Chapter 1

The Real Numbers

This course has two goals: (1) to develop the foundations that underlie calculus and all of post calculus mathematics, and (2) to develop students' ability to understand definitions and proofs and to create proofs of their own – that is, to develop students' *mathematical sophistication*.

The typical freshman and sophomore calculus courses are designed to teach the techniques needed to solve problems using calculus. They are not primarily concerned with proving that these techniques work or teaching why they work. The key theorems of calculus are not really proved, although sometimes proofs are given which rely on other reasonable, but unproved assumptions. Here we will give rigorous proofs of the main theorems of calculus. To do this requires a solid understanding of the real number system and its properties. This first chapter is devoted to developing such an understanding.

Our study of the real number system will follow the historical development of numbers: We first discuss the natural numbers or counting numbers (the positive integers), then the integers, followed by the rational numbers. Finally, we discuss the real number system and the property that sets it apart from the rational number system – the completeness property. The completeness property is the missing ingredient in most calculus courses. It is seldom discussed, but without it, one cannot prove the main theorems of calculus.

The natural numbers can be defined as a set satisfying a very simple list of axioms – Peano's axioms. All of the properties of the natural numbers can be proved using these axioms. Once this is done, the integers, the rational numbers, and the real numbers can be constructed and their properties proved rigorously. To actually carry this out would make for an interesting, but rather tedious course. Fortunately, that is not the purpose of this course. We will not give a rigorous construction of the real number system beginning with Peano's axioms, although we will give a brief outline of how this is done. However, the main purpose of this chapter is to state the properties that characterize the real number system and develop some facility at using them in proofs. The rest of the course will be devoted to using these properties to develop rigorous proofs of the main theorems of calculus.

1.1 Sets and Functions

We precede our study of the real numbers with a brief introduction to sets and functions and their properties. This will give us the opportunity to introduce the set theory notation and terminology that will be used throughout the text.

Sets

A *set* is a collection of objects. These objects are called the *elements* of the set. If x is an element of the set A, then we will also say that x *belongs* to A or x is *in* A. A shorthand notation for this statement that we will use extensively is

$$x \in A.$$

Two sets A and B are the same set if they have the same elements – that is, if every element of A is also an element of B and every element of B is also an element of A. In this case, we write $A = B$.

One way to define a set is to simply list its elements. For example, the statement

$$A = \{1, 2, 3, 4\}$$

defines a set A which has as elements the integers from 1 to 4.

Another way to define a set is to begin with a known set A and define a new set B to be all elements $x \in A$ that satisfy a certain condition $Q(x)$. The condition $Q(x)$ is a statement about the element x which may be true for some values of x and false for others. We will denote the set defined by this condition as follows:

$$B = \{x \in A : Q(x)\}.$$

This is mathematical shorthand for the statement "B is the set of all x in A such that $Q(x)$". For example, if A is the set of all students in this class, then we might define a set B to be the set of all students in this class who are sophomores. In this case, $Q(x)$ is the statement "x is a sophomore". The set B is then defined by

$$B = \{x \in A : x \text{ is a sophomore}\}.$$

Example 1.1.1. Describe the set $(0, 3)$ of all real numbers greater than 0 and less than 3 using set notation.

Solution: In this case the statement $Q(x)$ is the statement "$0 < x < 3$". Thus,

$$(0, 3) = \{x \in \mathbb{R} : 0 < x < 3\}.$$

A set B is a *subset* of a set A if B consists of some of the elements of A – that is, if each element of B is also an element of A. In this case, we use the shorthand notation

$$B \subset A.$$

Of course, A is a subset of itself. We say B is a *proper* subset of A if $B \subset A$ and $B \neq A$.

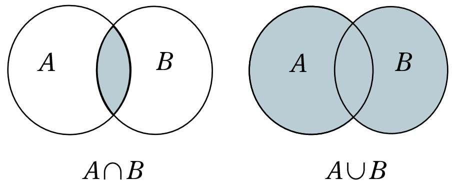

Figure 1.1: Intersection and Union of Two Sets.

For example, the open interval $(0,3)$ of the preceding example is a proper subset of the set $\mathbb{R}$ of real numbers . It is also a proper subset of the half open interval $(0,3]$ – that is, $(0,3) \subset (0,3]$, but the two are not equal because the second contains 3 and the first does not.

There is one special set that is a subset of every set. This is the empty set $\emptyset$. It is the set with no elements. Since it has no elements, the statement that "each of its elements is also an element of A" is true no matter what the set A is. Thus, by the definition of subset,

$$\emptyset \subset A$$

for every set A.

If A and B are sets, then the *intersection* of A and B, denoted $A \cap B$, is the set of all objects that are elements of A and of B. That is,

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

Similarly, the *union* of A and B, denoted $A \cup B$, is the set of objects which are elements of A or elements of B (possibly elements of both). That is,

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

Example 1.1.2. If A is the closed interval $[-1,3]$ and B is the open interval $(1,5)$, describe $A \cap B$ and $A \cup B$.

