Mathematical Foundations

Justin Lariviere and Tim Traynor

Contents

Chapter 0

Preliminaries

What to Expect

This course is an introduction to the reading and writing of mathematical proofs. Due attention is given to the style and practices that are expected in modern written mathematics. Grades will be a reflection of both the correctness of the mathematics as well as the style in which it is written.

0.1 Sentence Structure

The first requirement when writing mathematics is that our sentences be phrased clearly and precisely. We may leave no ambiguity. In particular, our ability to judge a statement as being true or false ought never to depend on the clarity of the language.

Open Sentences

To begin our discussion of precision in language, we identify two components of a statement. The first is the subject, which is the thing about which the statement is made, and the other is the property or declaration that is being asserted about this subject. For example, if one says '2 is even,' then the subject is 2, and the property asserted about this subject is that it is even. In general, the same property can be asserted of many different subjects, for example '2 is even,' '4 is even,' and '6 is even' are all statements in which the same predicate (or asserted property) is applied to different objects. To examine the predicate itself, without reference to a particular subject, we consider the subject as an open variable. That is, 'x is even' is a predicate that would make a sensible proposition if the variable x were replaced by any integer. For a more precise characterization of predicates we offer the following:

An **open sentence** or **predicate** is a declarative statement containing one or more open variables, whose truth or falsity depends on the values of those variables.

Example 0.1.1.

The following statements are examples of open sentences. The open variables in each sentence are given in parentheses.

1. 'The number is positive.' (*the number*)
2. 'The vector is in the null space of the matrix.' (*the vector, the matrix*)
3. 'The function is continuous at a.' (*the function, a*)
4. '$x \leq y$' (x, y)
5. 'The equation of the line is $y = 4x + 2$.' (*the line*)
6. '$\int_a^b f(x)\,dx = 0$.' (a, b, f)
7. '$2x + 1 = 4$.' (x)
8. 'If x is even then x is divisible by 4.' (x)
9. 'For every value of a in the domain of f, $\lim_{x \to a} f(x) = f(a)$.' (f)

Universe of Discourse

Each variable in an open sentence has a set of possible values that the variable may take. For example, in the open sentence 'x is even,' the values that x can take (in order to make this a sensible proposition) are the integers. This set of values is called the **universe of discourse** for the variable. Note that different variables may have different universal sets. For example, the open sentence 'The vector is in the null space of the matrix' may be written as '$\vec{x}$ is in the null space of A,' where the universal set for $\vec{x}$ is say $\mathbb{R}^3$, and the universal set for A is the set of all 3×3 matrices.

Making an Open Sentence into a Proposition

In practice, there are three ways in which an open sentence can be made into a proposition. We illustrate with the following example:

Example 0.1.2.

Consider the open sentence '*the number is positive*.' This is an example of an open sentence, because '*the number*' is an open variable. We may use this open sentence to make propositions in the following ways:

1. We may assign one specific value to the variable, as in '3 is positive'
2. We may assert that the sentence must be true for every allowable value of the variable, as in '*All real numbers are positive.*'
3. We may assert that the sentence must be true for at least one value of the variable, as in '*Some real numbers are positive.*'

In the proposition '3 *is positive.*', we have simply removed the variable from the open sentence. The variable '*the number*' has been replaced with '3,' which is not a variable; it is *one specific number*. Since the sentence no longer contains a variable that affects its truth or falsity, it now allows itself to be judged as either true or false, without any need to clarify the language: the proposition '3 is positive' is *true*.

In the propositions '*All real numbers are positive*' and '*Some real numbers are positive*,' the variable *the number* remains. The identity of *the number* is still unknown; hence *the number* is still a variable. However, when judging whether the propositions '*All real numbers are positive*' and '*Some real numbers are positive*' are true or false, we are no longer concerned with the identity of *the number* but rather with a *quantity* of numbers. Since in both cases, the quantity has been specified (as 'all' in one case and 'some' in the other), the *quantity* of numbers for which the sentence must be true is not a variable. Further, the truth or falsity of the sentence depends only on this *quantity* and not on the identity of any specific number. In this way, the value of the variable no longer affects the truth or falsity of the sentence. In fact, the proposition '*All real numbers are positive*' is *false*, and the proposition '*Some real numbers are positive*' is *true*.

Quantifiers

We will focus on sentences that make a statement about a *quantity* of items, such as '*all real numbers are positive*,' or '*some real numbers are positive*.' Formally, we introduce two new symbols ($\forall$ and $\exists$), called **quantifiers**, to denote the quantities of numbers whose positiveness is being asserted (i.e. the quantity of values that make our open sentence true). We illustrate by revisiting example 0.1.2.

Example 0.1.3.

Again, consider the open sentence '*the number is positive*.' Since *the number* is an open variable, we may write this sentence as 'x is positive,' or better still, '$x > 0$.' The universe of discourse for x is the set of all real numbers, which we denote by $\mathbb{R}$.

1. We write the proposition 'All real numbers are positive' using the symbolic form

   '$\forall x \in \mathbb{R},\ x > 0$.'

   Read: 'For all x in $\mathbb{R}$, x is positive.'

2. We write the proposition 'Some real numbers are positive' using the symbolic form

   '$\exists x \in \mathbb{R},\ x > 0$.'

   Read: 'There exists an x in $\mathbb{R}$ such that x is positive.'

The symbol $\forall$ is called the **universal quantifier**. We use $\forall$ to denote 'for all.' That is, '$\forall x \in \mathbb{R},\ x > 0$' is read 'For all x in $\mathbb{R}$, x is positive.'

The symbol $\exists$ is called the **existential quantifier**. We use $\exists$ to denote 'for some,' or more commonly 'there exists.' That is, '$\exists x \in \mathbb{R},\ x > 0$' is read 'There exists an x in $\mathbb{R}$ such that x is positive.' The meaning is that there is *at least one* real number that is positive. A more general description of this notation is as follows:

For an open sentence $P(x)$, where the universe of discourse for the variable x is U, the proposition

$$\forall x \in U,\ P(x)$$

is true exactly when $P(x)$ is true for every value of x in the universe of discourse U.

The proposition

$$\exists x \in U,\ P(x)$$

is true exactly when there is at least one value of x in the universe of discourse U for which $P(x)$ is true.

In practice, we will often quantify the variable over a *subset* of the universe of discourse. That is, if A is a subset of U, one can write $\forall x \in A$, $P(x)$, which asserts that $P(x)$ is true for all values of x in the set A. This same statement could be made using U as the universe of discourse by saying $\forall x \in U$, if $x \in A$ then $P(x)$. Similarly, one may wish to write $\exists x \in A$, $P(x)$, asserting that there is at least one value of x in the set A for which $P(x)$ is true. Since this same value of x is also in the universe of discourse U, the same statement could be made as $\exists x \in U$, $x \in A$ and $P(x)$. In general, we have the following rule:

For an open sentence $P(x)$, where the universe of discourse for the variable x is U, and for a subset $A \subseteq U$, we have

$$\forall x \in A,\ P(x) \ \Leftrightarrow\ \forall x \in U,\ \text{if } x \in A,\ \text{then } P(x)$$

and

$$\exists x \in A,\ P(x) \ \Leftrightarrow\ \exists x \in U,\ x \in A \text{ and } P(x).$$

In the above rule, we use the symbol $\Leftrightarrow$ to indicate that the two statements are equivalent. That is, one is true if and only if the other is true; they assert the same fact, only in different notation.

It is also quite common to encounter open sentences containing more than one variable. For example, $x \geq y$ contains two open variables. In cases where the two variables are quantified in the same way, that is either both are universally quantified, or both are existentially quantified, we will usually alter the notation to put the two quantifiers together. That is, rather than writing $\forall x \in U$, $\forall y \in U$, $P(x, y)$, we will combine the two quantifiers into one: $\forall x, y \in U$, $P(x, y)$. This is done only for the sake of producing a more readable notation and does not alter the meaning of the statement in any way.

Notation

For an open sentence $P(x, y)$, where x and y take values in a universe of discourse U, we use the following notation:

$$\forall x, y \in U,\ P(x, y) \text{ means } \forall x \in U,\ \forall y \in U,\ P(x, y)$$

and

$$\exists x, y \in U,\ P(x, y) \text{ means } \exists x \in U,\ \exists y \in U,\ P(x, y).$$

This degree of formality can seem tedious at first, but with practice we accustom ourselves to it and begin to depend on it. Like any skill, the ability to think and speak precisely is developed over time. One of the major goals of this course is to enable the student to organize his or her thoughts on mathematics in a formal way and to express those thoughts clearly and precisely. Developing the ability to identify subjects, predicates, and quantifiers in a statement is a very important first step toward this goal.

The Benefits of Symbolic Form

Identifying the variables in a proposition, and translating the statement into symbolic form, are useful skills for mathematicians. Not only does this process remove ambiguity from the statement, but we will also see that the symbolic form of a statement determines, to a large degree, the structure of the proof of that statement. We will discuss several different proof structures in this course, and we will frequently associate these proof structures with the symbolic form of the statements they prove.

For now, it will be beneficial to practice our translation skills. It can be helpful to remember that when translating a statement into symbolic form, we are writing a symbolic sentence with the same *meaning* but not necessarily the same *sentence structure*. We do not need to translate the sentence *word for word*. We need only determine the *intended meaning* of the sentence and write this meaning in symbolic form.

Example 0.1.4.

Write the symbolic form of the following propositions, by identifying and quantifying each variable and determining the universal set for each variable.

1. The square of every even integer is even.
   Let $\mathbb{E}$ denote the set of all even integers. $\forall x \in \mathbb{E}$, $x^2 \in \mathbb{E}$.

2. Some prime numbers have even squares.
   Let $\mathbb{P}$ denote the set of all prime numbers. $\exists x \in \mathbb{P}$, $x^2 \in \mathbb{E}$.

3. No odd integers have even squares.
   Let $\mathbb{O}$ denote the set of all odd numbers. $\forall x \in \mathbb{O}$, $x^2 \notin \mathbb{E}$.

4. Not all prime numbers have even squares.
   $\exists x \in \mathbb{P}$, $x^2 \notin \mathbb{E}$.

5. Every integer has a prime divisor.
   $\forall x \in \mathbb{Z}$, $\exists y \in \mathbb{P}$, $\exists a \in \mathbb{Z}$, $x = ay$.

6. There is a smallest natural number.
   $\exists x \in \mathbb{N}$, $\forall y \in \mathbb{N}$, $x \leq y$.

7. There is no largest prime number.
   $\forall x \in \mathbb{P}$, $\exists y \in \mathbb{P}$, $x < y$.

8. Between any two distinct real numbers is another real number.
   $\forall x, y \in \mathbb{R}$, if $x \neq y$ then $\exists z \in \mathbb{R}$, $x < z < y$ or $\exists z \in \mathbb{R}$, $y < z < x$.

9. If as many odd numbers as we please are added together, and their multitude is even, then the sum is even.
   $\forall n \in \mathbb{N}$, $\forall x_1, x_2, \ldots, x_n \in \mathbb{O}$, if n is even, then $x_1 + x_2 + \cdots + x_n$ is even.

10. If a cubic number multiplied by any number makes a cubic number, then the multiplied number is also cubic.
    $\forall x, y \in \mathbb{N}$, if $\exists a \in \mathbb{N}$, $x = a^3$ and $\exists b \in \mathbb{N}$, $xy = b^3$, then $\exists c \in \mathbb{N}$, $y = c^3$.

Exercises 0.1.

Common Notation for Sets of Numbers

$\mathbb{N}$:	*Natural numbers.*
$\mathbb{Z}$:	*Integers.*
$\mathbb{E}$:	*Even numbers.*
$\mathbb{O}$:	*Odd numbers.*
$\mathbb{Q}$:	*Rational numbers.*
$\mathbb{Q}^c$:	*Irrational numbers.*
$\mathbb{R}$:	*Real numbers.*

Give an example of open sentences $P(x)$ and $Q(x)$ and a universe of discourse U for which the following hold:

1. The statement '$\forall x \in U$, $P(x)$ or $Q(x)$' is true, but the statement '$\forall x \in U$, $P(x)$, or $\forall x \in U$, $Q(x)$' is false.
2. The statement '$\exists x \in U$, $P(x)$, and $\exists x \in U$, $Q(x)$' is true, but the statement '$\exists x \in U$, $P(x)$ and $Q(x)$' is false.

State whether the proposition is true or false.

3. $\exists x \in \mathbb{R}$, $x < 0$.
4. $\forall x \in \mathbb{N}$, $0 \leq x$.
5. $\forall x \in \mathbb{Z}$, if $0 \leq x$, then $x \in \mathbb{N}$.
6. $\forall x \in \mathbb{R}$, $0 < x^2$.
7. $\exists x \in \mathbb{R}$, $x^2 < 0$.
8. $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$, $x = 2y$.
9. $\forall x \in \mathbb{Z}$, $\exists y \in \mathbb{Z}$, $x = 2y$.
10. $\forall x \in \mathbb{Z}$, $\exists y \in \mathbb{Z}$, $y = 2x$.
11. $\forall x \in \mathbb{R}$, $\exists n \in \mathbb{Z}$, $n < x$.
12. $\exists x \in \mathbb{R}$, $\forall n \in \mathbb{Z}$, $n < x$.
13. $\forall x \in \mathbb{Z}$, if x is odd, then $\forall y \in \mathbb{Z}$, $x = 2y + 1$.
14. $\forall x, y \in \mathbb{R}$, if $\exists a \in \mathbb{R}$, $x < a$ and $a \leq z$, then $x < z$.
15. $\forall x \in \mathbb{N}$, $\exists y \in \mathbb{N}$, $y < x$.
16. $\forall x \in \mathbb{N}$, $\exists y \in \mathbb{N}$, $x < y$.
17. $\exists x \in \mathbb{N}$, $\forall y \in \mathbb{N}$, $y \leq x$.
18. $\exists x \in \mathbb{N}$, $\forall y \in \mathbb{N}$, $x \leq y$.
19. $\forall x, y \in \mathbb{Z}$, if $\exists a \in \mathbb{Z}$, $y = ax$, then $\exists b \in \mathbb{Z}$, $x = by$.
20. $\forall x \in \mathbb{R}$, if $\exists a \in \mathbb{R}$, $ax \leq 0$, then $x \leq 0$.
21. $\forall x \in \mathbb{Z}$, if $x \leq 0$, then $\forall a \in \mathbb{Z}$, $ax \leq 0$.
22. $\forall x \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $ax \leq 0$, then $\forall b \in \mathbb{R}$, $0 \leq bx$.
23. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $x \leq xa$, then $1 \leq a$.
24. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax \leq x$, then $a = 1$.
25. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $ax > 1$, then $\exists y \in \mathbb{R}$, $ay < -1$.
26. $\forall x \in \mathbb{R}$, if $\exists a \in \mathbb{R}$, $ax < 0$, then $\exists b \in \mathbb{R}$, $0 < bx$.

Write the following propositions in symbolic form by identifying all variables and using the appropriate quantifiers.

27. Every natural number is positive
28. The negative of any even integer is even.
29. The negative of any odd integer is odd.
30. The sum of any two odd integers is even.
31. Some integers have even squares.
32. Not all integers have even squares.
33. No odd integers have even squares.
34. If an integer's square is even, then the integer itself is even.
35. Not all integers are even.
36. No odd integers are even.
37. All integers are either even or odd.
38. 6 is a multiple of 3.
39. 6 is not a multiple of 5.
40. No odd integer is a multiple of an even integer.
41. Some even integers are multiples of odd integers.

42. Every real number is smaller than some natural number.

43. There is no natural number that is larger than every real number.

44. Every element of the interval $(0, 1)$ is smaller than every element of the interval $(1, 2)$.

45. 1 is the smallest positive integer. (NOTE: 1 is not a variable. It is a constant.)

46. There is a smallest natural number.

47. There is no largest natural number.

48. Between any two distinct real numbers, there is a rational number.

49. The equation $y^2 = 4x + 3$ has no integer solutions.

50. There is no real number whose square is negative.

51. There is a real number whose square is not positive.

52. 0 and 1 are the only real numbers that are equal to their own squares.

53. 1 and 7 are the only positive divisors of 7.

54. There is no largest real number in the interval $(0, 1)$.

55. If a number multiplied by two numbers makes certain numbers, then the numbers so produced have the same ratio as the numbers multiplied. (Here, 'number' should be read as 'natural number.')

56. If a number multiplied by itself makes a cubic number, then it itself is also cubic. (Again, 'number' should be read as 'natural number.')

0.2 Negation

Our goal in the previous section was to write propositions that are free of ambiguity. By making use of the symbolic writing style we discussed, we may ensure that our language does not hinder our ability to judge a proposition as true or false. If we decide that a proposition is true, we will attempt to prove its truth. However, if we decide that a proposition is false, we first need to express what it means for the proposition to be false. The statement asserting that a given proposition is false is known as the **negation** *of that proposition.*

For a proposition P, the **negation** (or **denial**) of P, denoted $\neg P$, is the proposition asserting that P is false. Hence $\neg P$ is true when P is false and false when P is true.

Example 0.2.1.

Write the negation of each of the following propositions.

1. 2 is odd.
   Negation: 2 is not odd.
2. All odd numbers are prime.
   Negation: Some odd numbers are not prime.
3. Some real numbers are not smaller than their squares.
   Negation: All real numbers are smaller than their squares.

Negating Statements with Quantified Variables

Consider the example '*all odd numbers are prime*.' The negation of this statement is '*some odd numbers are not prime*.' '*All odd numbers are prime*' can be written in symbolic form as '$\forall x \in \mathbb{O}$, x is prime.' The symbolic form of the negation, '*some odd numbers are not prime*,' is '$\exists x \in \mathbb{O}$, x is *not* prime.'

$$\neg(\forall x \in \mathbb{O},\ x \text{ is prime }) \Leftrightarrow \exists x \in B,\ x \text{ is not prime.}$$

Notice that to deny the statement '*all odd numbers are prime*,' we only need at least one composite odd number, for example 15. This means that when we are denying a statement about *all odd numbers*, we need only make a statement about *some odd numbers*. In general, we have the following rule:

Let $P(x)$ be an open sentence and U be the universe of discourse for the variable x.

$$\neg(\forall x \in U,\ P(x)) \ \Leftrightarrow\ \exists x \in U,\ \neg P(x).$$

Next, consider the example '*some real numbers are not smaller than their squares*.' The negation is '*all real numbers are smaller than their squares*.' The symbolic form of '*some real numbers are not smaller than their squares*' is '$\exists x \in \mathbb{R},\ x \geq x^2$.' The symbolic form of it's negation, '*all real numbers are smaller than their squares*,' is '$\forall x \in \mathbb{R},\ x < x^2$.'

$$\neg(\exists x \in \mathbb{R},\ x \geq x^2) \Leftrightarrow \forall x \in \mathbb{R},\ x < x^2.$$

In this case, since '*some real numbers are not smaller than their squares*' is true provided there is *at least one* real number that is not smaller than its square, to give a denial of this statement we must ensure that *all real numbers* are smaller than their squares. i.e. to deny a statement about *some real numbers*, we must make a statement about *all real numbers*. In general:

Let $P(x)$ be an open sentence and U be the universal set for the variable x.

$$\neg(\exists x \in U,\ P(x)) \ \Leftrightarrow\ \forall x \in U,\ \neg P(x).$$

Example 0.2.2.

Write the negations of the following propositions.

1. $\forall x \in \mathbb{N},\ x > 1$.
   Negation: $\exists x \in \mathbb{N},\ x \leq 1$.
2. $\exists x, y \in \mathbb{Z},\ 3x + 4 = 3y + 2$.
   Negation: $\forall x, y \in \mathbb{Z},\ 3x + 4 \neq 3y + 2$.
3. $\exists x \in \mathbb{R},\ \forall y \in \mathbb{N},\ x \leq y$.
   Negation: $\forall x \in \mathbb{R},\ \exists y \in \mathbb{N},\ x > y$.
4. $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ xy = 1$.
   Negation: $\exists x \in \mathbb{R},\ \forall y \in \mathbb{R},\ xy \neq 1$.
5. $\forall x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ \forall z \in \mathbb{Z},\ xy = zy$.
   Negation: $\exists x \in \mathbb{Z},\ \forall y \in \mathbb{Z},\ \exists z \in \mathbb{Z},\ xy \neq zy$.

Compound Propositions

Some propositions may be composed of several statements joined together with the connectives **or**, **and**, or the implication **if, ... then**. For example:

1. All integers are divisible by 2 *or* divisible by 3.
2. All integers are both even *and* positive.
3. *If* an integer is divisible by 2 *then* it is divisible by 3.

We will pay close attention to how these statements are negated and attempt general rules for negating statements involving **or**, **and**, *and* **if, ... then**.

First, notice that all of the statements listed above are *false*. The reason the statement 'All integers are divisible by 2 *or* divisible by 3' is false, is that there are some integers (for example: 5) that are not divisible by 2 *and* not divisible by 3. The negation of this proposition is in fact:

1. Some integers are not divisible by 2 *and* not divisible by 3.

The proposition 'All integers are both even *and* positive' is false for two reasons. We may deny this on the grounds that some integers (for example: 3) are not even, *or* we may deny it on the grounds that some integers (for example: -1) are not positive. The full negation of the statement is:

2. Some integers are not even *or* not positive.

Finally, the statement '*If* an integer is divisible by 2 *then* it is divisible by 3' is false because there are integers (for example: 2) that *are* divisible by 2, *and yet are not* divisible by 3. The proper negation of this statement is:

3. Some integers *are* divisible by 2 *and not* divisible by 3.

The general rules for negating statements containing *and*, *or*, or *if, then* become more evident when we examine the symbolic forms of these statements and their negations:

1. $\forall x \in \mathbb{Z}$, x is divisible by 2 *or* x is divisible by 3.
   Negation: $\exists x \in \mathbb{Z}$, x is not divisible by 2 *and* x is not divisible by 3.
2. $\forall x \in \mathbb{Z}$, x is even *and* x is positive.
   Negation: $\exists x \in \mathbb{Z}$, x is not even *or* x is not positive.
3. $\forall x \in \mathbb{Z}$, *If* x is divisible by 2 *then* x is divisible by 3.
   Negation: $\exists x \in \mathbb{Z}$, x *is* divisible by 2 *and* x *is not* divisible by 3.

The fact that universal ($\forall$) quantifiers are changed to existential ($\exists$) quantifiers, under negation, was discussed in the previous section. What is of interest here is:

1. Negating a statement with an 'or' connective results in a statement with an 'and' connective.
2. Negating a statement with an 'and' connective results in a statement with an 'or' connective.
3. Negating a conditional statement with 'if, then' results in a statement with an 'and' connective, with the hypothesis affirmed and the conclusion denied.

The general rules for negating statements containing *and*, *or*, or *if, then* are as follows:

1. $\neg(P \text{ or } Q) \Leftrightarrow \neg P \text{ and } \neg Q$.
2. $\neg(P \text{ and } Q) \Leftrightarrow \neg P \text{ or } \neg Q$.
3. $\neg(\text{if } P \text{ then } Q) \Leftrightarrow P \text{ and } \neg Q$.

The rules concerning *and* and *or* (rules 1 and 2) are commonly called **DeMorgan's Laws**.

Example 0.2.3.

Write the negations of the following propositions. Determine which is true, the proposition or its negation.

1. $\exists x, y \in \mathbb{R}$, $x < y$ and $y < x$.
   Negation: $\forall x, y \in \mathbb{R}$, $x \geq y$ or $y \geq x$.
   The negation is true.

2. $\forall x \in \mathbb{Z}$, $x < 0$ or $x \geq 1$.
   Negation: $\exists x \in \mathbb{Z}$, $x \geq 0$ and $x < 1$.
   The negation is true.

3. $\exists x \in \mathbb{Z}$, $x \geq 0$ and $\forall y \in \mathbb{Z}$, $xy \leq 0$.
   Negation: $\forall x \in \mathbb{Z}$, $x < 0$ or $\exists y \in \mathbb{Z}$, $xy > 0$.
   The original proposition is true.

4. $\forall x \in \mathbb{Z}$, $\exists a \in \mathbb{Z}$, $x = 2a$ or $\exists b \in \mathbb{Z}$, $x = 2b + 1$.
   Negation: $\exists x \in \mathbb{Z}$, $\forall a \in \mathbb{Z}$, $x \neq 2a$ and $\forall b \in \mathbb{Z}$, $x \neq 2b + 1$.
   The original proposition is true.

5. $\forall x \in \mathbb{R}$, $\exists n \in \mathbb{N}$, $n - 1 < x$ and $x \leq n$.
   Negation: $\exists x \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $n - 1 \geq x$ or $x > n$.
   The negation is true.

6. $\forall x \in \mathbb{R}$, $\exists n \in \mathbb{Z}$, $x < n$ and $\exists m \in \mathbb{Z}$, $m < x$.
   Negation: $\exists x \in \mathbb{R}$, $\forall n \in \mathbb{Z}$, $x \geq n$ or $\forall m \in \mathbb{Z}$, $m \geq x$.
   The original proposition is true.

7. $\forall x \in \mathbb{R}$, if $\exists y \in \mathbb{R}$, $xy > 0$ then $x > 0$.
   Negation: $\exists x \in \mathbb{R}$, $\exists y \in \mathbb{R}$, $xy > 0$ and $x \leq 0$.
   The negation is true.

8. $\forall x \in \mathbb{Z}$, if $x^2 = 1$ then $x = 1$ or $x = -1$.
   Negation: $\exists x \in \mathbb{Z}$, $x^2 = 1$ and $x \neq 1$ and $x \neq -1$.
   The original proposition is true.

9. $\forall x \in \mathbb{Z}$, if $\exists a \in \mathbb{Z}$, $x = 15a + 8$, then $\exists b \in \mathbb{Z}$, $x = 5b + 3$ and $\exists c \in \mathbb{Z}$, $x = 3c + 5$.
   Negation: $\exists x \in \mathbb{Z}$, $\exists a \in \mathbb{Z}$, $x = 15a+8$, and $\forall b \in \mathbb{Z}$, $x \neq 5b+3$, or $\forall c \in \mathbb{Z}$, $x \neq 3c+5$.
   The original proposition is true.

