# Sets

A **set** is a collection of objects, called **elements** or **members**

- The set, call it $A$, whose elements are *Shakespeare, Tasmania, and Monday*
- The set, call it $B$, of all even positive numbers

# Notation

$A = \{$*Shakespeare*, *Tasmania*, *Monday*$\}$  list all elements and enclose with $\{\ \}$

$B = \{2, 4, 6, 8, \dots\}$  **not entirely clear!**

$B = \{x \mid x$ is an even positive number$\}$  specify a common **property**

of elements

Write $a \in S$ to say that $a$ is an element of $S$  (from Greek $\varepsilon$)

Write $a \notin S$ to say that $a$ is <u>not</u> an element of $S$

$8 \in B$     $7 \notin B$     $C = \{x \mid x \in \mathbb{N}$ and $x \notin B\}$

where $\mathbb{N}$ is the set of all natural numbers.  What is $C$?

# Three fundamental features of sets

- **A set must be distinguished from its description**

  For instance, the following descriptions define the same set:

  $$\{2, 3, 4\} \quad \{3, 2, 4\} \quad \{2, 2, 3, 4, 4\} \quad \{x \in \mathbb{N} \mid 2 \leq x \leq 4\} \quad \{y \in \mathbb{N} \mid 1 < y < 5\}$$

- **All elements of a set are distinct**

  In other words, no element may 'occur' more than once in a set

  We do not distinguish between $\{3, 2, 4\}$ and $\{2, 2, 3, 4, 4\}$

- **The elements of a set are not ordered in any way**

  We do not distinguish between $\{3, 2, 4\}$ and $\{2, 3, 4\}$

- A set can be an element of another set

  For example, $\{0, \{0\}\}$ has two elements: $0$ and $\{0\}$

# Subsets

A set $B$ is a **subset** of a set $A$ if every element of $B$ is an element of $A$

Notation:    $B \subseteq A$.                    Also say:    $B$ is **included** in $A$
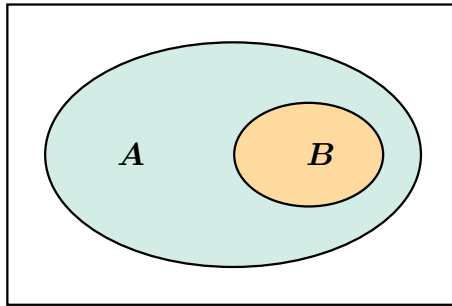


Figure 1: **Venn diagram** of $B \subseteq A$.

John Venn was a 19th-century British philosopher and mathematician who introduced

the Venn diagram in 1881

$$\{3, 4, 5\} \subseteq \{1, 5, 4, 2, 1, 3\} \qquad \{3, 3, 5\} \subseteq \{3, 5\} \qquad \{5, 3\} \subseteq \{3, 5\}$$

# Equal sets, proper subsets

Two sets $A$ and $B$ are **equal** if they have exactly the same elements

Notation: $A = B$

$$A = B \quad \text{iff} \quad A \subseteq B \quad \text{and} \quad B \subseteq A$$

$\{1\} = \{1, 1, 1\}$    $\{1\} \neq \{\{1\}\}$    $\{0, 2, 8\} = \{\sqrt{4}, 0/5, 2^3\}$

$B$ is a **proper subset** of $A$ if $B \subseteq A$ and $A \neq B$

Notation: $B \subset A$ or $B \subsetneq A$

Also say: $B$ is **properly included** in $A$

$\{1\} \subset \{1, 1, 2\}$    $\{1\} \not\subseteq \{\{1\}\}$

**Exercise:** Suppose $S = \{s, \emptyset\}$. Which of the following statements are true?

(a) $s \in S$    (b) $\{s\} \in S$    (c) $\emptyset \subseteq S$    (d) $\emptyset \in S$

# Important sets

$\emptyset \; = \; \{\,\}$                                         **empty set**, the set with no elements

$\mathbb{N} \; = \; \{0, 1, 2, 3, \dots\}$                       natural numbers

$\mathbb{N}^+ \; = \; \{1, 2, 3, \dots\}$                       positive natural numbers

