LECTURE 12: SUMMARY

The goal of today's lecture was to prove comparability of infinite cardinals: given any two infinite sets, one of them must inject into the other. Before we can prove this, we need to discuss a bizarre result called the Well-Ordering Theorem, discovered a century ago by the German mathematician Ernst Zermelo.

The sets of numbers we're familiar with ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$) are different from other sets because they are ordered: any two (or even 200) given numbers can be arranged in increasing order, for example. But is this a special feature of numbers? Certainly not: a collection of stuffed animals can also be put in order. Even though it's clear intuitively what it means for an arbitrary set to be ordered, writing down a precise criterion is not so easy. After thinking about it for a while, people figured out that there are three key properties a binary relation $\prec$ on a set A should satisfy which makes A an ordered set:

(1) Antisymmetry: $a \not\prec a$ for any $a \in A$;
(2) Transitivity: if $a \prec b$ and $b \prec c$, then $a \prec c$; and
(3) Comparability: for any $a, b \in A$, we have either $a = b$, $a \prec b$, or $b \prec a$.

It's easy to check that $(\mathbb{N}, <)$ is an ordered set, where $<$ denotes the usual ordering 'less than'. Of course, the same is true of $(\mathbb{R}, <)$. One difference we noticed right away is that in $(\mathbb{N}, <)$, every element (except for 1) has an immediate predecessor, which is not the case in $(\mathbb{R}, <)$. Is this a property of $\mathbb{N}$, or of the ordering $<$ we chose? Turns out, it's the ordering. For example, consider the following ordering of $\mathbb{N}$:

$$1, 3, 5, 7, \ldots, 2, 4, 6, 8, \ldots$$

Formally, we are defining a relation $\prec$ on $\mathbb{N}$ as follows:

(*) $$a \prec b \quad \text{iff} \quad \begin{cases} a < b \text{ and } a, b \text{ have the same parity; or} \\ a \text{ is odd and } b \text{ is even.} \end{cases}$$

It is straightforward to check that $\prec$ is an ordering on $\mathbb{N}$. However, the natural number 2 has no immediate predecessor in this ordering!

We also saw an important non-example: the power set $\mathcal{P}(\{1, 2, 3\})$ is not ordered by the subset relation $\subset$. The first two properties of being an order are satisfied, but the third fails: the two elements $\{1, 3\}$ and $\{2\}$ are not comparable, for example.

In addition to the "immediate predecessor" property, $(\mathbb{N}, <)$ has another remarkable feature: the well-ordering principle. Namely, every nonempty subset of $\mathbb{N}$ has a least element. More generally, given an ordered set $(A, \prec)$, we'll say it's well-ordered iff every nonempty subset of A has a least element. In other words, given any nonempty $B \subseteq A$, there must exist $b \in B$ such that $b \prec x$ for all $x \in B - \{b\}$.

Date: February 14th, 2013.

We already know that $(\mathbb{N}, <)$ is well-ordered, and it's not too hard to check that $(\mathbb{N}, \prec)$ is as well, where $\prec$ is the order defined in (*) above. On the other hand, $(\mathbb{Z}, <)$ is not well-ordered: the entire set $\mathbb{Z}$ has no least element. However, by ordering $\mathbb{Z}$ differently, we can make it well-ordered; Victor proposed the ordering

$$0, -1, 1, -2, 2, \cdots$$

For $\mathbb{R}$, however, the situation is more complicated. Clearly it is not well-ordered under the standard order $<$, since the open interval $(0, 1)$ has no least element. Is there some ordering which does make $\mathbb{R}$ well-ordered? Some playing around should convince you that the answer is not obvious one way or the other. The following theorem answers the question in the affirmative:

Well-Ordering Theorem (Zermelo, 1904)**.** *Every infinite set can be well-ordered.*

Despite the fact that this theorem guarantees its existence, no one has been able to describe a well-ordering of $\mathbb{R}$. This made people very suspicious of Zermelo's theorem, but the proof is not particularly complicated. It eventually became clear that the only potentially fishy step was the following assumption:

