/surjectivity is “easy” if we can draw the function completely.

How to check if a function is injective/surjective if the sets are infinite/big?

- To check f is injective: **prove** that if $f(a) = f(a')$, then $a = a'$.

Theorem. The function $f: \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.

Hypothesis 1: $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = 2x + 1$

Hypothesis 2: $2a + 1 = 2a' + 1$

Hypothesis 3: $2a = 2a'$

Hypothesis 4: $a = a'$

Goal: $a = a'$.

Proof.

1. By definition of injectivity, we need to check that if $f(a) = f(a')$, then $a = a'$.
2. So let a, a' be such that $f(a) = f(a')$.
3. Subtract 1 on both sides of Hyp. 2
4. Divide by 2 on both sides of Hyp. 3
5. Done! $\square$

Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.

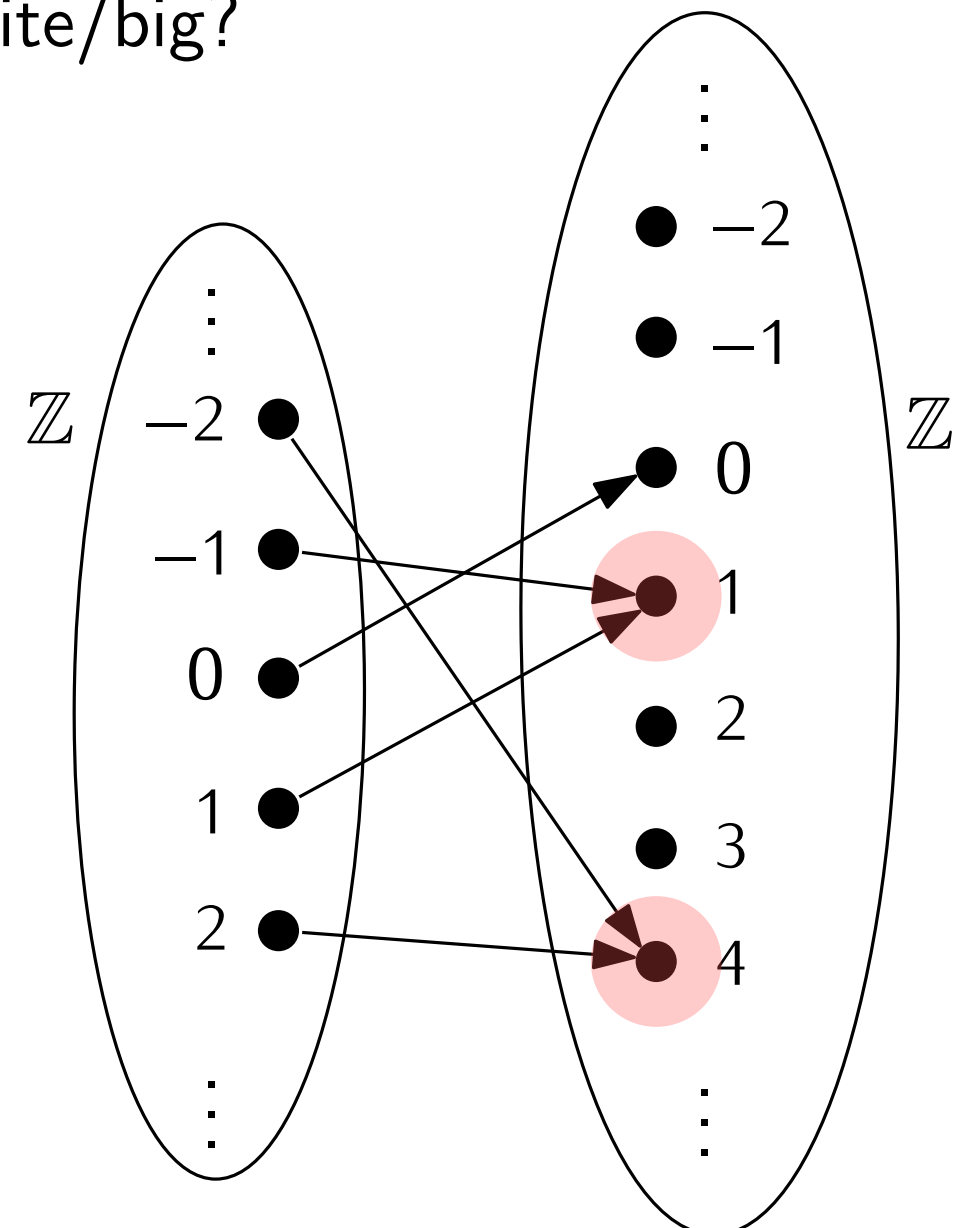
Checking injectivity/surjectivity is “easy” if we can draw the function completely.

How to check if a function is injective/surjective if the sets are infinite/big?