$\mathbb{Z} \; = \; \{0, 1, -1, 2, -2, 3, -3, \dots\}$     integer numbers

$\mathbb{Q} \; = \; \{x/y \mid x, y \in \mathbb{Z}, \; y \neq 0\}$        rational numbers

$\mathbb{R} \; = \; \{\text{decimals}\}$                      real numbers

# Set operations: union

The **union** of sets $A$ and $B$ is the set $\ A \cup B \ = \ \{x \mid x \in A \ \text{or} \ x \in B\}$

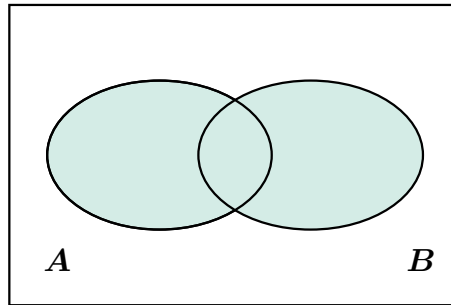$A \cup B$ is the set consisting of those elements that are in $A$ or in $B$ or both



Figure 2: Venn diagram of $A \cup B$.

Suppose $\quad A \ = \ \{4, 7, 8\} \quad$ and $\quad B \ = \ \{10, 4, 9\}$

Then $\qquad\qquad A \cup B \ = \ \{4, 7, 8, 9, 10\}$

# Set operations: intersection

The **intersection** of sets $A$ and $B$ is the set $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$

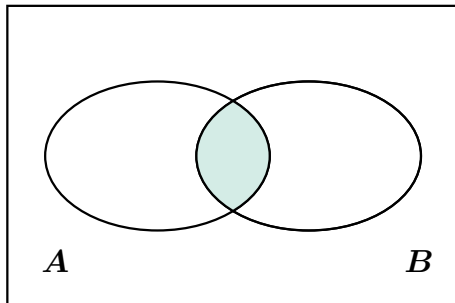$A \cap B$ is the set consisting of all elements which are both in $A$ and in $B$



Figure 3: Venn diagram of $A \cap B$.

Suppose $\quad A = \{4, 7, 8\} \quad$ and $\quad B = \{10, 4, 9\}$

Then $\qquad A \cap B = \{4\}$

If $A \cap B = \emptyset$ then $A$ and $B$ are called **disjoint**

# Set operations: relative complement

The **complement** of a set $B$ **relative** to a set $A$ is the set

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

$A - B$ is also called the **difference** of $A$ and $B$

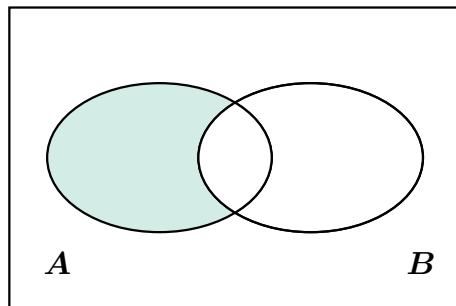$A - B$ is the set of all elements that belong to $A$ but not to $B$



Figure 4: Venn diagram of $A - B$.

If $\quad A = \{4, 7, 8\} \quad$ and $\quad B = \{10, 4, 9\} \quad$ then $\quad A - B = \{7, 8\}$

# Set operations: (absolute) complement

In certain contexts we may regard all sets under consideration as being

subsets of some given **universal set** $U$.

For instance, if we are investigating properties of the real numbers $\mathbb{R}$

(and subsets of $\mathbb{R}$), then we may take $\mathbb{R}$ as our universal set

Given a universal set $U$ and $A \subseteq U$, the **complement** of $A$ (in $U$) is the set
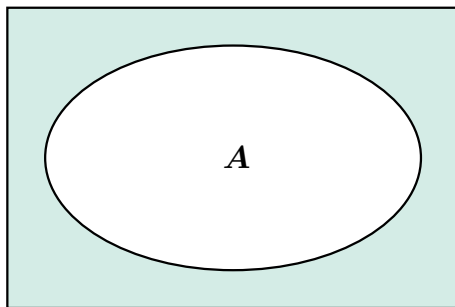$$-A = U - A = \{x \in U \mid x \notin A\}$$



