Sets, Functions and Induction (Natural numbers)

quarta-feira, 13 de janeiro de 2021 07:52

Preliminaries (Bartle, 2011)

1.1. Sets and Functions

- If an element x is in a set A, we write $x \in A$, otherwise $x \notin A$
- If every element of a set A belongs to a set B, we say A is a **subset** of B and write $A \subseteq B$ or $B \supseteq A$, otherwise $A \not\subseteq B$
- We say that B is a **proper subset** of A if $B \subseteq A$, but there is at least one element of B that is not in A

Def Two sets A and B are said to be **equal**, and we write $A = B$, if they contain the same elements, that is, $A \subseteq B$ and $B \subseteq A$.

- A set is defined by either listing its elements explicitly, or by specifying a property that determines the elements of the set
- If P denotes a property that is meaningful and unambiguous for elements of a set S, then we write $S = \{x : P(x)\}$

Set Operations

Def (a) The **union** of sets A and B is the set $A \cup B := \{x : x \in A \text{ or } x \in B\}$

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

(c) The **complement** of A relative to B is the set $A \setminus B := \{x : x \in A \text{ and } x \notin B\}$

- The set that has no elements its called the **empty set** and is denoted $\emptyset$
- Two sets A and B are called **disjoints** if $A \cap B = \emptyset$

Theorem If A, B, C are sets, then (De Morgans Law)

(a) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

(b) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

} useful to prove set equalities

Proof

(a) ⊢ $\forall x \in A \setminus (B \cup C) \Rightarrow x \in (A \setminus B)$ and $x \in (A \setminus C)$

If $x \in A \setminus (B \cup C) \Rightarrow x \in A$ and $x \notin B \cup C \Rightarrow x \in A$ and $x \notin B$ nor $x \notin C \Rightarrow x \in (A \setminus B) \cap (A \setminus C)$

⊢ $\forall x \in (A \setminus B) \cap (A \setminus C) \Rightarrow x \in A$ and $x \notin B \cup C$

If $x \in (A \setminus B) \cap (A \setminus C) \Rightarrow x \in A$ and $x \notin B$ and $x \notin C \Rightarrow x \notin B \cup C \Rightarrow$
$\Rightarrow x \in A \setminus (B \cup C)$ ∎

- Sometimes its useful to form unions and intersections of more than two sets, that is, for a finite collection of sets $\{A_1, \dots, A_n\}$, their **union** is the set A consisting of all elements that belong to **at least** one A_k, and their **intersection** consists of all elements that belong to **all** the sets A_k
- This extends to an infinite collection of sets $\{A_1, A_2, \dots\}$ as follows

$$\bigcup_{n=1}^{\infty} A_n := \{x : x \in A_n \text{ for some } n \in \mathbb{N}\} \quad \text{(union)}$$

$$\bigcap_{n=1}^{\infty} A_n := \{x : x \in A_n \text{ for all } n \in \mathbb{N}\} \quad \text{(intersection)}$$

Functions

Def If A and B are nonempty sets, then the **cartesian product** $A \times B$ of A and B is the set of all ordered pairs (a, b) s.t. $a \in A$ and $b \in B$. That is

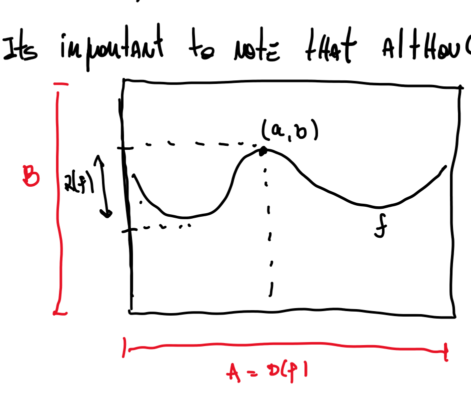
$$A \times B := \{(a, b) : a \in A, b \in B\}$$

Def* A **function** f from set A into B is a rule of correspondence ? that assigns to each element $x \in A$ a uniquely determined element $f(x) \in B$

Def Let A and B be sets. Then a **function** from A to B is a set f of ordered pairs in $A \times B$ s.t. for each $a \in A$ there exists a unique $b \in B$ with $(a, b) \in f$.

