Mathematical Analysis Lecture Notes

Prof J.J.Halliwell

1. Sets and Numbers

1.1 Sets and Subsets

A **set** is a collection of objects, called elements or members. The numbers $1, 2, 3$ form a set, for example, which we write as

$$S = \{1, 2, 3\}.$$

Although the members can be anything at all, such as $\{cat, dog\}$. If S is a set, we use the notation $x \in S$ to denote the statement "x belongs to the set S", or simply, "x is in S"; and $x \notin S$ to denote "x is not in S".

The most interesting and useful sets are set of numbers. Here are some important ones. There is the set of natural numbers (or counting numbers)

$$\mathbb{N} = \{1, 2, 3, ...\}.$$

This set is infinite, which means, loosely, that if you try and count its elements one by one, the counting never stops. If the counting procedure stops eventually, the set is finite, and we can assign a **cardinality** or **size** to a set S, denoted $|S|$, which is the number of elements it contains. So, for example

$$|\{1, 2, 3, \}| = 3.$$

Another important set is the set of all integers,

$$\mathbb{Z} = \{... - 2, -1, 0, 1, 2...\}.$$

Sets are commonly written using the notation

$$S = \{x \mid x \in P(x)\}.$$

which means, the set of all elements x which satisfy a certain property $P(x)$. For example, the natural numbers may be written in terms of the integers as

$$\mathbb{N} = \{x \mid x \in \mathbb{Z}, x > 0\}.$$

A natural object to define is a **subset** of a set. If A and B are sets, then A is a subset of B if every x in A is also in B. That is, $x \in A \Rightarrow x \in B$, and we write

$$A \subseteq B.$$

If there are elements in B which are not contained in A, then A is a **proper subset** of B and we write

$$A \subset B$$

So we have, for example, $\mathbb{N} \subset \mathbb{Z}$.

The relation $\subseteq$ is an example of an **order relation** and is similar to the relation $a \leq b$ for ordinary numbers. For example, we have, for sets A and B,

- $A \subseteq A$.
- If $A \subseteq B$ and $B \subseteq A$ then $A = B$.
- If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

The last property is often stated by saying that the relation $\subseteq$ is **transitive**.

There is an important difference between these relations and usual order relations for numbers in that every pair of numbers a, b satisfies either $a \leq b$ or $b \leq a$ but this is not true for sets. Take for example, the sets

$$A = \{1, 2, 3\}, \quad B = \{2, 3, 4\}$$

Then neither of the statements $A \subseteq B$ or $B \subseteq A$ are true. For this reason, the relation $\subseteq$ is called a **partial ordering** of sets.

Also, note that the definition of set equality has an interesting property. It means that the sets

$$\{1, 2, 3\}, \quad \{3, 2, 1\}, \quad \{1, 2, 3, 3\}$$

are all equal, even though they don't look quite the same. This is because what distinguishes one set from another is quite simply **membership**, and this doesn't distinguish between listing the elements in different orders, or including the same element twice.

1.2 Operations on Sets

Three operations on sets are particularly useful. These are:

- Union: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$
- Intersection: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$
- Difference: $A \backslash B = \{x \mid x \in A \text{ and } x \notin B\}$

(The difference is also written $A - B$ in some older texts but we won't use that here.) These definitions are easily visualized using Venn diagrams. Note the direct correspondence to the logical operations *or*, *and*, *not*.

The operators of union and intersection are both **commutative**, which means that

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

for all sets A, B. They are also **associative**, which means that

$$(A \cup B) \cup C = A \cup (B \cup C)$$

$$(A \cap B) \cap C = A \cap (B \cap C)$$

so we may simply drop the brackets in the above expressions without ambiguity. Also of interest is combinations of intersection and union – in this case brackets may **not** be dropped since the order of operation matters. We have

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

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

These are readily proved either algebraically or using Venn diagrams (and it is important to be familiar with both methods or proof).

It is often useful to define a fixed set of objects of interest, U, called the **universal set**, or universe of discourse, and then all discussion involves subsets of this set. Then it is natural, for a given set $A \subseteq U$ to define the **complement** of A, denoted A', which is the set of all elements in U not in A. Also written,

$$A' = \{x \mid x \in U \text{ and } x \notin A\} = U \backslash A$$

The complement has the property that if $A \subseteq B$, then $B' \subseteq A'$.

The "opposite" of U is the so-called **empty set** $\emptyset$, which arises when we intersect two sets A and B with no elements in common,

$$A \cap B = \emptyset$$

U and $\emptyset$ satisfy the following properties for any set A and its complement A'

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

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

Finally, not so obvious are De Morgan's laws,

$$(A \cup B)' = A' \cap B'$$

$$(A \cap B)' = A' \cup B'$$

Again all the above are readily proved algebraically or using Venn diagrams.

The size (cardinality) of sets under the operations of union or intersection are related by theorem:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

This is readily proved as follows. Suppose the elements $a_1, \cdots a_k$ lie in A but not B, the elements $b_1 \cdots b_\ell$ lie in B but not A, and the elements $x_1, \cdots x_n$ lie in A and B. Then we clearly have $|A| = k + n$, $|B| = n + \ell$, $|A \cup B| = k + n + \ell$ and $|A \cap B| = n$. The result then follows.

A generalization to three sets is readily proved, namely:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

One more operation on sets which is of interest is to contsruct is the **power set** $P(A)$ from a set A, which is the set of all possible subsets. For example the set $A = \{a_1, a_2\}$ has four subsets: the empty set $\emptyset$, $\{a_1\}$, $\{a_2\}$ and the set A itself. In general the power set has size 2^n for a set A of size n, i.e. $|P(A)| = 2^{|A|}$, and we therefore often use the notation $P(A) = 2^A$.

A useful way of combining sets is the **Cartesian product**, defined for sets A, B by

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

That is, $A \times B$ is the set of ordered pairs (a, b). It is not hard to see that, for finite sets, the size of this product is $|A \times B| = |A|\ |B|$. A familiar example of this product is the 2-dimensional plane, $\mathbb{R}^2$, which is defined to be the Cartesian product

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}.$$

1.3 Russell's Paradox

A set is a collection of elements. Can these elements be anything we like? An example of a "wild" set is the **set of all sets**:

$$S = \{x|x \text{ is a set}\}$$

Problems in the definitions of sets arise when we take the members of sets to be themselves sets in an unrestricted manner.

Russell's Paradox: Define the set of all sets that do not have themselves as an element:

$$R = \{x|x \text{ is a set },\ x \notin x\}$$

Now R is a set whose elements are sets. Is it an element of itself?

- Suppose the answer were yes, so $R \in R$. This is a contradiction since the elements x of R obey $x \notin x$.
- Suppose the answer were no, so $R \notin R$. This is a contradiction since R contains all sets x that do not contain themselves, ie. $x \notin x$.

Thus either answer, yes or not, leads to contradiction.

1.4 Functions on Sets

We often think of a function in terms of a curve $y = f(x)$ in the xy-plane, such as $y = x^2$. Functions of this type are real-valued functions of real numbers, i.e. maps from $\mathbb{R}$ to itself. However, for functions such as

$$f(x) = \frac{\ln(x^2 - 1)}{(x-2)(x-3)}$$

one has to give attention to restrictions on possible values of x in order for the function to be well-defined – in this case we need $x^2 > 1$, $x \neq 2$, $x \neq 3$. Similarly, there are questions as to the extent that relations such as $y = x^2$ have an inverse. We might naively write $x = \pm\sqrt{y}$ but specification of the admissable ranges of x and y is necessary to make the inverse well-defined. These sorts of issues are readily handled using a very general definition of a function, as a map between specified sets.

1.4.1 Definitions

A **function** or **map** is a rule which, for every element of a set D, uniquely assigns an element of another set T.

- D is known as the **domain**
- T is known as the **target** or **codomain**
- If we label the map itself by f, we write

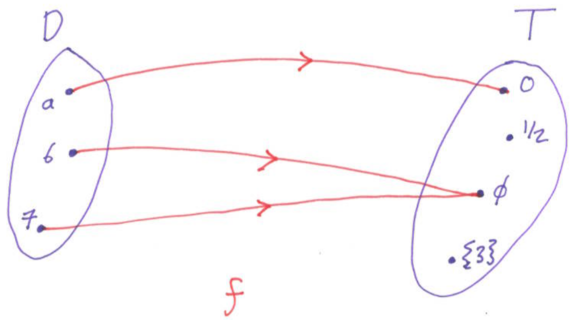
  $$f: \ D \to T$$

  or if we are more explicit about specifying the map,

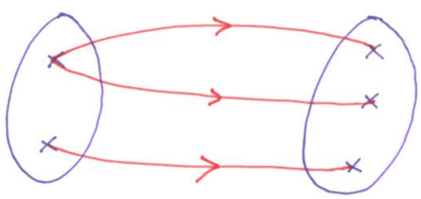
  $$\begin{aligned} f: \quad D &\to T \\ x &\to f(x) \end{aligned}$$

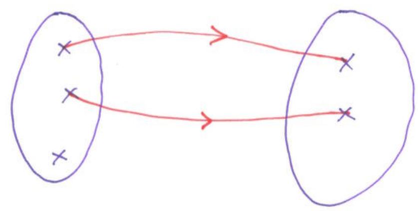
  where $x \in D$ and $f(x) \in T$.

Example: $D = \{a, 6, 7\}$ to $T = \{0, \frac{1}{2}, \emptyset, \{3\}\}$. Consider a map $g : D \to T$ defined as $g(a) = 0$, $g(6) = \emptyset$, $g(7) = \emptyset$.



Note that the definition of map does not permit certain situations, such as these two:





In the first, a single point in D maps to two points in T and is excluded since the definition of map means that the point in T mapped to is *unique*. In the second, there are points in D for which no point in T is given, and this possibility is excluded since the definition of map means that *every* element of D is assigned a point in T.

The **image** (or **range**) of a map $f : D \to T$ is the set of elements of T that those of D are mapped to.

$$\text{Image}(f) = \{y \in T \,|\, \exists\, x \in D \text{ s.t. } f(x) = y\}$$

This is sometime written $f(D) = \text{Image}(f)$.

Example. Consider the map $f(x) = x^2 - 4$, where $D = \{1, 2, 3\}$ and $T = \mathbb{Z}$. We have $f(1) = -3, f(2) = 0, f(3) = 5$ so $\text{Image}(f) = \{-3, 0, 5\}$.

1.4.2 Examples

1. $f : \mathbb{R} \to \mathbb{R}$, with $f(x) = 1/x$, is **not** a map as $f(0)$ is not well defined. However, it can be made well-defined by removing $x = 0$ from the domain and

$$\begin{aligned} g : \mathbb{R} \setminus \{0\} &\to \mathbb{R} \\ x \quad &\to \frac{1}{x} \end{aligned}$$

   is a well defined map.

2. $f : \mathbb{R} \to \mathbb{R}$, with $f(x) = \tan(x)$, is **not** a map. The map is not well defined at $x = \pm\frac{\pi}{2}, \pm\frac{3\pi}{2}, \ldots$. However,

$$\begin{aligned} g : (-\frac{\pi}{2}, +\frac{\pi}{2}) &\to \mathbb{R} \\ x \quad &\to \tan x \end{aligned}$$

   is a well defined map.

3. $f : \mathbb{R} \to \mathbb{R}$, with $f(x)$ defined so that $\sin(f(x)) = x$, (i.e. $f(x)$ is the inverse of $\sin(x)$) is **not** a map. Firstly there are many values z such that $\sin z = 0$ so there is no unique specification of a map. Secondly consider $|x| > 1$ which doesn't get mapped anywhere. However,

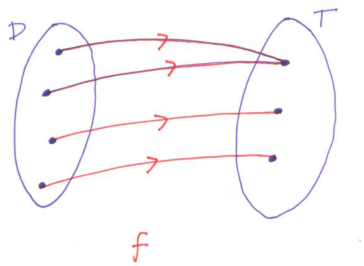
$$\begin{aligned} g : [-1, +1] &\to [-\frac{\pi}{2}, +\frac{\pi}{2}] \\ x \quad &\to \arcsin x \end{aligned}$$

   is a well defined map. Note that Image$(g) = [-\frac{\pi}{2}, +\frac{\pi}{2}]$.

1.4.3 The Three Important Types of Maps

Amongst the maps defined in the way above, it is of interest to highlight three particular types.

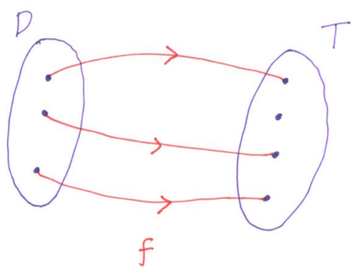
A map $f : D \to T$ is **surjective** (or **onto**) if for every $y \in T$ there exists an $x \in D$ s.t. $f(x) = y$.



No target element is "missed out"

Note: for a surjection $f : D \to T$ then $\text{Image}(f) = T$.

A map $f : D \to T$ is **injective** (or **one-to-one**) if $x \neq y$ implies $f(x) \neq f(y)$ for all $x, y \in D$.

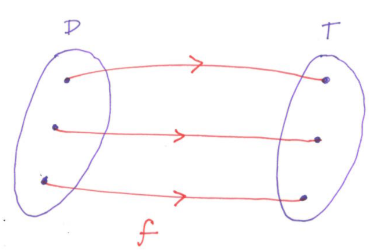


Alternatively, a map $f : D \to T$ is **injective** (or **one-to-one**) if $f(x) = f(y)$ implies $x = y$ for all $x, y \in D$.

Every domain element is uniquely paired with one in the target.

For an injective map $\text{Image}(f) \subseteq T$ and indeed we may have $\text{Image}(f) \subset T$.

A map $f : D \to T$ is **bijective** if it is both **injective** and **surjective**.



Each domain element is uniquely paired with a target element and vice versa.

Given a **bijective map** $f : D \to T$, then the **inverse map** exists. It is denoted f^{-1} and is defined by,

$$\begin{aligned} f^{-1} : T &\to D \\ y &\to x(y) \end{aligned}$$

such that $y = f(x)$. Such a map exists because f is surjective, and is unique because f is an injection.

Example. Consider the map $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x$. It is injective but not surjective, because odd numbers in the target space have no corresponding elements in the domain.

Example. Consider the map $f : \mathbb{N} \to \mathbb{N}$ defined by $f(1) = 1$ and $f(x) = x - 1$ for $x \geq 2$. The map is surjective but not injective, because $x = 1$ and $x = 2$ are both mapped to $x = 1$.

Example. Consider the map $f(x) = x^2$ and determine whether it is surjective, injective and bijective for various choices of domains D and targets T. The choices of domains are $\mathbb{R}$, $\mathbb{R}_0^+$, $\mathbb{R}_0^-$ and the choices of targets are $\mathbb{R}$ and $\mathbb{R}_0^+$. Here, $\mathbb{R}_0^+$ denotes the set of points $x \in \mathbb{R}$ with $x \geq 0$ and $\mathbb{R}_0^-$ denotes points $x \in \mathbb{R}$ with $x \leq 0$.

Note that surjective, injective and bijective are **not the only possibilities**. Consider for example the map $f : D \to T$ where $|D|$ and $|T|$ are both greater than or equal to 2, and suppose f maps every point in D to a single point in T. It is not surjective, since points in T are missd out, and it is not injective, since it is many to one.

Theorem: Let $f : A \to B$ be a map between **finite** sets A and B. Then,

1. If f is a surjection then $|A| \geq |B|$
2. If f is an injection then $|A| \leq |B|$
3. If f is a bijection then $|A| = |B|$

Proof: Let $A = \{a_1, a_2, \ldots, a_n\}$ so $n = |A|$. Let,

$$R = \text{Image}(f) = \{b \in B | \exists\, a_i \in A \text{ s.t. } f(a_i) = b\}$$

Hence we may write, $R = \{f(a_1), f(a_2), \ldots, f(a_n)\} \subseteq B$ although generally some $f(a_i)$ will be equal, and hence the list for R may have repeated elements. Hence we have $|R| \leq |A| = n$ and $|R| \leq |B|$. Now,

1. If f is a surjection then $R = B$ and so $|B| \leq n$. Therefore $|B| \leq |A|$.
2. If f is an injection then $f(a_i) \neq f(a_j)$ for $i \neq j$, and so $|R| = |A| = n$. Then, $|A| \leq |B|$.
3. If f is a bijection then both $|B| \leq |A|$ and $|A| \leq |B|$ must be true which implies $|A| = |B|$.

The Pigeonhole Principle: If you have N pigeons and M pigeonholes and $N > M$, some pigeon hole must contain more than one pigeon.

Differently put, if $f : A \to B$ for finite sets A, B such that $|A| > |B|$ then f is not an injection, i.e. it must be $2 : 1$ somewhere.

Example. This principle is a very useful one for proving various simple results. For example, given any six numbers $n_i \in \mathbb{N}$, $i = 1, 2 \cdots 6$, then there exists a pair whose difference is divisible by 5. To prove this we write

$$\frac{n_i}{5} = p_i + F_i$$

where $p_i \in \mathbb{N}$ and the six remainders F_i takes one of the five values $0/5, 1/5, 2/5, 3/5, 4/5$. By the pidgeonhole principle two of the F_i must be the same, lets say $F_2 = F_4$. It follows that

$$\frac{n_4 - n_2}{5} = p_4 - p_2$$

which is an integer. QED.

Example. Show that there are two people in London with the same number of hairs on their head.

Example. Imagine a party has $n \geq 2$ people and everyone knows at least one other person. Then there must be at least two people who have exactly the same number of friends.

1.4.4 Functional Composition

Given maps $f : X \to Y$ and $g : Y \to Z$ then we define the **composition** of f with g as,

$$\begin{aligned} g \circ f : X &\to Z \\ x &\to g \circ f(x) = g(f(x)) \end{aligned}$$

Note: $g \circ f(x)$ means act first with f, then act with g on the result.

Proposition: Let $f : X \to Y, g : Y \to Z$ and $h : Z \to W$ be maps. Then,

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

This means we can unambiguously write the composition of these three maps as $h \circ g \circ f$.

Proof: Consider LHS:

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

Consider RHS:

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

Hence the LHS = RHS.

2. Numbers

This section of the course concerns the important foundational questions about the properties and definitions of different types of numbers – the natural numbers, rationals and reals. We will in particular build up to **the formal definition of the real numbers**, a definition more precise than its intuitive definition as the set of all possible infinite decimals. We will also in this section discuss different **types of proof** in mathematical arguments.

2.1 Prime Numbers

Amongst the natural numbers $\mathbb{N}$, an important subset are the prime numbers, numbers which have only themselves and 1 as divisors. So $2, 3, 5, 7, 11, 13, 17...$ are prime. An important result, due to Euclid, is that **there are an infinite number of primes**.