10. $\forall x \in \mathbb{Z}$, if $\exists b \in \mathbb{Z}$, $x = 5b + 3$ and $\exists c \in \mathbb{Z}$, $x = 3c + 5$, then $\exists a \in \mathbb{Z}$, $x = 15a + 8$.
    Negation: $\exists x \in \mathbb{Z}$, $\exists b \in \mathbb{Z}$, $x = 5b + 3$, and $\exists c \in \mathbb{Z}$, $x = 3c + 5$, and $\forall a \in \mathbb{Z}$, $x \neq 15a + 8$.
    The original proposition is true.

Exercises 0.2.

Write the negation of each of the following propositions. Determine which is true, the proposition or its negation.

1. $\forall x \in \mathbb{R}$, $x \leq x$.
2. $\exists x \in \mathbb{R}$, $x^2 < 0$.
3. $\exists x \in \mathbb{R}$, $\forall y \in \mathbb{Z}$, $x \leq y$.
4. $\forall x \in \mathbb{Z}$, $\exists y \in \mathbb{R}$, $x \leq y$.
5. $\forall x \in \mathbb{Q}$, $\exists y \in \mathbb{Q}$, $xy = 1$.
6. $\exists x \in \mathbb{Q}$, $\forall y \in \mathbb{Q}$, $xy = 1$.
7. $\forall x \in \mathbb{Z}$, $x + (x + 1)$ is odd and $x(x + 1)$ is even.
8. $\forall x, y \in \mathbb{Z}$, x divides y or y divides x.
9. $\exists x, y \in \mathbb{R}$, xy is rational, and x or y is irrational.
10. $\forall x \in \mathbb{Z}$, $\exists y \in \mathbb{Z}$, y is prime and y divides x.
11. $\forall x, y \in \mathbb{Z}$, if $x - y$ is even, then $x + y$ is even.
12. $\forall x, y \in \mathbb{R}$, if x is rational and y is irrational, then $x + y$ is irrational.
13. $\forall x, y \in \mathbb{R}$, if $x > 0$, then $\exists n \in \mathbb{N}$, $y < nx$.
14. $\forall x \in \mathbb{R}$, if $x > 0$, then $\exists y \in \mathbb{R}$, $0 < y$ and $y < x$.
15. $\forall x, y \in \mathbb{Q}$, if $x < y$, then $\exists z \in \mathbb{R}$, $z \notin \mathbb{Q}$ and $x < z < y$.
16. $\forall x \in \mathbb{Z}$, if x is prime, then $\exists y \in \mathbb{Z}$, y is prime and $y > x$.
17. $\forall x \in \mathbb{R}$, if $\exists y \in \mathbb{R}$, $y \neq 0$ and $xy = y$, then $\forall z \in \mathbb{R}$, $xz = z$.
18. $\forall x \in \mathbb{R}$, if $\forall y \in \mathbb{Z}$, $xy \leq 0$, then $\forall z \in \mathbb{Z}$, $xz \geq 0$.
19. $\forall x \in \mathbb{Z}$, if $\exists t \in \mathbb{Z}$, $x^2 = 3t$, then $\exists s \in \mathbb{Z}$, $x = 3s$.
20. $\forall x, y \in \mathbb{Z}$, if $\exists a \in \mathbb{Z}$, $xy = 6a$, then $\exists b \in \mathbb{Z}$, $x = 6b$ or $\exists c \in \mathbb{Z}$, $y = 6c$.
21. $\forall n \in \mathbb{N}$, if $n = 1$ or $n = 7$, then $\forall x \in \mathbb{N}$, $\exists t \in \mathbb{N}$, $7x = nt$.
22. $\forall n \in \mathbb{N}$, if $\forall x \in \mathbb{N}$, $\exists t \in \mathbb{N}$, $7x = nt$ then $n = 1$ or $n = 7$.
23. $\forall x \in \mathbb{R}$, if $\forall y \in \mathbb{R}$, if $y > 0$ then $x \leq y$, then $x \leq 0$.

0.3 Logical Operators

Taking a closer look at the terms *and*, *or*, and *if, then*, we see that the function of each of these connectives is to combine two propositions into one *compound proposition*. For example, '16 is divisible by 4' and '16 is divisible by 3' are two propositions, the first being *true* and the second *false*. Using the connectives *and*, *or*, and *if, then*, we can create the following *compound propositions*:

'16 is divisible by 4 *and* 16 is divisible by 3.'
'16 is divisible by 4 *or* 16 is divisible by 3.'
'*if* 16 is divisible by 4, *then* 16 is divisible by 3.'

In this example, the first compound proposition is false, the second is true, and the third is false. It is interesting to note that whether the resulting compound proposition is true or false depends only on whether the two component propositions are true or false. It does not depend on the meaning of the propositions or on any relationship between the two. In fact, there does not need to be any relationship between the two propositions. For example, though there is no relationship between the propositions '16 is divisible by 4' and 'all triangles are isosceles,' the compound proposition '16 is divisible by 4 *or* all triangles are isosceles' is a true compound proposition. The compound proposition is true simply by virtue of the fact that one of the component propositions (namely, '16 is divisible by 4') is true.

To help us phrase this observation in a more precise way, we introduce the following term:

A **Boolean** value is one of either **False** or **True**. The *Boolean* value of a proposition is *True* provided the proposition is true and *False* provided the proposition is false. The Boolean values {*False*, *True*} are also sometimes denoted by {*F*, *T*}, {0, 1}, {−1, 1}, or {⊥, ⊤}.

For example, the *Boolean* value of the proposition '16 is divisible by 4' is *True*; the *Boolean* value of the proposition '16 is divisible by 3' is *False*; the Boolean value of the compound proposition '*if* 16 is divisible by 4, *then* 16 is divisible by 3' is *False*.

Earlier, we observed that whether a compound proposition is true or false depends only on whether the component propositions are true or false. We can rephrase this by saying the Boolean value of a compound proposition is determined by the Boolean values of its component propositions. Because of this, we can view the connectives *and*, *or*, and *if, then* as *functions* that take two Boolean values as input and return a single Boolean value as output. Functions that take a number of Boolean values as input and return a single Boolean value as output are called **logical operators**. The logical operators *and*, *or*, and *if, then* are given by the following rules:

The *logical operator* $\wedge$ (read 'and') is the function accepting two Boolean values as input and returning one Boolean value as output, according to the following rule: for Boolean values x, y

x	y	$x \wedge y$
T	T	T
T	F	F
F	T	F
F	F	F

The *logical operator* $\vee$ (read 'or') is the function accepting two Boolean values as input and returning one Boolean value as output, according to the following rule: for Boolean values x, y

x	y	$x \vee y$
T	T	T
T	F	T
F	T	T
F	F	F

The *logical operator* $\Rightarrow$ (read 'implies' or 'if, ... then') is the function accepting two Boolean values as input and returning one Boolean value as output, according to the following rule, for Boolean values x, y

x	y	$x \Rightarrow y$
T	T	T
T	F	F
F	T	T
F	F	T

Not all logical operators accept two Boolean values as input. For example, the logical operator $\neg$ ('not') accepts a single Boolean value as input and returns a single Boolean value as output, according to the rule: for a Boolean value x

x	$\neg x$
T	F
F	T

To justify the definition of the logical operator $\neg$ above, consider for example the proposition '2 is odd.' The Boolean value of this proposition is *False*. The negation of this proposition, '$\neg$(2 is odd),' is the proposition '2 is not odd,' which has a Boolean value of *True*. Likewise, the negation of a true proposition will be a false proposition. Thus, the negation, as we understand it from section 0.2, can be viewed as a logical operator that maps the *True* Boolean value to *False*, and the *False* Boolean value to *True*.

Since the $\neg$ logical operator takes only *one* Boolean value as input, we call it a **unary** logical operator. Likewise, since the $\wedge$, $\vee$, and $\Rightarrow$ connectives take *two* Boolean values as input, we call them **binary** logical operators. There are also logical operators that take three or more Boolean values as input. For example, consider the logical operator $x \Rightarrow (y \vee z)$. This operator is given by the rule: for Boolean values x, y, z

x	y	z	$x \Rightarrow (y \vee z)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	F
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

The logical operator above accepts *three* Boolean values as input and returns a single Boolean value as output.

Equivalent Logical Operators

Two logical operators are called **equivalent** provided they are the same *function*. That is, when the two operators are given the same Boolean inputs, they produce the same Boolean output. We have already seen several examples of *equivalent* logical operators in the previous section. For example, consider DeMorgan's Law: for propositions P and Q,

$$\neg(P \text{ and } Q) \Leftrightarrow \neg P \text{ or } \neg Q.$$

One way of justifying the equivalence of these propositional forms is that the corresponding logical operators $\neg(x \wedge y)$ and $\neg x \vee \neg y$ are equivalent (in the sense that they are the same function). Indeed, the table of inputs/outputs for these operators is as follows:

x	y	$\neg(x \wedge y)$	$\neg x \vee \neg y$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	T	T

Since these two functions always produce the same output when given the same inputs, we say the logical operators $\neg(x \wedge y)$ and $\neg x \vee \neg y$ are *equivalent*. We denote this equivalence by

$$\neg(x \wedge y) \equiv \neg x \vee \neg y$$

Likewise, the other rules for negating compound propositions

$$\neg(P \text{ or } Q) \Leftrightarrow \neg P \text{ and } \neg Q$$

$$\neg(\text{if } P, \text{ then } Q) \Leftrightarrow P \text{ and } \neg Q$$

are justifiable in the same way. That is, the corresponding logical operators are *equivalent*:

$$\neg(x \vee y) \equiv \neg x \wedge \neg y$$

$$\neg(x \Rightarrow y) \equiv x \wedge \neg y.$$

For a slightly more elaborate example of equivalent logical operators, consider the operators $x \Rightarrow (y \vee z)$ and $(x \wedge \neg y) \Rightarrow z$. The table of values for these functions is:

x	y	z	$x \Rightarrow (y \vee z)$	$(x \wedge \neg y) \Rightarrow z$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	T	T

We see that $x \Rightarrow (y \vee z)$ and $(x \wedge \neg y) \Rightarrow z$ yield the same output whenever they are given the same inputs. Thus,

$$x \Rightarrow (y \vee z) \equiv (x \wedge \neg y) \Rightarrow z.$$

Changing the Form of a Proposition

In practice, we often use equivalent logical operators to change the form of a proposition into a form that is easier to work with. Consider for example the pair of equivalent logical operators just mentioned: $x \Rightarrow (y \vee z) \equiv (x \wedge \neg y) \Rightarrow z$. Since these logical operators are equivalent, if we were to replace the Boolean variables x, y, and z with propositions P, Q, and R, then the proposition 'if P, then Q or R' would necessarily have the same Boolean value as the proposition 'if P and not Q, then R,' regardless of the choice of propositions P, Q, and R. That is, any compound proposition of the form 'if P, then Q or R' is true if and only if the proposition 'if P and not Q, then R' is true.

For example, consider the proposition '$\forall x, y \in \mathbb{Z}$, if xy is even, then x is even or y is even.' For any $x, y \in \mathbb{Z}$, if we identify P, Q and R as

P : xy is even

Q : x is even

R : y is even,

then the proposition 'if xy is even, then x is even or y is even' has the form

if P, then Q or R.

Since the logical operator $x \Rightarrow (y \vee z)$ is equivalent to the logical operator $(x \wedge \neg y) \Rightarrow z$, we have that this proposition is equivalent to the proposition

if P and not Q, then R.

That is, it is equivalent to 'if xy is even and x is not even, then y is even.'

In fact, any compound proposition of the form

if P, then Q or R

can be rewritten in the form

if P and not Q, then R,

because the corresponding logical operators $x \Rightarrow (y \vee z)$ and $(x \wedge \neg y) \Rightarrow z$ are equivalent.

Example 0.3.1.

For each of the following propositions of the form $P \Rightarrow (Q \vee R)$, rewrite the proposition in the form $(P \wedge \neg Q) \Rightarrow R$.

1. $\forall x \in \mathbb{R}$, if $1 < x^2$, then $1 < x$ or $x < -1$.
   Solution: $\forall x \in \mathbb{R}$, if $1 < x^2$ and $x \leq 1$, then $x < -1$.
2. $\forall x, y \in \mathbb{R}$, if xy is irrational, then x is irrational or y is irrational.
   Solution: $\forall x, y \in \mathbb{R}$, if xy is irrational and x is rational, then y is irrational.
3. $\forall x, y \in \mathbb{R}$, if $xy < 0$, then $x < 0$ or $y < 0$.
   Solution: $\forall x, y \in \mathbb{R}$, if $xy < 0$ and $0 \leq x$, then $y < 0$.
4. $\forall x, y \in \mathbb{R}$, if $x^2 = y^2$, then $x = y$ or $x = -y$.
   Solution: $\forall x, y \in \mathbb{R}$, if $x^2 = y^2$ and $x \neq y$, then $x = -y$.

Boolean Algebraic Properties of Logical Operators

A few fundamental equivalent logical operators form what we call the **Boolean algebraic** properties of logical operators. We will see many of these same basic properties reoccurring in other branches of mathematics throughout the course. All of the *Boolean algebraic* properties can be easily verified by writing out a table of Boolean values for each operator.

Boolean Algebraic Properties of Logical Operators

Let **T** be the logical operator that returns the Boolean value *True* for every input, and let **F** be the logical operator that returns the Boolean value *False* for every input. Then

$$\neg \mathbf{T} \equiv \mathbf{F} \qquad \neg \mathbf{F} \equiv \mathbf{T}$$

Idempotence

$$x \wedge x \equiv x \qquad x \vee x \equiv x$$

Commutativity

$$x \wedge y \equiv y \wedge x \qquad x \vee y \equiv y \vee x$$

Associativity

$$x \wedge (y \wedge z) \equiv (x \wedge y) \wedge z \qquad x \vee (y \vee z) \equiv (x \vee y) \vee z$$

Absorption

$$x \wedge (x \vee y) \equiv x \qquad x \vee (x \wedge y) \equiv x$$

Distributivity

$$x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z) \qquad x \vee (y \wedge z) \equiv (x \vee y) \wedge (x \vee z)$$

Annihilator

$$x \wedge \mathbf{F} \equiv \mathbf{F} \qquad x \vee \mathbf{T} \equiv \mathbf{T}$$

Identity

$$x \wedge \mathbf{T} \equiv x \qquad x \vee \mathbf{F} \equiv x$$

Complementation

$$x \wedge \neg x \equiv \mathbf{F} \qquad x \vee \neg x \equiv \mathbf{T}$$

Double Negation

$$\neg(\neg x) \equiv x$$

De Morgan's Laws

$$\neg(x \vee y) \equiv \neg x \wedge \neg y \qquad \neg(x \wedge y) \equiv \neg x \vee \neg y$$

The Contrapositive of an Implication

There is another pair of equivalent logical operators that is of particular importance, so we take the time to highlight it here. The implication $x \Rightarrow y$ is equivalent to the implication $\neg y \Rightarrow \neg x$. To verify that these logical operators are the same, we check the table of values:

x	y	$x \Rightarrow y$	$\neg y \Rightarrow \neg x$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Since the two logical operators $x \Rightarrow y$ and $\neg y \Rightarrow \neg x$ always produce the same outputs, they are the same function; thus, $x \Rightarrow y \equiv \neg y \Rightarrow \neg x$. This equivalence of logical operators motivates the following definition:

For propositions P and Q, the implication

$$\text{if } \neg Q, \text{ then } \neg P$$

is called the **contrapositive** form of the implication

$$\text{if } P, \text{ then } Q.$$

Since the corresponding logical operators $x \Rightarrow y$ and $\neg y \Rightarrow \neg x$ are equivalent, we have that every implication is true if and only if its contrapositive is true. In other words, we may replace any implication with its contrapositive without changing whether the statement is true or false.

Example 0.3.2.

Rewrite each of the following propositions by replacing the implication with its contrapositive:

1. $\forall x, y \in \mathbb{R}$, if $x < y$, then $1 + x < 2 + y$.
   Solution: $\forall x, y \in \mathbb{R}$, if $2 + y \leq 1 + x$, then $y \leq x$.
2. $\forall x, y \in \mathbb{R}$, if $x + y$ is irrational, then x is irrational or y is irrational.
   Solution: $\forall x \in \mathbb{R}$, if x is rational and y is rational, then $x + y$ is rational.
3. $\forall x, y \in \mathbb{Z}$, if xy is odd, then x is odd and y is odd.
   Solution: $\forall x \in \mathbb{Z}$, if x is even or y is even, then xy is even.
4. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $x \neq 1$ and $ax = a$, then $a = 0$.
   Solution: $\forall a \in \mathbb{R}$, if $a \neq 0$, then $\forall x \in \mathbb{R}$, $x = 1$ or $ax \neq a$.
   Alternate Solution: $\forall a \in \mathbb{R}$, if $a \neq 0$, then $\forall x \in \mathbb{R}$, if $x \neq 1$, then $ax \neq a$.
   Alternate Solution: $\forall a \in \mathbb{R}$, if $a \neq 0$, then $\forall x \in \mathbb{R}$, if $ax = a$, then $x = 1$.
5. $\forall x, y \in \mathbb{R}$, if $\forall n \in \mathbb{N}$, $|x - y| < \dfrac{1}{n}$, then $x = y$.
   Solution: $\forall x, y \in \mathbb{R}$, if $x \neq y$, then $\exists n \in \mathbb{N}$, $\dfrac{1}{n} \leq |x - y|$.

The Converse of an Implication

For the implication $x \Rightarrow y$, another related, though *not* equivalent, logical operator is the implication that reverses the antecedent and the consequent. That is, the implication $y \Rightarrow x$. We call the operator $y \Rightarrow x$ the *converse* of the operator $x \Rightarrow y$ and we use the same word to describe propositions of the corresponding forms:

For propositions P and Q, the implication

if Q, then P

is called the **converse** of the implication

if P, then Q.

It is important to stress that the *converse* of an implication is *not* equivalent to the original implication. That is,

$$x \Rightarrow y \not\equiv y \Rightarrow x.$$

This can easily be seen by comparing the tables of Boolean values for these two operators:

x	y	$x \Rightarrow y$	$y \Rightarrow x$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Since these logical operators are not equivalent, it is possible to find an implication that does not have the same Boolean value as its converse. This is possible even when the implication is part of a proposition with quantified variables. For example, the proposition

$$\forall x, y \in \mathbb{Z}, \text{ if } x \text{ is even and } y \text{ is even, then } x + y \text{ is even}$$

is true. However, if we replace the implication in this proposition with its converse, we get the proposition

$$\forall x, y \in \mathbb{Z}, \text{ if } x + y \text{ is even, then } x \text{ is even and } y \text{ is even}$$

which is false. The converse is false because it is possible to find integers, say $x = 1$ and $y = 3$ for which $x + y$ is even, but in this case neither x nor y are even.

Exercises 0.3.

".. you should say what you mean," the March Hare went on.
"I do," Alice hastily replied; "at least... at least I mean what I say... that's the same thing, you know."
"Not the same thing a bit!" said the Hatter. "You might just as well say that 'I see what I eat' is the same thing as 'I eat what I see'!"
"You might just as well say," added the March Hare, "that 'I like what I get' is the same thing as 'I get what I like'!"
"You might just as well say," added the Dormouse, who seemed to be talking in his sleep, "that 'I breathe when I sleep' is the same thing as 'I sleep when I breathe'!"
(Alice's Adventures in Wonderland) [1]

The following exercises are related to logical operators and equivalent propositional forms.

1. Let $x, y \in \mathbb{Z}$. Let P be the Boolean value of the proposition 'x is odd,' and let Q be the Boolean value of the proposition 'y is even.' Using $\wedge$, $\vee$, and $\neg$, write each of the following as a logical operator applied to P and Q:
   (a) x is odd and y is even.
   (b) x is even and y is odd.
   (c) Both x and y are even.
   (d) Neither x nor y is even.
   (e) At least one of x or y is even.
   (f) At least one of x or y is odd.
   (g) At most one of x or y is even.
   (h) At most one of x or y is odd.
   (i) Exactly one of x or y is even.
   (j) Exactly one of x or y is odd.
2. Given the following pairs of equivalent logical operators:
   (a) $x \Rightarrow (y \Rightarrow z) \equiv (x \wedge y) \Rightarrow z$
   (b) $x \Rightarrow (y \vee z) \equiv (x \wedge \neg y) \Rightarrow z$
   (c) $(x \wedge y) \Rightarrow z \equiv (x \wedge \neg z) \Rightarrow \neg y$
   (d) $(x \vee y) \Rightarrow z \equiv (x \Rightarrow z) \wedge (y \Rightarrow z)$
   (e) $x \Rightarrow (y \wedge z) \equiv (x \Rightarrow y) \wedge (x \Rightarrow z)$

   rewrite the following propositions using the corresponding equivalences above.
   (a) $\forall a, x \in \mathbb{R}$, if $a \neq 0$, then if $ax = a$, then $x = 1$.
   (b) $\forall x, y, z \in \mathbb{R}$, if $xy = 0$, then $y = 0$ or $x = 0$.
   (c) $\forall x, y, z \in \mathbb{Z}$, if $xz = yz$ and $z \neq 0$ then $x = y$.
   (d) $\forall x \in \mathbb{Z}$, if x is even or x is odd, then $x^2 - 3x + 1$ is odd.
   (e) $\forall x, y \in \mathbb{Z}$, if xy is odd, then x is odd and y is odd.

The following exercises are related to the converse and contrapositive of an implication.

3. State the converse and contrapositive of each of the following implications:
   (a) $\forall x \in \mathbb{R}$, if $0 < x$, then $-x < 0$.
   (b) $\forall x, y, a \in \mathbb{R}$, if $ax = ay$ and $a \neq 0$, then $x = y$.
   (c) $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax = 0$, then $a = 0$.
   (d) $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $x \neq 0$ and $ax = 0$, then $a = 0$.
   (e) $\forall a, b, x \in \mathbb{R}$, if $a < x$ and $x < b$, then $\exists t \in (0, 1)$, $x = (1 - t)a + tb$.
4. In the passage above, taken from "Alice's Adventures in Wonderland" by Lewis Carroll, Alice, the March Hare, the Dormouse, and the Mad Hatter have a conversation about whether or not converse statements are equivalent to one another.
   (a) Rewrite each of the implications in the conversation in the form 'if P then Q' and 'if Q then P' to see that each pair are in fact converse statements.
   (b) Write the negation of each statement.
   (c) Is Alice right when she says "that's the same thing, you know" or is the Hatter right when he says they are "Not the same thing a bit!"?
5. Give, if possible, an example of a **true** implication statement for which:
   (a) the converse is true.
   (b) the converse is false.

(c) the contrapositive is true.

(d) the contrapositive is false.

6. Give, if possible, an example of a **false** implication statement for which:

   (a) the converse is true.

   (b) the converse is false.

   (c) the contrapositive is true.

   (d) the contrapositive is false.

7. (a) Show, using a truth table, that for any Boolean values x and y, at least one of $x \Rightarrow y$ or $y \Rightarrow x$ must be true.

   (b) Give reasons why the following propositions are both false:

      i. $\forall x \in \mathbb{R}$, if $x < 0$, then $x^2 < 1$.

      ii. $\forall x \in \mathbb{R}$, if $x^2 < 1$, then $x < 0$.

   (c) Explain why part 7b does not contradiction part 7a.

0.4 Set Notation

We use the word **set** to describe a collection of objects. The objects in the set are called **elements** of the set. The notation that we use to describe this relationship between sets and elements is

$$x \in A$$

which denotes that the object x is an element of the set A. To describe a particular set, we commonly refer to the collection of objects satisfying a certain condition. To do this, we need a *universe of discourse* from which the objects are taken and an *open sentence* that gives the condition that these objects must satisfy to be considered elements in the set. Consider for example

$$\{x \in \mathbb{N} \mid x < 6\}$$

Here, the universe of discourse is $\mathbb{N}$. This tells us that the type of objects considered when defining the set are natural numbers. The open sentence that must be satisfied for x to be an element is $x < 6$. This tells us that those and only those natural numbers satisfying the condition $x < 6$ are considered elements of the set. Hence for any given natural number $a \in \mathbb{N}$, if $a < 6$ we write

$$a \in \{x \in \mathbb{N} \mid x < 6\}$$

whereas if $a \geq 6$ we write

$$a \notin \{x \in \mathbb{N} \mid x < 6\}.$$

In general, given a universe of discourse U and an open sentence $P(x)$, we can define the set

$$\{x \in U \mid P(x)\}.$$

Some common examples of sets defined in this way, which will make frequent appearances throughout the course, are the **real intervals**:

Definition 0.4.1. For $a, b \in \mathbb{R}$,

$$\begin{aligned}
(a, b) &= \{x \in \mathbb{R} \mid a < x \text{ and } x < b\} \\
(a, b] &= \{x \in \mathbb{R} \mid a < x \text{ and } x \leq b\} \\
[a, b) &= \{x \in \mathbb{R} \mid a \leq x \text{ and } x < b\} \\
[a, b] &= \{x \in \mathbb{R} \mid a \leq x \text{ and } x \leq b\} \\
(a, \infty) &= \{x \in \mathbb{R} \mid a < x\} \\
[a, \infty) &= \{x \in \mathbb{R} \mid a \leq x\} \\
(-\infty, b) &= \{x \in \mathbb{R} \mid x < b\} \\
(-\infty, b] &= \{x \in \mathbb{R} \mid x \leq b\} \\
(-\infty, \infty) &= \mathbb{R}.
\end{aligned}$$

Another example that may be less familiar but will also be used very often, is the **ideals** of the integers:

Definition 0.4.2. For $a \in \mathbb{Z}$, the **ideal** of $\mathbb{Z}$ generated by a is the set

$$\langle a \rangle = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = at\}.$$

Another set that at first glance may not seem very important but we will see is useful in many arguments is the **empty set** $\emptyset$. The empty set is the set with no elements. Hence, given a universe of discourse U, the statement

$\forall x \in U,\ x \notin \emptyset$ is true.

Equivalently,

$\exists x \in U,\ x \in \emptyset$ is false.

Further, given a set A whose elements are in the universe of discourse U,

$A \neq \emptyset$ means $\exists x \in U,\ x \in A$.

Equivalently,

$A = \emptyset$ means $\forall x \in U,\ x \notin A$.