Solution: $A \cap B = (1,3]$ and $A \cup B = [-1,5)$.

If $\mathcal{A}$ is a (possibly infinite) collection of sets, then the intersection and union of the sets in $\mathcal{A}$ are defined to be

$$\bigcap \mathcal{A} = \{x : x \in A \text{ for all } A \in \mathcal{A}\}$$

and

$$\bigcup \mathcal{A} = \{x : x \in A \text{ for some } A \in \mathcal{A}\}.$$

Note how crucial the distinction between "for all' and "for some' is in these definitions.

The intersection $\bigcap \mathcal{A}$ is also often denoted

$$\bigcap_{A \in \mathcal{A}} A \quad \text{or} \quad \bigcap_{s \in S} A_s$$

if the sets in $\mathcal{A}$ are indexed by some index set S. Similar notation is often used for the union.

Example 1.1.3. If $\mathcal{A}$ is the collection of all intervals of the form $[s,2]$ where $0 < s < 1$, find $\bigcap \mathcal{A}$ and $\bigcup \mathcal{A}$.

Solution: A number x is in the set

$$\bigcap \mathcal{A} = \bigcap_{s \in (0,1)} [s,2]$$

if and only if

$$s \le x \le 2 \quad \text{for every positive } s < 1. \tag{1.1.1}$$

Clearly every x in the interval $[1,2]$ satisfies this condition. We will show that no points outside this interval satisfy (1.1.1).

Certainly an $x > 2$ does not satisfy (1.1.1). If $x < 1$, then $s = x/2 + 1/2$ (the midpoint between x and 1) is a number less than 1 but greater than x, and so such an x also fails to satisfy (1.1.1). This proves that

$$\bigcap \mathcal{A} = [1,2].$$

A number x is in the set

$$\bigcup \mathcal{A} = \bigcup_{s \in (0,1)} [s,2]$$

if and only if

$$s \le x \le 2 \quad \text{for some positive } s < 1. \tag{1.1.2}$$

Every such x is in the interval $(0,2]$. Conversely, we will show that every x in this interval satisfies (1.1.2). In fact, if $x \in [1,2]$, then x satisfies (1.1.2) for every $s < 1$. If $x \in (0,1)$, then x satisfies 1.1.2 for $s = x/2$. This proves that

$$\bigcup \mathcal{A} = (0,2].$$

If $B \subset A$, then the set of all elements of A which are not elements of B is called the *complement* of B in A. This is denoted $A \setminus B$. Thus,

$$A \setminus B = \{x \in A : x \notin B\}.$$

Here, of course, the notation $x \notin B$ is shorthand for the statement "x is not an element of B".

If all the sets in a given discussion are understood to be subsets of a given *universal* set X, then we may use the notation B^c for $X \setminus B$ and call it simply the *complement* of B. This will often be the case in this course, with the universal set being the set $\mathbb{R}$ of real numbers or, in later chapters, real n dimensional space $\mathbb{R}^n$ for some n.

Example 1.1.4. If A is the interval $[-2,2]$ and B is the interval $[0,1]$, describe $A \setminus B$ and the complement B^c of B in $\mathbb{R}$.

Solution: We have

$$A \setminus B = [-2,0) \cup (1,2] = \{x \in \mathbb{R} : -2 \leq x < 0 \text{ or } 1 < x \leq 2\},$$

while

$$B^c = (-\infty, 0) \cup (1, \infty) = \{x \in \mathbb{R} : x < 0 \text{ or } 1 < x\}.$$

Theorem 1.1.5. *If A and B are subsets of a set X and A^c and B^c are their complements in X. then*

(a) $(A \cup B)^c = A^c \cap B^c$; *and*

(b) $(A \cap B)^c = A^c \cup B^c$.

Proof. We prove (a) first. To show that two sets are equal, we must show that they have the same elements. An element of X belongs to $(A \cup B)^c$ if and only if it is not in $A \cup B$. This is true if and only if it is not in A and it is not in B. By definition this is true if and only if $x \in A^c \cap B^c$. Thus, $(A \cup B)^c$ and $A^c \cap B^c$ have the same elements and, hence, are the same set.

If we apply part (a) with A and B replaced by A^c and B^c and use the fact that $(A^c)^c = A$ and $(B^c)^c = B$, the result is

$$(A^c \cup B^c)^c = A \cap B.$$

Part (b) then follows if we take the complement of both sides of this identity. □

A statement analogous to Theorem 1.1.5 is true for unions and intersections of collections of sets (Exercise 1.1.7).

Two sets A and B are said to be *disjoint* if $A \cap B = \emptyset$. That is, they are disjoint if they have no elements in common. A collection $\mathcal{A}$ of sets is called a *pairwise disjoint* collection if $A \cap B = \emptyset$ for each pair A, B of distinct sets in $\mathcal{A}$.