We state this is a theorem, and the proof is an elegant example of the method of **proof by contradiction**, or *reductio ad absurdum*. In this method, to prove a proposition P, we start by supposing that P is false and then examine the consequences. If we can show that P false leads to a contradiction, then P cannot be false. P cannot be false means that P must be true, which proves our theorem.

Theorem

There are infinitely many prime numbers.

Proof

- Suppose, for a contradiction, that there are finitely many primes, $p_1, p_2, \cdots p_n$, where p_n is the largest. Any number larger must therefore be divisible by one of these numbers.

- We produce a contradiction by writing down a number which is a larger than any of them, but not divisible by them. The number is

$$A = p_1 p_2 \cdots p_n + 1$$

  Clearly A is larger than any one of $p_1 \cdots p_n$.

- However, it is not divisible by any of them, since it always leaves remainder 1. Contradiction! Hence the original statement that there are finitely many primes must be false. QED.

It is good practice to end a proof with the letters QED (*Quod Erat Demonstrandum* – "which was to be proved") or with square $\square$. For very simple theorems we don't even bother to set it out as theorem-proof. For example, the square of an even number is even, because $(2n)^2 = 4n^2$ which is clearly even for any n. Similarly, the square of an odd number is odd, because, an odd number has the form $2n + 1$, and

$$(2n + 1)^2 = 4n^2 + 4n + 1$$

which has the form of an even number plus 1, so is odd.

Natural numbers which are not prime are called composites. Given that both the primes and the composites are infinite in number, it is natural to wonder how they are distributed. There are a number of results in this direction.

- $n! + 1$ can be prime for some n, but the numbers

$$n! + 2,\ n! + 3,\ n! + 4, \cdots n! + n$$

  are all composites.

- A very deep result about the distribution of primes is that for large n, the number of prime numbers less than n is approximately $n/\log n$.

- The Goldbach conjecture: every even number is the sum of two primes. (Unproved)

- The Twin Primes conjecture: there are infinitely many primes p such that $p + 2$ is also prime. (Unproved)

It is not hard to guess that every composite number may be expressed in terms of produces of primes. For example,

$$24 = 2 \times 2 \times 2 \times 3$$

To obtain this expression we divide by 2 as many times as we can, then by 3 and so on. This leads to another very important result of Euclid:

The Fundamental Theorem of Arithmetic

> Every number has a unique factorization as products of prime numbers. That is, every number N may be uniquely expressed in terms of primes $p_1, p_2, \cdots$ as
>
> $$N = p_1^a \times p_2^b \times p_3^c \cdots$$
>
> where the natural numbers $a, b, c \cdots$ are unique.

Proof

> A proof is easily sketched along the lines of the simple example above. For given N, divide repeatedly by p_1 until no longer possible. This fixes a. Then divide repeatedly by p_2, until it stops, which fixes b. This process is clearly finite so proceeding in this way yields the above factorization.
>
> To see that the factorization is unique, suppose there was another factorization with powers $a', b', c' \cdots$. We then have
>
> $$p_1^a \times p_2^b \times p_3^c \cdots = p_1^{a'} \times p_2^{b'} \times p_3^{c'} \cdots .$$
>
> However, by simply cancelling out powers of the primes on each side, it is readily seen that we must have $a = a'$, $b = b'$, etc. QED.

2.2 Proof by Induction and Proof Generally

We have used proof by contradiction above. A second and very important method of proof is **proof by induction**. Suppose we want to prove a class of propositions $P(n)$ that depend on a number n. For example, consider the sum

$$S_n = \sum_{k=1}^{n} k = 1 + 2 + 3 + \cdots n$$

and we would like to prove that

$$S_n = \frac{1}{2}n(n+1)$$

for all n. (Of course, in this case, this can be calculated, but here we use it to illustate the method). In proof by induction, we proceed by proving two things.

(i) That $P(1)$ is true.

(ii) That for each $r \in \mathbb{N}$, if $P(r)$ is true, then $P(r+1)$ is true.

If we can prove both of these statements, then $P(n)$ is true for all n. To illustrate, let us use proof by induction to prove the above proposition.

(i) $P(1)$ is the assertion that

$$S_1 = \frac{1}{2}.1.2. = 1$$

This is clearly true. (But one must always prove this step, no matter how trivial!).

(ii) Now we suppose that $P(r)$ is true, so

$$S_r = \frac{1}{2}r(r+1)$$

Then,

$$S_{r+1} = S_r + r + 1 = \frac{1}{2}r(r+1) + r + 1$$

which rearranges to

$$S_{r+1} = \frac{1}{2}(r+1)(r+2)$$

This shows that if the statement is true for $n = r$ then it is also true for $n = r + 1$. We have established both parts which proves the proposition. QED.

Proof by contradiction and proof by induction are two of the most important methods of proof in mathematics. A proof is quite simply a **clear and convincing argument**. A few comments about this should be kept in mind.

- Try to write the proof out in a clear and well written way - just as you would want to read it.
- To contradict a proposition a single counterexample is sufficient.
- Obviously do not use the result you are trying to prove. I.e. pay attention to the direction of the logic.

Example. To illustrate the last point suppose we want to prove that $\sqrt{6} - \sqrt{2} > 1$. A false proof is as follows: squaring the inequality yields

$$1 < (\sqrt{6} - \sqrt{2})^2 = 8 - 2\sqrt{12} \implies 2\sqrt{12} < 7 \implies 48 < 49$$

a true result. However, this does not prove the original inequality since the logic runs in the wrong direction. A correct way to prove the result would be to use a proof by contradiction and suppose that $\sqrt{6} - \sqrt{2} \leq 1$. Following the same steps we get

$$1 \geq (\sqrt{6} - \sqrt{2})^2 = 8 - 2\sqrt{12} \implies 2\sqrt{12} \geq 7 \implies 48 \geq 49$$

which is false. Hence the original supposition $\sqrt{6} - \sqrt{2} \leq 1$ is false. QED.

The phrase **necessary and sufficient condition** is frequently used.

- A is a sufficient condition for B means $A \implies B$.
- A is a necessary condition for B means $B \implies A$.
- A is a necessary and sufficient condition for B means A and B are logically equivalent (i.e. imply each other).

The phrase **if and only if** is also often used.

- A only if B means $A \implies B$.
- A if B means $B \implies A$.
- A if and only if B means that A and B are logically equivalent.

2.3 Rational and Irrational Numbers

The next important set of numbers of interest is the set of **rational numbers**, meaning numbers of the form m/n. Precisely, the rationals are denoted by $\mathbb{Q}$ and defined by

$$\mathbb{Q} = \{m/n \mid m, n \in \mathbb{Z}, n > 0\}.$$

These arise because in basic numerical operations, counting is not enough. We often need to divided things into equal parts. So we need also to consider the numbers $1/2, 2/3, 3/4 \cdots$.

It is readily shown that addition, subtraction, multiplication and divison of rational numbers produces a rational number. I.e. the rationals are closed under basic arithmetic operations.

From the point of view of physics, the rational numbers are enough, since every number we come across in physics is only ever measured to within finite precision. This naturally raises the question as to whether all numbers we ever come across are rational. Yet another great achievement of the Greeks was to show that this is not the case. In particular, numbers like $\sqrt{2}$ cannot be expressed in rational form. They can be approximated arbitrarily closely by rationals, but the exact number is not rational (as we show below). Numbers of the form $\sqrt{2}$ clearly arise in **geometry** – it is the hypotenuse of a right-angled triangle whose two shorter sides are length 1. Also, as we will see later, many interesting objects in physics are defined in terms of **limits** and these naturally throw up irrational numbers.

Theorem

$\sqrt{2}$ is irrational.

Proof

The proof is a very elegant example of proof by contradiction. To see the logic most clearly it is useful to number the key steps.

1. We suppose, for contradiction, that $\sqrt{2}$ is rational. Then it may be written

$$\sqrt{2} = \frac{p}{q}$$

for $p, q \in \mathbb{N}$. (There is nothing lost in taking both $p, q > 0$).

2. Now an important comment. If p and q have any common factors, we may cancel these out. Hence, without loss of generality, we may take p and q to have no common factors. This means in particular that they cannot both be even.

3. Squaring up, we get

$$p^2 = 2q^2$$

which means that p^2 is even. This implies that p must be even. (If it was odd, it would square to an odd number, as we showed above). So $p = 2r$, for $r \in \mathbb{N}$.

4. Inserting $p = 2r$, we get

$$4r^2 = 2q^2$$

or $q^2 = 2r^2$. This means that q^2 is even, and so q is even.

5. We now have that both p and q are even. But this contradicts point number 2 above. QED.

Similar methods may be used to prove the irrationality of $\sqrt{3}$ and $2^{\frac{1}{3}}$.

An **alternative method** is to make use of the **fundamental theorem of arithmetic**. For example, to show that $\sqrt{5}$ is irrational, we write $\sqrt{5} = n/m$, for $n, m \in \mathbb{N}$, hence $n^2 = 5m^2$. Using the fundamental theorem of arithmetic we may write

$$n = 2^a 3^b 5^c 7^d \cdots \quad \text{and} \quad m = 2^{a'} 3^{b'} 5^{c'} 7^{d'} \cdots$$

where $a, b, c, d \cdots$ and $a', b', c', d' \cdots$ must be integers. Since $n^2 = 5m^2$, we have

$$2^{2a} 3^{2b} 5^{2c} 7^{2d} \cdots = 2^{2a'} 3^{2b'} 5^{2c'+1} 7^{2d'} \cdots$$

From this it must follow that $a = a'$, $b = b'$, $d = d'$ etc but $2c = 2c' + 1$, which is a contradiction, since c and c' are integers. QED. This method clearly generalizes readily.

Exercise A different technique is required to show that e is irrational. We have

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}$$

and we suppose, for contradiction, that $e = p/q$, for $p, q \in N$. Hence $p = eq$ and

$$(q-1)!\ p = e\ q! = q!\ \left[\left(2 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{q!}\right) + \frac{1}{(q+1)!} + \cdots\right]$$

This equation has the form

$$\text{integer} = \text{integer} + R$$

where

$$R = q!\ \left[\frac{1}{(q+1)!} + \frac{1}{(q+2)!} + \cdots\right] = \frac{1}{(q+1)} + \frac{1}{(q+1)(q+2)} + \cdots .$$

We show that $R < 1$, hence obtain a contradiction. Clearly nothing is lost by taking $q > 2$ so $1/(q+1) < 1/3$ and we have

$$R < \frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots = \frac{1}{2} < 1$$

which proves the result.

Having established that irrationals such as $\sqrt{2}$ exist, we can say a bit more about them. Irrational numbers such as $\sqrt{2}$ or $3^{1/4}$ are examples of so-called **algebraic numbers**. These are numbers x which satisfy a polynomial equation of the form

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots a_1 x + a_0 = 0$$

where the coefficients a_k are all integers. So $\sqrt{2}$ satisfies

$$x^2 - 2 = 0$$

for example. It seems reasonable to ask whether all algebraic numbers may be expressed in terms of roots of whole numbers. This is certainly true for the quadratic case and it turns out to be true for cubic and quartic equations. However, the important work of Abel and Galois showed that 5th order and higher algebraic equations have roots which are not expressable in simple roots.

But are the algebraic numbers all there is? It turns out that the answer to this is no. It can be shown that numbers such as e and π are not solutions to algebraic equations with integer coefficients. Such numbers are called **transcendental**. It is hard to prove that a given number if transcendental but it is not hard to prove that"most" numbers are in fact transcendental.

2.4 The Decimal Representation

The largest class of numbers we encounter, which includes natural numbers, rationals, algebraic and transcendental numbers is referred to as the **real numbers**, denoted $\mathbb{R}$. This has yet to be properly defined, but in practical terms, it is most easily thought of in terms of the decimal representation and we now explore this.

When we write down a number such as 23.792 what we mean by this notation is

$$23.792 = 23 + \frac{7}{10} + \frac{9}{100} + \frac{2}{1000}$$

Generally, every real number has a decimal representation, i.e. may be expressed in the form

$$x = a_0 + \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \cdots ,$$

and we write

$$x = a_0 \cdot a_1 a_2 a_3 \cdots$$

Here, $a_0 \in \mathbb{Z}$ and a_i for $i = 1, 2, 3 \cdots$ take values $0, 1 \cdots 9$. The decimal expansion may of course be infinite. The existence of the decimal representation follows from a more fundamental definition of the reals (given later) and by dividing the real line into progressively smaller intervals each ten times smaller than the previous one.

The decimal expansion is **not unique** since infinite decimals ending in an infinite sequence of nines have two different representations. For example

$$0.999 \cdots = 9 \left(\frac{1}{10} + \frac{1}{100} + \frac{1}{1000} + \cdots \right)$$

Using the convenient formula

$$x + x^2 + x^3 + \cdots = \frac{x}{(1-x)}$$

we may sum the series and find that $0.999 \cdots = 1.000 \cdots$.

A natural question to ask is whether the difference between rational and irrational numbers can be seen in the decimal representation. The answer to this is yes, as is easily seen. First, consider the rational number $6/7$, which can be computed in decimal by explicitly doing a long division, with the result:

$$\frac{6}{7} = 0.857142857142 \cdots = 0.\overline{857142}$$

That is, its decimal representation is periodic. This happens because in carrying out the long division of 7 into $6.000\cdots$, each operation produces a remainder, but eventually we must get a remainder which occured before. It is not hard to see that this is always the case for a rational number, hence **rational numbers are always represented by periodic decimals**, that is those of the general form

$$x = a_0.a_1a_2\cdots a_j\overline{b_1b_2\cdots b_k}$$

Conversely, **a periodic decimal is always a rational number**. For example, consider

$$x = 0.121212\cdots$$

We see that

$$100x = 12.121212\cdots = 12 + x$$

which is readily solved to yield $x = 4/33$. More generally, consider the periodic decimal

$$x = 0.\overline{b_1b_2\cdots b_k}$$

and define $B = 0.b_1b_2\cdots b_k$, which is clearly rational (since its decimal is finite). We have

$$10^k x = 10^k B + x$$

and therefore

$$x = \frac{10^k B}{10^k - 1}$$

which is clearly rational.

Also of interest is the **binary representation** which arises when we divide up the real line into progressively smaller intervals each half the size of the previous one. Binary numbers have the form

$$x = a_1\cdots a_n.b_1b_2\cdots$$

where a_i, b_i take values 0 or 1. For example

$$x = 101.011 = 1\times 2^2 + 0\times 2^1 + 1\times 2^0 + 0\times\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} = \frac{43}{8}.$$

Generally for $x \le 1$, the binary representation has the form

$$x = \sum_{n=1}^{\infty}\frac{a_n}{2^n}$$

where $a_n = 0, 1$. Like the decimal representation it is not unique because, for example, $0.111\cdots$ is the same as 1.

We can actually use any natural number as the base. Later on we will have reason to use the **ternary representation** (base 3), in which any $x \leq 1$ may be written

$$x = \sum_{n=1}^{\infty} \frac{a_n}{3^n}$$

where $a_n = 0, 1, 2$. For example in ternary

$$x = 0.201 = \frac{2}{3} + \frac{0}{9} + \frac{1}{27} = \frac{19}{27}$$

2.5 Rational Approximations

Clearly in many numerical approximation technique it is necessary to approximate real numbers by rationals, since computers can handle only finite decimals. Hence it is of interest to see how good rational approximations can be. One might of thought that a rational approximation p/q to a real x would have error of order $1/q$ but it turns out one can do a lot better than this. For example, $\sqrt{2} = 1.414\cdots$ is approximated to an unusually surprising degree by $7/5 = 1.4$, And $\sqrt{3} = 1.732\cdots$ is well-approximated by $7/4 = 1.75$. These results are explained by the following theorem:

Theorem

For any $x \in \mathbb{R}$, there exists a rational p/q such that $\left|x - \frac{p}{q}\right| \leq \frac{1}{q^2}$.

This means that the error is of order $1/q^2$, not $1/q$. Proof of this statement is an elementary application of the pigeonhole principle (and is NE).

2.6 Countability and Uncountability

The sets of numbers we have been considering so far, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are all infinite sets, but such sets come in different types, that is, there are differen types of infinity. The key notion behind this is the **countability** of a set.

Definition

An infinite set of objects is said to be countable if the objects can be put into an ordered list of the form $\{a_1, a_2 \cdots\}$. More precisely, a set A is countable if there exists a bijection $f : \mathbb{N} \to A$.

For example, the set of even numbers is countable, since it can be arranged in a list $\{2, 4, 6, 8 \cdots\}$. Similarly, the set of positive and negative integers is countable, since it can be written as $\{0, -1, 1, -2, 2 - 3, 3 \cdots\}$. More formally, one can introduce the map $f(2n) = n$ and $f(2n-1) = -(n-1)$ which is a bijection from $\mathbb{N}$ to $\mathbb{Z}$.

A useful result is that any infinite subset $S \subset \mathbb{N}$ is also countable. This is trivial in some sense since S is clearly "smaller" than $\mathbb{N}$. A more precise proof is to order the elements of $S = \{s_1, s_2, s_3 \cdots\}$ so that $s_1 < s_2 < s_3 < \cdots$ and the required bijection is then $f(s_1) = 1$, $f(s_2) = 2$ etc which is clearly a bijection from S to $\mathbb{N}$.

Theorem

The rational numbers are countable.

Proof

There are a number of ways to prove this result. One is to write out the rational numbers as a matrix with elements m/n, where $m, n \in \mathbb{N}$. It is then easy to find a zig-zag line running through the array which includes all elements of the array, so is an ordered list of elements.

Another way to see it, is to note that we can associate every rational m/n (in lowest terms) with the natural number $2^m \times 3^n$. By the fundamental theorem of arithmetic, this gives a bijection correspondence between a subset of the natural numbers and the integer pair (m, n) (since $2^m 3^n = 2^p 3^q$ is equivalent to $m = p$ and $n = q$). QED.

This proof is in essence a proof that there is a bijection from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$, so the latter is countable. It readily follows by repeated application of this argument that $\mathbb{N} \times \mathbb{N} \times \cdots \mathbb{N}$ is also countable, for any number of copies of $\mathbb{N}$ (i.e. any set of n-tuples $(n_1, n_2, \cdots n_k)$, where each n_i is in $\mathbb{N}$). Unions of two infinite countable sets are readily shown to be countable. Slightly more subtle is the case of unions of an infinite number of infinite but countable sets, but these are also countable. (See problem sheets).

Theorem

The algebraic numbers are countable.