For example, the real interval $(1, 0) = \emptyset$. This is because $(1, 0)$ is a set whose elements are in the universe of discourse $\mathbb{R}$, and the statement $\forall x \in \mathbb{R},\ x \notin (1, 0)$ is true. To see that this is the case, notice that for $x \in \mathbb{R}$, to say $x \in (1, 0)$ means $1 < x$ and $x < 0$. Hence, to say $x \notin (1, 0)$ means $x \leq 1$ or $0 \leq x$. The statement '$x \leq 1$ or $0 \leq x$' is true for all values of x in the real numbers.

Subsets and Set Equality

Given two sets A and B, whose elements belong to a common universe of discourse U, to say that A is a **subset** of B means that B contains all of the elements of A and possibly, but not necessarily, more. Since mathematics requires the use of clear and precise language, we will give this definition formally in symbolic form:

Definition 0.4.3. For sets A and B whose elements belong to the universe of discourse U, A is a **subset** of B, denoted $A \subseteq B$, means

$$\forall x \in U, \text{ if } x \in A, \text{ then } x \in B.$$

For example, the number systems discussed earlier have the following inclusions

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Although it may seem unnecessary, we provide an explicit interpretation of what it means for two sets to be **equal**.

For sets A and B whose elements belong to the universe of discourse U, $A = B$ means

$$A \subseteq B \text{ and } B \subseteq A.$$

Notice that if we write out this definition in terms of the definitions of $A \subseteq B$ and $B \subseteq A$, we have that $A = B$ means

$$\forall x \in U, \text{ if } x \in A \text{ then } x \in B, \text{ and } \forall x \in U, \text{ if } x \in B \text{ then } x \in A.$$

Equivalently, this can be written as

$$\forall x \in U, \ x \in A \text{ if and only if } x \in B.$$

Hence two sets are equal means that the sets have exactly the same elements.

The reason it is necessary to specify this, is that in general two objects are considered **equal** provided they are one and the same object. In the case of sets, however, the notion of equality makes reference only to the elements of the sets and not to anything pertaining to containment of those elements. This can hopefully provide a better intuitive view of what the word *set* is meant to signify. The set is determined only by its elements. Hence, we do not view a set as a container with several objects inside. In this flawed view, the container is seen as a substance in itself that has an identity beyond the objects that it contains. In such a view, two containers could be interpreted as distinct even though the objects they contain are the same; the additional identity of the container provides the distinction. This is not the case with sets. As set is *only* a collective reference to its elements and has no other distinguishing properties or characteristics. Hence the method by which the elements are collected, or any other property related to the containment of the elements does not contribute to the identity of the set. Only the collective identities of the elements determine the identity of the set.

To make this point more clear, consider the example

$$A = \left\{ x \in \mathbb{R} \;\middle|\; \exists a \in \mathbb{Z},\ x = \sin\left(\frac{a\pi}{2}\right) \right\}$$

$$B = \{x \in \mathbb{R} \mid x \in \mathbb{Z} \text{ and } x^2 < 2\}.$$

The only elements in A are -1, 0, and 1. The same is true for B. Because the two sets contain exactly the same elements, we can say that $A \subseteq B$ and $B \subseteq A$; hence $A = B$. Thus A and B are considered to be identical, regardless of the fact that their elements were collected in different ways.

In the case where $A \subseteq B$ but $A \neq B$, we say that A is a **proper subset** of B. This is often denoted as $A \subsetneq B$. It is worth while to take a minute to dissect the statement '$A \subseteq B$ but $A \neq B$.' Since $A = B$ means $A \subseteq B$ and $B \subseteq A$, the statement $A \neq B$ can only mean $A \not\subseteq B$ or $B \not\subseteq A$. Hence, in the case where $A \subsetneq B$, we must have $A \subseteq B$ and $B \not\subseteq A$. That is,

$$\forall x \in U,\ \text{if } x \in A \text{ then } x \in B, \text{ and } \exists y \in U,\ y \in B \text{ and } y \notin A.$$

Complements

It is often useful to describe a set by the objects that are not elements. For example, we define the irrational numbers to be all of the real numbers that are not rational. To formalize this idea, we introduce the **complement** of a set.

Definition 0.4.4. Let A be a set whose elements are in the universe of discourse U. We define the **complement** of A, denoted A^c, to be

$$A^c = \{x \in U \mid x \notin A\}.$$

Further, given any two sets A and B, we define the **complement of A relative to B**, denoted $B \setminus A$ to be

$$B \setminus A = \{x \in U \mid x \in B \text{ and } x \notin A\}.$$

For a simple example, we may observe that in the universe of discourse $\mathbb{Z}$, the complement of the even integers is the odd integers, or that

$$\{1, 2, 3, 4\} \setminus \{1, 4\} = \{2, 3\}.$$

For now, the intention is not to examine these concepts in any great detail. A more rigorous treatment will be given in chapter 2. Presently, it will suffice to give the formal definitions of some basic set notation, for reference purposes in the coming chapters, and to develop a brief intuitive view of that which these notations represent.

Chapter 1

Structure of a Mathematical Proof

The linguistic rigor introduced in the previous section will be maintained throughout the course. Clear, precise language is the first requirement for writing mathematics. The second requirement is good definitions. Our definitions are the foundations upon which we build all of our theory.

When a mathematician believes he or she has discovered a mathematical truth, he or she is required to demonstrate this truth using only the following:

What we can use in a mathematical proof

1. Definitions
2. Rules of Logic
3. Prior theorems

In particular, we may not appeal to our intuition about what is true and what is false when writing a mathematical proof. Developing a good mathematical intuition is important, because it is often what leads us to our discoveries. However, intuition varies from one mathematician to another and can often deceive us. It is therefore not considered a valid justification of truth in a mathematical demonstration.

Since we have not proven any results as of yet, in the early stages of our theoretical development we will only have definitions and logic available to us. We begin by attempting a clear, precise definition of a *real number*. There are several different systems of numbers in mathematics, including natural numbers, integers, rational numbers, and real numbers. We will define each of these systems individually, however the observant reader will notice many similarities between the definitions.

1.1 The Real Numbers

Intuitively, the real numbers may be viewed as the set of points on a continuous unbroken line extending infinitely in both directions. We denote the set of real numbers with the symbol $\mathbb{R}$.

The definition we will give for the real numbers is what is known as an **axiomatic definition**. **Axioms** are defining properties of an object. They are propositions that are true of the object, by definition of the object. We give an *axiomatic definition* of the real numbers by listing several *axioms* of the real numbers and defining the real numbers as *any system satisfying these axioms*.

Definition 1.1.1. *The system of* **real numbers**, *denoted* $\mathbb{R}$ *is defined to be a set, containing constants* 0 *and* 1 *with* $0 \neq 1$, *binary operations given by* $(x, y) \mapsto x + y$ *and* $(x, y) \mapsto xy$, *unary operations given by* $x \mapsto -x$ *and for* $x \neq 0$, $x \mapsto x^{-1}$, *and a relation* $<$, *satisfying the following axioms:*

A1 *For all* $x, y \in \mathbb{R}$, $x + y = y + x$. *(Addition is commutative)*

A2 *For all* $x, y, z \in \mathbb{R}$, $(x + y) + z = x + (y + z)$. *(Addition is associative)*

A3 *For every* $x \in \mathbb{R}$, $x + 0 = x$ *and* $0 + x = x$. *(*0 *is an additive identity)*

A4 *For every* $x \in \mathbb{R}$, $x + (-x) = 0$ *and* $(-x) + x = 0$. *(*$-x$ *is an additive inverse of* x*)*

M1 *For all* $x, y \in \mathbb{R}$, $xy = yx$. *(Multiplication is commutative)*

M2 *For all* $x, y \in \mathbb{R}$, $(xy)z = x(yz)$. *(Multiplication is associative)*

M3 *For every* $x \in \mathbb{R}$, $x1 = x$ *and* $1x = x$. *(*1 *is a multiplicative identity)*

M4 *For all* $x \in \mathbb{R}$ *with* $x \neq 0$, $xx^{-1} = 1$ *and* $x^{-1}x = 1$. *(*x^{-1} *is a multiplicative inverse of non-zero* x*)*

DL *For all* $x, y, z \in \mathbb{R}$, $x(y + z) = (xy) + (xz)$ *and* $(y + z)x = (yx) + (zx)$. *(Multiplication distributes over addition)*

O1 *For all* $x, y \in \mathbb{R}$, *exactly one of* $x < y$, $x = y$, *or* $y < x$ *holds. (Trichotomy)*

O2 *For all* $x, y, z \in \mathbb{R}$, *if* $x < y$ *and* $y < z$ *then* $x < z$. *(Transitivity)*

O3 *For all* $x, y, z \in \mathbb{R}$, *if* $x < y$ *then* $x + z < y + z$. *(Addition preserves order)*

O4 *For all* $x, y, z \in \mathbb{R}$, *if* $x < y$ *and* $0 < z$, *then* $xz < yz$. *(Multiplication by a positive preserves order)*

C *If* A *and* B *are non-empty subsets of* $\mathbb{R}$ *such that for all* $a \in A$ *and all* $b \in B$, $a < b$, *then there is an element* $x \in \mathbb{R}$ *such that for all* $a \in A$, $a \leq x$, *and for all* $b \in B$, $x \leq b$. *(Completeness)*

To say that the operation given by $(x, y) \mapsto x + y$ is a *binary operation* means that $+$ combines a pair of real numbers (x, y) into a single real number $x + y$. This means that for all $x, y \in \mathbb{R}$, $x + y \in \mathbb{R}$ and that for $x, y, a, b \in \mathbb{R}$, if $x = a$ and $y = b$ then $x + y = a + b$. Similarly, to say that there is a binary operation given by $(x, y) \mapsto xy$ means that for all $x, y \in \mathbb{R}$, $xy \in \mathbb{R}$ and that for $x, y, a, b \in \mathbb{R}$, if $x = a$ and $y = b$ then $xy = ab$.

That there is a unary operation given by $x \mapsto -x$ means for every $x \in \mathbb{R}$, $-x \in \mathbb{R}$, and for all $x, a \in \mathbb{R}$, if $x = a$ then $-x = -a$. Similarly, for $x \in \mathbb{R}$ with $x \neq 0$ we have $x^{-1} \in \mathbb{R}$, and for all $x, a \in \mathbb{R}$ with $x \neq 0$ and $a \neq 0$, if $x = a$ then $x^{-1} = a^{-1}$.

The relation $<$ is intended to convey the usual intuitive meaning of relative size. However, formally, we require only that it is a relation, meaning for $x, y \in \mathbb{R}$, $x < y$ is a statement that is either true or false, and this relation obeys properties O1 through O4. We will also add to this the following commonly used notation:

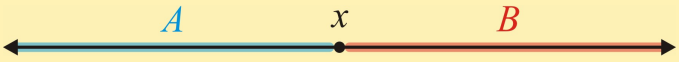
Notation

For $x, y \in \mathbb{R}$, the notation '$x \leq y$' means '$x < y$ or $x = y$.' Similarly, '$x \geq y$' means '$x > y$ or $x = y$.'

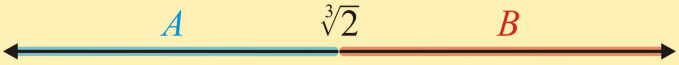
The final axiom (completeness) is the most difficult to decipher. It is worthwhile to pause a minute to comment on this axiom and its intended meaning.

A remark about the completeness axiom

The completeness axiom (axiom C) describes in what sense the real numbers are continuous and unbroken. If we imagine the real numbers as a line extending infinitely in both directions and we cut the line into two pieces A and B, then the point at which the cut is made must be a real number. That is, there is a real number x lying between all the points in piece A and the points in piece B.



Note that this condition is not satisfied by the rational numbers, since we may divide the rational numbers into two pieces $A = \{x \in \mathbb{Q} \mid x^3 \leq 2\}$ and $B = \{x \in \mathbb{Q} \mid x^3 \geq 2\}$. In this case, the cut is made at a gap in the rational numbers. That is, there is no rational number lying between the points in piece A and the points in piece B, since $\sqrt[3]{2}$ is irrational.



All of the properties listed as axioms are indeed properties that a set we call the real numbers should have. There are, however, several more properties of the real numbers that we know are true, which are not listed. Any other properties of the real numbers will need to be proven using our definition. To illustrate how this is done, we will prove some very trivial properties about the real numbers.

To ensure that we are only using the axioms, logic, and previously proven propositions, we will cite the source of each step in the proof. In general, this much citation is not needed in a proof. As propositions and their proofs become more involved, we will drop this practice. When writing your own proofs, you may freely use any part of a definition, logic, and previously proven proposition. Strict citation of everything used in the proof will become less necessary as the course progresses. However, references to propositions and explanations of logical steps are always valuable if they add clarity to your argument.

A good rule of thumb to ensure we are liberal enough with our citations and explanations is to write as if the reader is a fellow student in the class. That is, we should assume that the reader is only familiar with the concepts that have been introduced as of the particular stage in the course in which we are writing. Further, we should assume that the reader is only as comfortable with the material as a student in the class would be at that point in time. For example, since we have only just introduced the axioms of the real numbers, a student would not be expected to have committed them to memory at this point in time. Hence, in our proofs at this stage, we should include references to these axioms wherever we use them. Later, as we grow more familiar with these axioms and the references to them consequently become tedious and unnecessary, we will begin to drop the more obvious of these references.

Remember

A proof is written for the purpose of demonstrating the truth of your statement *to a reader*. Helpful explanations of how you are making your steps can make your proofs easier to read.

Proving Statements with Universal Quantifiers

The first proposition we will prove is that any number multiplied by zero will give zero as a result. In symbolic form, this can be written as $\forall x \in \mathbb{R}$, $0x = 0$ and $x0 = 0$. This may seem intuitively obvious, and it is. In fact, any set claiming to be the set of real numbers would need to abandon such a claim if $\forall x \in \mathbb{R}$ $0x = 0$ and $x0 = 0$ were found to be false. Hence, for a proposition this intuitive, the purpose of the proof is not so much to determine its truth, but rather to ensure that its truth can be derived from our definition. In addition, it provides a good example of the process by which one derives further properties from the defining axioms. This process, and the various techniques involved, will occupy our attention for the remainder of the chapter. In particular, in the case of the proposition $\forall x \in \mathbb{R}$, $0x = 0$ and $x0 = 0$, since this is a general statement about *all real numbers*, we are forced to consider what must be done in order to prove such statements containing *universal quantifiers*.

We add notes, pointing out the structure of the proof, in the left margin. These notes are not part of the proof itself and are only included to indicate the proof structures and techniques in use.

Proposition 1.1.1.

$\forall x \in \mathbb{R}$, $x0 = 0$ and $0x = 0$.

Proof.
Let $x \in \mathbb{R}$ ← Arbitrary element ▶
- The constants 0 and 1 are real numbers.
- Since $1 + 0 = 1$, by axiom A3, we have $x(1 + 0) = x1$.
- $(x1) + (x0) = x1$, by axiom DL.
- $x + (x0) = x$, by axiom M3.
- Applying the additive inverse unary operation, $-x \in \mathbb{R}$; hence $-x + (x + (x0)) = -x + x$.
- $(-x + x) + (x0) = -x + x$, by axiom A2.
- $0 + (x0) = 0$, by axiom A4.
- $x0 = 0$, by axiom A3.
- In addition to this, $0x = 0$, by axiom M1.
- Therefore, $x0 = 0$ and $0x = 0$.

Demonstration

Therefore, $\forall x \in \mathbb{R}$, $x0 = 0$ and $0x = 0$. ◻ ← Conclusion ▶

Notice, in the above proof, that we begin by letting x represent an arbitrary real number. We do this because the proposition we are proving,

$$\text{`}\forall x \in \mathbb{R},\ x0 = 0 \text{ and } 0x = 0,\text{'}$$

is a statement about *all real numbers*. It is not enough to prove the statement for one particular real number. i.e. we do not merely prove $1(0) = 0$, or $2(0) = 0$. We must prove *every* real number multiplied by zero gives zero; hence we must prove $x0 = 0$ for a nonspecific, *arbitrary*, real number x.

In general, when we are proving any statement about *all real numbers*, we will prove the statement for an arbitrary real number. More generally, proofs of propositions with the form '$\forall x \in U$, $P(x)$,' where $P(x)$ is an open sentence and U is the universe of discourse for the variable x, will have the following form:

Proof of $\forall x \in U$, $P(x)$:

Proof.
Let $x \in U$. ← Arbitrary element ▶
- ⋮
- *Demonstrate* $P(x)$.
- ⋮
- Therefore $P(x)$.

Demonstration

Therefore, $\forall x \in U$, $P(x)$. ◻ ← Conclusion ▶

The next proposition we consider is that for all real numbers x and y,

$$(-x)y = -(xy).$$

Notice that this proposition is again a statement about *all real numbers* x and y; hence our proof will involve arbitrary real numbers x and y. Indeed, the first line of the proof will be 'Let $x, y \in \mathbb{R}$.'

Proposition 1.1.2.

$\forall x, y \in \mathbb{R}, (-x)y = -(xy)$.

Proof.
Arbitrary elements ▶ Let $x, y \in \mathbb{R}$.
Demonstration
$(-x)y + (xy + (-(xy))) = ((-x)y + xy) + (-(xy))$, by axiom A2.
$(-x)y + 0 = ((-x) + x)y + (-(xy))$, by axioms A4 and DL.
$(-x)y = (0)y + (-(xy))$, by axioms A3 and A4.
$(-x)y = 0 + (-(xy))$, by proposition 1.1.1.
Conclusion ▶ Therefore, $(-x)y = -(xy)$, by axiom A4.
Therefore, $\forall x, y \in \mathbb{R}, (-x)y = -(xy)$. □

For practice in identifying the axioms that allow us to perform algebraic manipulations, the reader is invited to fill in the blanks in the following proof:

Proposition 1.1.3.

$\forall x, y \in \mathbb{R}, (-x)(-y) = xy$.

Proof.
Arbitrary elements ▶ Let $x, y \in \mathbb{R}$.
Demonstration
$(-x)(-y) + (-(xy) + xy) = ((-x)(-y) + (-(xy))) + xy$, by axiom _____.
$(-x)(-y) + 0 = ((-x)(-y) + (-x)y) + xy$, by axiom _____ and prop. _____.
$(-x)(-y) = (-x)((-y) + y) + xy$, by axioms _____ and _____.
$(-x)(-y) = (-x)(0) + xy$, by axiom _____.
$(-x)(-y) = 0 + xy$, by proposition _____.
Conclusion ▶ Therefore, $(-x)(-y) = xy$, by axiom _____.
Therefore, $\forall x, y \in \mathbb{R}, (-x)(-y) = xy$. □

Given the axioms of the real numbers, we see that the only real numbers whose existence is explicitly given in the definition are 0 and 1. Of course we know that there are more real numbers than only these two. Since the existence of other real numbers is not given in the definition, it will need to be proven. To prove that there are real numbers other than 0 and 1, we need to use the order axioms. That the non-order axioms are not sufficient on their own to guarantee the existence of more numbers can be seen by noticing that the set $\{0, 1\}$ satisfies all of the non-order axioms if we define addition and multiplication by the following tables:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

The reader may wish to verify that this system does in fact satisfy axioms A1, A2, A3, A4, M1, M2, M3, M4, and DL.

Proof By Contradiction

We introduce a proof technique known as *proof by contradiction*, or *reductio ad absurdum*. In this technique, we begin by assuming the negation of the proposition we wish to prove. From this assumption, we then derive a logical contradiction, demonstrating that the assumption must be false. We will illustrate this technique by using it to prove the existence of more real numbers. We begin by investigating the order relation between our two known real numbers, 0 and 1. If fact, we will demonstrate that $0 < 1$. We will then prove the existence of the number 2, which we define as $1 + 1$.

Proposition 1.1.4.

$0 < 1$

Proof.
Assumption ► Suppose that $0 \not< 1$
Demonstration
- By the trichotomy axiom, we have either $1 < 0$ or $1 = 0$.
- By axiom M3, we have that $1 \neq 0$, hence it must be the case that $1 < 0$.
- Then $1 + (-1) < 0 + (-1)$, by axiom O3.
- This reduces to $0 < -1$, by axioms A3 and A4.
- By axiom O4 we then have $(0)(-1) < (-1)(-1)$.
- Therefore, $0 < (-1)(-1)$, by proposition 1.1.1,
- and hence $0 < (1)(1)$, by proposition 1.1.3.
- This is then $0 < 1$, due to axiom M3.

Contradiction ► We now have $0 < 1$ and $0 \not< 1$, which is a logical contradiction.
Therefore, our initial assumption that $0 \not< 1$ must be false.
Conclusion ► Therefore $0 < 1$. □

Notice that, in this proof, we assume the negation of the statement we are proving and derive a logical contradiction from that assumption. In doing so, we demonstrate that the *negation* of our proposition is false, because it implies a contradiction. Since the negation of our proposition is shown to be false, we may then conclude that our proposition is true. In general, to prove a proposition P by contradiction, we use the following structure:

Proof by contradiction of a proposition P:

Proof.
Assumption ► Suppose $\neg P$.
Demonstration
    ⋮
    Demonstrate any contradiction.
    ⋮
Contradiction ► Therefore R and $\neg R$, which is a contradiction.
Conclusion ► Therefore P. □

The next two propositions demonstrate that the real number $1 + 1$ is neither 1 nor 0. It is therefore a new real number, which proves the existence of real numbers beyond 0 and 1. In both of the following propositions, we will use the *proof by contradiction* technique.

Proposition 1.1.5.

$1 + 1 \neq 1$

Proof.
Assumption ► Suppose $1 + 1 = 1$.
Demonstration
    Then $(1 + 1) + (-1) = 1 + (-1)$.
    By associativity, we have $1 + (1 + (-1)) = 1 + (-1)$.
    Therefore $1 + 0 = 0$,
    and hence $1 = 0$.
    However, by axiom M3, we have $1 \neq 0$.
Contradiction ► Therefore, $1 = 0$ and $1 \neq 0$, which is a contradiction.
Conclusion ► Therefore, $1 + 1 \neq 1$ □

Proposition 1.1.6.

$1 + 1 \neq 0$

Proof.
Assumption ► Suppose $1 + 1 = 0$.
Demonstration
$0 < 1$ from proposition 1.1.4.
Therefore, $0 + 1 < 1 + 1$.
Hence $1 < 1 + 1$, by axiom A4.
Our assumption reduces this to $1 < 0$.
Contradiction ► Therefore $0 < 1$ and $1 < 0$, which contradicts axiom O1.
Conclusion ► Therefore, $1 + 1 \neq 0$ □

From proposition 1.1.5, proposition 1.1.6, we see that $1 + 1$ is a new real number. The common notation for this real number is 2. We now have the existence of the real number 2 and the fact that $1 + 1 = 2$.

Proving Implications with a 'Direct Proof'

A direct proof is one method we can use to prove a statement of the form 'If P then Q,' where P and Q are propositions. In an implication of the form 'If P then Q,' we call the proposition P the **antecedent** and the proposition Q the **consequent**. In a direct proof, we assume that the *antecedent* P is true and use our assumption to derive the *consequent* Q, thereby proving that if P is true, then Q must also be true. A direct proof follows the form:

Proof of if P then Q.

Proof.
Assumption ► Assume P.
Demonstration
⋮
Demonstrate Q.
⋮
Conclusion ► Therefore Q.
Therefore, if P then Q. □

We will continue our development of the basic properties of real numbers with several examples of proofs using the *direct proof* method.

Proposition 1.1.7.

$\forall x \in \mathbb{R}$, if $x < 0$ then $0 < -x$.

Proof.
Let $x \in \mathbb{R}$. ← Arbitrary element ▶
  Assume $x < 0$ ← Assumption ▶
    Then $-x + x < -x + 0$.
    Therefore, $0 < -x$. ← Conclusion ▶
  Therefore, if $x < 0$ then $0 < -x$. ← Conclusion ▶
Therefore, $\forall x \in \mathbb{R}$, if $x < 0$ then $0 < -x$. □

Proposition 1.1.8.

$\forall x, y, a \in \mathbb{R}$, if $a + x = a + y$ then $x = y$.

Proof.
Let $x, y, a \in \mathbb{R}$. ← Arbitrary elements ▶
  Assume $a + x = a + y$ ← Assumption ▶
    Then $-a + (a + x) = -a + (a + y)$.
    By associativity, $(-a + a) + x = (-a + a) + y$.
    Hence, $0 + x = 0 + y$.
    Therefore, $x = y$. ← Conclusion ▶
  Therefore, if $a + x = a + y$ then $x = y$. ← Conclusion ▶
Therefore, $\forall x, y, a \in \mathbb{R}$, if $a + x = a + y$ then $x = y$. □

Proposition 1.1.9.

$\forall x, y, z \in \mathbb{R}$, if $x < y$ and $z < 0$ then $yz < xz$.

Proof.
Let $x, y, z \in \mathbb{R}$. ← Arbitrary elements ▶
  Assume $x < y$ and $z < 0$. ← Assumption ▶
    Then $0 < -z$ by proposition 1.1.7.
    We now have $x < y$ and $0 < -z$.
    By axiom O4, we then have $x(-z) < y(-z)$.
    Therefore, $-(xz) < -(yz)$ by proposition 1.1.2.
    Adding xz to both sides gives us $xz + (-(xz)) < xz + (-(yz))$.
    Hence $0 < xz + (-(yz))$.
    Adding yz to both sides gives us $0 + yz < xz + (-(yz) + yz)$.
    Hence, $0 + yz < xz + 0$.
    Therefore, $yz < xz$. ← Conclusion ▶
  Therefore, if $x < y$ and $z < 0$ then $yz < xz$. ← Conclusion ▶
Therefore, $\forall x, y, z \in \mathbb{R}$, if $x < y$ and $z < 0$ then $yz < xz$. □

Proving Statements with Existential Quantifiers

To prove a statement of the form $\exists x \in U$, $P(x)$, we must demonstrate the existence of at least one element $x \in U$ that satisfies the open sentence $P(x)$. One technique for proving *existence* is **construction**. In this method, we assign a specific value to the constant x. The specific value of x that we choose must be an element of the universe of discourse U, and it must satisfy the desired property $P(x)$. We then demonstrate that our chosen value of x does indeed have the property $P(x)$. We illustrate this technique with a very basic example, followed by some more involved examples.

Proposition 1.1.10.

$\exists x \in \mathbb{R}$, $x < 0$.

Proof.
Set a value ▶ Put $x = -1$.
Demonstration [Since $0 < 1$, we have $0 + (-1) < 1 + (-1)$; hence $-1 < 0$.
Conclusion ▶ Therefore $x < 0$.
Therefore, $\exists x \in \mathbb{R}$, $x < 0$. □

In the above example, we proved $\exists x \in \mathbb{R}$, $x < 0$ by identifying an example of a real number x with that property. In general, to prove a statement of the form $\exists x \in U$, $P(x)$, we may exhibit *one example* of a value of x that makes $P(x)$ true. We then demonstrate that $P(x)$ is indeed true for the x we found.

Proof of $\exists x \in U$, $P(x)$:

Proof.
Set a value ▶ Put $x =$ □.
Demonstration ⎡ ⋮
⎢ *Demonstrate* $P(x)$.
⎣ ⋮
Conclusion ▶ Therefore, $P(x)$.
Therefore, $\exists x \in U$, $P(x)$. □

Continuing with our investigation of the basic properties of real numbers, we can now show that one may construct more and more real numbers without end. In fact, the real numbers are unbounded. We show this by proving

$$\forall x \in \mathbb{R},\ \exists y \in \mathbb{R},\ x < y.$$

Notice that this proposition contains a universal quantifier followed by an existential quantifier. To prove this statement, we will first introduce an arbitrary real number x. For this x, we then need to demonstrate the statement '$\exists y \in \mathbb{R},\ x < y$.' To do so, we must prove the *existence* of the real number y, hence we must *exhibit* a real number y that has the desired property of being larger than x. We do this as follows:

Proposition 1.1.11.

$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x < y.$

Proof.
Arbitrary element ► Let $x \in \mathbb{R}$.
Set a value ► Put $y = x + 1$.
Demonstration ► By proposition 1.1.4, $0 < 1$.
We then have $x + 0 < x + 1$.
Conclusion ► Therefore, $x < y$.
Conclusion ► Therefore, $\exists y \in \mathbb{R}, x < y$.
Therefore, $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, x < y$. □

Notation

For $x, y, z \in \mathbb{R}$, the notation $x < y < z$ means $x < y$ and $y < z$. Also, for $x, y \in \mathbb{R}$ with $y \neq 0$, $\frac{x}{y}$ means xy^{-1}. Note that by commutativity, this is the same as $y^{-1}x$.

Proposition 1.1.12.

$\forall x, y \in \mathbb{R}$, if $x < y$ then $\exists z \in \mathbb{R}$, $x < z < y$.

Proof.
Let $x, y \in \mathbb{R}$. — Arbitrary elements ▸
  Assume $x < y$. — Assumption ▸
    Put $z = \dfrac{x+y}{2}$. — Set a value ▸
      Since $x < y$, we have $x + x < x + y$.
      Therefore, $2x < x + y$.
      By axiom O4, we then have $x < \dfrac{x+y}{2}$.
      Therefore, $x < z$.
      Further, since $x < y$, we have $x + y < y + y$.
      Therefore, $x + y < 2y$.
      We then have $\dfrac{x+y}{2} < y$.
      Therefore, $z < y$.
      We now have $x < z$ and $z < y$.
      Therefore, $x < z < y$. — Conclusion ▸
    Therefore, $\exists z \in \mathbb{R}$, $x < z < y$. — Conclusion ▸
  Therefore, if $x < y$ then $\exists z \in \mathbb{R}$, $x < z < y$. — Conclusion ▸
Therefore, $\forall x, y \in \mathbb{R}$, if $x < y$ then $\exists z \in \mathbb{R}$, $x < z < y$. □

Demonstration

Proving Implications by 'Contraposition'

Recall from section 0.3 that any implication 'if P, then Q' can be rewritten in its *contrapositive* form: 'if $\neg Q$, then $\neg P$.' The resulting proposition is necessarily equivalent to the original implication because the corresponding logical operators $x \Rightarrow y$ and $\neg y \Rightarrow \neg x$ are equivalent. Thus, to prove a statement of the form 'if P, then Q,' we can prove the equivalent statement 'if $\neg Q$, then $\neg P$." We do this by applying the *direct proof* method to the contrapositive form 'if $\neg Q$, then $\neg P$." That is, to prove a statement of the form 'if P, then Q,' we can assume $\neg Q$ and demonstrate $\neg P$.

In general, a proof by contraposition has the form:

Proof of if P then Q:

Proof.
Assume $\neg Q$. — Assumption ▸
  ⋮
  Demonstrate $\neg P$.
  ⋮
  Therefore $\neg P$. — Conclusion ▸
Therefore, if $\neg Q$ then $\neg P$. — Contrapositive ▸
Therefore, if P then Q. □

Demonstration

We illustrate this technique by proving the statement

$$\forall x, y \in \mathbb{R}, \text{ if } \underbrace{xy \leq 0}_{P} \text{ then } \underbrace{x \leq 0 \text{ or } y \leq 0}_{Q}.$$

Rewriting the implication in this statement in its contrapositive form gives us the equivalent proposition

$$\forall x, y \in \mathbb{R}, \text{ if } \underbrace{x > 0 \text{ and } y > 0}_{\neg Q} \text{ then } \underbrace{xy > 0.}_{\neg P}$$

We will then assume $x > 0$ and $y > 0$ and demonstrate $xy > 0$.

Proposition 1.1.13.

$\forall x, y \in \mathbb{R}$, if $xy \leq 0$ then $x \leq 0$ or $y \leq 0$.

Proof.
Let $x, y \in \mathbb{R}$. (Arbitrary elements ▶)
  Assume $x > 0$ and $y > 0$. (Assumption ▶)
    Then by axiom O4, $xy > 0y$.
    Therefore $xy > 0$, by proposition 1.1.1.
  Therefore, if $x > 0$ and $y > 0$ then $xy > 0$. (Demonstration [)
  Therefore, if $xy \leq 0$ then $x \leq 0$ or $y \leq 0$. (Conclusion ▶)
Therefore, $\forall x, y \in \mathbb{R}$, if $xy \leq 0$ then $x \leq 0$ or $y \leq 0$. (Contrapositive ▶) (Conclusion ▶) □

For another example, consider the statement

$$\forall a, b \in \mathbb{R}, \text{ if } \underbrace{\forall x \in \mathbb{R},\ a < x \Rightarrow b \leq x,}_{P} \text{ then } \underbrace{b \leq a}_{Q}.$$

Rewriting the implication in its contrapositive form gives us

$$\forall a, b \in \mathbb{R}, \text{ if } \underbrace{a < b}_{\neg Q} \text{ then } \underbrace{\exists x \in \mathbb{R},\ a < x \text{ and } x < b}_{\neg P}.$$

We will then assume $a < b$ and demonstrate $\exists x \in \mathbb{R}$, $a < x$ and $x < b$.

Proposition 1.1.14.

$\forall a, b \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $a < x \Rightarrow b \leq x$, then $b \leq a$.

Proof.
Let $a, b \in \mathbb{R}$. — Arbitrary elements ▶
  Assume $a < b$. — Assumption ▶
    Put $x = \dfrac{a+b}{2}$. — Set a value ▶
      Since $a < b$, we have $a + a < a + b$.
      Therefore, $2a < a + b$.
      By axiom O4, we then have $a < \dfrac{a+b}{2}$.
      Therefore, $a < x$.
      Further, since $a < b$, we have $a + b < b + b$.
      Therefore, $a + b < 2b$.
      We then have $\dfrac{a+b}{2} < b$.
      Therefore, $x < b$.
      We now have $a < x$ and $x < b$. — Demonstration
    Therefore, $\exists x \in \mathbb{R}$, $a < x$ and $x < b$. — Conclusion ▶
  Therefore, if $a < b$ then $\exists x \in \mathbb{R}$, $a < x$ and $x < b$. — Conclusion ▶
  Therefore, if $\forall x \in \mathbb{R}$, if $a < x$ then $b \leq x$, then $b \leq a$. — Contrapositive ▶
Therefore, $\forall a, b \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $a < x \Rightarrow b \leq x$, then $b \leq a$. — Conclusion ▶ □

Proving Implications by Contradiction

Yet another method for proving a statement of the form 'if P then Q' is to use the *proof by contradiction* technique discussed earlier. Recall that in a proof by contradiction, we assume the negation of the statement we are trying to prove and derive a logical contradiction from that assumption. If the statement we wish to prove has the form 'if P then Q,' then its negation will be 'P and $\neg Q$.' Hence, to prove an implication using a proof by contradiction, we use the following form:

Proof of if P then Q:

Proof.
Suppose P and $\neg Q$. — Assumption ▶
  ⋮
  Demonstrate any contradiction. — Demonstration
  ⋮
  Therefore R and $\neg R$, which is a contradiction. — Contradiction ▶
Therefore if P then Q. — Conclusion ▶ □

The above technique is not different from the proof by contradiction technique discussed earlier. In fact it is simply a special case of the earlier proof by contradiction method, in the case where the statement we are proving is an implication. However, since so many mathematical statements contain implications, it can be useful to practice using the proof by contradiction technique in this specific setting. To get accustomed to the application of the proof by contradiction method to implications, we give three examples:

Proposition 1.1.15.

$\forall x \in \mathbb{R}$, if $x \neq 0$, then $x^{-1} \neq 0$.

Proof.
Let $x \in \mathbb{R}$. ← Arbitrary elements ►
  Suppose $x \neq 0$ and $x^{-1} = 0$. ← Assumption ►
    Then $xx^{-1} = x(0)$.
    By axiom M4 and proposition 1.1.1, this becomes $1 = 0$.
    However, by axiom M3, we have $1 \neq 0$.
    We now have the contradiction: $1 = 0$ and $1 \neq 0$. ← Contradiction ►
  Therefore, if $x \neq 0$ then $x^{-1} \neq 0$. ← Conclusion ►
Therefore, $\forall x \in \mathbb{R}$, if $x \neq 0$, then $x^{-1} \neq 0$. ← Conclusion ►
□

(Demonstration: the indented block above)

Proposition 1.1.16.

$\forall x \in \mathbb{R}$, if $x > 0$, then $x^{-1} > 0$.

Proof.
Let $x \in \mathbb{R}$. ← Arbitrary elements ►
  Suppose $x > 0$ and $x^{-1} \leq 0$. ← Assumption ►
    We then have $x^{-1} < 0$ or $x^{-1} = 0$.
    Since $x \neq 0$, proposition 1.1.15 gives us $x^{-1} \neq 0$.
    It must then be the case that $x^{-1} < 0$.
    Since $0 < x$ and $x^{-1} < 0$, by proposition 1.1.9 we have $xx^{-1} < (0)x^{-1}$.
    By axiom M4 and proposition 1.1.1, this becomes $1 < 0$.
    However, by proposition 1.1.4, we have $0 < 1$.
    By trichotomy, $1 < 0$ and $0 < 1$ is a contradiction. ← Contradiction ►
  Therefore, if $x > 0$, then $x^{-1} > 0$. ← Conclusion ►
Therefore, $\forall x \in \mathbb{R}$, if $x > 0$, then $x^{-1} > 0$. ← Conclusion ►
□

(Demonstration: the indented block above)

Proposition 1.1.17.

$\forall x, y \in \mathbb{R}$, if $xy = 0$, then $x = 0$ or $y = 0$.

Proof.
Let $x, y \in \mathbb{R}$. ← Arbitrary elements
  Suppose $xy = 0$ and $x \neq 0$ and $y \neq 0$. ← Assumption
    By axiom M4, there is a real number x^{-1} for which $x^{-1}x = 1$.
    Therefore, $y = (1)y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(0) = 0$. ← Demonstration
    We now have $y = 0$ and $y \neq 0$, which is a contradiction. ← Contradiction
  Therefore, if $xy = 0$, then $x = 0$ or $y = 0$. ← Conclusion
Therefore, $\forall x, y \in \mathbb{R}$, if $xy = 0$, then $x = 0$ or $y = 0$. ← Conclusion □

Three Methods for Proving Implications

We have now discussed three methods for proving statements of the form 'if P then Q.' These methods are *direct proof*, *contraposition*, and *proof by contradiction*. Their structures are as follows:

Direct Proof

Proof of if P then Q:

Proof.
Assume P.
  ⋮
  Demonstrate Q.
  ⋮
  $\therefore Q$.
$\therefore$ if P then Q. □

Contraposition

Proof of if P then Q:

Proof.
Assume $\neg Q$.
  ⋮
  Demonstrate $\neg P$.
  ⋮
  $\therefore \neg P$.
$\therefore$ if $\neg Q$ then $\neg P$.
$\therefore$ if P then Q. □

Contradiction

Proof of if P then Q:

Proof.
Suppose P and $\neg Q$.
  ⋮
  Find a contradiction.
  ⋮
  $\therefore R$ and $\neg R$.
$\therefore$ if P then Q. □

Notice that the assumption in a proof by contradiction is the combined assumption of both the direct proof and the proof by contraposition. However, this superior assumption comes at a price: The direction of the proof is no longer decided. When doing a direct proof or a proof by contraposition, the direction of the proof is certain, and it is often useful to have knowledge of the conclusion one is working towards. On the other hand, in a proof by contradiction, we have only our assumption. It often takes some creativity to steer our assumption into a contradiction. There is no general rule to tell us which method we will find easiest. In practice, we try to use the method that results in the most natural and elegant proof.

Proof by Exhaustion (Cases)

One technique that has grown in popularity since computers have started to be used in mathematical proofs is called **proof by exhaustion.** We can use this method if there are only finitely many elements in our universe of discourse, or if the universe of discourse can be divided into finitely many categories (such as the integers into even and odd, or the real numbers into positive, negative, and zero). We can prove a statement with a universal quantifier by examining all of the possible values, or categories, the variable can take and proving the statement for each of these individually. For example:

Proposition 1.1.18.

$\forall x \in \mathbb{R}$, $x^2 \geq 0$.

Proof.
Let $x \in \mathbb{R}$. — Arbitrary element ►
  By the trichotomy axiom, we have either $x > 0$ or $x < 0$, or $x = 0$.
  We will consider each of these three cases.
  Case 1: $x > 0$.
    We have $x(x) > 0(x)$, by axiom O4.
    Hence, $x^2 > 0$, by proposition 1.1.1.
    Then the statement $x^2 > 0$ or $x = 0$ is true.
    Therefore, $x^2 \geq 0$. — Conclusion ►
  Case 2: $x < 0$.
    We have $-x + x < -x + 0$, hence $0 < -x$ by axioms A3 and A4.
    By axiom O4, we then have $0(-x) < (-x)(-x)$.
    By proposition 1.1.1, this becomes $0 < (-x)(-x)$.
    By proposition 1.1.3, we then have $0 < (x)(x)$.
    Therefore, $x^2 > 0$.
    Therefore, $x^2 \geq 0$. — Conclusion ►
  Case 3: $x = 0$.
    Then $(x)(x) = (0)(0)$.
    Therefore, $x^2 = 0$, by proposition 1.1.1.
    Therefore, $x^2 \geq 0$. — Conclusion ►
  In all cases we have $x^2 \geq 0$.
Therefore, $\forall x \in \mathbb{R}$, $x^2 \geq 0$. □

Demonstration
Demonstration
Demonstration

Note that *every case ends with the same conclusion*, that being the statement that is to be proven. This is an essential feature of a proof by exhaustion; we must end every case by concluding that the statement we are proving is true in that case. Further, notice that we have used the trichotomy axiom to prove that the cases we are considering cover the entire universe of discourse. In general, we must ensure that the cases chosen *exhaust all possibilities*. That is, we must show that every element in the universe of discourse, that is open for consideration under our hypotheses, falls into at least one of the categories being considered as cases.

The next three examples prove that axioms O2, O3, and O4 hold for the $\leq$ relation just as they do with the $<$ relation.

Proposition 1.1.19.

$\forall x, y, z \in \mathbb{R}$, if $x \leq y$ and $y \leq z$, then $x \leq z$.

Proof.
Let $x, y, z \in \mathbb{R}$. (Arbitrary element ►)
  Assume $x \leq y$ and $y \leq z$.
    Then ($x < y$ or $x = y$) and ($y < z$ or $y = z$).
    Case 1: $x < y$ and $y < z$
      In this case, we have $x < z$ by transitivity.
      Therefore, $x \leq z$.
    Case 2: $x < y$ and $y = z$
      Then $x < z$.
      Therefore, $x \leq z$.
    Case 3: $x = y$ and $y < z$
      Then $x < z$.
      Therefore, $x \leq z$.
    Case 4: $x = y$ and $y = z$.
      Then $x = z$.
      Therefore, $x \leq z$.
    In all cases, $x \leq z$.
  Therefore, if $x \leq y$ and $y \leq z$, then $x \leq z$.
Therefore, $\forall x, y, z \in \mathbb{R}$, if $x \leq y$ and $y \leq z$, then $x \leq z$. □

(Demonstration [Conclusion ►)

Proposition 1.1.20.

$\forall x, y, z \in \mathbb{R}$, if $x \leq y$, then $x + z \leq y + z$.

Proof.
Let $x, y, z \in \mathbb{R}$. (Arbitrary element ►)
  Assume $x \leq y$.
    Then $x < y$ or $x = y$.
    Case 1: $x < y$
      Hence, $x + z < y + z$ by axiom O3.
      Therefore, $x + z \leq y + z$.
    Case 2: $x = y$
      Then $x + z = y + z$.
      Therefore, $x + z \leq y + z$.
    In both cases, $x + z \leq y + z$.
  Therefore, if $x \leq y$, then $x + z \leq y + z$.
Therefore, $\forall x, y, z \in \mathbb{R}$, if $x \leq y$, then $x + z \leq y + z$. □

(Demonstration [Conclusion ►)

Proposition 1.1.21.

$\forall x, y, z \in \mathbb{R}$, if $x \leq y$ and $0 \leq z$, then $xz \leq yz$.

Proof.
Let $x, y, z \in \mathbb{R}$.
    Assume $x \leq y$ and $0 \leq z$.
        Then $x < y$ or $x = y$.
        Case 1: $x < y$
            Since $0 \leq z$, we have $0 < z$ or $0 = z$.
            We consider these two subcases.
            Case 1.1: $0 < z$.
                Since $x < y$ and $0 < z$, we have $xz < yz$ by axiom O4.
                Therefore, $xz \leq yz$.
            Case 1.2: $0 = z$.
                In this subcase, we have $xz = 0$ and $yz = 0$; hence $xz = yz$.
                Therefore, $xz \leq yz$.
            In both subcases, $xz \leq yz$.
        Case 2: $x = y$
            Then $xz = yz$.
            Therefore, $xz \leq yz$.
        In all cases, $xz \leq yz$.
    Therefore, if $x \leq y$ and $0 \leq z$, then $xz \leq yz$.
Therefore, $\forall x, y, z \in \mathbb{R}$, if $x \leq y$ and $0 \leq z$, then $xz \leq yz$. □

The max, min, and absolute value functions

We take some time now to introduce the max, min, and absolute value functions. These are functions of real numbers that will be used throughout the course and provide an opportunity to practice some of the proof techniques discussed above.

Definition 1.1.2. For $x, y \in \mathbb{R}$, we define the **maximum** of x and y to be

$$\max(x, y) = \begin{cases} x & \text{if } x \geq y \\ y & \text{if } x < y \end{cases}.$$

Similarly, we define the **minimum** of x and y to be

$$\min(x, y) = \begin{cases} x & \text{if } x \leq y \\ y & \text{if } y < x \end{cases}.$$

Proposition 1.1.22.

$\forall x, y \in \mathbb{R}$, $\max(x, y) \geq x$ and $\max(x, y) \geq y$.

Proof.
Let $x, y \in \mathbb{R}$.
We have either $x \geq y$ or $x < y$, which we consider in cases.
Case 1: $x \geq y$.
In this case, we have $\max(x, y) = x$.
Hence, $\max(x, y) \geq x$.
Since $\max(x, y) = x$ and $x \geq y$, we have $\max(x, y) \geq y$.
Therefore, $\max(x, y) \geq x$ and $\max(x, y) \geq y$.
Case 2: $x < y$.
In this case, we have $\max(x, y) = y$.
Hence, $\max(x, y) \geq y$.
Since $\max(x, y) = y$ and $x < y$, we have $x < \max(x, y)$.
Therefore, $\max(x, y) \geq x$.
We then have $\max(x, y) \geq x$ and $\max(x, y) \geq y$.
In both cases, we have $\max(x, y) \geq x$ and $\max(x, y) \geq y$.
Therefore, $\forall x, y \in \mathbb{R}$, $\max(x, y) \geq x$ and $\max(x, y) \geq y$. □

In the next example, we prove a statement of the form 'P if and only if Q.' The meaning of this is that both the implication 'if P then Q,' and its converse 'if Q then P' are true. Hence, to prove a statement of the form 'P if and only if Q,' we are required to prove *both* 'if P then Q' and 'if Q then P.' These two proofs are generally done consecutively and are independent of one another. That is, we write a full proof of the statement 'if P then Q' including whichever assumptions and conclusions need to be made, and when this is finished we proceed to write a full proof of 'if Q then P.' When both proofs are completed, we may conclude 'P if and only if Q.' The two proofs need not be done using the same technique. That is, we could prove 'if P then Q' using a direct proof and 'if Q then P' using a proof by contraposition or any other combination of proof techniques.

Proposition 1.1.23.

$\forall x, y \in \mathbb{R}$, $\max(x, y) = \min(x, y)$ if and only if $x = y$.

Proof.
Let $x, y \in \mathbb{R}$.
Assume $x = y$.
Then $x \geq y$; hence $\max(x, y) = x$.
Also, $x \leq y$; hence $\min(x, y) = x$.
Therefore, $\max(x, y) = \min(x, y)$.
Therefore, if $x = y$ then $\max(x, y) = \min(x, y)$.
Conversely, assume $x \neq y$.
Then by trichotomy we have either $x < y$ or $y < x$.
Case 1: $x < y$.
In this case, we have $\max(x, y) = y$.
Also, since $x < y$, we have $x \leq y$; hence $\min(x, y) = x$.
Since $\min(x, y) = x$, $\max(x, y) = y$, and $x < y$,
we have $\min(x, y) < \max(x, y)$.
Therefore, $\min(x, y) \neq \max(x, y)$.
Case 2: $y < x$.
In this case, we have $\min(x, y) = y$.
Also, since $y < x$, we have $x \geq y$; hence $\max(x, y) = x$.
Since $\max(x, y) = x$, $\min(x, y) = y$, and $y < x$,
we have $\min(x, y) < \max(x, y)$.
Therefore, $\min(x, y) \neq \max(x, y)$.
In both cases, we have $\min(x, y) \neq \max(x, y)$.
Therefore, if $x \neq y$ then $\min(x, y) \neq \max(x, y)$.
Therefore, if $\min(x, y) = \max(x, y)$ then $x = y$.
We have now shown if $x = y$ then $\max(x, y) = \min(x, y)$,
and if $\min(x, y) = \max(x, y)$ then $x = y$.
Therefore, $\max(x, y) = \min(x, y)$ if and only if $x = y$.
Therefore, $\forall x, y \in \mathbb{R}$, $\max(x, y) = \min(x, y)$ if and only if $x = y$.

□

Definition 1.1.3. For $x, \in \mathbb{R}$, we define the **absolute** value of x to be

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

Proposition 1.1.24.

$\forall x \in \mathbb{R}, |x| \geq 0.$

Proof.
Let $x \in \mathbb{R}$.
By trichotomy we have $0 < x$, $x < 0$ or $x = 0$, which we consider in cases.
Case 1: $0 < x$.
In this case, we have $x \geq 0$; hence $|x| = x$.
Since $x \geq 0$ and $|x| = x$, we have $|x| \geq 0$.
Case 2: $x < 0$.
In this case, we have $|x| = -x$.
Since $x < 0$, we have $-x + x < -x + 0$; hence $0 < -x$.
Therefore, $-x \geq 0$; hence $|x| \geq 0$.
Case 3: $x = 0$.
In this case, we have $x \geq 0$; hence $|x| = x = 0$.
Therefore, $|x| \geq 0$.
In all cases we have $|x| \geq 0$.
Therefore, $\forall x \in \mathbb{R}, |x| \geq 0$. □

Proposition 1.1.25.

$\forall x \in \mathbb{R}, |x| = |-x|.$

Proof.
Let $x \in \mathbb{R}$.
By trichotomy we have $0 < x$, $x < 0$ or $x = 0$, which we consider in cases.
Case 1: $0 < x$.
In this case, we have $x \geq 0$; hence $|x| = x$.
Since $0 < x$, we have $-x + 0 < -x + x$; hence $-x < 0$.
Therefore, $|-x| = -(-x) = x$.
Therefore, $|x| = |-x|$.
Case 2: $x < 0$.
In this case, we have $|x| = -x$.
Since $x < 0$, we have $-x + x < -x + 0$; hence $0 < -x$.
Therefore, $-x \geq 0$; hence $|-x| = -x$.
Therefore, $|x| = |-x|$.
Case 3: $x = 0$.
In this case, we have $x \geq 0$; hence $|x| = x = 0$.
Further, since $-x = 0$, we have $-x \geq 0$; hence $|-x| = -x = 0$.
Therefore, $|x| = |-x|$.
In all cases we have $|x| = |-x|$.
Therefore, $\forall x \in \mathbb{R}, |x| = |-x|$. □

Proposition 1.1.26.

$\forall x \in \mathbb{R}$, $x \leq |x|$.

Proof.
Let $x \in \mathbb{R}$.
We consider the two cases $x \geq 0$ and $x < 0$.
Case 1: $x \geq 0$.
In this case, we have $|x| = x$; hence $x \leq |x|$.
Case 2: $x < 0$.
In this case, we have $|x| = -x$.
Since $x < 0$, we have $0 < -x$ by proposition 1.1.7.
Now, since $x < 0$ and $0 < -x$, we have $x < -x$ by transitivity.
Therefore, $x < |x|$; hence $x \leq |x|$.
In both cases we have $x \leq |x|$.
Therefore, $\forall x \in \mathbb{R}$, $x \leq |x|$. □

Proposition 1.1.27.

$\forall x, a \in \mathbb{R}$, $|x| < a$ if and only if $-a < x < a$.

Proof.
Let $x, a \in \mathbb{R}$.
Assume $|x| < a$.
Then $x \leq |x|$ and $|x| < a$, hence $x < a$.
Further, since $-x \leq |-x|$ and $|-x| = |x|$, we have $-x \leq |x|$.
We now have $-x \leq |x|$ and $|x| < a$, hence $-x < a$.
Adding $(x - a)$ to both sides gives us $-x + (x - a) < (x - a) + a$.
Hence $-a < x$.
Therefore, $-a < x$ and $x < a$, which means $-a < x < a$.
Therefore, if $|x| < a$ then $-a < x < a$.
Conversely, assume $-a < x < a$.
Since either $x \geq 0$ or $x < 0$, we consider two cases:
Case 1: $x \geq 0$.
In this case, $|x| = x$ and $x < a$, hence $|x| < a$.
Case 2: $x < 0$.
In this case, $|x| = -x$.
Adding $a - x$ to both sides of $-a < x$ gives us $-a + (a - x) < (a - x) + x$.
Therefore, $-x < a$; hence $|x| < a$.
In both cases we have $|x| < a$.
Therefore, if $-a < x < a$ then $|x| < a$.
We have now shown if $|x| < a$ then $-a < x < a$, and if $-a < x < a$ then $|x| < a$.
Therefore, $|x| < a$ if and only if $-a < x < a$.
Therefore, $\forall x, a \in \mathbb{R}$, $|x| < a$ if and only if $-a < x < a$. □

Theorem 1.1.28 (The Triangle Inequality)**.**

$\forall x, y \in \mathbb{R}, |x + y| \leq |x| + |y|$.

Proof.
Let $x, y \in \mathbb{R}$.
Since $|x| \leq |x|$, we have $-|x| \leq x \leq |x|$.
Similarly, since $|y| \leq |y|$, we have $-|y| \leq y \leq |y|$.
In particular, since $-|x| \leq x$ and $-|y| \leq y$, we have $-|x| - |y| \leq x + y$.
Similarly, since $x \leq |x|$, and $y \leq |y|$, we have $x + y \leq |x| + |y|$.
We now have $-|x| - |y| \leq x + y \leq |x| + |y|$.
By proposition 1.1.27, we then have $|x + y| \leq |x| + |y|$.
Therefore, $\forall x, y \in \mathbb{R}, |x + y| \leq |x| + |y|$. □

Proposition 1.1.29.

$\forall x, y \in \mathbb{R}, ||x| - |y|| \leq |x - y|$.

Proof.
Let $x, y \in \mathbb{R}$.
By the triangle inequality, we have $|(x - y) + y| \leq |x - y| + |y|$.
Therefore, $|x| \leq |x - y| + |y|$; hence $|x| - |y| \leq |x - y|$.
Similarly, $|(x - y) + (-x)| \leq |x - y| + |-x|$.
Therefore, $|-y| \leq |x - y| + |-x|$; hence $|y| \leq |x - y| + |x|$.
This gives us $-|x - y| \leq |x| - |y|$.
We now have $-|x - y| \leq |x| - |y| \leq |x - y|$.
By proposition 1.1.27, this gives us $||x| - |y|| \leq |x - y|$.
Therefore, $\forall x, y \in \mathbb{R}, ||x| - |y|| \leq |x - y|$. □

Proposition 1.1.30.

$\forall x, y \in \mathbb{R}$, if $0 \leq x$ and $0 \leq y$, then $|x - y| \leq \max(x, y)$.

Proof.
Let $x, y \in \mathbb{R}$.
Assume $0 \leq x$ and $0 \leq y$.
We consider two cases: $x \geq y$ and $x < y$.
Case 1: $x \geq y$.
In this case, we have $\max(x, y) = x$.
Further, adding $-y$ to both sides of $x \geq y$ gives us $x - y \geq 0$.
We then have $|x - y| = x - y$.
Now, since $0 \leq y$, we have $-y \leq 0$; hence $x - y \leq x$. Therefore, $|x - y| \leq \max(x, y)$.
Case 2: $x < y$.
In this case, $\max(x, y) = y$.
Further, adding $-y$ to both sides of $x < y$ gives $x - y < 0$.
Therefore, $|x - y| = -(x - y) = y - x$.
Now, since $0 \leq x$, we have $-x \leq 0$; hence $y - x \leq y$. Therefore again, $|x - y| \leq \max(x, y)$.
In both cases we have $|x - y| \leq \max(x, y)$.
Therefore, $\forall x, y \in \mathbb{R}$, if $0 \leq x$ and $0 \leq y$, then $|x - y| \leq \max(x, y)$. □

The techniques discussed above will often be used in combination with one another. Noting that some of the techniques allow us to make assumptions, we should take a moment to discuss the nature and limits of these assumptions. The first aspect of making assumptions that must be emphasized is that one cannot make any extra assumptions in addition to those determined by the structure of the sentence being proven. If an additional assumption is made, then it will change the conclusion that can be drawn from it accordingly; it will thus alter the proposition that has been proven. For example, if one is to prove the statement 'if $x \in \mathbb{Z}$, then $x^2 + 3x + 1$ is odd,' he or she is able to assume that $x \in \mathbb{Z}$. If the additional assumption that 'x is odd' is added into the proof, then even though the conclusion '$x^2 + 3x + 1$' may be reached, the statement 'if $x \in \mathbb{Z}$, then $x^2 + 3x + 1$ is odd' will not have been proven. Rather, the statement 'if $x \in \mathbb{Z}$ and x is odd, then $x^2 + 3x + 1$ is odd' will have been proven. Although this point may seem obvious, it suggests a general rule that must be followed strictly: The only assumptions that can be made are those determined by the structure of the sentence and the structure of the proof.

Assumptions Containing Quantifiers

Another consideration about assumptions is that the assumption itself may have a complex sentence structure involving quantifiers, connectives, or implications. We will examine some examples of these. The first situation to consider is when our assumption contains an *existential quantifier*. That is, we assume $\exists x \in U$, $P(x)$ for some predicate $P(x)$ and universe of discourse U. In this case, the assumption is that there is at least one value of x for which the statement $P(x)$ is true. This assumption tells us nothing of the *identity* of this value of x; it only tells us that such a value of x *exists*. For example, suppose a biologist were to inform us that there is at least one fish in the world that is able to breathe outside of the water. In saying this, the biologist does not provide us with the identity of such a fish; we only have knowledge of its existence. It is easy, in this context, to see that it would be a mistake to identify a fish of our choosing with the one that we are told exists. Indeed, if I confused my own goldfish with the unknown fish whose existence has been assured, then the consequences could be fatal for my goldfish. Thus, if a statement of the form $\exists x \in U$, $P(x)$ has been assumed, it is a mistake to assign a specific value of our choosing to x. Under such an assumption, we know only that there is at least one value in U that satisfies the predicate $P(x)$, but we do not know what that value is or anything about it except that $P(x)$ is true. However, since we know one exists, we may *choose a constant* to represent such a value in our proof. That is, we may assign a constant to denote the thing that is known to exist. For example, if in a proof we are able to assume $\exists x \in \mathbb{R}$, $x^2 < x$, we may choose $a \in \mathbb{R}$ with $a^2 < a$ and use this nonspecific constant a in our proof. By 'nonspecific', we mean that we do not know the value of a; in fact, we know nothing about the constant a except that it is a real number for which $a^2 < a$. The following proposition provides an example:

Proposition 1.1.31.

$\forall x, y \in \mathbb{R}$, if $\exists a \in \mathbb{R}$, $x < a$ and $a < y$, then $x < y$.

Proof.
Arbitrary elements ▶ Let $x, y \in \mathbb{R}$.
Assumption ▶ Assume $\exists a \in \mathbb{R}$, $x < a$ and $a < y$.
Demonstration
Choose $t \in \mathbb{R}$ with $x < t$ and $t < y$.
We then have $x < t$ and $t < y$.
Therefore, $x < y$ by transitivity.
Conclusion ▶ Therefore, if $\exists a \in \mathbb{R}$, $x < a$ and $a < y$, then $x < y$.
Conclusion ▶ Therefore, $\forall x, y \in \mathbb{R}$, if $\exists a \in \mathbb{R}$, $x < a$ and $a < y$, then $x < y$. □

The next situation to consider is when our assumption contains a *universal quantifier*. That is, we assume $\forall x \in U$, $P(x)$, for some predicate $P(x)$ and universe of discourse U. In this case, our assumption tells us that $P(x)$ is true for every value of x in the universe of discourse U. It does not, however, tell us that such an x exists. After all, the universe of discourse could be empty. For example, the assumption that every perfect leader must be benevolent does not in itself make the claim that there is such a thing as a perfect leader. The assumption would be true even if there were no perfect leaders, but in this case it would not be very informative. In fact, the assumption $\forall x \in U$, $P(x)$ is only useful to us if we independently know of some element or elements of the set U. That is, if, independent of this assumption, we establish that some value a is an element of U, then the assumption $\forall x \in U$, $P(x)$ informs us that $P(a)$ is true. For example, suppose that at some point in a proof we assume $\forall x \in \mathbb{R}$, $x^2 < x$. This assumption alone does not inform us of the existence of any real numbers for which $x^2 < x$. However, since we know, independent of this assumption, that $1 \in \mathbb{R}$, the assumption $\forall x \in \mathbb{R}$, $x^2 < x$ tells us that $1^2 < 1$ (If this particular example were part of a proof by contradiction, we would then have our contradiction). We give an example of the application of this principle:

Proposition 1.1.32.

$\forall x, y \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, if $x \leq a$ then $y \leq a$, then $y \leq x$.

Proof.
Arbitrary elements ▶ Let $x, y \in \mathbb{R}$.
Assumption ▶ Assume $\forall a \in \mathbb{R}$, if $x \leq a$ then $y \leq a$.
Demonstration [Since $x \in \mathbb{R}$ and $x \leq x$, we then have $y \leq x$.
Conclusion ▶ Therefore, $y \leq x$.
Conclusion ▶ Therefore, if $\forall a \in \mathbb{R}$, if $x \leq a$ then $y \leq a$, then $y \leq x$.
Therefore, $\forall x, y \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, if $x \leq a$ then $y \leq a$, then $y \leq x$. □

Notice also that in the above proof, the assumption contains an implication. It is important to note that when we assume a statement of the form 'if P then Q,' this does not make claims about the truth or falsity of the propositions P and Q. In particular, it does *not* tell us that P and Q are true. It only tells us that *if* P were true, *then* we would be able to conclude that Q would also be true. Such an assumption only becomes usable if we can establish, independently, that P is true. That is, having assumed 'if P then Q,' if we are able at any point in our proof to demonstrate that P is true, then our assumption will inform us that Q is also true. If we are not able to establish the truth of P independently, then our assumption tells us nothing of the truth of Q.

Examining the above example in more detail, we see that our assumption is '$\forall a \in \mathbb{R}$, if $x \leq a$ then $y \leq a$.' As mentioned earlier, this does *not* inform us of the *existence* of an $a \in \mathbb{R}$ satisfying the predicate 'if $x \leq a$ then $y \leq a$.' However, since x is a known element of $\mathbb{R}$, the assumption informs us that the statement 'if $x \leq x$ then $y \leq x$' is true. Since this is an implication, it tells us nothing unless we can establish the truth of the statement $x \leq x$ independently. Since $x \leq x$ is indeed true regardless of our assumption, the assumed fact that 'if $x \leq x$ then $y \leq x$' is true then informs us that $y \leq x$ is true. This completes the proof. For another example of these same principles at work, consider the following:

Proposition 1.1.33.

$\forall x, y \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $a < x$ if and only if $a < y$, then $x = y$.

Proof.
Let $x, y \in \mathbb{R}$.
Arbitrary elements ▶
Assumption ▶
Suppose $\forall a \in \mathbb{R}$, $a < x$ if and only if $a < y$, and $x \neq y$.
Since $x \neq y$, by trichotomy, we have either $x < y$ or $y < x$.
We consider these as cases.
Case 1: $x < y$.
Demonstration [
Contradiction ▶
Since $x \in \mathbb{R}$ and $x < y$, by our assumption we must have $x < x$.
We then have $x = x$ and $x < x$, which contradicts trichotomy.
Case 2: $y < x$.
Demonstration [
Contradiction ▶
Since $y \in \mathbb{R}$ and $y < x$, by our assumption we must have $y < y$.
We then have $y = y$ and $y < y$, which contradicts trichotomy.
Both cases lead to a contradiction.
Conclusion ▶
Therefore, if $\forall a \in \mathbb{R}$, $a < x$ if and only if $a < y$, then $x = y$.
Conclusion ▶
Therefore, $\forall x, y \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $a < x$ if and only if $a < y$, then $x = y$. □

A remark about 'if and only if'

For propositions P and Q, to say 'P if and only if Q' means 'if P, then Q, and if Q, then P'. That is, it makes the statement that *both* the implication 'if P, then Q' and its *converse* 'if Q, then P' are true. 'P if and only if Q' is sometimes denoted by '$P \Leftrightarrow Q$', which recalls the similar notation $P \Rightarrow Q$ which stands for 'if P, then Q'. On occasion, one also sees 'P if and only if Q' abbreviated as 'P iff Q'.

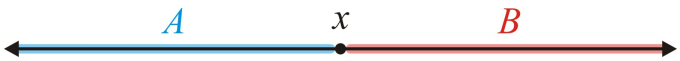
The Archimedean Property

The Archimedean property gives us an important connection between the real numbers and the natural numbers (the positive whole numbers). To understand what the Archimedean property says, consider the length of a single step to be a real number a, with $a > 0$. Next, consider another real number b that represents a great distance that we must travel. The Archimedean property optimistically guarantees us that it is possible to complete our journey. That is, there is a number of steps n for which $na > b$. Although this may seem intuitively obvious, the proof requires an axiom that we have not yet used in a proof: the completeness axiom.

The completeness axiom

If A and B are non-empty subsets of $\mathbb{R}$ such that for all $a \in A$ and all $b \in B$, $a < b$, then there is an element $x \in \mathbb{R}$ such that for all $a \in A$, $a \leq x$, and for all $b \in B$, $x \leq b$.

Recall the remark earlier, that if we imagine the real numbers as a line and we cut the line into two pieces A and B, then the cut must fall on a real number. That is, there is a real number x lying between all the points in piece A and the points in piece B.



To prove the Archimedean property, we use the proof by contradiction technique. Hence, we are able to assume that there is a distance b that cannot be traveled in any number of steps of length a. That is, $b > na$ for all $n \in \mathbb{N}$. With a view to using the completeness axiom, we introduce a set A consisting of all possible distances travelable by taking steps of size n. That is,

$$A = \{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = an\}.$$

Since under our assumption, the distance b is larger than every element of A, we define the set B to be all such distances that are too long to be reached by steps of size a. That is,

$$B = \{y \in \mathbb{R} \mid \forall n \in \mathbb{N},\ na \leq y\}.$$

We then have all of the travelable distances in A and the distances that are too large to be traversed in B. Hence, we can show that the elements of A are all smaller than the elements of B.

With this setup, the completeness axiom gives us the existence of a $c \in \mathbb{R}$, larger than all the elements of A and smaller that all of the elements of B. A contradiction arises when we take one step back from c and consider the length $c - a$. This length is too small to be in B, yet if it is reachable by n steps of size a, that is if $na \geq c - a$, then one more step to $(n + 1)a$ will take us beyond c, which is likewise not allowable under the given circumstances. Thus we can reach a contradiction. The details of this argument are worked out as follows:

Theorem 1.1.34 (The Archimedean Property)**.**

$\forall a, b \in \mathbb{R}$, if $a > 0$ then $\exists n \in \mathbb{N}$, $na > b$.

Proof.
Let $a, b \in \mathbb{R}$.
Assume $a > 0$.
Suppose there does not exist $n \in \mathbb{N}$, such that $na > b$.
Then for all $n \in \mathbb{N}$, $na \leq b$.
Let $A = \{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = na\}$ and let $B = \{y \in \mathbb{R} \mid \forall n \in \mathbb{N},\ na \leq y\}$.
Then, $a = 1a \in A$ and $b \in B$, so A and B are non-empty sets.
Let $x \in A$ and $y \in B$.
Then, we can choose $m \in \mathbb{N}$ such that $x = ma$.
and, by definition of B, $x = ma \leq y$.
Thus, $x \leq y$.
Hence, $\forall x \in A$, $\forall y \in B$, $x \leq y$.
Thus, by the completeness axiom of $\mathbb{R}$, we can choose $c \in \mathbb{R}$, such that for all $x \in A$ and $y \in B$, $x \leq c$ and $c \leq y$.
Now, let $n \in \mathbb{N}$.
Then, $n + 1 \in \mathbb{N}$, so $(n + 1)a \in A$.
Therefore, $(n + 1)a \leq c$.
But then, $na \leq c - a$.
Therefore, $\forall n \in \mathbb{N}$, $na \leq c - a$.
Hence, $c - a \in B$, so $c \leq c - a$.
This is a contradiction, since $a > 0$.
Thus, there exists $n \in \mathbb{N}$, such that $na > b$.
Therefore, if $a > 0$ then $\exists n \in \mathbb{N}$, $na > b$.
Therefore, $\forall a, b \in \mathbb{R}$, if $a > 0$ then $\exists n \in \mathbb{N}$, $na > b$. □

The following two corollaries associated with the Archimedean property are also very useful:

Corollary 1.1.35.

$\forall b \in \mathbb{R}$, $\exists n \in \mathbb{N}$, $n > b$.

Proof.
Let $b \in \mathbb{R}$.
Since $1 > 0$, we have by the Archimedean property, $\exists n \in \mathbb{N}$, $n(1) > b$.
Therefore, $\forall b \in \mathbb{R}$, $\exists n \in \mathbb{N}$, $n > b$. □

Corollary 1.1.36.

$\forall a \in \mathbb{R}$, if $a > 0$ then $\exists n \in \mathbb{N}$, $\frac{1}{n} < a$.

Proof.
Let $a \in \mathbb{R}$.
Assume $a > 0$.
By the Archimedean property, since $1 \in \mathbb{R}$, we have $\exists n \in \mathbb{N}$, $na > 1$.
For such an n, we have $a > \frac{1}{n}$.
Therefore, $\exists n \in \mathbb{N}$, $\frac{1}{n} < a$.
Therefore, if $a > 0$ then $\exists n \in \mathbb{N}$, $\frac{1}{n} < a$.
Therefore, $\forall a \in \mathbb{R}$, if $a > 0$ then $\exists n \in \mathbb{N}$, $\frac{1}{n} < a$. □

Exercises 1.1.

Notation:
For all $x, y \in \mathbb{R}$, $x - y$ means $x + (-y)$.
For all $x, y \in \mathbb{R}$ with $y \neq 0$, $\frac{x}{y}$ means $x(y^{-1})$.
For all $x, y \in \mathbb{R}$, $x \leq y$ means $x < y$ or $x = y$.
For all $x, y, z \in \mathbb{R}$, $x < y < z$ means $x < y$ and $y < z$.
2 is defined by $2 = 1 + 1$; 3 is defined by $3 = 2 + 1$; 4 is defined by $4 = 3 + 1$; and so on.

Prove the following propositions. At each step indicate the axiom or proposition you have used.

1. $\forall x, y \in \mathbb{R}$, $-(x + y) = -x - y$.
2. $\forall x, y \in \mathbb{R}$, $-(x - y) = y - x$.
3. $\forall x \in \mathbb{R} \setminus \{0\}$, $(x^{-1})^{-1} = x$.
4. $\forall x \in \mathbb{R}$, $\forall y \in \mathbb{R} \setminus \{0\}$, $yx(y^{-1}) = x$.
5. $\forall x, y \in \mathbb{R} \setminus \{0\}$, $(xy)^{-1} = y^{-1}x^{-1}$.
6. $\forall x, y \in \mathbb{R} \setminus \{0\}$, $(x^{-1}y)^{-1} = y^{-1}x$.
7. $\forall a, b \in \mathbb{R}$, $\forall x \in \mathbb{R} \setminus \{0\}$, $\frac{xa+xb}{x} = a + b$.
8. $\forall a \in \mathbb{R}$, $\forall b, x \in \mathbb{R} \setminus \{0\}$, $\frac{xa}{xb} = \frac{a}{b}$.
9. $\forall a, b \in \mathbb{R}$, $\forall x \in \mathbb{R} \setminus \{0\}$, $\frac{a}{x} + \frac{b}{x} = \frac{a+b}{x}$.
10. $\forall a, x \in \mathbb{R}$, $\forall b, y \in \mathbb{R} \setminus \{0\}$, $\frac{a}{b} + \frac{x}{y} = \frac{ay+bx}{by}$.
11. $\forall a, x \in \mathbb{R}$, $\forall b, y \in \mathbb{R} \setminus \{0\}$, $\left(\frac{a}{b}\right)\left(\frac{x}{y}\right) = \frac{ax}{by}$.
12. $\forall a \in \mathbb{R}$, $\forall b, x, y \in \mathbb{R} \setminus \{0\}$, $\left(\frac{a}{b}\right)\left(\frac{x}{y}\right)^{-1} = \frac{ay}{bx}$.
13. $1 < 3$.
14. $1 < 4$.
15. $\forall x \in \mathbb{R}$, $x < x + 1$.
16. $\forall x \in \mathbb{R}$, $x < x + 2$.

Prove the following propositions using a direct proof.

17. $\forall x, y, a \in \mathbb{R}$, if $ax = ay$ and $a \neq 0$, then $x = y$.
18. $\forall x \in \mathbb{R}$, if $0 < x$, then $-x < 0$.
19. $\forall a, x \in \mathbb{R}$, if $a + x = 0$, then $a = -x$. (That is, $-x$ is the only additive inverse of x).
20. $\forall a, x \in \mathbb{R}$, if $ax = 1$, then $a = x^{-1}$. (That is, x^{-1} is the only multiplicative inverse of x).
21. $\forall x \in \mathbb{R}$, if $0 < x$, then $0 < x + 1$.
22. $\forall x \in \mathbb{R}$, if $0 < x - 2$, then $3 < 2x$.
23. $\forall x, y \in \mathbb{R}$, $x < y$ if and only if $-y < -x$.
24. $\forall x, y \in \mathbb{R}$, if $0 < x < y$, then $y^{-1} < x^{-1}$.
25. $\forall x, y \in \mathbb{R}$, if $x < 0$ and $y < 0$, then $0 < xy$.
26. $\forall x, y \in \mathbb{R}$, if $x < 0$ and $0 < y$, then $xy < 0$.
27. $\forall x, y \in \mathbb{R}$, if $x < y$ and $0 < y$, then $2x < 4y$.
28. $\forall x, y \in \mathbb{R}$, if $x < y$, then $2 + x < 4 + y$.
29. $\forall a, b, x, y \in \mathbb{R}$, if $a < b$ and $x < y$, then $a + x < b + y$.
30. $\forall a, b, x, y \in \mathbb{R}$, if $0 < a < x$ and $0 < b < y$, then $ab < xy$.

Prove the following propositions using a proof by contraposition.

31. $\forall x, y \in \mathbb{R}$, if $x \leq y$ and $y \leq x$, then $x = y$.
32. $\forall x \in \mathbb{R}$, if $2x \leq 0$, then $x - 1 \leq 0$.
33. $\forall x \in \mathbb{R}$, if $x^2 \leq x$, then $x \leq 1$.
34. $\forall x, y \in \mathbb{R}$, if $3 + x \leq 1 + y$, then $x \leq y$.
35. $\forall x, y \in \mathbb{R}$, if $x^2 \leq y^2$, then $y \leq 0$ or $x \leq y$.
36. $\forall x, y \in \mathbb{R}$, if $2x \leq y$, then $x \leq y$ or $x \leq 0$.
37. $\forall x, y \in \mathbb{R}$, if $x^2 - xy \leq xy - y^2$, then $x \leq y$.
38. $\forall x, y \in \mathbb{R}$, if $x^2 - xy \leq xy - y^2$, then $y \leq x$.

Prove the following propositions using a proof by contradiction.

39. $\forall x, y \in \mathbb{R}$, if $x < 0$ and $0 < xy$, then $y < 0$.
40. $\forall x, y \in \mathbb{R}$, if $0 < x$ and $0 < xy$, then $0 < y$.
41. $\forall x \in \mathbb{R}$, if $x \neq 0$, then $x^{-1} \neq 0$.
42. $\forall x \in \mathbb{R}$, if $x < 0$, then $x^{-1} < 0$.
43. $\forall x, y \in \mathbb{R}$, if $x < y < 0$, then $y^{-1} < x^{-1}$.

44. $\forall x, y \in \mathbb{R}$, if $xy < 0$ and $x \leq 0$, then $0 \leq y^{-1}$.

45. $\forall a, x, y \in \mathbb{R}$, if $ax < ay$ and $y \leq x$, then $a \leq 0$.

46. $\forall a, x, y \in \mathbb{R}$, if $0 < a$ and $xy < a^2$, then $x < a$ or $y < a$.

Prove the following propositions.

47. $\exists x \in \mathbb{R}$, $x < x^2$.

48. $\exists x \in \mathbb{R}$, $x^2 < x$.

49. $\exists x \in \mathbb{R}$, $x = x^2$.

50. $\exists x \in \mathbb{R}$, $x^2 - 3x = 4$.

51. $\forall y \in \mathbb{R}$, $\exists x \in \mathbb{R}$, $y = x + 1$.

52. $\forall y \in \mathbb{R}$, $\exists x \in \mathbb{R}$, $y = 3x$.

53. $\forall y \in \mathbb{R}$, $\exists x \in \mathbb{R}$, $y = 5x - 2$.

54. $\forall y \in \mathbb{R}$, $\exists x \in \mathbb{R}$, $2y = 3x + 5$.

55. $\forall a, b \in \mathbb{R}$, if $a < b$, then $\exists x \in (0, \infty)$, $a + x = b$.

56. $\forall a, b \in \mathbb{R}$, if $a \neq 0$, then $\exists x \in \mathbb{R}$, $ax = b$.

57. $\forall x \in (0, 1)$, $\exists y \in (0, 1)$, $y < x$.

58. $\forall x \in (0, 1)$, $\exists y \in (0, 1)$, $x < y$.

59. $\forall x, y \in \mathbb{R}$, if $x < y$, then $\exists a \in (0, \infty)$, $x + a < y$.

60. $\forall x, y \in \mathbb{R}$, if $x < y$, then $\forall b \in (0, \infty)$, $\exists a \in (0, \infty)$, $x + ab < y$.