Figure 5: Venn diagram of $-A$

# Set operations: powerset

The **powerset** of a set $A$ is defined to be the set of **all** subsets of $A$

Notation:   $\mathbf{Pow}(A) = \{X \mid X \subseteq A\}$

**Examples:**

1. Let $A = \{2\}$. Then
$$\mathbf{Pow}(A) = \{\emptyset, \{2\}\}$$

2. Let $B = \{1, 2, 3\}$. Then
$$\mathbf{Pow}(B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$$

3. Let $C = \emptyset$. Then
$$\mathbf{Pow}(C) = \{\emptyset\} \qquad (\neq \emptyset)$$

More common notation:     $\mathbf{Pow}(A) = 2^A$                    **Why?**

Because when $A$ has $n$ elements, then $\mathbf{Pow}(A)$ has $2^n$ elements

# Important equalities

- **Associative laws:**

$$A \cup (B \cup C) = (A \cup B) \cup C, \quad A \cap (B \cap C) = (A \cap B) \cap C$$

- **Commutative laws:**

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$

- **Identity laws (where $U$ is the universal set):**

$$A \cup \emptyset = A, \quad A \cup U = U, \quad A \cap U = A, \quad A \cap \emptyset = \emptyset$$

- **Distributive laws:**

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

- **Complement laws (where $U$ is the universal set):**

$$A \cup -A = U, \quad -U = \emptyset, \quad -(-A) = A, \quad A \cap -A = \emptyset, \quad -\emptyset = U$$

- **De Morgan's laws:**

$$-(A \cup B) = -A \cap -B, \quad -(A \cap B) = -A \cup -B$$

# Exercises

**Exercise 1** Prove that $-(A \cap B) = (-A) \cup (-B)$ for any sets $A$ and $B$

**Solution** We have to show that    (*i*)   $-(A \cap B) \subseteq -A \cup -B$   and

                                               (*ii*)   $-A \cup -B \subseteq -(A \cap B)$

(*i*) Let $x \in -(A \cap B)$ be arbitrary. Then $x \notin A$ or $x \notin B$

                      (because if $x$ belonged to both $A$ and $B$, then $x \in A \cap B$ would hold)

If $x \notin A$ then $x \in -A$, and so $x \in -A \cup -B$.

                            If $x \notin B$ then $x \in -B$, and so also $x \in -A \cup -B$.

(*ii*) Let $x \in -A \cup -B$. Then $x \in -A$ or $x \in -B$. If $x \in -A$ then $x \notin A$.

   If $x \in -B$ then $x \notin B$. So in any case, $x \notin A \cap B$. Therefore, $x \in -(A \cap B)$.

**Exercise 2** Show that there are sets $A, B, C$ such that $(A \cap B) \cup C \neq A \cap (B \cup C)$

**Solution** There can be several different solutions, here is one.

Let $A = \{1\}, B = \{1, 2\}$ and $C = \{3, 4\}$. Then $A \cap B = \{1\}$ and $(A \cap B) \cup C = \{1, 3, 4\}$.
On the other hand, $B \cup C = \{1, 2, 3, 4\}$, and so $A \cap (B \cup C) = \{1\}$. And $\{1, 3, 4\} \neq \{1\}$

                            (as, for example, $3 \in \{1, 3, 4\}$ but $3 \notin \{1\}$)

# Russell's paradox (1901)

Russell's paradox shows that the 'object' $\{x \mid P(x)\}$ is not always meaningful.

Consider the set $A = \{B \mid B \notin B\}$

> Give an example of an element of $A$

Problem: do we have $A \in A$?

For every set $C$, denote by $P(C)$ the statement $C \notin C$

Then $A = \{B \mid P(B)\}$.

- Suppose $A \in A$. Then not $P(A)$. Therefore, we must have $A \notin A$.

- But if $A \notin A$, then $P(A)$. Therefore, $A \in A$, which is a contradiction

Visit also   http://plato.stanford.edu/entries/russell-paradox/

## Popular version: the barber paradox

Suppose there is a town with just one male barber. According to law in this town, the barber shaves all and only those men in town who do not shave themselves.

