

Notes for 13th Jan (Friday)

1 Recap

1. We defined multiplication, ordering, negation, and reciprocals of reals and said that you can prove all the usual properties in principle for these things.
2. We proved the supremum property of reals assuming the density of rationals and the Archimedean property.
3. We proved that n^{th} roots of positive reals exist and if required to be positive, are unique.

2 Reals (cont'd)..

As a corollary of the existence and uniqueness of positive roots, $a^{1/n}b^{1/n} = (ab)^{1/n}$ because of commutativity of multiplication and uniqueness of the n th root.

We haven't yet proved the density of rationals and their Archimedean property ! Let's remedy that.

Lemma 2.1. *If $x < y \in \mathbb{R}$ then there exists a rational p/q such that $x < p/q < y$.*

Proof. Indeed, there exists a natural N so that $x_i < y_i$ for all $i > N$ (by definition). Actually there exists an N so that $y_i - x_i > u$ for some rational $u > 0$ for all $i \geq N$. (This is because $y - x > 0$ is the same thing as saying that $y_i \geq x_i$ and $y - x \neq 0$ which is the same as saying that $|y_i - x_i| \geq \epsilon$ for some $\epsilon > 0$ for all sufficiently large i .)

Assume that \tilde{N} is such a large natural number that $|x_i - x_j| < \frac{u}{4}$ and $|y_i - y_j| < \frac{u}{4}$ for all $i, j \geq \tilde{N}$. We claim that $r = x_{\tilde{N}} + \frac{u}{2}$ lies between x and y . Indeed, $r - x_i = \frac{u}{2} + x_{\tilde{N}} - x_i > \frac{u}{2} - \frac{u}{4} = \frac{u}{4} > 0$ and $y_i - r > y_{\tilde{N}} - \frac{u}{4} - x_{\tilde{N}} - \frac{u}{2} > u - \frac{3u}{4} = \frac{u}{4} > 0$. \square

The following one is about the Archimedean property.

Lemma 2.2. *If x and y are two reals, and $x > 0$ then there exists a positive integer m such that $mx > y$.*

Proof. We only need to consider the case of $0 < x < y$ (Why?). By density of rationals, there exists rationals r_1, r_2, r_3 such that $0 < r_1 < x < r_2 < y < r_3$. The Archimedean property holds for rationals. (Why?) Therefore $r_1N > r_2$ and $r_2M > r_3$. Therefore $NMx > NMr_1 > Mr_2 > r_3 > y$. \square

We are used to writing real numbers in terms of their decimal expansion (certainly not as Cauchy sequences of rationals). Here is the justification for the same.

Let $x > 0$ wLOG. If a_0 is the largest natural $\leq x$ (Archimedean property), then $x - a_0 \geq 0$. Applying the Archimedean property again, $\exists a_1$ the largest natural number such that $x - a_0 - \frac{a_1}{10} \geq 0$. Likewise, we get a sequence of naturals a_0, a_1, \dots such that $x - a_0 - \frac{a_1}{10} - \frac{a_2}{100} \dots \geq 0$. The sequence of rationals $s_n = \sum_{i=0}^n \frac{a_i}{10^i}$ is then bounded above by x . The least above bound of the set (s_0, \dots) is then x . Conversely, any infinite decimal represents a Cauchy sequence of rationals and thus a real number. However, the map is not 1-1. (Some reals have two decimal expansions like $0.999999\dots = 1$. Prove as an exercise that a real can have at most two decimal expansions.)

Cardinality of real numbers : Later on we will define $\tan(\frac{\pi}{2}x)$ and prove its properties. In particular, we will show that it is a bijection from $(-1, 1) \rightarrow \mathbb{R}$. (We will not use the cardinality of reals anywhere after this. So the following argument is not circular.) There is the obvious bijection $f(x) = 2x - 1$ from $(0, 1) \rightarrow (-1, 1)$. We will calculate the cardinality of $(0, 1)$.

