APPENDIX A

Prerequisite Knowledge

Given that we are making every effort to make our course rigorous, the truth of all of our proofs will ultimately rely on the axioms of mathematics (which are typically formulated in terms of the theory of sets). In this appendix, we will review all of our basic assumptions. They are of two varieties: the general theory of sets and the assumptions we will place specifically on the set of real numbers and on the set of natural numbers. The latter can be proved from the former, but doing so would take us outside of the scope of the text.

1. Set Theory

We will not try and define what we mean by a **set**. Surprisingly this point is quite complicated and philosphical and many mathematics have devoted their lives to these considerations. **Set theory** is the study of the basic definitions and properties surrounding the notion of a set.

Definition. You are probably already familiar with the most basic concepts of set theory:

(1) $\varnothing$ is the **empty** set, i.e. the set with no elements.
(2) $A \subseteq B$ means that every element of A is an element of B, or for all $x \in A$, $x \in B$. It is read "A is a **subset** of B."
(3) $A = B$ means that A and B have the same elements. Another way of saying this is $x \in A$ if and only if $x \in B$.
(4) $A \cap B = \{x : x \in A \text{ and } x \in B\}$. $A \cap B$ is read as "A intersect B" and is called the **intersection** of A and B.
(5) $A \cup B = \{x : x \in A \text{ or } x \in B\}$. $A \cup B$ is read as "A union B" and is called the **union** of A and B. If $x \in A \cup B$ then $x \in A$ or $x \in B$. It could be in both.
(6) A and B are called disjoint sets if $A \cap B = \varnothing$. A and B are disjoint if they have no elements in common.

Logically speaking, we are taken for granted the fact that given two sets, there is another set that is their union (and likewise with

intersections and so forth). In the mundane cases with which we will be primarily concerned, this fact is of course trivial, but again one must be quite careful when formulating these notions in general. It turns out that the operations of union and intersection satisfy "distributive laws" (similar to those that hold for numbers: see the next section).

A.1. Suppose that A, B, and C are sets. Then the following identities hold:

(1) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(2) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Definition. (1) $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$. $A \setminus B$ is read as "A minus B" and is called the "set theoretic difference of A and B."
(2) $A \triangle B = (A \setminus B) \cup (B \setminus A)$ and is called the **symmetric difference** of A and B.
(3) $A^c = \{x : x \notin A\}$ is called the **complement** of A.

Caution: Actually, A^c is not really a set. When we use A^c we must have a ambient set U in mind. This set is often unspecified and is simply inferred from the context. To be explicit, we can write $A^c = U \setminus A$ which is unambiguous.

A.2. Let A and B be sets. Then the following are true:

(1) $(A^c)^c = A$.
(2) $(A \cap B)^c = A^c \cup B^c$.
(3) $(A \cup B)^c = A^c \cap B^c$.
(4) $A \triangle B = (A \cup B) \setminus (A \cap B)$.

Statements (2) and (3) are called **De Morgan's Laws**.

Definition. If A and B are sets then the **Cartesian product** of A and B is defined to be

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$$

where (a, b) denotes the ordered pair.

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the Cartesian plane.

Definition. We can define unions and intersections of large collections of sets. If I is a set, called the **index set**, and for all $i \in I$, A_i is a set

then we define

$$\bigcup_{i\in I} A_i = \{x : \text{ there exists } i \in I \text{ such that } x \in A_i\}$$
$$\bigcap_{i\in I} A_i = \{x : \text{ for all } i \in I,\, x \in A_i\}.$$

A.3. If I is a set and for all $i \in I$, A_i is a set, then

(1) $(\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} A_i^c$.
(2) $(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c$.

These are the De Morgan's laws for unions and intersections over arbitrary index sets.

2. The Field Properties of the Real Numbers

In this and the following two section, we formulate precisely the properties we are assuming regarding the set of real numbers with the exception of the completeness axiom which is discussed in Chapter 3. The completeness axiom is a major object of study in this course.

Mathematicians study many different types of mathematical objects. You may have heard of groups, rings, topological spaces, smooth manifolds, vector spaces, Banach spaces, affine varieties, elliptic curves, etc. One of the objects which mathematicians study is called a *field*. In the introduction to the chapter, we mentioned several algebraic properties of $\mathbb{R}$. The crucial algebraic properties of $\mathbb{R}$ can be summarized by saying that $\mathbb{R}$ is a field. Notice that all the field properties (listed below) would certainly be demanded of any number system.

