Chapter 1: The Real Numbers

The title of this course really should be "Calculus I Done Correctly." The idea is that we will present the results that you may have been shown in Calculus I — and you may even have been shown proofs of them — but as a student, my reaction was, "Okay, all these look like true statements, but why is this list of true statements considered a proof of that true statement? The latter doesn't seem any more 'basic' or 'axiomatic' than the former. So why is it a proof?" Our objective is at least to list <u>first</u> the statements that we take as axioms (i.e., assume to be true) and then to show how the statements in calculus follow from them. Anyone who wants to prove anything must start with some assumptions. If you do not find these assumptions satisfying, you are welcome to pick your own set of axioms (and perhaps try to prove our "axioms" on the basis of yours).

Let's begin by listing my (Lantz's) notations that I will use on the board. If <u>any</u> of them are not clear, please feel free to ask for more explanation.

//	end of proof (QED)
$-\!\!\!\times\!\!\!-$	contradiction
BWOC	by way of contradiction
WLOG	without loss of generality
$\mathbb{N}$	the set of natural numbers $\{1, 2, 3 \ldots\}$
($\mathbb{Z}$	the set of integers $\{0, 1, -1, 2, -2, 3, -3, \ldots\}$)
$\mathbb{Q}$	the set of rational numbers (quotients of two integers)
$\mathbb{R}$	the set of real numbers
($\mathbb{C}$	the set of complex numbers)
$\forall$	for all (for every)
$\exists$	there exists (there is)
s.t.	such that
$\emptyset$	the empty set
$A \backslash B$	the set of elements of A that are not in B

The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are "fields," i.e., within each of them it is possible to add, subtract, multiply and divide (except by 0). (Some subtractions are impossible in $\mathbb{N}$; some divisions are impossible in $\mathbb{Z}$; so these are not fields.) The "algebraic numbers" $\mathbb{A}$, consisting of all the complex numbers that are roots of polynomials with integer coefficients, is also a field.

The concept of "field" is part of algebra; it is defined in Math 320. For real analysis we will need an additional property beyond the operations of arithmetic: that of "order." The rationals and the reals are "ordered fields", i.e., they have a working sense of "greater than" and "less than" between any pair of their elements. (The complex field does <u>not</u> have that, because squares have to be greater than 0, but both 1 and -1 are squares in $\mathbb{C}$.) The "algebraic reals" $\mathbb{A} \cap \mathbb{R}$ is an ordered field, as is the "surd field" $\mathbb{S}$ that we will talk about in geometry. (It's the smallest field where all the positive elements have square roots.)

One way that we could define an ordered field F is to say that it has a subset P (the "positive" elements) that is closed under addition and multiplication and for which F is the disjoint union of P, the set of additive inverses of P, and $\{0\}$. Then we would define the binary relation $<$ and the unary relation $|\cdot|$ (absolute value) on F by: $a < b$ means $b - a \in P$, and $|a|$ means a if $a \in P$ or $a = 0$, and $-a$ otherwise. But all this sounds too much like Math 320, and all we really need to know about $<$ and $|\cdot|$ is contained in the following list of axioms (which we could prove on the basis of this definition, but we won't):

1. Inequalities: For numbers a, b, c:
   - If $a < b$, then $a + c < b + c$ and $a - c < b - c$.
   - If $a < b$ and $c > 0$, then $ac < bc$.
   - If $a < b$ and $c < 0$, then $ac > bc$.
   - If $0 < a < b$, then $0 < (1/b) < (1/a)$.
2. Absolute values: For numbers a, b, c:
   - $|ab| = |a||b|$
   - $|a + b| \leq |a| + |b|$ (the "Triangle Inequality")
   - $|a - b| = |b - a|$
   - (from the Triangle Inequality) $|a - b| + |b - c| \geq |a - c|$.

   Note: The (unsigned) distance between a, b on the real line is $|a - b|$.

Proposition. $|a - b| \geq ||a| - |b||$.

Proof. $|a-b|+|b| \geq |a-b+b| = |a|$, the inequality by the Triangle Inequality; so $|a-b| \geq |a|-|b|$. And $|a - b| + |a| = |b - a| + |a| \geq |b - a + a| = |b|$, so again $|a - b| \geq |b| - |a| = -(|a| - |b|)$. So $|a - b| \geq ||a| - |b||$. □

Or, just to give an example of a proof using WLOG:

Proof. Because neither side changes value if we reverse a and b, WLOG we may assume that $|a| \geq |b|$, so that $||a| - |b|| = |a| - |b|$. Then $|a - b| + |b| \geq |a - b + b| = |a|$, the inequality by the Triangle Inequality; so $|a - b| \geq |a| - |b| = ||a| - |b||$. □

Note: If $a < b < c$, then $|b| \leq \max\{|a|, |c|\}$.

