Math 521: Analysis I

Much of this course will focus on the real numbers, $\mathbb{R}$. In the first few lectures we will look specifically at the axioms required to define the real numbers and its algebraic structure.

Axioms are statements that we take to be self-evidently true, on which our mathematical structure is based.

Natural numbers $\mathbb{N}$

We build up the real numbers step by step. We begin with the natural numbers $\mathbb{N}$, which satisfy the Peano axioms

N1 : $1 \in \mathbb{N}$

N2 : If $n \in \mathbb{N}$, then its successor $n+1 \in \mathbb{N}$

N3 : 1 is not the successor of any element in $\mathbb{N}$

N4 : If n and m in $\mathbb{N}$ have the same successor, then $n = m$

N5 : A subset of $\mathbb{N}$ which contains 1, and which contains $n+1$ whenever it contains n, must equal $\mathbb{N}$

N5 is the only axiom that does not appear obvious. Suppose we take a subset S of $\mathbb{N}$ as described in N5. Then $1 \in S$. Since S contains $n+1$ whenever it contains n, it follows that $2 = 1+1 \in S$. Similarly $3 = 2+1 \in S$. By continuing this indefinitely, it is reasonable to conclude that $S = \mathbb{N}$.

For an alternative viewpoint, suppose N5 is false. Then $\exists\, S \subseteq \mathbb{N}$ such that

- $1 \in S$,
- if $n \in S$ then $n+1 \in S$,

but $S \neq \mathbb{N}$. Examine the smallest member of the set $T = \{n \in \mathbb{N} \mid n \notin S\}$, called n_0. Since $n_0 \notin 1$ it must be the successor to some number $n_0 - 1$. But $n_0 - 1 \in S$, since it is smaller than n_0. But its successor must be in S also, which is a contradiction (written as $\divideontimes$). Thus N5 must be true.

Note that the above argument relies on additional assumptions: (1) every non-empty subset of $\mathbb{N}$ contains a least element, and (2) if $n_0 \neq 1$ then n_0 is the successor to some number in $\mathbb{N}$. Thus we have not proved N5 from N1 – N4.

Induction

N5 is the basis for mathematical induction. Let $P_1, P_2, P_3, \ldots$ be a list of propositions that may or may not be true. Then if

- P_1 is true, (Basis for induction)
- P_{n+1} is true whenever P_n is true, (Induction step)

then all P_i are true.

Example

Proposition $11^n - 4^n$ is divisible by 7 $\forall n \in \mathbb{N}$

Proof For the basis for induction, consider $n=1$:

$$11^1 - 4^1 = 11 - 4 = 7$$

which is divisible by 7. For the induction step, assume that P_n is true, and consider P_{n+1}:

$$\begin{aligned} 11^{n+1} - 4^{n+1} &= (7+4)11^n - 4 \cdot 4^n \\ &= \underbrace{7 \cdot 11^n}_{\text{divisible by } 7} + \underbrace{4(11^n - 4^n)}_{\text{divisible by } 7 \text{ is } P_n \text{ is true}} \end{aligned}$$

Thus P_{n+1} holds. Hence by induction P_n is true $\forall n \in \mathbb{N}$.

Integers and rational numbers

We now want to do arithmetic. We want to work with a set of numbers F that has a group structure for the addition operator. This requires five axioms for a commutative group:

A0: $\forall a, b \quad a+b \in F$ (completeness)

A1: $a+(b+c) = (a+b)+c \quad \forall a,b,c$ (associativity)

A2: $a+b = b+a \quad \forall a,b$ (commutativity)

A3: $a+0 = a \quad \forall a$ (identity element)

A4: $\forall a, \exists -a$ such that $a+(-a)=0$ (inverse)

Note that A0 is not listed in the Ross textbook but is commonly included as a group axiom, where the result of adding two elements in the set must also be an element. Ross takes this as true for the number sets under consideration. Axioms A0, A1, A3, A4 define a group, and if A2 also holds then they defina a commutative group.

To satisfy the addition axioms we can no longer work with just $\mathbb{N}$. We need to use the integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ in order to have additive inverses, so that A4 holds.

We also want our set F to have a multiplicative operator. For two numbers $a, b \in F$ we write this as $a.b$, or simply ab. The multiplicative axioms are

$$M0: \ \forall a, b \quad ab \in F$$

$$M1: \ a(bc) = (ab)c \quad \forall a, b, c$$

$$M2: \ ab = ba \quad \forall a, b$$

$$M3: \ a.1 = a$$

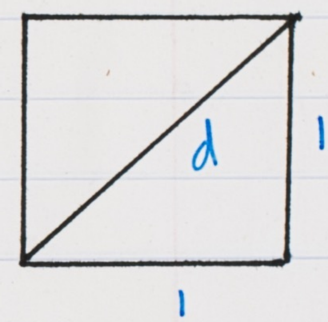
$$M4: \ \forall a \neq 0, \ \exists a^{-1} \text{ s.t } aa^{-1} = 1$$

In addition, we need a distributive law linking addition and multiplication together

$$DL: \ a(b+c) = ab + ac \quad \forall a, b, c$$

If the properties A0–A4, M0–M4, and DL are satisfied, then our set F is a field. We need to work with the rational numbers $\mathbb{Q}$ in order for M4 to hold.

The rational numbers $\mathbb{Q}$ are a very useful arithmetic system. It contains all terminating decimals.



However, we face problems when we start to solve algebraic equations, which arise in geometry. In the diagram to the right, we know that $d^2 = 2$ by Pythagoras' theorem.

Write the positive solution to this equation as $\sqrt{2}$. We can get very close to $\sqrt{2}$ in $\mathbb{Q}$:

- $1.4142^2 = 1.99996164$
- $1.4143^2 = 2.00024449$

But $\sqrt{2}$ is not rational.

Proof Suppose that $\sqrt{2}$ is rational so that $\sqrt{2} = p/q$. Choose the smallest form p/q by dividing through by a common divisor.

$$\frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2 \Rightarrow p \text{ is even.}$$

Hence $\exists\, k$ such that $p = 2k$. But then

$$4k^2 = 2q^2 \Rightarrow 2k^2 = q^2 \Rightarrow q \text{ is even.}$$

But then 2 is a common divisor of p and q, which is a contradiction. Therefore $\sqrt{2}$ must be irrational.

Definition

A number is algebraic if it satisfies a polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

where $n \geq 1$, $a_i \in \mathbb{Z}$ and $a_n \neq 0$. All rational numbers are algebraic.

Other examples include

$$\sqrt[3]{7}, \quad (\sqrt{2} + \sqrt{3})^{1/16}.$$

Rational zeroes theorem

Suppose $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ with $a_n \neq 0$, $a_0 \neq 0$ and $n \geq 1$. Suppose that $r \in \mathbb{Q}$ satisfies

$$a_n x^n + \ldots + a_1 x + a_0 = 0.$$

If $r = p/q$ where p & q are coprime and $q \neq 0$, then q divides a_n and p divides a_0.

Proof

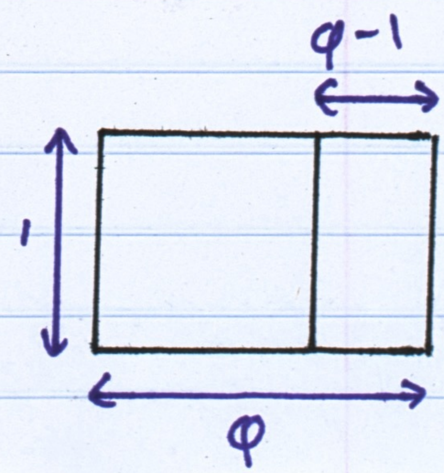
$$a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{r}{q}\right)^{n-1} + \ldots + a_0 = 0$$

$$a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_0 q^n = 0$$

Then $a_n p^n = -q[\ldots]$. Hence $q \mid a_n p^n$ and hence $q \mid a_n$ because p & q are coprime.

Similarly $a_0 q^n = -p[\ldots]$. Hence $p \mid a_0 q^n$ and therefore $p \mid a_0$.

Example



Consider a rectangle with side lengths 1 and φ. Suppose that a square is removed from the rectangle, and that the remainder of the rectangle has the same aspect ratio as the original shape. Then

$$\frac{\varphi}{1} = \frac{1}{\varphi - 1} \Rightarrow \varphi^2 = \varphi + 1 \Rightarrow \varphi^2 - \varphi - 1 = 0$$

φ is called the golden ratio and has been known since antiquity. If φ is rational so that $\varphi = p/q$, then $p \mid 1$ and $q \mid 1$. Thus the only candidate rational solutions are ± 1. But

$$1^2 - 1 - 1 = -1 \quad \text{(not satisfied)}$$
$$(-1)^2 - (-1) - 1 = 1 \quad \text{(not satisfied)}$$

and hence φ is irrational. Solving the equation shows that $\varphi = \frac{1+\sqrt{5}}{2}$.

Ordering

$\mathbb{Q}$ has an order structure given by

O1: Either $a \leq b$ or $b \leq a$.

O2: If $a \leq b$ and $b \leq a$, then $a = b$.

O3: If $a \leq b$ and $b \leq c$, then $a \leq c$.
(transitivity)

O4: If $a \leq b$ then $a + c \leq b + c$.

O5: If $a \leq b$ and $0 \leq c$ then $ac \leq bc$

Taken together with the previous axioms for arithmetic, O1 – O5 define an <u>ordered field.</u>

<u>Consequences of the field properties (Ross theorem 3.1)</u>

<u>(i) $a + c = b + c \Rightarrow a = b$</u>

<u>Proof</u> $\exists -c$ such that $c + (-c) \overset{(A4)}{=} 0$. Hence

$$(a+c) + (-c) = (b+c) + (-c)$$

$$\Rightarrow a + (c + (-c)) = b + (c + (-c)) \quad (A1)$$

$$\Rightarrow a + 0 = b + 0 \overset{(A3)}{\Rightarrow} a = b.$$

<u>(ii) $a.0 = 0$ for all a</u>

<u>Proof</u>
$$a.0 \overset{(A3)}{=} a.(0+0) \overset{(DL)}{=} a.0 + a.0$$

Hence $\overset{(A3)}{0 + a.0} = a.0 + a.0$ and using result (i) shows that $a.0 = 0$.

(iii) $(-a)b = -ab$ for all a, b

Proof We know that $a + (-a) = 0$. Hence

$$ab + (-a)b \overset{(DL)}{=} [a + (-a)]b \overset{(A4)}{=} 0.b \overset{(ii)}{=} 0$$

We also know $\overset{(A4)}{ab + (-ab) = 0}$ and by using result (i) we have $(-a)b = (-ab)$.

(iv) $(-a)(-b) = ab$ for all a, b

Proof We have by result (iii) that

$$\begin{aligned} (-a)(-b) + (-ab) &= (-a)(-b) + (-a)b \\ &= (-a)[(-b) + b] && (DL) \\ &= (-a).0 && (A4) \\ &= 0. && (ii) \end{aligned}$$

Adding ab to both sides shows that

$$[(-a)(-b) + (-ab)] + ab = 0 + ab$$

$$(-a)(-b) \overset{(A1)}{+} [(-ab) + (ab)] = 0 + ab$$

$$\underset{(A3)}{(-a)(-b) + 0} = 0 + ab \quad \Rightarrow (-a)(-b) = ab.$$

Example proof of an ordered field property (Ross theorem 3.2 (vi))

If $0 < a$, then $0 < a^{-1}$

Note that $a < b$ means that $a \leq b$ and $a \neq b$.

Proof Suppose that $0 < a$ but $0 < a^{-1}$ fails. Then $a^{-1} \leq 0$. Add $-a^{-1}$ to both sides and use O4 to obtain $0 \leq -a^{-1}$.

Now use O5: $0 \leq a$ and $0 \leq -a^{-1}$ so

$$0 \leq a(-a^{-1})$$
$$0 \leq -(a a^{-1})$$
$$0 \leq -1$$

Adding 1 to both sides shows that $1 \leq 0$. This can be proven not to be true as a homework exercise.

Hence by contradiction $0 < a^{-1}$.

Definition The absolute value of a is called $|a|$ and is given by

$$|a| = \begin{cases} +a & \text{if } a \geq 0, \\ -a & \text{if } a \leq 0. \end{cases}$$

Note that if $a=0$, then $-a=0$ and hence both cases of the definition are equivalent.

Definition $\operatorname{dist}(a,b) = |a-b|$.