As we mentioned above, we will take all the properties on faith. Hence will call them axioms (in mathematics an axiom is a basic statement which is accepted without proof, for example the statement which intuitively says "there exists a set" is a basic axiom of mathematics).

Axiom 1: There exists a set $\mathbb{R}$, which contains $\mathbb{Q}$. We may define two operations on $\mathbb{R}$ called addition and multiplication, which extend normal addition and multiplication of rational numbers.

When we say that addition on $\mathbb{R}$ extends addition on $\mathbb{Q}$, we mean that adding two real numbers which happen to be rational would be the same as the normal addition of rational numbers (and likewise for multiplication).

We will use all the standard notations regarding operations among numbers. For example $a+b$ is the sum of $a, b \in \mathbb{R}$. As always, we write the symbol '=' between two real numbers which are the same and the symbol '$\neq$' between two which are not.

AXIOM 2: Addition of real numbers is commutative: For every $a, b \in \mathbb{R}$, $a + b = b + a$.

AXIOM 3: Addition of real numbers is associative: For every $a, b, c \in \mathbb{R}$, $a + (b + c) = (a + b) + c$.

AXIOM 4: The real number zero is an additive identity: For each $a \in \mathbb{R}$, $0 + a = a$.

AXIOM 5: Every real number has an additive inverse: For every $a \in \mathbb{R}$, there is a number $b \in \mathbb{R}$ such that $a + b = 0$.

We mentioned above that there are many obvious facts about the real numbers that, strictly speaking, must be proven from the axioms. The following is an example (as are most of the exercises in this section).

A.4. For every $a \in \mathbb{R}$, the additive inverse of a is unique. That is, if b and c are real numbers which satisfy $a + b = 0$ and $a + c = 0$, we may conclude that $b = c$.

The previous problem justifies us saying *the* additive inverse of $a \in \mathbb{R}$ (rather then *an* additive inverse). As usual, we will use the symbol $-a$ for the additive inverse of a. Notice that, strictly speaking, $-a$ is not the same symbol as $(-1) \cdot a$ (that is the number negative 1 times the number a). That the two symbols represent the same number will be one the obvious facts we prove below.

We can also now define subtraction: If a and b are natural numbers, then $a - b$ is defined to be $a + (-b)$ (in words $a - b$ is the the sum of a and the additive inverse of b).

AXIOM 6: Multiplication of real numbers is commutative: For every $a, b \in \mathbb{R}$, $ab = ba$.

AXIOM 7: Multiplication of real numbers is associative: For every $a, b, c \in \mathbb{R}$, $a(bc) = (ab)c$.

AXIOM 8: The number one is a multiplicative identity: For every $a \in \mathbb{R}$, $a \cdot 1 = a$.

AXIOM 9: Every real number besides zero has a multiplicative inverse: For every $a \in \mathbb{R}$ with $a \neq 0$, there is a number b such that $ab = 1$.

We have a result about multiplicative inverses analogous to the one we had for additive inverse.

A.5. For every $a \in \mathbb{R}$ (other than zero), the multiplicative inverse of a is unique. That is, if b and c are real numbers which satisfy $ab = 1$ and $ac = 1$, we may conclude that $b = c$.

Again we are now justified in referring to *the* multiplicative inverse of a, which we will denote by a^{-1}. We define division in a similar manner as subtraction: a/b is defined to be ab^{-1} (that is, a/b is defined to be the product of a and the multiplicative inverse of b).

AXIOM 10: Multiplication and addition satisfy the distributive property: For every $a, b, c \in \mathbb{R}$, $a(b + c) = ab + ac$.

These algebraic properties of the real numbers are very important, but they are not unique to $\mathbb{R}$. $\mathbb{Q}$ would satisfy all of these axioms and so is also a field. In general, there exist many different fields. The collection of complex numbers, $\mathbb{C}$, (with usual notions of addition and subtraction) is a field. For a prime number p, you may be familiar with the collection of numbers modulo p, often denoted $\mathbb{Z}_p$. It too is a field (and in contrast to $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ has finitely many elements). We will thus need more properties of $\mathbb{R}$ to describe it uniquely.

The following (relatively simple) question might help you to better understand the axioms:

A.6. Which axioms would still be satisfied if $\mathbb{R}$ were replaced with $\mathbb{Q}$? with $\mathbb{Z}$? with $\mathbb{N}$?

We will now give some more basic properties about the real numbers which follow from these axioms.

