Notes for 11th Jan (Wednesday)

1 Recap

1. Proved that the cardinality of X is strictly less than that of $\mathcal{P}(X)$.
2. Defined Integers and stated their usual properties.
3. Likewise for rationals.
4. Defined an ordered set, a field, and an ordered field.

2 Real numbers

Firstly, we prove that

Proposition 2.1. *There is no rational number x so that $x^2 = 2$.*

Proof. Indeed, if $x = p/q$ (where $p, q > 0$) did satisfy $x^2 = 2$, then $p^2 = 2q^2$. Since p is either even xor odd, and $(2k)^2 = 4k^2 = 2(2k^2)$ is even, and $(2k+1)^2 = 2(2k^2+k)+1$ is odd, we know that $p = 2k$. Therefore, $4k^2 = 2q^2$ which means that $2k^2 = q^2$. This means that $y = q/k$ also satisfies the equation such that $||(p,q)|| > ||(q,k)||$. Since integers satisfy the well-ordering property, this sequence of solutions to $x^2 = 2$ must terminate. This is a contradiction. (Method of infinite descent.) □

What is really going on is that

Proposition 2.2. *Let A be the set of all rationals $x = p/q$ such that $x^2 < 2$ and B be the set of all rationals p/q such that $x^2 > 2$. For every $x \in A$ there exists a rational $y \in A$ such that $y > x$ and likewise for B.*

Proof. Indeed, if $x \in A$, then $y = x + \frac{2-x^2}{x+2}$ is indeed $> x$ (and likewise $< x$ if $x \in B$). $y = \frac{2x+2}{x+2}$. Thus

$$y^2 - 2 = \frac{4x^2+8x+4}{x^2+4x+4} - 2 = \frac{2x^2-4}{x^2+4x+4} < 0 \tag{1}$$

□

The previous proposition shows that indeed A has no largest number and B no smallest. Therefore, the rationals have gaps in between. The proposition also gives us an idea of how to correct them. Indeed,

Definition : Let $(S, \leq)$ be a totally ordered set (where $a \geq b$ means that $b \leq a$). S is said to satisfy where the "least upper bound" (sup) property if every non-empty subset A that is bounded above has a least upper bound, i.e., if $\exists m \in S$ such that $x \leq m$ for every $x \in A$, then $\exists n \leq m \in S$ such that

1. n is an upper bound of A, i.e., $x \leq n$ for every $x \in A$, and
2. Any element q strictly less than n is not an upper bound of A, i.e. $\exists y \in A$ such that $q < y$.

Such an n (written as $\sup A$) is called the supremum or the least upper bound of A. (Likewise for $\inf A$ or greatest lower bound.) So A in the proposition does not have a least upper bound in rationals. Please note that the supremum if it exists, *need not be an element of A.*

Theorem 1. *If a set $S, \leq$ has the sup property, then it automatically has the inf property.*

Proof. Indeed, if $A \subset S$ is bounded below, then let L be the set of all lower bounds of A (which is non-empty by assumption). Clearly L is bounded above (by any element of A). Let $l = \sup L$. We claim that $l = \inf A$. Indeed,

1. l is a lower bound on A. Assume the contrary. If $a \in A < l$ then by definition $\exists x \in L$ such that $x > a$. But this is a contradiction.
2. Any $x > l$ cannot be a lower bound of A. Indeed, if it is so, then $x \in L$ contradicting the supremality of l.

□

By the way, it is easy to prove the supremum if it exists, is unique.

Finally, we have Dedekind's theorem.

Theorem 2. *There exists a unique ordered field $\mathbb{R}$ having the sup property. Moreover, $\mathbb{Q} \subset \mathbb{R}$.*

The proof of this statement is somewhat long. We first sketch the proof of uniqueness and then prove existence. (There are many constructions of real numbers from rationals. We will construct them using Cauchy sequences.)

Uniqueness : Firstly, any ordered field F has to contain the rationals. Indeed, there exists no non-zero $p \in F$ so that $p.1 = 1 + 1 + 1 + ...1(p \ times) = 0$ (i.e. $p.x = 0 \ \forall \ x \neq 0$). If there was one, then if $x < y$ then $px = 0 < py = 0$ (by the axioms of an ordered field), a contradiction. Therefore, the map $\mathbb{Z} \to F$ given by $f(n) = n.1$ is an injection (and respects addition, multiplication, and ordering). Hence, the map $\mathbb{Q} \to F$ given by

$f(p/q) = \frac{f(p)}{f(q)}$ is an injection (and respects the other properties).

Define the map $g : \mathbb{R} \to F$ as follows. If x is rational, then $g(x) = f(x)$. If x is irrational, let $L_x\mathbb{R}$ be the set of all rationals less than x. Let $g(x) = \sup_{a \in L_x} g(a)$. (We know that $g(L_x)$ is bounded above. (Why ?) We claim that this map is injective, surjective, and preserves all the properties. (Why?)

Existence : To do this, let's return to $\sqrt{2}$. Note that we can find very good rational approximations to this "number", i.e., $1, 1.4, 1.41, 1.414$ etc. The problem is that while the sequence above consists of rational numbers that get very close to one another eventually, the sequence itself does not "converge" to any rational number. So, roughly speaking, we want to define the real number $\sqrt{2}$ as the sequence of rationals $1, 1.4, 1.41, 1.414, \ldots$ (we want to artificially plug in the holes in the rationals). However, naughty people might come up with another sequence of rationals $0.9, 1, 1.41, 1.41, 1.414, 1.414, \ldots$ which also seems to "converge" to $\sqrt{2}$. So we need to say that both sequences represent the same number. To make all of these things precise, here are some definitions.

Sequence of rationals : We already know what this means. It is a function $f : \mathbb{N} \to \mathbb{Q}$. But write it informally as $a_1, a_2, \ldots$.
Convergence of a sequence : A sequence $\{a_i\}$ of rationals is said to converge to a rational x if for every rational $\epsilon > 0$ there exists a natural N so that $n > N \to |a_n - x| < \epsilon$. (Note that here we are using a "norm" $|\ |$ to "measure" how "large" a rational is. There are other choices of norms that lead to completely different fields (when the following construction is applied). These are called the p-adic number fields. They are very important in number theory.)
Cauchy sequence : A Cauchy sequence of rationals is a sequence $\{a_i\}$ such that for every rational $\epsilon > 0$, there exists a natural N such that $m, n > N \to |a_m - a_n| < \epsilon$. In other words, the sequence eventually consists of nearby numbers.
Equivalence relation between Cauchy sequences : Two Cauchy sequences a_i and b_i are said to be related (and you can verify that it is an equivalence relation) if they eventually become close, i.e., for every rational $\epsilon > 0$ there exists a natural N such that $n > N \to |a_n - b_n| < \epsilon$.

Finally, the set $\mathbb{R}$ is the set of equivalence classes of Cauchy sequences of rationals. In plain english it means "Every real number is a sequence of rational numbers (the sequence need not be unique)."

Now we are not done yet! We still have to make this set an ordered field and prove that it has the goddamned least upper bound property!

Zero : The equivalence class of the sequence $(0, 0, \ldots)$ is defined to be 0.
One : The equivalence class of the sequence $(1, 1, \ldots)$ is defined to be 1.
Addition : If $x = [a_i]$ and $y = [b_i]$ then $x+y$ is defined to be the Cauchy sequence $[a_i + b_i]$. (Why is this Cauchy ?)