Who shaves the barber?
- if the barber does shave himself, then the barber (himself) must not shave himself
- if the barber does not shave himself, then the barber (himself) must shave himself

# Sequences, tuples, and Cartesian products

A **sequence** of objects is a list of these objects **taken in a certain order**

The sequences    $(1, 2, 3)$    $(2, 1, 3)$    $(3, 1, 2)$    are **different**

The sets          $\{1, 2, 3\}$    $\{2, 1, 3\}$    $\{3, 1, 2\}$    are **the same**

Finite sequences are called **tuples**. A sequence with $k$ elements is a $k$**-tuple**

A 2-tuple is also called a **pair**

The **Cartesian product** $A \times B$ of sets $A$ and $B$ is the *set* of all pairs $(a, b)$

where $a \in A$ and $b \in B$

$$A \times B \ = \ \{(a, b) \mid a \in A \text{ and } b \in B\}$$

**Example.** Let $A = \{1, 2\}$ and $B = \{a, b, c\}$. Then

$$A \times B \ = \ \{(1, a), (2, a), (1, b), (2, b), (1, c), (2, c)\}$$

$\mathbb{R} \times \mathbb{R}$ is the **Euclidean plane**.    What is $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$?

# Binary relations

Let $S$ be the set of students at Birkbeck, and $C$ the set of available courses. The registration database or the relationship **'registered for'** can be represented

as the set $R = \{(s, c) \in S \times C \mid s \text{ registered for } c \}$



**S**tudents    **C**ourses    $S \times C$
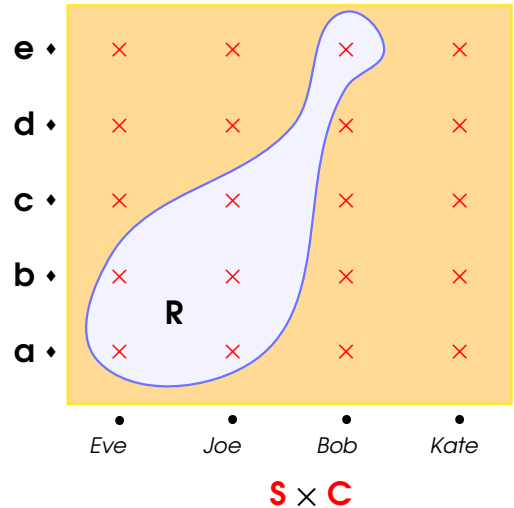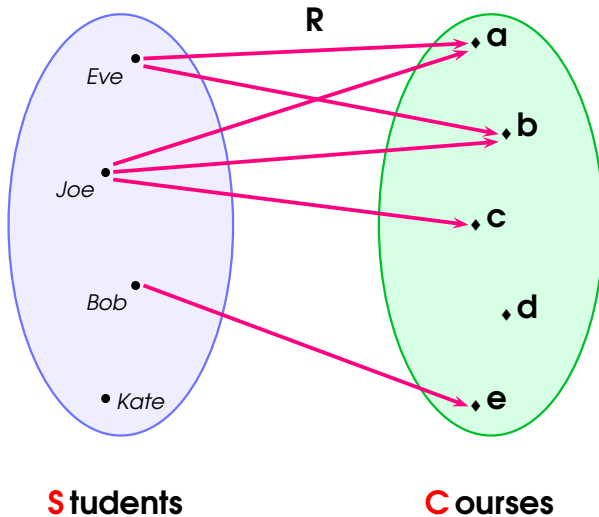
# Binary relations: definitions and examples

A **binary relation** between two sets $A$ and $B$ is a subset $R$
of the Cartesian product $A \times B$.    If $A = B$, then $R$ is a **relation on $A$**
    If $(x, y) \in R$ then we say that $x$ **is $R$-related to** $y$ and write $xRy$

- 'Smaller than' on $\mathbb{Z}$      $< \ = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x < y\}$

    $-1 < 0, \quad -1 < 1, \quad 0 < 2, \ldots$    but    $1 \not< 0, \quad 1 \not< -1, \quad 2 \not< 0, \ldots$

- 'Smaller than or equal to' on $\mathbb{Z}$      $\leq \ = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \leq y\}$

    $-1 \leq -1, \quad -1 \leq 1, \quad 0 \leq 0, \ldots$    but    $1 \not\leq 0, \quad 1 \not\leq -1, \quad 2 \not\leq 0, \ldots$