Axiom of Choice. *Given nonempty sets A_α, there exists a set A which intersects each A_α nontrivially (i.e. $A \cap A_\alpha \neq \emptyset$ for every α).*

This statement seems completely obvious,[1] and it is provably true if we're only dealing with finitely many sets A_α. For infinitely many sets, in particular for uncountably many, it is a much less obvious statement. The Axiom of Choice is implicitly used in the proofs of many theorems; for example, we made use of it in our proof that $A \hookrightarrow B$ iff $B \twoheadrightarrow A$. (Actually, AC is only used in one of the directions; in the other direction, one only needs to make a single choice, not multiple choices. Which direction requires AC?) The natural question is: is the AC really so weird? OK, so it implies the Well-Ordering Theorem, which is counterintuitive. So what? The Axiom of Choice actually implies all sorts of theorems; some of them are desirable (e.g. every vector space has a basis), while some are fairly alien (e.g. the Banach-Tarski paradox). As we discussed in lecture, it turns out (again due to work of Gödel and, subsequently, Cohen) that AC is independent of the ZF axioms of set theory. Thus, people frequently talk about ZFC: the Zermelo-Fraenkel Axioms + Axiom of Choice.

Unfortunately, we don't have time to prove that AC implies the Well-Ordering Theorem. (A bit of thought shows that the Well-Ordering Theorem implies AC, so the two statements are actually equivalent.) Instead, we'll assume the Well-Ordering theorem and use it to prove that any two infinite cardinals are comparable. The strategy will be very similar to our proof from last lecture that $\aleph_0$ is the smallest infinite cardinal.

Theorem 1. *Given two infinite sets A and B. If $B \not\precsim A$, then $A \precsim B$.*

Proof. Suppose $B \not\precsim A$; in other words, there are no injections from B into A. We wish to find an injection from A into B. To do this, we recursively define a function $h : A \to B$ as follows. First, set

$$h(\text{Least}[A]) := \text{Least}[B]$$

[1] The Axiom of Choice is equivalent to a statement which sounds even more obvious: the Cartesian product of any family of nonempty sets is nonempty.

(We are assuming the Well-Ordering theorem, so it makes sense to talk about the least elements of A and B.) Next, we send the second-smallest element of A to the second-smallest element of B, the third-smallest to the third-smallest, etc. To write this down formally: for any $\alpha \in A$, we recursively define

$$h(\alpha) := \text{Least}[B - h(A_{<\alpha})].$$

I claim that $h : A \hookrightarrow B$. Why? Suppose α and β are two distinct elements of A. Since A is well-ordered (and, in particular, ordered), we must have either $\alpha < \beta$ or $\beta < \alpha$. WLOG, let's say that $\alpha < \beta$. It follows that

$$h(\alpha) \notin B - h(A_{<\beta})$$

On the other hand,

$$h(\beta) \in B - h(A_{<\beta})$$

by definition (it's the smallest element of this set!). It follows that whenever $\alpha \neq \beta$, we have $h(\alpha) \neq h(\beta)$; so h is an injection.

But there's something fishy about this argument, as Kelvin pointed out. Nowhere have we used the hypothesis that $B \not\preceq A$! In fact, as things stand, the same argument seems to prove the existence of an injection from $\mathbb{R}$ into $\mathbb{N}$, contradicting a lot of the theory we've been developing. So what's wrong?

Jerry came to the rescue by observing that we were pretty cavalier with our application of the Well-Ordering theorem; the least element of a set is defined only for *nonempty* sets. Thus, for our recursive definition of h to make sense, we need to know that $B - h(A_{<\alpha}) \neq \emptyset$ for all $\alpha \in A$. And now our hypothesis saves the day: there are no injections from B into A, which means (by an earlier theorem) that there are no surjections from A onto B. But *this* means that $h(A_{<\alpha})$ cannot possibly be all of B, or else h itself would be a surjection from A onto B! Thus, our hypothesis implies that $B - h(A_{<\alpha}) \neq \emptyset$ for all $\alpha \in A$, and so our recursive definition of h makes sense. This concludes the proof. $\square$