61. $\forall a, b, x \in \mathbb{R}$, if $a < x < b$, then $\exists t \in (0, 1)$, $x = (1 - t)a + tb$.

62. $\forall a, b, x \in \mathbb{R}$, if $a < b$ and $\exists t \in (0, 1)$, $x = (1-t)a+tb$, then $a < x < b$.

63. $\forall x, y \in \mathbb{R}$, $\exists z \in \mathbb{R}$, $x < z$ and $y < z$.

64. $\forall x, y \in (0, 1)$, $\exists z \in (0, 1)$, $z < x$ and $z < y$.

Prove the following propositions.

65. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $a + x = x$, then $a = 0$. (That is, 0 is the only additive identity).

66. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax = x$, then $a = 1$. (That is, 1 is the only multiplicative identity).

67. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax = a$, then $a = 0$.

68. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax = 0$, then $a = 0$.

69. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax \leq x$, then $a = 1$.

70. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax \leq a$, then $a = 0$.

71. $\forall a \in \mathbb{R}$, if $\forall x \in \mathbb{R}$, $ax \leq 0$, then $a = 0$.

72. $\forall x \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $ax \leq 0$, then $\forall b \in \mathbb{R}$, $0 \leq bx$.

73. $\forall x \in \mathbb{R}$, if $\forall a \in (0, \infty)$, $x \leq a$, then $x \leq 0$.

74. $\forall x, y \in \mathbb{R}$, if $\forall a \in (0, \infty)$, $x \leq a + y$, then $x \leq y$.

75. $\forall x \in \mathbb{R}$, if $\forall a \in (0, \infty)$, $x \leq a$, then $\forall b \in (0, \infty)$, $x < b$.

76. $\forall x \in \mathbb{R}$, if $\forall a \in (0, \infty)$, $x < a$, then $\forall b, c \in (0, \infty)$, $cx < b$.

77. $\forall x \in \mathbb{R}$, if $\forall a \in (0, \infty)$, $x < 100a$, then $\forall b \in (0, \infty)$, $x < b$.

78. $\forall x \in \mathbb{R}$, if $\exists m \in (0, \infty)$, $\forall a \in (0, \infty)$, $x < ma$, then $\forall b \in (0, \infty)$, $x < b$.

79. $\forall x, y \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $x \leq a$ if and only if $y \leq a$, then $x = y$.

80. $\forall x, y \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $x < a$ if and only if $y < a$, then $x = y$.

81. $\forall x, y \in \mathbb{R}$, if $\forall a \in (-\infty, x]$, $a < y$, then $\exists b \in (-\infty, y]$, $x < b$.

82. For a subset $S \subseteq \mathbb{R}$, $\forall a, b \in S$, if $\forall x \in S$, $a \leq x$ and $\forall x \in S$, $b \leq x$, then $a = b$.
(That is, the smallest element of a set is unique.)

Prove the following propositions.

83. $\forall a \in \mathbb{R}$, if $\exists x \in (0, \infty)$, $x < a$, then $0 < a$.

84. $\forall x, y \in \mathbb{R}$, if $\exists a \in \mathbb{R}$, $x < a$ and $a \leq z$, then $x < z$.

85. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $a + x = x$, then $a = 0$.

86. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $x \neq 0$ and $ax = x$, then $a = 1$.

87. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $x \neq 1$ and $ax = a$, then $a = 0$.

88. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $x \neq 0$ and $ax = 0$, then $a = 0$.

89. $\forall a \in \mathbb{R}$, if $\exists x \in \mathbb{R}$, $ax > 1$, then $\exists y \in \mathbb{R}$, $ay < -1$.

90. $\forall a, b \in \mathbb{R}$, if $\exists x \in (0, \infty)$, $a + x = b$, then $a < b$.

91. $\forall x \in \mathbb{R}$, if $\exists a \in (0, \infty)$, $a \leq x$, then $\exists b \in (0, \infty)$, $b < x$.

92. $\forall x \in \mathbb{R}$, if $\exists a, b \in (0, \infty)$, $a < bx$, then $\exists c \in (0, \infty)$, $c < x$.

93. $\forall x \in \mathbb{R}$, if $\exists a \in (0, \infty)$, $a < x$, then $\forall b \in (0, \infty)$, $0 < bx$.

94. $\forall x \in \mathbb{R}$, if $\exists a \in (0, \infty)$, $x + a < 0$, then $\forall b \in (0, \infty)$, $bx < 0$.

95. $\forall x \in \mathbb{R}$, if $\exists a \in (0, \infty)$, $ax < 0$, then $\forall b \in (0, \infty)$, $bx < 0$.

96. $\forall x \in \mathbb{R}$, if $\exists a \in \mathbb{R}$, $ax < 0$, then $\exists b \in \mathbb{R}$, $0 < bx$.

Prove the following inequalities.

97. $\forall x, y \in \mathbb{R}$, $2xy \leq x^2 + y^2$.

98. $\forall x, y \in \mathbb{R}$, $4xy \leq x^2 + 4y^2$.

99. $\forall x, y \in \mathbb{R}$, $4xy \leq (x + y)^2$.

100. $\forall x, y \in \mathbb{R}$, $8xy \leq (x + 2y)^2$.

101. $\forall x, y \in \mathbb{R}$, $4xy \leq (y + 2x)^2 - y^2$.

102. $\forall x, y \in \mathbb{R}$, $4xy \leq (y + 2x)^2 - x^2$.

Prove the following propositions involving the max **and** min **functions.**

103. $\forall x, y \in \mathbb{R}$, $\min(x, y) \leq x$ and $\min(x, y) \leq y$.

104. $\forall x, y \in \mathbb{R}$, $x + y = \max(x, y) + \min(x, y)$.

105. $\forall a, x, y \in \mathbb{R}$, if $x \leq y$, then $\max(a, x) \leq \max(a, y)$.

106. $\forall a, x, y \in \mathbb{R}$, if $x \leq y$, then $\min(a, x) \leq \min(a, y)$.

107. $\forall a, b, x, y \in \mathbb{R}$, if $x \leq y$ and $a \leq b$, then $\max(a, x) \leq \max(b, y)$.

108. $\forall a, b, x, y \in \mathbb{R}$, if $x \leq y$ and $a \leq b$, then $\min(a, x) \leq \min(b, y)$.

109. $\forall a, x, y \in \mathbb{R}$, if $\max(a, x) = \max(a, y)$ and $\min(a, x) = \min(a, y)$, then $x = y$.

110. $\forall a, x, y \in \mathbb{R}$, if $\max(a, x) = \min(a, y)$, then $x \leq y$.

111. $\forall x, y, z \in \mathbb{R}$, if $x \leq z$, then $\max(x, \min(y, z)) = \min(\max(x, y), z)$.

112. $\forall x, y, z \in \mathbb{R}$, if $x \leq z$, then $\max(x, \max(y, z)) = \max(y, z)$.

113. $\forall a, b, x \in \mathbb{R}$, if $a < x < b$, then $\max(b - x, x - a) < b - a$.

114. $\forall a, b, x \in \mathbb{R}$, if $a < x < b$, then $2\min(b - x, x - a) \leq b - a$.

115. $\forall x, y, a \in \mathbb{R}$, $\max(x, y) > a$ if and only if $x > a$ or $y > a$.

116. $\forall x, y, a \in \mathbb{R}$, $\min(x, y) < a$ if and only if $x < a$ or $y < a$.

117. $\forall x, y, a \in \mathbb{R}$, $\max(x, y) < a$ if and only if $x < a$ and $y < a$.

118. $\forall x, y, a \in \mathbb{R}$, $\min(x, y) > a$ if and only if $x > a$ and $y > a$.

119. $\forall x, y, z \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $z \leq a$ if and only if $x \leq a$ and $y \leq a$, then $z = \max(x, y)$.

120. $\forall x, y, z \in \mathbb{R}$, if $\forall a \in \mathbb{R}$, $a < z$ if and only if $a < x$ and $a < y$, then $z = \min(x, y)$.

Prove the following propositions involving the absolute value function.

121. $\forall x, y \in \mathbb{R}$, $|xy| = |x||y|$.

122. $\forall x \in \mathbb{R}$, $|x|^2 = x^2$.

123. $\forall x, y \in \mathbb{R}$, $||x| - |y|| \leq |x + y|$.

124. $\forall x, y, z \in \mathbb{R}$, $|x - y| \leq |x - z| + |z - y|$.

125. $\forall x, y \in \mathbb{R}$, $y < |x|$ if and only if $x < -y$ or $y < x$.

126. $\forall x, y \in \mathbb{R}$, if $|x| < y$, then $x^2 < y^2$.

127. $\forall x, y \in \mathbb{R}$, if $-y < x < y$, then $x^2 < y^2$.

128. $\forall x, a \in \mathbb{R}$, if $x^2 \leq a^2$, then $|x| \leq |a|$.

129. $\forall x, y \in (0, 1)$, $|x - y| < 1$.

130. $\forall a, b, x, y \in \mathbb{R}$, if $a < x < b$ and $a < y < b$, then $|x - y| < b - a$.

131. $\forall x \in \mathbb{R}$, if $|x - 1| < 1$, then $x^2 + 3x - 4 < 6$.

132. $\forall x \in \mathbb{R}$, if $|x - 2| < 3$, then $|x^2 - 4| < 21$.

133. $\forall x, y \in \mathbb{R}$, if $\forall a \in (0, \infty)$, $|x - y| \leq a$, then $x = y$.

134. $\forall x, y \in \mathbb{R}$, if $\exists b \in (0, \infty)$, $\forall a \in (0, \infty)$, $|x - y| \leq \frac{a}{b}$, then $x = y$.

Prove the following propositions.

135. $\forall x, y \in \mathbb{R}$, $\max(x, y) = \frac{1}{2}(|x - y| + x + y)$.

136. $\forall x, y \in \mathbb{R}$, $\min(x, y) = \frac{1}{2}(x + y - |x - y|)$.

137. $\forall x, y \in \mathbb{R}$, if $\min(x, y) < |x - y|$, then $2\min(x, y) < \max(x, y)$.

138. $\forall x, y \in \mathbb{R}$, if $|x - y| < \min(x, y)$, then $\max(x, y) < 2\min(x, y)$.

139. $\forall x, y \in \mathbb{R}$, if $x > 0$ and $y > 0$, then $|x - y| < \max(x, y)$.

140. $\forall x, y \in \mathbb{R}$, if $|x - y| < \max(x, y)$, then $x > 0$ and $y > 0$.

Prove the following propositions using the Archimdedean property.

141. $\forall x, y \in \mathbb{R}$, if $0 < x$, then $\exists n \in \mathbb{N}$, $y \leq nx$.

142. $\forall x \in \mathbb{R}$, $\exists k \in \mathbb{Z}$, $k < x$.

143. $\forall x, y \in \mathbb{R}$, $\exists n \in \mathbb{N}$, $y \leq x + n$.

144. $\forall x \in \mathbb{R}$, if $0 < x$, then $\exists n \in \mathbb{N}$, $\frac{3}{n} < x$.

145. $\forall x \in \mathbb{R}$, if $\forall n \in \mathbb{N}$, $x \leq 3 + \frac{1}{n}$, then $x \leq 3$.

146. $\forall x \in \mathbb{R}$, if $\forall n \in \mathbb{N}$, $x \leq 3 + \frac{5}{n}$, then $x \leq 3$.

147. $\forall x \in \mathbb{R}$, if $\forall n \in \mathbb{N}$, $3 - \frac{1}{n} \leq x$, then $3 \leq x$.

148. $\forall x \in \mathbb{R}$, if $\forall n \in \mathbb{N}$, $3 - \frac{5}{n} \leq x$, then $3 \leq x$.

149. $\forall a, x, y \in \mathbb{R}$, if $\forall n \in \mathbb{N}$, $x + an \leq y$, then $a \leq 0$.

150. $\forall x, y \in \mathbb{R}$, if $\forall n \in \mathbb{N}$, $|x - y| < \frac{1}{n}$, then $x = y$.

151. $\forall x, y \in \mathbb{R}$, if $\exists b \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $|x-y| < \frac{b}{n}$, then $x = y$.

152. Let $S \subseteq \mathbb{R}$. If $\exists a \in \mathbb{R}$, $\forall x \in S$, $x \leq a$, then $\exists n \in \mathbb{N}$, $\forall x \in S$, $x \leq n$.

153. $\forall x, \varepsilon \in \mathbb{R}$, if $\varepsilon > 0$, then $\exists n \in \mathbb{N}$, $\frac{x}{n} < \varepsilon$.

154. $\forall x, y \in \mathbb{R}$, if $x < y$, then $\exists n \in \mathbb{N}$, $x(n+1) < y(n-1)$.

155. $\forall a, x, y \in \mathbb{R}$, if $x < y$, then $\exists n \in \mathbb{N}$, $x(n + a) < y(n - a)$.

156. $\forall x \in \mathbb{R}$, if $1 < x$, then $\exists n \in \mathbb{N}$, $\frac{n+1}{n} < x$.

157. $\forall x \in \mathbb{R}$, $x < 10$ if and only if $\exists n \in \mathbb{N}$, $x + \frac{1}{n} \leq 10$.

158. $\forall x \in \mathbb{R}$, $x \leq 10$ if and only if $\forall n \in \mathbb{N}$, $x < 10 + \frac{1}{n}$.

Let $x, y, z \in [0, 1]$. Compare the following properties of the max and min functions to the *Boolean algebraic* properties given in section 0.3.

$1 - 0 = 1$ $\qquad$ $1 - 1 = 0$

Idempotence

$\max(x, x) = x$ $\qquad$ $\min(x, x) = x$

Commutativity

$\max(x, y) = \max(y, x)$ $\qquad$ $\min(x, y) = \min(y, x)$

Associativity

$\max(x, \max(y, z)) = \max(\max(x, y), z)$

$\min(x, \min(y, z)) = \min(\min(x, y), z)$

Absorption

$\max(x, \min(x, y)) = x$ $\qquad$ $\min(x, \max(x, y)) = x$

Distributivity

$\max(x, \min(y, z)) = \min(\max(x, y), \max(x, z))$

$\min(x, \max(y, z)) = \max(\min(x, y), \min(x, z))$

Annihilator

$\max(x, 1) = 1$ $\qquad$ $\min(x, 0) = 0$

Identity

$\max(x, 0) = x$ $\qquad$ $\min(x, 1) = x$

Double Negation

$1 - (1 - x) = x$

De Morgan's Laws

$1 - \min(x, y) = \max(1 - x, 1 - y)$

$1 - \max(x, y) = \min(1 - x, 1 - y)$

1. Prove the Idempotence properties for max and min.

2. Prove the Associativity properties for max and min.

3. Prove the Absorption properties for max and min.

4. Prove the Distributivity properties for max and min.

5. Prove De Morgan's Laws for max and min.

6. Give an example of a value of $x \in [0, 1]$ for which the analogous properties to Complementation: $\min(x, 1 - x) = 0$ and $\max(x, 1 - x) = 1$ do not hold.

1.2 The Integers

Definition 1.2.1. *The system of* **integers**, *denoted* $\mathbb{Z}$ *is defined to be a set, containing constants* 0 *and* 1 *with* $0 \neq 1$, *binary operations given by* $(x, y) \mapsto x + y$ *and* $(x, y) \mapsto xy$, *a unary operation given by* $x \mapsto -x$, *and a relation* $<$, *satisfying the following axioms:*

A1 *For all* $x, y \in \mathbb{Z}$, $x + y = y + x$. *(Addition is commutative)*

A2 *For all* $x, y, z \in \mathbb{Z}$, $(x + y) + z = x + (y + z)$. *(Addition is associative)*

A3 *For every* $x \in \mathbb{Z}$, $x + 0 = x$ *and* $0 + x = x$. *(*0 *an additive identity)*

A4 *For every* $x \in \mathbb{Z}$, $x + (-x) = 0$ *and* $(-x) + x = 0$. *(*$-x$ *is an additive inverse of* x*)*

M1 *For all* $x, y \in \mathbb{Z}$, $xy = yx$. *(Multiplication is commutative)*

M2 *For all* $x, y \in \mathbb{Z}$, $(xy)z = x(yz)$. *(Multiplication is associative)*

M3 *For every* $x \in \mathbb{Z}$, $x1 = x$ *and* $1x = x$. *(*1 *is a multiplicative identity)*

FZ *For all* $x, y \in \mathbb{Z}$, *if* $xy = 0$ *then* $x = 0$ *or* $y = 0$. *(Zero is not a product of non-zero factors)*

DL *For all* $x, y, z \in \mathbb{Z}$, $x(y + z) = (xy) + (xz)$ *and* $(y + z)x = (yx) + (zx)$. *(Multiplication distributes over addition)*

O1 *For all* $x, y \in \mathbb{Z}$, *exactly one of* $x < y$, $x = y$, *or* $y < x$ *holds. (Trichotomy)*

O2 *For all* $x, y, z \in \mathbb{Z}$, *if* $x < y$ *and* $y < z$ *then* $x < z$. *(Transitivity)*

O3 *For all* $x, y, z \in \mathbb{Z}$, *if* $x < y$ *then* $x + z < y + z$. *(Addition preserves order)*

O4 *For all* $x, y, z \in \mathbb{Z}$, *if* $x < y$ *and* $0 < z$, *then* $xz < yz$. *(Multiplication by a positive preserves order)*

WOP *If* $S \subseteq \mathbb{Z}$ *is a non-empty subset with the property that for all* $x \in S$, $0 \leq x$, *then there is an element* $a \in S$ *with the property that for all* $x \in S$, $a \leq x$. *(The Well-Ordering Property)*

Since the integers are defined using many of the same axioms as the real numbers, several properties we proved for the real numbers hold for the integers as well and can be proven using the same arguments. One must be cautious however, that since not all non-zero integers have multiplicative inverses, any results that made use of axiom $M4$ for the real numbers may not hold in the integers. In particular, one result we proved for the real numbers was $\forall x, y \in \mathbb{R}$, if $x < y$ then $\exists z \in \mathbb{R}$, $x < z < y$. The proof of this result used the existence of the multiplicative inverse of 2. This same argument cannot be applied in the integers, and in fact we will see that this result is false for the integers.

Although we give the definition of the integers independently of the real numbers, it is often useful to view the integers as a subset of the real numbers. One can show that $\mathbb{Z}$ can be identified with the smallest subset A of $\mathbb{R}$ such that $0 \in A$, and $\forall x \in A$, $x + 1 \in A$ and $x - 1 \in A$. We will elaborate on this construction of the integers throughout the section. For now, it will suffice to consider the integers as the set defined above and to keep in mind that in some situations we will find it useful to think of the integers as being a subset of the real numbers. For example, the Archimedean property and the notion of a rational number make use of a link between $\mathbb{Z}$ and $\mathbb{R}$.

The Well-Ordering Property

On the other hand, there is one axiom of the integers that is not satisfied by the real numbers. This is axiom *WOP*; the well-ordering property. Using axiom *WOP*, we may prove statements about the integers that are not true in the real numbers. This section is concerned with this axiom and its implications.

The Well-Ordering Property

If $S \subseteq \mathbb{Z}$ is a non-empty subset with the property that for all $x \in S$, $0 \leq x$, then there is an element $m \in S$ with the property that for all $x \in S$, $m \leq x$.

For $a \in S$, the statement 'for all $x \in S$, $a \leq x$' means a is the smallest element in the set S. Hence this property is ensuring that every non-empty set of non-negative integers will have a minimum. That the integers must be non-negative merely ensures that we have a lower bound on the set S. In fact, the lower bound need not be 0; it can be any integer.

Theorem 1.2.1.

Let $A \subseteq \mathbb{Z}$, with $A \neq \emptyset$. If A is bounded below, then A has a smallest element. That is, if $\exists b \in \mathbb{Z}, \forall x \in A, b \leq x$, then $\exists a \in A, \forall x \in A, a \leq x$.

Proof.
Assume $\exists b \in \mathbb{Z}, \forall x \in A, b \leq x$.
    Choose such a b.
    Let $S = \{x \in \mathbb{Z} \mid x + b \in A\}$.
    Since $A \neq \emptyset$, we have that $\exists y \in \mathbb{Z}, y \in A$. Choose such a y.
    Let $z = y - b$.
        Then $z + b = (y - b) + b = y \in A$.
        Therefore, $z \in S$.
    Therefore, $\exists z \in \mathbb{Z}, z \in S$.
    Therefore, $S \neq \emptyset$.
    Let $x \in S$.
        Hence, $x + b \in A$.
        Therefore, $b \leq x + b$.
        We then have $0 \leq x$.
    Therefore, $\forall x \in S, 0 \leq x$.
    We now have $S \neq \emptyset$ and $\forall x \in S, 0 \leq x$.
    By the well-ordering property, we then have $\exists m \in S, \forall x \in S, m \leq x$.
    Choose such an m, and set $a = m + b$.
        Since $m \in S$, we have that $a = m + b \in A$.
        Let $x \in A$.
            Since $(x - b) + b = x \in A$, we have $x - b \in S$.
            Therefore, $m \leq x - b$.
            This gives us $m + b \leq x$; hence $a \leq x$.
        Therefore, $\forall x \in A, a \leq x$.
    Therefore, $\exists a \in A, \forall x \in A, a \leq x$.
Therefore, if $\exists b \in \mathbb{Z}, \forall x \in A, b \leq x$, then $\exists a \in A, \forall x \in A, a \leq x$. □

An exercise in the previous section asks the reader to write a proof of the fact that for a subset $S \subseteq \mathbb{R}$, $\forall a, b \in S$, if $\forall x \in S$, $a \leq x$ and $\forall x \in S$, $b \leq x$, then $a = b$. Since the order axioms of the integers are the same as those of the real numbers, an identical proof will suffice to show that the same is true for subsets of the integers. After a careful reading of this proposition, we can see that the elements a and b are assumed to be *smallest elements* of the set S. The conclusion that follows from this assumption is that $a = b$. This gives us the rather intuitive result that there can only be *one* smallest element of a set. Applied to the topic at hand, this means that the smallest element of a set, whose existence is given by the well-ordering property, is *unique*.

In general, given any non-empty set $S \subseteq \mathbb{Z}$, by virtue of the set being non-empty, we know $\exists x \in \mathbb{Z}, x \in S$; hence we can choose an element $a \in S$ to work with in our proof. However, in the case where the non-empty subset of $\mathbb{Z}$ is bounded below, the well-ordering property gives us the existence of a unique smallest element. Hence given a non-empty set $S \subseteq \mathbb{Z}$ that is bounded below, we may choose *the smallest element* $a \in S$.

We may also prove a reversal of the well-ordering property; that every non-empty set of integers that is bounded above has a largest element.

Theorem 1.2.2.

Let $A \subseteq \mathbb{Z}$, with $A \neq \emptyset$. If A is bounded above, then A has a largest element. That is, if $\exists b \in \mathbb{Z}, \forall x \in A, x \leq b$, then $\exists a \in A, \forall x \in A, x \leq a$.

Proof.
Assume $\exists b \in \mathbb{Z}, \forall x \in A, x \leq b$.
    Choose such a b.
    Let $S = \{x \in \mathbb{Z} \mid -x \in A\}$.
    Since $A \neq \emptyset$, choose $y \in A$.
    Choose $z = -y$.
        Then $-z = -(-y) = y \in A$.
        Therefore, $z \in S$.
    Therefore, $\exists z \in \mathbb{Z}, z \in S$.
    Therefore, $S \neq \emptyset$.
    Let $x \in S$.
        Hence, $-x \in A$.
        Therefore, $-x \leq b$.
        We then have $-b \leq x$.
    Therefore, $\forall x \in S, -b \leq x$.
    We now have $S \neq \emptyset$ and $\forall x \in S, -b \leq x$.
    By the previous theorem, we can choose m to be the smallest element of S.
    Choose $a = -m$.
        Since $m \in S$, we have that $a = -m \in A$.
        Let $x \in A$.
            Since $-(-x) = x \in A$, we have $-x \in S$.
            Therefore, $m \leq -x$.
            This gives us $x \leq -m$; hence $x \leq a$.
        Therefore, $\forall x \in A, x \leq a$.
    Therefore, $\exists a \in A, \forall x \in A, x \leq a$.
Therefore, if $\exists b \in \mathbb{Z}, \forall x \in A, x \leq b$, then $\exists a \in A, \forall x \in A, x \leq a$. □

Proofs Using the Well-Ordering Property

A common technique, using the well-ordering property, is often used to prove statements of the form '$\forall x \in \mathbb{Z}, P(x)$,' where $P(x)$ is an open sentence. Using a proof by contradiction, we assume '$\exists x \in \mathbb{Z}, \neg P(x)$.' This assumption is identical to the assumption that the set

$$S = \{x \in \mathbb{Z} \mid \neg P(x)\}$$

is non-empty. If we can show that S is bounded below, then the well-ordering property ensures that S has a smallest element. If we are able to construct a smaller element of the set S then we can establish a contradiction. This argument usually follows the following structure:

Proof of $\forall x \in \mathbb{Z}$, $P(x)$.

Proof.
Assumption ► Suppose $\exists x \in \mathbb{Z}$, $\neg P(x)$.
Define S ► Let $S = \{x \in \mathbb{Z} \mid \neg P(x)\}$. By our assumption, $S \neq \emptyset$.
Demonstration
⋮
Demonstrate that S is bounded below.
⋮
Therefore S is bounded below.
Apply WOP ► By the WOP, choose a to be the smallest element of S.
Set a value ► Put $b =$ □.
Demonstration
⋮
Demonstrate that $b \in S$ and $b < a$.
⋮
Conclusion ► Therefore, $\exists b \in S$, $b < a$.
Contradiction ► This is a contradiction, since a is the smallest element of S.
Conclusion ► Therefore $\forall x \in \mathbb{Z}$, $P(x)$. □

We demonstrate this technique by proving one of the most fundamental properties of the integers. This property may seem intuitively obvious, but since it is not shared by the real numbers, its proof must use the well-ordering property.

Theorem 1.2.3.

$\forall x \in \mathbb{Z}$, if $x > 0$ then $x \geq 1$.