What is special about $\mathbb{R}$ is the fact that it is "complete." To make sense of completeness, we need the following definitions:

Definition. (1) Let A be a set of numbers. A number b is an *upper bound* of A if $a \leq b$ for every a in A. If b^* is an upper bound of A and $b^* \leq b$ for every upper bound b of A, then b^* is the *least upper bound* (lub) or *supremum* (sup) of A. [The use of the word "the" here assumes that a set has only one sup; this can and should be proved.] If b^* is an element of A, as well as being the lub of A, then b^* is called the *maximum* (max) of A.

(2) Let A be a set of numbers. A number b is a *lower bound* of A if $a \geq b$ for every a in A. If b^* is a lower bound of A and $b^* \geq b$ for every upper bound b of A, then b^* is the *greatest lower bound* (glb) or *infimum* (inf) of A. If b^* is an element of A, as well as being the glb of A, then b^* is called the *minimum* (min) of A.

Example. (1) If $P = \{3, 3.1, 3.14, 3.141, 3.1415, 3.14159, \ldots\}$, then $\text{lub}(P) = \pi$.

(2) $A = \{a \in \mathbb{Q} : a^2 \leq 2\} = \{a \in \mathbb{Q} : -\sqrt{2} \leq a \leq \sqrt{2}\}$ has upper and lower bounds in $\mathbb{Q}$: -3 is a lower bound and 3 is an upper bound. But A has no lub or glb in $\mathbb{Q}$. In $\mathbb{R}$, $\text{lub}(A) = \sqrt{2}$ and $\text{glb}(A) = -\sqrt{2}$. And A has no maximum or minimum.

(3) The half-open interval $B = [2, 3)$ has $\inf(B) = \min(B) = 2$ and $\sup(B) = 3$, but B has no maximum.

(4) The infinite interval $C = \{x \in \mathbb{R} : x > 5\}$ has no upper bound and hence no sup, We might write $\sup(C) = \infty$ just as notation, and write $C = (5, \infty)$. Similarly, $\inf((-\infty, 3)) = -\infty$. But ∞ and $-\infty$ are just symbols, not real numbers and not elements of the field $\mathbb{R}$ — we won't do arithmetic with them.

With this notation, $\mathrm{lub}(\emptyset) = -\infty$ and $\mathrm{glb}(\emptyset) = \infty$.

Axiom. (Completeness) *For any subset A of $\mathbb{R}$, if A has a (finite) upper bound, then A has a sup in $\mathbb{R}$.*

Corollary. *For any subset B of $\mathbb{R}$, if B has a finite lower bound, then B has an inf in $\mathbb{R}$.*

You are challenged to write a proof for the corollary to the completeness axiom — it is clearly just the mirror image of the axiom. We'll go on to collect some consequences of completeness.

The logical approach that we are taking in this course is to start with the reals, assuming that they are complete ordered field. That means we need to explain how we identify the important subsets. Once we have identified the natural numbers $\mathbb{N}$, it is pretty clear how we get the integers $\mathbb{Z}$ (namely, $\mathbb{N}$, its negatives and 0), and the rationals $\mathbb{Q}$ (the quotients of two integers, with 0 not allowed in the denominator). So how do we identify $\mathbb{N}$? Well, as a field, $\mathbb{R}$ has a multiplicative identity 1. Then $\mathbb{N}$ is the sum of any number of copies of 1. So the defining property of $\mathbb{N}$ is sometimes called the induction principle: "Let B be a set of numbers. If $1 \in B$ and if the implication $n \in B \implies n + 1 \in B$ holds, then $\mathbb{N} \subseteq B$." A consequence is that $\mathbb{N}$ is "well-ordered", i.e., every nonempty subset of $\mathbb{N}$ has a smallest element. (Notice that this is not true of the positive rationals or the positive reals, or the set of even integers, if we include negatives.)