Proof

The algebraic numbers of order n are defined by

$$\mathcal{A}_n = \{x | x \in \mathbb{R}, p_n(x) = 0\}$$

where $p_n(x)$ denotes the polynomial

$$p_n(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots a_1 x + a_0$$

with $a_i \in \mathbb{Z}$. That is, $\mathcal{A}_n$ is the set of real numbers satisfying an order n polynomial equation with positive or negative integer coefficients. The set of algebraic numbers is then defined as

$$\mathcal{A} = \bigcup_{n=0}^{\infty} \mathcal{A}_n.$$

It follows from an earlier result on the infinite union of countable sets that $\mathcal{A}$ is countable if the $\mathcal{A}_n$ are countable.

Each point in $\mathcal{A}_n$ is specified by firstly, the set of coefficients a_i determing $p_n(x)$, and hence by elements of $\mathbb{Z}^n = \mathbb{Z} \times \mathbb{Z} \times \cdots \mathbb{Z}$; and secondly, by the particular solutionx_r to $p_n(x) =$, where $r \in \mathbb{N}$. Therefore $\mathcal{A}_n$ is subset of $\mathbb{Z}^n \times \mathbb{N}$, which is countable. Hence $\mathcal{A}$ is countable. QED.

Now the really interesting question is what about the real numbers. Are they countable? It was shown by the mathematician Georg Cantor that the real numbers are in fact not.

Theorem

The real numbers are uncountable.

Proof

The proof is remarkably simple. We suppose, for a contradiction, that the real numbers are countable. This means that they can be arranged as $\{r_1, r_2, r_3, \cdots\}$. Each number in the list may be written as a decimal,

$$\begin{aligned} r_1 &= m_1.a_{11}a_{12}a_{13}\cdots \\ r_2 &= m_2.a_{21}a_{22}a_{23}\cdots \\ &= \cdots \\ r_n &= m_n.a_{n1}a_{n2}a_{n3}\cdots \\ &= \cdots \end{aligned}$$

where m_n are positive or negative integers and the numbers a_{ij} are integers from 0 to 9. Now we use the diagonal elements of this array to construct the number

$$0.b_1b_2b_3\cdots$$

where each b_n is chosen to be either 1 or 2 in such a way that $b_n \neq a_{nn}$. But now we have constructed a real number that does not exist anywhere in the list $r_1, r_2, r_3, \cdots$, since it is different from every number in the list! So we have obtained a contradiction and the original supposition that the reals are countable must be false. QED.

This is Cantor's famous "diagonal argument" and has applications in many other areas of mathematics (and also computer science).

Another Proof

Another, more informal, proof is quite enlightening. This concerns the unit interval, the set of points $0 \leq x \leq 1$ (although note that the reals may be mapped onto this interval in a $1:1$ way, as is easy to show). We once again suppose, for a contradiction, that the set of real numbers in this interval may be written in a list $r_1, r_2, r_3, \cdots$. Then, we surround each point r_n with a region of size 10^{-n}. So r_1 is surrounded by a region of size $1/10$, r_2 by a region of size $1/100$, and so on. (The regions may overlap each other and also extend beyond the unit interval). The total size of the surrounding regions is

$$\frac{1}{10} + \frac{1}{100} + \frac{1}{1000} + \cdots = \frac{1}{10}\sum_{n=0}^{\infty} 10^{-n} = \frac{1}{9}$$

But this is a contradiction, since we have, by hypothesis, included every point in the unit interval and surrounded each point by a region of non-zero size. Hence the supposition that the points are countable is false. QED.

What about subsets of $\mathbb{R}$ such as the interval $[0,1]$? These are also uncountable. This is easily shown by by writing down a bijection which maps the real line $(-\infty, \infty)$ to $[0,1]$. For example the map $f(x) = (1 + \tanh x)/2$ does the job but there are many other examples.

The uncountability of $\mathbb{R}$ has a number of interesting consequences. One is that the irrationals must be uncountable. Recall that we have split the reals $\mathbb{R}$ in to rationals $\mathbb{Q}$, which are countable, and the irrationals, which may be written as $\mathbb{R}\backslash\mathbb{Q}$, i.e set of numbers in $\mathbb{R}$ that are not in $\mathbb{Q}$. Hence we may write,

$$\mathbb{R} = \mathbb{Q} \cup (\mathbb{R}\backslash\mathbb{Q})$$

Since the union of two countable sets must be countable, and $\mathbb{Q}$ is countable but $\mathbb{R}$ is not, we deduce that $\mathbb{R}\backslash\mathbb{Q}$ is uncountable.

A second consequence is that $\mathbb{R}\times\mathbb{R}$ (i.e. the set of points in a plane), is also uncountable, but no more so than $\mathbb{R}$. For simplicity we focus on the unit interval $[0,1]$ since this can be mapped onto $\mathbb{R}$. We consider a pair of points $(x, y) \in \mathbb{R}\times\mathbb{R}$, and use the decimal representiontation so $x = 0.a_1a_2a_3\cdots$ and $y = 0.b_1b_2b_3\cdots$. This pair of numbers can clearly be represented by a single number in $\mathbb{R}$, namely

$$z = 0.a_1b_1a_2b_2\cdots$$

so there is a bijection from $\mathbb{R}$ to $\mathbb{R}\times\mathbb{R}$.

Another uncountable set is the Cartesian product $\mathbb{N}^k = \mathbb{N} \times \mathbb{N} \times \cdots \mathbb{N}$ in the limit $k \to \infty$. (Prove this). Note that as discussed earlier $\mathbb{N}^k$, which is the set of finite length k-tuples $(n_1, n_2, \cdots n_k)$ for $n_i \in \mathbb{N}$, is countable.

2.7 The Real Numbers

We have established that the real numbers, regarded as all possible infinite decimals, are considerably more numerous than the rational or algebraic numbers. We can now be more precise about what we mean by the real numbers. There are numerous ways of doing this, but a very standard way, used in much of mathematics, is to proceed by introducing a set of definitions and axioms to define the reals. We will not go into this here, because they are pretty obvious, except to say that they are the axiomatization of the usual arithmetic properties, together with the familiar ordering properties. There is, however, one axiom that distinguishes the reals from the rationals. It is formulated in a not immediately obvious way, in terms of bounds on sets of numbers. To explain this, we need some definitions.

Examples: Consider the set $A = \{1, 2, 3 \cdots 9, 10\}$. It has largest element (maximum) of 10 smallest element (minimum) 1. Now consider the set of real numbers

$$[0, 1] = \{x \; |x \in \mathbb{R}, 0 \leq x \leq 1\}$$

i.e. the closed interval. It has max 1 and min 0. By contrast the open interval

$$(0, 1) = \{x \; |x \in \mathbb{R}, 0 < x < 1\}$$

has no max or min elements. However, it is **bounded** as we now discusss.

Definition

> Let A be a set of real numbers. If there is a real number b such that $a \leq b$ for all $a \in A$, then b is said to be an **upper bound** for the set A, and we say that A is bounded from above. Lower bound is similarly defined.

Most sets of numbers have many upper bounds. For example the set $(0, 1)$ has upper bounds 2 and 17.6. The upper bound therefore does not need to be in the set, or even close to it.

Although clearly in the case of the set $(0, 1)$ the numbers 0 and 1 are of special significance. This brings us to the following:

Definition

> Let A be a bounded set of real numbers. The **least upper bound** (l.u.b.) or **supremum** of A is an upper bound b such that $b \leq c$ for any upper bound c.

In a similar way we define the **infinum** or **greatest lower bound** (g.l.b.).

It may be shown that **the least upper bound is unique** (If L and L' are two least upper bounds, then $L \leq L'$ and $L' \leq L$ so $L = L'$).

Examples: The set $(0, 1)$ which has least upper bound of 1 (which lies outside the set). The set $[0, 1]$ has the same least upper bound (but in this case 1 does lie in the set).

A useful **equivalent definition** of least upper bound is the following:

> If b is the least upper bound of a set A, then there exists $a \in A$ such that $b - \epsilon < a \leq b$ for any $\epsilon > 0$.

In simple terms the existence of a least upper bound means that we can always "squeeze in" an element of A just beneath the l.u.b. This is equivalent to the earlier definition because, if false, then we must have that $a \leq b - \epsilon$ for all a, which would mean that the least upper bound is $b - \epsilon$, not b.

Example: Consider the following subset of the rationals:

$$A = \{x \ |x = \frac{n}{n+1}, n \in \mathbb{N}\}$$

Clearly all $a \in A$ satisfy $a < 1$. The set has minimum $x = 1/2$ but no maximum. It has least upper bound of 1, which lies outside the set. We can readily prove this using the above second definition of l.u.b, which means we need to show that there is an n such that

$$1 - \epsilon < \frac{n}{n+1} < 1.$$

Simple algebra readily shows that any $n > 1/\epsilon - 1$ does the job, hence 1 is the l.u.b.

Example: Another example involving a subset of the rationals is:

$$S = \{a_n \; |a_n^2 \leq 2, a_n \in \mathbb{Q} \text{ and } 10^n a_n \in \mathbb{N}\}$$

That is, a_n is the largest number less than $\sqrt{2}$ to n decimal places: $a_0 = 1$, $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$ etc. The set therefore clearly has an upper bound. It also has a least upper bound of $\sqrt{2}$ in $\mathbb{R}$ but the l.u.b. does not lie in S.

This last example brings us to the following important axiom for the real numbers.

Completeness Axiom

If $A \subset \mathbb{R}$ is bounded from above, then A has a least upper bound in $\mathbb{R}$.

It is this axiom that is not satisfied by the rationals and will turn out to be very useful in various proofs. For example, the set

$$S = \{x \mid x^2 < 2, \; x \in \mathbb{Q}\}$$

does not have a l.u.b. (Prove this briefly). But it does if $\mathbb{Q}$ is replaced by $\mathbb{R}$, namely $\sqrt{2}$. This simple but subtle axiom allows us to prove a number of things. In particular, we have the following:

Theorem

There exists $x \in \mathbb{R}$ such that $x^2 = 2$.

Proof

We consider the set,

$$S = \{x \mid x^2 < 2, \; x \in \mathbb{R}\}$$

and invoke the completeness axiom which states that S must have a l.u.b. $\ell \in \mathbb{R}$. We then prove that $\ell^2 < 2$ and $\ell^2 > 2$ are both impossible, which leaves $\ell^2 = 2$ as the only possibility.

First, suppose $\ell^2 < 2$. Then we find $\alpha > 0$ which is sufficiently small that $(\ell + \alpha)^2 < 2$. This is readily shown to be possible by simple algebra, if α is small enough. It implies that ℓ is not the *upper* bound.

Second, suppose $\ell^2 > 2$. It is also convenient to suppose that $\ell^2 < 4$ but this is not a significant restriction on the proof. Then we find a $\beta > 0$ so that $(\ell - \beta)^2 > 2$, which again is readily shown using simple algebra. Hence ℓ is not a *least* upper bound. QED.

Since the completeness axiom is the defining property of $\mathbb{R}$ it is of interest to relate this to our earlier definition of $\mathbb{R}$, namely as the set of all decimals. To proceed note that the decimal representation is a process of dividing up the real line into a sequence of progressively smaller "bins", each of which is contained by the previous bin. To be precise we define a **nested set of closed intervals** as intervals of the form

$$I_n = [a_n, b_n] = \{x \mid a_n \leq x \leq b_n,\ x \in \mathbb{R}, n \in \mathbb{N}\}$$

where the end-points are such that,

$$I_1 \supseteq I_2 \supseteq I_3 \cdots I_n \supseteq I_{n+1} \cdots .$$

Then we have the following result:

Theorem

(i) For any nested set of closed intervals, there exists a point $\xi \in \mathbb{R}$ such that $\xi \in I_n$ for all n.

(ii) If the intervals are such that $|a_n - b_n| \to 0$ as $n \to \infty$ then ξ is unique.

We will prove this result later on once we have developed some theory about sequences. Needless to say it involves the completeness axiom. In fact, it is possible to develop this subject using the above theorem as an *axiom* which *defines* the real numbers (and then the completeness axiom follows as a consequence, not the other way round).

The nested intervals property of $\mathbb{R}$ allows us to give **another proof that $\mathbb{R}$ is uncountable**. For simplicity we focus on the interval $[0, 1]$ and suppose for contradiciton that all points in the interval may be put in an ordered list $\{x_1, x_2, x_3 \cdots\}$. Now we choose nested set of intervals

$$[0, 1] \supseteq I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

where the intervals are chosen so that $x_1 \notin I_1$, $x_2 \notin I_2$ etc so that every point x_i has an interval I_i which does not contain it. But, by the nested intervals property there exists $\xi \in [0, 1]$ such that $\xi \in I_n$ for all n. I.e. there exists a number that sits in *every* interval, hence cannot belong in the original list since that consists of points which lie outside at least one interval. QED.

Another consequence of the completeness axiom is the so-called **Archimedean property** of the reals, which states that if a, b are any two positive real numbers, then there exists a positive integer n such at $na > b$. It is trivially proved for the rationals but involves a simple application of the completeness axiom to prove it for the reals. It shows that **the reals do not include "infinitesimally small" numbers** (despite what one is told in elementary calculus), since any number may always be scaled up to be arbitrarily large by multiplying by a sufficiently large integer. It is equivalent to the statement that for any $x \in \mathbb{R}$ one can always find $n \in \mathbb{N}$ such that $n > x$.

The proof, in brief, goes as follows. Suppose for contradiction that $n < x$ for some x and for all $n \in \mathbb{N}$, then the set of numbers

$$S = \{n \mid n \in \mathbb{N}\}$$

must have a l.u.b., ℓ, say. So $n \leq \ell$ for all n. But since for any $n \in \mathbb{N}$, $n + 1$ is also in $\mathbb{N}$, we must have $n + 1 \leq \ell$ for all n. This implies that $n \leq \ell - 1$ for all n, in contradiction with the statement that ℓ is the *least* upper bound. QED.

We can now prove a number of results about the relationships between the reals and the rationals.

Theorem

Between any two real numbers a and b there are both rational and irrational numbers.

Proof

Consider first the rational case. Suppose $b > a$. By the Archimedean property we can always find an integer n such that $n > 1/(b-a)$, which implies that

$$\frac{1}{n} < (b-a)$$

This means that if we step along the real axis in steps of size $1/n$, we will not be able to step over an interval of size $(b-a)$ with a single jump. Or in other words, there must exist a number m/n, for integer m, such that

$$a < \frac{m}{n} < b$$

To prove the irrational case, we use the fact that $\sqrt{2}$ is irrational, and note that, using the above argument, there exists a number n such that

$$\frac{1}{n\sqrt{2}} < \frac{1}{n} < (b-a)$$

and so there exists m such that

$$a < \frac{m}{n\sqrt{2}} < b$$

QED.

This theorem shows that the rationals and irrationals are thoroughly intermixed on the real line. There are no intervals that contain no rationals, or not irrationals.

2.8 The Cantor Set

We now briefly discuss a very challenging example of a subset of $\mathbb{R}$ which has two properties that seem almost contradictory: it is **uncountable and yet has zero size geometrically**. It is constructed by defining a sequence of nested subsets of the real line. We first define

$$\Delta_0 = [0, 1].$$

Then we remove the middle third of this interval giving the set,

$$\Delta_1 = [0, \tfrac{1}{3}] \cup [\tfrac{2}{3}, 1].$$

The middle thirds of these two intervals are then removed yielding,

$$\Delta_2 = [0, \tfrac{1}{9}] \cup [\tfrac{2}{9}, \tfrac{1}{3}] \cup [\tfrac{2}{3}, \tfrac{7}{9}] \cup [\tfrac{8}{9}, 1].$$

Continuing this process of removing middle thirds indefinitely we obtain a sequence of subsets,

$$\Delta_0 \supset \Delta_1 \supset \Delta_2 \supset \Delta_3 \cdots$$

The Cantor set is then defined to be

$$\Delta = \cap_{k=1}^{\infty} \Delta_k$$

that is the set of points $x \in \Delta_k$ for all k. Or in other words, the set of points that remain after the process of removing middle thirds has been repeated infinitely many times.

A natural question to ask is then whether there is anything left? The length of sections removed is easily seen to be:

$$\frac{1}{3} + \frac{2}{9} + \frac{4}{27} + \frac{8}{81} + \cdots = \frac{1}{3} \sum_{n=0}^{\infty} \left(\frac{2}{3} \right)^n = 1$$

The total length removed is 1, the size of the whole interval $[0, 1]$. It follows that the Cantor set has zero size.

It is then natural to ask if anything remains? Clearly the points that remain are the end-points of each interval Δ_k because the process of removing middle thirds leaves these intact. For example the points $0, 1, \frac{1}{3}, \frac{2}{3}, \frac{1}{9}, \frac{2}{9} \cdots$ are in the Cantor set.

It is not hard to see that this process of removing middle thirds is very readily handled using the ternary representation discussed earlier, in which points in $[0, 1]$ are represented in the form

$$x = \sum_{n=1}^{\infty} \frac{a_n}{3^n}$$

where $a_n = 0, 1, 2$. The point here is that this representation is a successive partitioning into a sequence of intervals each a third the size of the previous one. The values of $a_n = 0, 1, 2$ then determine whether the number lies in the first, middle, or third section of the interval. This means that removing the middle third corresponds to not allowing any $a_n = 1$ in the ternary representation. Therefore the Cantor set consists of all numbers whose ternary representation involves just 0 and 2.

Examples: $x = 0.02020202\cdots$ lies in the Cantor set and by summing the series may be seen to be equal to $1/4$. On the other hand 0.012, which is $5/27$, does not lie in the set.

One might wonder why numbers like $1/3$ lie in the Cantor set, since it is 0.1 in ternary. However, one has to remember that these representations are not unique and we have, for example,

$$0.1 = 0.02222222\cdots$$

so lies in the set.

Finally, we ask if the Cantor set is countable. Since it involves strings of just two numbers it is clearly equivalent to the binary representation, which we know is a representation of $\mathbb{R}$. Hence **the Cantor set is uncountable**.

2.9 Power Sets of Infinite Sets

As discussed earlier the power set $P(A)$ of a set A is the set of all subsets of A. It has cardinality $|P(A)| = 2^{|A|}$. Clearly $P(A) > |A|$ for a finite set A. However, it is also true in a specific sense for infinite sets. In particular a theorem due to Cantor shows that for an infinite set there cannot exist a bijection from A to $P(A)$. Hence if A is countable, $P(A)$ must be uncountable. This means for example that the power set of $\mathbb{N}$ is uncountable.

The proof of Cantor's theorem is a simple but subtle proof by contradiction. We will not give it here but instead give some a sense as to why the power set of a countable set is uncountable.