- To check f is injective: **prove** that if $f(a) = f(a')$, then $a = a'$.
- To check f is **not** injective: **find** $a \neq a'$ such that $f(a) = f(a')$.

Theorem. $f: \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $f(x) = x^2$ is **not** injective.

Proof. $f(-1) = f(1)$. □



Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.

Checking injectivity/surjectivity is “easy” if we can draw the function completely.

How to check if a function is injective/surjective if the sets are infinite/big?

- To check f is injective: **prove** that if $f(a) = f(a')$, then $a = a'$.
- To check f is **not** injective: **find** $a \neq a'$ such that $f(a) = f(a')$.
- To check that f is surjective: for every $b \in B$, **find** $a \in A$ such that $f(a) = b$.

Theorem. The function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $f(x) = -x + 3$ is surjective.

Proof.

1. Let $b \in \mathbb{Z}$.
2. Define $a := -b + 3$.
3. We check that $f(a) = -a + 3 = -(-b + 3) + 3 = b - 3 + 3 = b$.
4. Done! $\square$

Definition. A function $f: A \rightarrow B$ is:

- **injective** if for all $b \in B$, there is **at most one** $a \in A$ such that $f(a) = b$,
- **surjective** if for all $b \in B$, there is **at least one** $a \in A$ such that $f(a) = b$,
- **bijective** if for all $b \in B$, there exists **exactly one** $a \in A$ such that $f(a) = b$.

Checking injectivity/surjectivity is “easy” if we can draw the function completely.

How to check if a function is injective/surjective if the sets are infinite/big?

- To check f is injective: **prove** that if $f(a) = f(a')$, then $a = a'$.
- To check f is **not** injective: **find** $a \neq a'$ such that $f(a) = f(a')$.
- To check that f is surjective: for every $b \in B$, **find** $a \in A$ such that $f(a) = b$.
- To check that f is **not** surjective: **find** $b \in B$ and **prove** that there is no $a \in A$ such that $f(a) = b$.

Theorem. The function $f: \mathbb{N} \rightarrow \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective.

Proof.

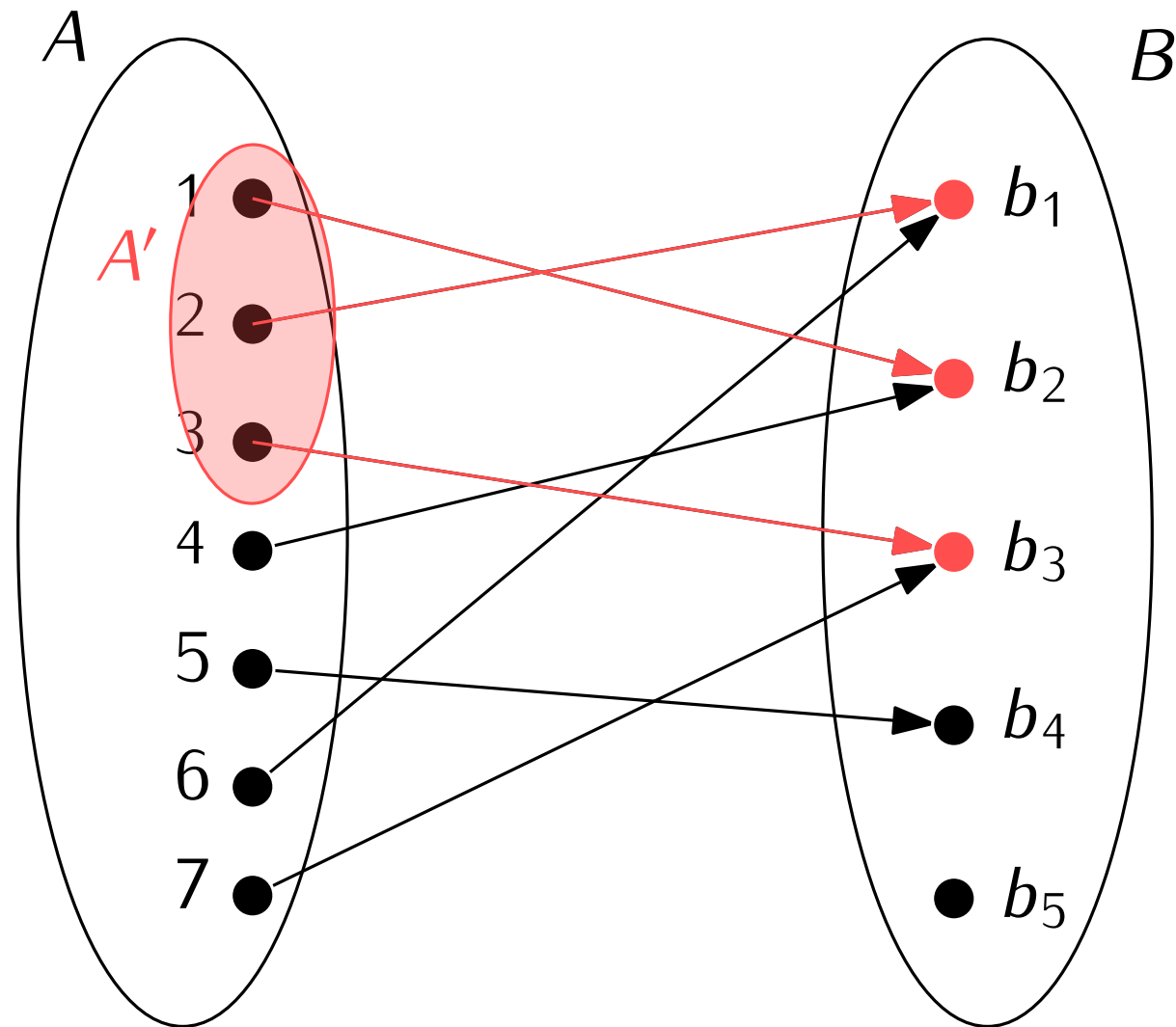
1. Let $b = -1$.
2. Known fact: $a^2 \geq 0$ for all $a \in \mathbb{N}$
3. So $b \neq a^2$ for all $a \in \mathbb{N}$
4. Done! □