    Note that    $< \ \underset{\neq}{\subset} \ \leq$

- 'Input–output' relation $\mathsf{IO}_P$ for a given computer program $P$
Let $I$ be the set of possible inputs for $P$, and $O$ the set of possible outputs

$$\mathsf{IO}_P \ = \ \{(x, y) \in I \times O \mid P(x) = y\}$$

$x \ \mathsf{IO}_P \ y$    iff    given $x$ as an input, $P$ returns $y$

# Functions

A **function** from a set $A$ to a set $B$ is a binary relation $R \subseteq A \times B$ in which **every element** of $A$ is $R$-related a **unique** element of $B$, or, in other words: for each $a \in A$ there is precisely one pair of the form $(a, b)$ in $R$.
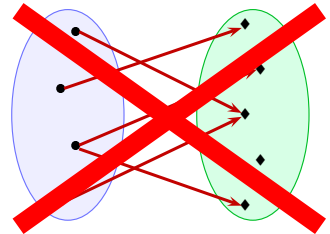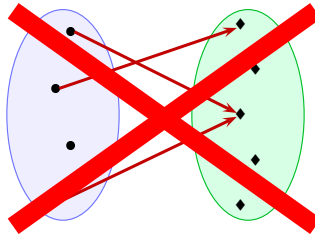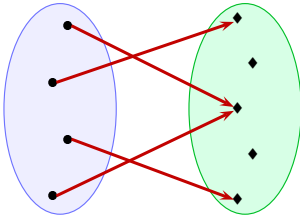


Which of the following relations are functions?

- $\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y = x - 1\}$
- $\{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid y = x - 1\}$
- $\{(x, y) \in \mathbb{N} \times \mathbb{R} \mid y^2 = x\}$

# Notation

–  Let $f$ be a function from a set $A$ to a set $B$. Since for each $x \in A$ there exists
   a uniquely determined $y \in B$ with $(x, y) \in f$, we write $\boxed{y \;=\; f(x)}$ and
   refer to $f(x)$ as the **image** of $x$ under $f$

–  We write $\boxed{f : A \rightarrow B}$ to indicate that $f$ is a function from $A$ to $B$

–  $A$ is called the **domain** of $f$.  $B$ is called the **codomain** of $f$

–  The **range** of $f$ is the set $\boxed{f(A) \;=\; \{f(x) \mid x \in A\}}$

– **every** element of the domain has to be mapped somewhere
   in the codomain

– but **not everything** in the codomain has to be a value of a
   domain element

– one element **cannot** be mapped to 2 different places

– but it **can** happen that 2 different elements are mapped to the same place
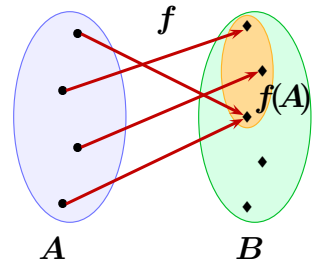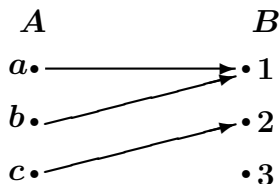
## Different ways of describing functions
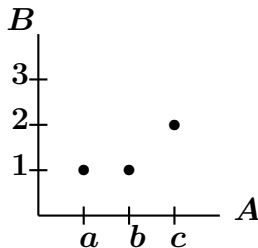
**Example:**  Let $A = \{a, b, c\}$  and  $B = \{1, 2, 3\}$.

– We can describe a function $f : A \to B$ by listing all of its associations:

$$f(a) = 1, \qquad f(b) = 1, \qquad f(c) = 2.$$

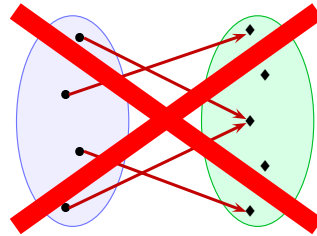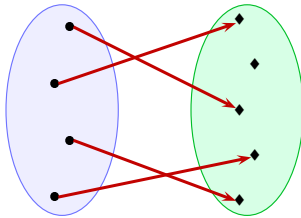– We can describe the same $f$ by drawing points and arrows:



– We can describe the same $f$ by drawing its **graph**:

# Injective functions

A function $f : A \to B$ is called an **injective** (or **'one-to-one'**) function if
for all $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$ then $a_1 = a_2$



This is logically equivalent to the implication $\boxed{a_1 \neq a_2 \implies f(a_1) \neq f(a_2)}$

In other words, different inputs give different outputs.

