Chapter 1

Axioms of the Real Number System

1.1 Introductory Remarks: What constitutes a proof?

One of the hurdles for a student encountering a rigorous calculus course for the first time, is what level of detail is expected in a proof. If every statement is completely justified, the proof that $1 + 1 = 2$ takes over 200 pages of Principia Mathematics (Russell & Whitehead). So obviously, some things must be taken for granted. Just how much? Knowing the answer requires some sophistication...for instructor and student to agree on what is to be assumed and what is to be justified.

Often, precisely what a proof is is stated explicitly. For the record

Definition 1.1 *A* **proof** *is a finite sequence of statements, each of which is an axiom, one of the hypotheses of the theorem, or follows from the preceding statements of the proof by elementary rules of inference, and the last statement of the proof is the conclusion of the theorem.*

At the end of this chapter is an example of detailed mathematical reasoning, beyond what we shall require in this text, but detailed enough to indicate to the reader what truths rest upon what assumptions.

1.2 Propositional Logic and the Predicate Calculus

1.2.1 Propositional Logic

We shall often need to prove sentences of the form

$$p \Longrightarrow q \tag{1.1}$$

where p and q are "propositions". A **proposition** is a statement, like

"2 is an integer"

or "4 is a prime".

Of course, the first of these propositions is true, and the second is false.

The meaning of Equation 1.1 is taken as "if p is true, then q is also true." We shall understand that this sentence is to be regarded as true if p and q are both true, or if p is false, regardless of the truth value of q. This has the same logical value as "if q is false, then p also must be false." (See Exercise 1.) That is,

$$\neg q \Longrightarrow \neg p, \tag{1.2}$$

where

$$\neg q$$

stands for "not q," the proposition which is true when q is false, and which is false when q is true.

To say two sentences (involving propositions $p, q, \ldots$) have the "same logical value" (or are **equivalent**) is to say that they are simultaneously either both true or both false, regardless of the truth value of $p, q, \ldots$.

The form in Equation 1.2 is called the **contrapositive** form of the sentence "$p \Longrightarrow q$." You should take a few minutes to convince yourself that the two forms have the same logical value. In many places in the book, we shall prove "$p \Longrightarrow q$" by proving "$\neg q \Longrightarrow \neg p$". In summary, then,

$$p \Longrightarrow q \text{ if and only if } \neg q \Longrightarrow \neg p.$$

We represent "p **and** q" by

$$p \wedge q,$$

which will be true if and only if both p and q are true. We represent "p **or** q" by

$$p \vee q,$$

which will be true if and only if (1) p is true or (2) q is true or (3) both p and q are true.

In the exercises, you will be asked to verify that "$p \Longrightarrow q$" is logically equivalent to the expression "$\neg p \vee q$."

Exercise 1 a. Make a "truth table" for $p \Longrightarrow q$, by enumerating each of the four cases (true,true), (true, false), (false, true), and (false, false) of values for (p, q). Then decide for each of the cases whether $p \Longrightarrow q$ is true or false, and enter it in the second column in the table.

p	q	$p \Longrightarrow q$	$\neg q \Longrightarrow \neg p$	$\neg p \vee q$
T	T			
T	F			
F	T			
F	F			

b. Using the same truth table as in Part (a), decide for each of the four cases whether $\neg q \Longrightarrow \neg p$ is true or false. Enter your values in the third column of the table. Compare with $p \Longrightarrow q$. Recall that two expressions are "equivalent" if they have the same truth value for all possible truth values of the variables (in this case p and q.)

c. Using the same truth table as in Part (a), decide for each of the four cases whether $\neg p \vee q$ is true or false. Compare with $p \Longrightarrow q$.

Another form of proof we shall employ is **proof by contradiction**:

If the assumption of the proposition $\neg p$ leads to a contradiction (e.g. "$0 = 1$"), then we may conclude that $\neg p$ is false, i.e. that p is true.

Example 1 The familiar proof, due to Euclid, that there are infinitely many primes, proceeds as follows:

Suppose there were only finitely many primes, and we list ALL of them:

$$p_1, p_2, \ldots, p_k$$

Now consider the integer

$$n = 1 + p_1 p_2 \dots p_k.$$

We claim that n is also prime, because for any i, $1 \leq i \leq k$, if p_i divides n, since p_i divides $p_1 p_2 \dots p_k$, it would divide their difference, i.e. p_i divides 1, impossible. Hence the assumption that p_i divides n is false (since it led to contradiction), and hence p_i does not divide n, for any i. Hence n is prime. But we listed ALL the primes above, as $p_1, \dots p_k$, and n is not among them (since it is larger than each of them). This contradicts the assumption that we listed all the primes, and hence our assumption that there were only finitely many primes is false. Hence there are infinitely many primes[1].

In the above proof, note that we actually used the principle of proof by contradiction *twice*.

The form of "proof by contradiction" written in propositional logic is the following:

$$(\neg p \Longrightarrow \text{FALSE}) \Longrightarrow p.$$

If $p \Longrightarrow q$ and $q \Longrightarrow p$ then p and q are logically equivalent, and we write

$$p \equiv q$$

or

$$p \Longleftrightarrow q.$$

1.2.2 Predicate Calculus

We shall often make and prove statements of the form

"for every x, $P(x)$" which is written: "$\forall x P(x)$"

or

"there exists an x such that $P(x)$" which is written: "$\exists x P(x)$."

Here we understand that P is a proposition (see above) with a variable x in it, which becomes either true or false when we substitute a number in for x. For example $P(x)$ could be the statement

[1] 2000 years later, Euler gave a totally different proof. Euler's proof is much more sophisticated, and was the first proof which used Analysis to prove a result in number theory, and thus introduced the field of Analytic Number Theory. See Chapter ** for his proof.

$$P(x) \equiv \text{“}x \text{ is divisible by 2”},$$

a statement which is true when you substitute 4 for x, so $P(4)$ is true, and $P(122)$ as well. But $P(3)$ is false.

So, for the $P(x)$ we just defined, the statement

$$\forall x P(x)$$

is false, while the statement

$$\exists x P(x)$$

is true.

We understand the universe over which the “quantifiers” range to be understood from the context. For our purposes, typically the universe will be the real numbers, or sometimes the natural numbers. Other universes are possible.

Furthermore, the statement

$$\forall x P(x)$$

will be regarded as **true** if there are NO x's in the universe, regardless of what x is! Thus, we are going to regard the sentence

“All unicorns have 5 feet.”

as true.

But the statement

$$\exists x P(x)$$

will be taken as **false** if there are no x's in the universe.

Thus, the statement

“Some unicorns have 5 feet.”

will be taken as false.

To say that “it is false that for all $x, P(x)$” is to say that there must be some x such that $P(x)$ does not hold. The negation of

$$\forall x P(x)$$

is the sentence

$$\exists x \neg P(x),$$

and the negation of

$$\exists x P(x)$$

is the sentence

$$\forall x \neg P(x).$$

Quantifiers are read left-to-right, like English, so we have the possibility of statements like

$$\forall x \exists y P(x, y).$$

Supppose, for example, that $P(x, y)$ is the proposition "$x < y$," where the variables x and y are understood to range over the real numbers. Then the statement

$$\forall x \exists y (x < y)$$

is true, since for every real number x there is another real number (e.g. $x + 1$) which is greater than x. But the statement

$$\exists x \forall y (x \leq y)$$

is false, since it asserts there is a number (x) which is the "smallest" real number. Note also that as the quantifiers are read left-to-right, in $\forall x \exists y (x < y)$, y depends upon x, but in $\exists x \forall y (x \leq y)$, x does not depend upon y.

