Notes for 6th Jan (Friday)

1 Recap

1. Defined addition, multiplication, ordering, and exponentiation of natural numbers. Also stated their properties and the strong principle of induction.
2. Defined the cardinality equivalence relation between sets.
3. Proved that an infinite subset of a countable set is countable, $\mathbb{N} \times \mathbb{N}$ is countable, and the countable union of countable sets is countable.

2 Cardinality (cont'd...)

Here is a fundamental result.

Theorem 1. *There is no surjection from X to its power set $\mathcal{P}(X)$, i.e., the power set has strictly "larger" cardinality.*

Proof. The following proof is due to Georg Cantor. He introduced a revolutionary idea of a proof, now called "Cantor's diagonalisation". Cantor was branded a charlatan (by Kronecker) and his ideas "a disease" by Herni Poincaré. Cantor has been well vindicated. Suppose there is a surjection $f : X \to \mathcal{P}(X)$. Then consider the subset of X given by $A = \{a \in X | a \notin f(a)\}$. This we claim cannot be in the image of f thus producing a contradiction. Indeed, if $f(b) = A$, then there are two possibilities. Either $b \in f(b)$ which means it cannot be in $f(b)$, or $b \notin f(b)$ which means it has to be in $f(b)$ (the barber paradox). □

This means that $\mathbb{N}$ has strictly "smaller" than its power set. A natural question is :

The continuum hypothesis : Is there any set in between the naturals and its power set ? That is, one that admits an injection from the naturals, but not a surjection and does not surject to the power set of the naturals ?

Paul Cohen won a fields medal for proving that this question can neither be proven or disproven in ZFC.

Natural numbers are said to be countable. (If you are not countable, then you are uncountable. But in this course when we say uncountable, we are specifically referring to the cardinality of the power set of the naturals.)

There are two theorems which sound intuitively plausible but are not immediately obvious to prove. I shan't prove them. I suggest you try proving them on your own before you look up on wikipedia.

The first of these is the Schroeder-Bernstein theorem.

Theorem 2. *If A injects into B and B injects into A, then there exists a bijection between A and B. (Does not use the axiom of choice.)*

The second is of the same flavour.

Theorem 3. *If A surjects into B and B surjects into A, then there exists a bijection between A and B. (Uses the axiom of choice. Not sure whether it is equivalent to it though.)*

3 Integers

So far we have addition, and a "cancellation" property but we do not have numbers to add to 1 to get 0, i.e., you can borrow money but not lend it. So we want to define integers as follows :
An integer is a pair of natural numbers (a, b) written as $a - b$.
But let's be more precise. First, we need to know what an equivalence relation on a set A is : It is a subset R in $A \times A$ such that

1. Reflexivity : $(a, a) \in R$
2. Symmetry : $(a, b) \in R \Rightarrow (b, a) \in R$
3. Transitivity : $(a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R$.

If $(a, b) \in R$ we write $a \equiv b$. An equivalence relation partitions a set into equivalence classes, i.e., subsets E such that they are disjoint and their union is A. Each E consists of elements equivalent to one another.
Define an equivalence relation on pairs of natural numbers saying $(a, b) \equiv (c, d)$ if $a + d = b + c$. This splits the pairs into equivalence classes. The set of these equivalence classes (which is a subset of $\mathbb{N} \times \mathbb{N}$) is called $\mathbb{Z}$ (integers). Every integer is written as $a - b$ instead of (a, b) where (a, b) is any representative of the equivalence class.

Addition : $(a - b) + (c - d)$ is defined to be $(a + c) - (b + d)$.

Multiplication : $(a - b) \times (c - d) = (ac + bd) - (ad + bc)$.

We need to show that these are well-defined, i.e. if we replace $a - b$ with another representative $\alpha - \beta$ such that $a + \beta = b + \alpha$, then we should get the same integers in the above definitions (and likewise for $c - d$ replaced with $\gamma - \delta$). Let's verify that addition is well-defined. Multiplication is similar.

We claim that $(\alpha + \gamma) - (\beta + \delta) \equiv (a + c) - (b + d)$. Indeed,

$$(\alpha + \gamma) + (b + d) = b + \alpha + d + \gamma = a + \beta + c + \delta = (a + c) + (\beta + \delta)$$

Now define a map $\iota : \mathbb{N} \to \mathbb{Z}$ as $\iota(n) = n - 0$. This is a bijection that respects addition and multiplication. (Exercise.) Thus the natural numbers "sit" inside the integers.

The negation of an integer $a - -b$ is defined as $-(a - b) = b - a$. One can prove the trichotomy law, i.e., every integer is either 0, a positive natural number, or $-n$ where n is a positive natural number.

Now we may state and prove that integers satisfy all the nice properties that we are used to :

1. $x + y = y + x$
2. $x + 0 = 0 + x = x$
3. $x + (-x) = (-x) + x = 0$
4. $(x + y) + z = x + (y + z)$
5. $x \times y = y \times x$
6. $x \times (y + z) = x \times y + x \times z$
7. $(x \times y) \times z = x \times (y \times z)$
8. $x \times 1 = 1 \times x = x$

Objects that obey the above laws are called commutative rings. (So the properties above say that $\mathbb{Z}$ is a commutative ring.) We can define subtraction of two integers $x - y$ as $x + (-y)$. (Check that this is well-defined.)

Some other properties are

1. No zero divisors (i.e. $ab = 0$ if and only if $a = 0$ or $b = 0$).
2. Cancellation law : If $ac = bc$ and $c \neq 0$ then $a = b$.