Consider first a finite set $A = \{a_1, a_2, \cdots a_n\}$. Its subsets are $\emptyset, \{a_1\}, \{a_2\}, \{a_1, a_2\} \cdots$. We can label the elements of $P(A)$ using binary strings involving yes (Y) and no (N) which characterize whether or not a given element of $P(A)$ (i.e. a given subset) contains the element $a_i \in A$. So for example the subset $\emptyset$ is denoted by the binary string $NN \cdots N$, the subset $\{a_1\}$ is denoted by the string $YN \cdots N$, the subset $\{a_1, a_2\}$ is denoted by the string $YYN \cdots N$ etc. (This is best illustrated by a simple table). In this way we see the elements of $P(A)$ correspond to the 2^n binary strings of length n consisting of Y or N.

Turning now to the case of infinite countable sets, it is readily seen that the same labelling procedure may still be used. Hence the elements of the power set $P(A)$ for an infinite countable A are labelled by the set of all infinite binary strings (i.e. there is a bijection between them). This establishes that the cardinality of $P(A)$ is the same as the cardinality of the binaries, which is the same as the cardinality of the reals, $|P(A)| = |\mathbb{R}|$, so $P(A)$ is uncountable.

What happens when we take the power set of $\mathbb{R}$? The answer, according to Cantor's theorem, is that it must lead to a set of cardinality greater than $\mathbb{R}$: $|P(\mathbb{R})| > |\mathbb{R}|$. This takes us into the world of progressively higher order infinities.

3. Sequences

The informal idea of a sequence is of a set of numbers, $a_1, a_2, \cdots$, collectively denoted $\{a_n\}$. For example, $1, 1/2, 1/3, 1/4 \cdots$ is a sequence, which we can also write as $a_n = 1/n$. However, a more formal definition is required.

3.1 Definitions, Examples and Properties

Definition of a Sequence

> A **sequence** $\{a_n\}$ is a map from the natural numbers $\mathbb{N}$ into another set of numbers (such as the reals or the rationals).

Sequences are useful in a number of contexts. **First** of all, they are an important prelude to studying infinite series, since an infinite series is the limit of a sequence

$$a_n = \sum_{k=1}^{n} b_k$$

Secondly, sequences naturally arise in the solutions to algebraic equations of the type

$$x = f(x)$$

This can be solved by guessing the solution x, then inserting into $f(x)$, and iterating. This defines the sequence x_n, by

$$x_{n+1} = f(x_n)$$

A study of sequences determines the conditions under which the sequence converges and whether there are solutions to the equation. **Third**, sequences are also useful mathematical devices for exploring topology – the study of sets of points. Sequences may be used to distinguish between, for example, the closed set $[0, 1]$ and the open set $(0, 1)$.

The most interesting sequences are infinite and it is then interesting to know what happens to them as $n \to \infty$. For example, $a_n = 1/n$ tends to zero as $n \to \infty$, and we say it is convergent, whereas $a_n = n$ blows up as $n \to \infty$, so we call this divergent. However, this is rather unrigorous and we need a more formal and precise way of expressing the idea that a_n tends to a fixed limit a, say, as $n \to \infty$. The key thing is that ∞ cannot be treated like a normal number, so we need to formulate a definition of the concept of a limit without using ∞.

Loosely, we can define $a_n \to a$ as $n \to \infty$ to mean that a_n can be made as close as a as we want to by taking n to be sufficiently large. More formally, we use the following more legalistic set of words.

Definition of a Convergent Sequence

> A sequence of numbers $\{a_n\}$ is **convergent** to the value a if for all $\epsilon > 0$, there exists N such that $|a_n - a| < \epsilon$ whenever $n > N$. We then write
>
> $$\lim_{n\to\infty} a_n = a$$

This type of definition is very important in rigorous mathematics an we will use similar definitions again. Note that it does not explicitly involve the idea of ∞. It may seem rather abstract and unnecessary at present but its strength is that it can be used in mathematical proofs.

A **divergent** sequence is then defined as one that is not convergent, as defined above. A sequence that grows without bound, such as $a_n = n$, is clearly divergent. However, the description divergent also includes sequences such as $a_n = (-1)^n$, which do not settle down to a fixed value, even though they don't blow up.

This definition of sequences also allows us to prove certain properties that are not obvious from naively inserting $n = \infty$ in a_n. For example, if $a_n > 0$, then it is easy to prove that the limit a cannot be negative (although $a = 0$ is possible even if the a_n are strictly positive for all n).

Example. This extremely important definition is readily illustrated with an example. Consider the sequence $a_n = e^{-n}$, which clearly converges to 0 as $n \to \infty$. We prove this rigorously. The definition requires us to find an N depending on ϵ such that $n > N$ implies that

$$e^{-n} < \epsilon.$$

The strategy in this (and all similar problems) is in effect to reorganize this inequality so that it is a lower bound on n. We readily see that the the inequality is equivalent to

$$n > \ln(1/\epsilon)$$

which means that we choose $N = \ln(1/\epsilon)$. QED.

One might wonder whether the process of taking $n \to \infty$ can give different answers. However, it is readily shown that **the limit of a sequence is unique**. We give a brief proof. Suppose for contradiction that $a_n \to a$ and $a_n \to b$ as $n \to \infty$. Then the triangle inequality gives us

$$|a - b| = |a - a_n - b + a_n| \leq |a - a_n| + |b - a_n|.$$

The two terms on the right may be made arbitrarily small which means that $a = b$.

A number of simple results about the **algebra of sequences** may be proved. Suppose that $a_n \to a$ and $b_n \to b$. The it can be shown that $a_n + b_n \to a + b$, $a_n b_n \to ab$, $a_b/b_n \to a/b$ and $ka_n \to ka$ for any real k. The proof of all of these follows reasonably directly (although not always briefly) from the definition of convergence.

Example. An example of the algebra of sequences is to show that $a_n \to a$ implies that $a_n^2 \to a^2$. We need to prove that

$$|a_n^2 - a^2| < \epsilon, \ \forall \ \epsilon > 0 \text{ if } n > N, \tag{1}$$

given that $a_n \to a$, i.e given that

$$|a_n - a| < \eta, \ \forall \ \eta > 0 \text{ if } n > N. \tag{2}$$

That is we need to show that η can be chosen in Eq.(2) so that Eq.(1) holds for any ϵ. We write $a_n = a + \bar{a}_n$ so Eq.(2) implies that $|\bar{a}_n| < \eta$ for $n > N$. We now have

$$|a_n^2 - a^2| = |\bar{a}_n^2 + 2a\bar{a}_n| \leq |\bar{a}_n|^2 + 2|a||\bar{a}_n| < \eta^2 + 2|a|\eta$$

We now need to show that we can choose η so that

$$\eta^2 + 2|a|\eta \ < \ \epsilon \tag{3}$$

There are a number of ways to do this but a simple way is to do it in two steps. If we first choose $\eta < |a|$, then $\eta^2 < |a|\eta$ and the inequality now reads

$$3|a|\eta \ < \ \epsilon$$

so we must also choose $\eta < \epsilon/(3|a|)$. These two upper bounds on η are concisely summarized

$$\eta < \min\left\{|a|, \frac{\epsilon}{3|a|}\right\}.$$

This proves the result. QED.

Note that a more systematic way of analyzing Eq.(3) would be to look at the roots of the corresponding quadratic equation which would determine *all* possible values of η, but the theorem only requires us to find *some* η which does the job and the two-step process is adequate and clearly simpler.

The formal definition of convergence is not in practice the most convenient way to establish convergence in many examples. It is therefore useful to develop a collection of simpler practical tests more readily applicable to examples of interest. We will do this in what follows.

A simple example is **the squeezing theorem**, which states that if we have three sequences a_n, b_n, c_n with

$$a_n \leq b_n \leq c_n$$

and both a_n and c_n converge to the same limit a, then b_n must converge to a also, i.e. it is "squeezed" to the value a for large n. This is again readily proved from the standard definition.

Example. A simple example is the sequence $a_n = x^n$, where $|x| < 1$. We show that $a_n \to 0$ using the squeezing theorem. We write $|x| = 1/(1+c)$ where $c > 0$ and we then have

$$0 \leq |x|^n = \frac{1}{(1+c)^n} \leq \frac{1}{(1+nc)} \to 0 \text{ as } n \to \infty$$

where we used the inequality $(1+c)^n \geq 1 + nc$.

The squeezing theorem can also be used to prove the following useful theorem:

Theorem

Let x_n be a sequence of positive numbers and let

$$L = \lim_{n\to\infty} \frac{x_{n+1}}{x_n}$$

If $L < 1$ then $x_n \to 0$. If $L > 1$ the sequence diverges. If $L = 1$ the test is indecisive.

Proof.

The definition of L means that for all $\epsilon > 0$ there exists N such that

$$\left|\frac{x_{n+1}}{x_n} - L\right| \ < \ \epsilon$$

which we may rewrite as

$$L - \epsilon \ < \ \frac{x_{n+1}}{x_n} \ < \ L + \epsilon$$

Consider first the case $L < 1$. We may clearly choose ϵ to be small enough that $R = L + \epsilon < 1$ and we then have

$$0 \ < \ \frac{x_{n+1}}{x_n} \ < \ R \ < \ 1$$

It follows that $x_{n+1} < Rx_n$ and, by iteration,

$$0 < x_{n+1} < Rx_n < R^2 x_{n-2} < \cdots < R^{n-1} x_1$$

Since $R^{n-1} \to 0$ as $n \to \infty$, it follows that $x_{n+1} \to 0$ by the squeezing theorem.

If on the other hand $L > 1$, we can always make ϵ small enough that $L - \epsilon > 1$ and we then have that $x_{n+1} > (L - \epsilon)x_n$, and so by a similar argument the sequence diverges.

To show that $L = 1$ is indecisive, note that $x_n = n$ and $x_n = 1/n$ both give $L = 1$ but the first is divergent and the second convergent.

Example. Consider the sequence $a_n = x^n n^p$ where $0 < x < 1$ and $p > 1$. We readily find

$$L = x\left(1 + \frac{1}{n}\right)^p \to x < 1$$

as $n \to \infty$. Hence $a_n \to 0$.

3.2 Monotone Sequences

Now some more theory building up to more practically useful theorems about convergent sequences.

Definition

> A sequence is called **monotonically increasing** if $a_{n+1} > a_n$, and **monotonically decreasing** if $a_{n+1} < a_n$. If it is one or the other it is simply called **monotone**.

The interesting sequences are those that are limited in some way.

Definition

> A sequence is called **bounded** if there is a number R such that $|a_n| < R$ for all n. It is **bounded above**, if $a_n < R$ for all n, and **bounded below**, if $a_n > R$ for all n.

Clearly, we have the following theorem:

Theorem

A convergent sequence is bounded

Proof

For a convergent sequence, for any $\epsilon > 0$, we may find an N such that for $n > N$

$$|a_n| = |(a_n - a) + a| \leq |a_n - a| + |a| < \epsilon + |a|$$

Now we simply choose ϵ to be some fixed number, such as $\epsilon = 1$, and hence the sequence is bounded for n larger than the corresponding N. For $n \leq N$, clearly we have

$$|a_n| \leq \max\{|a_1|, |a_2|, \cdots |a_N|\}$$

so $|a_n|$ is bounded for all n. QED.

However, the converse need not be true. The sequence $(-1)^n$ is clearly bounded, but does not converge, since it does not approach a limit point as $n \to \infty$. Can we do anything to a bounded sequence to make it converge?

There are two options here: one is to look at **sequences that are also monotone**; the other is to look at **subsequences**. We take each in turn.

Theorem (Bounded Monotone Sequences)

> If a sequence of real numbers a_n is monotonically increasing and bounded above, then it converges.

This result is almost obvious – a sequence that is increasing but not allowed to increase beyond a certain value must stop somewhere! But the interesting question is to spell this out using the rigorous definitions we have put in place.

Proof

> The key idea is the completeness axiom, which ensures that, since the sequence is bounded, the set of a_n possesses a *least upper bound*, which we denote a. We shall show that the sequence converges to a.
>
> Recall that the definition of least upper bound implies that for any $\epsilon > 0$, there exists an element a_N of the sequence for some $N \in \mathbb{N}$ such that
>
> $$a - \epsilon < a_N \leq a$$
>
> (because $a - \epsilon \geq a_N$ for all N would violate the statement that a is the least upper bound).
>
> Since the sequence is monotonically increasing, we have $a_N \leq a_n$ for $n > N$, which means that
>
> $$a - \epsilon < a_n$$
>
> for $n > N$. Rearranging, and noting that $a_n \leq a$, we see that there exists N for any $\epsilon > 0$ such that
>
> $$|a - a_n| < \epsilon$$
>
> for $n > N$. Or in other words, the sequence converges to a. QED.

Notice that the proof uses the completeness axiom so does not apply to the rationals $\mathbb{Q}$. Also note that there is an analogous result for monotonically decreasing sequences that are bounded from below. This is one of the most practically useful theorems for proving the convergence of sequences.

Example. Let a_n be $\sqrt{2}$ to n decimal places, so $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$ etc. Then clearly $a_n \leq a_{n+1}$ so is monotone increasing. The series is also bounded above since, by inspection, $a_n < 1.5$. Hence it converges.

Example. Consider the sequence defined as follows:

$$a_k = \max\{\sin(1), \sin(2), \cdots \sin(k)\}$$

Determine the first eight terms of the sequence (use a calculator). A simple plot may help. Determine its convergence properties.

Example. Consider the sequence $a_n = (1 + 1/n)^n$. We show it is monotonically increasing and bounded above, hence converges. Using a binomial expansion we find

$$\begin{aligned} a_n &= \sum_{k=0}^{n} \frac{1}{k!} \frac{n!}{(n-k)!n^k} = \sum_{k=0}^{n} \frac{1}{k!} \frac{n(n-1)(n-2)\cdots(n-k+1)}{n^k} \\ &\leq \sum_{k=0}^{n} \frac{1}{k!} = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots < 2 + \frac{1}{2} + \frac{1}{2^2} + \cdots = 3. \end{aligned}$$

This shows that the sequence is bounded above. To show that it is monotone increasing consider

$$\begin{aligned} \frac{a_n}{a_{n-1}} &= \left(\frac{n+1}{n}\right)^n \left(\frac{n-1}{n}\right)^{n-1} = \left(\frac{n^2-1}{n^2}\right)^n \left(\frac{n}{n-1}\right) = \left(1 - \frac{1}{n^2}\right)^n \left(1 - \frac{1}{n}\right)^{-1} \\ &\geq \left(1 - \frac{n}{n^2}\right) \left(1 - \frac{1}{n}\right)^{-1} = 1 \end{aligned}$$

where we have used the inequality $(1-x)^n \geq 1 - nx$ proved earlier. Hence the sequence is bounded and monotone so converges. As we know it converges to e but this is not shown here.

An important consequence of the above theorem is a proof of the nested intervals property of $\mathbb{R}$.

Theorem

Consider a set of intervals in $\mathbb{R}$ defined by $I_n = [a_n, b_n]$ which are nested, i.e.

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

Then there exists a point $\xi \in \mathbb{R}$ such that $\xi \in I_n$ for all n. Furthermore if $|a_n - b_n| \to 0$ as $n \to \infty$ then ξ is unique.

Proof

The fact that the intervals are nested implies that the lower end of each interval defines a monotonically increasing sequence, $a_n \leq a_{n+1}$ and the upper end b_n defines a monotonically decreasing sequence $b_{n+1} \leq b_n$.

Furthermore $a_n \leq b_n \leq b_1$, so the sequence a_n is bounded above. Hence it converges, $a_n \to a$, for some a. Similarly, $b_n \geq a_n \geq a_1$, so b_n is bounded below. So it also converges, $b_n \to b$, for some b.

We have $a \leq b$ so we can always find ξ such that $a \leq \xi \leq b$. Hence there exists $\xi \in I_n$ for all n.

To prove the uniqueness part we use $|a_n - b_n| \to 0$, together with the fact that $a_n \to a$ to show that $b_n \to a$. There exists some N such that $n > N$ implies

$$|b_n - a| = |b_n - a_n + a_n - a| \leq |b_n - a_n| + |a_n - a| < \epsilon_1 + \epsilon_2$$

for any non-negative ϵ_1, ϵ_2. This shows that $b_n \to a$. Since a_n and b_n both converge to a then we must have $\xi = a$ uniquely (because if $\xi > a$ of $\xi < a$ then $\xi > b_n$ or $\xi < a_n$ for sufficiently large n which is not possible). QED.

3.3 Subsequences and Cauchy Sequences

There is another way to make a bounded sequence converge. In the example $(-1)^n$ we could drop every other term and obtain a convergent sequence. This is an example of the general idea of defining a *subsequence* from a sequence. That is, a subsequence is a new sequence whose elements form a proper subset of the original sequence. More formally,

Definition

Let $\{\ a_n\}$ be a sequence and let

$$n_1 < n_2 < n_3 \cdots$$

be a strictly increasing sequence in $\mathbb{N}$. Then the sequence $\{b_n\}$ defined by $b_i = a_{n_i}$ is called a **subsequence** of $\{a_n\}$.

For example, $b_n = a_{2n} = \{a_2, a_4, a_6 \cdots\}$ is a subsequence of $\{a_n\}$. We now have the following theorem.

Theorem

Every sequence has a subsequence that is monotonically increasing or decreasing.

Proof

Again this result is almost obvious. We can think of the sequence as the discrete points on a curve in a plane. Graphically, it is then very easy to see how to select sections of the curve to produce a monotically increasing or decreasing function.

Consider a sequence $\{a_n\}$. We say that the term a_m is a *peak* of the sequence if $a_m \geq a_n$ for $n \geq m$. That is, the term a_m is never exceeded by any subsequent term in the sequence. Clearly in a decreasing sequence, every term is a peak, and in an increasing sequence, no term is. There are then clearly two cases: the sequences has either infinitely many peaks or finitely many (the latter including the case of zero peaks).

In the case of infinitely many peaks, we denote them $a_{m_1}, a_{m_2}, \cdots$, and since each term is a peak we have

$$a_{m_1} \geq a_{m_2} \geq a_{m_3} \cdots$$

We therefore obtain an infinite, monotically decreasing subsequence.

Now consider the second case of finitely many or zero peaks. Denote these by

$$a_{m_1}, a_{m_2}, \cdots a_{m_r}$$

So for $n > m_r$, there are no more peaks. Let $s_1 = m_r + 1$. Since a_{s_1} is not a peak, there must exist $s_2 > s_1$ such that $a_{s_1} < a_{s_2}$. Similarly, a_{s_2} is not a peak, which means there must exist $s_3 > s_2$ such that $a_{s_2} < a_{s_3}$. Continuing in this way, we obtain an increasing subsequence, a_{s_k}. QED.