**Examples:** – $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = x^2$ is not injective

– $h : \mathbb{Z} \to \mathbb{Z}$ given by $h(x) = 2x$ is injective

# Surjective and bijective functions

$f : A \rightarrow B$ is **surjective** (or **'onto'**) if the range of $f$ coincides with the codomain of $f$, that is, if for every $b \in B$ there exists $a \in A$ with $b = f(a)$.
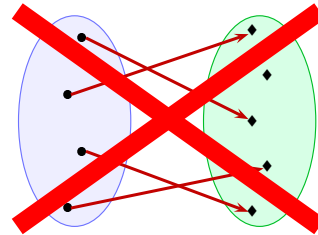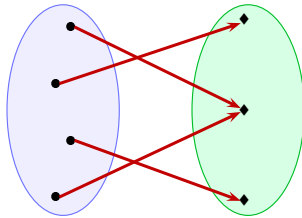


**Examples:**
- $f : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $f(x) = x^2$ is not surjective
- $h : \mathbb{Z} \rightarrow \mathbb{Z}$ given by $h(x) = 2x$ is not surjective
- $g : \mathbb{Q} \rightarrow \mathbb{Q}$ given by $g(x) = 2x$ is surjective and injective

We call $f$ **bijective** or a **one-to-one correspondence** if
$f$ is both injective and surjective

# Examples
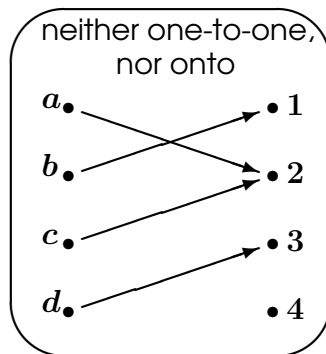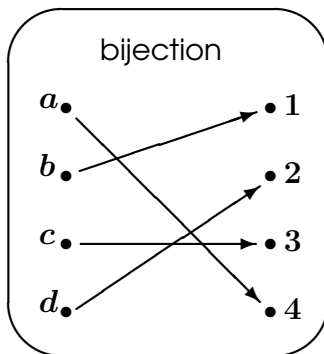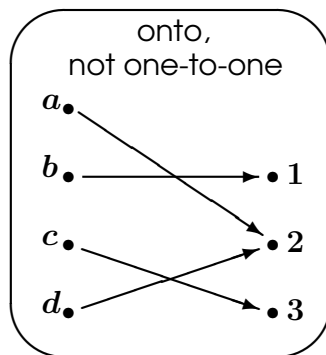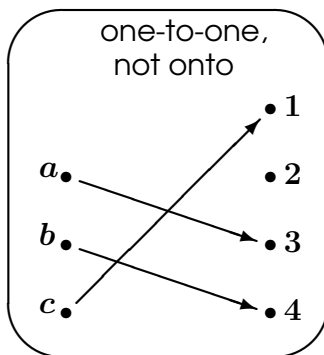
# Bijections and cardinality

If $A$ and $B$ are **finite** sets, then there exists a bijection between $A$ and $B$ iff
$A$ and $B$ have the same number of elements

---

Sets $A$ and $B$ have the same **cardinality** if there is a bijection from $A$ to $B$

In this case we write   $|A| = |B|$.

$A$ has cardinality **strictly greater** than the cardinality of $B$ if there is an injective function from $B$ into $A$, but $A$ and $B$ do not have the same cardinality

In this case we write   $|A| > |B|$.

---

According to a legend, Tamerlane (1336–1405), during one of his campaigns, ordered all his warriors to put one stone onto the pile on their way to the battle and upon their return pick a stone off the pile. This allowed him to deduct how many warriors he had lost in the battle. A stone barrow as a tomb to the lost, which they themselves had constructed with their own hands.

