Notes on Calculus I

Jacopo Tissino

October 4, 2016

Chapter 1

Naïve set theory

1.1 Basic sets

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}, \qquad 0 \notin \mathbb{N} \tag{1.1.1}$$

$$\mathbb{R}^+ := \{x \in \mathbb{R} : x > 0\} \tag{1.1.2}$$

Remarks

- "$\in$" is for elements belonging to sets, "$\subseteq$" is for subsets
- $\{x\} \neq x$: the first is a set with x as its only element, and is called a "singlet"
- $\subsetneq$ means "is a subset of, but not equal to"
- the elements of $\mathcal{P}(A)$ are precisely all the subsets of A
- $\sharp A$ is the cardinality of A
- $\sharp\mathcal{P}(A) = 2^{\sharp A}$

The naïve definitions of $A \cup B$, $A \cap B$, $A \smallsetminus B$ are given.

Properties

- $A = (A \cap B) \cup (A \smallsetminus B)$
- $(A \cap B) \cap (A \smallsetminus B) = \emptyset$
- $C \cap (A \cup B) = (C \cap A) \cup (C \cap B)$
- $C \cup (A \cap B) = (C \cup A) \cap (C \cup B)$

Complement

Definition 1.1.1. With respect to a "universe" set U, we define the complement of A as $U \setminus A$, denoted A^C.

The following hold:

- $(A \cup B)^C = A^C \cap B^C$
- $(A \cap B)^C = A^C \cup B^C$

Cartesian product

Definition 1.1.2. An *ordered pair* is a set of the form $\{\{x\}, \{x, y\}\}$, denoted (x, y) (where order matters).

Definition 1.1.3. We define the *cartesian product* $A \times B$ of two sets A and B as:

$$A \times B := \big\{(a, b) : a \in A, b \in B\big\} \tag{1.1.3}$$

1.2 Propositional logic

Implication

Definition 1.2.1.

$$p \implies q \iff (\neg p) \vee q \tag{1.2.1}$$

Double implication

Definition 1.2.2.

$$(p \iff q) \iff (p \implies q \wedge q \implies p) \tag{1.2.2}$$

Quantifiers $P(x)$ is a *predicate.* We say that $\forall x : P(x)$ if $P(x)$ is true independently of x, and that

$$\exists x : P(x) \iff \neg(\forall x : \neg P(x)) \tag{1.2.3}$$

Chapter 2

Number sets

2.1 The set $\mathbb{N}$

The Peano axioms

1. $1 \in \mathbb{N}$
2. $\forall n \in \mathbb{N} : \exists S(n) : \mathbb{N} \to \mathbb{N}$
3. $\forall n \in \mathbb{N} : S(n) \neq 1$
4. $\forall m, n \in \mathbb{N} : m \neq n \implies S(n) \neq S(m)$ or $S(n) = S(m) \implies n = m$
5. $(A \subseteq \mathbb{N}) \wedge (1 \in A) \wedge (n \in A \implies S(n) \in A) \implies A = \mathbb{N}$

Any set that verifies these axioms is isomorphic to $\mathbb{N}$. $\mathbb{R}^+$, for example only satisfies the first 4.

2.2 Induction

If $P(n)$ is a proposition, $P(1)$ and $P(n) \implies P(n+1)$[1] (the *inductive hypothesis*); then $\forall n \in \mathbb{N}, P(n)$.

Proof. Define $A := \{n \in \mathbb{N} : P(n)\}$. By axiom 5, $A = \mathbb{N}$. □

If a property $a' : P(k)$ holds for some $k \in \mathbb{N}$ and $b' : P(n) \implies P(n+1)$, then $\forall n \geq k : P(n)$.

Examples Example: we can show by induction that

$$\sum_{i=1}^{n} = \frac{n(n+1)}{2} \tag{2.2.1}$$

Example 2: we can show by induction that $P(\sharp A) : \sharp\mathcal{P}(A) = 2^{\sharp A}$.

[1]We introduce the notation $n+1$ to signify $S(n)$.

Proof. $P(1)$ is true. We see that for any A we can take an element such that $A = \{a\} \cup B$. Then for any subset I, either $a \in I$ or $a \notin I$. If $a \in I$, $I = \{a\} \cup J$, but there are 2^n possible Js. If $a \notin I$, we have 2^n I's. So there are 2^{n+1} possible subsets. $\square$

Example 3: show that $n! > 2^n$, which is true for $n > 3$.

Proof. We will use the second form of the induction principle. $P(4)$ is true. If $n > 4$ and $n! > 2^n$, we need to show that $(n+1)n! > 2 \cdot 2^n$. But $n + 1 > 2$ by hypothesis, so the inequality always holds. $\square$

Observation: the notation $1 + 2 + 3 + 4 + \cdots + n$ is unclear, we should use $\sum_{i=1}^{n} i$.

Recursive formulas: we know the first term, and an algorithm to derive any term from the one before it, such as the definition of the factorial:

$$\begin{cases} 0! = 1 \\ (n+1)! = (n+1)n! \end{cases} \tag{2.2.2}$$

Another example is the sequence:

$$\begin{cases} S_1 = 2 \\ S_{n+1} = S_n + (2n+1) \end{cases} \tag{2.2.3}$$

Proof that $S_n = n^2 + 1$. Assume that $S_n = n^2+1$. Then $S_{n+1} = n^2+1+2n+1 = (n+1)^2 + 1$. $\square$

Formal definition of summation:

$$\sum_{i=0}^{n} a_i = a_0 + a_1 + a_2 + a_3 + \cdots + a_n \tag{2.2.4}$$

by recursion: for an increment in n, we just add the $n+1$-th term. So it comes down to the formal definition of induction.