The last two theorems lead to an important result.

Theorem (Bolzano-Weierstrass)

Every bounded sequence has a convergent subsequence in $\mathbb{R}$.

Proof

The result follows very simply from the last two theorems. First, we can always find a monotone subsequence. Second, if the sequence is bounded, then clearly any subsequence is bounded. Any monotone subsequence will also be bounded, so will converge. QED.

Example. Consider the sequence $b_k = \sin(k)$. Earlier we found that $\sin(1) = 0.84$ (to two decimal places), $\sin(2) = 0.91$, $\sin(3)$ to $\sin(7)$ are all smaller but $\sin(8) = 0.99$ etc. That is, the sequence b_k has a convergent subsequence, $\sin(1), \sin(2), \sin(8) \cdots$ of the general form

$a_k = \sin(n_k)$ where the sequence n_k is chosen so that $\sin(n_k) > \sin(n_{k-1})$. (Note this is slightly different to the sequence considered earlier).

The last result has an important consequence. We don't want to have to use the rather cumbersome definition of convergence given above every time we want to check for convergence. More seriously, the definition of convergence involves the limit explicitly, which we may not be able to find. So we need to evolve the concept a bit more and derive some more practically useful tests. In a convergent sequence, like $a_n = 1/n$, the terms get closer together as we go down the sequence. This leads to the following useful definition.

Definition

> A sequence $\{a_n\}$ is called a **Cauchy sequence** if for all $\epsilon > 0$, there exists N such that $|a_n - a_m| < \epsilon$ whenever $n, m > N$.

In loose terms, in a Cauchy sequence, the terms can be made arbitrarily close together by going sufficiently far down the sequence. This is clearly similar to the idea of convergence but it is important to see that it is not quite the same. First a simple theorem.

Example. Show that $a_n = 1/n$ is a Cauchy sequence.

Theorem

> Every Cauchy sequence is bounded.

Proof

> Setting $\epsilon = 1$, as we may, in the definition of Cauchy sequence, we see that the there exists an N such that
> $$|a_n - a_m| < 1$$
> for $n, m \geq N$ and we may set $m = N$, to obtain
> $$|a_n - a_N| < 1$$

This means that, by the triangle inequality,

$$|a_n| = |a_n - a_N + a_N| \leq 1 + |a_N|$$

for $n \geq N$. What about $n < N$? Well clearly in that case

$$|a_n| \leq \max\{a_1, a_2, \cdots a_{N-1}\}$$

So $|a_n|$ is bounded for all n. QED.

Now a very important result:

Theorem

A sequence of real numbers is convergent if and only if it is a Cauchy sequence.

Proof

1. We first supppose the sequence converges. We use our rigorous definition of convergence, which says that for any $\epsilon' > 0$, there is an N such that we have

$$|a_n - a| < \epsilon'$$

for all $n > N$. It follows that

$$\begin{aligned} |a_n - a_m| &= |a_n - a - (a_m - a)| \\ &\leq |a_n - a| + |a_m - a| \\ &\leq \epsilon' + \epsilon' \quad \text{for} \quad n, m > N \end{aligned}$$

(where the second line follows from the triangle inequality). We may now choose $2\epsilon' = \epsilon$, which proves that the sequence is Cauchy.

2. Now suppose the sequence is Cauchy. The key point here is to note that a Cauchy sequence is a bounded sequence, so we may appeal to the Bolzano-Weierstrass theorem, which states it must contain a convergent subsequence

$\{b_k\} = \{a_{n_k}\}$ say, for some set $\{n_1, n_2, \cdots\}$. We suppose the subsequence converges to some number a, which means that there is an N_1 such that

$$|a_{n_k} - a| < \epsilon/2$$

for all k such that $n_k > N_1$.

Using for a second time the fact that the sequence is a Cauchy sequence, we have that for any $\epsilon > 0$ there is an N_2 such that

$$|a_n - a_m| < \epsilon/2$$

for all $n, m > N_2$.

Now, using the triangle inequality, we have

$$\begin{aligned} |a_n - a| &= |(a_n - a_{n_k}) + (a_{n_k} - a)| \\ &\leq |a_n - a_{n_k}| + |a_{n_k} - a| \end{aligned}$$

The first term on the right-hand side is bounded from above by $\epsilon/2$ for $n, n_k > N_2$, since the sequence is Cauchy. The second term is bounded from above by $\epsilon/2$ for $n_k > N_1$, since the subsequence converges. Hence, if we choose $N = \max\{N_1, N_2\}$, we find that

$$|a_n - a| < \epsilon$$

for $n > N$ and the sequence is convergent. QED.

Example. We again use the example of the sequence a_n given by the decimal expansion of $\sqrt{2}$, $a_1 = 1.4$, $a_2 = 1.41$, $a_3 = 1.414$ etc. The general form for a_n and a_m with $m > n$ is

$$a_n = 1.c_1 c_2 c_3 \cdots c_n 000 \cdots$$

$$a_m = 1.c_1 c_2 c_3 \cdots c_n c_{n+1} \cdots c_m 000 \cdots$$

It follows that

$$|a_m - a_n| = 0.00 \cdots 0 c_{n+1} \cdots c_m 000 \cdots \; < \; \frac{1}{10^n}$$

This can clearly be made smaller than any $\epsilon > 0$ if $m > n > N$ for a suitable N. Hence the sequence is a Cauchy sequence so converges.

Example. Show that

$$a_n = \sum_{k=0}^{n} \frac{1}{k!}$$

is a Cauchy sequence. (Prove and use $2^{n-1} < n!$).

3.4 Contractive Sequences

Definition

A sequence x_n is called **contractive** if there exists $K \in (0,1)$ such that

$$|x_{n+1} - x_n| \leq K|x_n - x_{n-1}|$$

for all $n \in \mathbb{N}$.

Theorem

A contractive sequence is a Cauchy sequence (and so converges in $\mathbb{R}$).

Proof

By iterating the definition of contractive above we have

$$|x_{n+1} - x_n| \leq K|x_n - x_{n-1}| \leq K^2|x_{n-1} - x_{n-2}| \leq \cdots \leq K^{n-1}|x_2 - x_1|$$

Now use this to check if the sequence is Cauchy. We have for $m > n$,

$$\begin{aligned}
|x_m - x_n| &= |x_m - x_{m-1} + x_{m-1} \cdots + x_{n+1} - x_n| \\
&\leq |x_m - x_{m-1}| + |x_{m-1} - x_{m-2}| \cdots |x_{n+1} - x_n| \\
&= (K^{m-2} + K^{m-3} \cdots K^{n-1})|x_2 - x_1| \\
&= K^{n-1}\frac{(1 - K^{m-n})}{(1 - K)}\ |x_2 - x_1|
\end{aligned}$$

This clearly goes to zero for $m > n$ and $n \to \infty$ hence the sequence is Cauchy. QED.

Example. The Fibonacci sequence F_n is defined by $F_{n+2} = F_{n+1} + F_n$, where $F_1 = F_2 = 1$. The next few terms are $2, 3, 5, 8, 13, 21 \cdots$. The sequence diverges but we can instead consider the ratio of terms $x_n = F_{n+1}/F_n$ and we have $x_n > 1$ for $n \geq 2$. It satisfies

$$x_{n+1} = 1 + \frac{1}{x_n}$$

Show that it is contractive, and hence convergent, and find what limit it converges to.

3.5 Solving Equations with Iterative Sequences

Sequences crop up in the numerical solution to algebraic equations. For example, suppose we want to solve the equation

$$x = f(x)$$

for some function f. We might try to solve it by guessing the value of x and inserting it in $f(x)$. It probably won't give back exactly the same answer unless we were very lucky. But a reasonable strategy might be then to put back in the value of $f(x)$ we got out, and repeat.

More precisely, we define a sequence $\{x_n\}$ by

$$x_{n+1} = f(x_n)$$

There is some reasonable hope that, depending on how we choose the initial value, the sequence will converge to a value of x which satisfies the equation. However, this needs to be proved.

Let us concentrate on a simple example. Consider the sequence defined by

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right)$$

This sequence does in fact give successive approximations to $\sqrt{a}$. To see this, suppose $x_n \to x$ as $n \to \infty$. Then we solve

$$x = \frac{1}{2}\left(x + \frac{a}{x}\right)$$

which is also written as $x^2 = a$, hence has solutions $x = \pm\sqrt{a}$. We take $x > 0$ for simplicity. Now we can prove some things rigourously about this sequence.

Theorem

The sequence x_n converges to $\sqrt{a}$ as $n \to \infty$.

Proof

1. We take $x_0 > 0$. Clearly $x_{k+1} > 0$ if $x_k > 0$, so by induction, $x_n > 0$ for all n.
2. We have $x_k^2 \geq a$ for all $k \geq 1$ because

$$\begin{aligned} x_{k+1}^2 - a &= \frac{1}{4}\left(x_k + \frac{a}{x_k}\right)^2 - a \\ &= \frac{1}{4}\left(x_k - \frac{a}{x_k}\right)^2 \geq 0 \end{aligned}$$

So the sequence is bounded from below by $\sqrt{a}$.

3. The sequence is monotonically decreasing because

$$\begin{aligned} x_k - x_{k+1} &= x_k - \frac{1}{2}\left(x_k + \frac{a}{x_k}\right) \\ &= \frac{1}{2}\left(x_k - \frac{a}{x_k}\right) \\ &\geq 0 \end{aligned}$$

4. Since it is bounded from below and monotonically decreasing, the sequence converges.

Example. Set up an iterative contractive sequence of the form $x_{n+1} = f(x_n)$ where $0 < x_1 < 1$ that can solve $x^3 - 7x + 2 = 0$.

4. Series

One of the most important reasons for studying sequences is their relationship to series and this we now investigate. Consider for example, infinite sums such as

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots$$

The key thing is that the dots $\cdots$ doesn't really have any meaning so we have to tame the infinite sum by definitions.

4.1 Definitions

Given an infinite sum

$$s = \sum_{k=1}^{\infty} a_k$$

that we wish to study, we define the **partial sums**

$$s_n = \sum_{k=1}^{n} a_k$$

The partial sums define a sequence $\{s_n\}$ and we can use what we know about sequences to study the convergence of the infinite sum. In particular, we **define convergence of the infinite series** to be equivalent to convergence of the sequence $\{s_n\}$ as $n \to \infty$. That is

Definition

A series $\sum_{k=1}^{\infty} a_k$ is called **convergent** to the value s if for all $\epsilon > 0$, there exists N such that

$$\left| s - \sum_{k=1}^{n} a_k \right| < \epsilon$$

for all $n > N$.

For sequences, Cauchy sequences were particularly useful. Noting that

$$s_n - s_m = \sum_{k=n}^{m} a_k$$

we have

Definition

A series is a **Cauchy series** when for all $\epsilon > 0$, there exists N such that

$$\left| \sum_{k=n}^{m} a_k \right| < \epsilon$$

whenever $n, m > N$. As with sequences, a Cauchy series converges in the reals.

Definition

A series $\sum_{k=1}^{\infty} a_k$ converges **absolutely** if the series $\sum_{k=1}^{\infty} |a_k|$ converges. Otherwise the series is said to **conditionally**.

We will mainly concentrate on series with absolute convergence, such as series of positive terms. Conditionally convergent series have some interesting subtleties that we will address later.

4.2 Tests for Convergence

An important task is to use these abstract definitions of convergence to derive practically useful tests. Clearly a necessary, but not sufficient, condition is that the terms in the series decay to zero. We state this as a simple theorem:

Theorem

If the series $\sum_{k=1}^{\infty} a_k$ converges, then $a_k \to 0$ as $k \to \infty$.

Proof

The series is convergent so is a Cauchy series. If we set $m = n$ in the above definition of the Cauchy series, we find that for all $\epsilon > 0$, there exists N such that

$$|a_n| < \epsilon$$

whenever $n > N$. This is equivalent to the statement $a_k \to 0$ as $k \to \infty$. QED.

This is not however a sufficient condition. There can be series such that a_k goes to zero, but not fast enough to add up to a finite number.

Example A simple but important example is the series

$$\sum_{k=1}^{\infty} \frac{1}{k}$$

The terms decay to zero but the series does not in fact converge. To see that it diverges, we group the terms in the following way:

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots$$

Each term in each bracketed group is greater than the last term, so we have

$$\sum_{k=1}^{\infty} \frac{1}{k} \geq 1 + \frac{1}{2} + 2 \times \frac{1}{4} + 4 \times \frac{1}{8} + \cdots = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} \cdots$$

so the series clearly diverges.

Example Another very useful example is the series

$$\sum_{k=1}^{\infty} \frac{1}{k(k+1)}$$

It is easy to prove, by induction (exercise) that the partial sums are

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$$

Taking the limit $n \to \infty$ we get the simple result,

$$\sum_{k=1}^{\infty} \frac{1}{k(k+1)} = 1$$

This example may be used to prove convergence in other examples of interest. In particular, note that

$$\frac{1}{k(k+1)} > \frac{1}{(k+1)^2}$$

That is, every term in the series

$$\sum_{k=1}^{\infty} \frac{1}{(k+1)^2}$$

is bounded from above by the terms of a convergent series, so we anticipate that the series will converge. (This also means the series $\sum_{k=1}^{\infty} 1/k^2$ will converge since it differs by a finite constant). More precisely, we have a series of tests.

Theorem. (The Comparison Test)

> Let $\sum_{k=1}^{\infty} c_k$ be a convergent series of positive terms. Then any other series $\sum_{k=1}^{\infty} a_k$ converges absolutely if $|a_k| \leq c_k$.

Proof.

The series $\sum_{k=1}^{\infty} c_k$ converges so is a Cauchy series. This means that for all $\epsilon > 0$ there exists N such that for $n, m > N$ we have

$$\sum_{k=m}^{m} |a_k| \leq \sum_{k=m}^{m} c_k = \sum_{k=m}^{m} |c_k| < \epsilon$$

This means that $\sum_{k=1}^{\infty} |a_k|$ is a Cauchy series so converges. QED.

Theorem. (D'Alembert's Ratio Test).

Given a series $\sum_{k=1}^{\infty} a_k$, define

$$\rho = \lim_{n\to\infty} \left| \frac{a_{n+1}}{a_n} \right|$$

Then the series converges absolutely if $\rho < 1$ and properly diverges if $\rho > 1$. When $\rho = 1$ the test yields no definite conclusion.

Proof

1. Consider first the case $\rho < 1$. The existence of the limit means that, for sufficiently large n, the ratio $|a_{n+1}|/|a_n|$ can be made arbitrarily close to ρ, which is strictly less than 1. This means that there exists a positive number $\beta < 1$ such that

$$\left| \frac{a_{n+1}}{a_n} \right| < \beta$$

for n larger than some number $N = N(\beta)$. (This is essentially obvious but it can be proved in two lines using ϵ's etc – see the analogous theorem for sequences in Section 3). It follows that $|a_{n+1}| < \beta |a_n|$, and iterating, we find

$$\begin{aligned} |a_{N+m}| &< \beta |a_{N+m-1}| \\ &< \beta^2 |a_{N+m-2}| \\ &< \cdots \\ &< \beta^m |a_N| \end{aligned}$$

Since $\beta < 1$, the series

$$\sum_{m=1}^{\infty} \beta^m |a_N|$$

is convergent. By the comparison test, it therefore follows that the series

$$\sum_{m=1}^{\infty} a_{N+m}$$

is convergent, and hence the series $\sum_{m=1}^{\infty} a_m$ is convergent, because it differs only by a finite number of finite terms. This completes the case $\rho < 1$.

2. When $\rho > 1$, there exists a number $\beta > 1$ such that

$$\left|\frac{a_{n+1}}{a_n}\right| > \beta$$

for $n > N$. So we have

$$|a_{N+m}| > \beta^m |a_N|$$

The series

$$\sum_{m=1}^{\infty} \beta^m |a_N|$$

is properly divergent, and again by the comparison test we find that $\sum_{k=1}^{\infty} a_k$ is divergent.

3. To see that the case $\rho = 1$ is indecisive, note that both of the series

$$\sum_{n=1}^{\infty} \frac{1}{n}, \qquad \sum_{n=1}^{\infty} \frac{1}{n(n+1)}$$

have $\rho = 1$, but the first is divergent, whereas the second is convergent. QED.

Theorem. (Cauchy's Root Test).

Given a series $\sum_{k=1}^{\infty} a_k$, define

$$\rho = \lim_{n\to\infty} |a_n|^{1/n}$$

Then the series converges absolutely if $\rho < 1$ and properly diverges if $\rho > 1$. When $\rho = 1$ the test yields no definite conclusion.

Proof The proof is very similar to the ratio test. See PS6.

4.3 Conditionally Convergent Series

Some interesting subtleties arise with conditionally convergent series. These are series such that $\sum |a_n|$ diverges but $\sum a_n$ converges. An important example of a conditionally convergent series is

$$\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots$$

which converges to $\ln 2$. We derive some conditions ensuring convergence. Convergence is in fact easier to obtain for these series.

Theorem (Alternating Series Test).

> Let a_n be a monotonically decreasing sequence of positive numbers with $a_n \to 0$ as $n \to \infty$. Then the series $a_1 - a_2 + a_3 - a_4 \cdots$ converges.

Note that $\sum_n |a_n|$ need not converge.

Proof

We consider the sequence of particle sums

$$s_n = \sum_{k=1}^{n} (-1)^{k+1} a_k$$

and use our knowledge of sequences to show that this converges as $n \to \infty$. Consider the sequence consisting of an even number of terms. We have

$$\begin{aligned} s_{2n} &= (a_1 - a_2) + (a_3 - a_4) + \cdots + (a_{2n-1} - a_{2n}) \\ &= a_1 - (a_2 - a_3) - \cdots - (a_{2n-2} - a_{2n-1}) - a_{2n} \end{aligned}$$

Recalling that $a_n > a_{n+1}$, the first line shows that $\{s_{2n}\} = s_2, s_4, s_6 \cdots$ is a monotonically increasing sequence. The second line shows that it is bounded above, $s_{2n} \le a_1$. Together these two facts imply that the sequence s_{2n} converges as $n \to \infty$. Since $s_{2n+1} = s_{2n} + a_{2n+1}$ and $a_{2n+1} \to 0$ as $n \to \infty$, the sequence s_{2n+1} converges to the same limit. Hence the series converges. QED.

The alternating series test is a special case of a more general result, which applies to useful series such as

$$\sum_n a_n \sin(nx), \quad \sum_n a_n \cos(nx)$$

which arise in Fourier analysis. Clearly it is important to know the conditions under which these converge.

