Discrete Algebraic Structures

WiSe 2025/2026

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

Organizational

- 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)

Recap from last week

- 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

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
```

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
```

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): $\cos, \sin, \exp, \ldots$

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): $\cos, \sin, \exp, \ldots$
- The input set is called the domain of the function

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): $\cos, \sin, \exp, \ldots$
- The input set is called the domain of the function
- The output set is called the codomain of the function

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
```

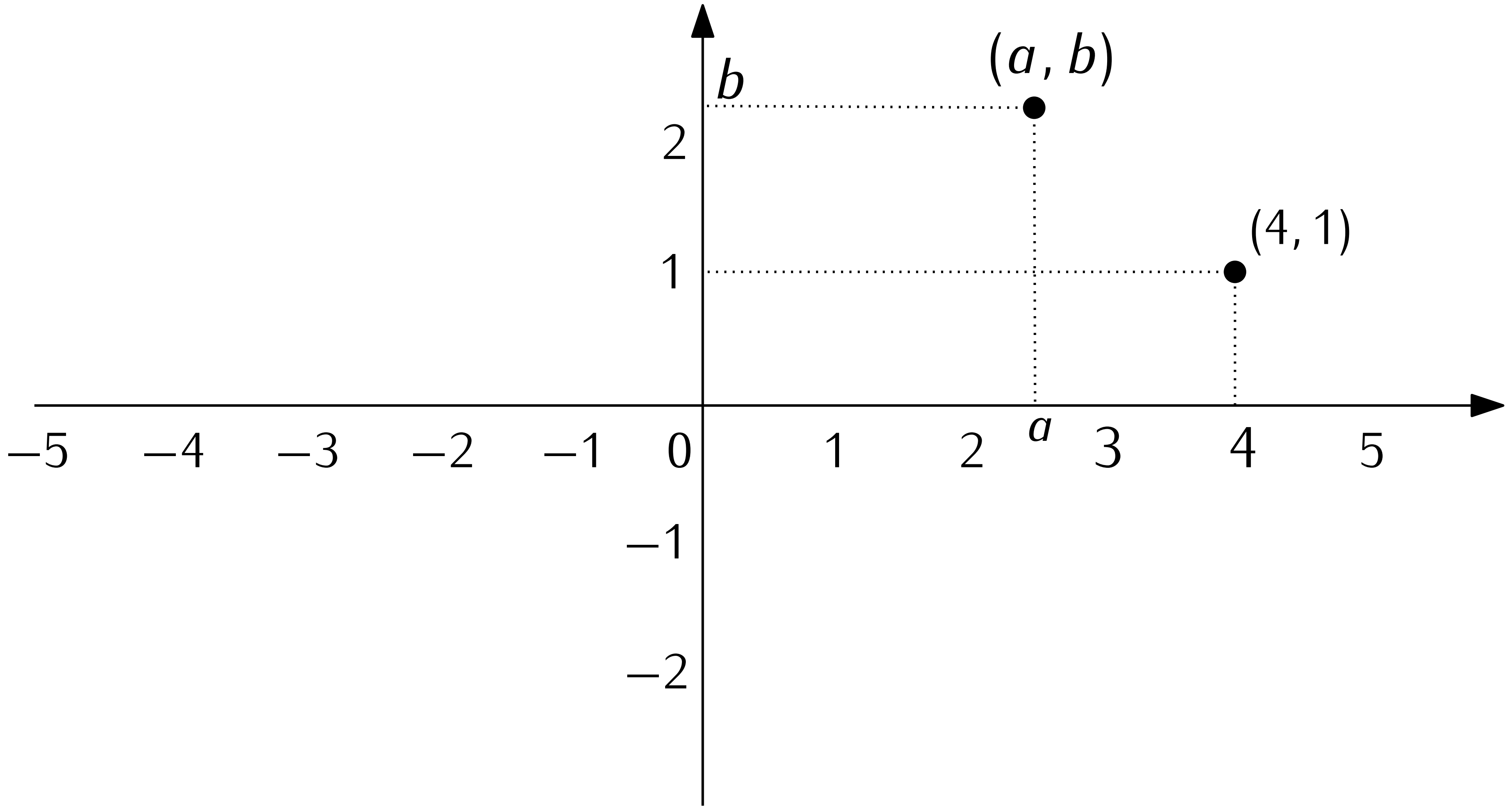
- Functions you already know from school (but not important here): $\cos, \sin, \exp, \ldots$
- The input set is called the domain of the function
- The output set is called the codomain of the function

Notation. $f\colon A \to B$ means "f is a function with domain A and codomain B".
$f(a)$: output of the function on the input a

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

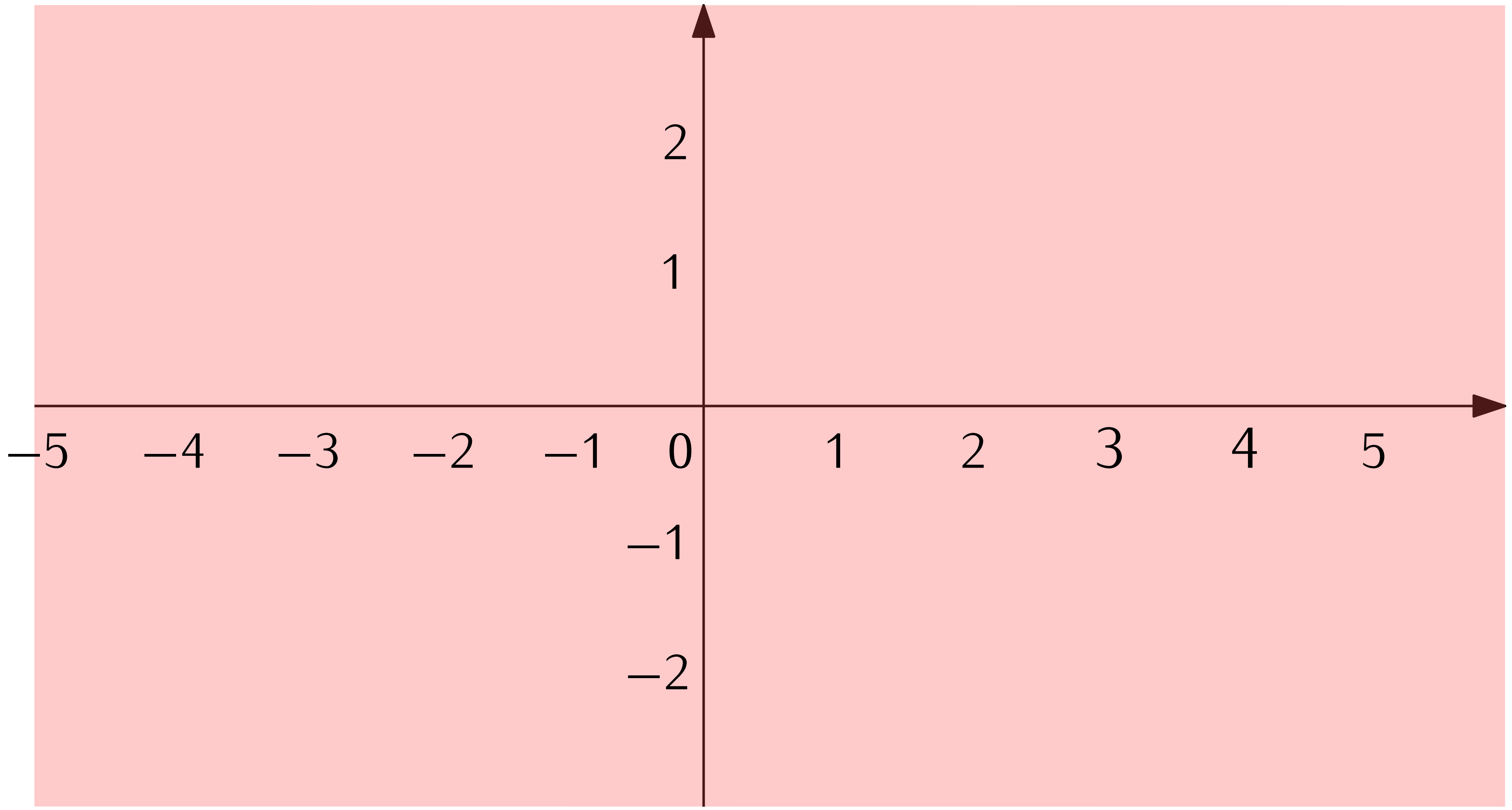
Definition. A function $f\colon A \to B$ is a set $f \subseteq A \times B$ such that for every $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

$\mathbb{R} \times \mathbb{R}$



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

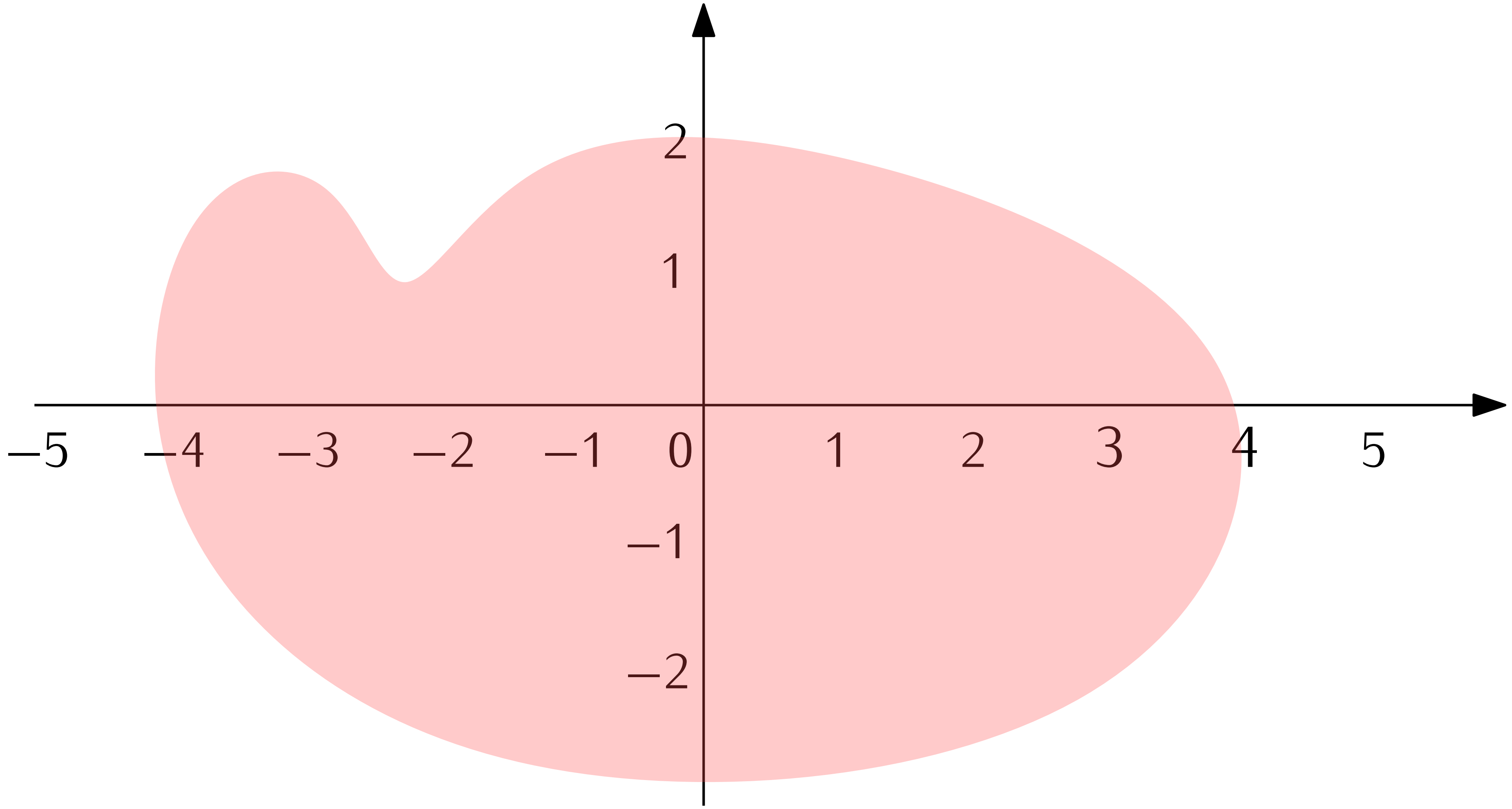
$f \subseteq \mathbb{R} \times \mathbb{R}$



Question. Is this a function?

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

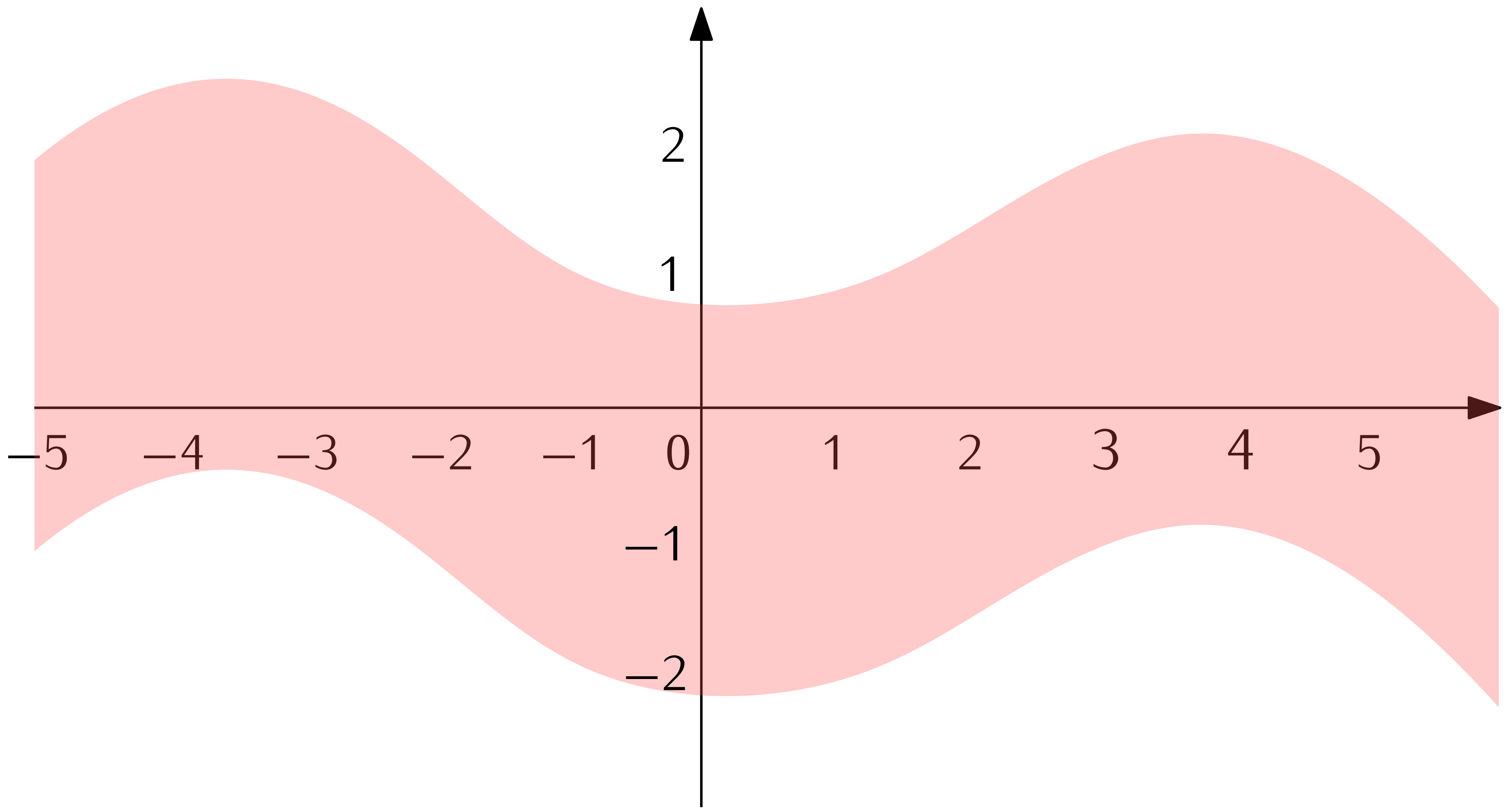
$f \subseteq \mathbb{R} \times \mathbb{R}$



Question. Is this a function?

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

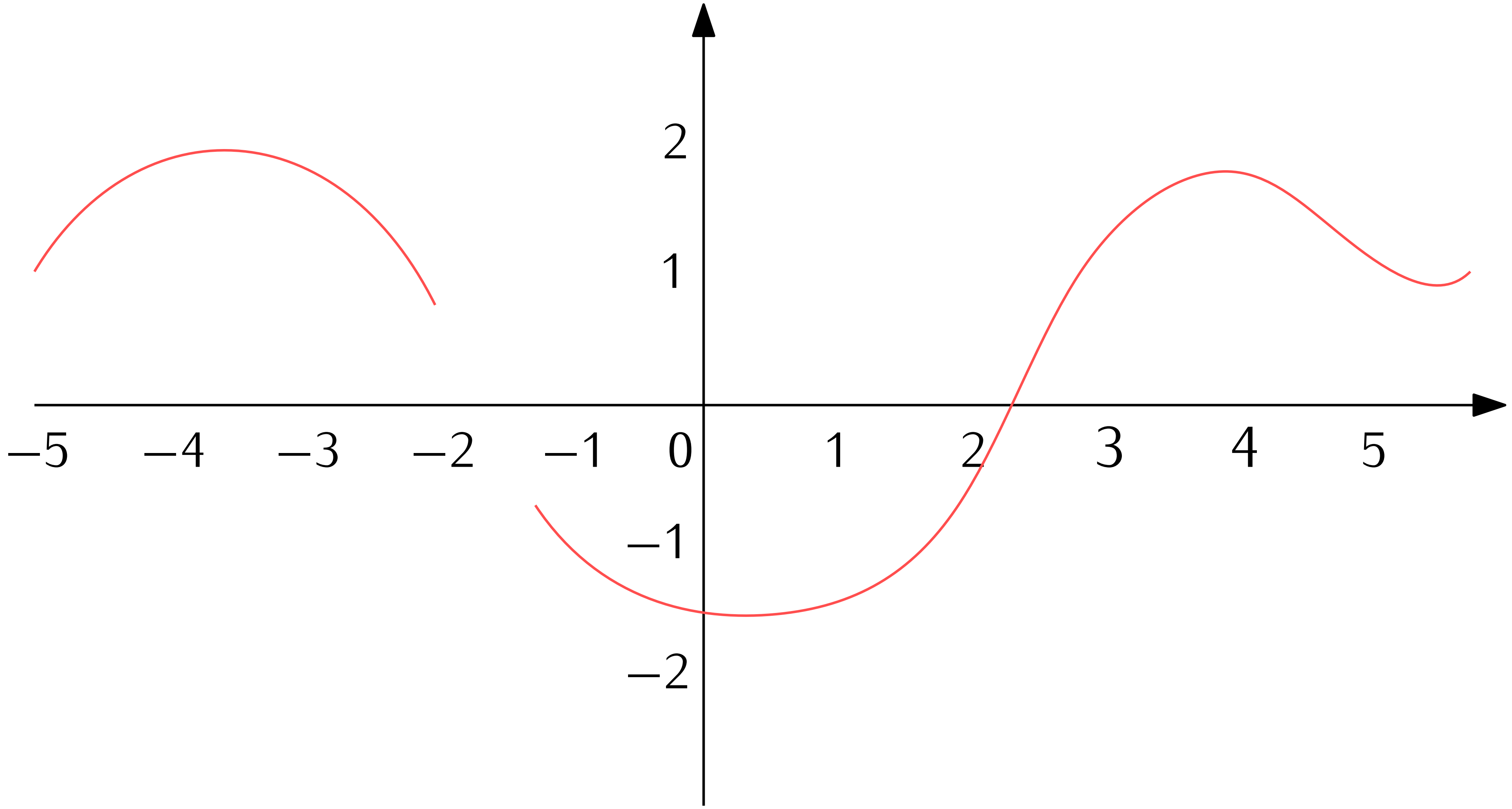
$f \subseteq \mathbb{R} \times \mathbb{R}$



Question. Is this a function?

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

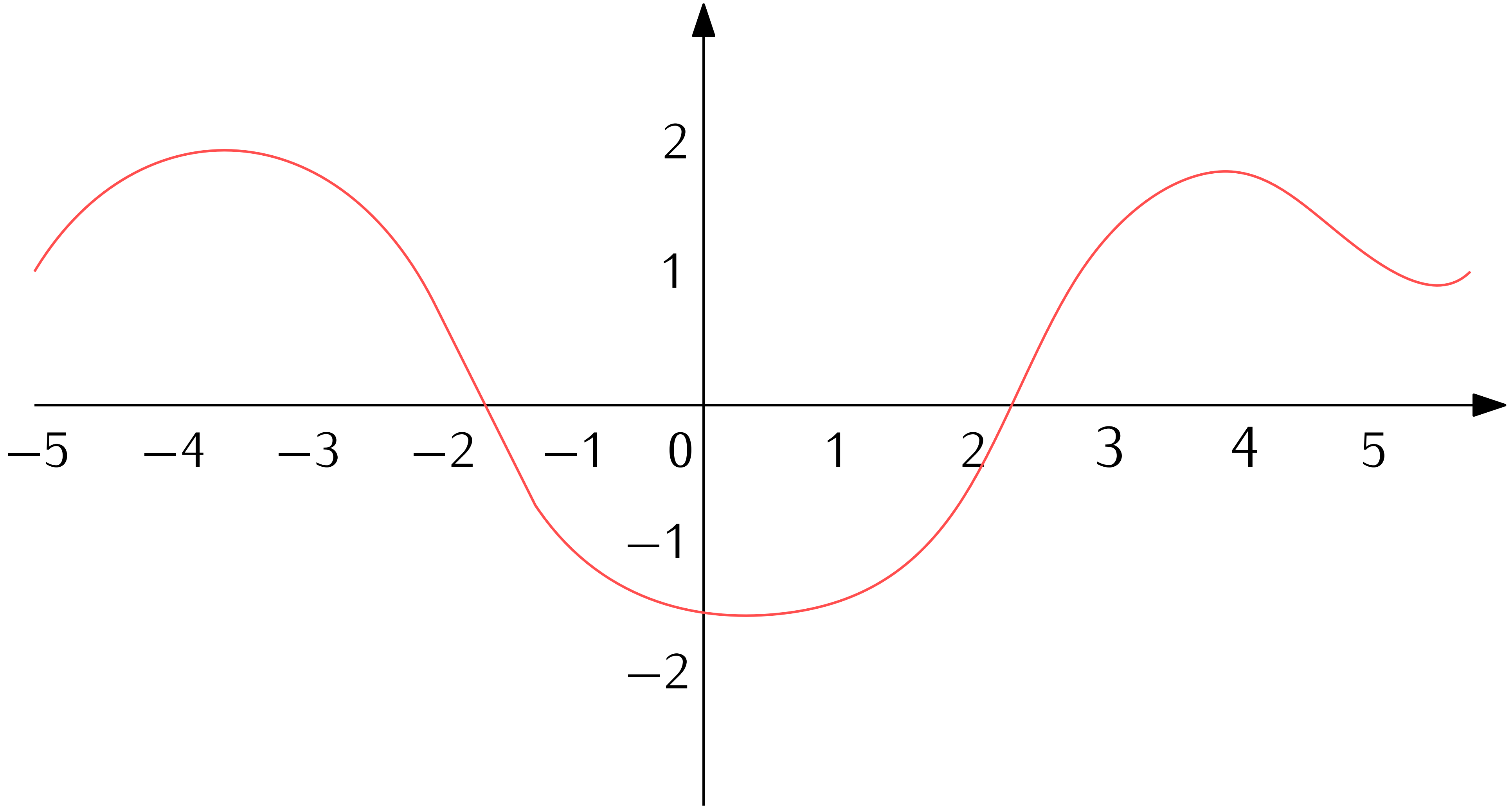
$f \subseteq \mathbb{R} \times \mathbb{R}$



Question. Is this a function?

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

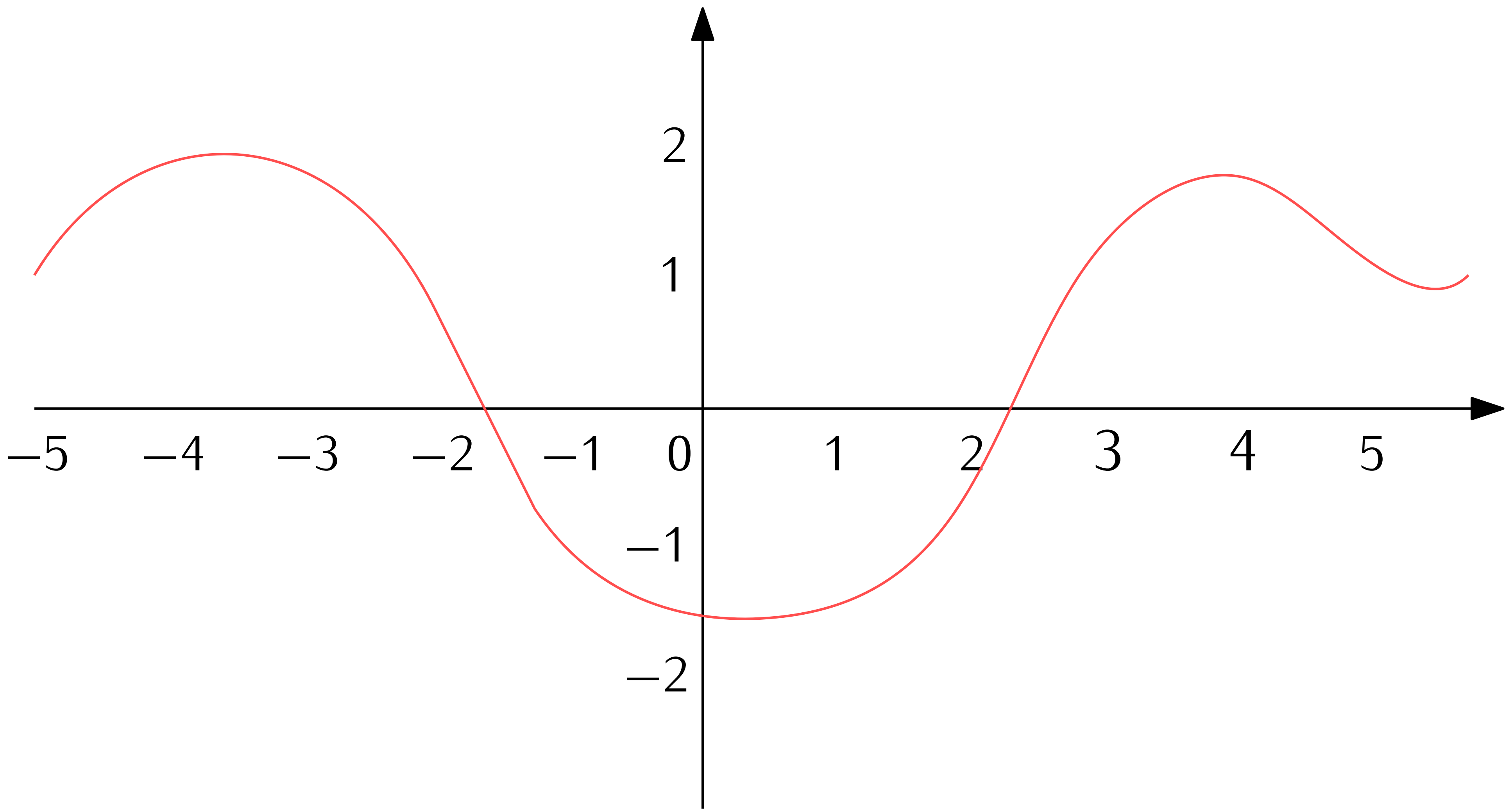
$f \subseteq \mathbb{R} \times \mathbb{R}$



Question. Is this a function?

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

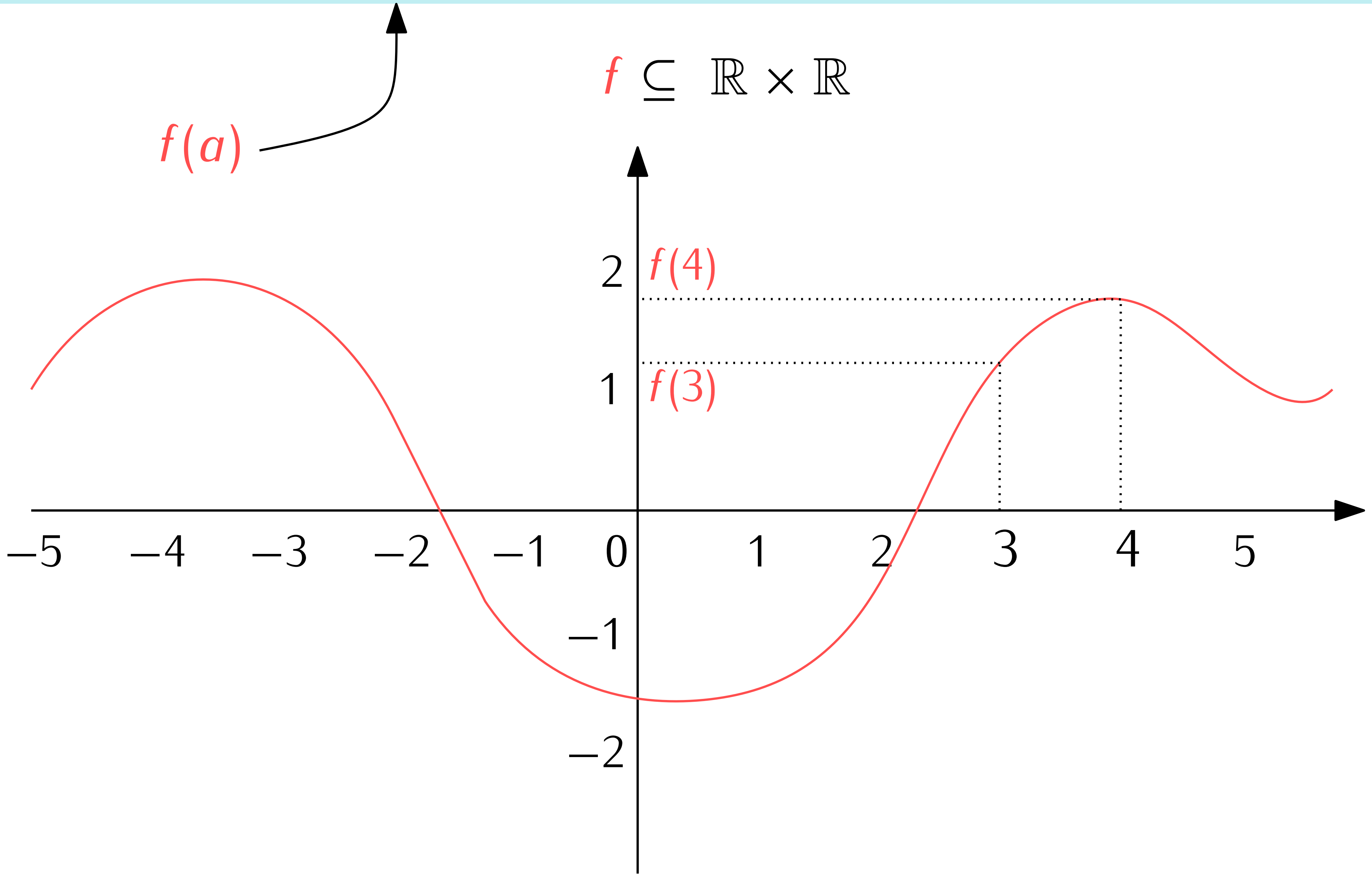
$f \subseteq \mathbb{R} \times \mathbb{R}$



Question. Is this a function?

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

Definition. A function $f\colon A \to B$ 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?

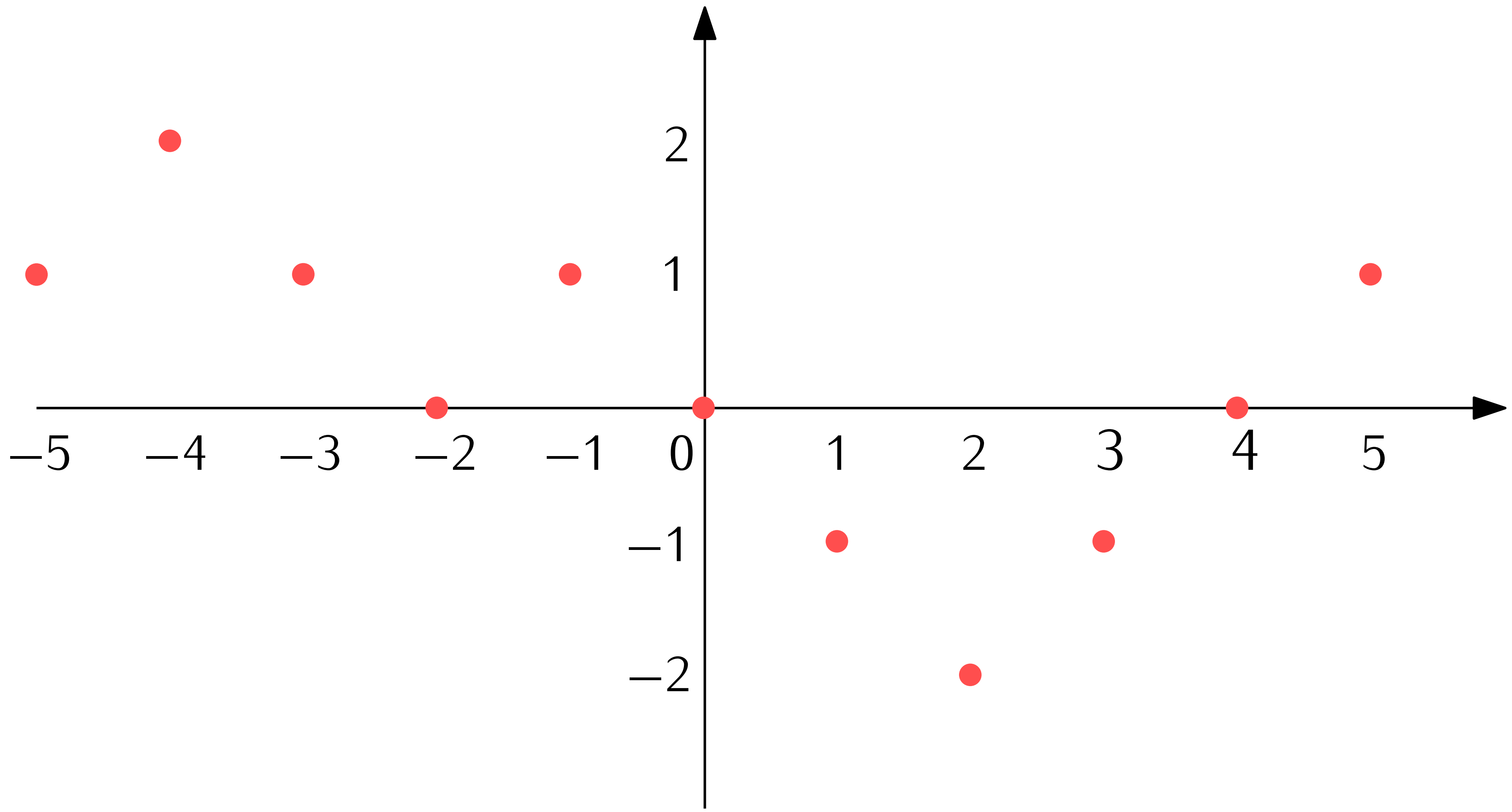
Remark. The definition corresponds to the idea of a "graph of a function".

Definition. A function $f\colon A \to B$ 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?

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

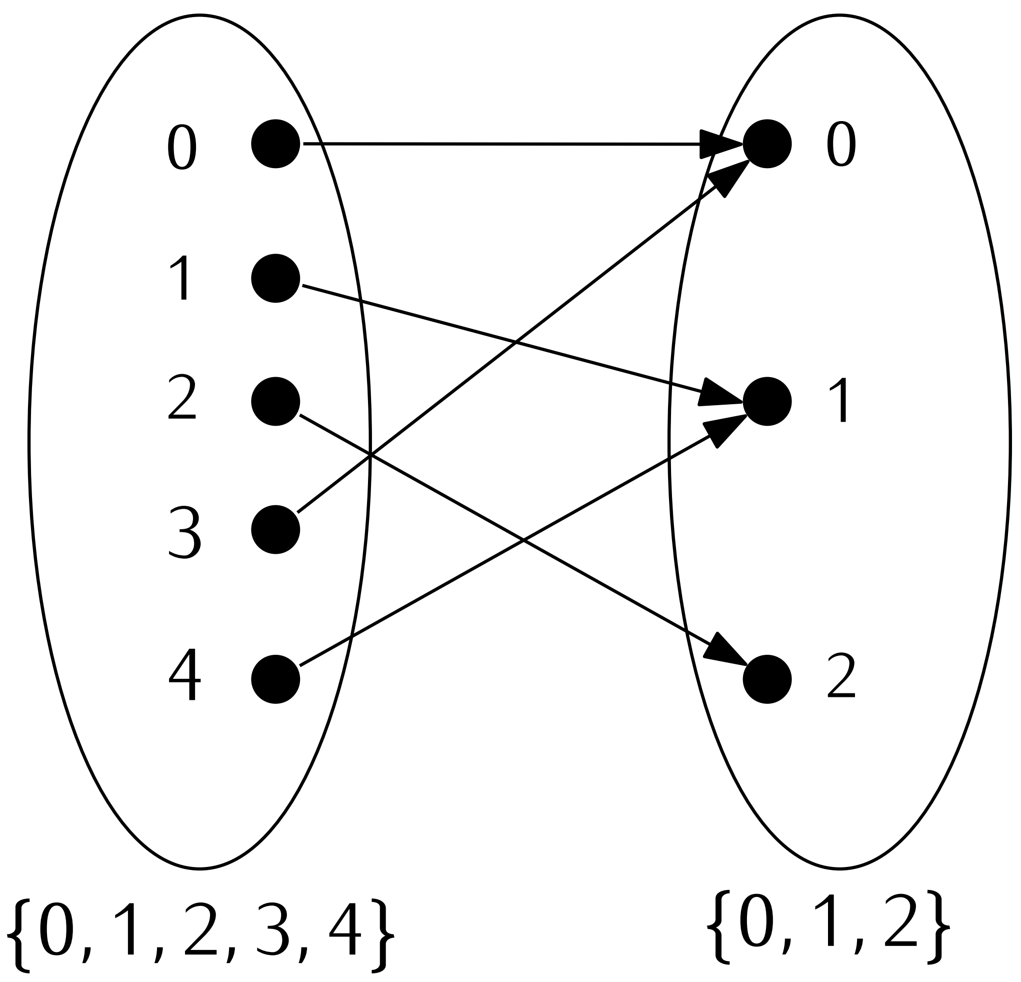
In discrete maths, we don't talk about $\mathbb{R}$! But sets like $\mathbb{N}, \mathbb{Z}, \{0, 2, 4\}, \dots$