Ordering : $n \geq m$ if $n = m + a$ for some natural number a. If $n \geq m$ and $n \neq m$, we say $n > m$. With this definition, it is easy to prove the usual properties of order :

1. $a > b$ if and only if $a - b$ is a positive natural number.
2. If $a > b$, then $a + c > b + c$.
3. If $a > b$, and $c > 0$ then $ac > bc$.
4. If $a > b$ then $-a < -b$.
5. If $a > b$ and $b > c$, then $a > c$.
6. Either $a = b$ xor $a > b$ xor $a < b$.

Finally, the set of integers has the same cardinality as that of natural numbers. Indeed, a bijection is $f(2n - 1) = n, f(2n) = -n$.

4 Rational numbers

We do not know how to divide a banana into two equal parts. So now we define the rational numbers formally -

The set $\mathbb{Q}$ of rational numbers is the set of equivalence classes of pairs of integers (a, b) (written as a/b) where $b \neq 0$ such that $a/b \equiv c/d \Leftrightarrow ad = bc$.

Using "countable unions of countable sets is countable" and the Schroeder-Bernstein type results we can prove that rationals are countable.

We may define negation as $-p/q = (-p)/q$, addition as $p/q + r/s = (ps + qr)/qs$ and multiplication as $p/q \times r/s = (pr)/(qs)$.

You can make $\mathbb{Z}$ sit bijectively in $\mathbb{Q}$ whilst respecting addition, multiplication (and ordering as we shall see) via : $\iota(n) = n/1$.

Define the reciprocal x^{-1} of a non-zero rational (i.e. when $x \neq 0/1$) as follows : If $x = p/q$, then $x^{-1} = q/p$.

Properties of rationals :

1. $x + y = y + x$
2. $x + (y + z) = (x + y) + z$
3. $x + 0 = 0 + x = x$
4. $x + (-x) = (-x) + x = 0$
5. $xy = yx$
6. $(xy)z = x(yz)$
7. $(x + y)z = xz + yz$
8. $x.1 = 1.x = x$

and finally,
$x.x^{-1} = x^{-1}.x = 1$ if $x \neq 0$.
Objects satisfying the above properties are called "Fields". ($\mathbb{Q}$ is a field.)
We define *division* of rationals x and $y \neq 0$ as $x \div y = xy^{-1}$.
We say that x is positive if $x = p/q$ for two positive integers p and $q \neq 0$. x is negative if $x = -y$ for some positive rational y. Also, x is said to be $\geq y$ if $x = y + z$ for some positive rational and $x > y$ if $x \geq y$ and $x \neq y$. Likewise for $\leq$.
We have the following properties of ordering :

1. $x = 0$ xor x is positive xor x is negative.
2. For every x and y, $x = y$ xor $x > y$ xor $x < y$.

3. If $x < y$ then $y > x$.

4. $x < y, y < z \Rightarrow x < z$.

5. $x < y \Rightarrow x + z < y + z$.

6. If $x < y$ and z is positive, then, $xz < yz$.

The above properties make $\mathbb{Q}$ into an ordered field. Read about the absolute value function $|x|$ and exponentiation x^n (where n is an integer such that if $x = 0$ then $n > 0$) from Terence Tao's book. All of these things have the same flavour.
While we are on the topic, let us (once and for all) define these terms - Ordered set, Well-ordering property, Field, Ordered field.

1. An order (written as $\leq$) on a set S is a binary relation satisfying

   (a) For every $x, y \in S$ we have either $x \leq y$ or $y \leq x$.

   (b) If $x \leq y$ and $y \leq x$ then $x = y$.

   (c) If $x \leq y$, $y \leq z$ then $x \leq z$.

   This is also called a total order sometimes. (As opposed to a partial order where the first axiom is dropped. For example, it is not true that if you take two subsets of a set, one of them is contained in the other.) Examples :

   (a) The usual order on rational numbers makes it into an ordered set.

   (b) Suppose X is a countable collection of subsets S_i of a set A satisfying $0 \subset S_1 \subset S_2 \ldots$, then define an order $<$ on X as : $S_i < S_j$ if and only if $S_i \subset S_j$. Clearly this satisfies the axioms of ordering. (This by the way is called a "chain" of subsets.)

2. The well-ordering property is a property of a given order that *every* non-empty subset has a least element. Of course this is not the case with rational numbers equipped with the usual order. But the well-ordering theorem states that the axiom of choice is equivalent to being able to choose a well order on *every* set.

3. Field : A field is a set S containing two *distinct* special elements 0, 1, and equipped with two binary operations $+$ and $\times$ satisfying the following properties.

   (a) Addition satisfies closure (i.e. if you add two elements you get an element of the field) commutativity, associativity, existence of additive inverses ($x + (-x) = 0$), $x + 0 = 0 + x = x$ (0 is the additive identity).

   (b) Multiplication satisfies closure (if you multiply elements you get an element of the field), commutativity, associativity, distributivity, 1 is the multiplicative identity, and every non-zero x has a reciprocal.

   Examples of fields :

   (a) The rationals form a field.

   (b) As we shall see later, reals and complex numbers form fields.

(c) You can define fields containing finite number of elements (that you will study in your algebra class). I shan't define them.

4. Ordered field. An ordered field is a field $(S, +, \times, 0, 1)$ equipped with an order $\leq$ such that the field properties are compatible with the order, i.e.,

   (a) If $y \leq z$ then $x + y \leq x + z$.

   (b) If $x \geq 0$ and $y \geq 0$ then $xy \geq 0$.

   An ordered field satisfies all the usual properties like if $x \geq 0$ then $-x \leq 0$ if $x \geq 0$ then $x^2 \geq 0$, if $0 < x \leq y$ then $\frac{1}{y} \leq \frac{1}{x}$, etc.