If $(a, b) \in f$ and $(a', b') \in f \Rightarrow b = b'$

- The set A of first elements of a function f is called the **domain** of f and is often denoted $D(f)$
- The set B of second elements of f is called the **range** of f and its often denoted $R(f)$
- Its important to note that although $A = D(f)$, we have $R(f) \subseteq B$

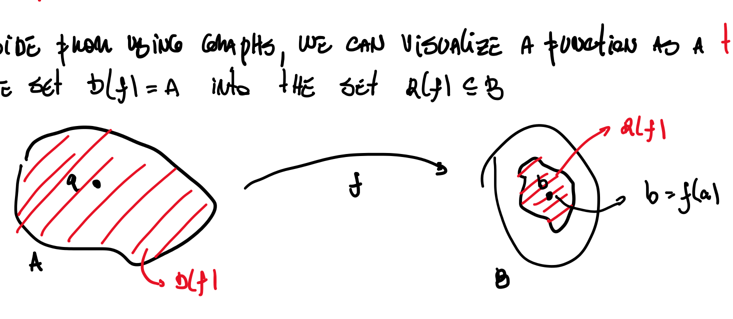


$b = f(a)$ or $a \mapsto b$

- If $b = f(a)$, we often refer to b as the **value / image** of a under f

Transformations

- Aside from using graphs, we can visualize a function as a **transformation** of the set $D(f) = A$ into the set $R(f) \subseteq B$



Direct and Inverse Images

- Let $f : A \to B$ be a function with domain $D(f) = A$ and range $R(f) \subseteq B$

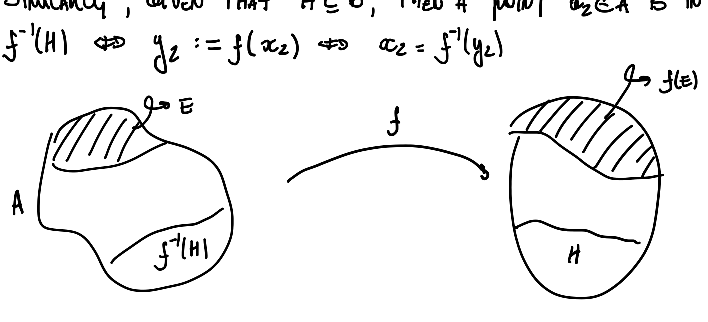
Def If E is a subset of A, then the **direct image** of E under f is the subset $f(E)$ of B given by

$$f(E) := \{f(x) : x \in E\}$$

If H is a subset of B, then the **inverse image** of H under f is the subset $f^{-1}(H)$ of A given by

$$f^{-1}(H) := \{x \in A : f(x) \in H\}$$

- Thus, given that $E \subseteq A$, then a point $y_1 \in B$ is in the direct image of $E \Leftrightarrow \exists\, x_1 \in E$ s.t. $y_1 = f(x_1)$
- Similarly, given that $H \subseteq B$, then a point $x_2 \in A$ is in the inverse image $f^{-1}(H) \Leftrightarrow y_2 := f(x_2) \Leftrightarrow x_2 = f^{-1}(y_2)$



Special types of functions

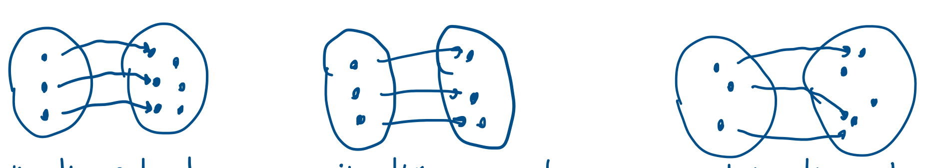
Def Let $f : A \to B$ be a function from A to B.

(a) The function f is said to be **injective** (or **one-one**) if $\forall x_1, x_2$ s.t. $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

onto: para a superfície ⑤ into: para dentro

(b) The function f is said to be **surjective** (or to map A onto B) if $f(A) = B$, that is, if the range $R(f) = B$.

(c) If f is both injective and surjective, then f is said to be **bijective**.



injective, but not surjective ⇒ not bijective

injective and surjective ⇒ bijective

not injective, not surjective ⇒ not bijective

- To prove that a function f is injective, we must establish that:

$$\forall x_1, x_2 \in A, \text{ if } f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

- To do this we assume that $f(x_1) = f(x_2)$ and show that $x_1 = x_2$
- To prove that a function f is surjective, we must show that for any $b \in B$ there $\exists$ at least one $x \in A$ s.t. $f(x) = b$

Def If $f : A \to B$ is a bijection of A onto B, then $g := \{(b, a) \in B \times A : (a, b) \in f\}$ is a function on B in A. This function is called the **inverse function** of f, and is denoted f^{-1}.