Functions

A *function* f from a set A to a set B is a rule which assigns to each element $x \in A$ exactly one element $f(x) \in B$. The element $f(x)$ is called the image of x under f or the value of f at x. We will write

$$f : A \to B$$

to indicate that f is a function from A to B. The set A is called the *domain* of f. If E is any subset of A then we write

$$f(E) = \{f(x) : x \in E\}$$

and call $f(E)$ the *image* of E under f.

We don't assume that every element of B is the image of some element of A. The set of elements of B which are images of elements of A is $f(A)$ and is called the *range* of f. If every element of B is the image of some element of A (so that the range of f is B), then we say that f is *onto*.

A function $f : A \to B$ is is said to be *one-to-one* if, whenever $x, y \in A$ and $x \neq y$, then $f(x) \neq f(y)$ – that is, if f takes distinct points to distinct points.

If $g : A \to B$ and $f : B \to C$ are functions, then there is a function $f \circ g : A \to C$, called the *composition* of f and g, defined by

$$f \circ g(x) = f(g(x)).$$

Since $g(x) \in B$ and the domain of f is B, this definition makes sense.

If $f : A \to B$ is a function and $E \subset B$, then the *inverse image* of E under f is the set

$$f^{-1}(E) = \{x \in A : f(x) \in E\}.$$

That is, $f^{-1}(E)$ is the set of all elements of A whose images under f belong to E.

Inverse image behaves very well with respect to the set theory operations, as the following theorem shows.

Theorem 1.1.6. *If $f : A \to B$ is a function and E and F are subsets of B, then*

(a) $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$;

(b) $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$; *and*

(c) $f^{-1}(E \setminus F) = f^{-1}(E) \setminus f^{-1}(F)$ *if* $F \subset E$.

Proof. We will prove (a) and leave the other two parts to the exercises.

To prove (a), we will show that $f^{-1}(E \cup F)$ and $f^{-1}(E) \cup f^{-1}(F)$ have the same elements. If $x \in f^{-1}(E \cup F)$, then $f(x) \in E \cup F$. This means that $f(x)$ is in E or in F. If it is in E, then $x \in f^{-1}(E)$. If it is in F, then $x \in f^{-1}(F)$. In either case, $x \in f^{-1}(E) \cup f^{-1}(F)$. This proves that every element of $f^{-1}(E \cup F)$ is an element of $f^{-1}(E) \cup f^{-1}(F)$.

On the other hand, if $x \in f^{-1}(E) \cup f^{-1}(F)$, then $x \in f^{-1}(E)$, in which case $f(x) \in E$, or $x \in f^{-1}(F)$, in which case $f(x) \in F$. In either case, $f(x) \in E \cup F$, which implies $x \in f^{-1}(E \cup F)$. This proves that every element of $f^{-1}(E) \cup f^{-1}(F)$ is also an element of $f^{-1}(E \cup F)$. Combined with the previous paragraph, this proves that the two sets are equal. □

Image does not behave as well as inverse image with respect the set operations. The best we can say is the following:

Theorem 1.1.7. *If $f : A \to B$ is a function and E and F are subsets of A, then*

(a) $f(E \cup F) = f(E) \cup f(F)$;

(b) $f(E \cap F) \subset f(E) \cap f(F)$;

(c) $f(E) \setminus f(F) \subset f(E \setminus F)$ *if* $F \subset E$.

Proof. We will prove (c) and leave the others to the exercises.

To prove (c), we must show that each element of $f(E) \setminus f(F)$ is also an element of $f(E \setminus F)$. If $y \in f(E) \setminus f(F)$, then $y = f(x)$ for some $x \in E$ and y is not the image of any element of F. In particular, $x \notin F$. This means that $x \in E \setminus F$ and so $y \in f(E \setminus F)$. This completes the proof. □

The above theorem cannot be improved. That is, it is not in general true that $f(E \cap F) = f(E) \cap f(F)$ or that $f(E) \setminus f(F) = f(E \setminus F)$ if $F \subset E$. The first of these facts is shown in the next example. The second is left to the exercises.

Example 1.1.8. Give an example of a function $f : A \to B$ for which there are subsets $E, F \subset A$ with $f(E \cap F) \neq f(E) \cap f(F)$.

Solution: Let A and B both be $\mathbb{R}$ and let $f : A \to B$ be defined by

$$f(x) = x^2.$$

If $E = (0, \infty)$ and $F = (-\infty, 0)$, then $E \cap F = \emptyset$, and so $f(E \cap F)$ is also the empty set. However, $f(E) = f(F) = (0, \infty)$, and so $f(E) \cap f(F) = (0, \infty)$ as well. Clearly $f(E \cap F)$ and $f(E) \cap f(F)$ are not the same in this case.

Cartesian Product

If A and B are sets, then their *Cartesian product* $A \times B$ is the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$. Similarly, the Cartesian product of n sets $A_1, A_2, \cdots, A_n$ is the set $A_1 \times A_2 \times \cdots A_n$ of all ordered n-tuples $(a_1, a_2, \cdots, a_n)$ with $a_i \in A_i$ for $i = 1, \cdots, n$.