Later on, we shall need to be familiar with reasoning such as, "Above, we just concluded that in the domain of real numbers it is false that there is a number (x) which is less than every real number (y). Hence

$$\neg \exists x \forall y (x \leq y),$$

which is equivalent to

$$\forall x \exists y \neg (x \leq y),$$

i.e.,

$$\forall x \exists y (x > y),$$

which is the statement that for every real number (x) there is another real number y smaller than it (e.g. $y = x - 1$.)"

Also when the existence of an x with a certain property is asserted, we shall frequently name one, say x_0, as in the following:

"...$f(x)$ is not continuous on all of $[0, 1]$ and hence there exists an $x \in [0, 1]$ such that f is not continuous at x. Let x_0 be such an x."

Exercise 2 Construct the negation of "$p \Longrightarrow q$."

Exercise 3 Construct the negation of " $\forall x[P(x) \Longrightarrow Q(x)]$."

Exercise 4 Construct the negation of "$\forall x \exists y[P(x, y) \Longrightarrow Q(x, y)]$."

Exercise 5 Construct the negation of "$\forall x \exists y \forall z[P(x, y, z) \Longrightarrow Q(x, y, z)]$."

Exercise 6 The definition of "f is continuous at $x = a$" is the following:

"for every $\epsilon > 0$ there exists a $\delta > 0$ such that for all x, if $|x - a| < \delta$ then $|f(x) - f(a)| < \epsilon$."

a. Write this as a logical expression in the Predicate Calculus, identifying the component pieces. (Assume that the "universe" of ϵ and δ is all positive numbers.)

b. Construct the negation of "f is continuous at $x = a$."

1.3 Properties of $\mathcal{R}$, the Real Numbers:

1.3.1 The Axioms of a Field:

The real numbers $\mathcal{R} = (-\infty, \infty)$ form a set which is also a **field**, as follows: There are two binary operations on $\mathcal{R}$, addition and multiplication, which satisfy a set of axioms which make the set $\mathcal{R}$ a **commutative group under addition**: (all quantifiers in what follows are assumed to be over the "universe" of real numbers, $\mathcal{R}$.)

1. For every x and y, $x + y = y + x$. (Commutativity)

2. For every x, y and z, $x + (y + z) = (x + y) + z$. (Associativity)

3. There exists an element x such that for every y, $x + y = y$. (We call this element the additive identity, and after proving that it is unique, we label it 0. See Theorem 1.1 for a proof of uniqueness.)

   Restated: $\forall x[0 + x = x]$. (Identity)

4. For every x there exists a y such that $x + y = 0$. (Additive inverse). Note that from the order of the quantifiers, y depends upon x. We usually denote this y by "$-x$".

The non-zero elements of $\mathcal{R}$ form a **commutative group under multiplication**:

1. For every x and y $x \cdot y = y \cdot x$. (Commutativity)

2. For every x, y and z, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. (Associativity)

3. There exists an x such that for every y, $x \cdot y = y$. (We call this element the multiplicative identity, and after proving that it is unique, we label it "1". See Theorem 1.1 below for a proof of uniqueness.)

   Restated: $\forall x[1 \cdot x = x]$. (Identity)

4. For every x there exists a y such that $x \cdot y = 1$. (Multiplicative inverse). Note that from the order of the quantifiers, y depends upon x. We usually denote y by "x^{-1}", or by "$1/x$".

   To relate the additive group structure to the multiplicative structure, we require that multiplication "distribute" over addition:

5. For every x, y and z, $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

We need one additional axiom to ensure the field contains at least two elements:

1. There exists at least one element $a \neq 0$.

This guarantees us two elements, since by the axioms of the additive group, there exists an additive identity (0.)

We shall also omit the multiplication symbol, and write ab for $a \cdot b$ when the context makes this clear.

Theorem 1.1 *In $\mathcal{R}$ the additive identity and multiplicative identity are unique.*

Proof: Suppose that there are two elements, 0 and $0'$ which both satisfy the axiom of identity:

$$\text{For every } x \in \mathcal{R},\ 0 + x = x$$

and

$$\text{For every } x \in \mathcal{R},\ 0' + x = x.$$

Then

$$0' = 0 + 0' =^{2} 0' + 0 = 0,$$

i.e. $0 = 0'$.

The proof that the multiplicative identity is unique is similar[3].

Theorem 1.2 *For every $x \in \mathcal{R}$, $x \cdot 0 = 0$.*

Proof:

$$x \cdot 0 = x(0 + 0) = x0 + x0 \tag{1.3}$$

$$\text{so } 0 = x0 + (-x0) = (x0 + x0) + (-x0) = x0 + (x0 - x0) = x0. \tag{1.4}$$

(We are writing "$a - b$" for "$a + (-b)$", of course.)

Theorem 1.3 $-x = (-1)x$

Proof: See Exercise 11.

Exercise 7 Prove that if $a + x = x$ for *some* x, then $a = 0$. Note that with this result we could conclude immediately from Equation 1.3 that $x0 = 0$.

Exercise 8 Prove that if 1 and $1'$ are both multiplicative identities in $\mathcal{R}$, then $1 = 1'$.

Exercise 9 Justify the two steps in equation 1.3 and the four steps in equation 1.4.

[2] Why is $0 + 0' = 0' + 0$?

[3] See Exercise 8.

Exercise 10 Prove: $(-1)(-1) = 1$. Justify every step. Hint: what does (-1) stand for?

Exercise 11 Prove: $-x = (-1)x$. [Hint: show that $(-1)x$ is the additive inverse to x.]

Exercise 12 Prove $-(-x) = x$. [Hint: what does $-(-x)$ denote?]

1.3.2 The Order Axioms

The above axioms, A1-A4, and M1-M5, together with the requirement that there are at least two elements (i.e. that "$0 \neq 1$"), make $\mathcal{R}$ a field. $\mathcal{R}$ is actually a **complete ordered field**. We will discuss completeness in Section 1.5. To obtain an **ordered field**, we need to require an additional set of axioms, about the order relations among the elements, as follows: There is a binary relation[4], "$\leq$" on $\mathcal{R}$ with the following properties:

1. For every x and y, $x \leq y$ and $y \leq x$ implies $x = y$.

2. For every x and y, either $x \leq y$ or $y \leq x$.

   These first two axioms together are called the **Axiom of Trichotomy** (because there are three possible relationships between x and y.)

3. For every x, y, and z, $x \leq y$ and $y \leq z$ implies $x \leq z$.

4. For every x, y, and z, $y \leq z$ implies $x + y \leq x + z$.

5. For every x, y, and z, $y \leq z$ and $0 \leq x$ implies $xy \leq xz$.

We shall often used a strengthened version of Order Axiom 4, which we now prove.

Theorem 1.4 *For all x, y and z, if $y < z$ then*

$$x + y < x + z.$$

[4]The reader who wishes a precise definition of **relation** will find one in Section 1.7

Proof: From Order Axiom 4, under the hypotheses of the theorem, $x + y \leq x + z$. If $x + y = x + z$, by adding the additive inverse of x to both sides, using Associativity, Commutivity and Identity, we obtain[5]

$$y = z.$$

But this contradicts the hypothesis of the theorem. Hence our supposition that $x+y = x+z$ was false, and that together with $x + y \leq x + z$ implies that

$$x + y < x + z. \quad \text{QED}$$

The corresponding multiplicative theorem is the following

Theorem 1.5 *For all x, y and z, if $y < z$ and $x > 0$ then*

$$xy < xz.$$

Proof: The hypotheses of the theorem and Order Axiom 5 imply that $xy \leq xz$. But if $xy = xz$, since $x \neq 0$, we can multiply both sides by $1/x$ and obtain

$$y = z,$$

a contradiction. Hence $xy \neq xz$, and the theorem is proved.