For our first result, we will see that the multiplication operation on $\mathbb{R}$ still boils down to repeated addition (as long as one of the numbers is a natural number).

A.7. Multiplication of real numbers by natural numbers is just repeated addition. That is, if $a \in \mathbb{R}$ and $n \in \mathbb{N}$, na is the same as the number which results when a is added to itself n times.

Hint: Use induction.

As promised, we will show that the additive inverse of a real number is just that number, multiplied by -1.

A.8. For every $a \in \mathbb{R}$, the product of a and -1 is the additive inverse of a. That is, $-a = (-1)a$.

We can also define integral powers of real numbers (that is, raising a real number to an integral) in the usual way.

Definition. Let $a \in \mathbb{R}$. If n is a natural number, we define a^n to be the product of a with itself n times. Likewise a^{-n} is defined to be the product of a^{-1} with itself n times. We also define a^0 to be 1.

We have the usual basic properties of powers:

A.9. If $a, b \in \mathbb{R}$ and $m, n \in \mathbb{Z}$, then

(1) $(a^m)^n = a^{mn} = (a^n)^m$,
(2) $a^{m+n} = a^m a^n$, and
(3) $(ab)^m = a^m b^m$.

Hint: These properties are by no means automatic. They must be proven, by careful reasoning, from the axioms.

3. The Order Properties of the Real Numbers

In the previous section we saw the algebraic (or field) properties of $\mathbb{R}$. In this one we will study the order properties. As mentioned in the introduction, a set is ordered if we have a rule which tells us, given two elements of the set, which is bigger.

Axiom 11: The real numbers come equipped with an order which extends the order on $\mathbb{Q}$.

Again by 'extends,' we mean that if a and b are rational numbers, then a is less than b according to the order on $\mathbb{Q}$ if and only if a is less than b according to the order on $\mathbb{R}$.

As usual, we denote the order by $\leq$.

Axiom 12: The order is reflexive: For every $a \in \mathbb{R}$, $a \leq a$.

Axiom 13: The order is transitive: For every $a, b, c \in \mathbb{R}$ such that $a \leq b$ and $b \leq c$, we have $a \leq c$.

Axiom 14: The order is antisymmetric: For every $a, b \in \mathbb{R}$ such that $a \leq b$ and $b \leq a$, we have $a = b$.

Axiom 15: The order is a total order: For every $a, b \in \mathbb{R}$, either $a \leq b$ or $b \leq a$.

$\mathbb{R}$ is by no means the only set that comes with an order. In fact, an order can be defined on any set (and many sets, like for example the set consisting of all the months in the year, have an obvious order). Actually, there are many different ways to define an order on $\mathbb{R}$, but there is only one order that will satisfy all the axioms we will list (and have listed).

We will also use the symbols $<$, $>$, and $\geq$ with their usual meanings (i.e., $a < b$ means $a \leq b$ and $a \neq b$). To make our words precise, we will pronounce $a \leq b$ as "a is less than b" and $a < b$ as "a is strictly less than b" (with similar phrasing for $\geq$ and $>$). Note then that "a is less than b" includes the possibility that $a = b$. This is only a convention, but it is one used by many mathematicians.

Again we have many basic and obvious properties.

A.10. $\mathbb{R}$ satisfies the trichotomy property: if $a, b \in \mathbb{R}$, then exactly one of the following holds:

(1) $a < b$,
(2) $a > b$, or
(3) $a = b$.

As expected, a number which is strictly greater than zero is called **positive**, whereas a number which is either positive or zero (in other words a number that is greater then zero) is called **nonnegative**. We use the terms **negative** and **nonpositive** similarly (though nonpositive is typically used with less frequency).

4. The Ordered Field Properties of the Real Numbers

In this section, we will discuss how the algebraic (field) properties of $\mathbb{R}$ interact with the order properties (again in ways that, if you think about them, should work in any system of numbers).

Axiom 16: The order is preserved under addition by a fixed number: If $a, b, c \in \mathbb{R}$ and $a \leq b$ then $a + c \leq b + c$.

Axiom 17: The product of two nonnegative numbers is again nonnegative: If $a, b \in \mathbb{R}$, $0 \leq a$, and $0 \leq b$ then $0 \leq ab$.

