LECTURE 5

Last lecture we introduced Axiom III, which states the following:

Axiom III: if $S \subset \mathbb{R}$ is non-empty and bounded above, then S has a least upper bound.

We saw that Axiom III$'$ implies Axiom III. In fact the converse is also true; hence the two axioms are logically equivalent, i.e. one is true if and only if the other is true.

Axiom III is sometimes called the *least upper bound axiom* or the *axiom of completeness*. It is the axiom most commonly assumed over Axiom III$'$ and related variants. For this reason it is the axiom that we will assume.

The set of real numbers

Recall where we are at: we have stated Axioms I, II and III and derived some simple consequences of them. However, we need to know that there is answer to the following question: is there a set $\mathbb{R}$ which actually satisfies these three axioms? The following theorem gives the best possible answer to this question.

Theorem 1.5: there is a 'unique' set $\mathbb{R}$ satisfying Axioms I, II, and III.

Here 'unique' has a certain technical sense: more precisely what the Theorem is asserting is that there is an ordered field (i.e. a set satisfying Axioms I and II) which also satisfies Axiom III, and moreover this ordered field is *unique up to isomorphism* of ordered fields. Thus the real numbers are uniquely determined by the three axioms — this is the sense in which the theorem gives the best possible answer to the question above.

Here are some (non examinable) comments on the proof of Theorem 1.5. Firstly, we won't prove this theorem — it will take too long. The actual proof consists of two parts: first you have to construct the set $\mathbb{R}$, then you have to show that the set is unique in the technical sense alluded to above. There are several different ways of constructing the set $\mathbb{R}$. In one construction, the real numbers are constructed in terms of what are known as *Dedekind cuts*, after Richard Dedekind.

A Dedekind cut is a subset A of $\mathbb{Q}$ with the following properties: (a) $A \neq \emptyset$ and $A \neq \mathbb{Q}$, (b) if $p \in A$, $q \in \mathbb{Q}$ and $q < p$ then $q \in A$, (c) if $p \in A$ then $p < r$ for some $r \in A$. For example the set

$$A = \{\, q \in \mathbb{Q} \mid q^2 < 2 \text{ or } q < 0 \,\}$$

satisfies these requirements (this is not completely obvious — have a look at the comments at the end of Lecture 3). A real number is then defined to be a Dedekind cut. One then has to prove that the set of real numbers so obtained satisfies Axioms I, II and III. Thus operations of addition and multiplication need to be defined, and an order relation. Verifying that all of the axioms are satisfied is somewhat time consuming. We will take it on faith that all this can be done.

So we finally have our set of real numbers. Probably you will feel that not much has changed, perhaps the only new insight into the nature of the real numbers that you have come away with is the fact that they satisfy Axiom III. We will proceed on the basis that we can manipulate real numbers the way that we have been used to doing, but we will not take anything for granted about the set of real numbers (therefore we will sometimes prove some results which might seem very obvious).

Greatest lower bounds

One thing you might have been wondering in the discussion of upper bounds and least upper bounds in the previous lecture is 'What happened to lower bounds?'. We began by defining upper and lower bounds, but then forsook the latter in defining least upper bounds. It is perhaps a little strange that we went to the trouble of defining what is meant by a least upper bound, and then to the trouble of mandating that every non-empty bounded above set has a least upper bound in Axiom III. We might wonder why we did not define the notion of greatest lower bound, and why we didn't mandate the existence of greatest lower bounds for suitable subsets of $\mathbb{R}$. In fact, we will soon see that greatest lower bounds come for free with Axiom III.

We first define what is meant by a greatest lower bound.

Definition: Let $S \subset \mathbb{R}$ be a non-empty set which is bounded below. We say that a nunber $b \in \mathbb{R}$ is a *greatest lower bound* or *infimum* for S if (a) b is a lower bound for S and (b) if b' is another lower bound for S then $b' \leq b$.

Put another way,

$$b = \max \{ x \in \mathbb{R} \mid x \text{ is a lower bound for } S \} .$$

If such a b exists, it is denoted $\inf S$. Just as for least upper bounds, a greatest lower bound (if it exists) is unique.