If $f : A \to B$ is function from a set A to a set B, then the *graph* of f is the subset of $A \times B$ defined by $\{(a, b) \in A \times B : b = f(a)\}$.

Exercise Set 1.1

1. If $a, b \in \mathbb{R}$ and $a < b$, give a description in set theory notation for each of the intervals $(a, b), [a, b], [a, b)$, and $(a, b]$ (see Example 1.1.1).

2. If A, B, and C are sets, prove that
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

3. If A and B are two sets, then prove that A is the union of a disjoint pair of sets, one of which is contained in B and one of which is disjoint from B.

4. What is the intersection of all the open intervals containing the closed interval $[0, 1]$? Justify your answer.

5. What is the intersection of all the closed intervals containing the open interval $(0, 1)$? Justify your answer.

6. What is the union of all of the closed intervals contained in the open interval $(0,1)$? Justify your answer.

7. If $\mathcal{A}$ is a collection of subsets of a set X, formulate and prove a theorem like Theorem 1.1.5 for the intersection and union of $\mathcal{A}$.

8. Which of the following functions $f : \mathbb{R} \to \mathbb{R}$ are one to one and which ones are onto. Justify your answer.

   (a) $f(x) = x^2$;

   (b) $f(x) = x^3$;

   (c) $f(x) = \mathrm{e}^x$.

9. Prove Part (b) of Theorem 1.1.6.

10. Prove Part (c) of Theorem 1.1.6.

11. Prove Part (a) of Theorem 1.1.7.

12. Prove Part (b) of Theorem 1.1.7.

13. Give an example of a function $f : A \to B$ and subsets $F \subset E$ of A for which $f(E) \setminus f(F) \neq f(E \setminus F)$.

14. Prove that equality holds in Parts (b) and (c) of Theorem 1.1.7 if the function f is one-to-one.

15. Prove that if $f : A \to B$ is a function which is one-to-one and onto, then f has an *inverse function* – that is, there is a function $g : B \to A$ such that $g(f(x)) = x$ for all $x \in A$ and $f(g(y)) = y$ for all $y \in B$.

16. Prove that a subset G of $A \times B$ is the graph of a function from A to B if and only if the following condition is satisfied: for each $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in G$.

1.2 The Natural Numbers

The natural numbers are the numbers we use for counting, and so, naturally, they are also called the *counting numbers*. They are the positive integers $1, 2, 3, \cdots$.

The requirements for a system of numbers we can use for counting are very simple. There should be a first number (the number 1), and for each number there must always be a next number (a successor). After all, we don't want to run out of numbers when counting a large set of objects. This line of thought leads to Peano's axioms which characterize the system of natural numbers $\mathbb{N}$:

N1. there is an element $1 \in \mathbb{N}$;

N2. for each $n \in \mathbb{N}$ there is a successor element $s(n) \in \mathbb{N}$;

N3. 1 is not the successor of any element of $\mathbb{N}$;

N4. if two elements of $\mathbb{N}$ have the same successor, then they are equal;

N5. if a subset A of $\mathbb{N}$ contains 1 and is closed under succession (meaning $s(n) \in A$ whenever $n \in A$), then $A = \mathbb{N}$.

Note: at this stage in the development of the natural number system, all we have are Peano's axioms; addition has not yet been defined. When we define addition in $\mathbb{N}$, $S(n)$ will turn out to be $n + 1$.

Everything we need to know about the natural numbers can be deduced from these axioms. That is, using only Peano's axioms, one can define addition and multiplication of natural numbers and prove that they have the usual arithmetic properties. One can also define the order relation on the natural numbers and prove that it has the appropriate properties. To do all of this is not difficult, but it is tedious and time consuming. We will do some of this here in the text and the exercises, but we won't do it all. We will do enough so that students should understand how such a development would proceed. Then we will state and discuss the important properties of the resulting system of natural numbers.

Our main tool in this section will be *mathematical induction*, a powerful technique that is a direct consequence of Axiom **N5**.

Induction

Axiom **N5** above is often called the *induction* axiom, since it is the basis for mathematical induction. Mathematical induction is used in making definitions that involve a sequence of objects to be defined and in proving propositions that involve a sequence of statements to be proved. Here, by a *sequence* we mean a function whose domain is the natural numbers. Thus, a sequence of statements is an assignement of a statement to each $n \in \mathbb{N}$. For example, "n is either 1 or it is the successor of some element of $\mathbb{N}$" is a sequence of statements, one for each $n \in \mathbb{N}$. We will use induction to prove that all of these statements are true once we prove the following theorem.

The following theorem states the mathematical induction principle as it applies to proving propositions.