- We can express the connection between f and its inverse f^{-1} by noting that $D(f) = R(f^{-1})$ and $R(f) = D(f^{-1})$ and that $b = f(a) \Leftrightarrow a = f^{-1}(b)$

Def If $f : A \to B$ and $g : A \to B$, and if $R(f) \subseteq D(g) = B$, then the **composite function** $g \circ f$ is the function from A into C defined by

$$(g \circ f)(x) := g(f(x))$$

Theorem Let $f : A \to B$ and $g : B \to C$ be functions and let H be a subset of C. Then we have $(g \circ f)^{-1}(H) = f^{-1}(g^{-1}(H))$
↳ reversal

Restrictions of functions

- If $f : A \to B$ is a function and if $A_1 \subseteq A$, we can define a function $f_1 : A_1 \to B$ by $f_1(x) := f(x)$ for $x \in A_1$
- The function f_1 is called **the restriction of f to A_1**

1.2. Mathematical Induction (Bartle, 2011)

- Method of proof that is frequently used to establish the validity of statements that are given in terms of natural numbers
- We shall assume familiarity with the set of natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$ with the usual arithmetic operations of **addition** and **multiplication**, and with the meaning of a **natural number being less than another one**

Well-Ordering Property of $\mathbb{N}$ Every nonempty subset of $\mathbb{N}$ has a least element

Detailed version If S is a subset of $\mathbb{N}$ and if $S \neq \emptyset$, then there $\exists\, m \in S$ s.t. $m \leq k$ for $\forall k \in S$.

- We shall derive a version of the principle of induction on the basis of the principle of the well-ordering property

Principle of Mathematical Induction Let S be a subset of $\mathbb{N}$ that possesses the two properties:

(1) $1 \in S$

(2) for $\forall k \in \mathbb{N}$, if $k \in S \Rightarrow k+1 \in S$

Then, we have $S = \mathbb{N}$.

Section 1 - Natural Numbers (Lau, 2014)

Axiom (Well-ordering property of $\mathbb{N}$) If S is a nonempty subset of $\mathbb{N}$, then $\exists\, m \in S$ s.t. $m \leq k$, $\forall k \in S$.

Theorem (Principle of Mathematical Induction) Let $P(n)$ be a statement that is either true or false for $\forall n \in \mathbb{N}$. Then $P(n)$ is true for $\forall n \in \mathbb{N}$, provided that:

(a) $P(1)$ is true

(b) $\forall k \in \mathbb{N}$, if $P(k)$ is true $\Rightarrow P(k+1)$ is true

Proof

Proof strategy: proof by contradiction. $(p \Rightarrow q) \Leftrightarrow [(p \wedge \neg q) \Rightarrow c]$
suppose (a) and (b) are true but $P(n)$ is false for some $n \in \mathbb{N}$

Let $S = \{n \in \mathbb{N} : P(n) \text{ is false}\} \Rightarrow S \neq \emptyset$ and the well-ordering property guarantees the existence of an $m \in S$ that is least of S. Since $P(1)$ is true by hypothesis $\Rightarrow 1 \notin S \Rightarrow m > 1$. It follows that $m - 1 \in \mathbb{N}$, and since m is the least of $S \Rightarrow$
$\Rightarrow m - 1 \notin S \Rightarrow P(m-1)$ must be true (Basis of induction)
We now apply (b) $k = m - 1$ to conclude that $P(k+1) = P(m)$ is true $\Rightarrow m \notin S$, which contradicts the original statement. Therefore, it must be that $P(n)$ is true for $\forall n \in \mathbb{N}$ (induction step)

assumption that $P(k)$ holds - Induction hypothesis

Example - Prove that $1 + 2 + \dots + n = \frac{1}{2} n(n+1)$, $\forall n \in \mathbb{N}$

Let $P(n)$ be the statement $1 + 2 + \dots + n = \frac{1}{2} n(n+1)$.