Definition. Let $f: A \rightarrow B$ be a function, $A' \subseteq A, B' \subseteq B$.

- The **image** of A' under f : $f[A'] = \{b \in B \mid b = f(a) \text{ for some } a \in A'\}$
- The **preimage** of B' under f : $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

- $f[\{1, 2, 3\}] =$

- $f^{-1}[\{b_3\}] =$

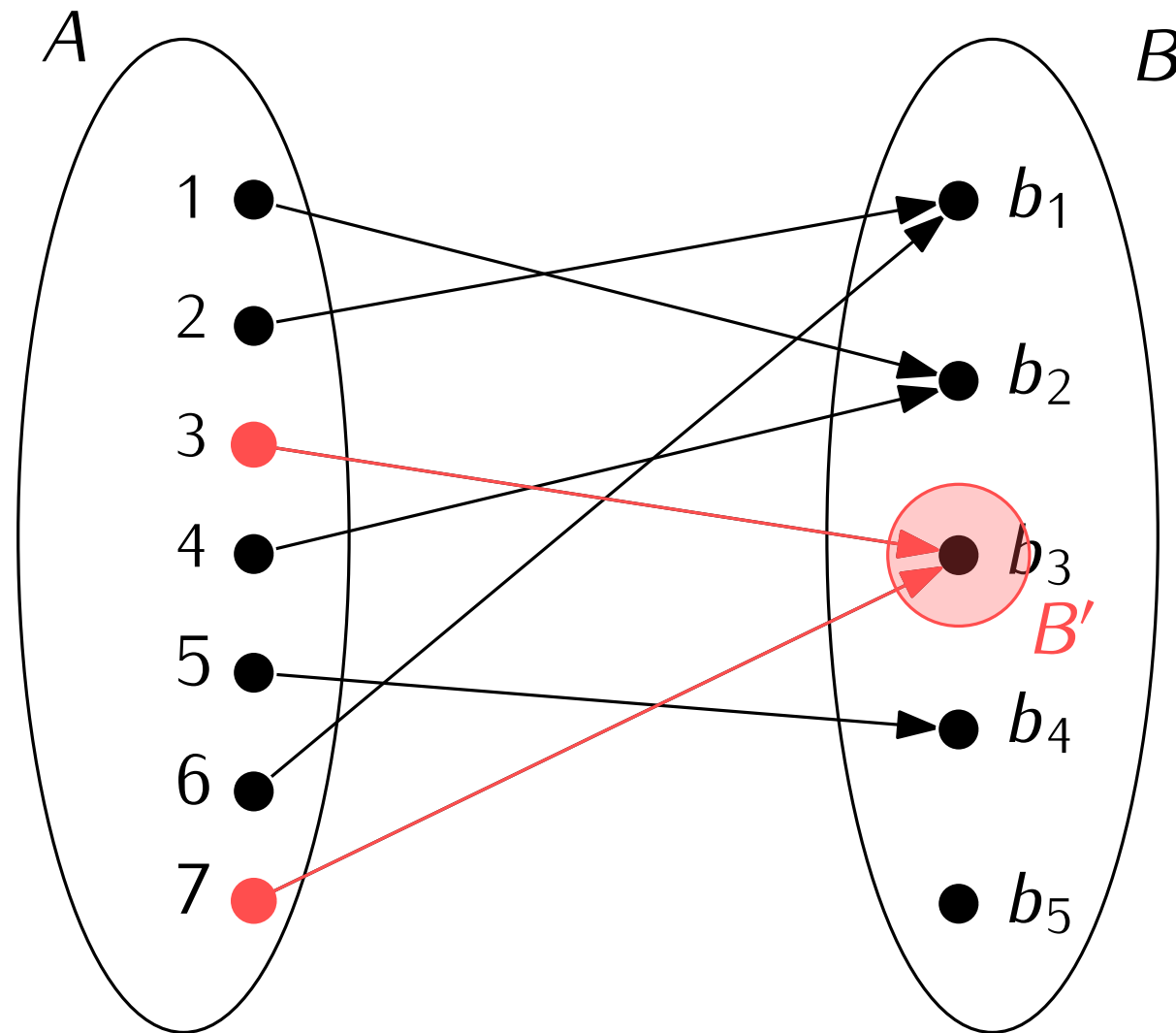


Definition. Let $f: A \rightarrow B$ be a function, $A' \subseteq A, B' \subseteq B$.

- The **image** of A' under f : $f[A'] = \{b \in B \mid b = f(a) \text{ for some } a \in A'\}$
- The **preimage** of B' under f : $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

- $f[\{1, 2, 3\}] = \{b_1, b_2, b_3\}$

- $f^{-1}[\{b_3\}] =$



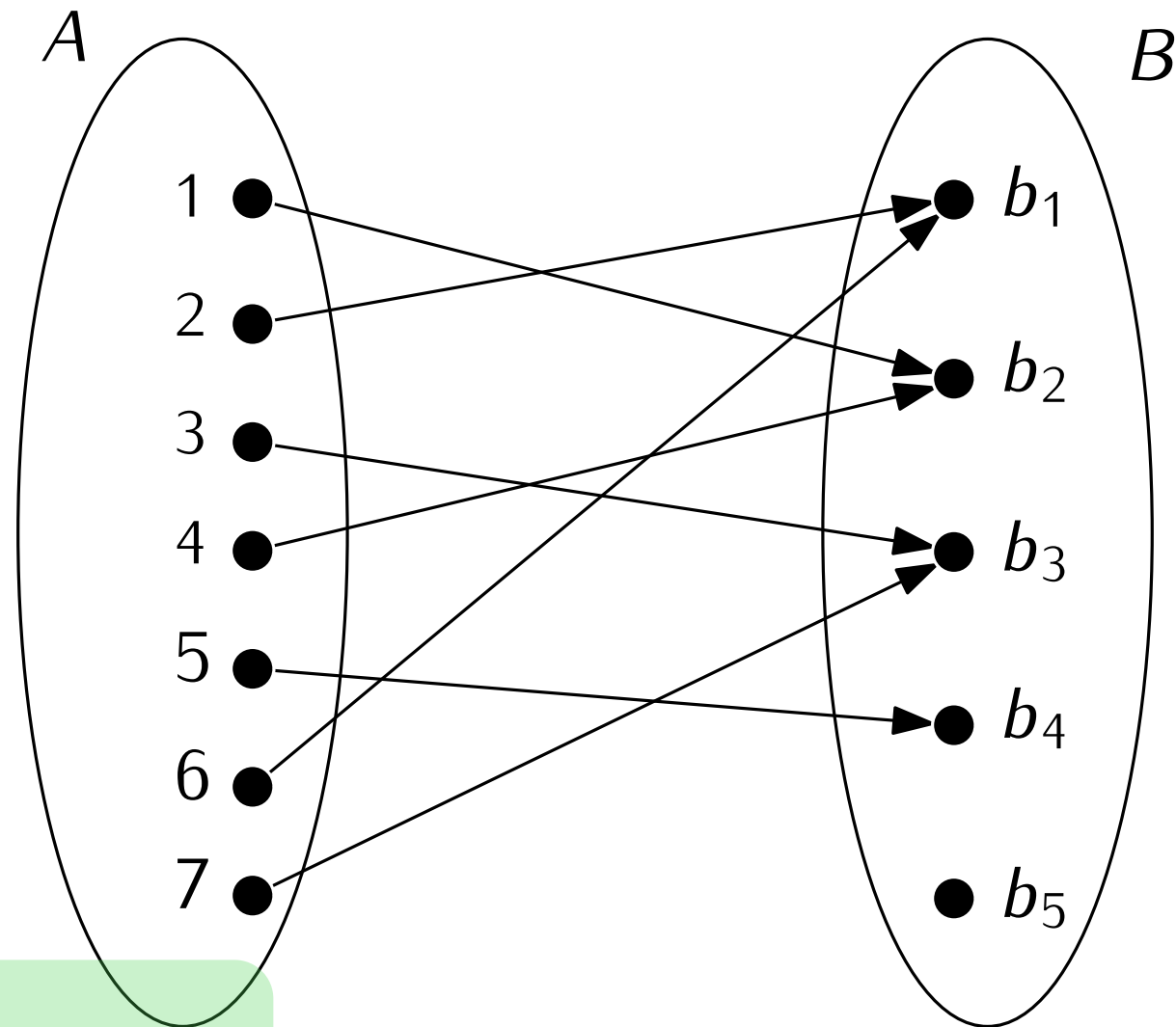
Definition. Let $f: A \rightarrow B$ be a function, $A' \subseteq A, B' \subseteq B$.

- The **image** of A' under f : $f[A'] = \{b \in B \mid b = f(a) \text{ for some } a \in A'\}$
- The **preimage** of B' under f : $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

- $f[\{1, 2, 3\}] = \{b_1, b_2, b_3\}$
- $f^{-1}[\{b_3\}] = \{3, 7\}$

Your turn!

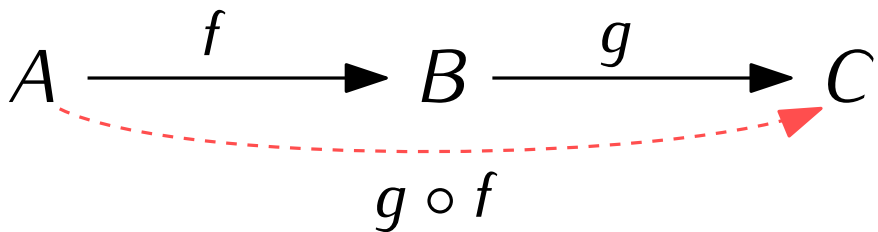
- $f[\{2, 6, 7\}] =$
- $f^{-1}[\{b_5\}] =$
- $f^{-1}[\{b_2, b_4\}] =$



Self-check. Some things to think about:

- f injective ... what can we say about $f^{-1}[\{b\}]$?
- f surjective ... what can we say about $f^{-1}[\{b\}]$?

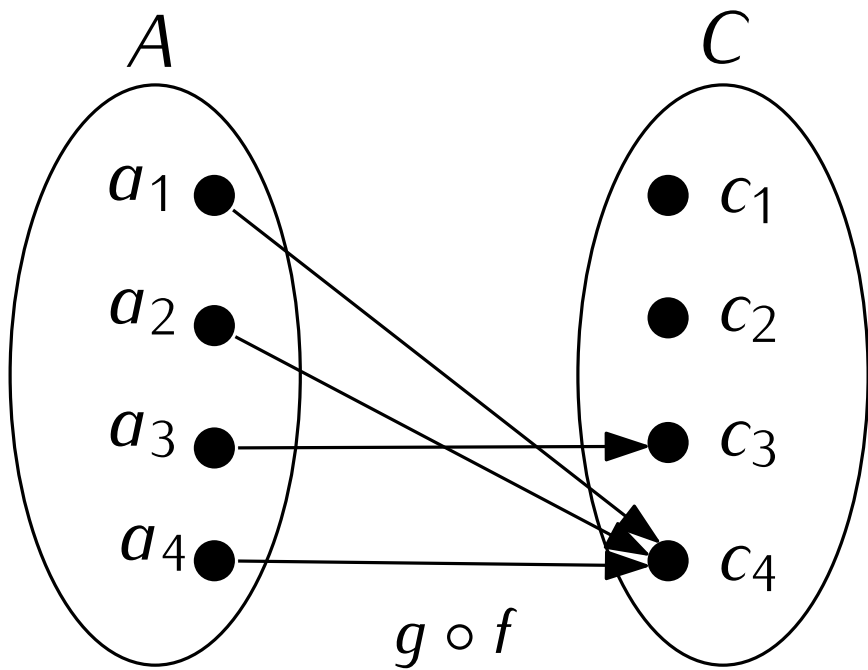
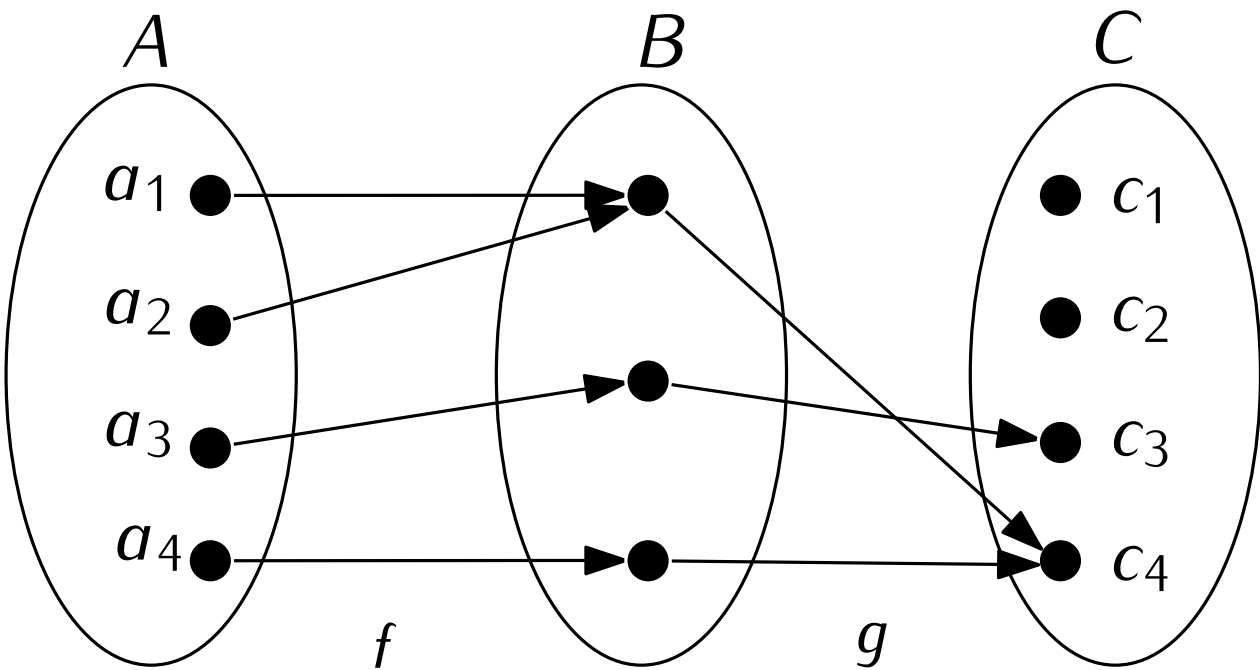
Definition. If $f: A \rightarrow B$ and $g: B \rightarrow C$, the **composition** of f and g is the function $g \circ f: A \rightarrow C$ defined by

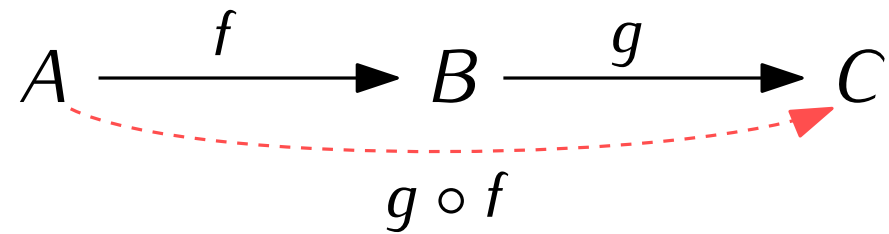
$$(g \circ f)(a) = g(f(a))$$


```
def f(x: int) -> int:
    y = 2*x+1
    return y
```

```
def g(x:int) -> int:
    y = y+3
    return y
```

```
print(f(g(2))) # ???
print(g(f(2))) # ???
```



$$(g \circ f)(a) = g(f(a))$$


- $f \circ g$ is not necessarily the same as $g \circ f$,
- $g \circ f$ only makes sense if the codomain of f is the same as the domain of g .

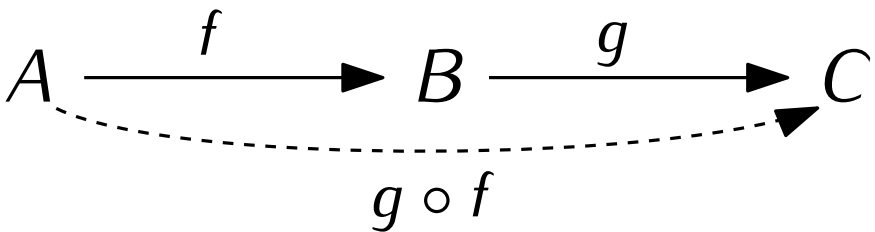
Let $f: \mathbb{N} \rightarrow \mathbb{N}$ and $g: \mathbb{N} \rightarrow \mathbb{Q}$ be defined by $f(x) = x + 1$ and $g(x) = \frac{1}{x}$. Which of the following hold?