Theorem 1.2.1. *Suppose $\{P_n\}$ is a sequence of statements, one for each $n \in \mathbb{N}$. These statements are all true provided*

1. *P_1 is true (the base case is true); and*

2. *whenever P_n is true for some $n \in \mathbb{N}$, then $P_{s(n)}$ is also true (the induction step can be carried out).*

Proof. Let A be the subset of $\mathbb{N}$ consisting of those n for which P_n is true. Then hypothesis (1) of the theorem implies that $1 \in A$, while hypothesis (2) implies that $s(n) \in A$ whenever $n \in A$. By Axiom **N5**, $A = \mathbb{N}$, and so P_n is true for every n. $\square$

Example 1.2.2. Prove that each $n \in \mathbb{N}$ is either 1 or is the successor of some element of N.

Solution: If n is 1 then the statement is obviously true. Thus, the base case is true. If the statement is true of n then it is certainly true of $s(n)$, because it is true of any element which is the successor of something in $\mathbb{N}$. Thus, by induction, the statement is true for every $n \in \mathbb{N}$.

Another way to say what was proved in this example is that every natural number except 1 has a predecessor. This statement doesn't seem obvious at this stage of development of $\mathbb{N}$, but its proof was a rather trivial application of induction.

Inductive Definitions

Inductive definitions are used to define sequences. The sequence $\{x_n\}$ to be defined is a sequence of elements of some set X, which may or may not be a set of numbers. We wish to define the sequence in such a way that x_1 is a specified element of X and, for each $n \in \mathbb{N}$, $x_{s(n)}$ is a certain function of x_n. That is, we are given an element $x_1 \in X$ and a sequence of functions $f_n : X \to X$ and we wish to construct a sequence $\{x_n\}$, beginning with x_1, such that

$$x_{s(n)} = f_n(x_n) \quad \text{for all} \quad n \in \mathbb{N}. \tag{1.2.1}$$

This equation, defining $x_{s(n)}$ in terms of x_n, is called a *recursion relation*. Sequences defined in this way occur very often in mathematics. Newton's method from calculus and Euler's method for numerically solving differential equations are two important examples.

Theorem 1.2.3. *Given a set X, an element $x_1 \in X$, and a sequence $\{f_n\}$ of functions from X to X, there is a unique sequence $\{x_n\}$ in X, beginning with x_1, which satisfies $x_{s(n)} = f_n(x_n)$ for all $n \in \mathbb{N}$.*

Proof. Consider the Cartesian product $\mathbb{N} \times X$ – that is, the set of all ordered pairs (n, x) with $n \in \mathbb{N}$ and $x \in X$. We define a function $S : \mathbb{N} \times X \to \mathbb{N} \times X$ by

$$S(n, x) = (s(n), f_n(x)) \tag{1.2.2}$$

We say that a subset E of $\mathbb{N} \times X$ is closed under S if S sends elements of E to elements of E. Clearly the intersection of all subsets of $\mathbb{N} \times X$ that are closed under S and contain $(1, x_1)$ is also closed under S and contains $(1, x_1)$. This is the smallest subset of $\mathbb{N} \times X$, that is closed under S and contains $(1, x_1)$. We will call this set A.

To complete the argument, we will show that the set A is the graph of a function from $\mathbb{N}$ to X – that is, it has the form $\{(n, x_n) : n \in \mathbb{N}\}$ for a certain sequence $\{x_n\}$ in X. This is the sequence we are seeking. To prove A is the graph of a function from $\mathbb{N}$ to X we must show that each $n \in \mathbb{N}$ is the first element of exactly one pair $(n, x) \in A$. We prove this by induction.

The element 1 is the first element of the pair $(1, x_1)$, which is in A by the construction of A. If there were another element $x \in X$ such that $(1, x) \in A$, then we could remove $(1, x)$ from A and have a smaller set containing $(1, x_1)$ and closed under S. This is due to the fact that $(1, x)$ cannot be in the image of S, since 1 is not the successor of any element of $\mathbb{N}$ by **N3**.

Now, for the induction step, suppose for some n we know that there is a unique element $x_n \in X$ such that $(n, x_n) \in A$. Then $S(n, x_n) = (s(n), f_n(x_n))$ is in A. Suppose there is another element $(s(n), x) \in A$ with $x \neq f_n(x_n)$ and suppose this element is in the image of S – that is $(s(n), x) = S(m, y) = (s(m), f_m(y))$ for some $(m, y) \in A$. Then $n = m$ by **N4**, and $y = x_n$ by the induction assumption. Thus if $(s(n), x)$ is really different from $(s(n), f_n(x_n)$, then it cannot be in the image of S. As before this means we can remove it from A and still have a set closed under S and containing $(1, x_1)$. Since A is the smallest such set, we conclude there is no such element $(s(n), x)$. By induction, for each element of $\mathbb{N}$ there is a unique element $x_n \in X$ such that $(n, x_n) \in A$. Thus, A is the graph of a function $n \to x_n$ from $\mathbb{N}$ to X.

