Preliminaries / Review

Pedro Vilanova

October 25, 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.

Sets

- (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.

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

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

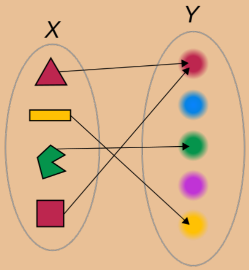
Functions

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

Functions

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.

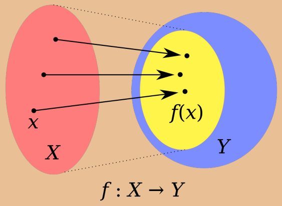


Figure credit: wikipedia

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 $f^{-1}(B) = \{x : f(x) \in B\}$.*

Functions

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

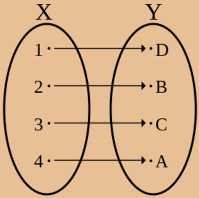
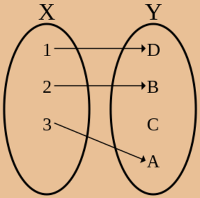
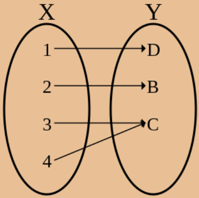
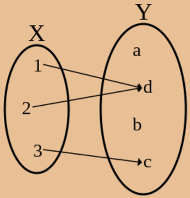
	surjective	non-surjective
injective	 bijective	 injective-only
non-injective	 surjective-only	 general

Figure credit: wikipedia

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

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

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

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

Functions

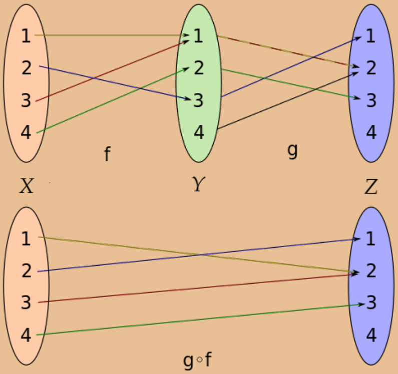


Figure: wikipedia

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

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

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}

Real numbers - Infimum and Supremum

Previous definitions (sets and functions) were very general. In this course we are interested in sets and functions on the real numbers:

Definition

The real numbers $\mathbb{R}$ is a set of objects satisfying a set of algebraic axioms (addition and multiplication), a total order axiom, and the least upper bound axiom.

We now discuss a fundamental property idea behind real numbers: Infimum and Supremum. First we recall the following: The *well-ordering principle* states that every non-empty subset of the natural numbers $\mathbb{N}$ has a least element (minimum). However, this property does not extend to arbitrary subsets of the real numbers $\mathbb{R}$:

A subset of $\mathbb{R}$ may or may not have a minimum element.

Infimum and Supremum

Example: interval $(0, 1] \subset \mathbb{R}$. This set does not have a minimum element, as for any $x \in (0, 1]$, you can always find another element in the set that is smaller than x but still greater than 0. On the other hand, $[0, 1] \subset \mathbb{R}$ does have a minimum element, which is 0.

This issue is addressed through the concepts of the least upper bound (supremum) and the greatest lower bound (infimum).

The least upper bound and greatest lower bound provide a way to "complete" the real numbers, ensuring that there are no "gaps" in the number line. This completeness property is essential for the development of calculus and real analysis.

Then, while the open interval $(0, 1)$ does not have a minimum or maximum, we can say that its infimum is 0 and its supremum is 1.

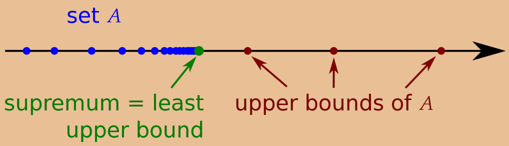
Infimum and Supremum

Let A be a nonempty subset of $\mathbb{R}$. The set of upper bounds of A, denoted $U(A)$, is defined as

$$U(A) = \{u \in \mathbb{R} \mid u \geq a \text{ for all } a \in A\},$$

while the set of lower bounds of A, denoted $L(A)$, is given by

$$L(A) = \{l \in \mathbb{R} \mid l \leq a \text{ for all } a \in A\}.$$



Task: draw an analogous figure for infimum.

Infimum and Supremum

Remark: Any $U(A)$ and $L(A)$ could be empty. Examples:

- If $A = \mathbb{N}$ then $U(A)$ is empty.
- If $A = \mathbb{Z}$, the set of all integers, then both $U(A)$ and $L(A)$ are empty.
- If $U(A)$ is nonempty, then A is said to be bounded above.
- If $L(A)$ is nonempty, then A is said to be bounded below.

Definition

The supremum of A, denoted $\sup(A)$, is defined to be the least upper bound of A. Namely, if $U(A)$ is nonempty, then $\sup(A)$ is defined to be the unique point $a^* \in U(A)$ such that $a^* \leq u$ for all $u \in U(A)$. If $U(A)$ is empty, by convention, we set $\sup(A) = +\infty$.