Theorem (Dirichlet's Test).

If the sequence $\{a_n\}$ is monotonically decreasing with $a_n \to 0$ as $n \to \infty$, and if the partial sums
$$t_n = \sum_{k=1}^{n} b_k$$
are bounded, $|t_n| \leq B$, for some B and for all n, then the series $\sum_n a_n b_n$ converges.

Proof (Non-examinable)

1. We will show that the series in question is a Cauchy series which involves finding an N such that for any $\epsilon > 0$,
$$\left| \sum_{k=n}^{m} a_k b_k \right| < \epsilon$$
for all $n, m > N$.

2. We first note that
$$b_k = t_k - t_{k-1}$$
(hence b_n is expressed in terms of its partial sums, about which we have information). It follows that
$$\sum_{k=n}^{m} a_k b_k = \sum_{k=n}^{m} a_k (t_k - t_{k-1})$$
We rearrange the right-hand side by the discrete equivalent of an integration by parts. We have
$$\sum_{k=n}^{m} a_k t_{k-1} = \sum_{k=n-1}^{m-1} a_{k+1} t_k = \sum_{k=n}^{m} a_{k+1} t_k - a_{m+1} t_m + a_n t_{n-1}$$
It follows that
$$\sum_{k=n}^{m} a_k b_k = \sum_{k=n}^{m} (a_k - a_{k+1}) t_k + a_{m+1} t_m - a_n t_{n-1}$$

3. We now have
$$\left| \sum_{k=n}^{m} a_k b_k \right| \leq \left| \sum_{k=n}^{m} (a_k - a_{k+1}) t_k \right| + |a_{m+1} t_m| + |a_n t_{n-1}|$$

Clearly the last two terms can be made arbitrarily small by taking n, m sufficiently large, since t_n is bounded and $a_n \to 0$ as $n \to \infty$. For the first term on the right, we have

$$\left| \sum_{k=n}^{m} (a_k - a_{k+1}) t_k \right| \leq \sum_{k=n}^{m} |a_k - a_{k+1}| \; B$$

But $a_k > a_{k+1}$ since the series is monotonically decreasing, so the modulus sign may be dropped and we have

$$\left| \sum_{k=n}^{m} (a_k - a_{k+1}) t_k \right| \leq \sum_{k=n}^{m} (a_k - a_{k+1}) \; B = (a_n - a_{m+1}) B$$

This term can also be made arbitrarily small by taking n, m sufficiently large, again using $a_n \to 0$. This establishes that the series is a Cauchy series, so it converges. QED.

Example. An application of the above theorem is the series $\sum_{k=1}^{\infty} a_k \cos(kx)$ mentioned above, where the a_k are monotonically decreasing. To establish convergence we need to show that the partial sums

$$t_n = \sum_{k=1}^{n} \cos(kx)$$

are bounded for all n. To show this either look up the formula for the sum or write the cosine in terms of e^{ikx}.

4.4 Riemann's Reordering Theorem

When we add a finite set of numbers, the sum is obviously independent of the order in which we add them. We might be inclined to think that this is also true for an infinite sum. For an absolutely convergent series, this is indeed true. But what is particularly interesting about a conditionally convergent series is that the sum **depends on the order of the terms**. In fact, a remarkable theorem due to Riemann tells us that a conditionally convergent series may be reordered in such a way that it converges to **any real number**.

These ideas are easily illustrate using the above example. The series

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots$$

in the order given is equal to $\ln 2$, as one can see from the expansion of $\ln(1+x)$ with $x = 1$. However, it is not too difficult to indicate how one can get other results.

We give an informal proof. First we note that the series is the difference between two different series. The first is

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{6} \cdots = \frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots\right)$$

so this series is divergent (as we have shown). The second series is

$$1 + \frac{1}{3} + \frac{1}{5} + \cdots > \frac{1}{2} + \frac{1}{4} + \frac{1}{6}$$

so this one is also divergent.

Now suppose that we want to add up the series in a suitable order to obtain the result c. Suppose for simplicity $c > 0$. First, we take the first few positive terms in the series $1 + 1/3 + 1/5 + \cdots$ and add them up until we overshoot c by no more than one term. We then get just over c, by an amount r_1, say. Clearly we can always do this since the series of positive terms is divergent, so a finite number of the terms can be added to make an arbitrarily large number. Then, we start adding the first few negative terms from the series $-1/2 - 1/4 - \cdots$ to $c + r_1$, until we get just less than c by a small amount r_2 say. So we get a number $c - r_2$. Now add more positive terms. These will be smaller than the first lot of positive terms so we will again overshoot c, but this time by an amount $r_3 < r_1$. And we may then add more negative terms thereby getting a number just less than c but now by a remainder $r_4 < r_2$. Proceeding in this way we define a sequence $c + r_k$ where the remainder terms r_k get progressively smaller, so the sequence tends to c in the infinite limit. Hence, we may add up the series in such a way as to obtain any real number.

4.5 Power Series

An important type of series is **power series**, i.e. one of the form

$$\sum_{n=0}^{\infty} a_n x^n$$

where $x \in \mathbb{R}$, whose convergence will depend in general on x. Such series arise in the Taylor expansion of familiar functions.

Example. Consider the series

$$\sum_n \frac{n^2 x^n}{2^n}$$

By the ratio test is can be seen that it converges if $|x| < 2$ and diverges if $|x| > 2$. When $x = \pm 2$, the series is $\sum_n (-1)^n n^2$ which diverges.

Theorem

> In determining the convergence or divergence of any power series $\sum_n a_n x^n$, there are only three possibilities:
>
> - Convergence for all x. An example is the series $\sum_n x^n/n!$
> - Divergence for all x. An example is the series $\sum n!\ x^n$
> - There exists a real number R, the **radius of convergence** such that $|x| < R$ implies absolute convergence and $|x| > R$ implies divergence. (There are no general results for the case $x = \pm R$ and these require special investigation).

The proof may be found in many textbooks and is not given here (and is NE).

Example. By the ratio test the series $\sum_n x^n/n^2$ coverges for $|x| < 1$ and diverges for $|x| > 1$ hence $R = 1$. At $x = \pm 1$ the series converges. Hence we have convergence for $|x| \leq 1$.

Example. The series $\sum_n n^2 x^n$ converges for $|x| < 1$, using the ratio test so $R = 1$. It diverges for $x = \pm 1$ and for $|x| > 1$.

Example. A slightly more subtle example is the series

$$\ln(1+x) = \sum_{n=1}^{\infty} (-1)^n \frac{x^n}{n}$$

We find $R = 1$ using the ratio test. At $x = +1$ the series is $\sum_n (-1)^n/n$ which we know converges conditionally. For $x = -1$ the series is $\sum_n 1/n$ which diverges. Hence we have convergence for $-1 < x \leq 1$.

4.6 Series and Integrals

Series are clearly related to integrals and indeed it is not hard to find simple examples in which the convergence or not of a series parallels the convergence or not of an integral. For example the series $\sum_n 1/n$ diverges, as does the integral $\int_1^\infty dx/x$. Similarly the series $\sum_n 1/n^2$ converges, as does the integral $\int_1^\infty dx/x^2$. These examples illustrate a very general relationship.

Theorem (Integral Comparison Test)

> Consider the integral $\int_1^\infty dx f(x)$ and the series $\sum_{n=1}^\infty f(n)$ where $f(x) \geq 0$ and decreases monotonically. Then the series converges if and only if the integral converges.

Proof

> (i) We first prove that if the integral converges then the series converges. Consider the sequence
>
> $$c_k = \sum_{n=2}^{k} f(n)$$
>
> (The lower limit of 2 is for convenience in what follows and clearly if c_k converges as $k \to \infty$ then the series with lower limit $n = 1$ also converges). Since the $f(n) \geq 0$, the series is clearly monotonically increasing $c_k \geq c_{k-1}$. Now we show it is bounded above.

By inspecting the rectangle beneath the curve $f(x)$ in the interval $[n-1, n]$ is readily seen that

$$f(n) \leq \int_{n-1}^{n} dx\ f(x)$$

(I.e. $\mathcal{A}_{DC} \leq \mathcal{A}_{AC}$ in the figure). We therefore have

$$c_k = \sum_{n=2}^{k} f(n) \ \leq \ \sum_{n=2}^{k} \int_{n-1}^{n} dx\ f(x) = \int_{1}^{k} dx\ f(x) \leq \int_{1}^{\infty} dx\ f(x)$$

where in the last step we used the fact that $f(x) \geq 0$. The final integral on the right-hand side is finite since the integral converges. This implies that c_k is bounded above. Since it is also monotonically increasing, it converges.

(ii) We now prove the reverse implication. Suppose that the series converges. By looking at the rectangles both below and above the curve $f(x)$ we have

$$f(n) \leq \int_{n-1}^{n} dx\ f(x) \leq f(n-1)$$

(I.e. $\mathcal{A}_{DC} \leq \mathcal{A}_{AC} \leq \mathcal{A}_{AB}$ in the figure). Summing over n from $n = 2$ to k we find

$$\sum_{n=2}^{k} f(n) \leq \int_{1}^{k} dx\ f(x) \leq \sum_{n=1}^{k-1} f(n)$$

Since the two series bounding the integral from above and below both converge as $k \to \infty$, the integral must also converge in that limit. QED.

Examples. The integral comparison test often works when other simple test like the ratio and root test fail. For example, consider the series $\sum_n 1/n^p$. We have

$$\int_{1}^{\infty} \frac{dx}{x^p} = \left[\frac{x^{-p+1}}{1-p}\right]_1^{\infty}$$

which diverges if $p \leq 1$ and converges if $p > 1$. Other important examples include the series $\sum 1/(n \ln n)$ and $\sum 1/(n(\ln n)^2)$. (See PS7).

There is also an interesting relationship between a series and the corresponding integral when both of them diverge – the difference between them is actually finite as we now show.

Theorem

The sequence

$$a_k = \sum_{n=1}^{k} f(n) - \int_1^k dx \ f(x)$$

is convergent as $k \to \infty$ even if the series and integral each diverge.

Proof

Using the inequality in part (ii) of the proof of the previous theorem ($\mathcal{A}_{AC} \leq \mathcal{A}_{AB}$), with n replaced by $n+1$, we have

$$f(n) \geq \int_n^{n+1} dx \ f(x)$$

from which it follows that,

$$a_k \geq \int_1^{k+1} dx \ f(x) - \int_1^k dx \ f(x) = \int_k^{k+1} dx \ f(x) \geq 0,$$

since $f(x) \geq 0$, hence the sequence is bounded from below. Similarly, using the inequality from part (i) of the previous proof ($\mathcal{A}_{DC} \leq \mathcal{A}_{AC}$) with $n = k+1$, we have

$$a_{k+1} - a_k = f(k+1) - \int_k^{k+1} dx \ f(x) \leq 0$$

hence the sequence is monotonically decreasing. It follows that a_k converges as $k \to 0$. QED.

Example. The sequence defined above can converge to any constant but one particular example in which the constant has been computed is the sequence

$$a_k = \sum_{n=1}^{k} \frac{1}{n} - \int_1^k \frac{dx}{x} = \sum_{n=1}^{k} \frac{1}{n} - \ln k$$

This converges to Euler's constant $\gamma = 0.5772\cdots$. (Not to be confused with Euler's *number* e).

4.7 Miscellaneous Results

Although establishing convergence of a series is a reasonably straightforwards and systematic matter using the tests described, actually summing a series explicitly is difficult if not impossible in general. However one interesting result in this area is the formula derived by Euler,

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

(Before Euler's solution this problem was known as the "Basel problem"). It can be obtained using the following imaginative argument. We consider the function f defined in terms of an infinite product

$$f(x) = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{(2\pi)^2}\right)\left(1 - \frac{x^2}{(3\pi)^2}\right)\cdots = \prod_{n=1}^{\infty}\left(1 - \frac{x^2}{n^2\pi^2}\right)$$

This product clearly needs some care in its definition but we proceed informally here. We note that $f(0) = 1$, and also that, assuming $f(x)$ can be expanded in a power series in x, the result has the form

$$f(x) = 1 + c_1 x^2 + c_2 x^4 + \cdots$$

where, crucially

$$c_1 = -\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}$$

precisely the quantity we are interested in. We therefore need to show by independent means that $c_1 = -1/6$.

The question is whether there is an alternative expression for $f(x)$. To this end note that the fundamental theorem of algebra states that any finite polynomial of order n of the form

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$$

may be equivalently written in factored form

$$p(x) = (x - r_1)(x - r_2)\cdots(x - r_n)$$

for a set of n roots r_i. It means that a function of polynomial form is completely determined by its roots (except perhaps to an overall factor).

Let us then assume that the same is true for infinite n. We note that $f(x)$ has zeros at the infinite set of points $x = n\pi$, where $n \in \mathbb{Z}$. Hence we need to think of another function, which can be expressed as in infinite power series in x, which also has these roots. It is not hard to guess that the function we are looking for is $\sin(x)/x$. We therefore assert that the infinite product $f(x)$ is also equal to

$$f(x) \equiv \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right) = \frac{\sin x}{x}$$

since both expressions for $f(x)$ have exactly the same roots and satisfy $f(0) = 1$ (which fixes any issues around the overall factor). Expanding for small x we have

$$f(x) = 1 - \frac{1}{6}x^2 + \frac{1}{120}x^4 + \cdots$$

This means that $c_1 = -1/6$ as desired and then the formula follows.

5. The Topology of the Reals

Having introduced the real numbers, we now concentrate on the nature of sets of real numbers. As promised in Section 3, we make use of sequences to explore the properties of different types of sets.

5.1 Open and Closed Intervals

Definition

An **open interval** (a, b) of the real line $\mathbb{R}$ is defined to be the set of points

$$(a, b) = \{x | x \in \mathbb{R}, a < x < b\}$$

In particular, the points a and b are not in the set. We sometimes write the entire real line $\mathbb{R}$ as $(-\infty, \infty)$, although note that ∞ is not really a number.

Definition

A **closed interval** $[a, b]$ of $\mathbb{R}$ is the set of points

$$[a, b] = \{x | x \in \mathbb{R}, a \leq x \leq b\}$$

so a closed interval includes the end-points a, b.

This is a provisional definition of open and closed, to fix ideas, and we will be more general shortly. The difference between open and closed intervals is quite important and subtle.

5.2 Closed Sets

A much more general definition of open and closed sets can be obtained by considering the behaviour of sequences.

Example. Consider the sequence $x_n = n/(n+1)$. We have $x_n \in (0,1)$, but $x_n \to 1 \notin (0,1)$. On the other hand both the sequence and its limit do live in $[0,1]$.

Definition

Consider a set $S \subset \mathbb{R}$. A point $\bar{x}$ is called a **limit point** of S if there exists a sequence $x_n \in S$ which converges to $\bar{x}$.

Definition

A set S is **closed** if it contains all its limit points.

Example. The closed interval

$$[0,1] = \{x | x \in \mathbb{R}, 0 \leq x \leq 1\}$$

and consider a sequence in $x_n \in [0,1]$ converging to $\bar{x}$. It is very easy to find sequences which converge to 0 or 1. Furthermore, any sequence in $[0,1]$ which converges cannot converge to a point outside the interval. For suppose that it did, that is, we have a sequence which converges to a point $1+\eta$, where $\eta > 0$. This means that we can make $|1+\eta - x_n| < \epsilon$, for any $\epsilon > 0$, by taking n sufficiently large. But this now means that by taking ϵ sufficiently small we can force $x_n > 1$, contrary to the statement that $x_n \in [0,1]$. Hence the set $[0,1]$ contains all its limit points so is closed.

For **finite sets of numbers every set is closed** – there is no sense in which the limit point of a sequence defined on a finite set can be outside the set.

5.3 Open Sets

Now we consider the more general definition of open sets.

Definition

A point $x \in \mathbb{R}$ is an **interior point** of a set $S \subset \mathbb{R}$ if there exists a **neighbourhood** of x in S. That is, if there exists $\epsilon > 0$ such that the interval

$$(x - \epsilon, x + \epsilon) \subset S$$

Definition

A set S is said to be **open** if all its points are interior points.

Example. The open interval

$$(0, 1) = \{x | x \in \mathbb{R}, 0 < x < 1\}$$

is open, since every point has a neighbourhood – for any point x, take ϵ to be smaller than both $x/2$ and $(1 - x)/2$, then clearly

$$(x - \epsilon, x + \epsilon) \subset (0, 1).$$

On the other hand, the closed interval $[0, 1]$ has many interior points, such as $x = 1/2$, but the points 0 and 1 are not interior points, since, for example, $(1 - \epsilon, 1 + \epsilon)$ is not a subset of $[0, 1]$. So clearly an open set cannot contain all of its limit points.

Open and closed are not exclusive alternatives. The sets

$$(0, 1] = \{x | x \in \mathbb{R}, 0 < x \leq 1\}$$

$$[0, 1) = \{x | x \in \mathbb{R}, 0 \leq x < 1\}$$

(in an obvious notation) are neither open nor closed. They are sometimes called half-open or half-closed. They contain some, but not all of their limit points, so are not closed.

Furthermore, for each of the two cases above, there is one point which is not an interior point, so the sets are not open either.

These definitions imply that intervals such as $(-\infty, 0)$ and $(0, \infty)$ are open, whereas $(-\infty, 0]$ and $[0, \infty)$ are in fact closed. This ensures that, for example, that the complement of the open set (a, b) is the closed set, $(-\infty, a] \cup [b, \infty)$.

This is an example of the general result: **The set A is open if its complement A' is closed** (and vice versa).

Examples. What can you say about $\mathbb{R}$ and $\mathbb{Q}$? Are they open, closed, both, or neither?

Definition

> The **closure** of a set $S \subset \mathbb{R}$ is defined to be the union of S together with its limits points, and is denoted $\bar{S}$. Clearly $\bar{S}$ is closed.

Examples. If $S = (0, 1)$, $\bar{S} = [0, 1]$. Another example, suppose we consider the set S defined by dividing the unit interval $[0, 1]$ into two equal parts but omitting the mid-point, so $S = [0, \frac{1}{2}) \cup (\frac{1}{2}, 1]$. Then $\bar{S} = [0, 1]$.

Definition

> If a set A is a subset of B, then we say that the set A is **dense** in B if we can always find a point in A which is arbitrarily close to any given point in B. More precisely, if for all points $x \in B$ we can always find a point $y \in A$ such that $|x - y| < \epsilon$ for any $\epsilon > 0$.

For example, the sets $(0, 1)$ and $S = [0, \frac{1}{2}) \cup (\frac{1}{2}, 1]$ are both dense in $[0, 1]$. Another example: the rationals $\mathbb{Q}$ are dense in the reals $\mathbb{R}$ since we can always find a rational number which is arbitrarily close to any real number.