Theorem 1.6 *For all x,*

$$x < 0 \Longleftrightarrow -x > 0.$$

Proof:

$$x < 0$$

implies

$$x + (-x) < 0 + (-x)$$

implies

$$0 < -x,$$

by Additive Inverse, Theorem 1.4, and Additive Identity.

[5]Provide the details!

Conversely, if $0 < -x$, then

$$0 + x < -x + x$$

which implies

$$x < 0,$$

again by Theorem 1.4, Additive Identity, and Additive Inverse.

Exercise 13 Prove that under the asssumption that a field has at least two elements, then $0 \neq 1$.

Exercise 14 Verify that the set $\{0\}$ satisfies all the axioms for an ordered field, except for $0 \neq 1$. Note: just exactly what plays the role of 1, the multiplicative identity?

Exercise 15 Prove: $0 < 1$. [In light of the preceding exercise, note that you MUST use $0 \neq 1$. Why?]

Exercise 16 Prove: $a < b \Longleftrightarrow -b < -a$. [Hint: Make use of Theorem 1.4.]

Exercise 17 Prove: if $a > 0$ and $b > 0$ then $a < b \Longleftrightarrow a^2 < b^2$.

Exercise 18 Prove that for any x, $x^2 \geq 0$.

Exercise 19 Prove that a field has no zero-divisors, i.e. if $ab = 0$ then either $a = 0$ or $b = 0$.

1.3.3 Open and Closed Intervals; Absolute value; The Triangle Inequality

Definition 1.2 *If a and b are real numbers, and $a < b$, we write $[a, b]$ to denote the set of x's for which*
$a \leq x \leq b$. We write (a, b) to denote the set of x's for which $a < x < b$. Intervals of the form $[a, b]$ are called **closed intervals** *and intervals of the form (a, b) are called* **open intervals** *for reasons which will become clear when we study the topology of the real numbers in Chapter 9. It is also possible to have half-closed, half-open intervals. Note that closed intervals contain their endpoints, while open intervals do not. We shall also write (a, ∞) to denote the set of x's for which $a < x$ and similarly $(-\infty, a]$ to denote the set of x's for which $x \leq a$.*

Definition 1.3 *By the* **absolute value** *of x, denoted $|x|$, we mean*

$$|x| = \begin{cases} x, & \text{if } x \geq 0. \\ -x, & \text{if } x < 0. \end{cases}$$

Theorem 1.7 *The following are properties of absolute value:*

1. *For all x, if $x \neq 0$ then $|x| > 0$. If $x = 0$ then $|x| = 0$.*

2. *$|xy| = |x||y|$ for all real numbers x and y.*

3. *$-|x| \leq x \leq |x|$, for all x.*

Proof: (1) By cases: if $x > 0$, then $|x| = x > 0$. If $x < 0$, $|x| = -x > 0$. From the definition, $|0| = 0$.

(2) also proved by cases. See Exercise 23.

(3) By cases: if $x > 0$, $-|x| = -x < 0 < x = |x|$.

If $x < 0$, $-|x| = x < 0 < -x = |x|$.

If $x = 0$, $-|x| = x = |x|$.

In all three cases, then, $-|x| \leq x \leq |x|$.

The following will be needed literally dozens of times throughout the book. Needless to say, it is very important!

Theorem 1.8 *For all real numbers x and M,*

$$|x| \leq M \Longleftrightarrow -M \leq x \leq M.$$

Proof: Suppose $|x| \leq M$. Then by Exercise 16 above, $-M \leq -|x|$, and by Theorem 1.7,

$$-M \leq -|x| \leq x \leq |x| \leq M.$$

Conversely, suppose $-M \leq x \leq M$. Then $-M \leq x$, which implies that $-x \leq M$. But $x \leq M$ by assumption. Then since $|x| = x$ or $|x| = -x$, and in either case, $x \leq M$, it follows[6] that $|x| \leq M$.

Because the theorem above is so important, we give an example, and then have several homework problems which involve it.

[6]The interested reader may wish to note that the form of this reasoning, so called "on the horns of a dilemma", is: $[p \Rightarrow r,\ \ q \Rightarrow r,\ \ p \vee q] \Rightarrow r$.

Example 2 Find the set of y's for which $|y - L| \leq \epsilon$. This is used heavily in our study of limits, in Chapter 2.

By the theorem above,

$$-\epsilon \leq y - L \leq \epsilon,$$

which is equivalent to

$$L - \epsilon \leq y \leq L + \epsilon.$$

So, the set of y's is the interval $[L-\epsilon, L+\epsilon]$. This reasoning will be used frequently throughout the book.

A similar theorem holds for "strict" inequalities:

Theorem 1.9 *For all real numbers x and M,*

$$|x| < M \Longleftrightarrow -M < x < M.$$

The proof is similar to the proof above.

Exercise 20 Prove Theorem 1.9.

Exercise 21 Find the set of x's for which $|x - 3| \leq 4$.

Exercise 22 Find the set of y's for which $|y - L| < \epsilon$.

Exercise 23 Prove $|xy| = |x||y|$, for all $x, y \in \mathcal{R}$.

Theorem 1.10 (Triangle Inequality) *For all real numbers x, y,*

$$|x + y| \leq |x| + |y|.$$

Proof: [We call this "triangle inequality" because of the geometric interpretation when x and y are vectors in $\mathcal{R}^2$. This will have nothing to do with our proof, however.]

$$-|x| \leq x \leq |x| \quad \text{from Theorem 1.7}$$

and

$$-|y| \leq y \leq |y|.$$

Adding these two double inequalities yields

$$-(|x| + |y|) = -|x| - |y| \leq x + y \leq |x| + |y|$$

But then

$$|x + y| \leq |x| + |y| \quad \text{from Theorem 1.8}$$

QED

1.4 Suprema and Infima: sup's and inf's

Definition 1.4 *A set is* **non-empty** *if it possesses at least one element. The* **empty set**, *denoted* $\emptyset$, *is the set consisting of no elements. More on this in Section 1.7*

Definition 1.5 *A non-empty set E is said to be* **bounded above** *if there exists an M such that for every $x \in E$,*

$$x \leq M.$$

Definition 1.6 *A non-empty set E is said to be* **bounded below** *if there exists an N such that for every $x \in E$,*

$$x \geq N.$$

Definition 1.7 *A non-empty set E is said to be* **bounded** *if there exists M, N such that for every $x \in E$,*

$$N \leq x \leq M.$$

It is obvious from the definitions that a set E is bounded if and only if E is bounded above and E is bounded below.

Example 3 $[0, 1]$ is bounded above, by 10, for example. $[0, 1]$ is also bounded above by 1. It is bounded below by -10. Therefore, $[0, 1]$ is bounded as well.

Example 4 $[0, \infty)$ is bounded below (by 0), but not bounded above. For suppose $[0, \infty)$ were bounded above by M, say. Then $M + 1 \in [0, \infty)$ implies $M + 1 \leq M$, a contradiction.[7]

[7] To what, exactly?

Example 5 $(-\infty, \infty)$ is neither bounded below nor bounded above.