Proof. (Of the well-ordering of $\mathbb{N}$) Let $A \subseteq \mathbb{N}$, and assume that A has no smallest element; we will show that $A = \emptyset$, by showing that the set B of all n's in $\mathbb{N}$ for which <u>none</u> of $1, 2, 3, \ldots, n$ are in A is equal to $\mathbb{N}$. (We have to be a little fussy about the description of B — it can't just be the complement of A in $\mathbb{N}$ because of the way the argument runs.): If $1 \in A$, then because 1 is the smallest element in $\mathbb{N}$, 1 is the smallest element of A, $\rightarrow\!\leftarrow$ because A <u>has</u> no smallest element; so $1 \notin A$, and so $1 \in B$. Suppose $n \in B$, so that $1, 2, 3, \ldots, n$ are not in A. If $n + 1 \in A$, then $n + 1$ is the smallest element in A, $\rightarrow\!\leftarrow$; so $n + 1 \notin A$, $\rightarrow\!\leftarrow$; so $n + 1$, as well as $1, 2, 3, \ldots, n$, is not in A. Thus, $n + 1 \in B$. It follows by the induction principle that $\mathbb{N} \subseteq B$ and by definition $B \subseteq \mathbb{N}$, so $\mathbb{N} = B$. $\square$

There are ordered fields in which some elements are so small that adding them together as many times as you want will never give a sum greater than 1. (As a result, the reciprocals of such elements are so large that they are greater than any positive integer.) Such fields are called "non-Archimedean" and appear in "nonstandard" treatments of calculus. (Ask Prof. Saracino for more information about such treatments.) But such fields are not complete — a complete field must be Archimedean:

Theorem. (Archimedean Property) *For any positive $\varepsilon, M \in \mathbb{R}$ [no matter how small ε is and how large M is], $\exists\, n \in \mathbb{N}$ s.t. $n\varepsilon > M$.*

Proof. It is enough to find an n in $\mathbb{N}$ for which $n > M/\varepsilon$, so we need to show that it is <u>not</u> true that $n \leq M/\varepsilon \;\forall\, n \in \mathbb{N}$, i.e., that M/ε is not an upper bound for $\mathbb{N}$. It is enough to show that there is no upper bound for $\mathbb{N}$ in $\mathbb{R}$.

So assume BWOC that $\mathbb{N}$ has an upper bound in $\mathbb{R}$. The it has a sup, say L, in $\mathbb{R}$. Now because L is a sup, and $L - \frac{1}{2} < L$, $L - \frac{1}{2}$ is not an upper bound for $\mathbb{N}$, so there is an n in $\mathbb{N}$ for which $L - \frac{1}{2} < n$. But then $n + 1 \in \mathbb{N}$ and

$$n + 1 > (L - \frac{1}{2}) + 1 = L + \frac{1}{2} > L \ ,$$

$\rightarrow\!\leftarrow$. $\square$

Corollary. *$\forall\, r \in \mathbb{R}$, $\exists\, z \in \mathbb{Z}$ s.t. $z < r \leq z + 1$.*

Corollary. *$\forall\, \varepsilon > 0$ in $\mathbb{R}$, $\exists\, n \in \mathbb{N}$ s.t. $0 < (1/n) < \varepsilon$.*

Proof. Pick n so that $n\varepsilon > 1$. $\square$

Theorem. ($\mathbb{Q}$ is "dense" in $\mathbb{R}$) *$\forall\, a, b \in \mathbb{R}$ with $a < b$, $\exists\, q \in \mathbb{Q}$ s.t. $a < q < b$.*

Proof. We have $b - a > 0$, so $\exists\, n \in \mathbb{N}$ s.t. $0 < (1/n) < b - a$. Then $nb - na > 1$. Now $\exists\, z \in \mathbb{Z}$ s.t. $z < nb \leq z + 1$, and $nb - z \leq 1 < nb - na$, so $z > na$. Thus, $na < z < nb$, so $q = z/n$ satisfies $a < q < b$. $\square$

The next few results are simply intended as examples to help you in doing the homework.

Example. Let A, B be subsets of $\mathbb{R}$ such that $\forall\, a \in A\ \exists\, b \in B$ s.t. $a < b$. Prove that $\sup(A) \leq \sup(B)$, and show by example that it may <u>not</u> be true that $\sup(A) < \sup(B)$.

Proof. If $\sup(B) = \infty$, then this is clear, so suppose B has a finite sup, b^*. Then for all a in A, we can find a b in B for which $a < b \leq b^*$; so b^* is an upper bound for A, and hence $\sup(A) \leq b^*$.