How do we draw functions with such sets?



A function $f\colon \mathbb{Z} \to \{-2, -1, 0, 1, 2\}$

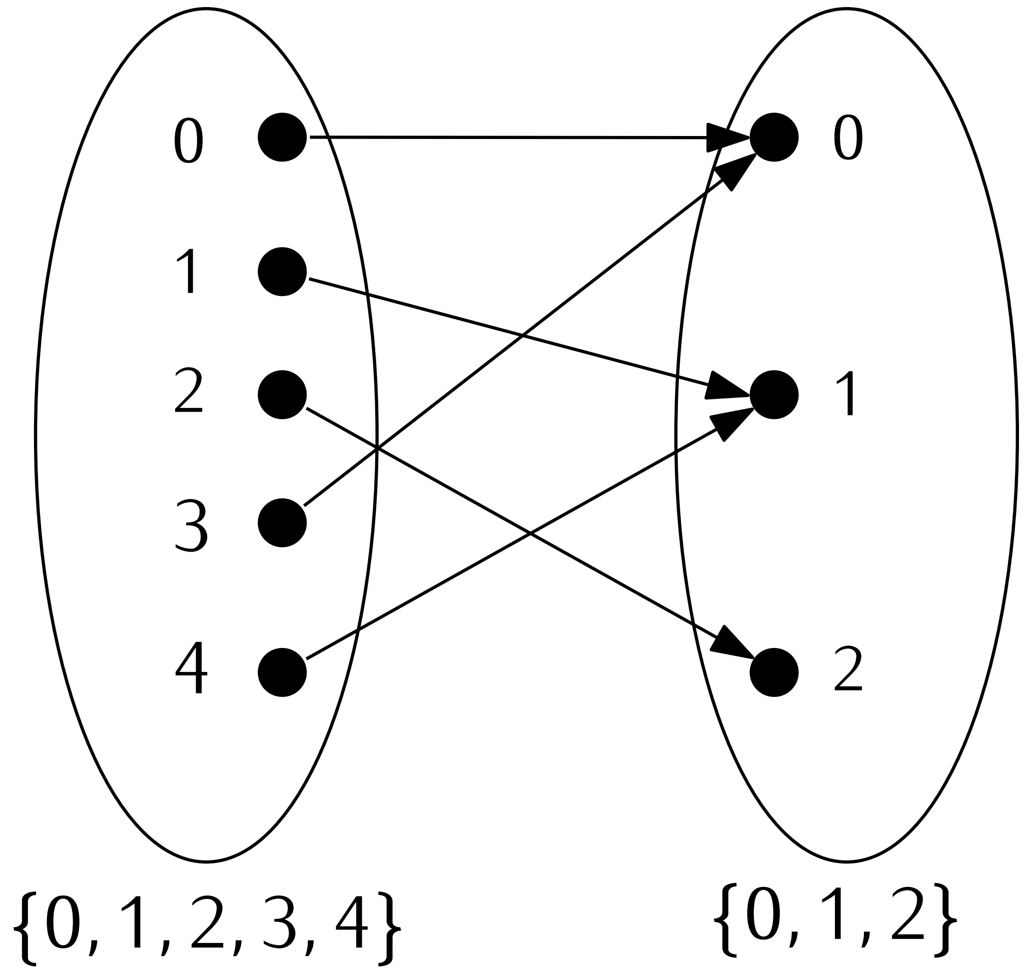
Definition. A function $f\colon A \to B$ is a set $f \subseteq A \times B$ such that for every $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

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



Definition. A function $f\colon A \to B$ 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 $\mathbb{N}, \mathbb{Z}, \{0, 2, 4\}, \ldots$
How do we draw functions with such sets?



This represents the function

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

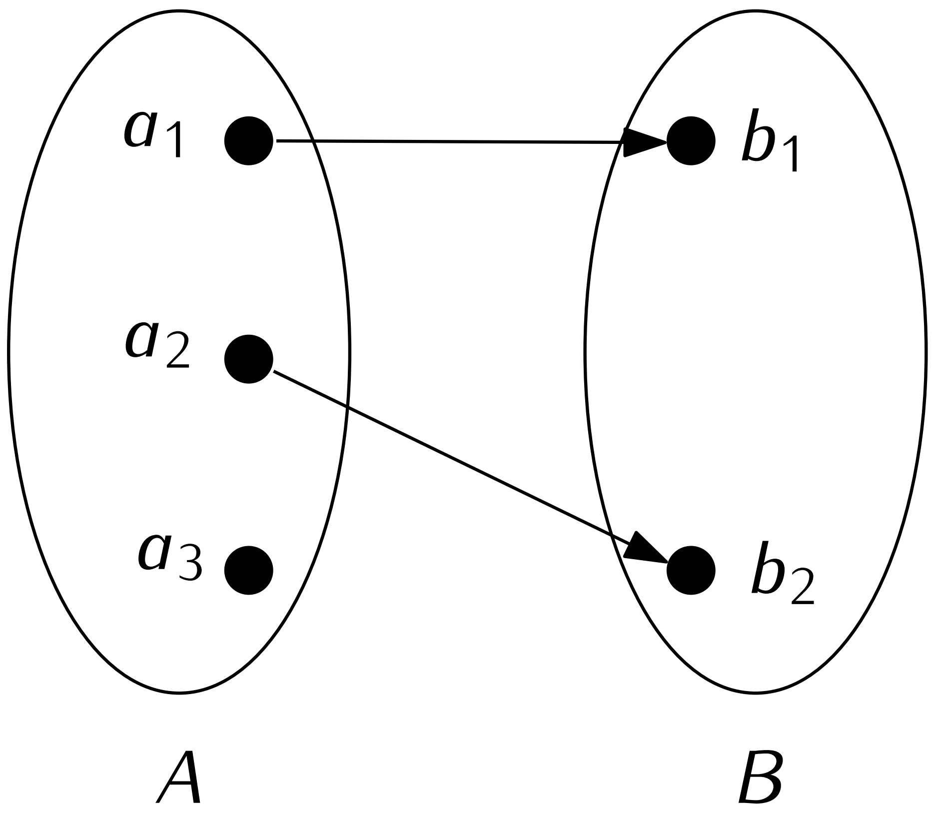
Definition. A function $f\colon A \to B$ is a set $f \subseteq A \times B$ such that for every $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

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

Definition. A function $f\colon A \to B$ 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 $A \to B$:

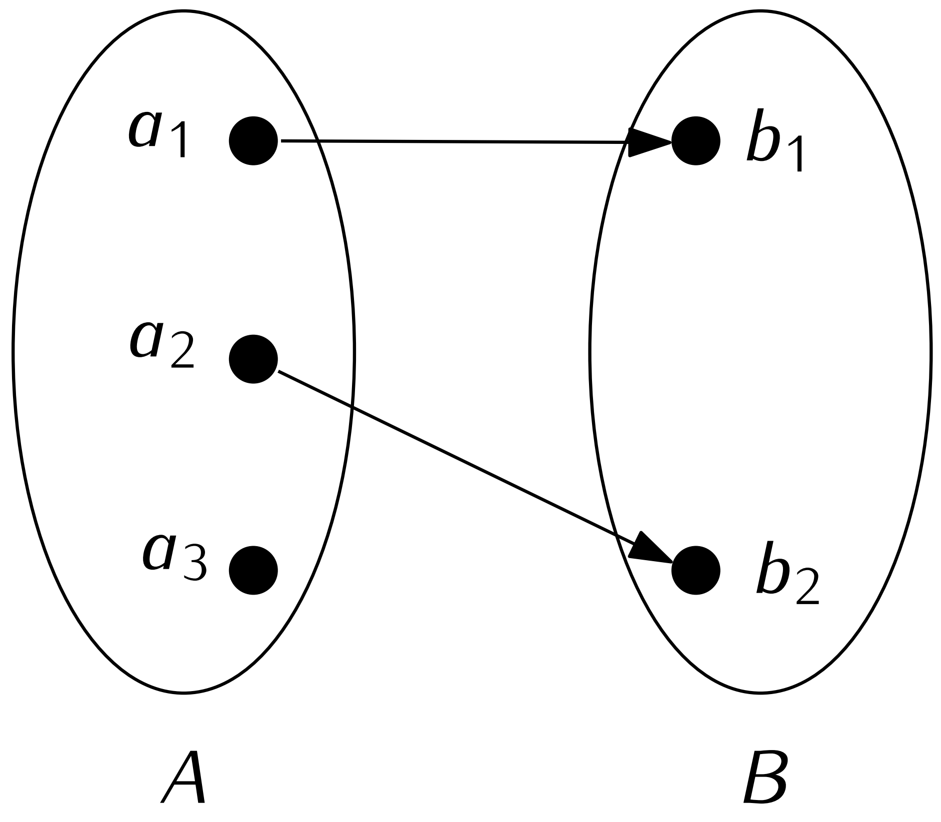
- It could be that for some $a \in A$, there are no $b \in B$ such that $(a, b) \in f$

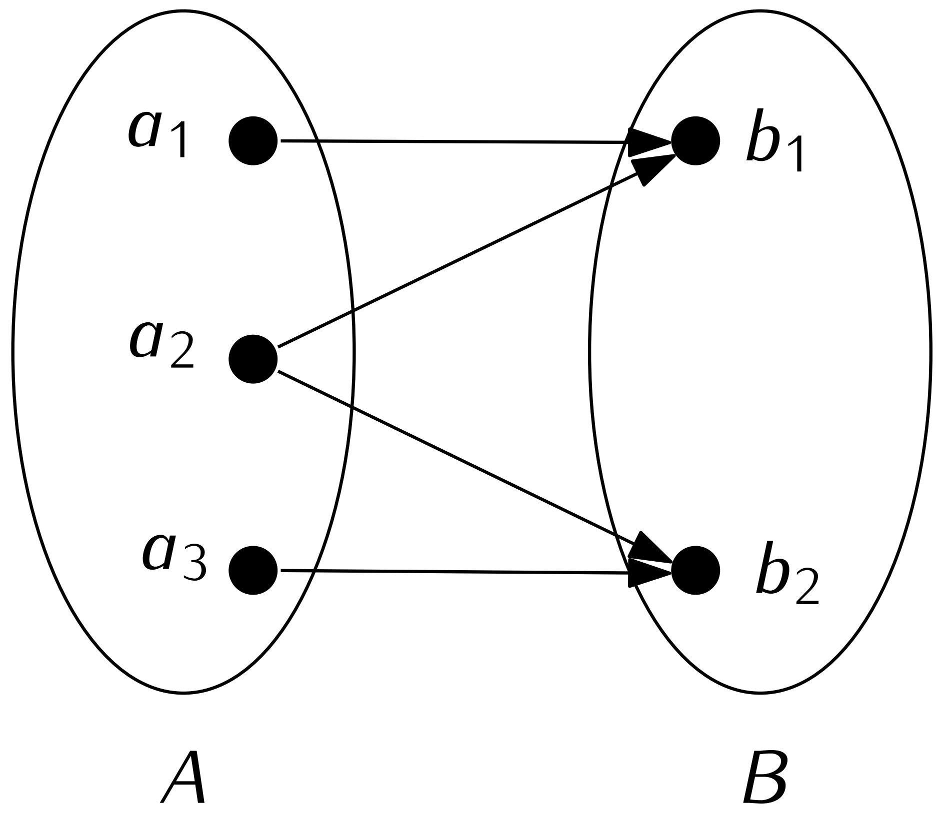


Definition. A function $f\colon A \to B$ is a set $f \subseteq A \times B$ such that for every $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

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

- 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 $(a, b') \in f$

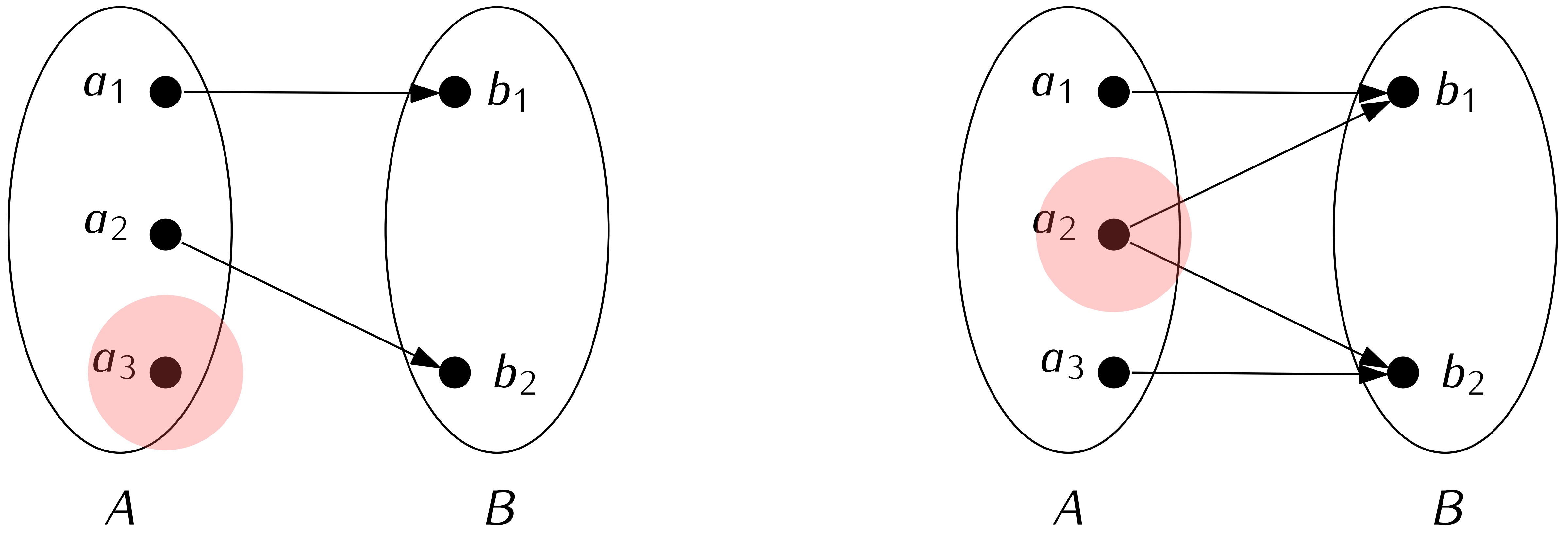




Definition. A function $f\colon A \to B$ is a set $f \subseteq A \times B$ such that for every $a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

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

- 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 $f\colon A \to B$ 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 $A \to B$:

- 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 $\{1, 2, 3\} \to \{1, 2\}$?

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

- Functions in programming languages:

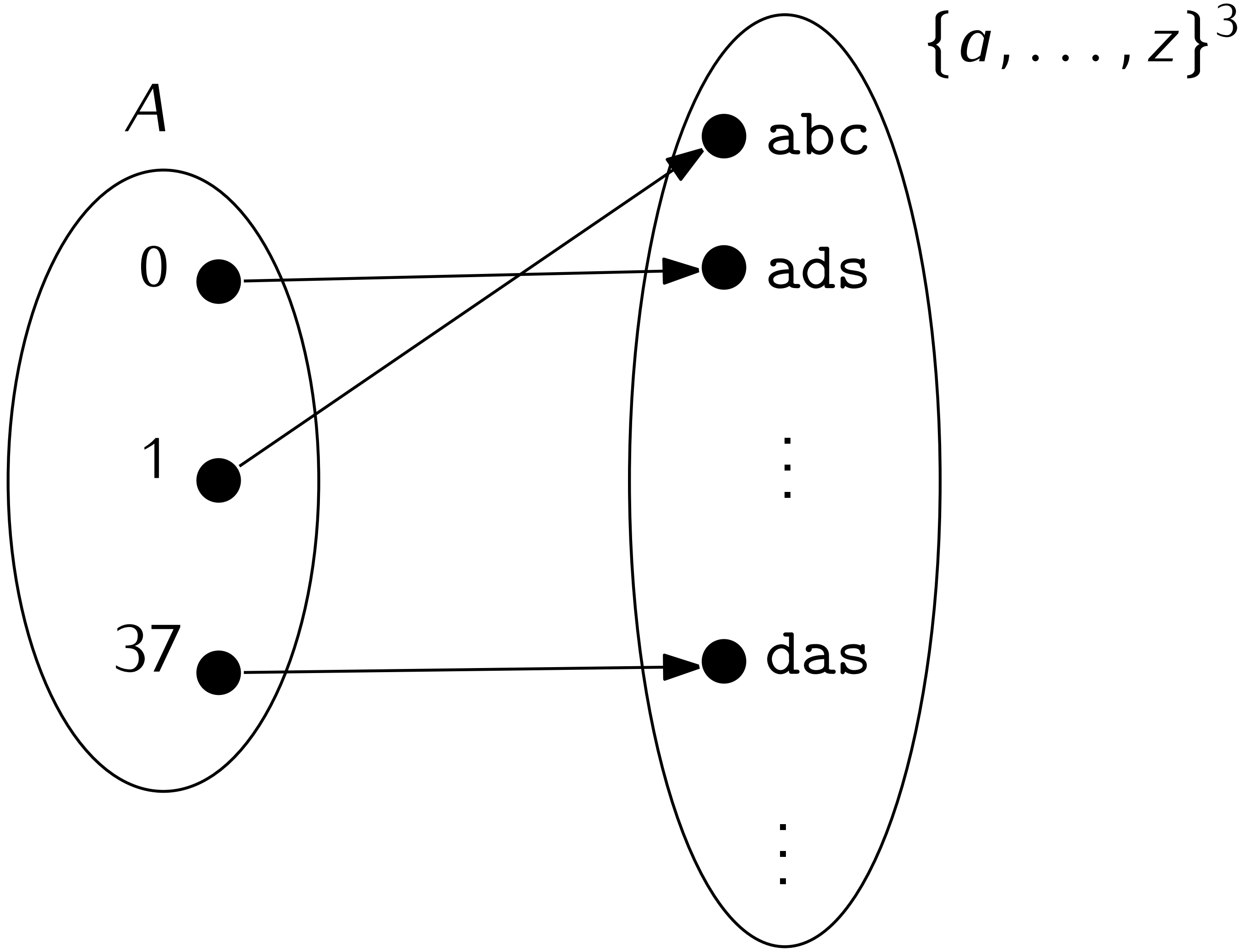
```
def Collatz(x: int) -> int:
    if x%2 == 0:
        return x/2
    else:
        return 3*x+1
```

- 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: $\mathtt{ASCIIencoding}\colon \mathtt{ASCII} \to \{0,1\}^8$

$$\mathtt{ASCIIencoding}('a') = 01100001$$
$$\mathtt{ASCIIencoding}('=') = 00111101$$

- 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:

$\mathtt{ASCIIencoding}\colon \mathtt{ASCII} \to \{0,1\}^8$

$\mathtt{ASCIIencoding}('a') = 01100001$

$\mathtt{ASCIIencoding}('=') = 00111101$

$\mathtt{UTF8encoding}\colon \mathtt{UTF8} \to \{0,1\}^{48}$

bit-strings of length 48

6 bytes

- 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: $\texttt{ASCIIencoding}\colon \texttt{ASCII} \to \{0,1\}^8$ $\texttt{UTF8encoding}\colon \texttt{UTF8} \to \{0,1\}^{48}$

$\texttt{ASCIIencoding}('a') = 01100001$
$\texttt{ASCIIencoding}('=') = 00111101$

bit-strings of length 48
6 bytes

- Encryption: $\texttt{EncryptionScheme}\colon \texttt{ClearText} \to \texttt{EncryptedText}$