- $(g \circ f)(1) = \frac{1}{2}$
- $(g \circ f)(2) = \frac{1}{2}$
- $(f \circ g)(1) = \frac{1}{2}$
- $(f \circ f)(2) = 4$

```
print(f(g(2))) # ???
print(g(f(2))) # ???
```



Definition. If $f: A \rightarrow B$ and $g: B \rightarrow C$, the **composition** of f and g is the function $g \circ f: A \rightarrow C$ defined by

$$(g \circ f)(a) = g(f(a))$$


The **identity function** on a set A is the function $\text{Id}_A: A \rightarrow A$ defined by $\text{Id}_A(x) = x$.

```
def Id(x: A) -> A:
  return x
```

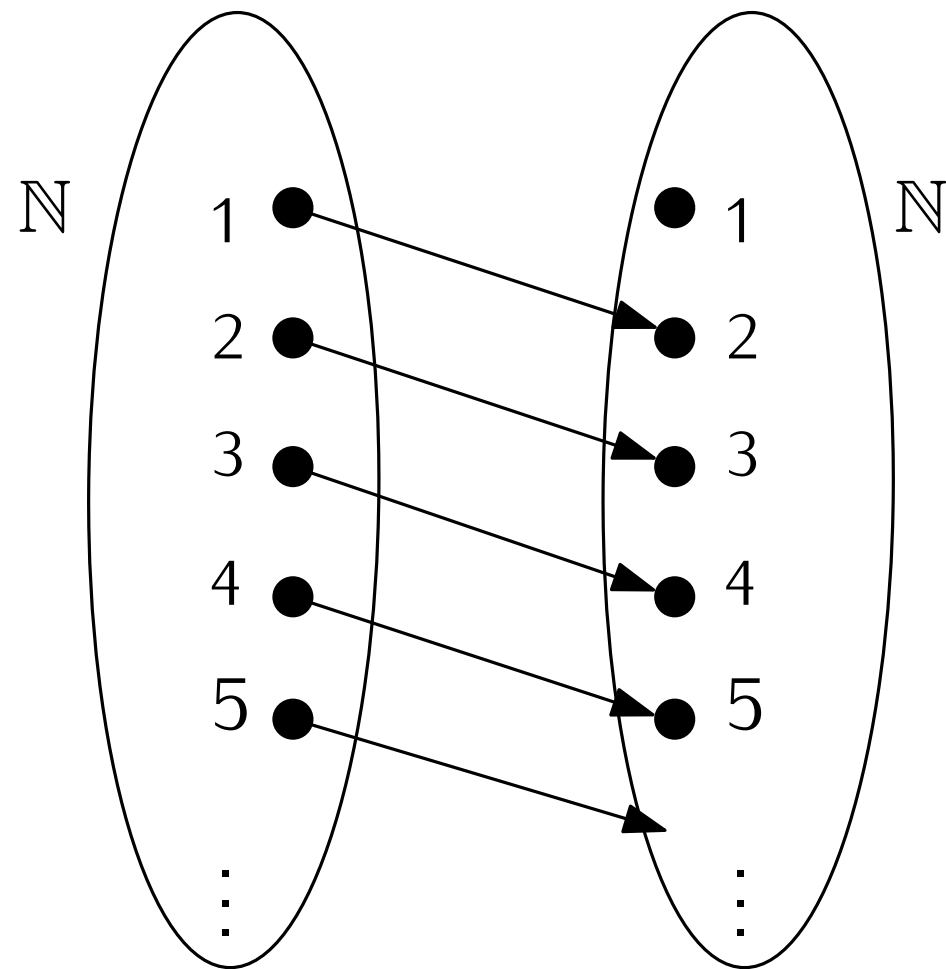
Useful things about Id:

- If $f: A \rightarrow B$, then $f \circ \text{Id}_A = f$
- If $f: A \rightarrow B$, then $\text{Id}_B \circ f = f$

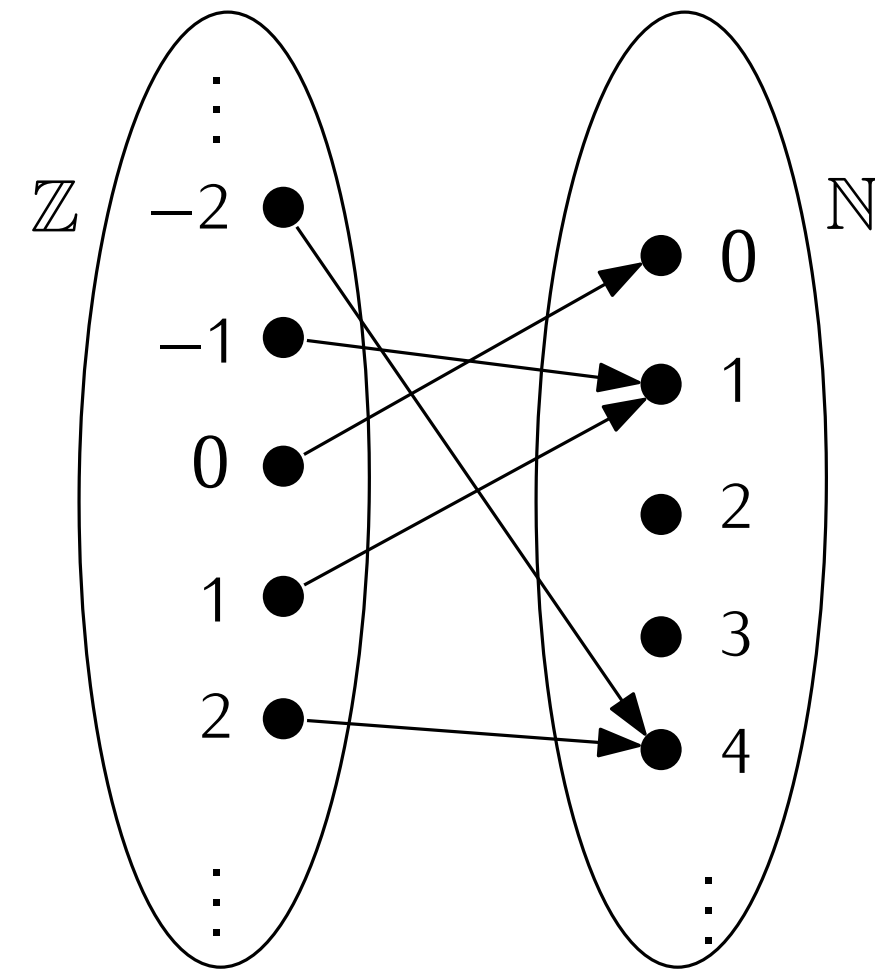
Analogies	
Numbers	Functions
Multiplication	Composition
$\times$	$\circ$
1	Id

