I. Introduction
   A. One of the goals of the course is to make sure that you have had some experience understanding mathematical proofs.
      1. The theorem-proof style is increasingly the language of economic research.
         a. The idea that economics should be logically sound isn’t new, but in recent decades the expected level of rigor and exactness of detail, and the range of mathematics employed in research, have increased quite a bit.
         b. In this lecture we consider basic issues concerning proofs.
   B. A proof is a matter of displaying “that which is to be proved” as a logical consequence of what is already known.
      1. Note that the very concept of a proof presumes an audience with a certain state of knowledge.
         a. In everything we do, and in all that you write, basic and obvious facts about propositional logic (e.g., if ‘P’ and ‘P
implies $Q'$, then $'Q'$) and set theory (e.g., the intersection of two sets is a subset of the union of the same two sets) will be more or less taken for granted.

b. Usually proofs appeal to ‘stuff that everyone with the pre-requisites should know’ like the chain rule, derivatives of basic functions, and so forth. Also, proofs take advantage of results proved earlier in the course.

c. After this lecture the axioms for the real numbers, and the most basic theorem derived from these axioms, will be available. An important point is that *everything we do should be logically derived from these axioms*. There is no other source of knowledge concerning the real numbers.

2. In practice a proof is not really an exact, step by step analysis, based on the postulated rules of symbolic manipulation, but instead a piece of prose directed at making another human being believe that there is no doubt that such a symbolic proof could be constructed.

a. Ideally a proof should be short, simple, and impossible to misunderstand.

b. Although there are some particular methods for achieving this, people who write proofs should think about whether the things they read are well or poorly written, and try to emulate good examples. Ultimately this is an art.
II. The Real Numbers

A. The set of real numbers, which we denote by \( \mathbb{R} \), is a set endowed with two binary operation \( +, \cdot : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R} \) and a binary relation \(<\) that satisfy Axioms R1-R16 below.

B. The real numbers are the basis of almost all of our work in this course.

C. We will comment on the axioms by mentioning some of the most important mathematical structures that are defined by subsets of these axioms. Since these concepts will not be studied in detail, you are not responsible for them.

Axiom R1: \((x+y)+z = x+(y+z)\) for all \(x, y, z \in \mathbb{R}\). (Addition is associative.)

Axiom R2: There is 0 \(\in \mathbb{R}\) such that, for all \(x \in \mathbb{R}\), \(0 + x = x + 0 = x\).

Axiom R3: For each \(x \in \mathbb{R}\) there is \(-x \in \mathbb{R}\) such that \(x + (-x) = 0\) and \((-x) + x = 0\).

A set \(G\) with an operation \(+\) satisfying these three axioms is called a group.

Groups play important roles throughout mathematics, and the study of groups is itself a large and important branch of mathematics. In some cases it is allowed, or mandatory, to write the group operation multiplicatively, in which case the identity element of R2 is denoted by 1.

D. For each example below, convince yourself that R1, R2, and R3 hold.

1. The collection of distance-preserving functions from \(\mathbb{R}^2\) to itself, with composition of functions as the group operation, is the group of Euclidean motions.

2. For a natural number \(n\), the symmetric group on \(n\) elements is the collection of bijections ("bijection" is the grown up word for
“one-to-one and onto function”) $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, with composition of functions as the group operation.

3. Let $A, B, C, D$ be the corners of a square in $\mathbb{R}^2$, let $G$ be the set of one-to-one functions $\sigma : \{A, B, C, D\} \to \{A, B, C, D\}$ that represent ways in which one could place a (rigid) copy of the square on top of the square, and let the group operation be composition of functions. How many elements does this group have? A fundamental principle is that the set of *symmetries* of a mathematical structure is a group.

**Axiom R4:** $x + y = y + x$ for all $x, y \in \mathbb{R}$.

If a group satisfies R4 it is said to be *commutative* or *abelian*, and for us the most important example of such a group is $\mathbb{R}^n$ with vector addition as the operation: $x + y = (x_1 + y_1, \ldots, x_n + y_n)$.

**E.** For each example, convince yourself that R1-R4 hold.

1. For a natural number $n$, the *integers mod n* is $\{0, 1, \ldots, n - 1\}$ with the operation

$$x \oplus y = \begin{cases} x + y, & x + y < n, \\ x + y - n, & x + y \geq n. \end{cases}$$

2. $\mathbb{R}^*$ is $\mathbb{R} \setminus \{0\}$ with multiplication as the group operation.

Groups that do not satisfy R4 are said to be *noncommutative*, and for such groups the operation must be written multiplicatively. For abelian groups the group operation is usually written additively, but there are some exceptions such as 2.

**Axiom R5:** $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in \mathbb{R}$.

**Axiom R6:** $x \cdot (y + z) = x \cdot z + y \cdot z$ and $(x + y) \cdot z = x \cdot z + y \cdot z$ for all $x, y, z \in \mathbb{R}$. 

4
A set $R$ with binary operations $+ : R \times R \to R$ satisfying the axioms to this point is called a ring. An example that will be important for us is the ring of $n \times n$ matrices with addition defined componentwise (the sum of $A = (a_{ij})$ and $B = (b_{ij})$ is the matrix with entries $a_{ij} + b_{ij}$) and multiplication given by matrix multiplication.

**Axiom R7:** $x \cdot y = y \cdot x$ for all $x, y \in R$.

The ring is said to be commutative if R7 is also satisfied.