Firstly, here is Cantor's original argument to show that Reals are not countable. Indeed, if they are countable, i.e., one can enumerate reals in $(0, 1)$ written using their decimal expansions (with no trailing 9s) as

$$\begin{aligned} x_1 &= 0.x_{11}x_{12}x_{13}\dots \\ x_2 &= 0.x_{21}x_{22}x_{23}\dots \\ &\vdots \end{aligned} \tag{1}$$

Then create a new real number $a = 0.a_1a_2\dots$ where a_i is any integer in $[1, 8]$ not equal to x_{ii} . This new number differs from every number on this list because if it differs from x_k in the k^{th} digit. This is a contradiction. (Cantor's diagonalisation.)

But this does not show that $\#\mathbb{R} = \#\mathcal{P}(\mathbb{N})$. There is an injection from $(0, 1)$ to infinite sequences of natural numbers (which form a subset of $\mathcal{P}(\mathbb{N} \times \mathbb{N})$). So assuming the continuum hypothesis we see that $\#\mathbb{R} = \#\mathcal{P}(\mathbb{N})$. But we definitely do not need the continuum hypothesis to prove this result. Indeed, the set of infinite binary sequences is bijective to $\mathcal{P}(\mathbb{N})$ (either choose a number to be in your subset or not). Now, consider an infinite sequence $0.a_1a_2\dots$ formed out of 0 and 1. This represents the base 3 expansion of a real number. It is $1 - 1$. Therefore, by the Schroeder-Bernstein theorem we are done.

3 Complex numbers

I will not do these in detail. (Largely because this course is not about complex numbers.)

The field of complex numbers \mathbb{C} is defined to be \mathbb{R}^2 endowed with the following addition and multiplication rules :

1. The 0 (additive identity) complex number is defined as $(0, 0)$.

2. The 1 (multiplicative identity) complex number is defined as $(1, 0)$.
3. Addition : $(a, b) + (c, d) = (a + b, c + d)$.
4. Multiplication : $(a, b)(c, d) = (ac - bd, ad + bc)$.
5. Negation : $-(a, b) = (-a, -b)$.
6. Reciprocal : If $(a, b) \neq (0, 0)$ then $(a, b)^{-1} = (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$

Of course, usually one writes i or $\sqrt{-1}$ as $(0, 1)$. So every complex number $z = a + ib$. One defines the conjugate $\bar{z} = a - ib$ for convenience. Also, the length of a complex number $|z| = \sqrt{x^2 + y^2}$. Hence $|z|^2 = z\bar{z}$. Moreover, one has the triangle inequality $||z_1| - |z_2|| \leq |z_1 + z_2| \leq |z_1| + |z_2|$. The rest of it as they say is history.

Lastly, *every* polynomial whose coefficients are complex numbers has a root in complex numbers. This is the fundamental theorem of algebra. Its proof is quite non-trivial.

The complex field *cannot* be made into an ordered field.

4 Euclidean space

Before we delve into this, let's have some fun. In school most of us would've seen things like $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$, i.e., examples of Pythagorean triplets. Can one come up with a general formula for producing all integers (a, b, c) satisfying $a^2 + b^2 = c^2$?

The question is equivalent to finding all rationals (x, y) such that $x^2 + y^2 = 1$. This looks tantalising. So we want to find all rational points on the unit circle. Clearly any rational point can be connected to $(1, 0)$ by a unique line of a rational slope m . Conversely, suppose you take $y = m(x - 1)$ such that $x^2 + y^2 = 1$ then you can see that $x = \frac{m^2-1}{m^2+1}$ and $y = \frac{-2m}{m^2+1}$. So we have found a general formula for a problem of number theory using geometry. Now someone could ask you a question like "Find all numbers (a, b, c, d, e) such that $e^2 = a^2 + b^2 + c^2 + d^2$ " and so on. To answer these questions (and many questions from real life that depend on more than one quantity), we need to study the geometry of \mathbb{R}^n (defined recursively as the Cartesian product of \mathbb{R}^{n-1} and \mathbb{R}).