This definition is equivalent to saying that A **is dense in** B **if** B **is the closure of** A**,** $\bar{A} = B$**.** This is because the definition implies that for every x in B we can always find a sequence y_n in A which converges to x, hence the union of A with all its limit points is B.

5.4 Unions and Intersections of Open and Closed Sets

Interesting possibilities arise when we take unions and intersections of finite and infinite numbers of sets. Given a finite number of sets $S_1, S_2 \cdots S_n$, we can define their union,

$$A = \bigcup_{k=1}^{n} S_k = S_1 \cup S_2 \cup \cdots \cup S_n$$

and intersection

$$B = \bigcap_{k=1}^{n} S_k = S_1 \cap S_2 \cap \cdots \cap S_n$$

It is not difficult to show that for unions and intersections of finite numbers of sets then A and B are, respectively, open or closed, if S_k are open or closed. (See PS7 for the open case). Note also that if we take the complement of A, we get

$$A' = \bigcap_{k=1}^{n} S'_k = S'_1 \cap S'_2 \cap \cdots \cap S'_n$$

Hence unions of say, closed sets, are simply related to intersections of open sets.

Things get more interesting for infinite unions and intersections and there are two interesting cases here. First, **the union of an infinite number of closed sets is not necessarily closed**.

Example. Let $I_n = [1/n, 1]$, which is clearly closed, and consider

$$S = \bigcup_{n=2}^{\infty} I_n = \ [1/2, 1] \ \cup \ [1/3, 1] \ \cup \ [1/4, 1] \cdots$$

This is the set

$$S = \left\{ x \;\middle|\; x \in \mathbb{R}, \ \frac{1}{n} \le x \le 1, \ \text{for some } n \in \mathbb{N} \right\}$$

Does this give $[0, 1]$ or $(0, 1]$? The key point is that $1/n > 0$ for all n, no matter how large n is, so the point 0 does not live in any of the sets I_n. So $S = (0, 1]$ which is not closed.

On the other hand, the intersection of an infinite number of closed sets is always closed (as illustrated for example, by the nested sub-intervals property of the reals).

The second thing we show is that **the intersection of an infinite number of open sets is not necessarily open**.

Example. Consider,

$$S = \bigcap_{n=1}^{\infty} \left(-\frac{1}{n},\ 1+\frac{1}{n}\right)$$

Is this equal to $(0,1)$ or $[0,1]$? S is the set

$$S = \left\{x \;\middle|\; x \in \mathbb{R},\ -\frac{1}{n} < x < 1+\frac{1}{n},\ \forall\, n \in \mathbb{N}\right\}$$

This clearly includes $x = 0$ and $x = 1$ but cannot include any points for which $x < 0$ or $x > 1$, since for sufficiently large n such points would lie outside $(-1/n, 1+1/n)$. This shows that this is in fact the closed set $[0,1]$.

Alternatively, the complement of S is the set of points such that, *for some* n, $x < -1/n$ and $x > 1 + 1/n$, which means that $x < 0$ and $x > 1$. This is an open set, so S is closed.

On the other hand, the union of an infinite number of open sets is open. (See PS7 in the infinite limit).

In summary:

(i) The union of an infinite number of open sets is open.

(ii) The intersection of an infinite number of closed sets is closed.

(iii) The intersection of an infinite number of open sets is not necessarily open.

(iv) The union of an infinite number of closed sets is not necessarily closed.

Note that statements (i) and (ii) are related by complementation and likewise (iii) and (iv).

Example. Is the Cantor set open or closed?

6. Continuous Functions of Real Variables

We now come to the general subject that is known as analysis, or mathematical analysis. Of course, the word analysis describes an activity one is frequently engaged in in mathematics, but analysis has come to refer to the branch of mathematics that gives calculus a solid and rigorous foundation.

Analysis is about the properties of functions. Recall that a function is a rule $f : A \to B$ which assigns a value in a set B to a number from a set A. We concentrate on the case $A \subseteq B = \mathbb{R}$. We are then interested in the various properties the function f may have.

6.1 Continuity

The most basic and important properties a function may have are continuity and differentiability. **Continuity** is the intuitive idea that a curve has no breaks in it – it may be drawn on a piece of paper without lifting the pen. **Differentiability** is the idea that the curve is in addition reasonably smooth – it doesn't have any kinks or sharp bends. We first concentrate on the idea of continuity we will return to differentiability later. Like many other ideas in mathematics, the proper expression of this intuitively simple idea is rather legalistic.

Definition

> A function $f(x)$ is **continuous** at the real number a if given any $\epsilon > 0$, there exists a $\delta > 0$ such that $|f(x) - f(a)| < \epsilon$ whenever $|x - a| < \delta$.

This is essentially the same as the idea of a limit: we could say that $f(x) \to f(a)$ as $x \to a$. Note that δ in general depends on ϵ. The idea is that we choose ϵ to be anything we like, and for a continuous function, the definition means that we can always find some number $\delta(\epsilon)$ for which the above condition holds. A number of simple examples confirm that this rather technical definition captures the intuitive idea of continuity.

Example. The function $f(x) = kx$ is continuous, for some real k at any point $x = a$. To prove this, we need to show that for any $\epsilon > 0$, we can find $\delta(\epsilon)$ such that

$$|x - a| < \delta \implies |kx - ka| < \epsilon$$

By inspection, the choice $\delta = \epsilon/|k|$ clearly does the job.

Example. Another important example is the step function $\theta(x) = 1$ for $x > 0$ and $\theta(x) = 0$ for $x < 0$. We define $\theta(0) = 1$. (Other choices are possible but don't in fact make any difference). To be continuous at $x = 0$, it must be possible to find δ such that,

$$|x| < \delta \implies |\theta(x) - \theta(0)| < \epsilon.$$

This is trivially true for $x \geq 0$. But for $x < 0$, $|\theta(x) - \theta(0)| = 1$ which cannot be made smaller than any $\epsilon < 1$ for any choice of δ. The function is not continuous at $x = 0$.

Example. A more challenging example is $f(x) = x^2$. (This case has similarities with the proof in Section 3 that the sequence a_n^2 converges to a^2, given that a_n converges to a.) We need to find $\delta(\epsilon)$ such that

$$|x - a| < \delta \implies |x^2 - a^2| < \epsilon$$

We note that

$$|x^2 - a^2| = |x - a|.|x + a| = |x - a|.|(x - a) + 2a| \leq |x - a| \left(|x - a| + 2|a|\right)$$

We determine a suitable δ in a two-step process.

First, we choose $\delta \leq |a|$. The requirement $|x - a| < \delta$ then implies that the term in brackets on the right is bounded by $3|a|$, and then

$$|x^2 - a^2| < 3|a|.|x - a|.$$

The second step is to choose $\delta \leq \epsilon/(3|a|)$, which implies that $|x^2 - a^2| < \epsilon$ when $|x - a| < \delta$.

Combining these two choices for δ, we see continuity is proved if we choose

$$\delta(\epsilon) = \min\{|a|, \frac{\epsilon}{3|a|}\}.$$

Example. Another similar example is the function $f(x) = 1/x$, for $x > 0$. Show that it is continuous at any point $a > 0$. Similar to the last example, it is necessary to choose δ twice, the first choice to control behaviour at $x = 0$.

Using similar methods to the above examples, it is possible to prove a number of simply and reasonably obvious results about the **alegbra of continuous functions**, e.g., if f and g are continuous functions, then so is $f + g$, fg, $f \circ g$, etc. (See PS8).

Continuity as defined above refers to continuity of the function at a single point. A natural extension of this idea is the idea of continuity on an interval: A function f is is said to be **continuous on the interval** I if it is continuous at every point $x \in I$.

Another intuitive property of a continuous function is that **its features don't vary too much from point to point**. This is illustrated by the following theorem.

Theorem

Suppose the function $f : \mathbb{R} \to \mathbb{R}$ is is continuous at some point a. Then:

(i) There exists an $\eta > 0$ such that f is bounded in the interval $(a - \eta, a + \eta)$.

(ii) If $f(a) > 0$, then $f(x) > 0$ in a neighbourhood of a.

Proof

Written out more explicitly, the definition of continuity $|x - a| < \delta$ implies $|f(x) - f(a)| < \epsilon$ reads,

$$a - \delta < x < a + \delta \implies f(a) - \epsilon < f(x) < f(a) + \epsilon$$

To prove part (i), we fix ϵ to some value e.g. $\epsilon = 1$. This then clearly shows that $f(x)$ has both a lower and upper bound in the open interval $(a - \delta, a + \delta)$.

To prove part (ii), we choose ϵ to keep $f(x)$ sufficiently close to $f(a)$ that it is positive. E.g. $\epsilon = f(a)/2$ does the job. This then shows that $f(x) > f(a)/2 > 0$ in the interval $(a - \delta, a + \delta)$.

6.2 Continuity and Sequences

Now a very useful result which makes contact with what we have studied on sequences. This provides an alternative definition of continuity that may be more intuitively appealing.

Theorem

Consider a function $f : I \to \mathbb{R}$. Then the following two statements are equivalent:

(A) f is continuous at the point $a \in I$.

(B) For every sequence a_n in I converging to a, the sequence $f(a_n)$ converges to $f(a)$.

Proof

We will prove the theorem by showing that if A is true, then B is true, and if A is false, then B is false. This establishes the equivalence of the two statements.

First, we assume that A is true so we assume continuity of $f(x)$. This means for all $\epsilon > 0$ we can find $\delta(\epsilon)$ such that $|x - a| < \delta$ implies

$$|f(x) - f(a)| < \epsilon.$$

Now we set $x = a_n$, a sequence which converges to a, which means for any δ there exists $N(\delta)$ such that $n > N$ implies $|a_n - a| < \delta$. Combining these two statements we have that $n > N$ implies

$$|f(a_n) - f(a)| < \epsilon$$

which is precisely the statement that $f(a_n)$ converges to $f(a)$. This proves that A implies B.

Second, we suppose that A is false. Falseness of B, which we seek to prove, would mean that there is *some* sequence a_n converging to a such that $f(a_n)$ does *not* converge to $f(a)$. So we suppose that the function is not continuous at a. This means that there is *some* $\epsilon > 0$ such that we can make

$$|f(x) - f(a)| \geq \epsilon$$

by taking x sufficiently close to a. Since a_n is a convergent sequence, converging to a, if we take $x = a_n$, we have that a_n may be arbitrarily close to a yet

$$|f(a_n) - f(a)| \geq \epsilon$$

which means that the sequence $f(a_n)$ does *not* converge to $f(a)$ even though a_n converges to a. So A false implies that B is false. Q.E.D.

This theorem is very useful for proving the absence of continuity in certain examples as we now see.

Example. The step function $\theta(x)$ considered already. We consider a sequence $a_n < 0$ which converges to 0. The sequence $\theta(a_n) = 0$ for all n so converges to zero, but $\theta(0) = 1$. So the function is not continuous at $x = 0$.

Example. The Dirichlet function is defined by

$$f(x) = \begin{cases} 0, & \text{for } x \text{ irrational} \\ 1, & \text{for } x \text{ rational} \end{cases}$$

We show that $f(x)$ is discontinuous for all x.

• If x is irrational, we consider a rational sequence $a_n \to x$. Then $f(a_n) = 1$ for all n which converges to 1, but $f(x) = 0$.

• Similarly if x is rational, we consider an irrational sequence $a_n \to x$. Then $f(a_n) = 0$ which converges to 0 but $f(x) = 1$. Hence the function is discontinuous for all x.

Example. Show that this unusual function arises from the function $f_{nm}(x) = \cos^{2n}(m!\pi x)$ in the limit that m and n go to infinity. (Consider what happens to the argument of the cosine in the rational and irrational cases as m becomes large).

Example. An intriguing modification of the Dirichlet function (sometimes also called the Thomae function) is

$$f(x) = \begin{cases} 0, & \text{for } x \text{ irrational} \\ \frac{1}{q}, & \text{for } x \text{ rational of the form } \frac{p}{q} \text{ (in lowest terms)} \end{cases}$$

This function is discontinuous on the rationals but, surprisingly, continuous on the irrationals.

• For rational x and an irrational sequence $a_n \to x$. Then as in the previous example $f(a_n) = 0$ for all n so $f(a_n) \to 0$. But $f(x) \neq 0$ so the function is discontinuous at rational x.

• For irrational x, $f(x) = 0$. If $a_n \to x$ along an irrational sequence a_n, then $f(a_n) = 0$ which converges to 0, i.e. $f(a_n)$ goes to $f(x)$ as required.

• The crucial case is that in which we approach irrational x along a rational sequence. Suppose we write the rational sequence as $a_n = p_n/q_n$, for integers p_n, q_n. We have $f(a_n) = 1/q_n$.

• Now the key point here is that, although $f(a_n)$ is non-zero, it becomes arbitrairly small as the rational sequence a_n approaches irrational x – this is because successive rational approximations to an irrational number involve progressively larger values of the denominator q_n, so if $a_n \to x$, then $f(a_n) \to 0$.

The last statement is intuitively obvious but find a simple way to make it more precise using the decimal representation, which indicates that any rational sequence tending to a real number can be written as a rational with denominator behaving like 10^n for large n.

Suppose we are given a function $f(x)$ which is defined only on the rationals. Can we extend it to the reals uniquely?

Without any further information this cannot be done uniquely since we can choose $f(x)$ on the irrationals as we please. However, if we are given that f is *continuous* (on both rationals and irrationals) then there is a unique extension to the reals.

Example. Suppose $f(x) = 0$ for all rational x. If we assume f is continuous what form must it take on the irrationals?

6.3 Fixed Point Theorems

Now a very important result that goes by the name of the intermediate value theorem (IVT), or Bolzano's theorem. First the intuitive idea: Suppose that, on a winter's day, we note that the temperature at noon, as measured on a thermometer, is 5 degrees centigrade. Then at midnight, we look at the thermometer again and note that the temperature is -2 degrees centigrade. Then, assuming (in a non-technical sense) the thermometer changes in a continuous way, we may deduce that the temperature *must* have been 0 degrees at some time in between.

This is of course obvious, but now we are given a mathematical definition of continuity, it is an interesting challenge to prove it, using the technical definition. This obvious result also turns out to have some useful (and less obvious) consequences.

Theorem (Bolzano)

Let $f : [a, b] \to \mathbb{R}$ be a continuous function, such that $f(a) < 0$ and $f(b) > 0$. Then there exists a point $c \in [a, b]$ such that $f(c) = 0$.

Proof

We first produce a sequence of nested subintervals, $I_1, I_2 \cdots$ defined as follows. Take the interval I and divide it in equal halves, and define I_1 to be the half in which $f(x)$ has opposite signs at its end-points. (Of course, $f(x)$ maybe zero at an end-point, in which case we are done). Then divide I_1 into equal halves, and define I_2 in a similar way. In this way, we obtain an infinite sequence of nested subintervals

$$I \supset I_1 \supset I_2 \supset I_3 \cdots$$

where each interval has the property that $f(x)$ has opposite signs at its extremes.

As we have shown, such a sequence of intervals has the property that it contains a point c common to all the intervals. That is, $c \in I_n$ for all n. We conjecture that in fact $f(c) = 0$, which seems reasonable since the intervals get smaller by a factor of 2 at each step, "squeezing" the possible zero of $f(x)$ into a smaller and smaller region.

To prove this precisely, we suppose, for a contradiction, that the point $c \in I_n$ satisfies $f(c) > 0$. Now we use the property of continuity (so far unused). As we proved earlier, $f(c) > 0$ together with continuity at c imply that there exists an interval $(c-\eta, c+\eta)$ on which $f(x) > 0$ for all $x \in (c-\eta, c+\eta)$, for some sufficiently small $\eta > 0$. But this is now a contradiction, since $f(x)$ must take both positive and negative values in all the intervals I_n, and for sufficiently large n the interval I_n will be smaller than the interval $(c-\eta, c+\eta)$. A similar argument rules out the case $f(c) < 0$, leaving $f(c) = 0$ as the only option. QED.

Note that the theorem would not in fact be true on the rationals. For consider the function $f(x) = x^2 - 2$. It is positive for $x = 2$ and negative for $x = 0$. Its zeros lie at $x = \pm\sqrt{2}$ and there are no rational points for which the function vanishes. This means that the proof must involve the completeness property (the defining property of the reals), and indeed it does, since the result on nested subintervals requires the completeness property.

Example An interesting geometric example concerns the problem of finding a line which bisects two areas. (See slide).

An important corollary of the intermediate value theorem is the following "fixed point" theorem, which indicates the conditions under which certain types of equations have a solution. This is a special example of a more general result called Brouwer's fixed point theorem.

Theorem

Suppose f is a continuous function mapping the interval $[a, b]$ into itself, $f : [a, b] \to [a, b]$. Then there exists a point $\xi \in [a, b]$ such that

$$f(\xi) = \xi$$

The theorem is reasonably easy to understand from a simple figure by drawing arrows between two copies of the interval $[a, b]$ – one can try to map every point to a different point but if the map varies in a continuous way from point to point it is impossible to avoid mapping at least one point to itself.

Proof

The proof follows quite easily from the intermediate value theorem. Since f maps $[a, b]$ into itself, the point we must have that $f(a) \geq a$. Similarly, $f(b) \leq b$. This means that the function

$$g(x) = f(x) - x$$

is a continuous function satisfying $g(a) \geq 0$ and $g(b) \leq 0$. By the intermediate value theorem, there therefore exists a point $\xi \in [a, b]$ such that $g(\xi) = 0$, or in other words, such that $f(\xi) = \xi$. QED.

Examples. We discuss now in an informal way some aspects of Brouwer's fixed point theorem, most of which are best understood using simple pictures. (See slides and also the Wikipedia page on this topic). It involves continous maps between different types of spaces, which can be in many dimensions but must include their boundary points (i.e. are closed) and cannot have any holes in them (i.e. must be simply connected).

The simplest example in the plane is the closed disk D,

$$D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$$

The map in this case can be visualized by noting that it defines a two-dimensional vector field indicating where each point goes. It is then not hard to see that such a vector field must have a source or sink somewhere representing the fixed point. However, if the region has a hole in the middle, the field can simply circulate around the hole without having a fixed point.

6.4 Differentiability

We now come to a discussion of the differentiability of functions on the reals, the question of how smooth the graph of a function is. This is not a systematic discussion of basic calculus, which has been covered anyway in earlier course, but will be a discussion of some of the deeper aspects of calculus and some of the more extreme examples of unusual functions.