**Axiom R8:** There is $1 \in R$ such that, for all $x \in R$, $1 \cdot x = x \cdot 1 = x$.

Commutative rings that also satisfy R8 are called commutative rings with unit, the prototypical examples being the integers $\mathbb{Z} = \{ \ldots, -1, 0, 1, \ldots \}$ and the polynomials in a single variable $X$ with coefficients in $R$. (As a matter of logical precision, we may define $\mathbb{Z}$ to be the smallest subset of $R$ satisfying $0 \in \mathbb{Z}$, $1 \in \mathbb{Z}$, $m + n \in \mathbb{Z}$ whenever $m, n \in \mathbb{Z}$, and $-n \in \mathbb{Z}$ whenever $n \in \mathbb{Z}$.)

**Axiom R9:** For each $x \in R$ other than 0 there is $x^{-1} \in R$ such that $x \cdot x^{-1} = 1$.

**Axiom R10:** $0 \neq 1$.

Structures satisfying all the axioms up to this point are called fields. In addition to $R$, the rational numbers, denoted by $\mathbb{Q}$, and the complex numbers, denoted by $\mathbb{C}$, are obvious and well known examples. A very different example is the field $F_p$, which is the group of integers mod $p$, where $p$ is a prime number, endowed with the multiplication $\otimes$ defined by letting $x \otimes y$ be the $z \in \{0, 1, \ldots, p-1\}$ such that $xy - z$ is divisible by $p$. Convince yourself that $F_p$ satisfies R1-R10. (For R9 you need to see that for each $x \in \{1, \ldots, p-1\}$, the function $y \mapsto x \otimes y$ is a bijection from $\{1, \ldots, p-1\}$ to itself.)
Axiom R11: For all $x, y \in \mathbb{R}$, exactly one of the following hold: $x = y$; $x < y$; $y < x$.

Axiom R12: If $x < y$ and $y < z$, then $x < z$. (Transitivity.)

Axiom R13: If $x < y$ then $x + z < y + z$.

Axiom R14: If $0 < x$ and $0 < y$, then $0 < x \cdot y$.

Axioms R1-R14 define the notion of an ordered field. An ordered field is Archimedean if it also satisfies

Axiom R15: For every $x \in \mathbb{R}$ there is some $n \in \mathbb{Z}$ such that $n > x$.

Note that this axiom easily implies that for any $x > 0$ there is some natural number $n$ such that $1/n < x$. The real numbers and the rational numbers are Archimedean ordered fields. Ordered fields that are not Archimedean are important in some advanced parts of mathematics, but not in this course, and we will not give any examples.

The following axiom is different in a critical way, in that it refers to arbitrary subsets of $\mathbb{R}$. All the other axioms are pretty well known, even to grade school students, so this is the one that might be new to you. It is critical to many facts concerning limits, and thus to the differential calculus generally.

Axiom R16: For any nonempty set $S \subset \mathbb{R}$ that is bounded above (i.e., there is some $K \in \mathbb{R}$ such that $s \leq K$ for all $s \in S$) there is a least upper bound, which is a number $M \in \mathbb{R}$ such that $s \leq M$ for all $s \in S$ and $M$ is less than any other number that has this property.
III. Some Proofs.

A. We now illustrate the idea of a proof by examining a couple simple facts about the reals. Later, we will regard facts like these as stuff that ‘everybody knows,’ and which can be used freely in arguments. But that is not the same as saying that constructing proofs like the following is easy, since (precisely because you already know all this stuff) one must be careful to keep track of what has been proved.

**Theorem 1:** For all $x \in \mathbb{R}$, $x \cdot 0 = 0$.

**Proof:** Applying R2, then R6, we have

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0.$$  

Using R3 to subtract $x \cdot 0$ from both sides yields the desired result. □

**Theorem 2:** For all $x \in \mathbb{R}$, $(-1) \cdot x = -x$.

**Proof:** Apply Theorem 1, R3, R6, then R8 yields:

$$0 = 0 \cdot x = (1 + (-1)) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x.$$  

Now use R3 to subtract $x$ from both sides. □

**Theorem 3:** For all $x, y, z \in \mathbb{R}$, if $x + y = x + z$ then $y = z$. In particular, each $x \in \mathbb{R}$, $-x$ is the only element of $\mathbb{R}$ whose sum with $x$ is 0.

**Proof:** Adding $-x$ to both sides of the given equation, then applying R1, R3, and then R2, yields

$$(-x) + (x + y) = (-x) + (x + z),$$

$$((-x) + x) + y = ((-x) + x) + z,$$
$0 + y = 0 + z$, and
\[ y = z. \]

**Theorem 4:** For all $x, y \in \mathbb{R}$, if $0 < x < y$, then $x^2 < y^2$.

**Proof:** Since $y^2 - x^2 = (y - x)(y + x)$, this follows from R14. □

**Theorem 5:** There is an $z \in \mathbb{R}$ such that $z > 0$ and $z^2 = 2$.

**Proof:** (A bit more informal.) Let $S = \{ x \in \mathbb{R} : x > 0 \text{ and } x^2 \leq 2 \}$. Then $S$ is nonempty because it contains 1, and Theorem 4 implies that it does not contain any number greater than 2, so it is bounded above. Therefore R16 implies that it has a least upper bound $z$. If $z^2 < 2$, then one can easily show that there is some natural number $n$ such that $(z + 1/n)^2 \leq 2$, so that $z + 1/n \in S$ and $z$ is not an upper bound of $S$. (This method of argument is called \textit{proof by contradiction} or \textit{reductio ad absurdum}.) If $z^2 > 2$, then one can easily show that there is some natural number $n$ such that $(z - 1/n)^2 > 2$, and Theorem 4 implies that $z - 1/n$ is an upper bound for $S$ that is less than $z$. Since $z^2 < 2$ and $z^2 > 2$ are impossible, it must be the case that $z^2 = 2$. □