Question. Let $f: A \rightarrow B$ be a function. Can one “undo” f ?
Given $b \in B$, is it possible to understand where b came from?

Example. $f: \mathbb{N} \rightarrow \mathbb{N}$, $f(x) = x + 1$.



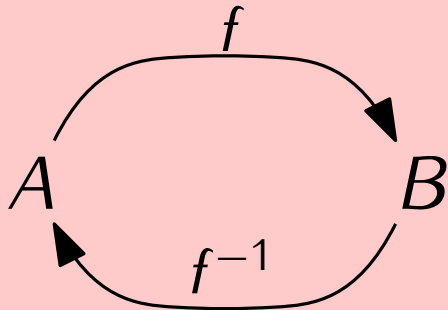
$g: \mathbb{Z} \rightarrow \mathbb{N}$, $g(x) = x^2$



Question. Let $f: A \rightarrow B$ be a function. Can one “undo” f ?
Given $b \in B$, is it possible to understand where b came from?

Need f to be both **injective** and **surjective**!

Theorem. If $f: A \rightarrow B$ is **bijective**, there exists $g: B \rightarrow A$ such that $g \circ f = \text{Id}_A$ and $f \circ g = \text{Id}_B$.
This g is **unique** and written f^{-1} .



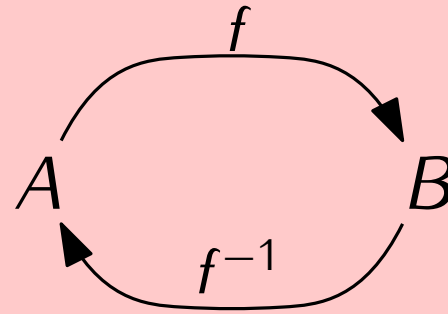
So $f^{-1}(f(a)) = a$ and $f(f^{-1}(b)) = b$ for all $a \in A, b \in B$.

Similarities		
Matrices	Numbers	Functions
Multiplication	Multiplication	Composition
$\times$	$\times$	$\circ$
I_n	1	Id
A^{-1} (for $\det(A) \neq 0$)	$1/x$ (for $x \neq 0$)	f^{-1} (for f bijective)

Question. Let $f: A \rightarrow B$ be a function. Can one “undo” f ?
Given $b \in B$, is it possible to understand where b came from?

Need f to be both **injective** and **surjective**!

Theorem. If $f: A \rightarrow B$ is **bijjective**, there exists $g: B \rightarrow A$ such that $g \circ f = \text{Id}_A$ and $f \circ g = \text{Id}_B$.
This g is **unique** and written f^{-1} .



So $f^{-1}(f(a)) = a$ and $f(f^{-1}(b)) = b$ for all $a \in A, b \in B$.

What is the inverse of $f: \mathbb{Q} \rightarrow \mathbb{Q}$ defined by $f(x) = 3x + 2$?

- Trick question! f has no inverse
- Trick question! f is not a function
- $f^{-1}(x) = \frac{1}{3}x - 2$
- $f^{-1}(x) = \frac{1}{3}(x - 2)$
- $f^{-1}(x) = \frac{3}{x-2}$



- Definition; be able to determine if a given set $f \subseteq A \times B$ is a function or not
- Properties of functions: injectivity, surjectivity, bijectivity
- Composition of functions
- Identity function
- Inverses