Example 6 $\{q \in \mathcal{Q} : q^2 < 2\}$ is bounded, as it is contained in the interval $[-100, 100]$.

Definition 1.8 *M is an* **upper bound** *for the non-empty set E if*

$$x \leq M \quad \textit{for all } x \in E.$$

Definition 1.9 *L is the* **least upper bound** *for the non-empty set E if*

1. *L is an upper bound for E.*
2. *If M is any upper bound for E, $L \leq M$. That is, of all the upper bounds for E, L is the "smallest."*

We denote "L is the least upper bound for E" by

$$L = \text{l.u.b. } E$$

or

$$L = \sup E,$$

where sup is an abbreviation for the latin: "supremum".

Example 7 10 is an upper bound for $\{3, 6, 9\}$.

Example 8 23 is also an upper bound for $\{3, 6, 9\}$.

Example 9 $\sup\{3, 6, 9\} = 9$.

In the above examples, things are simple, because for a *finite* set E, $\sup E = \max E$.

Example 10 10 is an upper bound for $(0, 1)$.

Example 11 23 is also an upper bound for $(0, 1)$.

Example 12 1 is the *least* upper bound for $(0,1)$. That is, $\sup(0,1) = 1$.

This last example is the first non-obvious one. Certainly, 1 is an upper bound for $(0,1)$, since $(0,1) = \{x : 0 < x < 1\}$.[8] So property (1) of the definition of least upper bound is satisfied. To show property (2), we must show that if M is any upper bound for $(0,1)$, then $1 \leq M$. We claim that no number less than 1 can be an upper bound for $(0,1)$. Clearly if $x \leq 0$ then x cannot be an upper bound for $(0,1)$. If $0 < r < 1$ then $0 < r < \frac{1+r}{2} < 1$, which implies that r is not an upper bound for $(0,1)$. (Precisely why?) Since every number less than 1 is not an upper bound for $(0,1)$, then if M is an upper bound for $(0,1)$, then $M \geq 1$. This establishes property (2). It follows that 1 is the **least upper bound** for $(0,1)$, i.e.,

$$\sup(0,1) = 1.$$

More Examples

Example 13 $\sup(0,\infty)$ does not exist, because $(0,\infty)$ is not bounded above.

Example 14 $\sup\{0, 1/2, 2/3, 3/4, \ldots\} = 1$. The proof for this will have to wait until after we introduce the Axiom of Completeness.

Definition 1.10 *M is an* **lower bound** *for the non-empty set E if*

$$x \geq M \quad \textit{for all } x \in E.$$

Definition 1.11 *G is the* **greatest lower bound** *for the non-empty set E if*

1. *G is a lower bound for E.*
2. *If M is any lower bound for E, $G \geq M$, that is, of all the lower bounds for E, G is the "largest."*

We denote G is the greatest lower bound for E by

$$G = \text{g.l.b. } E$$

[8] The "set-builder" notation is defined and discussed in Section 1.7.

or

$$G = \inf E,$$

where inf is an abbreviation for the latin: "infimum".

Example 15 1 is an lower bound for $\{3, 6, 9\}$.

Example 16 -23 is also an lower bound for $\{3, 6, 9\}$.

Example 17 $\inf\{3, 6, 9\} = 3$.

In the above examples, things are simple, again because for a *finite* set E, $\inf E = \min E$.

Theorem 1.11 (Approximation Property for Suprema) *Let E be a non-empty set bounded above, and suppose there exists $s = \sup E$. Then for every $\epsilon > 0$ there is an element of E in the interval $(s - \epsilon, s]$.*

Proof: If $s \in E$, the theorem is trivially true. If $s \notin E$, suppose to the contrary that in the interval $(s - \epsilon, s)$ there is no element of E. Since $s \notin E$, $s - \epsilon$ is therefore also an upper bound for E, contradicting the hypothesis that s was the least.

Corollary 1.12 (Approximation Property for Infima) *Let E be a non-empty set bounded below, and suppose there exists $t = \inf E$. Then for every $\epsilon > 0$ there is an element of E in the interval $[t, t + \epsilon)$.*

Proof: See Exercise 31.

Definition 1.12 *Let $E \neq \emptyset$. Then $-E = \{-e : e \in E\}$.*

Exercise 24 Determine $\sup\{.3, .33, .333, .3333, \ldots\}$. No need for a proof at this time.

Exercise 25 A set E is bounded if and only if there exists an M so that $|x| \leq M$ for all $x \in E$.

Exercise 26 M is an upper bound for the set E if and only if $-M$ is a lower bound for the set $-E$.

Exercise 27 E is bounded above if and only if $-E$ is bounded below.

Exercise 28 E is bounded if and only if $-E$ is bounded.

Exercise 29 Is the empty set bounded? Proof?

Exercise 30 $\sup E = -\inf\{-E\}$. This shows that any result we obtain about sup's can be translanted to a result about inf's, and conversely.

Exercise 31 Prove the Approximation Property for Infima.

Exercise 32 Prove: $A \subseteq B \Longrightarrow \inf B \leq \inf A \leq \sup A \leq \sup B$, for A and B bounded, non-empty sets.

Exercise 33 a. $\sup[a,b] = \sup(a,b) = b$.

b. $\inf[a,b] = \inf(a,b) = a$.

Exercise 34 Let E be a non-empty set bounded above. Let $F = \{x : x$ is an upper bound for the set $E\}$. Suppose $\inf F$ and $\sup E$ exist. Prove: $\inf F = \sup E$.

1.5 Axiom of Completeness

We have one final axiom which we need to assume about $\mathcal{R}$, which will distinguish $\mathcal{R}$ from $\mathcal{Q}$, the ordered field of rational numbers. This property is called **completeness**. We shall see that it is an essential property of the real number system, one which allows us to conclude that Cauchy sequences converge, that the Intermediate Value Theorem is true, the Extremal properties for continuous functions, etc., a great variety of properties and theorems all of which are consequences of the completeness of the real number system.

Axiom of Completeness: Every non-empty set of real numbers E which is bounded above has a supremum.

The Axiom of Completeness cannot be proved, in the context of the real numbers. It must be assumed, which is what we do with all axioms. The Completeness Axiom is what distinguishes the real number field from the field of rational numbers, which is a subfield of the real numbers. The rational numbers presented some trouble to the ancient Greek mathematicians. They came to understand that there were lengths that could be constructed from rational numbers, but which themselves were not rational: They knew that the diagonal of a square of side length 1 was of a length which was not a rational number.[9]

The Greeks tried to operate within the field of rational numbers, but were led outside it (as we saw, with the construction of $\sqrt{2}$.) The Axiom of Completeness is just what we need to "complete" the real numbers. There will be no operations which lead us outside the real numbers. We shall see, later, that sequences which ought to converge, do converge. This is a property which is not shared by the rational numbers, as we shall also see.

We shall see some of the consequences of the Axiom of Completeness shortly, after we introduce the Natural Numbers.

Theorem 1.13 (Completeness Axiom: Version II) *Every non-empty set bounded below has an infimum.*

Proof: Let E be a non-empty set, bounded below, say by M. Then (see Exercise 30) $-E =$

[9]Here is the classic proof, due to the Greeks, that $\sqrt{2}$ is not rational: Suppose $\sqrt{2}$ were rational; then $\sqrt{2} = p/q$, for some integers p, q. After dividing out any common factors, we may assume that p and q contain no common factors. Then squaring both sides,

$$p^2 = 2q^2.$$

Then p^2 is an even number (because it is a multiple of 2), which implies that p is an even number (since the square of an odd number is odd), so

$$p = 2k$$

for some integer k, so

$$2q^2 = p^2 = (2k)^2 = 4k^2,$$

and after dividing both sides by 2,

$$q^2 = 2k^2$$

which implies that q must be even (reasoning as we did, above, with p). But that is a contradiction, because then p and q have a common factor, 2. So, there cannot be such a p and q, i.e. $\sqrt{2}$ is not rational.