Theorem 1.6: A non-empty bounded below set $S \subset \mathbb{R}$ has a greatest lower bound.

Proof: Let $L = \{ x \in \mathbb{R} \mid \ x \text{ is a lower bound for } S \}$. Then L is non-empty by the assumption that S is bounded below. Let $s \in S$. Then if $x \in L$ then $x \leq s$ since x is a lower bound for S; hence we can make the key observation that $x \leq s$ for all $x \in S$. Thus s is an upper bound for L and hence L is bounded above. Since L is non-empty and bounded above, it has a least upper bound by Axiom III. Let $b = \sup(L)$. We have observed above that *any* $s \in S$ is an upper bound for L; hence $b \leq s$ for all $s \in S$. Therefore b is a lower bound for S, i.e. $b \in L$. Therefore $b = \max(L)$, since $b \in L$ and $b = \sup(L)$. In other words, $b = \inf(L)$. ■

The next result that we will prove might seem blindingly obvious, but we are proceeding on the basis of not taking anything for granted about $\mathbb{R}$; therefore we need to supply a proof.

Lemma 1.7: The set of natural numbers $\mathbb{N}$ is not bounded above.

Proof: Suppose that $\mathbb{N}$ is bounded above. Then by Axiom III, $\mathbb{N}$ has a least upper bound since $\mathbb{N}$ is non-empty and we are supposing that it is bounded above. Let $b = \sup(\mathbb{N})$. Let $n \in \mathbb{N}$. Then $n+1 \in \mathbb{N}$ and so $n+1 \leq b$ since b is an upper bound for $\mathbb{N}$. But then $n \leq b-1$. This is true for all $n \in \mathbb{N}$. Hence $b-1$ is an upper bound for $\mathbb{N}$. This is a contradiction since $b-1 < b$, and b was supposed to be the least upper bound for $\mathbb{N}$. Therefore $\mathbb{N}$ is not bounded above. ■

The main reason for proving Lemma 1.7 is that it lets us deduce the following crucial property of the real numbers, the so-called *Archimedean Property* of $\mathbb{R}$. We'll use this property lots of times throughout the course.

Corollary 1.8: (The Archimedean Property of $\mathbb{R}$) If $\epsilon > 0$ is a real number then there exists $n \in \mathbb{N}$ such that $1/n < \epsilon$.

Proof: We will give a proof by contradiction. Let $\epsilon > 0$. Suppose that $\epsilon \leq 1/n$ for all $n \in \mathbb{N}$. Then, since $\epsilon > 0$ and $n > 0$ for all $n \in \mathbb{N}$, we may re-arrange this inequality to deduce that $n \leq 1/\epsilon$ for all $n \in \mathbb{N}$. But this means that $1/\epsilon$ is an upper bound for $\mathbb{N}$, which contradicts the conclusion of Lemma 1.7 above, i.e. it contradicts the fact that $\mathbb{N}$ is not bounded above. Therefore our assumption that $\epsilon \leq 1/n$ for all $n \in \mathbb{N}$ is false and hence there exists $n \in \mathbb{N}$ such that $1/n < \epsilon$. ■

Theorem 1.9: There is a postive real number x such that $x^2 = 2$. This real number is denoted $\sqrt{2}$.

Proof: We will show that $\sqrt{2} = \sup(S)$, where $S = \{\, x \in \mathbb{R} \mid \ x \geq 1 \text{ and } x^2 < 2 \,\}$. Then $S \neq \emptyset$ (for instance $1 \in S$) and S is bounded above (for instance 2 is an upper bound for S). Therefore, by Axiom III, S has a least upper bound. Let $b = \sup(S)$.

We must have $b > 1$ (for instance $1.1 \in S$ since $(1.1)^2 = 1.21$, therefore $b \geq 1.21$). Since b is the least upper bound for S, the number $b - 1/n$ cannot be an upper bound for S for any $n \in \mathbb{N}$ (otherwise $b - 1/n$ would be an upper bound for S smaller than the least upper bound).

Let $n \in \mathbb{N}$. Choose $s \in S$ such that $b - 1/n < s$. Since $b > 1$, $b - 1/n > 0$. Therefore,

$$\begin{aligned}
&0 < (b - 1/n)^2 < s^2 < 2 \quad \text{since } s \in S \\
\Longrightarrow\ & b^2 - 2b/n + 1/n^2 < 2 \quad \text{by expanding } (b - 1/n)^2 \\
\Longrightarrow\ & b^2 - 2b/n < 2 \quad \text{since } b^2 - 2b/n < b^2 - 2b/n + 1/n^2 \\
\Longrightarrow\ & b^2 - 2 < 2b/n \\
\Longrightarrow\ & (b^2 - 2)/2b < 1/n \quad \text{since } 2b > 0
\end{aligned}$$

Hence $(b^2 - 2)/2b < 1/n$ for all $n \in \mathbb{N}$. Therefore, by the Archimedean Property of $\mathbb{R}$, $(b^2 - 2)/2b \leq 0$. Since $b > 0$ this implies that $b^2 - 2 \leq 0$, i.e. $b^2 \leq 2$.

We want to prove that $b^2 = 2$. Suppose instead that $b^2 < 2$. Then

$$(b + 1/n)^2 = b^2 + 2b/n + 1/n^2 \leq b^2 + 2b/n + 1/n$$

since $1/n^2 \leq 1/n$ if $n \in \mathbb{N}$ (this is because $n \leq n^2$ if $n \in \mathbb{N}$). Hence

$$(b + 1/n)^2 \leq b^2 + (2b + 1)/n.$$

The idea now is that by making n large enough, we can ensure that $b^2 + (2b + 1)/n < 2$ (we'll explain below why this leads to a contradiction). We are assuming that $b^2 < 2$ and hence $2 - b^2 > 0$. By the Archimedean Property of $\mathbb{R}$, there is an $n \in \mathbb{N}$ such that $(2b+1)/n < 2 - b^2$, since there is an $n \in \mathbb{N}$ such that $1/n < (2 - b^2)/(2b+1)$ (notice that the right hand side in this inequality is positive, since $2b + 1 > 0$).

Choose such an $n \in \mathbb{N}$. Then

$$(b + 1/n)^2 \leq b^2 + (2b + 1)/n < b^2 + 2 - b^2 = 2.$$

But this implies that $b + 1/n \in S$ (since $b + 1/n \geq 1$ and $(b + 1/n)^2 < 2$ by the above). This is a contradiction, since b is an upper bound for S and $b < b + 1/n$.

Therefore our assumption that $b^2 < 2$ leads to a contradiction. Therefore $b^2 = 2$. ■

We could adapt this proof to show that $\sqrt{3} \in \mathbb{R}$ or more generally that $\sqrt{n} \in \mathbb{R}$ for any $n \in \mathbb{N}$. With a little bit more work (using the binomial theorem to expand $(b - 1/n)^m$ etc), we could show that $\sqrt[m]{n} \in \mathbb{R}$ for any $m, n \in \mathbb{N}$. We'll take it as given that we could do this, rather than actually doing it ourselves.

Note that another strategy to show that $\sqrt{2} \in \mathbb{R}$ would be to use the Intermediate Value Theorem (once we had discussed functions, continuous functions and proven the Intermediate Value Theorem of course). We could consider the function $f\colon [0, 2] \to \mathbb{R}$ defined by $f(x) = x^2 - 2$. It satisfies $f(0) < 0$ and $f(2) > 0$, hence there exists an $x \in \mathbb{R}$ such that $0 < x < 2$ and $f(x) = 0$, i.e. $x^2 = 2$. Our proof above that $\sqrt{2} \in \mathbb{R}$ used crucially the least upper bound property of $\mathbb{R}$ (Axiom III); it turns out that in fact the Intermediate Value property of continuous functions is equivalent to Axiom III.