- 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: $\mathtt{ASCIIencoding}\colon \mathtt{ASCII} \to \{0,1\}^8$ $\mathtt{UTF8encoding}\colon \mathtt{UTF8} \to \{0,1\}^{48}$

$\mathtt{ASCIIencoding}('a') = 01100001$
$\mathtt{ASCIIencoding}('=') = 00111101$

bit-strings of length 48
6 bytes

- Encryption: $\mathtt{EncryptionScheme}\colon \mathtt{ClearText} \to \mathtt{EncryptedText}$
- Hash functions: MD5, SHA-1, SHA-256,...

- 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: $\texttt{ASCIIencoding}\colon \texttt{ASCII} \to \{0,1\}^8$ $\qquad$ $\texttt{UTF8encoding}\colon \texttt{UTF8} \to \{0,1\}^{48}$

$\texttt{ASCIIencoding}('a') = 01100001$
$\texttt{ASCIIencoding}('=') = 00111101$

bit-strings of length 48
6 bytes

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

- Definition; be able to determine if a given set $f \subseteq A \times B$ is a function or not

- 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

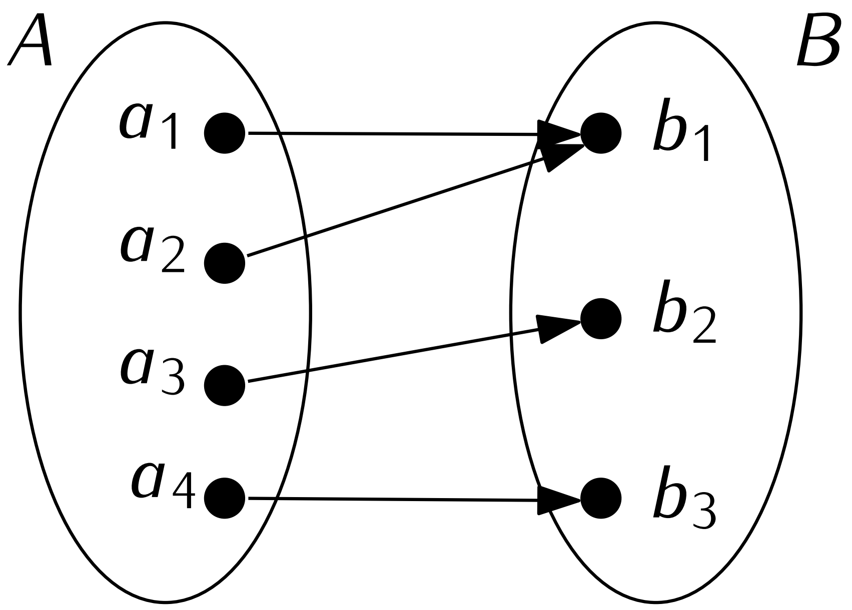
coming up

Definition. A function $f\colon A \to B$ 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 $f(a) = b$.

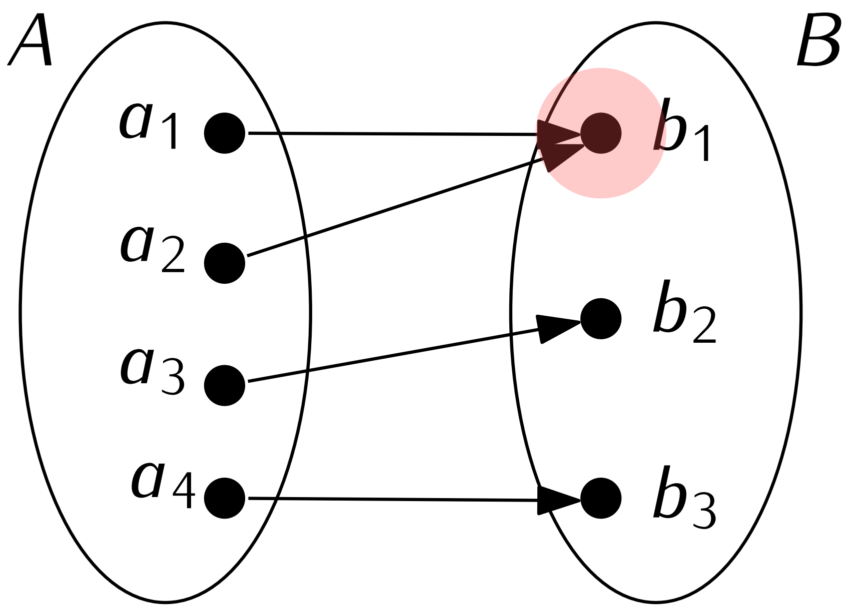
Definition. A function $f\colon A \to B$ is:

- 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 $f(a) = b$.



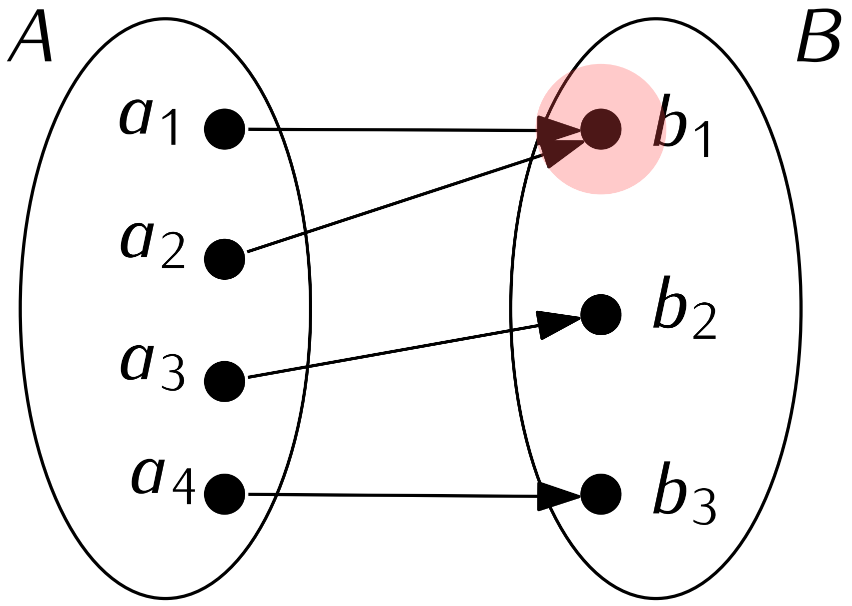
Definition. A function $f\colon A \to B$ is:

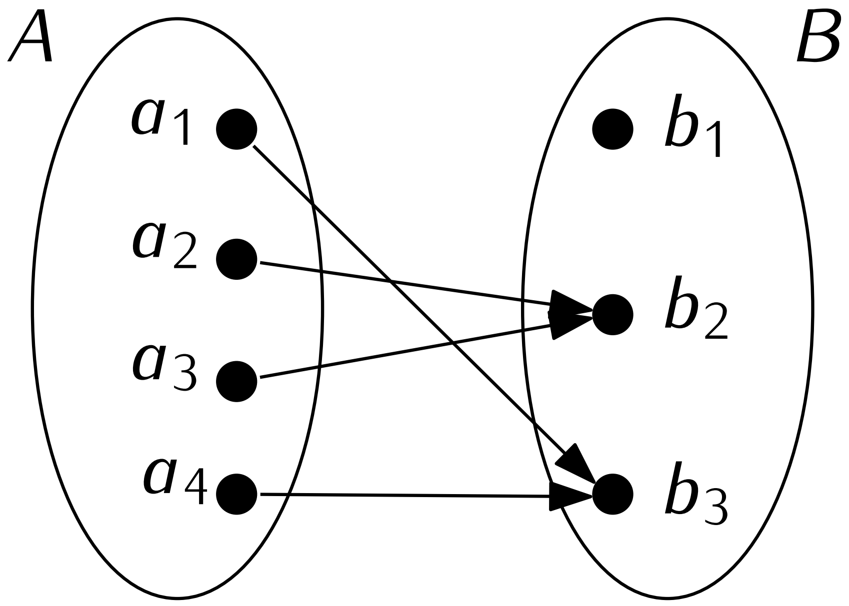
- injective if for all $b \in B$, there is at most one $a \in A$ such that $f(a) = b$,
- surjective if for all $b \in B$, there is at least one $a \in A$ such that $f(a) = b$,
- bijective if for all $b \in B$, there exists exactly one $a \in A$ such that $f(a) = b$.



Definition. A function $f\colon A \to B$ is:

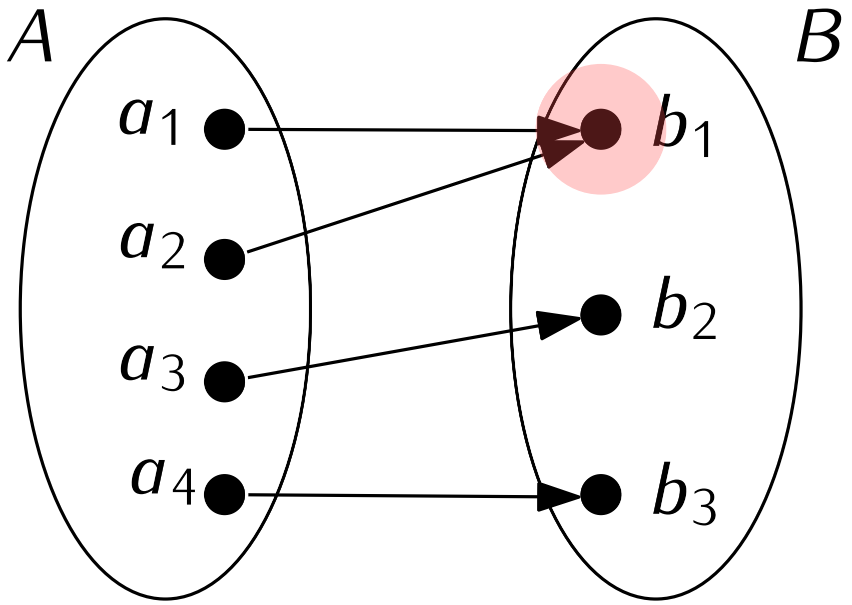
- injective if for all $b \in B$, there is at most one $a \in A$ such that $f(a) = b$,
- surjective if for all $b \in B$, there is at least one $a \in A$ such that $f(a) = b$,
- bijective if for all $b \in B$, there exists exactly one $a \in A$ such that $f(a) = b$.

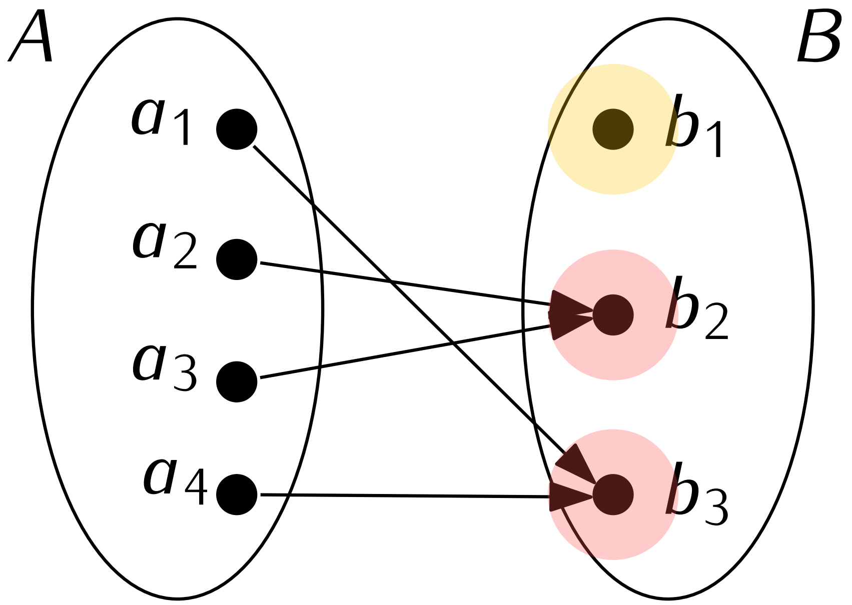




Definition. A function $f\colon A \to B$ is:

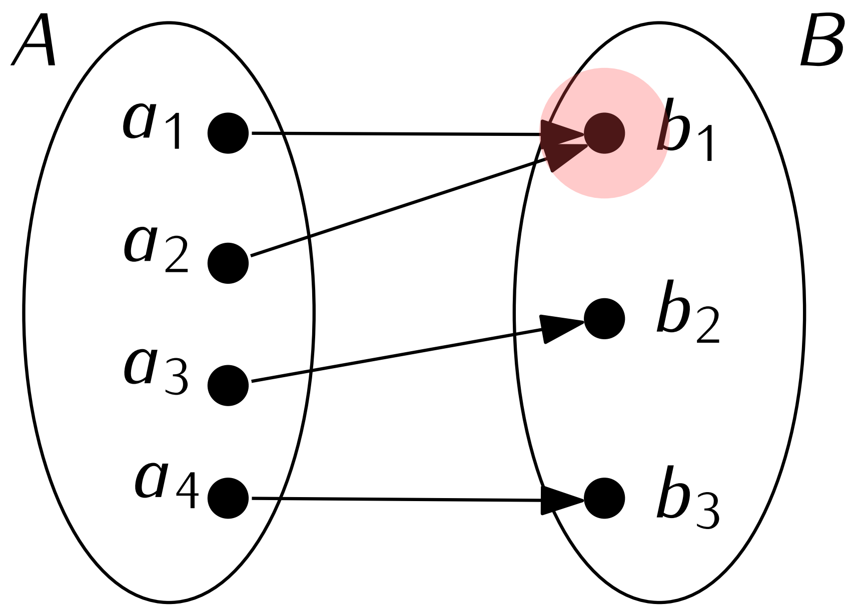
- injective if for all $b \in B$, there is at most one $a \in A$ such that $f(a) = b$,
- surjective if for all $b \in B$, there is at least one $a \in A$ such that $f(a) = b$,
- bijective if for all $b \in B$, there exists exactly one $a \in A$ such that $f(a) = b$.

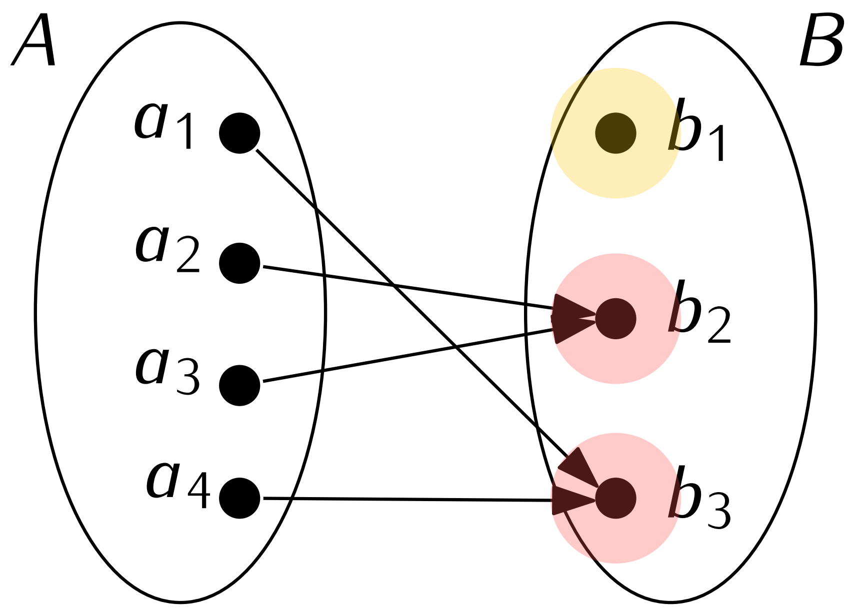


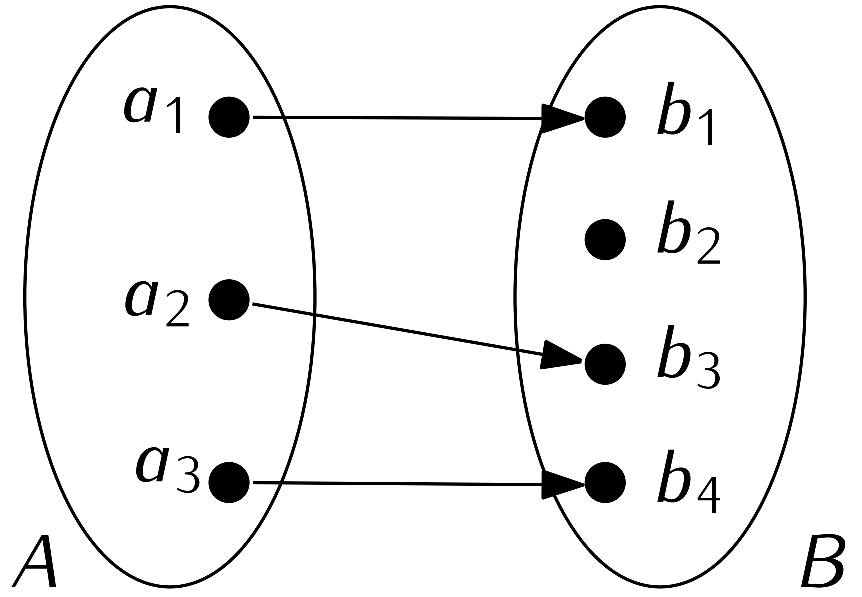


Definition. A function $f\colon A \to B$ is:

- 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 $f(a) = b$.

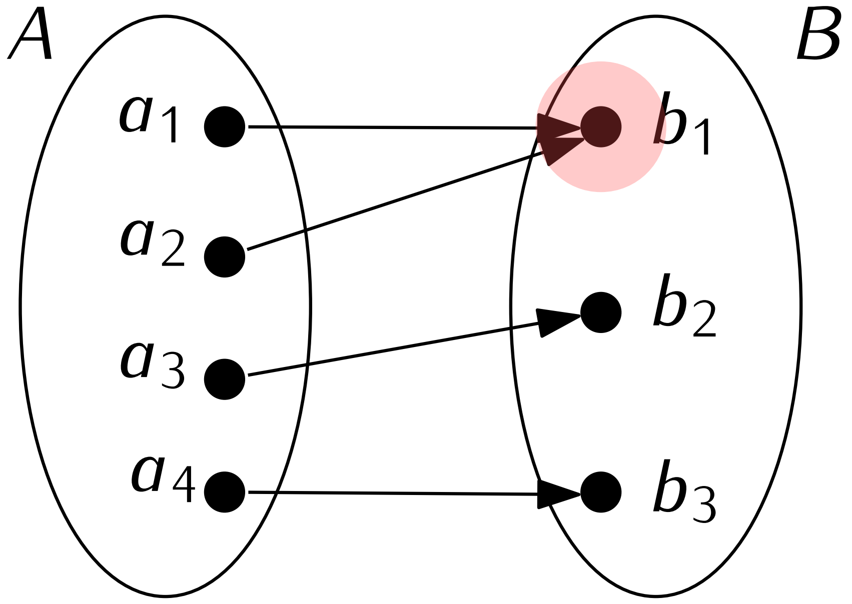


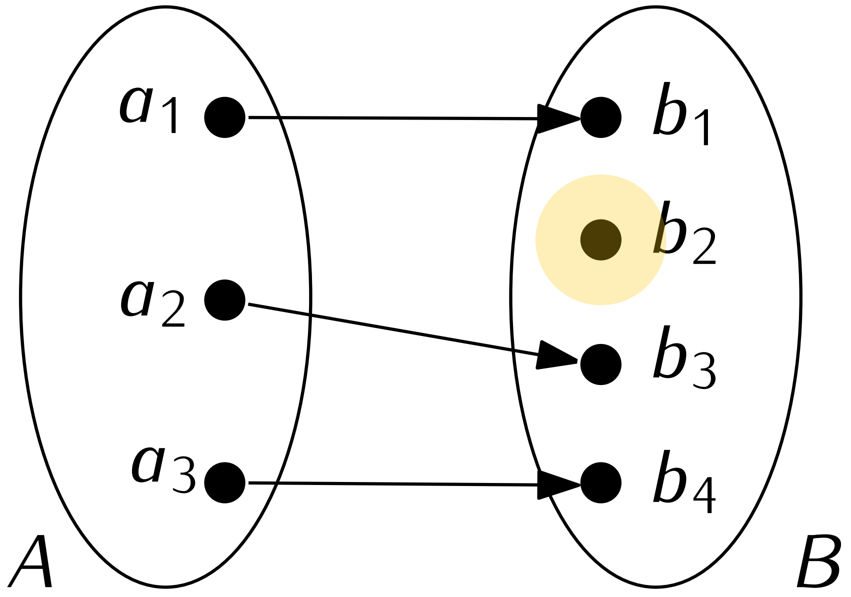


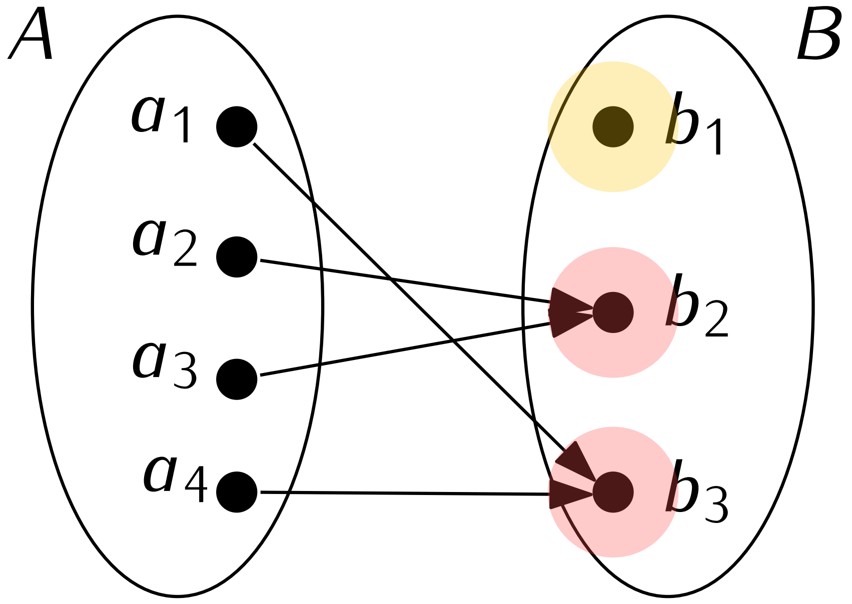


Definition. A function $f\colon A \to B$ is:

- 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 $f(a) = b$.

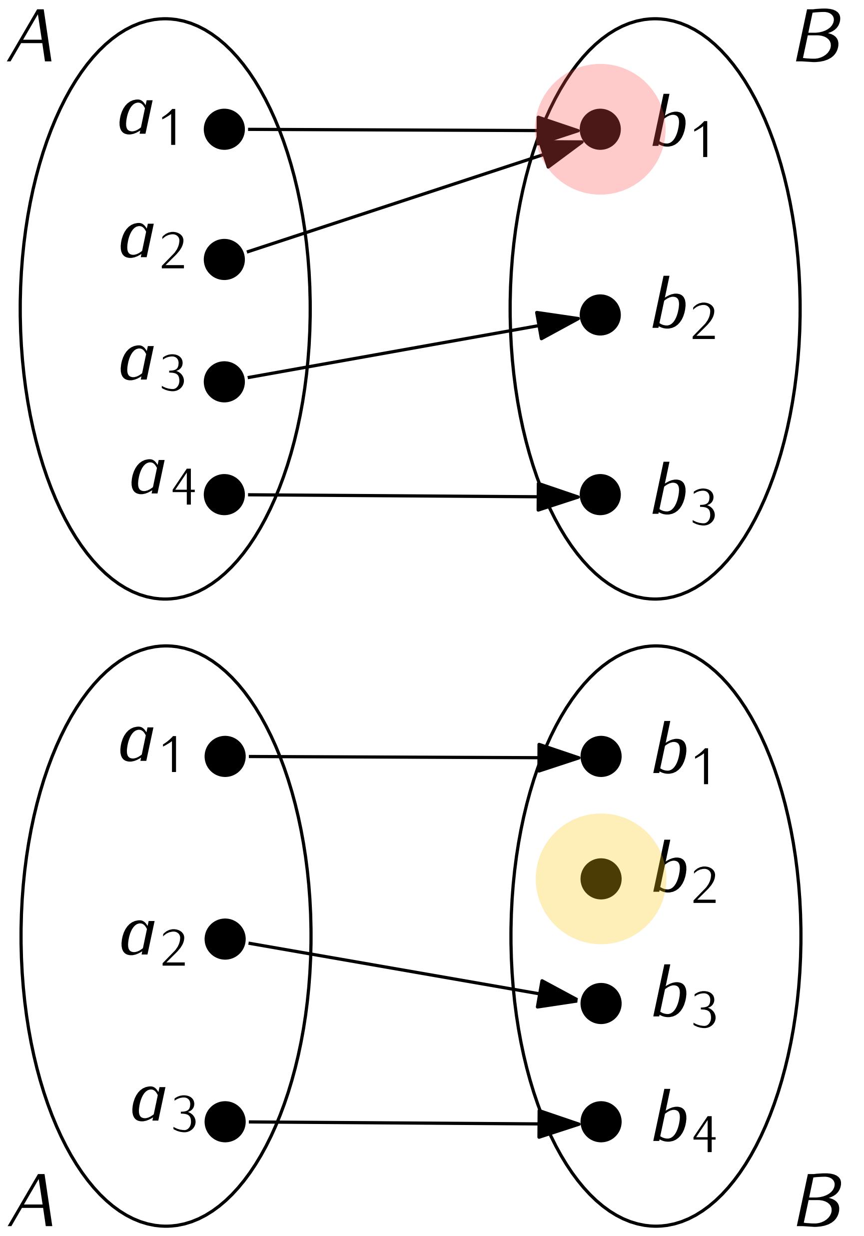






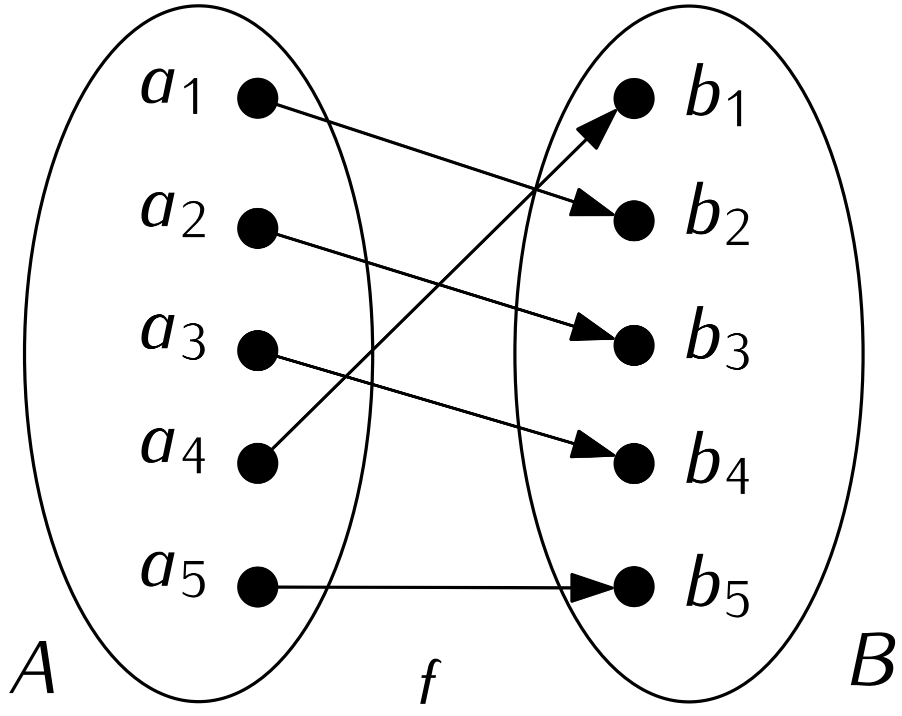
Definition. A function $f\colon A \to B$ is:

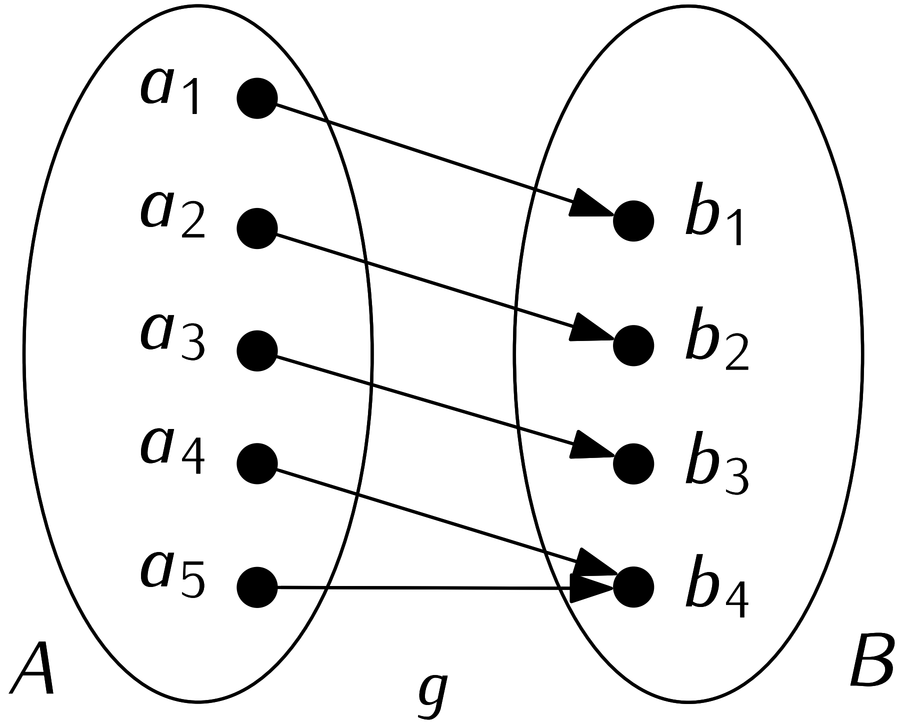