This shows the existence of a sequence with the required properties. We leave the proof that this sequence is unique to the exercises. □

Note that the proof of the above theorem used all of Peano's axioms, not just **N5**.

Using Peano's Axioms to Develop Properties of $\mathbb{N}$

In this subsection, we will demonstrate some of the steps involved in developing the arithmetic and order properties of $\mathbb{N}$ using only Peano's axioms. It is not a complete development, but just a taste of what is involved. We begin with the definition of addition.

Definition 1.2.4. We fix $m \in \mathbb{N}$ and define a sequence $\{m+n\}_{n\in\mathbb{N}}$ inductively as follows:

$$\begin{aligned} m + 1 &= s(m), \quad \text{and} \\ m + s(n) &= s(m+n). \end{aligned} \tag{1.2.3}$$

These two conditions determine a unique sequence $\{m + n\}_{n\in\mathbb{N}}$ by Theorem 1.2.3.

By the above definition, the successor $s(n)$ of n is our newly defined $n+1$. At this point we will begin using $n+1$ in place of $s(n)$ in our inductive arguments and definitions.

Example 1.2.5. Using the above definition and Peano's axioms, prove the associative law for addition in $\mathbb{N}$. That is, prove

$$m + (n + k) = (m + n) + k \quad \text{for all} \quad k, n, m \in \mathbb{N}.$$

Solution: We fix m and n and, for each $k \in \mathbb{N}$, let P_k be the proposition $m + (n + k) = (m + n) + k$. We prove that P_k is true for all $k \in \mathbb{N}$ by induction on k.

The base case P_1 is just

$$m + (n + 1) = (m + n) + 1. \tag{1.2.4}$$

which is the recursion relation (1.2.3) used in the definition of addition once we replace $s(n)$ with $n + 1$. Thus, P_1 is true by definition.

For the induction step, we assume P_k is true for some k – that is, we assume

$$m + (n + k) = (m + n) + k.$$

We then take the successor of both sides of this equation to obtain

$$(m + (n + k)) + 1 = ((m + n) + k) + 1.$$

If we use (1.2.4) on both sides of this equation, the result is

$$m + ((n + k) + 1) = (m + n) + (k + 1).$$

Using (1.2.4) again, this time on the left side of the equation, leads to

$$m + (n + (k + 1)) = (m + n) + (k + 1).$$

Since this is proposition P_{k+1}, the induction is complete.

Example 1.2.6. Using Definition 1.2.4 and Peano's axioms, prove that $1+n = n + 1$ for every $n \in \mathbb{N}$.

Solution: Let P_n be the statement $1 + n = n + 1$. We prove by induction that P_n is true for every n. It is trivially true in the base case $n = 1$, since P_1 just says $1 + 1 = 1 + 1$.

For the induction step, we assume that P_n is true for some n – that is we assume $1 + n = n + 1$. If we add 1 to both sides of this equation (i.e. take the successor of both sides), we have

$$(1 + n) + 1 = (n + 1) + 1.$$

By Definition 1.2.4, the left side of this equation is equal to $1 + (n + 1)$. Thus,

$$1 + (n + 1) = (n + 1) + 1.$$

Thus, P_{n+1} is true if P_n is true and the induction is complete.

A similar induction, this time on m, with n fixed can be used to prove the commutative law of addition – that is, $m + n = n + m$ for all $n, m \in \mathbb{N}$. The base case for this induction is the statement proved above. The associative law proved in Example 1.2.5 is needed in the proof of the induction step. We leave the details to the exercises.

We leave the definition of multiplication in $\mathbb{N}$ to the exercises. Its definition and the fact that it also satisfies the associative and commutative laws follows a pattern similar to the one above for addition. Once multiplication is defined, we can define factors and prime numbers:

Definition 1.2.7. If a number $n \in \mathbb{N}$ can be written as $n = mk$ with both $m \in \mathbb{N}$ and $k \in \mathbb{N}$, then k and m are called *factors* of n and are said to *divide* n. If $n \neq 1$ and the only factors of n are 1 and n, then n is said to be *prime*.

The order relation in $\mathbb{N}$ can be defined as follows:

Definition 1.2.8. If $n, m \in \mathbb{N}$, we will say that n is less than m, denoted $n < m$, if there is a $k \in \mathbb{N}$ such that $m = n + k$. We say n is less than or equal to m and write $n \leq m$ if $n < m$ or $n = m$.

Some of the properties of this order relation are worked out in the exercises. One of these is that each factor of n is necessarily less than or equal to n (Exercise 1.2.7).

Example 1.2.9. Prove that each natural number $n > 1$ is a product of primes.

Solution: Here we understand that a prime number itself is a product of primes – a product with only one factor. Note that if k and m are two numbers which are products of primes, then their product km is also a product of primes.

Let the proposition P_n be that every $m \in \mathbb{N}$, with $1 < m \leq n$, is a product of primes.

Base case: P_1 is true because there is no $m \in \mathbb{N}$ with $1 < m \leq 1$.

