Notes for 5th Jan (Thursday)

1 Recap

1. "Defined" sets and subsets. Stated the Zermelo-Fraenkel axioms of set theory with the axiom of choice. (ZFC.)

2. Stated Peano's axioms for the set of natural numbers (which is a subset of the infinite set in ZFC).

2 Natural numbers (cont'd....)

One can then give recursive definitions for addition, ordering, multiplication, and exponentiation.
Addition : $0 + m = m$. If $n + m = k$ then $(n + +) + m = k + +$. From this we can prove the usual properties, i.e., commutativity, associativity, and the cancellation law of addition. We prove commutativity here just to show the flavour of the proofs.

Theorem 1. *m+n=n+m for all natural numbers n and m.*

Proof. We use induction on n. For $n = 0$, $0 + m = m$ by definition. Let us first prove that $m + 0 = m$ for every natural number m. This is a lemma.

Lemma 2.1. *m+0=m*

Proof. For 0, 0+0 = 0 by definition. If this is true for m, then $(m{+}{+}){+}0 = (m{+}0){+}{+} = m + +$ by definition and induction hypothesis. Therefore this lemma is true by the principle of induction. □

If commutativity is true for n (with adding every natural number m) then we need to prove that $m + (n + +) = (n + +) + m$, i.e., that $m + (n + +) = (n + m) + +$, i.e. by induction hypothesis that $m + (n + +) = (m + n) + +$. We shall induct on m now.
For $m = 0$, this is true by the lemma. If true for m, then $(m{+}{+}){+}(n{+}{+})$ is by definition $(m{+}(n{+}{+})){+}{+}$. By induction hypothesis indeed the last expression is $((m{+}n){+}{+}){+}{+}$. But $((m + +) + n) + + = ((m + n) + +) + +$ by definition. Thus we are done. □

We still need to see how positivity and addition are related. A natural n is called positive if $n \neq 0$.

1. If a is positive and b is a natural number, then $a+b$ is positive.
   Indeed for $b=0$, $a+0=0+a=a$ and therefore positive. If true for b, then $a+(b++)=(a+b)++$ and by Peano's axioms this cannot be 0.

2. If $a+b=0$ then $a=0$ and $b=0$. This is a corollary of the previous proposition.

3. If a is positive, then there exists exactly one natural b so that $b++=a$. The proof is similar to the ones above.

Multiplication : $0\times m=0$. If $n\times m=k$ then $(n++)\times m=k+m$. One can as before prove all the usual properties of natural numbers (commutativity, associativity, distributivity, no zero divisors, and cancellation).
Exponentiation : $m^0=1$ for $m>0$. If $m^n=k$ then $m^{n++}=k\times m$.
Ordering : We say that $n\geq m$ if $n=m+a$ for some natural number a. If $n\neq m$ then we say that $n>m$.

1. Ordering is reflexive, transitive, anti-symmetric ($a\geq b$, $b\geq a$ implies that $a=b$).

2. Addition preserves order ($a\geq b$ implies that $a+c\geq b+c$).

3. $a<b$ iff $a++\leq b$.

4. $a<b$ iff $b=a+d$ for positive d.

5. Trichotomy : For any two a,b, either $a<b$, $a=b$, or $a>b$.

6. If $a>b$, then $ac>bc$ if c is positive.

7. Euclidean algorithm : If a is positive and $a\leq b$, then $b=na+r$ for a unique n and $0\leq r<a$.

The properties of ordering can be used to prove the strong principle of induction.

3 Cardinality

The cardinality of a finite set A is intuitively speaking, the number of elements of A. For infinite sets, obviously this notion does not make sense. However, one can still ask if two infinities are the same (!) in the following manner.
Two sets A and B are said to have the *same* cardinality if there exists a bijection from A to B.
We define a set to be finite and having cardinality n if it is in bijection with $\{1\leq i\leq n\}$. You might think that it is circular because at the very foundation of mathematics we assumed the notions of "finite" (as in finite alphabet for instance). However we are talking about "finite sets" here (treat it as a single noun if it makes more sense to you). This is the only way to define the notion.
One can prove that set of natural numbers is infinite. Indeed if it is in bijection with $\{1\leq i\leq n\}$ then natural numbers would have to be bounded (because if not, then there are more than n natural numbers and finite cardinality can be easily proven to be