But if $A = \{.9, .99, .999, .9999, \ldots\}$ and $B = \{1\}$, then $\sup(A) = 1 = \sup(B)$. (In fact, for another example, we could have let A be any set that does not contain its sup and set $B = A$.) $\square$

Example. Let A, B be subsets of $\mathbb{R}$ that are bounded below, and set $A + B = \{a + b : a \in A,\ b \in B\}$. Prove that $\mathrm{glb}(A) + \mathrm{glb}(B) = \mathrm{glb}(A + B)$.

Proof. Set $\mathrm{glb}(A) = a^*$ and $\mathrm{glb}(B) = b^*$. Each element of $A + B$ has the form $a + b$ where $a \in A$ and $b \in B$, and we know $a* \leq a$ and $b^* \leq b$, so $a^* + b^* \leq a + b^* \leq a + b$. Thus, $a^* + b^*$ is a lower bound for $A + B$.

Now take any lower bound c for $A + B$. Then for any (temporarily fixed) $b \in B$, we know that for all a in A, $c \leq a + b$, so $c - b \leq a$; thus, $c - b$ is a lower bound for A, so $c - b \leq a^*$, or equivalently $c - a^* \leq b$. Thus (letting b vary through B again), we see that $c - a^* \leq b$ for every b in B, i.e., $c - a^*$ is a lower bound for B; so $c - a^* \leq b^*$. So we have $c \leq a^* + b^*$.

Alternatively, we might be trickier in the second paragraph: Take any lower bound c for $A + B$, and assume BWOC that $c > a^* + b^*$. Then $a^* + \frac{1}{2}(c - (a^* + b^*))$ is greater than a^*, so it is not a lower bound for A; so there is an element a of A for which $a < a^* + \frac{1}{2}(c - (a^* + b^*))$. Similarly, we can find an element b of B for which $b < b^* + \frac{1}{2}(c - (a^* + b^*))$. But then

$$a + b < a^* + \frac{1}{2}(c - (a^* + b^*)) + b^* + \frac{1}{2}(c - (a^* + b^*)) = c \ ,$$

so c is not a lower bound for $A + B$, $\rightarrow\!\leftarrow$.

Either way the proof ends as follows: Because c is a lower bound for $A + B$ (from the first paragraph) and $c \leq a^* + b^*$ for every lower bound c of $A + B$ (from the second/third), we have $a^* + b^* = \mathrm{glb}(A + B)$. $\square$

Here is one last consequence of completeness that we will use later in the course:

Corollary. (Nested Interval Property) *Let $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ be closed finite (nonempty) intervals in $\mathbb{R}$. Then $\bigcap_{n=1}^{\infty} I_n \neq \emptyset$.*

Proof. Write $I_n = [a_n, b_n]$ for each $n \in \mathbb{N}$. Then for $m \geq n$, $I_m \subseteq I_n$, so $a_1 \leq a_2 \leq \cdots \leq a_m \leq b_m \leq b_n$; so every b_n is an upper bound for $\{a_m : m \in \mathbb{N}\}$, and similarly every a_n is a lower bound for $\{b_m : m \in \mathbb{N}\}$. Set $a^* = \text{lub}(\{a_m : m \in \mathbb{N}\})$ and $b^* = \text{glb}(\{b_m : m \in \mathbb{N}\})$. We want to show that $a^* \leq b^*$, so that $I^* = [a^*, b^*]$ will be nonempty (even if it is a single point) and $I^* \subseteq I_n$ for all n in $\mathbb{N}$, so it is in the intersection.

So assume BWOC that $a^* > b^*$. Then b^* is not an upper bound for $\{a_n : n \in \mathbb{N}\}$, so there is an n in $\mathbb{N}$ for which $a_n > b^*$. Thus, a_n is not a lower bound for $\{b_m : m \in \mathbb{N}\}$, $-\!\!\!\times\!\!\!-$, because we saw above that every a_n is a lower bound for this set. So the proof is complete. $\square$

Example. We need the hypotheses of closedness and boundedness on the intervals in the Nested Interval Property:

$$\bigcap_{n=1}^{\infty} (0, \frac{1}{n}] = \emptyset \qquad , \qquad \bigcap_{n=1}^{\infty} [n, \infty) = \emptyset$$

[At this point students are ready to do the first problem set.]