Properties of the absolute value

(i) $|a| \geq 0$ for all $a \in \mathbb{R}$

(ii) $|ab| = |a| \cdot |b|$ for all $a, b \in \mathbb{R}$

(iii) $|a+b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$

Proof of (iii) We have

$$-|a| \leq a \leq |a|, \qquad -|b| \leq b \leq |b|,$$

and hence

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

Therefore $-(|a|+|b|) \leq a+b \leq |a|+|b|$ and

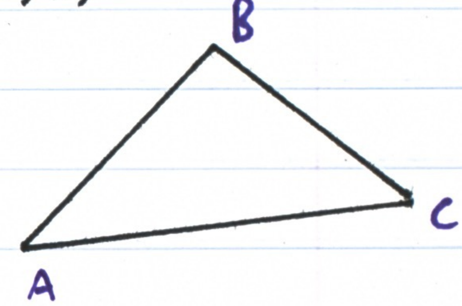
$$|a+b| \leq |a| + |b|.$$

Put $a = A-B$ and $b = B-C$. Then

$$|A-B+B-C| \leq |A-B| + |B-C|$$

$$|A-C| \leq |A-B| + |B-C|$$

$$\text{dist}(A,C) \leq \text{dist}(A,B) + \text{dist}(B,C)$$



This is called the triangle inequality. As demonstrated in the diagram, the distance from A to C directly will always be shorter than going via B. The triangle inequality is useful in many other contexts.

<u>Definition</u> Let S be a non-empty subset of $\mathbb{R}$. If it contains a largest element s_0, so that $s_0 \in S$ and $s \leq s_0 \ \forall s \in S$, the s_0 is the maximum of S and we write $s_0 = \max S$.

If S contains a smallest element, we call it the minimum and write it as $\min S$

<u>Example</u> Finite subsets always have a minumum and maximum. If $S = \{3, \pi, \pi^2\}$ then

$$\min S = 3, \qquad \max S = \pi^2.$$

Intervals Suppose $a<b$. Then define

- Open interval $(a,b)=\{x\in\mathbb{R} \mid a<x<b\}$
- Closed interval $[a,b]=\{x\in\mathbb{R} \mid a\leq x\leq b\}$
- Semi-open interval $(a,b]=\{x\in\mathbb{R} \mid a<x\leq b\}$

For the closed interval, $\min[a,b]=a$ and $\max[a,b]=b$. But the open interval does not have a maximum or minimum.

Consider $(0,1)$ and suppose that $d\in(0,1)$ is a minimum. Then since $d>0$, $\frac{d}{2}>0$ and $\frac{d}{2}\in(0,1)$. But $\frac{d}{2}<d$ and thus d is not a minimum. ⨳

The sets $\mathbb{Z}$ and $\mathbb{Q}$ have no minima or maxima.

Definition Let S be a non-empty subset of $\mathbb{R}$

(a) If $M\in\mathbb{R}$ satisfies $s\leq M$ $\forall s\in S$, then M is called an upper bound of S, and S is said to be bounded above.

(b) If $M\in\mathbb{R}$ satisfies $m\leq s$ $\forall s\in S$, then m is called a **lower bound**, and S is said to be **bounded below**.

(c) S is said to be **bounded** if it is bounded above and bounded below. Thus $\exists\, m, M$ s.t $S \subseteq [m, M]$.

A maximum is always an upper bound. For (a,b), b is an upper bound.

Consider $\{r \in \mathbb{Q} \mid 0 \le r \le \sqrt{2}\}$. Then the smallest upper bound is $\sqrt{2}$.

Definition Let S be a non-empty subset of $\mathbb{R}$

(a) If S is bounded above and S has a least upper bound, then we call it the **supremum** of S, $\sup S$.

(b) If S is bounded below and S has a greatest lower bound, then we call it the **infimum** of S, $\inf S$.

If $\max S$ exists then $\max S = \sup S$.

$\sup\,(a,b) = \sup\,(a,b] = \sup\,[a,b) = \sup\,[a,b] = b$.

(supremum exists in all four cases)

We now reach the key axiom that separates the rational numbers $\mathbb{Q}$ from the real numbers $\mathbb{R}$.

Completeness axiom

Every non-empty subset S of $\mathbb{R}$ that is bounded above has a least upper bound. $\sup S$ exists and is a real number.