To say that $\mathbb{R}$ satisfies these additional properties is to say that it is an **ordered field**. Notice that being an ordered field is much more restrictive than being a field and having an order. The field properties and the order properties must also interact in the right way (as described by the previous two axioms). For example, although there many orders on the set of complex numbers, $\mathbb{C}$, there is no order which makes it into an ordered field (this is not too difficult to prove and we will do so below). Demanding that our numbers form an ordered field tells us that we cannot include imaginary numbers (or complex numbers) in our number system. It also turns out that there is no order on $\mathbb{Z}_p$ which makes it into an ordered field.

Nevertheless, $\mathbb{R}$ is not the only ordered field. $\mathbb{Q}$ is an ordered field and there are many others. We will need one additional property, called the completeness axiom, to uniquely define $\mathbb{R}$. As we mentioned in the introduction to Chapter 2, the completeness axiom is significantly deeper than the others and we will need to develop several new concepts in the Chapter 3 before we can describe it.

Again, we have many basic properties that follow from the axioms. As always, be careful not to use any facts other than the axioms (and other facts we have proven).

The next result shows that we may multiply inequalities by -1 as long as we are willing to reverse the sign.

A.11. Let $a, b \in \mathbb{R}$. If $a \leq b$ then $-b \leq -a$.

More generally, we may multiply an inequality by a real number, but, as expected, we must reverse the sign if the number is negative.

A.12. Suppose $a, b \in \mathbb{R}$ and $a \leq b$. If $c \in \mathbb{R}$ is nonnegative, then $ac \leq bc$. If c is nonpositive then $bc \leq ac$.

Of course the same result holds for strict inequalities unless $c = 0$ (by a similar proof).

A.13. Given any number $a \in \mathbb{R}$, there is a number which is strictly larger.

Hint: Finding a number is not difficult, but prove rigorously that it is larger.

A.14. If $a \in \mathbb{R}$, $a^2 \geq 0$ with $a^2 = 0$ if and only if $a = 0$.

A.15. Suppose we have a field F (that is, F satisfies all the properties which we gave for $\mathbb{R}$ in the section on the field properties). In addition suppose there is an element $i \in F$ which satisfies $i^2 = -1$. Then there is no order on F which makes it into an order field (that is, no order which will satisfy all the properties given for $\mathbb{R}$ in this chapter).

Hint: Suppose F does indeed satisfy all the properties we have given so far for $\mathbb{R}$. How does i compare to zero?

We will not have occasion to use the next result, but they are of general interest and they provide insights into ordered fields.

A.16. There is no order on $\mathbb{C}$ which makes it an ordered field.

This last result is important because $\mathbb{C}$ does satisfy the completeness axiom (or at least an appropriate formulation of it). Thus there are fields other then $\mathbb{R}$ which satisfy the completeness axiom, but no other ordered fields which satisfy it. Notice that $\mathbb{Q}$ is an ordered field which is not complete and $\mathbb{C}$ is a completed field which is not ordered.

All of the assumed properties of $\mathbb{R}$ are now in place except completeness. The remaining statements must therefore be proven from our axioms.

5. Mathematical Induction

We mentioned in the introduction to Chapter 2 that we will assuming all the basic properties of $\mathbb{N}$. This includes the following fact.

Axiom 18: $\mathbb{N}$ is **well-ordered** under the usual ordering. In other words, every nonempty set of $\mathbb{N}$ contains an element which is smaller than the others.

The $\mathbb{N}$ is well-ordered axiom be proven from the more basic axioms of mathematics, but we will not attempt to carry out this proof. We use the previous axiom to prove the validity of an extremely important technique of proof. Hopefully you are already familiar with this method.

THE THEOREM OF MATHEMATICAL INDUCTION: Let $P(1), P(2), P(3), \ldots$ be a list of statements, each of which is either true or false. Suppose that

i) $P(1)$ is true
ii) For all $n \in \mathbb{N}$, if $P(n)$ is true then $P(n+1)$ is true.

Then for all $n \in \mathbb{N}$, $P(n)$ is true.

A.17. Prove the above theorem.

Hint: Suppose it were not true. Use the fact that $\mathbb{N}$ is well-ordered to find an n_0 which is the smallest element of $\mathbb{N}$ so that $P(n_0)$ is false.

A.18. Use mathematical induction to establish the following. Make sure in your proof to precisely state what you are taking "$P(n)$" to be.

a) For all $n \in \mathbb{N}$, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$
b) For all $n \in \mathbb{N}$, $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$
c) For all $n \in \mathbb{N}$, if $n \geq 4$ then $2^n < n!$.

Note: $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (n-1) \cdot n$. This is called "$n$ factorial."