Remark: Here we take an axiomatic approach to the real line. In this approach, the supremum of A is well defined, i.e., there is $a^* \in U(A)$ such that $a^* \leq u$ for all $u \in U(A)$ when $U(A)$ is non-empty. Other authors adopt a constructive approach to the real line. In the constructive approach the following must be proved as a theorem: Let A be a non-empty subset of $\mathbb{R}$. If A has an upper bound, then it must have exactly one least upper bound.

Definition

The infimum of A, denoted $\inf(A)$, is defined to be the greatest lower bound of A. That is, when $L(A)$ is nonempty, then $\inf(A)$ is the unique point $\hat{a} \in L(A)$ such that $\hat{a} \geq l$ for all $l \in L(A)$. If $L(A)$ is empty, by convention we set $\inf(A) = -\infty$.

What if $A = \emptyset$? Then by convention we set $\inf(\emptyset) = +\infty$ and $\sup(\emptyset) = -\infty$.

Remark: $+\infty$ and $-\infty$ are just symbols and not real numbers. We may add $+\infty$ and $-\infty$ to the reals to form the extended real numbers $\bar{\mathbb{R}}$, but this is not as convenient to work with as the real numbers. Many of the laws of algebra break down: what is $+\infty + -\infty$?

Infimum and Supremum

Two concepts closely related to sup and inf are the maximum and the minimum of a nonempty set $A \subset \mathbb{R}$:

Definition (Maximum and minimum)

The maximum of A, denoted $\max(A)$, is defined as a point $z \in A$ such that $z \geq a$ for all $a \in A$. The minimum of A, denoted $\min(A)$, is defined as a point $w \in A$ such that $w < a$ for all $w \in A$.

By definition, the maximum must be an upper bound of A, and the minimum must be a lower bound of A. Therefore, we can equivalently define $\max(A) = A \cap U(A)$, and $\min(A) = A \cap L(A)$.

While $\sup(A)$ and $\inf(A)$ are always defined for any nonempty set A (they could be infinite), $A \cap U(A)$ and $A \cap L(A)$ could both be empty, so $\max(A)$ and $\min(A)$ not always exist. This is true even if $\sup(A)$ and $\inf(A)$ are both finite.
For example, neither $\mathbb{R}$ nor the interval $(0, 1)$ has a minimum, but $\inf \mathbb{R} = -\infty$ and $\inf(0, 1) = 0$.

inf and sup properties

Let the sets $A, B \subseteq \mathbb{R}$, and scalar $r \in \mathbb{R}$. Define (arithmetic operations over sets):

- $rA = \{ra : a \in A\}$; the scalar product of a set is just the scalar multiplied by every element in the set.
- $A + B = \{a + b : a \in A, \;\; b \in B\}$; called the Minkowski sum, it is the arithmetic sum of two sets is the sum of all possible pairs of numbers, one from each set.

Proposition

In those cases where the infima and suprema of the sets A and B exist, the following identities hold:

- *If $A \subseteq B$ then $\inf(A) \geq \inf(B)$ and $\sup(A) \leq \sup(B)$.*
- *$A \neq \emptyset$ iff $\sup(A) \geq \inf(A)$, and otherwise $-\infty = \sup(\emptyset) < \inf(\emptyset) = \infty$.*
- *$p = \inf(A)$ iff p is a lower bound and for every $\epsilon > 0$ there is an $a(\epsilon) \in A$ such that $a(\epsilon) > p + \epsilon$. (lower bound that can be approximated).*
- *If $r \geq 0$ then $\inf(rA) = r \inf(A)$ and $\sup(rA) = r \sup(A)$.*
- *If $r \leq 0$ then $\inf(rA) = r \sup(A)$ and $\sup(rA) = r \inf(A)$.*
- *$\inf(A + B) = \inf(A) + \inf(B)$ and $\sup(A + B) = \sup(A) + \sup(B)$.*

Examples

- $\inf\{1, 2, 3, \dots\} = 1$.
- $\inf\{x \in \mathbb{R} : 0 < x < 1\} = 0$.
- $\inf\{x \in \mathbb{Q} : x^3 > 2\} = \sqrt[3]{2}$.
- $\inf\{(-1)^n + \frac{1}{n} : n = 1, 2, 3, \dots\} = -1$.
- *If* $\{x_n\}_{n=1}^{\infty}$ *is a decreasing sequence with limit* x*, then* $\inf x_n = x$.

Complementary videos:

http://www.youtube.com/watch?v=8Cyvdv7Sm2s
http://www.youtube.com/watch?v=dY8aAP0JgkA
http://www.youtube.com/watch?v=3Z0B95lalpI

Quiz

- Q1 Supremum of a Bounded Set:

  Let $A = \{x \in \mathbb{R} : 0 < x < 1\}$. Find the supremum and infimum of A, and determine whether the supremum and infimum are contained within the set.

- Q2 Infimum of a Sequence:

  Consider the sequence $\{a_n\}$ defined by $a_n = \frac{1}{n}$ for $n \in \mathbb{N}_+$. Determine the set $B = \{a_n : n \in \mathbb{N}_+\}$, and find the infimum and supremum of B.