(i) Basis of induction

$P(1) = 1 = \frac{1}{2} 1(1+1) = 1 \Rightarrow P(1)$ is true

(ii) Induction step

a) Induction Hypothesis: suppose $P(k) = 1 + \dots + k = \frac{1}{2} k(k+1)$ is true, $\forall k \in \mathbb{N}$.

$$P(k+1) = 1 + 2 + \dots + k + k+1 = \frac{1}{2} k(k+1) + k+1 = \frac{1}{2}\left[k(k+1) + 2(k+1)\right]$$

$$= \frac{1}{2}\left(k^2 + k + 2k + 2\right) = \frac{1}{2}\left[(k+1)^2 + 1 + k\right] = \frac{1}{2}(k+1)\left[(k+1) + 1\right]$$

$\Rightarrow P(k+1)$ is true for $\forall k \in \mathbb{N}$

PMI
$\Rightarrow P(n)$ is true for $\forall n \in \mathbb{N}$

Practice - Figure a general formula for the below statements and prove it using the PMI

$1 = 1^2 \qquad 1 + 3 = 2^2 \qquad 1 + 3 + 5 = 3^2 \qquad 1 + 3 + 5 + 7 = 4^2$

$2k - 1$, $k \in \mathbb{N}$
$k = 1 \Rightarrow 2 - 1 = 1$
$k = 2 \Rightarrow 4 - 1 = 3$
$k = 3 \Rightarrow 6 - 1 = 5$
⋮

$A = \{n \in \mathbb{N} : n = 2k - 1, k \in \mathbb{N}\}$

$$\sum_{k \in \mathbb{N}} (2k - 1) = k^2$$

$k = 1 \Rightarrow 2(1) - 1 = 1^2$
$k = 2 \Rightarrow 2(1) - 1 + 2(2) - 1 = 1 + 3 = 2^2$
⋮

Let $P(n)$ be the property $\sum_{n \in \mathbb{N}} (2n - 1) = n^2$.

(i) Basis of induction

$P(1) = \sum_{n=1}^{1} (2n - 1) = 2(1) - 1 = 1 = 1^2 \Rightarrow P(1)$ is true

(ii) Induction step

a) Induction Hypothesis: suppose $P(k) = \sum_{k \in \mathbb{N}} (2k + 1) = k^2$ is true, $\forall k \in \mathbb{N}$.

$P(k+1) = 1 + 3 + 5 + \dots + 2k - 1 + 2(k+1) - 1 = k^2 + 2k + 1 = (k+1)^2$

$2k + 2 - 1 = 2k + 1$

PMI
$\Rightarrow P(n)$ is true for $\forall n \in \mathbb{N}$

- There is a generalization of the PMI that enable us to conclude that a statement is true for every $n \in \mathbb{N}$ sufficiently large

Theorem Let $m \in \mathbb{N}$ and let $P(n)$ be a statement that is either true or false for $\forall n \geq m$. Then, $P(n)$ is true for $\forall n \geq m$, provided that:

(a) $P(m)$ is true

(b) for $\forall k \geq m$, if $P(k)$ is true $\Rightarrow P(k+1)$ is true

Proof - will use the original principle of induction

For $n \in \mathbb{N}$, let $Q(n)$ be the statement "$P(n + m - 1)$ is true".

Then from (a) we know that $Q(1)$ holds.

Now let $j \in \mathbb{N}$ and suppose that $Q(j)$ holds $\Rightarrow P(j + m - 1)$ is true $\Rightarrow Q(j+1)$ holds and the induction step is complete.

$P(j + 1 + m - 1) = P(j + m)$

∴ we conclude that $Q(n)$ holds for $\forall n \in \mathbb{N}$.

Now if $n \geq m$, let $n = n - m + 1$, $\forall n \in \mathbb{N}$. Since $Q(n)$ holds $\Rightarrow P(n + m - 1)$ is true. But $P(n + m - 1) = P(n) \Rightarrow P(n)$ is true for $\forall n \geq m$.

Section 1.2 (Bartle, 2011)

Theorem (Principle of Strong Induction) Let $S \subseteq \mathbb{N}$ such that:

(1') $1 \in S$

(2') for $\forall k \in \mathbb{N}$, if $\{1, 2, \dots, k\} \subseteq S$, $\Rightarrow k+1 \in S$

Then $S = \mathbb{N}$.