unique). But this is a contradiction by Peano's axiom ("no ceiling" axiom).
However infinite sets are weird. Define a number to be even if $n = 2k$ and odd if $n = 2k + 1$.
Firstly, every number is definitely either even or odd but not both. This follows from the Euclidean algorithm. Also, the k is unique given n.
Secondly, the set of even numbers is in bijection with natural numbers despite being contained in it. Indeed, map an even number $n = 2k$ to the corresponding k. This is a well-defined function. It is an injection because if $2k = 2l$ then by the cancellation law $k = l$. It is a surjection too. Likewise, positive naturals have the same cardinality as naturals. Any set that has the cardinality of naturals is said to be countably infinite.

Before we proceed further, a sequence of elements of X is simply a function $f : \mathbb{N}_+ \to X$. It is informally written as $x_1, x_2, \ldots$. Suppose $f : \mathbb{N}_+ \to \mathbb{N}_+$ is any ordering preserving $1-1$ map, then $x_{f(1)}, x_{f(2)}, \ldots$ is called a subsequence. The notion of set of all sequences is a perfectly well-defined set in ZFC because it is a subset of the power set of $N \times X$.

Countable sets represent the "smallest" infinity, i.e.,

Theorem 2. *Every infinite subset A of a countable set X is countable.*

Proof. Without loss of generality we may assume that $X = \mathbb{N}$ (why?). The bijection between $\mathbb{N}$ and A is simply k goes to the $(k+1)^{th}$ smallest element of A. But to make sense of this, we need to prove that this definition makes sense.
Firstly, natural numbers are well-ordered, i.e., every non-empty subset has a smallest element. (By smallest I mean an element x such that every other element is $\geq x$.) Indeed, consider a subset A. Since it is non-empty, there exists a natural number $n \in A$. Consider the subset B_n of $\mathbb{N}$ given by $\{x \in A | x \leq n\}$. Let's prove that this has a smallest element by induction. If $n = 0$, we are done. If this is true for n, then $B_{n++} = B_n \cup n++$ (by the trichotomy law). If B_n is non-empty, we are done by the induction hypothesis (because $n++ > n$). If B_n is empty, then the smallest element is $n++$.
Secondly, the k^{th} smallest element of A is defined as follows :
The 1^{st} smallest element is the smallest element of A.
If the first k smallest elements have been found and put in a set G_k, then the $(k+1)^{th}$ smallest element is the smallest element of $A - G_k$. □

Lots of sets are countable :

Theorem 3. $\mathbb{N} \times \mathbb{N}$ *is countable.*

Proof. Firstly, $2^{n_1}3^{n_2}$ represent different numbers for different values of n_1 and n_2. Indeed, if $2^a 3^b = 2^c 3^d$ and without loss of generality $a \geq c$ and $b \leq d$ then $a = c + x$, $d = b + y$. In other words, $2^{c+x}3^b = 2^c 3^{b+y}$. We haven't proven properties of exponentiation yet (and we actually will not prove them because the proofs are very similar and annoying). But assuming those we can see that $2^x = 3^y$. This we claim is impossible unless $x = y = 0$:
2^x is even for any $x \neq 0$ (Induction).
3^y is odd for any y (Induction).
This means that the map $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $(a, b) \to 2^a 3^b$ is injective. Therefore by the previous theorem we are done. □

As a consequence we have the following useful result. ("Countable unions of countable sets is countable.")

Theorem 4. *If E_i where $i \in \mathbb{N}$ are countable sets, then $U = \cup_i E_i$ is countable.*

Proof. Let $f_i : \mathbb{N} \to E_i$ be bijections. Then consider the map $g : \mathbb{N} \times \mathbb{N} \to U$ given by $g(i, j) = f_i(j)$. This is clearly a surjection. Using the axiom of choice to choose unique pre-images, we get an injection from U to $\mathbb{N} \times \mathbb{N}$. Since an infinite subset of a countable set is countable, we are done. Surely, there must be a way to do this without the axiom of choice..... $\square$