Proof.
Assumption ► Suppose $\exists x \in \mathbb{Z}$, $x > 0$ and $x < 1$.
Define S ► Let $S = \{x \in \mathbb{Z} \mid 0 < x < 1\}$. By our assumption, $S \neq \emptyset$.
Let $x \in S$.
Then $0 < x < 1$.
Demonstration In particular, $0 < x$; hence $0 \leq x$.
Therefore, $\forall x \in S$, $0 \leq x$.
Hence, S is bounded below.
Apply WOP ► By the well-ordering property, choose a to be the smallest element of S.
Set a value ► Put $b = a^2$.
Since $a < 1$, we have $a^2 < (1)a$, hence $b < a$.
Since $b < a$ and $a < 1$, we have $b < 1$.
Demonstration Since $0 < a$, we have $0(a) < a^2$, hence $0 < b$.
We now have $0 < b$ and $b < 1$, hence $b \in S$.
Conclusion ► Therefore, $\exists b \in S$, $b < a$.
Contradiction ► This is a contradiction, since a is the smallest element of S.
Conclusion ► Therefore, $\forall x \in \mathbb{Z}$, if $x > 0$ then $x \geq 1$. □

Corollary 1.2.4.

$\forall x, y \in \mathbb{Z}$, if $x < y$ then $x + 1 \leq y$.

Proof.
Let $x, y \in \mathbb{Z}$.
  Assume $x < y$.
  Then $y - x > 0$.
    Therefore, by theorem 1.2.3, we have $y - x \geq 1$.
    Therefore, $x + 1 \leq y$.
  Therefore, if $x < y$, then $x + y \leq y$.
Therefore, $\forall x, y \in \mathbb{Z}$, if $x < y$ then $x + 1 \leq y$. □

The above technique is not the only way that one can use the well-ordering property in a proof. Notice that since the well-ordering property implies the *existence* of a smallest element of the set S, it can be used in place of *construction* to prove statements of the form $\exists x \in \mathbb{Z}$, $P(x)$. If the smallest element of a particular set happens to satisfy the open sentence $P(x)$, then the existence of such an element can be given by the well-ordering property. Such an argument will often follow the following structure:

Proof of $\exists x \in \mathbb{Z}$, $P(x)$.

Proof.
Define S ► Let $S = \{x \in \mathbb{Z} \mid$ ☐ $\}$.
  ⋮
Demonstration *Demonstrate that S is non-empty and bounded below.*
  ⋮
  Therefore $S \neq \emptyset$ and S is bounded below.
Apply WOP ► By the WOP, choose a to be the smallest element of S.
  ⋮
Demonstration *Demonstrate $P(a)$.*
  ⋮
Conclusion ► Therefore, $\exists x \in \mathbb{Z}$, $P(x)$. □

We demonstrate this technique with several examples:

Proposition 1.2.5.

$\forall x \in \mathbb{R}, \exists n \in \mathbb{Z}, n - 1 < x \leq n.$

Proof.
Let $x \in \mathbb{R}$.
Define S ▶ Let $S = \{k \in \mathbb{Z} \mid x \leq k\}$.
Demonstration
By the Archimedean property, we have $\exists m \in \mathbb{N}, x < m$.
For such an m, we have $m \in S$; hence $S \neq \emptyset$.
Further, by the Archimedean property, we have $\exists p \in \mathbb{N}, -x < p$.
For such a p, we have $-p < x$.
Choosing $b = -p$ gives us $b \in \mathbb{Z}$ and $b < x$.
Let $k \in S$.
Then $b < x$ and $x < k$, hence $b < k$.
Therefore, $b \leq k$.
Therefore, $\forall k \in S, b \leq k$.
Therefore, $\exists b \in \mathbb{Z}, \forall k \in S, b \leq k$.
Hence, S has a lower bound.
Therefore $S \neq \emptyset$ and S is bounded below.
Apply WOP ▶ By the well-ordering property, choose n to be the smallest element of S.
Demonstration
Since $n \in S$, we have $x \leq n$.
Since $n - 1 < n$, we have $n - 1 \notin S$.
Therefore, $n - 1 < x$.
Conclusion ▶ Therefore, $\exists n \in \mathbb{Z}, n - 1 < x \leq n$.
Therefore, $\forall x \in \mathbb{R}, \exists n \in \mathbb{Z}, n - 1 < x \leq n$. □

Our next example is Euclid's *division algorithm*, which describes the idea of long division; the expression of a fraction as a quotient and remainder. The proof emerges out of the interpretation of division as repeated subtraction, along with a guarantee that we will not subtract ad-infinitum. For example, if we wish to reduce $\frac{14}{3}$ to a quotient and remainder, we may repeatedly add or subtract 3 from 14, forming the following sequence of possible remainders: $\{\ldots, 14, 11, 8, 5, 2, \ldots\}$. *The remainder* is the smallest non-negative element in this set (in this case 2), and *the quotient* is a count of the number of times 3 was subtracted from 14 in order to reach this remainder (in this case 4 times). We then obtain the expression $14 = (4)(3) + 2$, or $\frac{14}{3} = 4 + \frac{2}{3}$. In general, *the remainder* when x is divided by y will be the smallest non-negative element of the set of all possible remainders

$$\{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z},\ x = yq + a\}.$$

Since the well-ordering property guarantees the existence of a smallest element in any non-empty set of non-negative integers, its role in the proof of the division algorithm is to secure the existence of a smallest element in this chain of remainders. Hence, the well-ordering property ensures that by forming the set of all possible remainders ($\{\ldots, 14, 11, 8, 5, 2, \ldots\}$ in our example), we will inevitably arrive at a smallest non-negative element. Hence, *the remainder* will always exist.

Theorem 1.2.6 (The Division Algorithm)**.**

$\forall x, y \in \mathbb{Z}$, if $y > 0$ then $\exists q, r \in \mathbb{Z}$, $x = yq + r$ and $0 \leq r < y$.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume $y > 0$.
Define S ▶ Let $S = \{a \in \mathbb{Z} \mid 0 \leq a \text{ and } \exists q \in \mathbb{Z},\ x = yq + a\}$.
Demonstration
We have either $x \geq 0$ or $x < 0$.
In case $x \geq 0$, we see that since $x = y(0) + x$,
$\exists q \in \mathbb{Z}$, $x = yq + x$, and $0 \leq x$.
Therefore, $x \in S$; hence $S \neq \emptyset$.
In case $x < 0$, since $y > 0$, we have $x = yx + (x - yx)$.
Therefore, $\exists q \in \mathbb{Z}$, $x = yq + x(1 - y)$.
Further, since $x < 0$ and $1 - y \leq 0$, we have $x(1 - y) \geq 0$.
Therefore, $x(1 - y) \in S$; hence $S \neq \emptyset$.
In both cases we have $S \neq \emptyset$.
Further, for $a \in S$, we have $0 \leq a$; hence S is bounded below by 0.
Therefore, $S \neq \emptyset$ and S is bounded below.
Apply WOP ▶ By the well-ordering property, choose r to be the smallest element of S.
Demonstration
Since $r \in S$, we have that $\exists q \in \mathbb{Z}$, $x = yq + r$ and $0 \leq r$.
Choose $q_0 \in \mathbb{Z}$ such that $x = yq_0 + r$.
It only remains to show that $r < y$.
To this end, suppose $y \leq r$.
Then $0 \leq r - y$.
Put $q = q_0 + 1$.
Then $x = yq_0 + r = yq_0 + y + r - y = y(q_0 + 1) + (r - y) = yq + (r - y)$.
Therefore, $\exists q \in \mathbb{Z}$, $x = yq + (r - y)$ and $0 \leq r - y$.
Therefore, $r - y \in S$.
However, since $y > 0$, we have $r - y < r$.
Since r is the smallest element of S, this is a contradiction.
Therefore, $r < y$.
Conclusion ▶ Therefore, $\exists q, r \in \mathbb{Z}$, $x = yq + r$ and $0 \leq r < y$.
Therefore, if $y > 0$ then $\exists q, r \in \mathbb{Z}$, $x = yq + r$ and $0 \leq r < y$.
Therefore, $\forall x, y \in \mathbb{Z}$, if $y > 0$ then $\exists q, r \in \mathbb{Z}$, $x = yq + r$ and $0 \leq r < y$. □

One consequence of the division algorithm is that it partitions the integers into **evens** and **odds**. Since the remainder when an integer is divided by 2 must be strictly less than 2, it will either be 0 or 1. When the remainder is 0, we say the integer is *even*. When the remainder is 1, we say the integer is *odd*. A precise definition for even and odd can be given as follows:

Definition 1.2.2. For $x \in \mathbb{Z}$, x is **even** means

$$\exists q \in \mathbb{Z},\ x = 2q.$$

x is **odd** means

$$\exists q \in \mathbb{Z},\ x = 2q + 1.$$

Proposition 1.2.7.

$\forall x \in \mathbb{Z}$, x is odd if and only if x is not even.

Proof.
Let $x \in \mathbb{Z}$.
Suppose x is odd and x is even.
Then $\exists q \in \mathbb{Z}$, $x = 2q$, and $\exists q \in \mathbb{Z}$, $x = 2q + 1$.
Choose $a \in \mathbb{Z}$ such that $x = 2a$, and choose $b \in \mathbb{Z}$ for which $x = 2b + 1$.
We then have $2a = 2b + 1$; hence $2(a - b) = 1$.
If $a - b \leq 0$, then $2(a - b) \leq 0$, hence $1 \leq 0$ which is a contradiction.
If $a - b > 0$, then $a - b \geq 1$ by theorem 1.2.3; hence $2(a - b) \geq 2$.
Then $1 \geq 2$, which can be reduced to the contradiction $0 \geq 1$.
Therefore, if x is even then x is not odd.
Conversely, assume x is not odd.
Applying the division algorithm, we have $\exists q, r \in \mathbb{Z}$, $x = 2q + r$ and $0 \leq r < 2$.
Choose such q and r.
Since $r < 2$, we have $0 < 2 - r$; hence $1 \leq 2 - r$ by theorem 1.2.3.
Therefore, $r \leq 1$.
Since x is not odd, we have $r \neq 1$; hence $r < 1$.
Therefore, $0 < 1 - r$; hence $1 \leq 1 - r$ by theorem 1.2.3.
Therefore, $r \leq 0$.
We now have $0 \leq r$ and $r \leq 0$. Hence $r = 0$.
Therefore, $x = 2q + 0$; hence x is even.
Therefore, if x is not odd then x is even.
We now have if x is even then x is not odd, and if x is not odd then x is even.
Therefore, x is even if and only if x is not odd.
Therefore, $\forall x \in \mathbb{Z}$, x is even if and only if x is not odd. □

A remark about the exclusive *or*

The proposition above has the form 'P if and only if $\neg Q$'. Recall that this means 'if P, then $\neg Q$, and if $\neg Q$, then P'. That is,

$$P \Leftrightarrow \neg Q \;\equiv\; (P \Rightarrow \neg Q) \text{ and } (\neg Q \Rightarrow P).$$

Note that the negation of the first implication 'if P, then $\neg Q$' is 'P and Q'. Hence, the first implication is equivalent to '$\neg(P$ and $Q)$'. That is,

$$P \Rightarrow \neg Q \;\equiv\; \neg(P \text{ and } Q).$$

Further, using the fact that $A \Rightarrow B \equiv \neg A$ or B, we see that the second implication 'if $\neg Q$, then P' is equivalent to '$\neg(\neg Q)$ or P'. That is,

$$\neg Q \Rightarrow P \;\equiv\; Q \text{ or } P.$$

Putting these equivalent forms of the first and second implications together gives us

$$P \Leftrightarrow \neg Q \;\equiv\; (P \text{ or } Q) \text{ and } \neg(P \text{ and } Q).$$

That is, either P is true or Q is true but not both. This is sometimes written 'P or else Q' and is known as the **exclusive or**; it excludes the possibility that both are true. Hence, in the above proposition, to say 'x is odd if and only if x is not even' is equivalent to saying 'x is either even or odd but not both'. That is, x is even *or else* x is odd.

Definition 1.2.3. For $x, y \in \mathbb{Z}$, x **divides** y means

$$\exists a \in \mathbb{Z},\; y = xa.$$

Proposition 1.2.8.

$\forall x, y \in \mathbb{Z}$, if $y \neq 0$ and x divides y then $|x| \leq |y|$.

Proof.
Let $x, y \in \mathbb{Z}$.
  Assume $y \neq 0$ and x divides y.
    Then $\exists a \in \mathbb{Z}$, $y = xa$. Choose such an a.
    Since $y \neq 0$, we have $a \neq 0$; hence $|a| \neq 0$.
    Since $0 \leq |a|$ and $|a| \neq 0$, we have $0 < |a|$.
    Therefore, $1 \leq |a|$.
    Therefore, $|x| \leq |x||a|$; hence $|x| \leq |xa|$.
    Therefore, $|x| \leq |y|$.
  Therefore, if $y \neq 0$ and x divides y, then $|x| \leq |y|$.
Therefore, $\forall x, y \in \mathbb{Z}$, if $y \neq 0$ and x divides y then $|x| \leq |y|$. □

Definition 1.2.4. For $x, y, g \in \mathbb{Z}$, with $x \neq 0$ and $y \neq 0$, g is the **greatest common divisor** of x and y means

1. $g > 0$,
2. g divides x and g divides y, and
3. $\forall a \in \mathbb{Z}$, if a divides x and a divides y, then $a \leq g$.

We denote that g is the greatest common divisor of x and y by $g = \gcd(x, y)$.

Definition 1.2.5. For $x, y, f \in \mathbb{Z}$, with $x \neq 0$ and $y \neq 0$, f is the **least common multiple** of x and y means

1. $f > 0$,
2. x divides f and y divides f, and
3. $\forall a \in \mathbb{Z}$, if x divides a and y divides a and $a \neq 0$, then $f \leq |a|$.

We denote that g is the least common multiple of x and y by $f = \operatorname{lcm}(x, y)$.

Theorem 1.2.9.

$\forall x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\exists g \in \mathbb{Z}$, $g = \gcd(x, y)$.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume $x \neq 0$ and $y \neq 0$.
Define S ▶ Let $S = \{a \in \mathbb{Z} \mid a \text{ divides both } x \text{ and } y\}$.
Since $x = (1)x$ and $y = (1)y$, we have that 1 divides both x and y.
Therefore, $1 \in S$.
Therefore, $S \neq \emptyset$.
Demonstration: Let $a \in S$.
Then a divides x, and since $x \neq 0$, we have $|a| \leq |x|$.
Since $a \leq |a|$, we then have $a \leq |x|$ by transitivity.
Therefore, $\forall a \in S$, $a \leq |x|$.
Therefore, S is bounded above by $|x|$.
Therefore, $S \neq \emptyset$, and S is bounded above.
Apply *WOP* ▶ By theorem 1.2.2, choose g to be the largest element of S.
Demonstration: Since $g \in S$, we have that g divides both x and y.
Let $a \in \mathbb{Z}$, and assume a divides both x and y.
Then $a \in S$; hence $a \leq g$.
Therefore, $\forall a \in \mathbb{Z}$, if a divides both x and y then $a \leq g$.
Finally, since $1 \in S$, we have $1 \leq g$; hence $g > 0$.
Therefore, $g = \gcd(x, y)$.
Conclusion ▶ Therefore, $\exists g \in \mathbb{Z}$, $g = \gcd(x, y)$.
Therefore, if $x \neq 0$ and $y \neq 0$, then $\exists g \in \mathbb{Z}$, $g = \gcd(x, y)$.
Therefore, $\forall x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\exists g \in \mathbb{Z}$, $g = \gcd(x, y)$. □

There is a connection between the *common divisors* of x and y and the *linear combinations* of x and y. By linear combinations of x and y, we mean the numbers that can be written in the form $xs + ty$ for some s and t. In fact, we will show that the *greatest common divisor* is the *smallest linear combination*. Before we do this, however, we need the following characterization of the common divisors of x and y.

Lemma 1.2.10.

$\forall a, x, y \in \mathbb{Z}$, a divides both x and y if and only if $\forall s, t \in \mathbb{Z}$, a divides $xs + yt$.

Proof.
Let $a, x, y \in \mathbb{Z}$.
    Assume a divides both x and y.
        Choose $u, v \in \mathbb{Z}$ with $x = au$ and $y = av$.
        Let $s, t \in \mathbb{Z}$.
            Put $w = us + vt$.
                $xs + yt = aus + avt = a(us + vt) = aw$.
            Therefore, $\exists w \in \mathbb{Z}$, $xs + yt = aw$. Hence, a divides $xs + yt$.
        Therefore, $\forall s, t \in \mathbb{Z}$, a divides $xs + yt$.
    Therefore, if a divides both x and y, then $\forall s, t \in \mathbb{Z}$, a divides $xs + yt$.
    Conversely, assume $\forall s, t \in \mathbb{Z}$, a divides $xs + yt$.
        Taking $s = 1$ and $t = 0$ gives us that a divides x.
        Taking $s = 0$ and $t = 1$ gives us that a divides y.
        Therefore, a divides both x and y.
    Therefore, if $\forall s, t \in \mathbb{Z}$, a divides $xs + yt$, then a divides both x and y.
Therefore, $\forall a, x, y \in \mathbb{Z}$, a divides both x and y if and only if $\forall s, t \in \mathbb{Z}$, a divides $xs + yt$. □

With this view of common divisors in mind, we will show that the *greatest common divisor* is itself a linear combination of x and y. In fact, it is the smallest positive linear combination.

Theorem 1.2.11 (Bezout's Identity)**.**

$\forall x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\exists s, t \in \mathbb{Z}$, $\gcd(x, y) = sx + ty$.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume $x \neq 0$ and $y \neq 0$.
Let $S = \{a \in \mathbb{Z} \mid a > 0 \text{ and } \exists s, t \in \mathbb{Z},\ a = sx + ty\}$.
Since $x \neq 0$ and $y \neq 0$, we have $x^2 > 0$ and $y^2 > 0$.
Therefore, $x^2 + y^2 > 0$ and $x^2 + y^2 = (x)x + (y)y$, hence $x^2 + y^2 \in S$.
Therefore, $S \neq \emptyset$.
Further, for $a \in S$, we have $0 < a$; hence S is bounded below by 0.
Therefore, $S \neq \emptyset$ and S is bounded below.
By the well-ordering property, choose g to be the smallest element of S.
Since $g \in S$, $g > 0$ and $\exists s, t \in \mathbb{Z}$, $g = sx + ty$.
Choose such s and t.
We will show that $g = \gcd(x, y)$.
Applying the division algorithm, choose $q, r \in \mathbb{Z}$, $x = gq + r$ and $0 \leq r < g$.
Suppose $r \neq 0$.
Then $r > 0$.
Further, $r = x - gq = x - (sx + ty)q = (1 - sq)x + (-tq)y$.
Therefore $r \in S$.
We then have $g \leq r$, which is a contradiction, since $r < g$.
Therefore, $r = 0$.
Therefore, $x = gq$; hence g divides x.
Similarly, g divides y.
Let $a \in \mathbb{Z}$, and assume a divides both x and y.
Then, since $g = sx + ty$, a divides g by the previous lemma.
Therefore, $|g| \geq |a|$.
Since $g > 0$, we have $|g| = g$; hence $g \geq |a|$.
Since $|a| \geq a$, we then have $g \geq a$.
Therefore, $\forall a \in \mathbb{Z}$, if a divides both x and y, then $g \geq a$.
Therefore, $g = \gcd(x, y)$.
Therefore, $\gcd(x, y) = sx + ty$.
Therefore, $\exists s, t \in \mathbb{Z}$, $\gcd(x, y) = sx + ty$.
Therefore, if $x \neq 0$ and $y \neq 0$, then $\exists s, t \in \mathbb{Z}$, $\gcd(x, y) = sx + ty$.
Therefore, $\forall x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\exists s, t \in \mathbb{Z}$, $\gcd(x, y) = sx + ty$. □

Corollary 1.2.12.

$\forall x, y, a \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$ and a divides both x and y, then a divides $\gcd(x, y)$.

Proof.
Let $x, y, a \in \mathbb{Z}$.
Assume $x \neq 0$ and $y \neq 0$ and a divides both x and y.
By Bezout's identity, we may choose $s, t \in \mathbb{Z}$ with $\gcd(x, y) = sx + ty$.
Hence, a divides $\gcd(x, y)$ by lemma 1.2.10.
Therefore, if $x \neq 0$ and $y \neq 0$ and a divides both x and y, then a divides $\gcd(x, y)$.
Therefore, $\forall x, y, a \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$ and a divides both x and y, then a divides $\gcd(x, y)$. □

In the next example, we will prove that $\sqrt{2}$ is irrational. Since this example deals with the distinction between rational and irrational numbers, we must state a usable definition of rational and irrational numbers. Roughly speaking, rational numbers are those real numbers that can be expressed as a fraction of integers. Irrational numbers are those real numbers that are not rational. However, to give a definition that is usable in a proof, we must make sure our definition is precise (and preferably in symbolic form). We state the definition as follows:

Definition 1.2.6. For $x \in \mathbb{R}$, x is **rational** means

$$\exists a, b \in \mathbb{Z},\ a = bx \text{ and } b \neq 0.$$

x is **irrational** means x is not rational.

By insisting that the denominator b in the above definition is positive, we get a much more convenient characterization of the rational numbers. That we can place such a demand on the denominator is the subject of the next example:

Proposition 1.2.13.

$\forall x \in \mathbb{R}$, x is rational if and only if $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$.

Proof.
Let $x \in \mathbb{R}$.
    Assume x is rational.
        Then $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b \neq 0$.
        Accordingly, choose $s, t \in \mathbb{Z}$ with $s = tx$ and $t \neq 0$.
        Case 1: $t > 0$.
            Since $s = tx$ and $t > 0$, we have $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$.
        Case 2: $t < 0$.
            Put $a = -s$ and $b = -t$.
                Since $s = tx$, we have $-s = -tx$; hence $a = bx$.
                Also, since $t < 0$, we have $-t > 0$; hence $b > 0$.
            Therefore, $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$.
    Therefore, if x is rational, then $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$.
    Conversely, assume $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$.
        Choose such $a, b \in \mathbb{Z}$.
        Since $b > 0$, we have $b \neq 0$.
        Therefore, $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b \neq 0$.
        That is, x is rational.
    Therefore, if $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$, then x is rational.
    Therefore, x is rational if and only if $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$.
Therefore, $\forall x \in \mathbb{R}$, x is rational if and only if $\exists a, b \in \mathbb{Z}$, $a = bx$ and $b > 0$. □

Before proving that $\sqrt{2}$ is irrational, we give a property of the even integers that will be used in the proof that $\sqrt{2}$ is irrational.

Lemma 1.2.14.

$\forall x \in \mathbb{Z}$, if x^2 is even, then x is even.

Proof.
Let $x \in \mathbb{Z}$.
    Assume x is not even.
        In this case, x is odd.
        Therefore, $\exists t \in \mathbb{Z}$, $x = 2t + 1$. Choose such a t.
        Choose $s = 2t^2 + 2t$
            $x^2 = (2t + 1)^2 = 4t^2 + 4t + 1 = 2(2t^2 + 2t) + 1 = 2s + 1$.
        Therefore, $\exists s \in \mathbb{Z}$, $x^2 = 2s + 1$.
        Therefore, x^2 is odd.
        Therefore, x^2 is not even.
    Therefore, if x is not even, then x^2 is not even.
    Therefore, if x^2 is even, then x is even.
Therefore, $\forall x \in \mathbb{Z}$, if x^2 is even, then x is even. □

We are now ready to prove that $\sqrt{2}$ is irrational. To do this, we will return to the method discussed earlier for using a proof by contradiction and the well-ordering property.

Proposition 1.2.15.

$\sqrt{2}$ is irrational.

Proof.
Assumption ► Suppose $\sqrt{2}$ is rational.
Then $\exists x, y \in \mathbb{Z}$, $y = x\sqrt{2}$ and $x > 0$.
Hence, $\exists x, y \in \mathbb{Z}$, $y^2 = 2x^2$ and $x > 0$.
Define S ► Let $S = \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z},\ y^2 = 2x^2 \text{ and } x > 0\}$. By our assumption, $S \neq \emptyset$.
Demonstration [For all $x \in S$, $x > 0$, hence S is bounded below.
Apply WOP ► By the well-ordering property, choose a to be the smallest element of S.
Then $\exists y \in \mathbb{Z}$, $y^2 = 2a^2$ and $a > 0$. Choose such a y.
Since y^2 is even, we have that y is even by lemma 1.2.14.
Since y is even, choose $z \in \mathbb{Z}$ such that $y = 2z$.
We now have $(2z)^2 = 2a^2$; hence $4z^2 = 2a^2$.
This gives us $2z^2 = a^2$, which means a^2 is even, hence a is even.
Set a value ► Choose $b \in \mathbb{Z}$ such that $a = 2b$.
Demonstration
We then have $2z^2 = (2b)^2$; hence $z^2 = 2b^2$.
Therefore, $\exists z \in \mathbb{Z}$, $z^2 = 2b^2$.
Further, since $a > 0$ and $a = 2b$, we have $b > 0$.
Therefore, $b \in S$.
Further, since $1 < 2$, $b < 2b$; hence $b < a$.
Conclusion ► Therefore, $\exists b \in S$, $b < a$.
Contradiction ► This is a contradiction, since a is the smallest element of S.
Conclusion ► Therefore, $\sqrt{2}$ is irrational. □

The Principle of Mathematical Induction

We can define the set of **natural numbers** to be the set of positive integers:

Definition 1.2.7.

$$\mathbb{N} = \{x \in \mathbb{Z} \mid x > 0\}.$$

The definition of the natural numbers as positive integers may not be the most intuitive definition we can give, but it allows us the advantage of being able to use the properties of the integers that we have been able to prove so far. For a more natural definition, we note that the natural numbers are completely determined by the idea of counting. That is, if we start with 1*, and for each* n *that has been counted we proceed to its successor* $n + 1$*, then there is no natural number which cannot be reached by this process. The view of the natural numbers as 'numbers that can be produced by counting' is much closer to our intuitive notion of natural numbers than the definition given as 'positive integers.' It seems very likely that humans come to understand the idea of natural numbers by counting, long before we entertain any notions of negative numbers or the complete set of integers.*

Fortunately, the approach we have taken, of defining the integers by axioms and defining the natural numbers as a subset of these integers, is consistent with the intuitive notion of natural numbers as the elements of the counting process. That this is the case, is known as the **principle of mathematical induction**.