Recall first the definition of a limit. We say $\lim_{x\to a} f(x) = f(a)$ if for all $\epsilon > 0$, there exists δ such that

$$|x-a| < \delta \implies |f(x) - f(a)| < \epsilon.$$

A function is therefore continuous at a is $f(x) \to f(a)$ in the limit $x \to a$. In this section we will work with this slightly more informal notion of limit, rather than the formal $\epsilon - \delta$ definition used previously.

Definition

Let $A \subseteq \mathbb{R}$ and $f : A \to \mathbb{R}$. Then the **derivative** of f at the point $a \in A$ is defined by

$$f'(a) = \lim_{x\to a} \frac{(f(x) - f(a))}{(x-a)}.$$

The function f is said to be **differentiable** if this limit exists.

Example: The function,

$$f(x) = \begin{cases} 0 & x \leq 0 \\ x & x > 0 \end{cases}$$

is continuous not differentiable at $x = 0$.

Example: The function,

$$f(x) = \begin{cases} 0 & x \leq 0 \\ x^2 & x > 0 \end{cases}$$

is differentiable at $x = 0$ (with $f'(0) = 0$).

Example. Let f be defined for all real x and suppose that

$$|f(x) - f(y)| \leq (x - y)^2$$

for all real x, y. What is the most general possible form for f?

Although continuity does not imply differentiability, the converse is true.

Theorem

Let $A \subseteq \mathbb{R}$ and let $f : A \to \mathbb{R}$ be differentiable at the point $a \in A$. Then f is continuous at a.

Proof

We may write

$$f(x) - f(a) = \frac{(f(x) - f(a))}{(x - a)}.(x - a)$$

Since f is differentiable at a we may take the limit $x \to a$ throughout. The right-hand side tends to $f'(a)$ multiplied by zero, hence

$$\lim_{x \to a}(f(x) - f(a)) = 0$$

which shows that f is continuous at a. QED.

Definitions

The **second derivative** of a differentiable function at a point a (if it exists) is defined in the obvious way;

$$f''(y) = f^{(2)}(a) = \lim_{x \to a}\left(\frac{f'(x) - f'(a)}{x - a}\right)$$

If we may define $f^{(2)}(a)$ for all $a \in A$ we say that f is twice differentiable.

We may continue to define **higher derivatives** (if they exist) and the associated functions $f^{(n)}(x)$ on A. The n-th derivative is defined recursively in terms of the $(n-1)$-th derivative as:

$$\begin{aligned} f^{(m)}(a) &= \lim_{x \to a} \frac{f^{(m-1)}(x) - f^{(m-1)}(a)}{x-a} \qquad m \geq 1 \\ f^{(0)}(a) &= f(a) \end{aligned}$$

The following definitions are also useful:

Definitions

Let $A \subseteq \mathbb{R}$ and $f : A \to \mathbb{R}$. We say f is C^0 if it is continuous on A.

Let $n \in \mathbb{N}$. We say f is C^n **differentiable** if all its $f^{(k)}(x)$ derivatives are **continuous** functions on A for all integers $0 < k \leq n$.

We say f is C^∞ or **smooth** if all its $f^{(n)}(x)$ derivatives are **continuous** functions on A for all $n \in \mathbb{N}$.

Examples:

- Any polynomial is C^∞ on $\mathbb{R}$.
- e^x is C^∞ on $\mathbb{R}$.
- $|x|$ is C^0 on $\mathbb{R}$.
- The following is C^k;

$$f(x) = \begin{cases} 0 & x \leq 0 \\ x^{k+1} & x > 0\ , \quad k \in \mathbb{N} \end{cases}$$

- The following is C^∞ (smooth);

$$f(x) = \begin{cases} 0 & x \leq 0 \\ e^{-\frac{1}{x}} & x > 0 \end{cases}$$

Example. The "sawtooth function" can be used to construct an example of a function that is **continuous everywhere but differentiable nowhere**. We give here an informal understand of its properties. We construct a sequence of functions $f_n(x)$ defined on $[0, 1]$, where

$$f_1(x) = \begin{cases} x, \text{ if } 0 \le x \le 1/2, \\ 1 - x, \text{ if } 1/2 \le x \le 1 \end{cases}$$

Then $f_2(x)$ is defined by scaling down by a factor of $1/2$ (in both directions) and having two copies, one in $[0, 1/2]$ the other in $[1/2, 1]$. This process is repeated to generate all the $f_n(x)$. We are interested in the function

$$f(x) = \lim_{n\to\infty} f_n(x)$$

For large n, $f_n(x)$ is a very wiggly line of height 2^{-n}. It is clearly continuous for finite n, and since $f_n(x) \to 0$ for all x, it's limit $f(x)$ is also continuous. We argue that its derivative is defined nowhere in the same limit.

The derivative of $f_1(x)$ is ill-defined at $x = \frac{1}{2}$.

$f_2'(x)$ is ill-defined at $x = \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$.

$f_3'(x)$ is ill-defined at $x = \frac{1}{8}, \frac{1}{4}, \frac{3}{8}, \frac{1}{2}, \frac{5}{8}, \frac{3}{4}, \frac{7}{8}$.

$f_n'(x)$ is ill-defined at the points $x = \frac{m}{2^n}, \quad m = 1, 2 \cdots (2^n - 1)$.

These points are very conveniently characterized using the binary representation – they are points with a finite representation,

$$x = 0.a_1 a_2, a_3 \cdots a_n 0000 \cdots$$

where $a_i = 0, 1$ (excluding the end-points of the interval). Now as we consider the limit $n \to \infty$, we see that the points at which the derivative is ill-defined consist of all points with *infinite* binary representation, i.e. all points on the real line. Hence the derivative of the limit $f(x)$ is ill-defined everywhere.

6.5 Some Useful Theorems

We normally associate the maxima and minima of a function with the points at which the derivative vanishes. However, there is a deeper result about maxima and minima which does not assume differentiability.

Extreme Value Theorem

> If f is continuous on the interval $[a, b]$ then there exist points $x_1, x_2 \in [a, b]$ such that f achieves its maximum at x_1 and achieves its minimum at x_2.

A proof of this result is given in the Appendix at the end of this section.

Comments

- The function f does not have to be differentiable.
- The result is not true if the interval is not closed. For example, $1/x$ is unbounded on the interval $(0, 1]$.
- The result is not necessarily true if f is discontinuous. Consider for example the function

$$f(x) = \begin{cases} \frac{1}{2}, & \text{for } x \text{ rational} \\ x, & \text{for } x \text{ irrational} \end{cases}$$

defined on the interval $[0, 1]$. It is not hard to see that $f : [0, 1] \to (0, 1)$. This is because $f(x)$ can become arbitrarily close to the values 0 or 1, by choosing irrational values of x close to 0 or 1, but $f(0) = f(1) = 1/2$. But despite the fact that the function is bounded it cannot achieve a maximum or minimum value.

There is a corrollary to the Extreme Value Theorem. Recalling that for a differentiable function we have that $f'(x) = 0$ at the maximum or minimum, we have

Corrollary

If f is differentiable on $[a, b]$ and $f(a) = f(b) = 0$. Then either we have the trivial case in which $f(x) = 0$ for all $x \in [a, b]$, or we see from the Extreme Value Theorem that there exists $c \in [a, b]$ such that $f'(c) = 0$.

This result is also geometrically obvious from a simple diagram.

The Mean Value Theorem

If f is continuous on $[a, b]$ and differentiable on (a, b), then there exists $\xi \in (a, b)$ such that

$$\frac{f(b) - f(a)}{(b - a)} = f'(\xi).$$

Geometrically: the chord from a to b must be parallel to the tangent to the curve at some point.

Proof

We first rewrite the result as

$$f(b) = f(a) + (b - a)f'(\xi).$$

Now we define the function

$$h(x) = f(x) - f(a) - (x - a)K$$

where K is defined by

$$f(b) = f(a) + (b - a)K$$

i.e. it is the gradient of the chord between the end-points. This means that $h(x)$ is the vertical distance between the curve $f(x)$ and the chord, and note that $h(a) = 0 = h(b)$.

The corrollary to the Extreme Value Theorem then implies that either $h(x) = 0$ for all x, or, there exists a point $\xi \in [a, b]$ such that $h'(\xi) = 0$. We therefore have

$$0 = h'(\xi) = f'(\xi) - K$$

which fixes $K = f'(\xi)$ and the results follows.

Example. L'Hopital's rule. Suppose we wish to compute

$$\lim_{x \to a} \frac{g(x)}{f(x)}$$

when both $f(x)$ and $g(x)$ go to zero at $x = a$. By the Mean Value Theorem we may write

$$\frac{g(x)}{f(x)} = \frac{g(x) - g(a)}{f(x) - f(a)} = \frac{(x-a)g'(\xi_1)}{(x-a)f'(\xi_2)} = \frac{g'(\xi_1)}{f'(\xi_2)}$$

where the points $\xi_1, \xi_2 \in [a, x]$. It follows that

$$\lim_{x \to a} \frac{g(x)}{f(x)} = \frac{g'(a)}{f'(a)}$$

which is L'Hopital's rule.

Example. Uniqueness of fixed points. We showed that a continuous function $f : [a, b] \to [a, b]$ has a fixed point, but it is not necessarily unique (and it is easy to think of examples for which there is more than one). However, if f is differentiable and also $|f'| < 1$, then uniqueness follows.

To prove this we suppose for contradiction that there exist two fixed point $x_1 \neq x_2$, so that $x_1 = f(x_1)$ and $x_2 = f(x_2)$. Then from the Mean Value Theorem we have

$$|x_2 - x_1| = |f(x_2) - f(x_1)| = |x_2 - x_1|.|f'(\xi)|$$

for some $\xi \in [x_1, x_2]$. However, since $|f'(\xi| < 1$ this is a contradiction unless $x_1 = x_2$.

The Mean Value Theorem may be extended to second order. We have the following:

Theorem

If f is continuous on $[a, b]$ and twice differentiable on (a, b), then there exists $\xi \in (a, b)$ such that

$$f(b) = f(a) + (b-a)f'(a) + \frac{1}{2}(b-a)^2 f''(\xi)$$

Proof (NE)

Consider the function

$$g(x) = f(x) - f(a) - (x-a)f'(a) - \frac{1}{2}(x-a)^2 M$$

for some constant M. Clearly $g(a) = 0$. We now require that $g(b) = 0$, which fixes M via the relation

$$f(b) = f(a) + (b-a)f'(a) + \frac{1}{2}(b-a)^2 M$$

We now need to show that M is also given by $M = f''(\xi)$ for some ξ.

The Mean Value Theorem applied to $g(x)$ implies that there exists $c \in [a, b]$ such that $g'(c) = 0$, which means that

$$f'(c) - f'(a) - (c-a)M = 0$$

or in other words

$$M = \frac{f'(c) - f'(a)}{(c-a)}$$

Applying the Mean Value Theorem to $f'(x)$ we have that there exists $\xi \in [a, c]$ such that

$$f''(\xi) = \frac{f'(c) - f'(a)}{(c-a)} = M.$$

Noting that $\xi \in [a, c]$ implies that $x \in [a, b]$, this proves the theorem.

6.6 Taylor Series and Analytic Functions

The above results may be extended to arbitrary n, assuming all the derivatives $f^{(k)}(x)$ exist for $k = 1$ to n, which leads to **Taylor's theorem**:

$$f(b) = \sum_{k=0}^{n-1} \frac{(b-a)^k}{k!} f^{(k)}(a) + \frac{(b-a)^n}{n!} f^{(n)}(\xi)$$

for some $\xi \in (a, b)$. This gives a precise way of approximating functions by a finite power series about a point. The limit $n \to \infty$ in Taylor's theorem leads us into considering the Taylor series.

Definition

> Suppose a function f is C^∞ on an interval A. Its **Taylor series** about a point $a \in A$ is the function given by the infinite series:
>
> $$\sum_{k=0}^{\infty} \frac{(x-a)^k}{k!} f^{(k)}(a)$$

As we will see shortly there are some subtleties involved in equating the Taylor series with the function $f(x)$.

Examples: There are many familiar examples of Taylor series, such as the following series around $x = 0$:

- $e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$
- $\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots$
- $\frac{1}{1-x} = 1 + x + \frac{x^2}{2} + \ldots$

A given Taylor series may not converge and in that case cannot be equated with the function $f(x)$. The first two above converge for all x but the third example, the series for $1/(1-x)$, converges only for $|x| < 1$.

Even if the series does converge, there is another way in which it is not necessarily equal to the function in the neighborhood of the point ξ. A good example of what can go wrong is the function:

$$f(x) = e^{-\frac{1}{x^2}}$$

The Taylor expansion of this function at $x = 0$ is simply $f(x) = 0$, since $f^{(n)}(0) = 0$ for any $n \in \mathbb{N}$. (Prove this). This is certainly convergent, but doesn't agree with the function anywhere other than at $x = 0$. For this reason we have the following definition.

Definition

> Suppose a function f is C^∞ on an interval I. Then f is **real analytic** at a point $a \in I$ if and only if f is equal to its Taylor expansion in some open interval containing a.

Note that this implies the Taylor series must converge for x near a.

Examples. Elementary functions like e^x, $\cos x$ and x^n for any n are real analytic, as indicated above. Perhaps the most important example of a function which is C^∞ but not real analytic is the function

$$f(x) = \exp\left(-\frac{1}{x^2}\right).$$

All of its derivatives at $x = 0$ vanish so it is not equal to its Taylor series there.

The idea of an analytic function takes on particular importance in complex analysis – the extension of the ideas described in this course to functions f which may the complex plane into itself. There, the property of analyticity allows some particularly useful theorems to be proved.

6.7 Distribution Theory (NE)

In Fourier analysis you may have met the **Dirac delta-function**, $\delta(x)$, which is loosely defined by

$$\delta(x) = \begin{cases} 0, & \text{for} \;\; x \neq 0 \\ \infty & \text{for} \;\; x = 0 \end{cases}$$

It has the properties

$$\int_{-\infty}^{\infty} dx \; \delta(x) = 1, \qquad \int_{-\infty}^{\infty} dx \; \delta(x) f(x) = f(0)$$

for any function f. Despite the fact that $\delta(0) = \infty$, from the physicist's point of view this definition seems reasonable, since we could clearly define $\delta(x)$ as the limit of a function with unit area centred around the origin, e.g. the rectangular function

$$\delta_\sigma(x) = \begin{cases} \frac{1}{2\sigma}, & \text{for} \;\; x \in [-\sigma, \sigma] \\ 0 & \text{for} \;\; x \notin [-\sigma, \sigma] \end{cases}$$

However, the delta-function is not actually a function according to the definitions we have used here, since recall, a function is a map between sets from a clearly defined domain D to a clearly defined target T, and since ∞ is not a number, there is no target space. We could instead define $\delta(0) = c$ for some $c \in R$, with $\delta(x) = 0$ everywhere else, but this function would integrate to zero so does not have the above properties.

Fortunately, there is a way around this which is to note that the delta-function only ever arises within an integral, which inspired mathematicians to develop a rigiourous theory of objects more general than functions called **distributions**. In this approach, objects like $\delta(x)$ always appear in an integral alongside a class of functions $f(x)$ which are sufficiently well-behaved that the integral exists, despite the rather singular nature of the delta-function. Distribution theory allows some intuitively clear results involving $\delta(x)$ to be proved in a rigorous way, and this theory underlies a lot of important results in mathematical physics.

Appendix: Proof of the Extreme Value Theorem

We now give a standard proof of the extreme value theorem, which, recall states: if f is continuous on the interval $[a, b]$ then there exist points $x_1, x_2 \in [a, b]$ such that f achieves its maximum at x_1 and achieves its minimum at x_2. We give the proof for the case of the maximum. The case of the minimum is identical in form. The proof proceeds in two parts, the first part being to show that f is bounded from above. (We have shown that a function is bounded on an open neighbourhood if it is continuous at a point but this result is different.)

Boundedness Theorem

If f is continuous on the closed interval $[a, b]$ then it is bounded on that interval.

Proof

The fact that the result is not true on an open interval (e.g. $1/x$ on $(0, 1)$ is unbounded) mean that the closed property of the interval is key to the proof, and therefore suggests that convergent sequences in $[a, b]$ may play a key role. In addition it is natural also to use the fact that continuity implies that $f(a_n) \to f(a)$ for all sequences $a_n \to a$.

Suppose for contradiction that f is not bounded from above on $[a, b]$. This means that arbitrarily large values of $f(x)$ may be found for some x. Then for every $n \in \mathbb{N}$, there exists a number $x_n \in [a, b]$ such that $f(x_n) > n$. This defines a sequence x_n. We don't know if it converges, but by the Bolzano-Weierstrass theorem proved in Section 3 we know it must possess a convergent subsequence x_{n_k}, for some sequence $n_k \in \mathbb{N}$ for all $k \in \mathbb{N}$ (and note that $n_k \geq k$). Denoting the limit of the subsequence by x we have $x \in [a, b]$ because the interval is closed. Since f is continous on $[a, b]$ the subsequence $f(x_{n_k})$ must converge to $f(x)$,

However, the subsequence must also satisfy $f(x_n) > n$, i.e. $f(x_{n_k}) > n_k > k$ for all k, which means that the subsequence $f(x_{n_k})$ diverges, which is a contradiction. Hence the function must be bounded from above. QED.

We may now use this to prove the extreme value theorem.

Proof

The boundedness theorem implies that f is bounded from above on $[a, b]$. This means that the set $S = \{y \in \mathbb{R} \mid y = f(x),\ x \in [a, b]\}$ must possess a least upper bound M. There are then two possibilities. Either (i) $\exists\ x \in [a, b]$ such that $f(x) = M$, i.e. the maximum is achieved, or, (ii) $f(x) < M$ for all $x \in [a, b]$. We show that the second possibility is inconsistent with continuity of f. The following ingenious argument establishes this.

We consider the function

$$g(x) = \frac{1}{M - f(x)}$$

which is well-defined since $f(x) < M$ and is also continuous on $[a, b]$ since f is continuous. This implies that g is also bounded from above by the boundedness theorem.

However, since $f(x)$ can be arbitrarily close to M, g cannot in fact be bounded. More precisely, the key property of the least upper bound is that for any $\epsilon > 0$, there exists a member $f(x)$ of the set S such that $M - \epsilon < f(x) < M$, which in particular means that $M - f(x) < \epsilon$ and therefore that $g(x) > 1/\epsilon$ for any $\epsilon > 0$, which means that g is unbounded from above, which is a contradiction. Hence option (i) is the only possibility. QED.

This proof by contradiction is somewhat elusive. There exist more constructive proofs which make use of sequences. (See for example the Wikipedia page on the extreme value theorem). These two proofs are particularly instructive examples of the general techniques introduced in the course.