$\{-e : e \in E\}$ is non-empty, and bounded above by $-M$. By the Axiom of Completeness, $-E$ has a least upper bound, say L. It is routine to verify then that $-L$ is the greatest lower bound for E.

Exercise 35 Give an alternate proof of the Completeness Axiom for inf's, based on the following ideas: Let E be a non-empty set bounded below by L.

a. Let $F = \{x \in \mathcal{R} : x \text{ is a lower bound for } E\}$. Prove $\sup F$ exists. Let $f = \sup F$.

b. Using the Approximation Property for sup's, prove that if $e \in E$ and $e < f$, then there exists $f' \in F$, $e < f'$, a contradiction. Conclude that f is a lower bound for E.

c. Prove: for any $\epsilon > 0$, $f + \epsilon$ is not a lower bound for E.

d. Prove $f = \sup F$ is the greatest lower bound for E, that is, $\inf E = \sup F$.

1.5.1 The Complete, Ordered Field

Now we have enumerated the axioms of the real numbers: they form a Complete, Ordered Field. These properties characterize the real numbers, in that it can be proved (usually in a more advanced course on this subject) that any complete ordered field is "equivalent" to the real numbers, in the sense that there will be a one-to-one correspondence between the elements of the real numbers and those of the other field, and that this correspondence will preserve the properties of "+" and "$*$", as well as the order properties.

1.6 Properties of $\mathcal{N}$, the Natural Numbers:

We start with the Peano axioms, from which all the properties of $\mathcal{N}$ can be derived. We are going to "axiomatize" the set of positive integers, which we also call the Natural Numbers. We denote this set by $\mathcal{N}$.

Let $\mathcal{N}$ be a non-empty set, with a 1-1 function[10] $s(n)$ (which we shall be thinking of as $s(n) = n + 1$ and called "the successor of n") defined on it, with the following properties:

[10]This is actually defined in the next section, as Definition 1.21. Since we need it here, you may take the definition of a 1-1 function f as "if $f(x) = f(y)$ then $x = y$."

1) There is an element (which we call "1") in $\mathcal{N}$ which is not in the *range* of $s(n)$.

2) For every subset $M \subset \mathcal{N}$, if M has the following two properties:

   (a) $1 \in M$.

   (b) For every $n \in \mathcal{N}$, $n \in M \Rightarrow s(n) \in M$ (a set M with this property (b) is called **inductive**.)

then $M = \mathcal{N}$.

Examples of Inductive Sets

Example 18 $M = \mathcal{N}$ is an inductive set, because $s(n) \in \mathcal{N}$ for every n.

Example 19 $M = \emptyset$ is an inductive, set, because no n is in M, so the hypothesis in (b) above is trivially satisfied.

Example 20 $M = \{3, 4, 5, 6, \ldots\}$ is an inductive set.

(2) above is usually called the **Axiom of Induction**, and we will make use of it thoughout the text. Here is an example of its use:

Theorem 1.14 *For any real number $a \geq -1$, and all positive integers n:*

$$(1 + a)^n \geq 1 + na.$$

Proof: Let $a \geq -1$ be fixed. Let M be the set of natural numbers for which the above formula holds, i.e.

$$M = \{n \in \mathcal{N} \ : (1 + a)^n \geq 1 + na\}.$$

Note that since

$$(1 + a)^1 = 1 + a,$$

$$1 \in M.$$

Now suppose $n \in M$ (this is often called the "induction hypothesis"). Then

$$\begin{aligned}(1+a)^{n+1} &= (1+a)(1+a)^n \\ &\geq (1+a)(1+na) \quad \text{by the Induction hypothesis} \\ &= 1+na+a+na^2 \\ &\geq 1+(n+1)a \quad \text{since } na^2 \text{ is positive}\end{aligned}$$

i.e. $n+1 \in M$. Then M is inductive. But then M satisfies properties 2(a) and 2(b), and therefore $M = \mathcal{N}$. That is, the formula holds for all positive integers n.[11]

In the above proof, note what we did: to prove that a certain property holds for every n, we form a set (M) of natural numbers for which the property holds, and then show two things: $1 \in M$, and M is inductive. Then from Peano Axiom 2 it follows that $M = \mathcal{N}$, i.e. that the property holds for *all* n.

Theorem 1.15 (Corollary to the Axiom of Induction: Well- ordering Principle for $\mathcal{N}$) *Every non-empty set E of natural numbers has a smallest element.*

Proof: If $1 \in E$, then 1 is the smallest element of E. We proceed by assuming that $1 \notin E$, i.e., $1 \in E^c$.[12] Now let S be the set defined by the following property:

$$n \in S \Longleftrightarrow \{1, 2, \ldots, n\} \subseteq E^c.$$

Clearly, $1 \in S$. Suppose S were inductive, i.e. suppose for every n, $n \in S$ implies $n+1 \in S$. Then by the Peano axioms, $S = \mathcal{N}$, i.e. every n is in E^c. But then E would be empty, a contradiction. So S cannot be inductive. That means that there is an $n \in S$, but $n+1 \notin S$. Then $\{1, 2, \ldots, n\} \subseteq E^c$, but $n+1 \notin E^c$. I.e., $k \notin E$, for $1 \leq k \leq n$, but $n+1 \in E$. Then $n+1$ is the smallest element of E. QED

Exercise 36 Prove by induction, that

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

[11] Where exactly did we use the hypothesis that $a \geq -1$?

[12] E^c, called "E-complement", is the set of all elements (in the universe, in this case $\mathcal{N}$,) which are NOT in the set E.

Exercise 37 Prove by induction, that

$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + \ldots + n)^2.$$

Hint: you will need to use the result from the preceding exercise.

Exercise 38 The following exercise illustrates a method for showing that a property holds for "all sufficiently large integers."

a. Which natural numbers are in the set $A = \{k \in \mathcal{N} \ : k^2 < 2^k\}$? Why is A not inductive? Explain carefully.

b. It is true, however, that A contains all natural numbers larger than a certain N_0. What is N_0?

c. Prove that A is "almost inductive", i.e. that A has the property that

$$(\forall k \geq N_0)[k \in A \Longrightarrow k + 1 \in A]. \tag{1.5}$$

[Hint: you will need to show that a certain other set is inductive to do this.]

Exercise 39 Prove that $k^2 > 2k + 1$ if $k \geq 3$.

Exercise 40 Prove that $I = \{n : n^2 + n + 1 \text{ is even}\}$ is an inductive set. Is it true that $I = \mathcal{N}$? Explain.

Exercise 41 Prove the following Principle of "Strong" Induction:
Suppose M is a subset of $\mathcal{N}$, with the following properties:

1) $1 \in M$.

2) For every $n \in \mathcal{N}$, $\{1, 2, \ldots, n\} \subset M \Longrightarrow n + 1 \in M$.

Then $M = \mathcal{N}$.

(Hint: If $M \neq \mathcal{N}$, then $E = M^c$ is not empty. Apply the Well-Ordering principle to E to get a contradiction to 2).)