Induction step: suppose n is a natural number for which P_n is true. Then each m with $1 < m \leq n$ is a product of primes . Now $n + 1 > 1$ and so it is either a prime, or it factors as a product km with k and m not equal to 1 or $n + 1$. In the first case, P_{n+1} is true. In the second case, both k and m are less than $n + 1$ and, hence, less than or equal to n. Since P_n is true, k and m are products of primes. This implies that $n + 1 = km$ is also a product of primes and, in turn, this implies that P_{n+1} is true.

By induction, P_n is true for all $n \in \mathbb{N}$ and this means that every natural number $n > 1$ is a product of primes.

Additional Examples of the Use of Induction

At this point we leave the discussion of Peano's axioms and the development of the properties of the natural numbers. The remainder of the section is devoted to further examples of inductive proofs and inductive definitions. Some of these involve the real number system, which won't be discussed until Section 1.4. Never-the-less we are happy to anticipate its development and use its properties in these examples.

Example 1.2.10. Prove by induction that every number of the form $5^n - 2^n$, with $n \in \mathbb{N}$ is divisible by 3.

Solution: The proposition P_n is that $5^n - 2^n$ is divisible by 3.

Base case: Since $5 - 2 = 3$, P_1 is true;

Induction step: We need to show that P_{n+1} is true whenever P_n is true. We do this by rewriting the expression $5^{n+1} - 2^{n+1}$ as

$$5^{n+1} - 5 \cdot 2^n + 5 \cdot 2^n - 2^{n+1} = 5(5^n - 2^n) + (5 - 2)2^n.$$

If P_n is true then the first term on the right is divisible by 3. The second term on the right is also divisible by 3, since $5-2=3$. This implies that $5^{n+1}-2^{n+1}$ is divisible by 3 and, hence, that P_{n+1} is true. This completes the induction step.

By induction (that is, by Theorem 1.2.1), P_n is true for all n.

Example 1.2.11. Define a sequence $\{x_n\}$ of real numbers by setting $x_1 = 1$ and using the recursion relation

$$x_{n+1} = \sqrt{x_n + 1}. \tag{1.2.5}$$

Show that this is an increasing sequence of positive numbers less than 2.

Solution: The function $f(x) = \sqrt{x+1}$ may be regarded as a function from the set of positive real numbers into itself. We can apply Theorem 1.2.3, with each of the functions f_n equal to f, to conclude that a sequence $\{x_n\}$ is uniquely defined by setting $x_1 = 1$ and imposing the recursion relation (1.2.5).

Let P_n be the proposition that $x_n < x_{n+1} < 2$. We will prove that P_n is true for all n by induction.

Base Case: P_1 is the statement $x_1 < x_2 < 2$. Since $x_1 = 1$ and $x_2 = \sqrt{2}$, this is true.

Induction Step: Suppose P_n is true for some n. Then $x_n < x_{n+1} < 2$. If we add one and take the square root, this becomes

$$\sqrt{x_n+1} < \sqrt{x_{n+1}+1} < \sqrt{3}.$$

Using the recursion relation (1.2.5), this yields

$$x_{n+1} < x_{n+2} < \sqrt{3}$$

Since $\sqrt{3} < 2$, P_{n+1} is true. This completes the induction step.

We conclude that P_n is true for all $n \in \mathbb{N}$.

Binomial Formula

The proof of the binomial formula is an excellent example of the use of induction.

We will use the notation

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

This is the number of ways of choosing k objects from a set of n objects.

Theorem 1.2.12. *If x and y are real numbers and $n \in \mathbb{N}$, then*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Proof. We prove this by induction on n.

Base Case: Since $\binom{1}{0}$ and $\binom{1}{1}$ are both 1, the binomial formula is true when $n = 1$.

Induction Step: If we assume the formula is true for a certain n, then multiplying both sides of this formula by $x + y$ yields

$$\begin{aligned}(x+y)^{n+1} &= x\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} + y\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\\ &= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k+1}.\end{aligned} \tag{1.2.6}$$

If we change variables in the first sum on the second line of (1.2.6) by replacing k by $k-1$, then our expression for $(x+y)^{n+1}$ becomes

$$\begin{aligned}&x^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}x^k y^{n-k+1} + \sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1} + y^{n+1}\\ &= x^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]x^k y^{n+1-k} + y^{n+1}.\end{aligned} \tag{1.2.7}$$

If we use the identity (to be proved in Exercise 1.4.17)

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k},$$

then the right side of equation (1.2.7) becomes

$$x^{n+1} + \sum_{k=1}^{n}\binom{n+1}{k}x^k y^{n+1-k} + y^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}.$$

Thus, the binomial formula is true for $n + 1$ if it is true for n. This completes the induction step and the proof of the theorem. □

Exercise Set 1.2

In the first seven exercises use only Peano's axioms and results that were proved in Section 1.2 using only Peano's axioms.