Note This axiom may appear abstract. But it can be related to how we think about real numbers. Consider π: it can be represented by a non-repeating decimal expansion. Adding more digits gets us closer to the result. Consider a set of ever-more accurate decimal expansions.

$$S = \{3,\ 3.14,\ 3.14159,\ 3.1415926535,\ 3.1415926535897932384626433832795028841971693993751,\ \ldots\}$$

Then $\pi = \sup S$.

There are a number of alternative axioms to the completeness axiom, which result in the same mathematical structure.

Corollary Every non-empty subset S of $\mathbb{R}$ that is bounded below has a greatest lower bound $\inf S$

Proof Let $-S$ be the set $\{-s \mid s \in S\}$.

$\exists m \in \mathbb{R}$ s.t. $m \leq s \quad \forall s \in S$

Hence $-m \geq -s \quad \forall s \in S$, so $-m \geq u \quad \forall u \in -S$, and $-S$ is bounded above. Hence $\sup(-S)$ exists.

We aim to show that if $s_0 = \sup(-S)$, then $-s_0 = \inf S$. Consider two properties:

① $-s_0$ is a lower bound of S: $-s_0 \leq s \quad \forall s \in S$

If $s \in S$, then $-s \in -S$, so $-s \leq s_0$ and $s \geq -s_0$.

② $-s_0$ is the greatest lower bound of S: if $t \leq s \quad \forall s \in S$ then $t \leq -s_0$.

If $t \leq s \quad \forall s \in S$, then $-t \geq -s \quad \forall s \in S$, and hence $-t \geq x \quad \forall x \in -S$. Therefore $-t$ is an upper bound for $-S$, so $-t \geq \sup(-S) = s_0$. Therefore $t \leq -s_0$.

Archimedean property

If $a>0$ and $b>0$ then for some positive integer n, $na>b$.

Proof Assume it fails. Then $\exists a>0$ and $b>0$ such that $na \leq b$ for all n. Hence b is an upper bound for the set $S=\{na \mid n \in \mathbb{N}\}$. Let $s_0 = \sup S$, which must exist via the completeness axiom. Since $a>0$, $s_0 - a < s_0$. Then since s_0 is the least upper bound, $s_0 - a$ can't be an upper bound and $\exists n_0 \in \mathbb{N}$ such that $s_0 - a < n_0 a$, which implies $s_0 < (n_0+1)a$. But $(n_0+1)a \in S$, and thus s_0 is not an upper bound. $\#$

Denseness of $\mathbb{Q}$

If $a, b \in \mathbb{R}$ and $a<b$, $\exists r \in \mathbb{Q}$ such that $a<r<b$.

Proof We show that $a < \frac{m}{n} < b$ for $m,n \in \mathbb{Z}$ and $n \neq 0$. This is equivalent to $an < m < bn$.

We have $b-a>0$, so the Archimedean property says $\exists n \in \mathbb{N}$ s.t. $n(b-a)>1$. Hence $bn - an > 1$.

Using the Archimedean property again, there exists an integer $k > \max\{|an|, |bn|\}$, so that

$$-k < an < bn < k.$$

Consider the sets $K = \{j \in \mathbb{Z} \mid -k \leq j \leq k\}$ and $\{j \in K \mid an < j\}$. They are finite and non-empty since they both contain k. Let $m = \min\{j \in K \mid an < j\}$. Then $-k < an < m$. Since $m > -k$, we have $m - 1 \in K$, so $an < m-1$ is false by our choice of m. Thus $m - 1 \leq an$ and $m \leq an + 1 < bn$. Thus $an < m < bn$.

Infinity

∞ and $-\infty$ are useful symbols but they are not real numbers. We can extend ordering to $\mathbb{R} \cup \{-\infty, \infty\}$ by saying $-\infty \leq a \leq \infty$ $\forall a \in \mathbb{R}$. This is consistent with axioms O1–O3 but there is no algebraic structure.

We can use the symbols to specify intervals:

$(-\infty, \infty) = \mathbb{R}$

- $[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$ unbounded closed interval
- $(b, \infty) = \{x \in \mathbb{R} \mid b < x\}$ unbounded open interval.

Also:
- Define $\sup S = \infty$ if S is not bounded above
- Define $\inf S = -\infty$ if S is not bounded below