- injective if for all $b \in B$, there is at most one $a \in A$ such that $f(a) = b$,
- surjective if for all $b \in B$, there is at least one $a \in A$ such that $f(a) = b$,
- bijective if for all $b \in B$, there exists exactly one $a \in A$ such that $f(a) = b$.

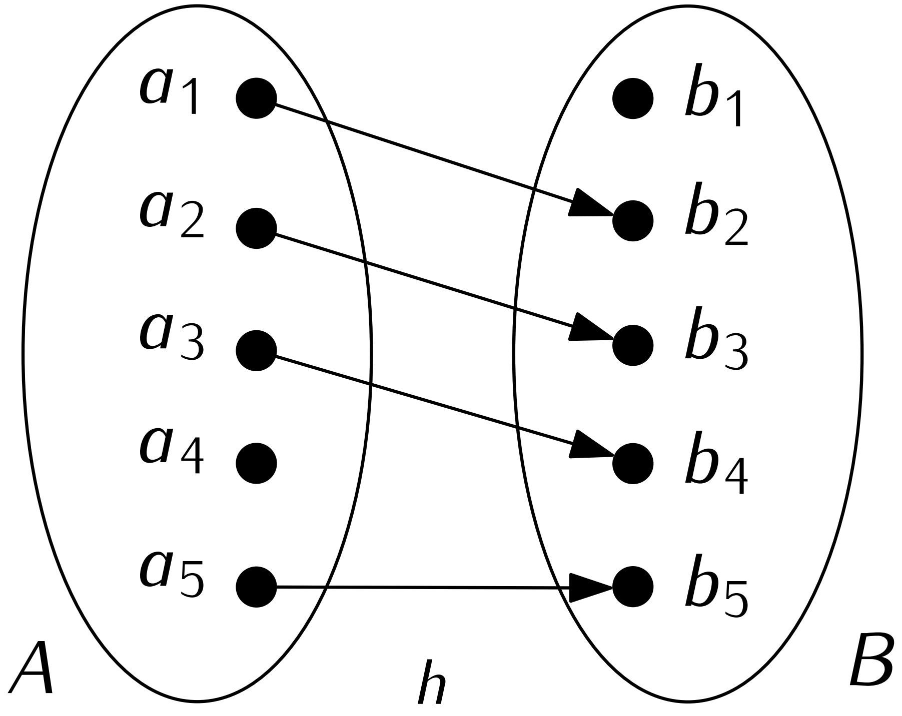


Definition. A function $f\colon A \to B$ is:

- 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 $f\colon A \to B$ 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?

Definition. A function $f\colon A \to B$ 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 $a = a'$.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.

Proof.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.

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

Goal: f is injective

Proof.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.

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

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 $f : A \to B$ 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 $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.
Hypothesis 1: $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 2x + 1$
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 $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.
Hypothesis 1: $f\colon \mathbb{N} \to \mathbb{N}$, $f(x) = 2x + 1$
Hypothesis 2: $2a + 1 = 2a' + 1$

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 $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.
Hypothesis 1: $f\colon \mathbb{N} \to \mathbb{N}$, $f(x) = 2x + 1$
Hypothesis 2: $2a + 1 = 2a' + 1$
Hypothesis 3: $2a = 2a'$

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

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.
Hypothesis 1: $f\colon \mathbb{N} \to \mathbb{N}$, $f(x) = 2x + 1$
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

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x + 1$ is injective.

Notes.
Hypothesis 1: $f\colon \mathbb{N} \to \mathbb{N}$, $f(x) = 2x + 1$
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 $f\colon A \to B$ 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 $f(a) = f(a')$.

Definition. A function $f\colon A \to B$ 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. $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not injective.

Definition. A function $f\colon A \to B$ 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 $f(a) = b$.

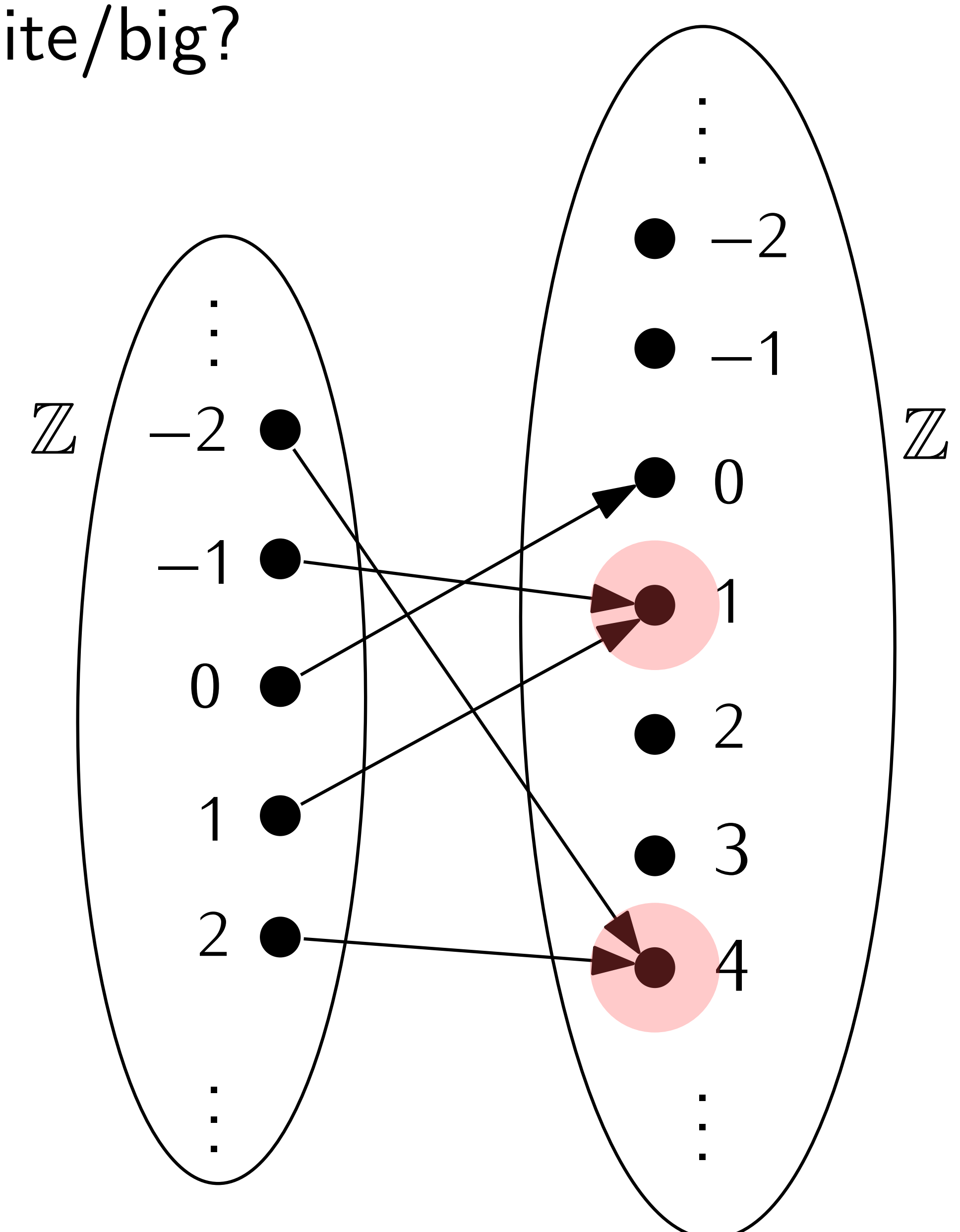
Checking injectivity/surjectivity is "easy" if we can draw the function completely.

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. $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not injective.

Proof. $f(-1) = f(1)$. $\square$



Definition. A function $f\colon A \to B$ 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 $f(a) = b$.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = -x + 3$ is surjective.

Proof.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = -x + 3$ is surjective.

Proof.

1. Let $b \in \mathbb{Z}$.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = -x + 3$ is surjective.

Proof.

1. Let $b \in \mathbb{Z}$.
2. Define $a := -b + 3$.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{Z} \to \mathbb{Z}$ 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 $f\colon A \to B$ 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 $f(a) = b$.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective.

Proof.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective.

Proof.

1. Let $b = -1$.

Definition. A function $f\colon A \to B$ 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 $f\colon \mathbb{N} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective.

Proof.

1. Let $b = -1$.
2. Known fact: $a^2 \geq 0$ for all $a \in \mathbb{N}$

Definition. A function $f\colon A \to B$ 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 $f(a) = b$.

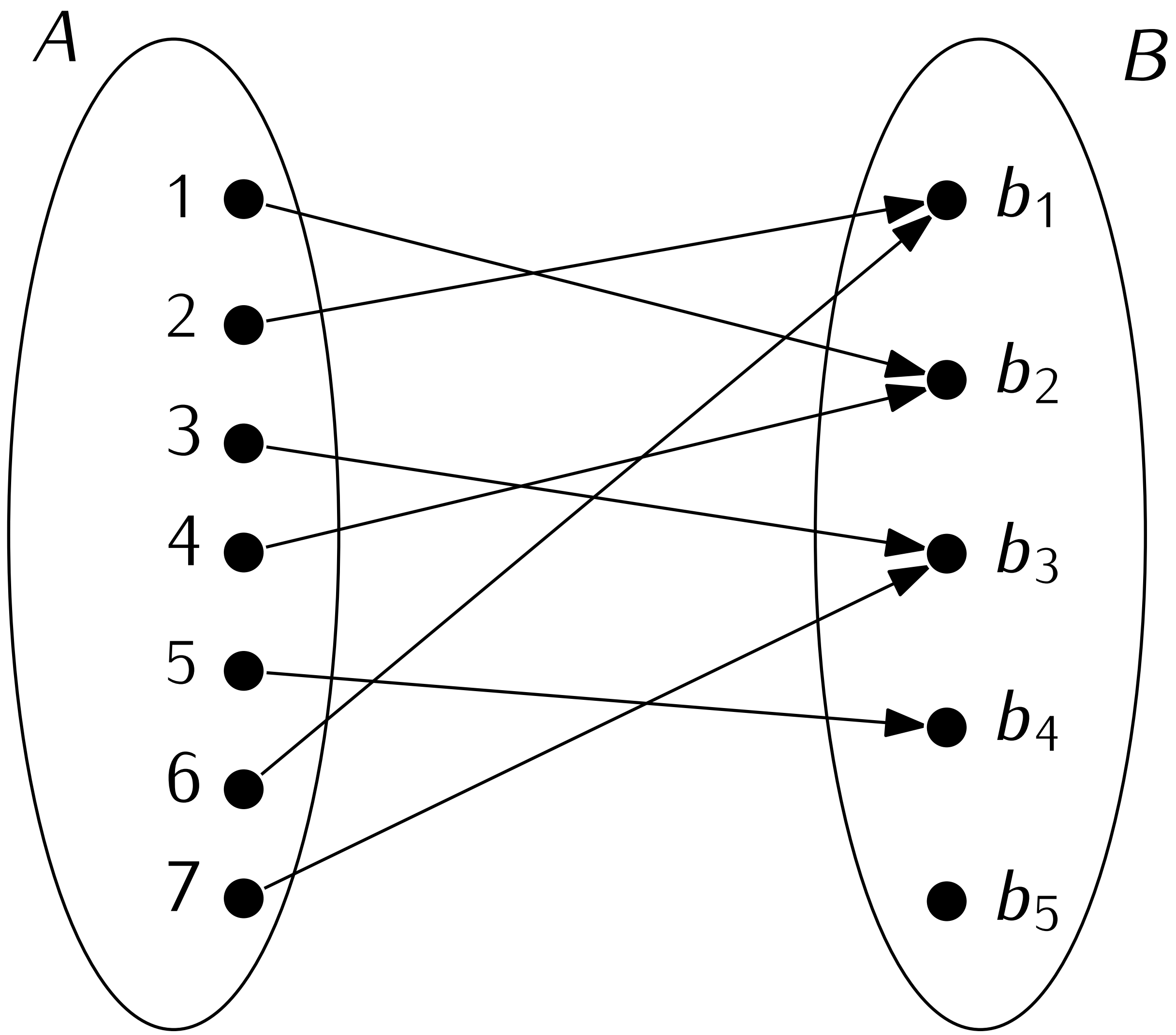
Theorem. The function $f\colon \mathbb{N} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective.

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! $\square$

Definition. Let $f\colon A \to B$ be a function, $A' \subseteq A, B' \subseteq B$.

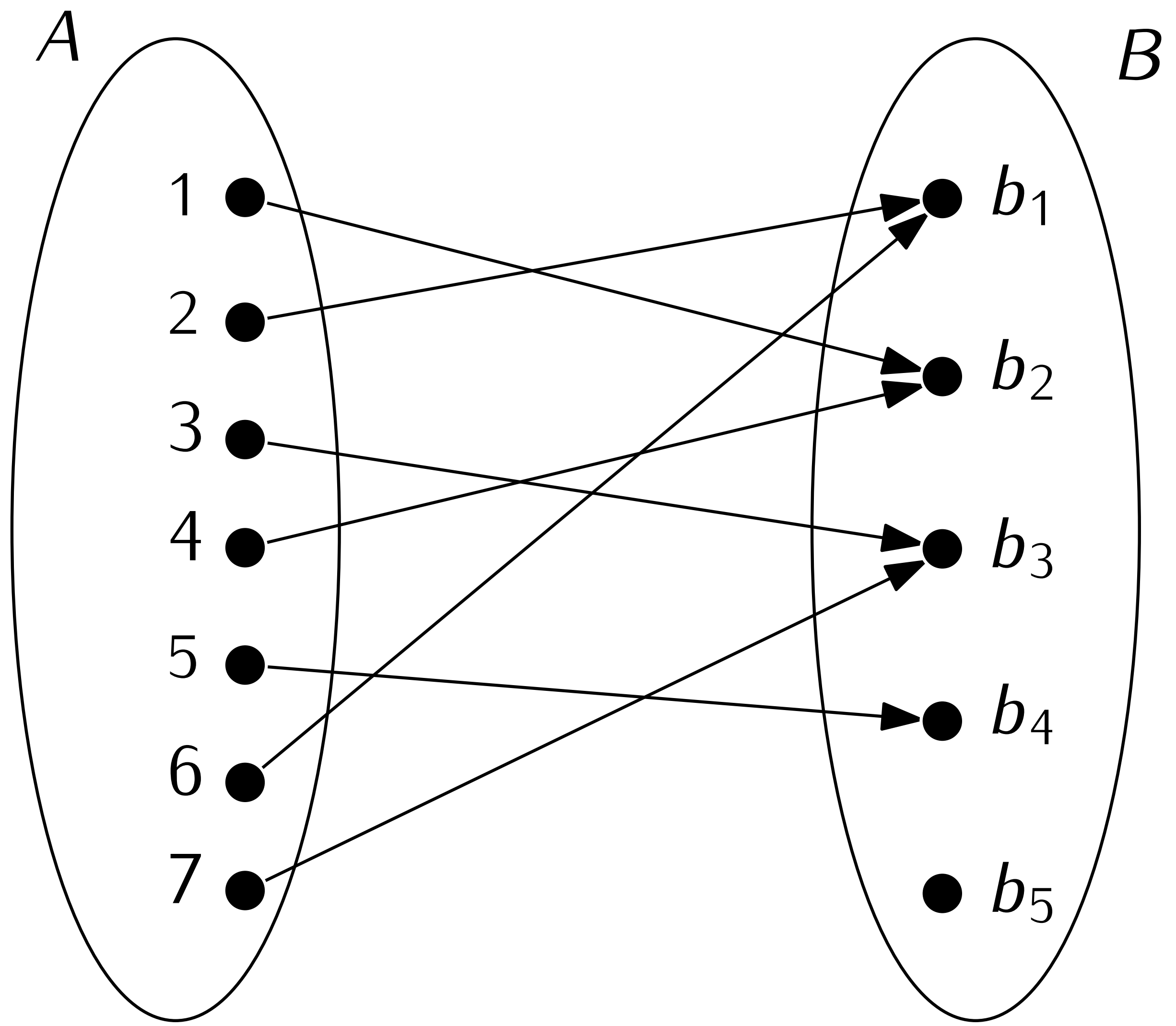
- The image of A' under f: $f[A'] = \{b \in B \mid b = f(a) \text{ for some } a \in A'\}$
- The preimage of B' under f: $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$



Definition. Let $f\colon A \to B$ 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: $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

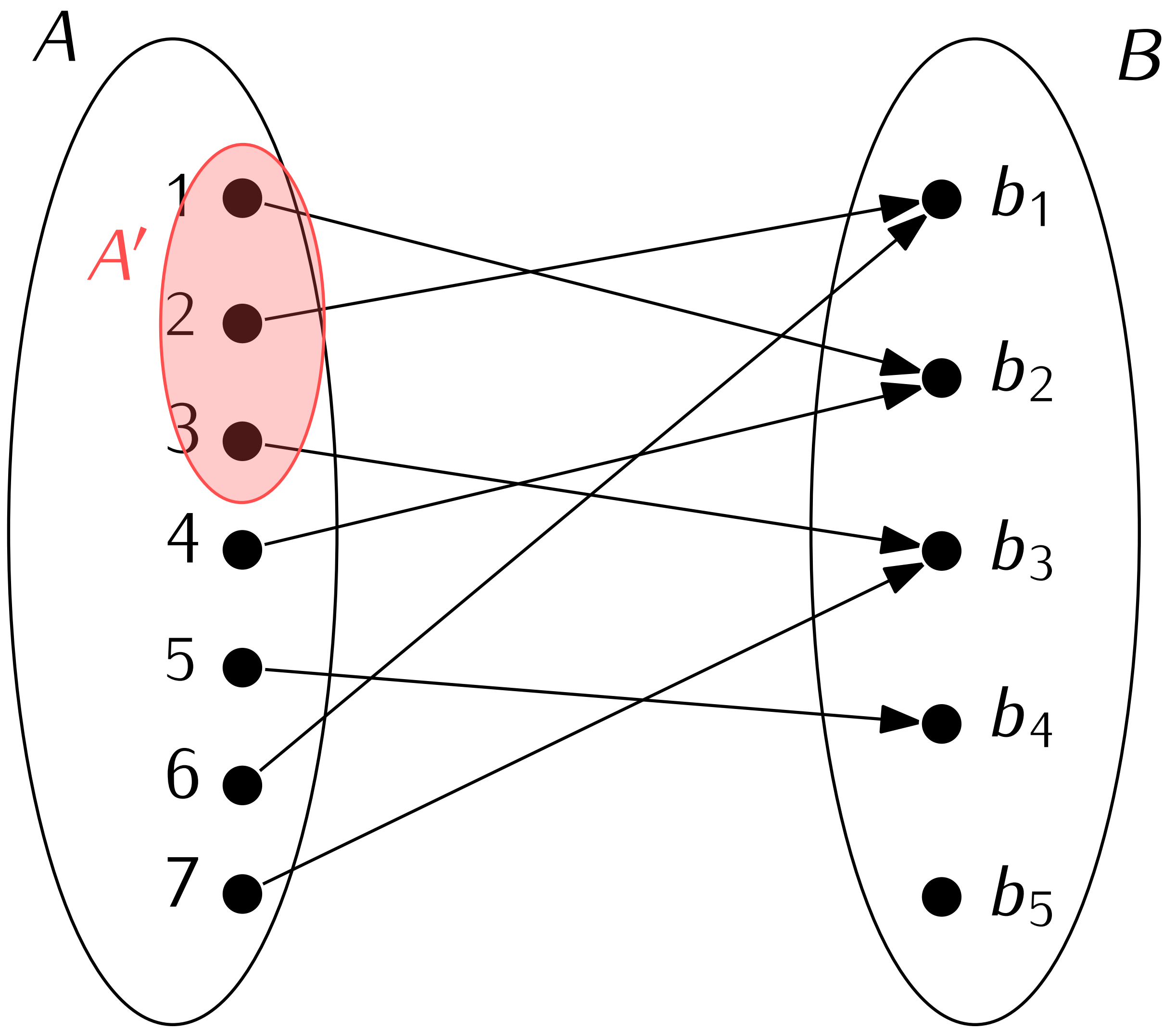
- $f[\{1,2,3\}] =$
- $f^{-1}[\{b_3\}] =$



Definition. Let $f\colon A \to B$ 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: $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

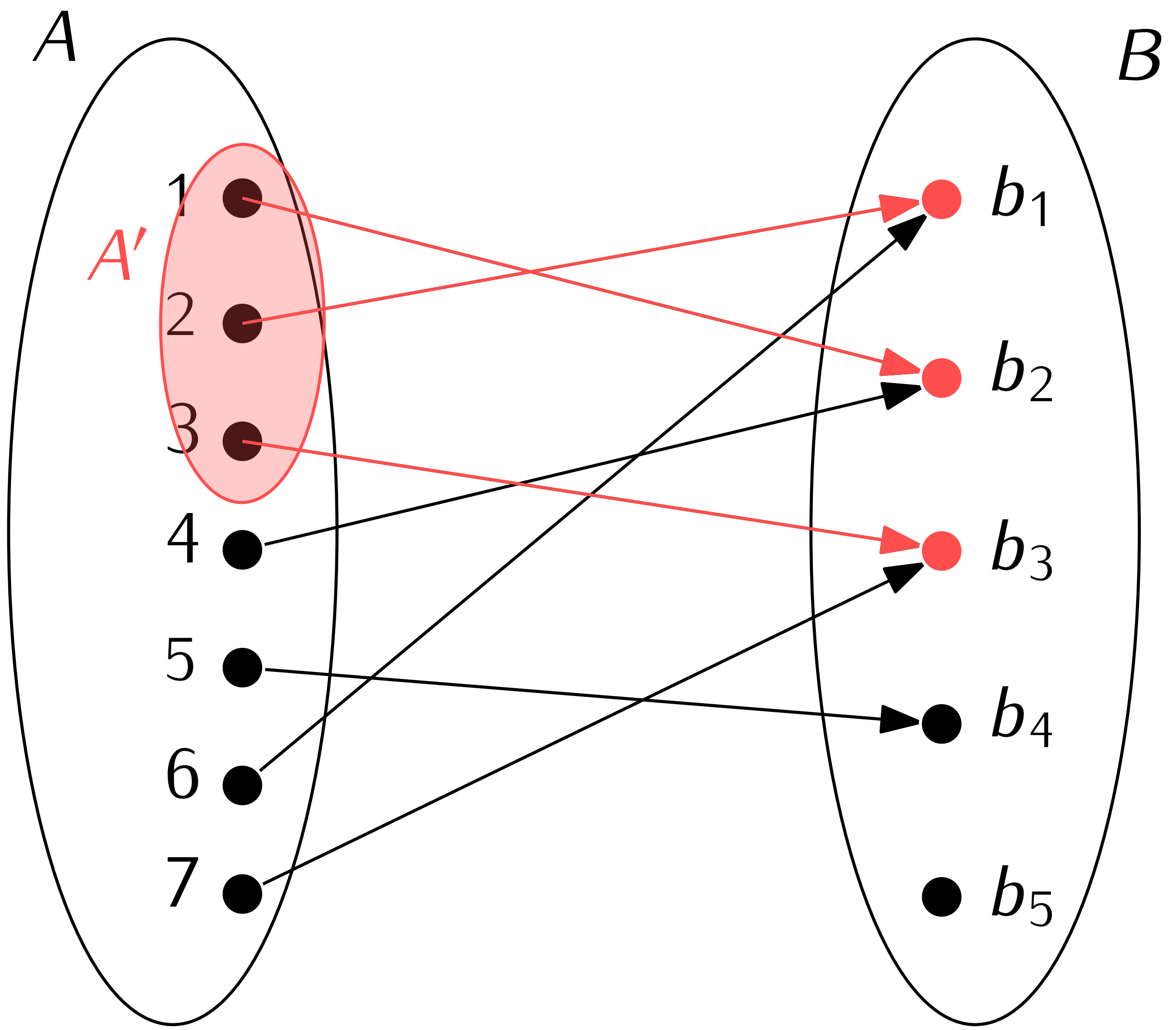
- $f[\{1,2,3\}] =$
- $f^{-1}[\{b_3\}] =$



Definition. Let $f\colon A \to B$ be a function, $A' \subseteq A$, $B' \subseteq B$.

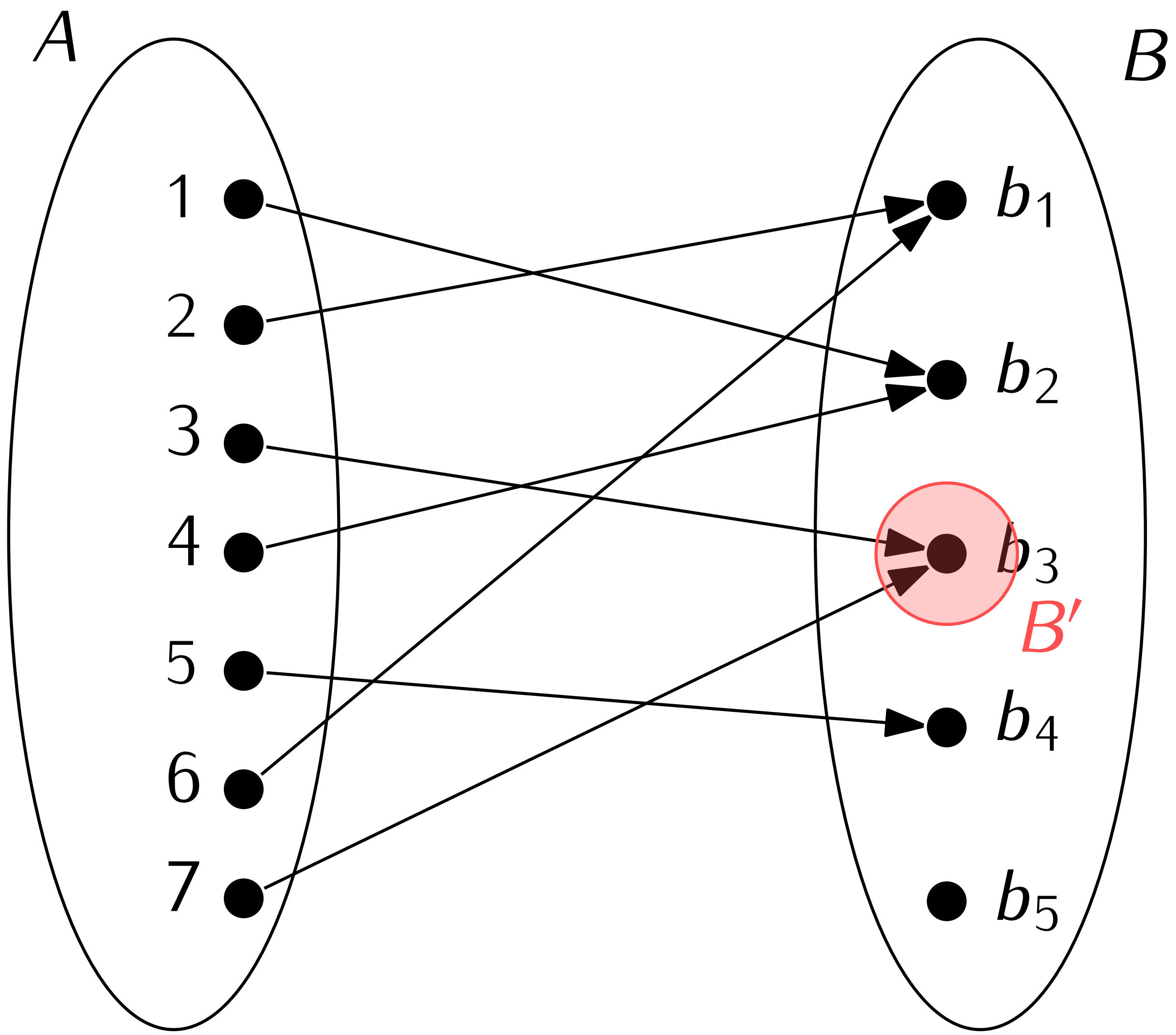
- The image of A' under f: $f[A'] = \{b \in B \mid b = f(a) \text{ for some } a \in A'\}$
- The preimage of B' under f: $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

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



Definition. Let $f\colon A \to B$ 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: $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

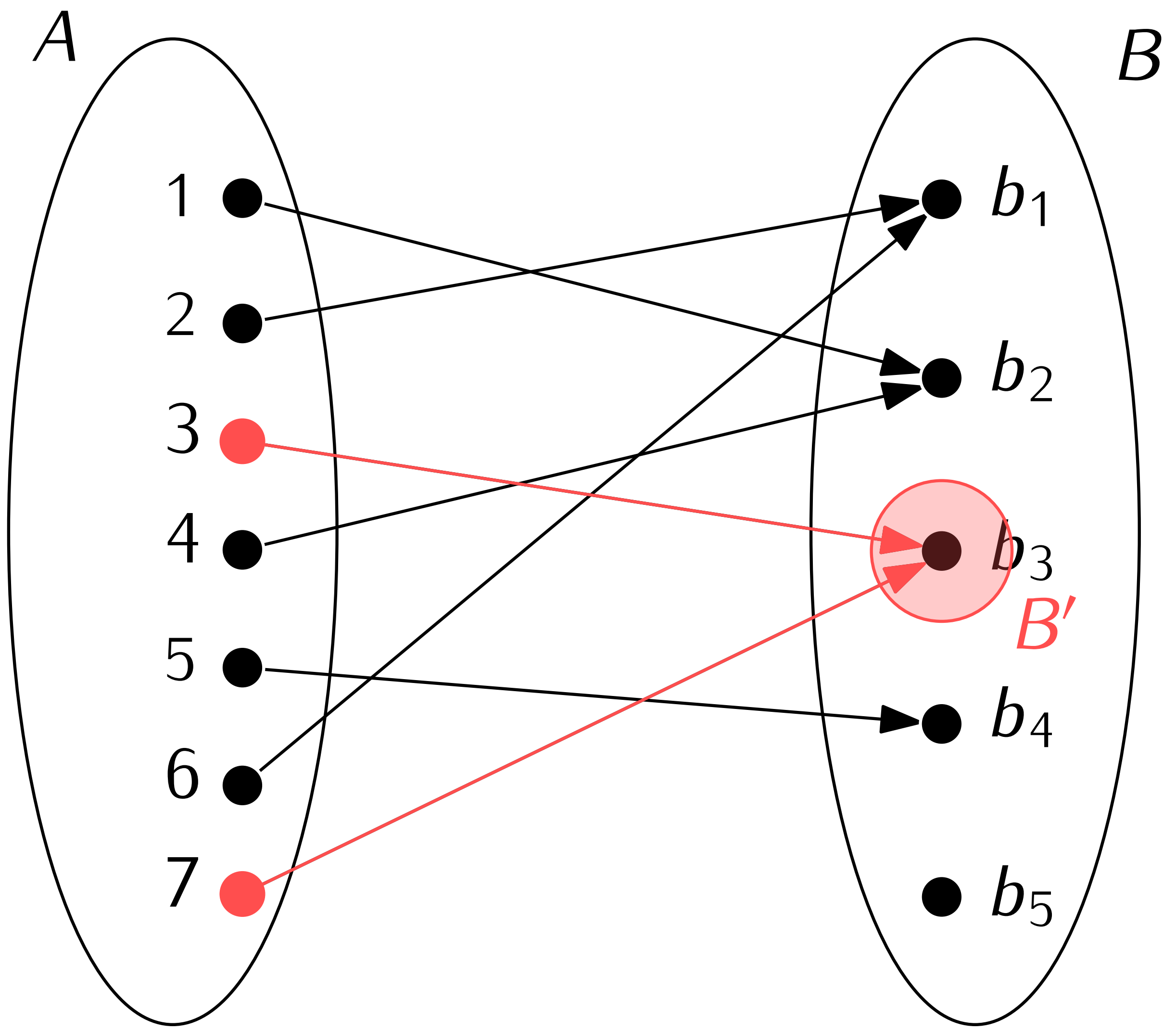
- $f[\{1,2,3\}] = \{b_1, b_2, b_3\}$
- $f^{-1}[\{b_3\}] =$



Definition. Let $f\colon A \to B$ 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: $f^{-1}[B'] = \{a \in A \mid f(a) \in B'\}$

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



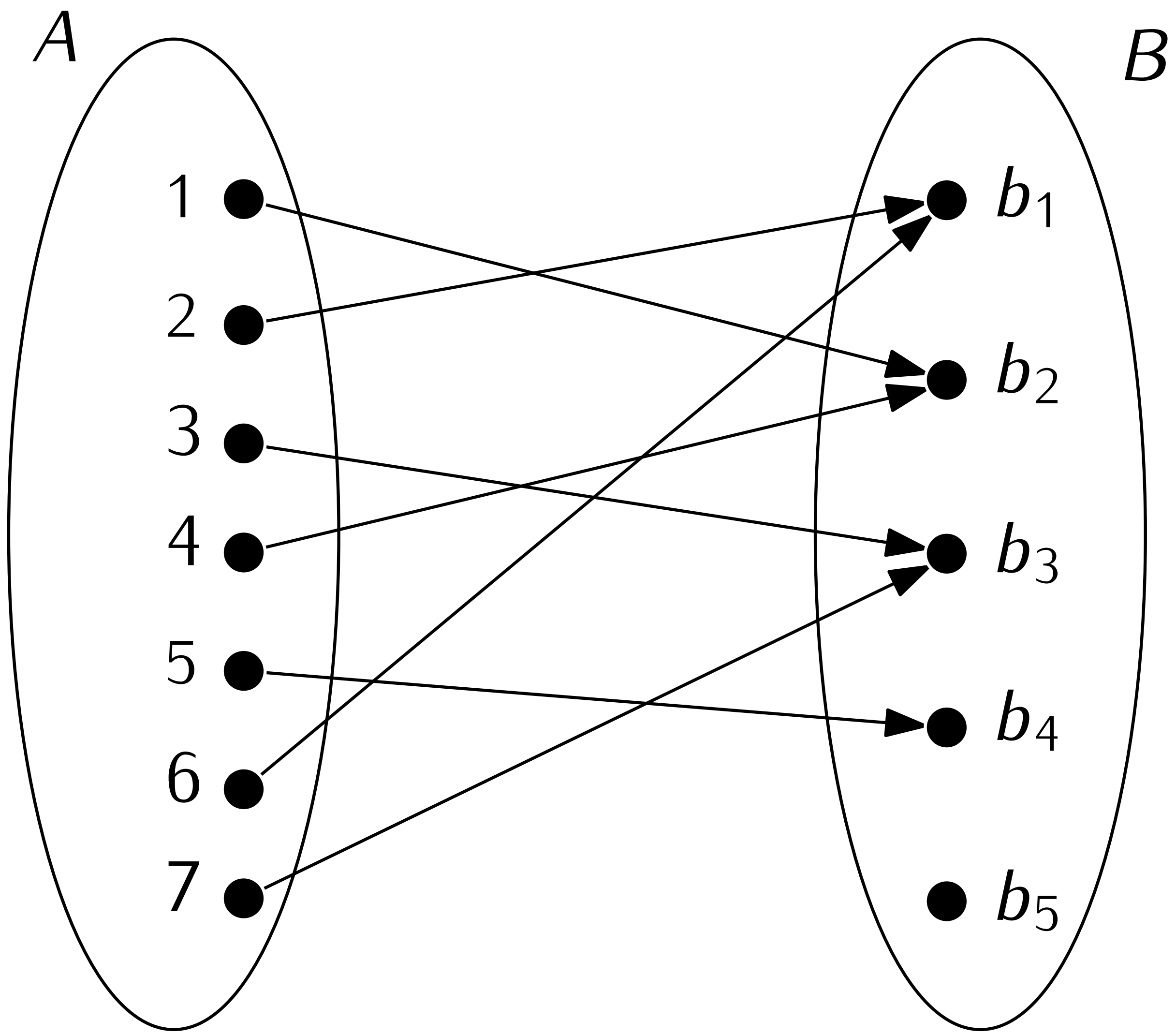
Definition. Let $f\colon A \to B$ be a function, $A' \subseteq A$, $B' \subseteq B$.

- 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!

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



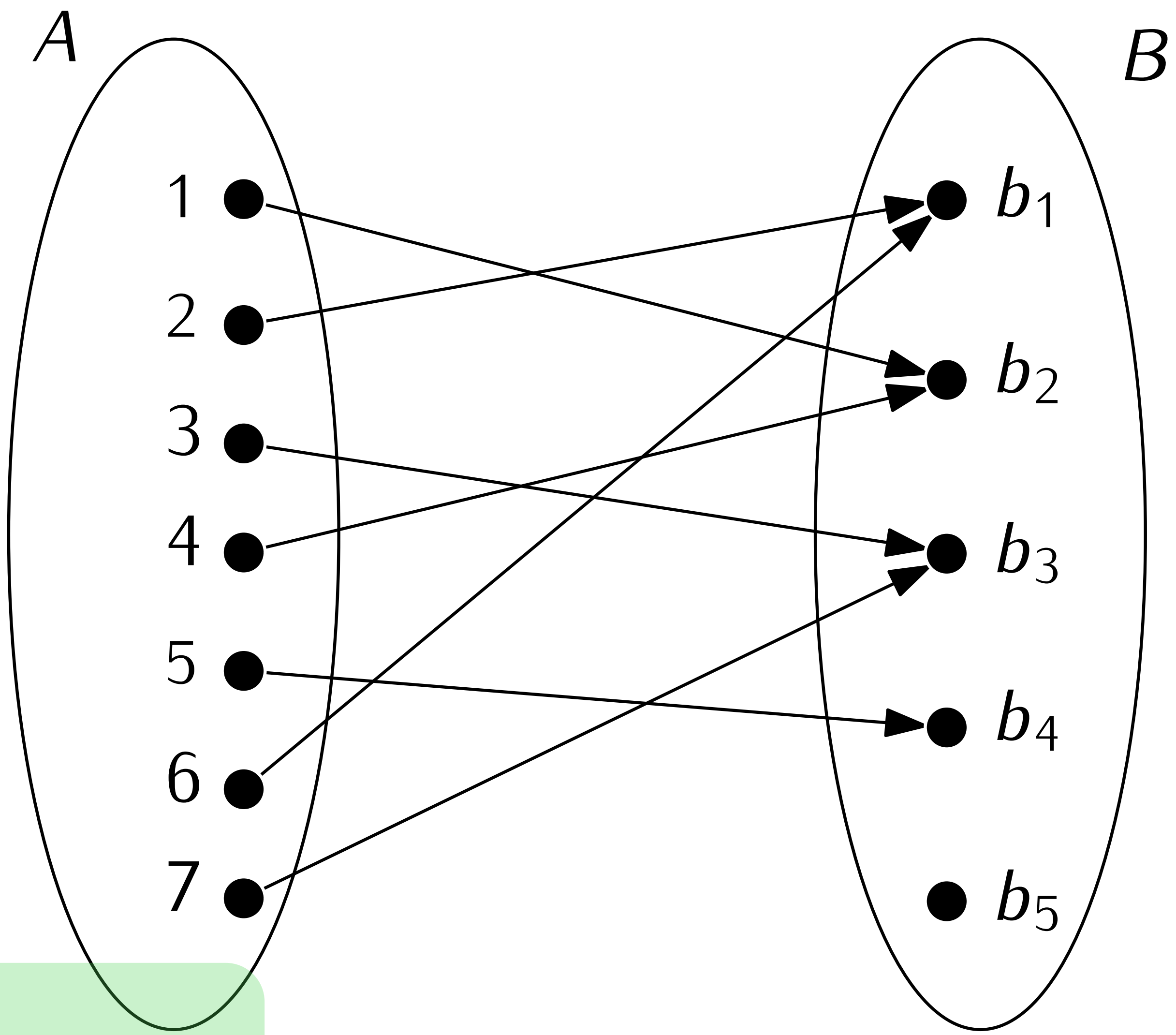
Definition. Let $f\colon A \to B$ be a function, $A' \subseteq A$, $B' \subseteq B$.

- 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 $f^{-1}[\{b\}]$?

Composing functions

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

```
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))) # ???
```

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

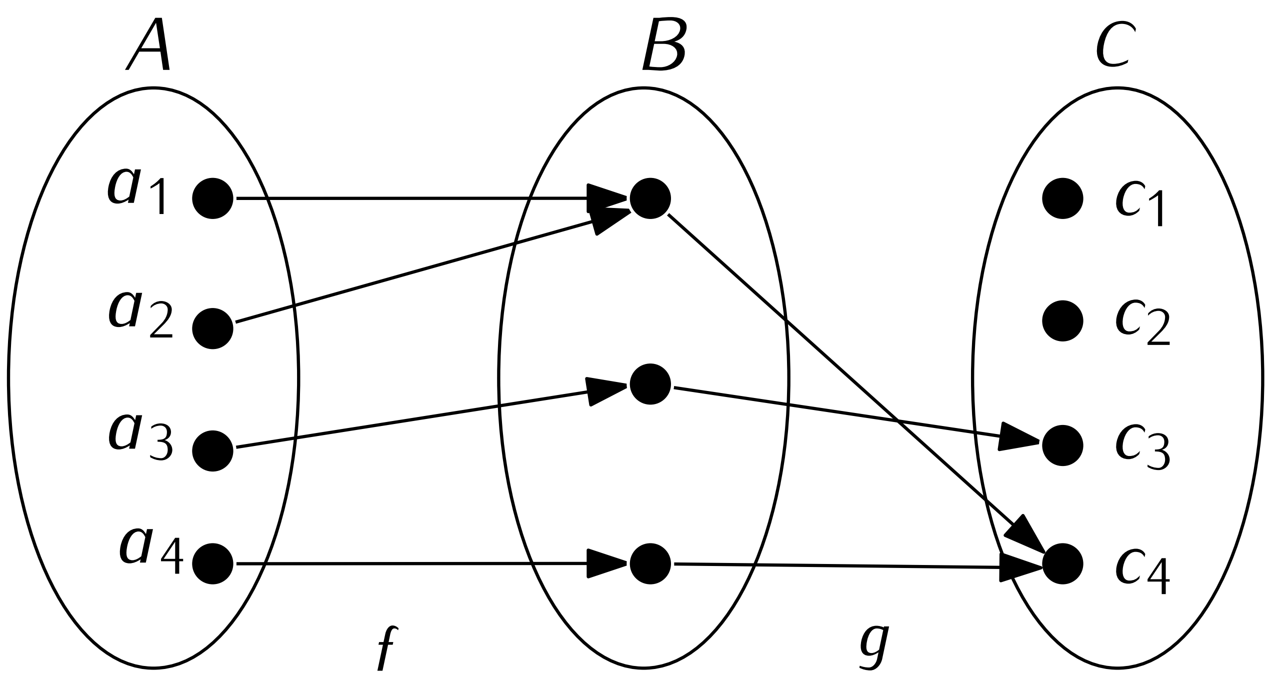
$$(g \circ f)(a) = g(f(a))$$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

```
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))) # ???
```



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

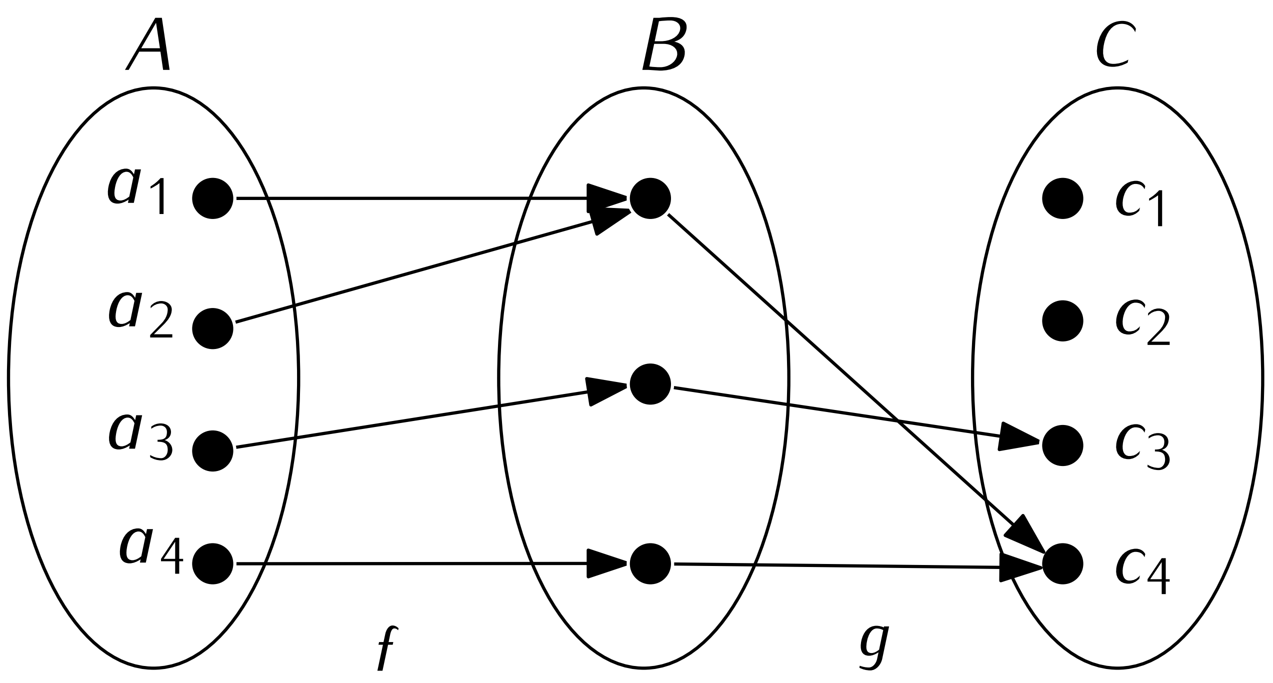
$$(g \circ f)(a) = g(f(a))$$

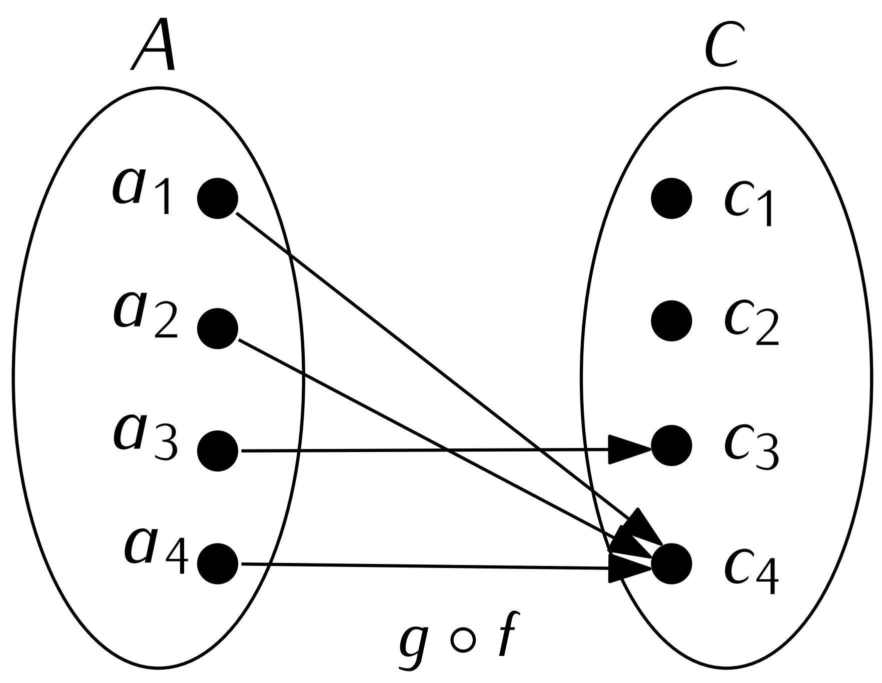
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

```
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))) # ???
```





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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

```
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))) # ???
```

Remark. Be careful!

- $f \circ g$ 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.

Same warning signs as with matrix multiplication!

Composing functions

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

```
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))) # ???
```

Remark. Be careful!

- $f \circ g$ 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.

Same warning signs as with matrix multiplication!

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

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

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

Composing functions: the identity function

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

The identity function on a set A is the function $\mathrm{Id}_A\colon A \to A$ defined by $\mathrm{Id}_A(x) = x$.

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

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

The identity function on a set A is the function $\mathrm{Id}_A\colon A \to A$ defined by $\mathrm{Id}_A(x) = x$.

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

Useful things about Id:

- If $f\colon A \to B$, then $f \circ \mathrm{Id}_A = f$
- If $f\colon A \to B$, then $\mathrm{Id}_B \circ f = f$

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

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, dashed, "g \circ f"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

The identity function on a set A is the function $\mathrm{Id}_A\colon A \to A$ defined by $\mathrm{Id}_A(x) = x$.

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

Useful things about Id:

- If $f\colon A \to B$, then $f \circ \mathrm{Id}_A = f$
- If $f\colon A \to B$, then $\mathrm{Id}_B \circ f = f$

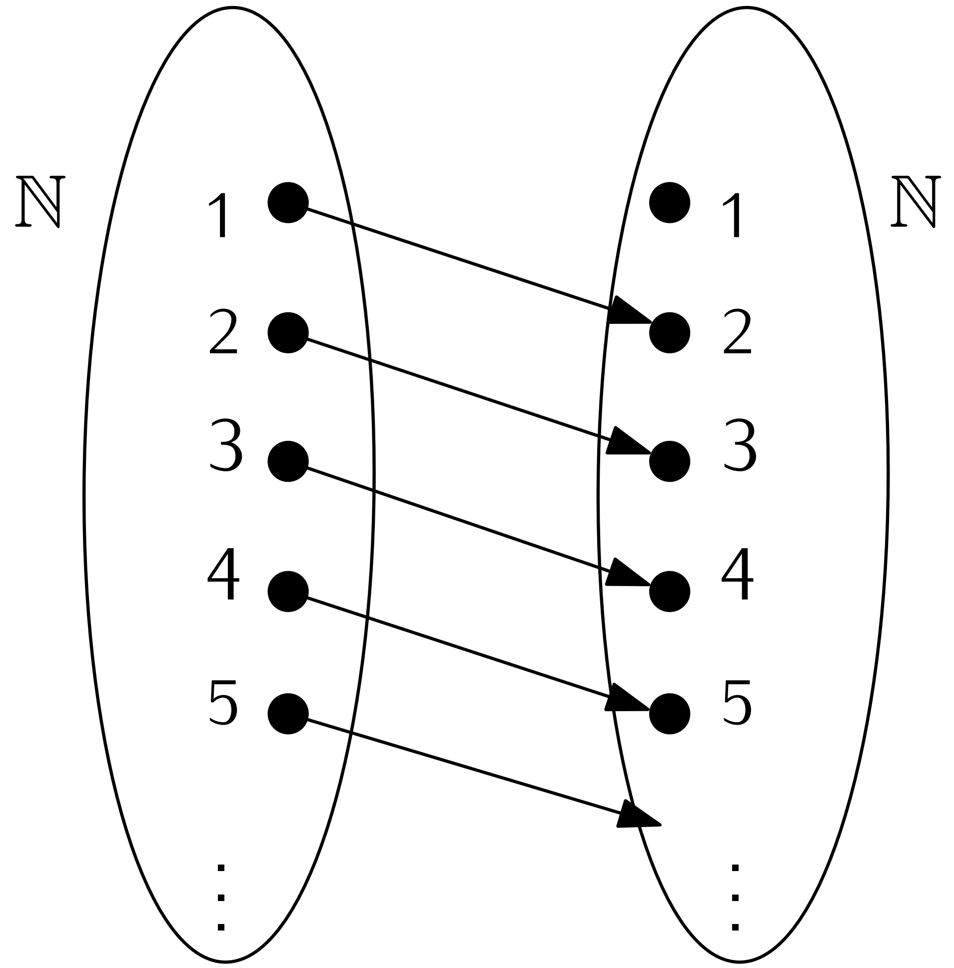
Analogies		
Numbers	$\longleftrightarrow$	Functions
Multiplication	$\longleftrightarrow$	Composition
$\times$		$\circ$
1		Id

Question. Let $f\colon A \to B$ be a function. Can one "undo" f?

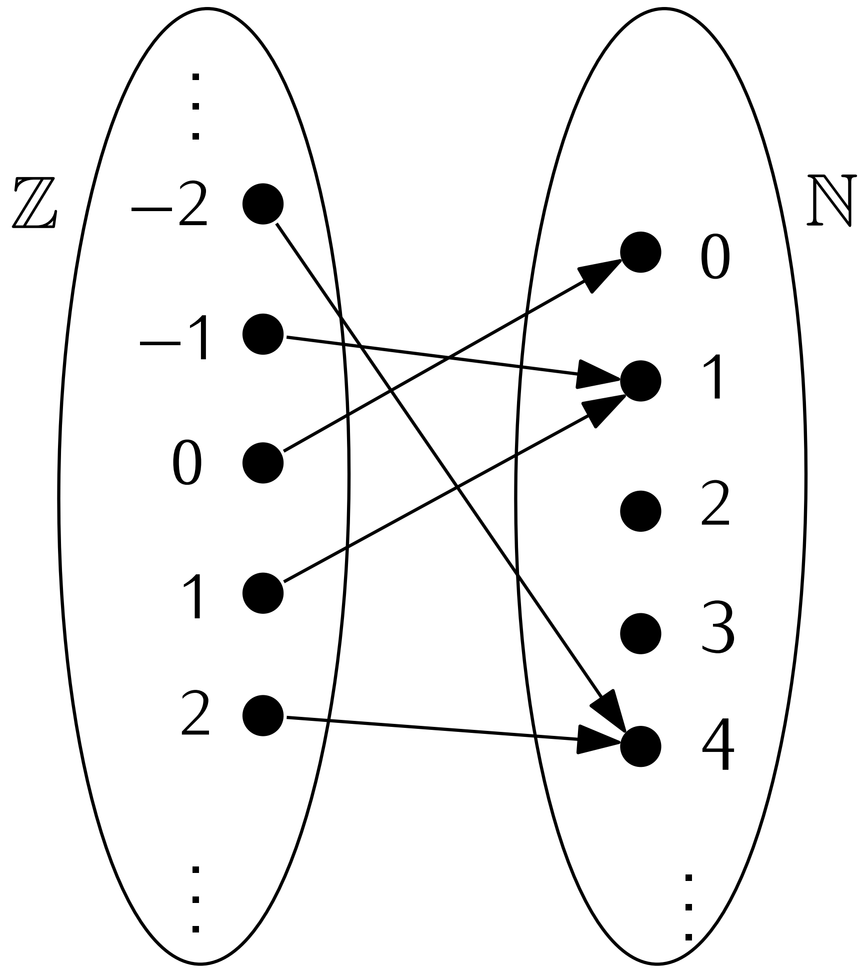
Question. Let $f\colon A \to B$ be a function. Can one "undo" f?
Given $b \in B$, is it possible to understand where b came from?

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

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



$g\colon \mathbb{Z} \to \mathbb{N}$, $g(x) = x^2$



Question. Let $f\colon A \to B$ 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!

Composing functions: inverses

Question. Let $f\colon A \to B$ 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 $f\colon A \to B$ is bijective, there exists $g\colon B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. This g is unique and written f^{-1}.

$$\begin{tikzcd} A \arrow[r, bend left, "f"] & B \arrow[l, bend left, "f^{-1}"] \end{tikzcd}$$

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

Question. Let $f\colon A \to B$ 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 $f\colon A \to B$ is bijective, there exists $g\colon B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. This g is unique and written f^{-1}.

$$\begin{tikzcd} A \arrow[r, bend left, "f"] & B \arrow[l, bend left, "f^{-1}"] \end{tikzcd}$$

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

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

Question. Let $f\colon A \to B$ 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 $f\colon A \to B$ is bijective, there exists $g\colon B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. This g is unique and written f^{-1}.

$$\begin{tikzcd} A \arrow[r, bend left, "f"] & B \arrow[l, bend left, "f^{-1}"] \end{tikzcd}$$

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 $f \colon A \to B$ 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 $f \colon A \to B$ is bijective, there exists $g \colon B \to A$ such that $g \circ f = \mathrm{Id}_A$ and $f \circ g = \mathrm{Id}_B$. This g is unique and written f^{-1}.

$$\begin{tikzcd} A \arrow[r, bend left, "f"] & B \arrow[l, bend left, "f^{-1}"] \end{tikzcd}$$

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 $f \colon \mathbb{Q} \to \mathbb{Q}$ 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