1. Prove the commutative law for addition, $n + m = m + n$, holds in $\mathbb{N}$. Use induction and Examples 1.2.6 and 1.2.5.

2. Prove that if $n, m \in \mathbb{N}$, then $m + n \neq n$. Hint: use induction on n.

3. Use the preceding exercise to prove that if $n, m \in \mathbb{N}$, $n \leq m$, and $m \leq n$ then $n = m$.

4. Prove that the order relation on $\mathbb{N}$ has the transitive property: if $k < n$ and $n < m$, then $k < m$.

5. Use the preceding exercise and Peano's axioms to prove that if $n \in \mathbb{N}$, then for each element $m \in \mathbb{N}$ either $m \le n$ or $n \le m$. Hint: use induction on n.

6. Show how to define the product nm of two natural numbers. Hint: use induction on m.

7. Use the definition of product you gave in the preceding exercise to prove that if $n, m \in \mathbb{N}$ then $n \le nm$.

For the remaining exercises you are no longer restricted to just using Peano's axioms and their immediate consequences.

8. Using induction, prove that $n^2 + 3n + 3$ is odd for every $n \in \mathbb{N}$;

9. Using induction, prove that $7^n - 2^n$ is divisible by 5 for every $n \in \mathbb{N}$.

10. Using induction, prove that $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$ for every $n \in \mathbb{N}$.

11. Using induction, prove that $\displaystyle\sum_{k=1}^{n} (2k-1) = n^2$ for every $n \in \mathbb{N}$.

12. Finish the prove of Theorem 1.2.3 by showing that there is only one sequence $\{x_n\}$ which satisfies the conditions of the theorem.

13. Let a sequence $\{x_n\}$ of numbers be defined recursively by
$$x_1 = 0 \quad \text{and} \quad x_{n+1} = \frac{x_n + 1}{2}.$$
Prove by induction that $x_n \le x_{n+1}$ for all $n \in \mathbb{N}$. Would this conclusion change if we set $x_1 = 2$?

14. Let a sequence $\{x_n\}$ of numbers be defined recursively by
$$x_1 = 1 \quad \text{and} \quad x_{n+1} = \frac{1}{1 + x_n}.$$
Prove by induction that x_{n+2} is between x_n and x_{n+1} for each $n \in \mathbb{N}$.

15. Mathematical induction also works for a sequence $P_k, P_{k+1}, \cdots$ of propositions, indexed by the integers $n \ge k$ for some $k \in \mathbb{N}$. The statement is: If P_k is true and P_{n+1} true whenever P_n is true and $n \ge k$, then P_n is true for all $n \ge k$. Prove this.

16. Use induction in the form stated in the preceding exercise to prove that $n^2 < 2^n$ for all $n \ge 5$.

17. Prove the identity
$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k},$$
which was used in the proof of Theorem 1.2.12.

18. Write out the binomial formula in the case $n = 4$.

19. Prove the well ordering principal for the natural numbers: each non-empty subset S of $\mathbb{N}$ contains a smallest element. Hint: apply the induction axiom to the set
$$T = \{n \in \mathbb{N} : n < m \text{ for all } m \in S\}.$$

20. Use the result of Exercise 1.2.19 to prove the division algorithm: If n and m are natural numbers with $m < n$, and if m does not divide n, then there are natural numbers q and r such that $n = qm + r$ and $r < m$. Hint: consider the set S of all natural numbers s such that $(s + 1)m > n$.

1.3 Integers and Rational Numbers

The need for larger number systems than the natural numbers became apparent early in mathematical history. We need the number 0 in order to describe the number of elements in the empty set. The negative numbers are needed to describe deficits. Also, the operation of subtraction leads to non-positive integers unless $n - m$ is to be defined only for $m < n$.

Beginning with the system of natural numbers $\mathbb{N}$ and its properties derivable from Peano's axioms, the system of integers $\mathbb{Z}$ can easily be constructed. One simply adjoins to $\mathbb{N}$ a new element called 0 and, for each $n \in \mathbb{N}$ a new element called $-n$. Of course, one then has to define addition and multiplication and an order relation "$\leq$" for this new set $\mathbb{Z}$ in a way that is consistent with the existing definitions of these things for $\mathbb{N}$. When addition and multiplication are defined, we want them to have the properties that $0 + n = n$, and $n + (-n) = 0$. It turns out that these requirements and the commutative, associative and distributive laws (described below) are enough to uniquely determine how addition and multiplication are defined in $\mathbb{Z}$.

When all of this has been carried out, the new set of numbers $\mathbb{Z}$ can be shown to be a *commutative ring*, meaning that it satisfies the axioms listed below.

The Commutative Ring of Integers

A binary operation on a set A is rule which assigns to each ordered pair (a, b) of elements of A a third element of A.

Definition 1.3.1. A *commutative ring* is set R with two binary operations, addition ($(a, b) \to a + b$) and multiplication ($(a, b) \to ab$), that satisfy the following axioms: