# Preliminaries / Review

**Pedro Vilanova**

August 27, 2023

# Sets

What is meant by a set is intuitively clear: "bag" of objects. Sets are denoted with uppercase, objects with lowercase.

- (Belongs). An object $x$ belongs to a set $A$ is denoted by $x \in A$. For instance, $3 \in \{1, 2, 3, 4, 5\}$ but $7 \notin \{1, 2, 3, 4, 5\}$.
- (Emptyset). A set which contains no elements is denoted $\emptyset$, i.e., for every object $x$ we have $x \notin \emptyset$.
- (Sets are objects). If $A$ is a set, then $A$ is also an object. In particular, given two sets $A$ and $B$, it is meaningful to ask $A \in B$?
- (Equality of sets). Two sets $A$ and $B$ are equal, $A = B$, iff [1] every element of $A$ is an element of $B$ and vice versa.

- (Subsets). Let $A$, $B$ be sets. We say that $A$ is a subset of $B$, denoted $A \subseteq B$, iff every element of $A$ is also an element of $B$

$$\forall x : (x \in A) \Rightarrow (x \in B) .$$

  We say that $A$ is a proper subset of $B$, denoted $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$.

- Given any set $A$, we always have $A \subseteq A$ (why?) and $\emptyset \subseteq A$ (why?). What about $A \in A$? Is 2 an element or a subset of $\{1, 2, 3\}$? Is $\{2\}$ an element or a subset of $\{1, 2, 3\}$? It is important to distinguish sets from their elements, as they can have different properties. Is it possible to have an infinite set consisting of finite numbers? Is it possible to have a finite set consisting of infinite objects?

- Examples: Is $\{\emptyset\} = \emptyset$ (why?). What about $\{\{\emptyset\}\}$ and $\{\emptyset, \{\emptyset\}\}$? Are those three sets equal? (why?)

# Sets

- (Axiom of specification). Let $A$ be a set, and for each $x \in A$, let $P(x)$ be a property pertaining to x that is either true or false. Then there exists the set

$$\{x \in A : P(x) \text{ is true}\}.$$

- (Pairwise union). Given any two sets $A$, $B$, there exists a set $A \cup B$, called the union of $A$ and $B$:

$$\forall x : (x \in A \cup B) \iff (x \in A \text{ or } x \in B).$$

  Recall that "or" in mathematics is by default inclusive.

- (Intersection). Given any two sets $A$, $B$, there exists a set $A \cap B$, called the intersection of $A$ and $B$:

$$\forall x : (x \in A \cap B) \iff (x \in A \text{ and } x \in B).$$

[1] if and only if

# Natural numbers

## Definition (informal)

*A natural number is any element of the set*

$$\mathbb{N} := \{0, 1, 2, 3, 4, \ldots\},$$

*which is the set of all the numbers created by starting with 0 and then counting forward indefinitely.*

In some texts the natural numbers start at 1 instead of 0, but this is a matter of notational convention more than anything else.

This definition of "start at 0 and count indefinitely" seems like an intuitive enough definition of $\mathbb{N}$, but it is not entirely acceptable, because it leaves many questions unanswered. For instance: how do we know we can keep counting indefinitely, without cycling back to 0?

Also, how do you perform operations such as addition, multiplication, or exponentiation?

# Natural numbers

We can define complicated operations in terms of simpler operations. Exponentiation is nothing more than repeated multiplication. Multiplication is nothing more than repeated addition. And addition? It is nothing more than the repeated operation of counting forward, or incrementing.

To define the natural numbers, we will use two fundamental concepts: the zero number 0, and the increment operation.

## Axiom (1)

*0 is a natural number.*

## Axiom (2)

*If $n$ is a natural number, then the successor of $n$, denoted $s(n)$ is also a natural number.*

# Natural numbers

## Definition

*We define 1 to be the number $s(0)$, 2 to be the number $s(s(0))$, 3 to be the number $s(s(s(0)))$, and so on.*

Consider a number system which consists of the numbers 0, 1, 2, 3, in which the increment operation wraps back from 3 to 0. This system obeys both axioms.

To prevent this sort of "wrap-around issue" we will impose another axiom:

## Axiom (3)

*0 is not the successor of any natural number; i.e., we have $s(n) \neq 0$ for every natural number $n$.*

However, even with our new axiom, it is still possible that our number system behaves in other pathological ways: Consider a number system consisting of five numbers 0,1,2,3,4, in which the increment operation hits a ceiling at 4. That is: $s(4) = 4$.

# Natural numbers

To prevent this to happen we add:

## Axiom (4)

*Different natural numbers must have different successors; i.e., if $n$, $m$ are natural numbers and $n \neq m$, then $s(n) \neq s(m)$. Equivalently (contrapositive), if $s(n) = s(m)$, then we must have $n = m$.*

An essential proof technique for natural numbers is

## Axiom (5, Principle of mathematical induction)

*Let $P(n)$ be any property pertaining to a natural number $n$. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(s(n))$ is also true. Then $P(n)$ is true for every natural number $n$.*

Note this axiom is more general than the previous ones since it refers to properties. This axiom is a template that can be instantiated to create other axioms depending on $P$. This Axiom prevents that any other numbers than integers belong to $\mathbb{N}$. For example, the set $\{0, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, ...\}$ satisfies all other axioms.

# Natural numbers

## Definition (Addition of natural numbers)

*Let $m \in \mathbb{N}$. To add zero to $m$, we define $0 + m := m$. Now suppose inductively that we have defined how to add $n$ to $m$. Then we can add $s(n)$ to $m$ by defining $s(n) + m := s(n + m)$.*

The following propositions can now be proved:

- (Addition is commutative). For any natural numbers $n$ and $m$, $n + m = m + n$.
- Addition is associative). For any natural numbers $a$, $b$, $c$, we have $(a + b) + c = a + (b + c)$.
- (Cancellation law). Let $a$, $b$, $c$ be natural numbers such that $a + b = a + c$. Then we have $b = c$.
- Many more.

# Natural numbers

Once we have a notion of addition, we can define order:

## Definition (Ordering of the natural numbers)

*Let $n, m \in \mathbb{N}$. We say that $n$ is greater than or equal to $m$, and write $n \geq m$ or $m \leq n$, iff we have $n = m + a$ for some $a \in \mathbb{N}$. We say that $n$ is strictly greater than $m$, and write $n > m$ or $m < n$, iff $n \geq m$ and $n \neq m$.*

## Definition (Multiplication of natural numbers)

*Let $m \in \mathbb{N}$. To multiply zero to $m$, we define $0 * m := 0$. Now suppose inductively that we have defined how to multiply $n$ to $m$. Then we can multiply $s(n)$ to $m$ by defining $s(n) * m := (n * m) + m$.*

The following propositions can now be proved:

- (Multiplication is commutative).
- (Positive natural numbers have no zero divisors).
- (Distributive law).

# Natural numbers

- (Multiplication is associative).
- (Multiplication preserves order).
- Many more.

# Functions

The concept of a function (or map) is central to all of mathematics. We begin with ordered pair using sets.

## Definition (Ordered pair)

*of elements $x$ and $y$, written $(x, y)$, is defined*

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

*Two ordered pairs $(a, b)$ and $(c, d)$ are equal iff $a = c$ and $b = d$.*

## Definition (Cartesian product)

*of sets $A$ and $B$ denoted $A \times B$ is*

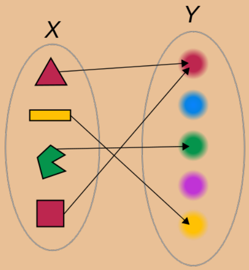
$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}.$$

## Definition (Function)

*A function from set $X$ into $Y$ is a subset of $X \times Y$ denoted $f : X \to Y$ that satisfies*

1. *If $(x, y)$ and $(x, y')$ belong to $f$, then $y = y'$.*
2. *If $x \in X$, then $(x, y) \in f$ for some $y \in Y$.*

The crucial property of a function is that with each (2) element $x$ in $X$ there is associated a unique (1) element $y$ in $Y$.




$X$ is called domain, $Y$ is called codomain. In this course usually $X = \mathbb{R}^n$ and $Y = \mathbb{R}$.

Figure credit: wikipedia

**Notation:** If $(x, y) \in f$, we write $y = f(x)$ and call $y$ the (direct) image of $x$ under $f$.

### Definition

*Let $f : X \to Y$. The range of $f$ is the set*

$$\{f(x) : x \in X\}.$$

*The range and the codomain are not necessary the same, the range is a subset of $Y$.*

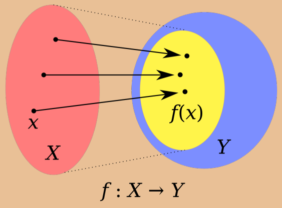



Figure credit: wikipedia

# Functions

**Definition**

*Let $f : X \to Y$. Let $A \subseteq X$ and $B \subseteq Y$.*

1. *The image of $A$ under $f$ is the set $f(A) = \{f(x) : x \in A\}$.*
2. *The inverse image of $B$ under $f$ is the set $f^{-1}(B) = \{x : f(x) \in B\}$.*

### Definition

*Let $f : X \to Y$.*

1. *$f$ is surjective if*
$$f(X) = Y\,.$$
*The range and codomain coincide.*
2. *$f$ is injective if*
$$\forall x, z \in X : (f(x) = f(z)) \Rightarrow (x = z)\,.$$
3. *$f$ is bijective if*
$$\forall y \in Y : \exists! x \in X \text{ such that } y = f(x)\,.$$
*where $\exists! x$ means "there exists exactly one $x$".*

# Functions

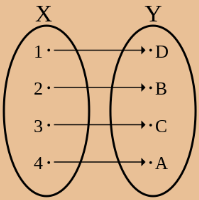
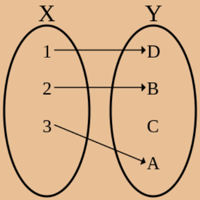
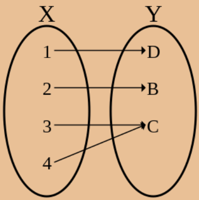
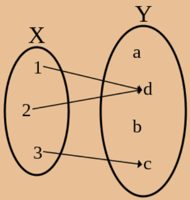
| | surjective | non-surjective |
|---|---|---|
| injective | <br>bijective | <br>injective-only |
| non-injective | <br>surjective-only | <br>general |

Figure credit: wikipedia

# Functions

## Definition (Inverse function)

*If $f : X \to Y$ is injective, we may define the inverse function to $f$, denoted $f^{-1}$, from the range of $f$ onto $X$ by*

$$(y, x) \in f^{-1} \textit{ iff } (x, y) \in f\,.$$

**Note:** The inverse function $f^{-1}$ is defined only if $f$ is injective but the inverse image $f^{-1}(B)$ is defined for an arbitrary function $f$ and for all sets $B \subseteq Y$.

## Definition

*If $f : X \to Y$ and $g : Y \to Z$, we define the composition $g \circ f : X \to Z$ by*

$$(g \circ f)(x) = g(f(x)) \quad \textit{for all } x \in X\,.$$

# Functions

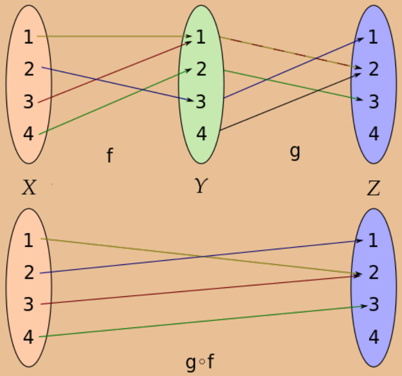



Figure: wikipedia

**Example:** Let

$$f = \{(1,1),(2,1),(3,4)\}, \quad A = \{1,2\}, \quad B = \{1\}\,.$$

The domain of $f$ is $\{1,2,3\}$ and the range of $f$ is $\{1,4\}$. The image of $A$ under $f$ is the set $f(A) = \{1\}$. The inverse image of $B$ under $f$ is the set $f^{-1}(B) = \{1,2\}$. If $Y = \{1,4\}$ then $f$ is surjective. The function $f$ is not injective since $f(1) = f(2)$.
Let $g = \{(1,1),(2,3)\}$. Then $g$ is injective and the inverse function is

$$g^{-1} = \{(1,1),(3,2)\}\,.$$

The composition $g \circ f$ is the function

$$g \circ f = \{(1,1),(2,4)\}\,.$$

# Functions

**Quiz:** Let $g = \{(1,2),(2,2),(3,1),(4,4)\}$, $f = \{(1,5),(2,7),(3,9),(4,17)\}$, and $A = \{1,2\}$. Determine

(a) The domain of $g$

(b) The range of $g$

(c) $g(A)$

(d) $g^{-1}(A)$

(e) $g \circ f$

(f) $f^{-1}$