# Bijections and cardinality (cont.)

**Examples:**

– $f : \mathbb{N} \to \mathbb{Z}$ given by $\quad f(x) = \begin{cases} -x/2 & \text{if } x \text{ is even} \\ (x+1)/2 & \text{if } x \text{ is odd} \end{cases}$

is a bijection. So $\mathbb{N}$ and $\mathbb{Z}$ are of the same cardinality (or $|\mathbb{N}| = |\mathbb{Z}|$)

---

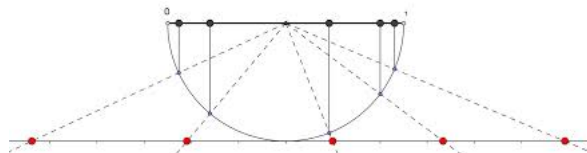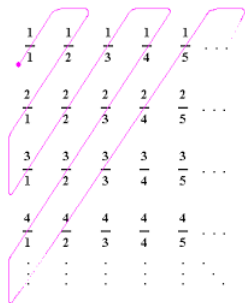An infinite set $A$ is **countable** if it has the same cardinality as $\mathbb{N}$.

An infinite set $A$ is **uncountable** if it is not countable.

---

– Are the following sets countable?

(a) $\mathbb{Q}$  (b) $(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$  (c) $\mathbb{R}$

# $\mathbb{R}$ is uncountable: Cantor's diagonal argument

Suppose, <u>on the contrary</u>, that the set of real numbers from $(0, 1)$ is **countable**

Then we can **enumerate** all the infinite decimal fractions of the form $0.d_1 d_2 \ldots$

Let us write such an enumeration as an infinite table

$$0.\ \textcolor{red}{d_{11}}\ d_{12}\ d_{13}\ d_{14}\ \ldots$$
$$0.\ d_{21}\ \textcolor{red}{d_{22}}\ d_{23}\ d_{24}\ \ldots$$
$$0.\ d_{31}\ d_{32}\ \textcolor{red}{d_{33}}\ d_{34}\ \ldots$$
$$0.\ d_{41}\ d_{42}\ d_{43}\ \textcolor{red}{d_{44}}\ \ldots$$
$$\ldots$$

For each $n = 1, 2, \ldots$ we choose a digit $c_n$ that is different from $d_{nn}$ and not equal to $9$, and consider the real number

$$0.\ c_1\ c_2\ c_3\ c_4\ \ldots$$

By construction, this number is different from every member of the given table

$\longrightarrow$ $(0, 1)$ and $\mathbb{R}$ cannot be countable

# Cantor's Theorem: $|A| \lneqq |2^A|$, for every set $A$

The set of all subsets of any set $A$ has a strictly greater cardinality than $A$ itself

Why? Let $f : A \to \textbf{Pow}(A)$ be any function.

Then, for every $x \in A$, $f(x)$ is a subset of $A$.

Now take the following subset $D$ of $A$: 
$$D \; = \; \{x \in A \mid x \notin f(x)\}$$

We show that $D$ **is not in the range of** $f$, that is, for every $x \in A$, $D \neq f(x)$

thus, for $A = \{1, 2\}$ and $f(1) = \{2\}$, $f(2) = \emptyset$, we have $D = \{1, 2\}$

Indeed, $x$ 'distinguishes' the sets $D$ and $f(x)$ :

– If $x \in D$, then $x$ should have the property describing $D$, so $x \notin f(x)$.

– If $x \in f(x)$, then the property describing $D$ does not hold for $x$, so $x \notin D$.

As $D$ is not in the range of $f$, we obtain that $f$ is **not onto**,
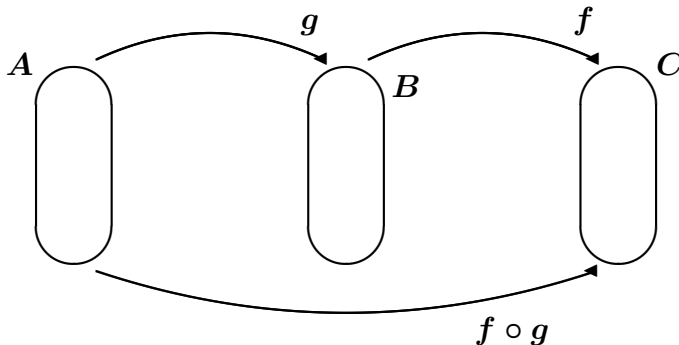
and so **can't be a bijection**

# Combining functions: composition

Let $g : A \to B$ and $f : B \to C$ be functions.