Theorem 1.16 *$\mathcal{N}$ is not bounded above.*

Proof: Suppose not[13]. Then there exists an M such that if $n \in \mathcal{N}$, then

$$n \leq M.$$

By the Completeness Axiom, since $\mathcal{N}$ is bounded above, $s = \sup \mathcal{N}$ exists. Since s is the least upper bound for $\mathcal{N}$, $s - 1/2$ is not an upper bound for $\mathcal{N}$. That is, there is an $n \in \mathcal{N}$ such that $s - 1 < n$. But then $s < n + 1$, which contradicts the fact that s was an upper bound for $\mathcal{N}$. QED.

Theorem 1.17 (Archimedean Property for $\mathcal{R}$) *For any $\epsilon > 0$ there exists $n \in \mathcal{N}$ such that $1/n < \epsilon$.*

Proof: $\epsilon > 0$ implies $1/\epsilon > 0$. Since $\mathcal{N}$ is not bounded above, there exists an $n \in \mathcal{N}$ such that $1/\epsilon < n$. Then $1/n < \epsilon$.

Theorem 1.18 (Second Archimedean Property for $\mathcal{R}$) *For any real numbers a and b such that $0 < a < b$ there exists $n \in \mathcal{N}$ such that*

$$na > b.$$

(Homely version: an arbitrarily large bathtub can be bailed out by an arbitarily small teaspooon.[14])

Proof: Let $\epsilon = a/b$. By the first Archimedean property, there is an n so that

$$1/n < a/b,$$

i.e.

$$na > b.$$

QED

Theorem 1.19 (The Rational Numbers are Dense in the Real Numbers) *For any real numbers a, b, if $a < b$ then there exists a $q \in \mathcal{Q}$ such that*

$$a < q < b.$$

[13]What kind of proof, i.e. what form, do you expect this to be?

[14]Identify which of a, b, n is the teaspoon, and which is the bathtub. What role does n play?

Proof: Case I: $0 \leq a < b$. Apply the Archimedean Property to $\epsilon = b - a$. Then there exists an $n \in \mathcal{N}$ such that

$$0 < 1/n < b - a.$$

Then

$$1 < nb - na,$$

[At this point, the idea is that since nb and na are more than 1 apart, then there is an integer strictly between them. The remainder of the proof establishes this.]

Since $\mathcal{N}$ is unbounded above, na is not an upper bound for $\mathcal{N}$, and hence $\{m \in \mathcal{N} : m > na\}$ is not empty. It therefore has a least element by the well-ordering property, call it m_0. Then $m_0 > na$. If $m_0 \geq nb$, then

$$m_0 - 1 \geq nb - 1 > na,$$

contradicting the fact that m_0 was the least such. Hence

$$na < m_0 < nb.$$

Then

$$a < m_0/n < b$$

and m_0/n is our desired rational number.

Case II: $a < 0 < b$. Then 0 is the desired rational.

Case III: $a < b \leq 0$. Then consider $0 \leq -b < -a$, apply Case I, find the rational number q such that $-b < q < -a$. Then $-q$ is rational, and $a < -q < b$. QED

Examples Using the Axiom of Completeness

Example 21 Consider the set

$$E = \{q \in \mathcal{Q} : q^2 < 2\}.$$

This set is bounded above, because 1.5 is an upper bound for E. (proof?) The set is not empty (why?). Then by the Axiom of Completeness, $\sup E$ exists. Actually, we will show that $\sup E = \sqrt{2}$. To see this we need to show two things:

(1) $\sqrt{2}$ is an upper bound for E.

(2) If M is any upper bound for E, then $\sqrt{2} \leq M$.

To establish (1), note[15] that $0 < q^2 < 2 \Longrightarrow 0 < \sqrt{q^2} < \sqrt{2}$, so that $q \in E \Longrightarrow q < \sqrt{2}$.

To establish (2), let $M < \sqrt{2}$. Then by the density of the rational numbers, there is a $q \in \mathcal{Q}$ so that

$$M < q < \sqrt{2},$$

or

$$q^2 < 2$$

which implies

$$q \in E.$$

But then M cannot be an upper bound for E since $M < q$. This establishes (2).[16]

Example 22 Let $E = \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots\}$. Then

$$\sup E = 1.$$

To see this, we reason as we did above:
Clearly 1 is an upper bound for E. If $r < 1$, by the Archimedean property there exists an $n \in \mathcal{N}$ such that $1/n < 1 - r$. Then

$$r < 1 - 1/n = \frac{n-1}{n} \in E,$$

i.e. r is not an upper bound for E. Therefore, 1 is the *least* upper bound for E, i.e. $\sup E = 1$.

Exercise 42 Prove the density of the irrationals: For all real numbers a, b where $a < b$, there exists an irrational c such that $a < c < b$. (Hint: the product of a rational and an irrational is irrational).

---

[15] We prove this in Section 17.

[16] We are using the form of proof:

$$p \Longrightarrow q$$

is equivalent to

$$\neg q \Longrightarrow \neg p.$$

Exercise 43 Prove: if E is bounded and non-empty, and $s = \sup E \notin E$, then for every $\epsilon > 0$, there exist $x, y \in E$ such that $0 < |x - y| < \epsilon$.

Exercise 44 Give an example of a bounded, non-empty set E such that the property in Problem 43 above does not hold.

1.7 Sets, Relations, Functions

Definition 1.13 *A* **set** *is a collection of elements, usually here, real numbers, or natural numbers.*

We occasionally use the "set-builder" notation, where a set is defined by some property $P(x)$,

$$A = \{x \in \mathcal{R} : P(x)\}.$$

For example:

$$A = \{x \in \mathcal{R} : x^2 \leq 1\}$$

is way of defining the set A as the collection of all real numbers whose square is less than or equal to 1, i.e.

$$A = [-1, 1].$$

Why would we use the set-builder notation when we have a simpler way of defining the set A? It is because the property $P(x)$ which characterizes the elements of A may not be so simple, as, for example, $A = \{x \in \mathcal{R} : x^3 + x^2 - 3x \leq 1\}$.

We say "A is a subset of B", and write

$$A \subset B$$

if every element of A is also an element of B, i.e.

$$\forall x[x \in A \Longrightarrow x \in B].$$

$A = B$ if and only if $A \subset B$ and $B \subset A$, that is, two sets are equal if and only if they have precisely the same elements:

$$\forall x[x \in A \Longleftrightarrow x \in B].$$

$\emptyset$ will be the symbol for "the empty set", the set which consists of no elements.[17]

Definition 1.14 *The* **cartesian product** *of two sets A and B, denoted $A \times B$, is the set of all ordered pairs of the form (a, b), where a is an element of A, and B is an element of B:*

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

Definition 1.15 *A* **relation** *R on a set A is a subset of $A \times A$.*

Example 23 The relation $L =$ " $<$" on $\mathcal{R}$ is the subset of $\mathcal{R} \times \mathcal{R}$:

$$L = \{(x, y) : x < y\},$$

which is the set in the cartesian plane of all points which lie *above* the principal diagonal: $y = x$.

Thus, for example, $(1, 3) \in L$ and $(2, 5) \in L$ but $(6, 4) \notin L$.

Definition 1.16 *An* **equivalence relation** *R* **on a set** *A is a relation R on a set A with three properties:*

a. For every $a \in A$, aRa. [Reflexivity]

b. For every $a, b \in A$, $aRb \Longrightarrow bRa$. [Symmetry]

c. For every a, b, and $c \in A$, aRb and bRc imply aRc. [Transitivity]

Exercise 45 Prove that the relation "aRb if and only if $b - a$ is a multiple of 9" is an equivalence relation on $\mathcal{N}$.