Example: show by induction that

$$\forall a \in \mathbb{N} \vee a = 0 \quad (a \neq 1): \quad \sum_{k=0}^{n} a^k = \frac{1 - a^{n+1}}{1 - a} \tag{2.2.5}$$

See the property for $n = 0$. Suppose that the property holds for n, show it for $n + 1$:

$$\sum_{i=0}^{n+1} a_k = \sum_{k=0}^{n} a^k + a^{n+1} = \frac{1 - a^{n+1}}{1 - a} + a^{n+1} = \frac{1 - a^{n+2}}{1 - a} \tag{2.2.6}$$

To do: given two real numbers, $\forall n \in \mathbb{N}$, show that

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{2.2.7}$$

2.3 Groups

We have a set A with an operation $*$: $a, b \in A \to a * b \in A$. Es: A strings, $*$ concatenation. $(A, *)$ is a group if the following are satisfied:

1. Associativity: $\forall a, b, c \in A : \quad a * (b * c) = (a * b) * c$
2. Identity: $\exists e \in A : \forall a \in A : \quad e * a = a * e = a$
3. Inverse: $\forall a \in A : \exists a^{-1} \in A : \quad a * a^{-1} = a^{-1} * a = e$

$(A, *)$ is also a commutative group if $\forall a, b \in A : \quad a * b = b * a$

Examples: $(\mathbb{N}, +)$ is not a group: there is no identity, but even if we add 0 there is no inverse. $(\mathbb{Z}, +)$ is a commutative group. $(\mathbb{R}, \times)$ is not a group because 0 has no inverse. $(\mathbb{R}_0, \times)$ is hower a group, as is $(\mathbb{R}_0, +)$. $(\mathbb{Z}_0, \times)$ is not a group because there is no inverse: $(\mathbb{Q}_0, \times)$ is a commutative group.

So we introduce $\mathbb{Q}$:

$$\mathbb{Q} := \left\{ \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N} \right\} / \sim \tag{2.3.1}$$

but $ad \sim bc$ and $\mathbb{Q}$ is isomorphic to $\mathbb{Z}$

Definition 2.3.1. Order relation:

$$\frac{a}{b} \leq \frac{c}{d} \iff ad \leq bc \tag{2.3.2}$$

Definition 2.3.2. Sum and product, subtraction and division are analogous:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{2.3.3}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd} \tag{2.3.4}$$

$(\mathbb{Q}, +, \times)$ is then a field:

1. $(\mathbb{Q}, +)$ is a commutative group;
2. $(\mathbb{Q}_0, \times)$ is a commutative group
3. $p(q + r) = pq + pr$

Roots The square root of a number $a \geq 0$ is a $b \geq 0$ such that $b^2 = a$.

Show that in $\mathbb{Q}$ there is no $\sqrt{2}$:

Proof. By contradiction:[2] if there were $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that

[2] In the form: to show that $p \implies q$, we show that $\neg q \implies \neg p$, since

$$(p \implies q) \iff (\neg q \implies \neg p) \tag{2.3.5}$$

$$\left(\frac{a}{b}\right)^2 = 2 \tag{2.3.6}$$

Suppose that a, b have $\gcd(a, b) = 1$. Then $a^2 = 2b^2$. So a is even, and $a = 2k$. Then $4k^2 = 2b^2 \implies b = 2n$: so $\gcd(a, b) \neq 1$ $\square$

To do: show that $\sqrt{3}$ is irrational, $\sqrt[3]{2}$ is irrational.

2.4 The set $\mathbb{R}$

The set is given. $\mathbb{R}$ is a completely ordered field:

1. $(\mathbb{R}, +)$ is a commutative group
2. $(\mathbb{R}_0, \times)$ is a commutative group
3. $a(b + c) = ab + ac$

There also exists a relation called $\leq$, such that $\forall a, b, c \in \mathbb{R}$:

1. $a \leq a$
2. $a \leq b \wedge b \leq a \implies a = b$
3. $a \leq b \wedge b \leq c \implies a \leq c$
4. $a \leq b \vee b \leq a$ (*completely* ordered)
5. $a \leq b \implies a + c \leq b + c$
6. $a \geq 0 \wedge b \geq 0 \implies ab \geq 0$ (of course, $a \geq 0$ means that $0 \leq a$)

$(\mathbb{Q}, +, \times)$ is also a completely ordered field?

Take the set of all the real numbers whose squares are greater or equal to 2: it has a minimum.

In $\mathbb{Q}$, it has no minimum.

Other statements: show that $a \leq 0 \wedge b \geq 0 \implies ab \leq 0$

Proof. Is $a \geq 0 \wedge -b \geq 0$? We first need to show that $a \geq 0 \iff -a \leq 0$: it suffices to add $-a$ to both sides. We also need to show that $a(-b) = -ab$: by an inverse application of the distributive property. $\square$

Contents