The **composition of $f$ and $g$** is the function $\boxed{(f \circ g) : A \to C}$ defined by

$$\boxed{(f \circ g)(a) \; = \; f\big(g(a)\big)} \qquad \text{for each } a \in A.$$



The composition $f \circ g$ is **only** defined when

'domain of $f$' = 'codomain of $g$'

# Composition of functions: examples

Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3\}$. Let function $g : X \to X$ be defined by

$$g(a) = b, \qquad g(b) = c, \qquad g(c) = a,$$

and function $f : X \to Y$ be defined by

$$f(a) = 3, \qquad f(b) = 2, \qquad f(c) = 1.$$

Then:

- $(f \circ g)(a) = f\big(g(a)\big) = f(b) = 2$,

  $(f \circ g)(b) = f\big(g(b)\big) = f(c) = 1$,

  $(f \circ g)(c) = f\big(g(c)\big) = f(a) = 3$.

- $(g \circ g)(a) = g\big(g(a)\big) = g(b) = c$,

  $(g \circ g)(b) = g\big(g(b)\big) = g(c) = a$,

  $(g \circ g)(c) = g\big(g(c)\big) = g(a) = b$.

- Watch out: $f \circ f$ and $g \circ f$ are not defined!

# Alphabets and words

An **alphabet** is a finite set $\Sigma$ of symbols

Examples:
- $\Sigma_1 = \{a, b, c, \ldots, z\}$, the set of all lower-case letters
- $\Sigma_2 = \{0, 1\}$, the binary alphabet
- $\Sigma_3 = \{\square, \diamond, \heartsuit\}$

A **word** or **string** (over an alphabet $\Sigma$) is a finite sequence of symbols from $\Sigma$

Examples:
- *abracadabra*, *azwzax* (over $\Sigma_1$)
- 11111111110000000000, 000110 (over $\Sigma_2$)
- $\heartsuit\heartsuit\square$, $\square\diamond\square\square\diamond\heartsuit$ (over $\Sigma_3$)
- the **empty word** $\varepsilon$ is a word over **any** alphabet $\Sigma$ (but we may assume that $\varepsilon$ is _NOT a symbol_ of any of our alphabets)

# Words (cont.)

–  $\boxed{\Sigma^*}$   is the set of all words over $\Sigma$ (always contains $\varepsilon$)

–  The **length**  $|w|$  of a word $w$ is the number of symbols in $w$

$$|w| \;=\; \text{the number of occurrences of symbols in } w$$

e.g.,   $|azwza| = 5$,   $|\heartsuit\heartsuit\square| = 3$,   $|\varepsilon| = 0$

–  The **concatenation** of words $x$ and $y$ (notation: $xy$) is

the word $x$ followed by the word $y$

–  $w^n \;=\; \underbrace{ww\ldots w}_{n}$   (e.g.,   $(\heartsuit\square)^0 = \varepsilon$, $(01)^3 = 010101$,  $a^4 = aaaa$)

–  $x\varepsilon \;=\; \varepsilon x = x$,   for every word $x$

–  if $w = xy$ then $x$ is a **prefix** of $w$, and $y$ a **suffix** of $w$

e.g.,   _tor_   is a prefix and   _se_   is a suffix of   _tortoise_

# Languages

> A **language** over an alphabet $\Sigma$ is a set of words over $\Sigma$,
>
> that is, a **language** is a subset of $\Sigma^*$

**Examples:**

(1)  $\Sigma = \{a, b, c, \ldots, z\}$

– $L_1 = $  all English words

– $L_2 = $  all Latin words

– $L_3 = \{kdpekvg, leih, hkiiw, wowiszk\}$

(2)  $\Sigma = \{0, 1\}$

– $L_4 = \{001, 101010, 111, 1001\}$

– $L_5 = \{0^n 1^m \mid n$ is an even, $m$ is an odd number$\}$