[17]The careful reader will have noted that by use of the word "the" when attached to "empty set", we are presuming that there are not possibly two different empty sets. This follows from the property above that two sets are the same (equal) if they have exactly the same elements. Thus, two empty sets are the same, because they have exactly the same elements.

Definition 1.17 *A* **function** $f : A \to B$ *is a subset of* $A \times B$ *with the following properties:*

a. *For every* $a \in A$ *there exists a* $b \in B$ *such that*

$$(a, b) \in f.$$

b. *If* $(a, b_1) \in f$ *and* $(a, b_2) \in f$ *then* $b_1 = b_2$. *(This expresses the single-valuedness of the function.)*

We shall also use the word **mapping** interchangeably for the name "function", especially as in "f is a mapping from A to B."

Definition 1.18 *The* **range** *of* f *is the collection of elements of* B *that are images of elements of* A*:*

$$\textbf{range } of\ f\ = \{b \in B : (\exists a)[(a, b) \in f]\}.$$

Definition 1.19 *The* **domain** *of* f *is the collection of elements of* A.

$$\textbf{domain } of\ f\ = \{a \in A : (\exists b)[(a, b) \in f]\}.$$

Definition 1.20 *A function* $f : A \to B$ *is called* **"onto"** *or "onto* B*" (and denoted* $f : A \overset{\text{onto}}{\to} B$*) if every element of* B *is in the range of* f*:*

$$(\forall b \in B)(\exists a \in A)(a, b) \in f.$$

Definition 1.21 *A function* f *is called* **one-to-one**, *denoted "*$1 - 1$*", if*

$$f(x) = f(y) \Longrightarrow x = y,$$

i.e. two different elements in the domain of f *do not correspond to the same element in the range.*

Definition 1.22 *Let* f *be a function,* $f : A \to B$. *The* **inverse of f**, *denoted* f^{-1}, *is the set*

$$f^{-1} = \{(b, a) : (a, b) \in f\}.$$

Theorem 1.20 *If* f *is a 1-1 function from* A *onto* B, *then the inverse of* f *is a 1-1 function from* B *onto* A.

Proof: See Exercise 48.

Exercise 46 Let $A = \{a, b, c\}, \quad B = \{0, 1\}$. Compute $A \times B$. Construct and exhibit a function $f : A \to B$. Can you construct a function from A into B which is 1-1? Why (or why not)?

Exercise 47 The function $f(x) = x^2$ does not have an inverse as yet, as we have defined it, because x^2 is not one-to-one, at least on the domain which is "understood", namely $(-\infty, \infty)$. However, if we restrict the domain of f to $[0, \infty)$, it is easy to see that in this case x^2 is a one-to-one function, so an inverse is possible to define. The inverse of x^2:

$$f^{-1} = \{(x^2, x) : x \in [0, \infty)\} = \{(y, \sqrt{y}) : y \in [0, \infty)\}$$

from which it is seen that the inverse to x^2 is the function $\sqrt{x}$. Verify that $\sqrt{x}$ is a 1-1 function on $[0, \infty)$.

Exercise 48 Prove Theorem 1.20.

Exercise 49 Define the relation between sets: $A \equiv B$ if and only if there exists a function $f : A \to B$ which is 1-1 and onto. Then prove that $\equiv$ is an equivalence relation on the class of all sets.

1.8 Cardinality: Countable and Uncountable Sets

Definition 1.23 *Two sets A and B are called* **cardinally equivalent** *if there exists a function $f : A \to B$ which is both 1-1 and onto.*

Informally, we think of A and B being of the "same size" when they are cardinally equivalent.[18]

[18] Cardinal equivalence is an equivalence relation on the class of all sets. The Fundamental Theorem of Equivalence Relations states that an equivalence relation on a set A partitions A into disjoint subsets called "equivalence classes". Bertrand Russell defined "cardinal number" as the equivalence class of all sets which are "equivalent" under this equivalence relation. The cardinal number "3" was then the equivalence class consisting of all sets with exactly three elements. The equivalence class "3" then embodied the property of "three-ness".

Definition 1.24 *A set A is called* **finite** *if there exists an $n \in \mathcal{N}$ and a 1-1 function f whose domain is A and whose range is contained in the set $\{1, 2, \ldots, n\}$, for some $n \in \mathcal{N}$. Note: this allows the empty set to be finite.*

(Equivalently: the finite sets are the ones which are either empty, or cardinally equivalent to the initial segments $\{1, 2, \ldots, n\}$ of the natural numbers.)

Definition 1.25 *A set A which is not finite is called* **infinite**.

There are two different kinds of infinite sets:

Definition 1.26 *An infinite set A which is cardinally equivalent to $\mathcal{N}$ is called* **countably infinite** *or* **denumerable**. *A set which is either denumerable or finite will be called* **countable**.

Definition 1.27 *An infinite set which is not countably infinite is called* **uncountable**.

Theorem 1.21 (Cantor's Diagonalization Theorem) *The real numbers in $(0, 1)$ are uncountable.*

Proof: Let $A = (0, 1)$. Suppose instead that A were countable. Then there would exist a 1-1 function $g : \mathcal{N} \overset{\text{onto}}{\to} A$. We list the range of g, as follows:

$$g(1) = 0.a_{11}a_{12}a_{13}\ldots$$
$$g(2) = 0.a_{21}a_{22}a_{23}\ldots$$
$$g(3) = 0.a_{31}a_{32}a_{33}\ldots$$
$$\ldots$$

where the a's are the decimal expansions of the elements of A which are so enumerated by the function g.

We now construct a number $b \in (0, 1)$ such that $b \notin \text{range}(g)$, a contradiction.

Define a sequence $\{b_1, b_2, \ldots\}$ by

$$b_k = \begin{cases} 5 \text{ if } a_{kk} = 6 \\ 6 \text{ if } a_{kk} \neq 6 \end{cases}$$

Note that $b_k \neq a_{kk}$, for each $k = 1, 2, \ldots$.

Now consider the number

$$b = 0.b_1b_2b_3\ldots = \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{b_3}{10^3} + \ldots .$$

Clearly, $0.5 < b < 0.7$, so $b \in (0, 1)$. But b was constructed so that b *disagrees* with each element in the range of g: If $b = g(k)$ for some k,

$$g(k) = 0.a_{k1}a_{k2}a_{k3}\ldots$$

then $b_k \neq a_{kk}$, so $b \neq g(k)$ after all! This contradicts the assumption that A is a countably infinite set, hence A is uncountable.

The Cantor Diagonal Argument has been applied in areas of mathematics as diverse from Real Analysis as to prove that The Halting Problem is recursively unsolvable[19], and to prove Godel's Incompleteness Theorem, that no system of logic sufficiently powerful to express "arithmetic" of natural numbers (e.g. what it is to be a prime number, multiplication, etc.) can express in an algorithmic way all the provable sentences (i.e. the "Theorems") and only the provable sentences. (More precisely, the set of provable sentences in "formal logic" is a recursively enumerable, not recursive[20].) set.)

Theorem 1.22 *A subset of a countably infinite set is either countably infinite or finite.*

Proof: Suppose $A \subset B$, B countably infinite, and A is not finite. We prove A is countably infinite by induction:

Since B was assumed countably infinite, there exists a 1-1 function $g : \mathcal{N} \overset{\text{onto}}{\to} B$. Let

$$b_k = g(k), \quad k = 1, 2, \ldots$$

and we construct the mapping: $\mathcal{N} \to A$ by choosing in order, $k = 1, 2, \ldots$, those b_k which are in A as well. Here are the details:

Consider the set

$$E = \{k \in \mathcal{N} : b_k \in A\}$$

[19]There is no computer program that can decide, for every computer program, and each possible input to the program, whether or not that program with that input will ever terminate.

[20]Cf, Martin Davis, Computability and Unsolvability, McGraw-Hill, New York, 1958.

which is a non-empty set of natural numbers (since A is assumed not finite.) By the Well-Ordering Principle, the set has a least element, call it j_1. Now suppose that

$$j_1 < j_2 < \ldots < j_n$$

have been chosen so that

$$b_{j_k} \in A, \quad k = 1, 2, \ldots, n$$

and for any m, $1 \leq m \leq j_n$, if $m \notin \{j_1, j_2, \ldots, j_n\}$, then $b_m \notin A$.

Now consider

$$\{k > j_n : b_k \in A\}$$

which is non-empty, because A was infinite, and which also has a least element by the Well-Ordering Principle. Call it j_{n+1}. Then $b_{j_{n+1}} \in A$.

Thus we have constructed a sequence

$$j_1 < j_2 < \ldots$$

such that $b_{j_k} \in A$ for every k, and $b_m \notin A$ if $m \notin \{j_1, j_2, \ldots\}$.

Let $f : \mathcal{N} \to A$ be defined by

$$f(n) = b_{j_n}.$$

It follows[21] that f is 1-1 and onto A, proving that A is a countable set.

Corollary 1.23 *: The real numbers, $\mathcal{R}$, are an uncountable set.*

Proof: $(0, 1) \subset \mathcal{R}$.

Theorem 1.24 *The union of countably infinitely many countably infinite sets is countably infinite. (Colloquially: the denumerable union of denumerable sets is denumerable.)*

Proof: Suppose $A_1, A_2, \ldots$ are the countably infinite sets. In light of the previous theorem, we may assume that all the A_i's are disjoint, for if not, extending them to be disjoint sets only increases the number of elements in their union.[22]

[21] Provide the details. See Exercise 54.

[22] This extension could be accomplished, for example, by replacing the set A_i by the new set

$$A_i' = A_i \times i = \{(a, i) : a \in A_i\}.$$

To prove that

$$B = \cup_{i=1}^{\infty} A_i$$

is countably infinite, it suffices to find an "enumerating function" $f : \mathcal{N} \to B$ which is 1-1 and onto. This will be accomplished if we find a way of "listing" all the elements of all the A_i's. What we need is a function which provides a mapping from $\mathcal{N}$ to $\mathcal{N} \times \mathcal{N}$ which is itself 1-1 and onto. Once we have this, the remainder of the construction is quite easy.

For the moment, however, let us enumerate each of the A_i, as follows:

$$A_1 = \{a_{11}, a_{12}, a_{13}, \ldots\}$$
$$A_2 = \{a_{21}, a_{22}, a_{23}, \ldots\}$$
$$A_3 = \{a_{31}, a_{32}, a_{33}, \ldots\}$$
$$\ldots$$

To be more specific, since each A_k was assumed to be countably infinite, there exists a $g_k : \mathcal{N} \to A_k$ which is 1-1 and onto. Then let $a_{k,j} = g_k(j)$, $j = 1, 2, \ldots$.

Lemma 1.25 *: There is a function $h : \mathcal{N} \to \mathcal{N} \times \mathcal{N}$ which is 1-1 and onto.*

Proof: Let m be any positive integer. Then m can be written as a power of 2 times an *odd* integer, and in only one way:

$$m = 2^{r-1}(2s - 1), \quad \text{where } r \geq 1 \text{ and } s \geq 1.$$

Now define $h(m) = (r, s)$, and observe that $h^{-1}(r, s) = 2^{r-1}(2s-1)$ is a 1-1 onto function: $\mathcal{N} \times \mathcal{N} \to \mathcal{N}$. It follows that h is the desired mapping.

To complete the proof of the theorem, define $f : \mathcal{N} \to B$ as follows:

$$f(m) = g_r(s)$$

where $h(m) = (r, s)$. Since $g_r(s) = g_{r'}(s')$ if and only if $r = r'$ and $s = s'$ it follows that f is 1-1 because h is.

Then

$$A'_i \cap A'_j = \emptyset \text{ if } i \neq j$$

since $(a, i) \neq (a, j)$ if $i \neq j$.

Now, let $x \in \cup A_i$. Then $x \in A_k$ for some k. Then $x = g_k(l)$ for some l, and hence $x = f(2^{k-1}(2l-1))$, which shows that f is onto.

Corollary 1.26 *The finite union of countably infinite sets is countably infinite.*

Proof: This follows from Theorem 1.22, when we recognize that the finite union of countably infinite sets can be identified with a subset of the countably infinite union of countably infinite sets.

Corollary 1.27 *The countably infinite or finite union of countably infinite or finite sets is countably infinite or finite.*

Proof: Suppose the sets are $A_1, A_2, \ldots$. If the number of A_i is finite, say $i = 1, 2, \ldots, n$, then let $A_k = \{(1, k)\}$ for $k > n$. In light of Theorem 1.22 we may now assume that the number of A_k is countably infinite.

If any A_k is a finite set, say $A_k = \{a_{k1}, \ldots, a_{kn}\}$, then extend A_k to an infinite set $A'_k = \{a_{k1}, \ldots, a_{kn}, (k, n+1), (k, n+2), \ldots\}$ and again in light of Theorem 1.22 we may assume that A_k is a countably infinite set.

Since the countably infinite union of countably infinite sets is countably infinite, the result follows.

Corollary 1.28 *The set $\mathcal{Z}$ of all integers, positive or negative, or 0, is a countably infinite set.*

Proof: $\mathcal{Z}$ can be identified as the union of three sets, a copy of the positive integers, a copy of the negative integers, and the set consisting of 0. It follows from the previous corollary that $\mathcal{Z}$ is countably infinite.

Corollary 1.29 *The set $\mathcal{Q}$ of all rational numbers is countably infinite.*

Proof: The set $\mathcal{Q}$ can be written as the union of three sets, the positive rationals, the negative rationals, and the set consisting of 0. $\mathcal{Q}^+$, the positive rationals, can be identified as a subset of the set of all ordered pairs of natural numbers: (m, n). Identify (m, n) with the rational number m/n, and observe that $(2m, 2n)$ is also identified with the same rational

number. Thus, $\mathcal{Q}^+$ can be identified with a subset of $\mathcal{N} \times \mathcal{N}$, and hence by the previous remarks in the previous corollaries, is a countably infinite set. The rest of the proof follows as in the case of $\mathcal{Z}$.

Exercise 50 Without using Corollary 1.28, prove directly from the definition that $\mathcal{Z}$ is a countable set.

Exercise 51 Construct a function $f : \mathcal{R} \to \mathcal{R}\backslash^{23}\{0\}$ which is 1-1 and onto.

Exercise 52 Construct a function $f : \mathcal{R} \to \mathcal{R}\backslash\mathcal{N}$ which is 1-1 and onto.

Exercise 53 Construct a function $f : (0, 1) \to \mathcal{R}$ which is 1-1 and onto.

Exercise 54 Complete the proof of Theorem 1.22 by performing the following steps:

a. Prove that $j_k = j(k), \quad k = 1, 2, \ldots$ is a 1-1 function.

b. Conclude that f is therefore 1-1.

c. Prove that f is onto A.

[23] $A\backslash B$ is the set $A \cap B^c$.