The Principle of Mathematical Induction

Let A be a set. If $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$, then $\mathbb{N} \subseteq A$.

The proof of the principle of mathematical induction makes use of the well-ordering property, using a proof by contradiction:

Theorem 1.2.16 (The Principle of Mathematical Induction)**.**

Let A be a set. If $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$, then $\mathbb{N} \subseteq A$.

Proof.
Let A be a set.
Assume $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
    Suppose $\mathbb{N} \nsubseteq A$; hence $\exists x \in \mathbb{N}$, $x \notin A$.
        Let $S = \{x \in \mathbb{N} \mid x \notin A\}$. By our assumption, $S \neq \emptyset$.
            Since $S \subseteq \mathbb{N}$, we have that S is bounded below by 0.
        By the well-ordering property, choose a to be the smallest element of S.
        Since $a \in \mathbb{N}$, we have $a > 0$; hence $a \geq 1$.
        Further, since $1 \in A$, we have $1 \notin S$. Therefore, $a \neq 1$.
        Therefore, $a > 1$.
        Choose $n = a - 1$.
            We then have $n > 0$; hence $n \in \mathbb{N}$.
            Since $n + 1 = a$ and $a \notin A$, we have $n + 1 \notin A$.
            Therefore, $n \notin A$.
            We now have $n \in \mathbb{N}$ and $n \notin A$, hence $n \in S$.
            Further, since $a - 1 < a$, we have $n < a$.
        Therefore, $\exists n \in S$, $n < a$
        This is a contradiction, since a is the smallest element of S.
    Therefore, $\mathbb{N} \subseteq A$.
Therefore, if $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$, then $\mathbb{N} \subseteq A$. □

Although this gives a nice characterization of the natural numbers in terms of counting, the starting point of 1 is somewhat arbitrary. We could reasonably begin the counting process at any integer, and the set produced would contain all integers after our chosen starting point. That is, the set would contain all elements of the set $\{x \in \mathbb{Z} \mid x \geq a\}$. To simplify notation, we use the following:

Notation

For $a \in \mathbb{Z}$, denote by $\mathbb{Z}_{\geq a}$, the set

$$\mathbb{Z}_{\geq a} = \{x \in \mathbb{Z} \mid x \geq a\}.$$

Similarly, denote by $\mathbb{Z}_{\leq a}$, the set

$$\mathbb{Z}_{\leq a} = \{x \in \mathbb{Z} \mid x \leq a\}.$$

If we allow the starting point to be flexible, then we obtain the following more general version of the principle of mathematical induction:

The Principle of Mathematical Induction Starting at $a \in \mathbb{Z}$

Let $a \in \mathbb{Z}$, and let A be a set. If $a \in A$ and $\forall n \in \mathbb{Z}_{\geq a}$, if $n \in A$ then $n + 1 \in A$, then $\mathbb{Z}_{\geq a} \subseteq A$.

The proof of this version of the principle of mathematical induction is similar to that of the version beginning from 1:

Theorem 1.2.17.

Let $a \in \mathbb{Z}$, and let A be a set. If $a \in A$ and $\forall n \in \{x \in \mathbb{Z} \mid x \geq a\}$, if $n \in A$ then $n + 1 \in A$, then $\{x \in \mathbb{Z} \mid x \geq a\} \subseteq A$.

Proof.
Let $a \in \mathbb{Z}$, and let A be a set.
Assume $a \in A$ and $\forall n \in \{x \in \mathbb{Z} \mid x \geq a\}$, if $n \in A$ then $n + 1 \in A$.
    Suppose $\{x \in \mathbb{Z} \mid x \geq a\} \nsubseteq A$; hence $\exists x \in \mathbb{Z}$, $x \geq a$ and $x \notin A$.
        Let $S = \{x \in \mathbb{Z} \mid x \geq a \text{ and } x \notin A\}$. By our assumption, $S \neq \emptyset$.
        For $x \in S$, we have $x \geq a$; hence S is bounded below by a.
        By the well-ordering property, choose m to be the smallest element of S.
        We then have $m \geq a$.
        Further, since $a \in A$, we have $a \notin S$. Therefore, $m \neq a$.
        Therefore, $m > a$; hence $m \geq a + 1$.
        Choose $n = m - 1$.
            We then have $n \geq a$; hence $n \in \{x \in \mathbb{Z} \mid x \geq a\}$.
            Since $n + 1 = m$ and $m \notin A$, we have $n + 1 \notin A$.
            Therefore, $n \notin A$.
            We now have $n \geq a$ and $n \notin A$, hence $n \in S$.
        Therefore, $\exists n \in S$, $n < m$
        This is a contradiction, since m is the smallest element of S.
    Therefore, $\{x \in \mathbb{Z} \mid x \geq a\} \subseteq A$.
Therefore, if $a \in A$ and $\forall n \in \mathbb{Z}$, if $n \in A$ then $n + 1 \in A$, then $\{x \in \mathbb{Z} \mid x \geq a\} \subseteq A$. □

Notice that these two versions of the principle of mathematical induction are identical, only with 1 replaced by a and $\mathbb{N}$ replaced by $\mathbb{Z}_{\geq a}$. In fact, since $\mathbb{N} = \mathbb{Z}_{\geq 1}$, we see that the original principle of mathematical induction is the special case of this more general version when we take $a = 1$.

To generalize the principle of mathematical induction further, we will consider how one might obtain the set of *negative* integers in a way that is analogous to the construction of the positive integers by induction. For ease in describing the set of negative integers, we introduce the notation:

Notation

Denote by $-\mathbb{N}$, the set

$$-\mathbb{N} = \{x \in \mathbb{Z} \mid x < 0\}.$$

The negative integers can also be arrived at by counting, only rather than proceeding from a number n to its successor $n + 1$, we must count backwards, proceeding from a number n to its predecessor $n - 1$. In this reversed version of the principle of mathematical induction, we will start the counting process at the largest negative number -1. We leave it as an exercise to verify that if this backwards counting process is started at any integer a, it will completely determine the set $\mathbb{Z}_{\leq a} = \{x \in \mathbb{Z} \mid x \leq a\}$.

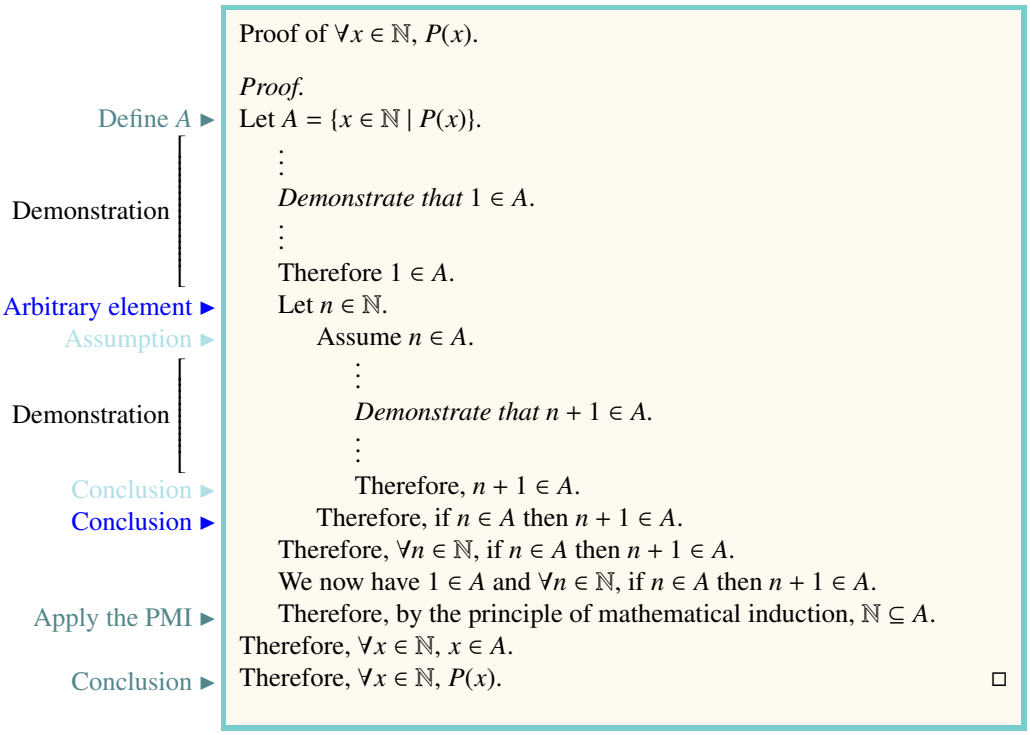
Theorem 1.2.18.

Let A be a set. If $-1 \in A$ and $\forall n \in -\mathbb{N}$, if $n \in A$ then $n - 1 \in A$, then $-\mathbb{N} \subseteq A$.

Proof.
Let A be a set.
Assume $-1 \in A$ and $\forall n \in -\mathbb{N}$, if $n \in A$ then $n - 1 \in A$.
    Suppose $-\mathbb{N} \nsubseteq A$; hence $\exists x \in -\mathbb{N}$, $x \notin A$.
        Let $S = \{x \in -\mathbb{N} \mid x \notin A\}$. By our assumption, $S \neq \emptyset$.
            Since $S \subseteq -\mathbb{N}$, we have that S is bounded above by 0.
        By theorem 1.2.2, choose a to be the largest element of S.
        Since $a \in -\mathbb{N}$, we have $a < 0$; hence $a \leq -1$.
        Further, since $-1 \in A$, we have $-1 \notin S$. Therefore, $a \neq -1$.
        Therefore, $a < -1$.
        Choose $n = a + 1$.
            We then have $n < 0$; hence $n \in -\mathbb{N}$.
            Since $n - 1 = a$ and $a \notin A$, we have $n - 1 \notin A$.
            Therefore, $n \notin A$.
            We now have $n \in -\mathbb{N}$ and $n \notin A$, hence $n \in S$.
            Further, since $a + 1 > a$, we have $n > a$.
        Therefore, $\exists n \in S$, $n > a$
        This is a contradiction, since a is the largest element of S.
    Therefore, $-\mathbb{N} \subseteq A$.
Therefore, if $-1 \in A$ and $\forall n \in -\mathbb{N}$, if $n \in A$ then $n - 1 \in A$, then $-\mathbb{N} \subseteq A$. □

Proofs Using the Principle of Mathematical Induction

The principle of mathematical induction provides us with a proof technique that can be very effective for proving statements of the form $\forall x \in \mathbb{N}$, $P(x)$, where $P(x)$ is an open sentence. The reasoning behind the technique is as follows: If we define the **truth set** of the open sentence $P(x)$ as the set $A = \{x \in \mathbb{N} \mid P(x)\}$, then to prove $\mathbb{N} \subseteq A$ is to prove $\forall x \in \mathbb{N}$, $P(x)$. Further, the principle of mathematical induction gives us a way to prove $\mathbb{N} \subseteq A$. That is, if we can show that $1 \in A$ and that $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$, then the principle of mathematical induction ensures us that our set A contains all of the natural numbers. Hence the *truth set* of the open sentence $P(x)$ contains *all* natural numbers, meaning $P(x)$ is true *for all* natural numbers x. The structure of such a proof will then be the following:



Note that to apply the principle of mathematical induction, we must demonstrate that the two conditions given in the principle are satisfied. The first demonstration must verify the statement '$1 \in A$.' This is sometimes easy and sometimes difficult, depending on the set A.

The second condition that must be verified in order to apply the principle of mathematical induction is '$\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.' Since this is a statement about *all natural numbers*, its proof involves the introduction of an arbitrary variable n. Hence the line 'Let $n \in \mathbb{N}$' in the above proof template. Further, the statement that must be demonstrated about this arbitrary natural number n is 'if $n \in A$ then $n+1 \in A$.' Since this statement is an implication of the form 'if P then Q,' its proof will use one of the three techniques for proving implications; those being *direct proof*, *contraposition*, and proof by *contradiction*. The above template shows a *direct proof* being used to show 'if $n \in A$ then $n + 1 \in A$.' That is, we assume '$n \in A$,' and demonstrate '$n + 1 \in A$.' If we were to use a proof by *contraposition* at this stage, then our assumption would be '$n + 1 \notin A$' and our conclusion would be '$n \notin A$.' Similarly, if we decide to employ a proof by *contradiction*, our assumption would be '$n \in A$ and $n+1 \notin A$,' and from this assumption we would need to derive a contradiction.

If we can successfully demonstrate that both of these conditions hold, then the principle of mathematical induction ensures that $A = \mathbb{N}$, which allows us to complete our proof. The following examples are intended to illustrate how one uses this structure to prove statements about the natural numbers.

Proposition 1.2.19.

$\forall x \in \mathbb{N}$, 7 divides $3^{2x-1} + 2^{x+1}$.

Proof.
Let $A = \{x \in \mathbb{N} \mid 7 \text{ divides } 3^{2x-1} + 2^{x+1}\}$. — Define A ▶
  Choose $a = 1$.
    $3^{2(1)-1} + 2^{1+1} = 7 = 7a$.
  Therefore, $\exists a \in \mathbb{Z}$, $3^{2(1)-1} + 2^{1+1} = 7a$.
  Therefore, 7 divides $3^{2(1)-1} + 2^{1+1}$.
  Hence, $1 \in A$. — Demonstration
  Let $n \in \mathbb{N}$. — Arbitrary element ▶
    Assume $n \in A$. — Assumption ▶
      Then, 7 divides $3^{2n-1} + 2^{n+1}$.
      That is, $\exists t \in \mathbb{Z}$, $3^{2n-1} + 2^{n+1} = 7t$. Choose such a t.
      Choose $s = 3^{2n-1} + 2t$.

$$\begin{aligned} 3^{2(n+1)-1} + 2^{(n+1)+1} &= 9(3^{2n-1}) + 2(2^{n+1}) \\ &= 7(3^{2n-1}) + 2(3^{2n-1}) + 2(2^{n+1}) \\ &= 7(3^{2n-1}) + 2(3^{2n-1} + 2^{n+1}) \\ &= 7(3^{2n-1}) + 2(7t) \\ &= 7(3^{2n-1} + 2t) \\ &= 7s \end{aligned}$$

      Therefore, $\exists s \in \mathbb{Z}$, $3^{2(n+1)-1} + 2^{(n+1)+1} = 7s$. — Demonstration
      Hence, 7 divides $3^{2(n+1)-1} + 2^{(n+1)+1}$.
      Therefore, $n + 1 \in A$. — Conclusion ▶
    Therefore, if $n \in A$ then $n + 1 \in A$. — Conclusion ▶
  Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
  We now have $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$. — Apply the PMI ▶
  Therefore, by the principle of mathematical induction, $\mathbb{N} \subseteq A$.
Therefore, $\forall x \in \mathbb{N}$, $x \in A$. — Conclusion ▶
Therefore, $\forall x \in \mathbb{N}$, 7 divides $3^{2x-1} + 2^{x+1}$. □

Proposition 1.2.20.

$\forall x \in \mathbb{N}, 2^x > x$.

Proof.
Define A ▸ Let $A = \{x \in \mathbb{N} \mid 2^x > x\}$.
Demonstration
Since $2^1 = 2$ and $2 > 1$, we have $2^1 > 1$.
Therefore, $1 \in A$.
Arbitrary element ▸ Let $n \in \mathbb{N}$.
Assumption ▸ Assume $n \in A$.
Demonstration
Hence, $2^n > n$.
Therefore, $2(2^n) > 2n$; hence $2^{n+1} > 2n$.
Since $n \geq 1$, we have $n + n \geq n + 1$. Therefore, $2n \geq n + 1$.
We now have $2^{n+1} > 2n$ and $2n \geq n + 1$.
Hence, by transitivity, $2^{n+1} > n + 1$.
Therefore, $n + 1 \in A$.
Conclusion ▸ Therefore, if $n \in A$ then $n + 1 \in A$.
Conclusion ▸ Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
We now have $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
Apply the PMI ▸ Therefore, by the principle of mathematical induction, $\mathbb{N} \subseteq A$.
Conclusion ▸ Therefore, $\forall x \in \mathbb{N}, 2^x > x$. □

In the next example, we will prove the statement

$$\forall x \in \mathbb{Z},\ \text{if } \exists a \in \mathbb{Z},\ x = 3a + 1,\ \text{then } \forall n \in \mathbb{N},\ \exists b \in \mathbb{Z},\ x^n = 3b + 1.$$

Since this is a statement about all integers x, we will introduce an arbitrary variable $x \in \mathbb{Z}$. For this x, we will need to demonstrate the implication

$$\text{if } \underbrace{\exists a \in \mathbb{Z},\ x = 3a + 1,}_{P} \text{ then } \underbrace{\forall n \in \mathbb{N},\ \exists b \in \mathbb{Z},\ x^n = 3b + 1}_{Q}.$$

Using a direct proof, we will assume $\exists a \in \mathbb{Z},\ x = 3a + 1$. We are then required to demonstrate

$$\forall n \in \mathbb{N},\ \exists b \in \mathbb{Z},\ x^n = 3b + 1.$$

This is a statement about all natural numbers, and we will prove it using induction. We then see that our technique of using the principle of mathematical induction need not be employed from the beginning of the proof. We may decide to use other more direct techniques until we reach a point in our demonstration where a proof by induction is appropriate.

Proposition 1.2.21.

$\forall x \in \mathbb{Z}$, if $\exists a \in \mathbb{Z}$, $x = 3a + 1$, then $\forall n \in \mathbb{N}$, $\exists b \in \mathbb{Z}$, $x^n = 3b + 1$.

Proof.
Let $x \in \mathbb{Z}$.
Assume $\exists a \in \mathbb{Z}$, $x = 3a + 1$. Choose such an a.
Define A ▶ Let $A = \{n \in \mathbb{N} \mid \exists b \in \mathbb{Z},\ x^n = 3b + 1\}$.
Demonstration [Since $x^1 = x = 3a + 1$, we have $1 \in A$.
Arbitrary element ▶ Let $n \in \mathbb{N}$.
Assumption ▶ Assume $n \in A$.
Then $\exists s \in \mathbb{Z}$, $x^n = 3s + 1$. Choose such an s.
Choose $t = 3as + a + s$.

Demonstration

$$\begin{aligned} x^{n+1} &= x(x^n) \\ &= (3a + 1)(3s + 1) \\ &= 9as + 3a + 3s + 1 \\ &= 3(3as + a + s) + 1 \\ &= 3t + 1 \end{aligned}$$

Therefore, $\exists t \in \mathbb{Z}$, $x^{n+1} = 3t + 1$.
Conclusion ▶ Therefore, $n + 1 \in A$.
Conclusion ▶ Therefore, if $n \in A$ then $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
We now have $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
Apply the PMI ▶ Therefore, by the principle of mathematical induction, $\mathbb{N} \subseteq A$.
Conclusion ▶ Therefore, $\forall n \in \mathbb{N}$, $\exists b \in \mathbb{Z}$, $x^n = 3b + 1$.
Therefore, if $\exists a \in \mathbb{Z}$, $x = 3a + 1$, then $\forall n \in \mathbb{N}$, $\exists b \in \mathbb{Z}$, $x^n = 3b + 1$.
Therefore, $\forall x \in \mathbb{Z}$, if $\exists a \in \mathbb{Z}$, $x = 3a + 1$, then $\forall n \in \mathbb{N}$, $\exists b \in \mathbb{Z}$, $x^n = 3b + 1$. □

The next example shows that every finite set of real numbers has a maximum element. That is, if $S \subseteq \mathbb{R}$ is a set with a finite number of elements, then $\exists a \in S$, $\forall x \in S$, $x \leq a$. We prove this using induction on the number of elements in the set.

Proposition 1.2.22.

$\forall m \in \mathbb{N}$, if $S \subseteq \mathbb{R}$ is a set with m elements, then $\exists a \in S, \forall x \in S, x \leq a$.

Proof.
Define A ▶ Let $A = \{m \in \mathbb{N} \mid$ if $S \subseteq \mathbb{R}$ is a set with m elements, then $\exists a \in S,\ \forall x \in S,\ x \leq a\}$.
Demonstration
    Assume $S \subseteq \mathbb{R}$ is a set with 1 element.
        Then $S = \{b\}$ for some $b \in \mathbb{R}$.
        Therefore, $\forall x \in S, x \leq b$.
        Therefore, $\exists a \in S, \forall x \in S, x \leq a$.
    Therefore, if $S \subseteq \mathbb{R}$ is a set with 1 element, then $\exists a \in S, \forall x \in S, x \leq a$.
    Therefore, $1 \in A$.
Arbitrary element ▶ Let $n \in \mathbb{N}$.
Assumption ▶ Assume $n \in A$.
        Assume $S \subseteq \mathbb{R}$ is a set with $n + 1$ elements.
            Since S is not empty, we may choose an element $b \in S$.
            The set $S \setminus \{b\}$ has n elements.
            Since $n \in A$, we have $\exists a \in S \setminus \{b\}, \forall x \in S \setminus \{b\}, x \leq a$.
            Choose such an a.
            Choose $c = \max(a, b)$.
                Let $x \in S$.
                    We consider two cases: $x = b$ and $x \neq b$.
                    Case 1: $x = b$.
                        In this case, $x = b \leq \max(a, b) = c$,
                        hence $x \leq c$.
                    Case 2: $x \neq b$.
                        Then, $x \in S \setminus \{b\}$.
                        Hence, $x \leq a \leq \max(a, b) = c$.
                        Therefore, $x \leq c$.
                    In both cases, $x \leq c$.
                Therefore, $\forall x \in S, x \leq c$.
            Therefore, $\exists c \in S, \forall x \in S, x \leq c$.
        So, if $S \subseteq \mathbb{R}$ is a set with $n + 1$ elements, then $\exists c \in S, \forall x \in S, x \leq c$.
Conclusion ▶ Therefore, $n + 1 \in A$.
Conclusion ▶ Therefore, if $n \in A$ then $n + 1 \in A$.
    Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
    We now have $1 \in A$ and $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
Apply the PMI ▶ Therefore, by the principle of mathematical induction, $\mathbb{N} \subseteq A$.
Conclusion ▶ Thus, $\forall m \in \mathbb{N}$, if $S \subseteq \mathbb{R}$ is a set with m elements, then $\exists a \in S, \forall x \in S, x \leq a$. □

Inductive Subsets of $\mathbb{R}$

Earlier, we considered a generalization of the principle of mathematical induction in which the starting point is allowed to be any integer, as opposed to the common starting point of 1 used to construct the natural numbers. To extend this idea further, we may also consider starting points outside of the integers. The common concept that is featured in all of our generalizations is that the set in question is closed under the counting process. To simplify the language in our discussion, it will be worth while giving a name to this feature of a set.

Definition 1.2.8. For a subset $S \subseteq \mathbb{R}$, with $S \neq \emptyset$, to say S is **inductive** means $\forall x \in \mathbb{R}$, if $x \in S$ then $x + 1 \in S$.

There are many inductive subsets of the real numbers. For example, the interval $(0, \infty)$ is inductive. To prove that this set is inductive, we simply show that the defining condition '$\forall x \in \mathbb{R}$, if $x \in S$ then $x + 1 \in S$' is satisfied when the set S is replaced by the set in question. Here is the proof:

Proposition 1.2.23.

$(0, \infty)$ is inductive.

Proof.
Let $x \in \mathbb{R}$.
Assume $x \in (0, \infty)$.
That is, $x > 0$.
Then, since $x > 0$, we have $x + 1 > 1$.
Since $x + 1 > 1$ and $1 > 0$, we have $x + 1 > 0$ by transitivity.
Therefore, $x + 1 \in (0, \infty)$.
Therefore, if $x \in (0, \infty)$ then $x + 1 \in (0, \infty)$.
Therefore, $(0, \infty)$ is inductive. □

Earlier, we showed that the principle of mathematical induction for the natural numbers can be proven using the well-ordering property. It should be noted again that the well-ordering property is not satisfied by all bounded subsets of the real numbers. For example, the set in the previous example, $(0, \infty)$ satisfies the condition that $\forall x \in (0, \infty)$, $x \geq 0$. However, the set $(0, \infty)$ does not have a smallest element. However, we will show that for any given $a \in \mathbb{R}$, the *smallest inductive subset* of the real numbers containing a will always satisfy the well-ordering property. By the 'smallest inductive subset containing a,' we mean that the set does not contain an proper subsets that are inductive and contain a. More formally:

Definition 1.2.9. Let $a \in \mathbb{R}$. The **smallest inductive set containing** a is an inductive set M_a containing a, satisfying the property that if $A \subseteq \mathbb{R}$ for which $a \in A$ and A is inductive, then $M_a \subseteq A$.

Letting $a \in \mathbb{R}$, and letting M_a be the smallest inductive set containing a, we obtain a proof technique similar to a proof by induction, to prove statements of the form $\forall x \in M_a$, $P(x)$, for some predicate P. By defining the set $A = \{x \in M_a \mid P(x)\}$, if we can show that $a \in A$ and A is inductive, then the fact that M_a is the smallest inductive set containing a will give us that $M_a \subseteq A$. The statement $\forall x \in M_a$, $x \in A$ would then be true, which due to the definition of A means $\forall x \in M_a$, $P(x)$ is true. The proof structure is very similar to that obtained from the original principle of mathematical induction:

Proof of $\forall x \in M_a$, $P(x)$.

Proof.
Define A ▶ Let $A = \{x \in M_a \mid P(x)\}$.
Demonstration
    ⋮
    Demonstrate that $a \in A$.
    ⋮
    Therefore $a \in A$.
Arbitrary element ▶ Let $x \in \mathbb{R}$.
Assumption ▶ Assume $x \in A$.
Demonstration
        ⋮
        Demonstrate that $x + 1 \in A$.
        ⋮
        Therefore, $x + 1 \in A$.
Conclusion ▶ Therefore, if $x \in A$ then $x + 1 \in A$.
Conclusion ▶ Therefore, A is inductive.
    We now have $a \in A$ and A is inductive.
Apply Defn of M_a ▶ Therefore, $M_a \subseteq A$.
Therefore, $\forall x \in M_a$, $x \in A$.
Conclusion ▶ Therefore, $\forall x \in M_a$, $P(x)$. □

The following examples make use of the above proof technique.

Proposition 1.2.24.

Let $a \in \mathbb{R}$, and let M_a be the smallest inductive set containing a. Then, $\forall x \in M_a$, $x \geq a$.

Proof.
Let $A = \{x \in \mathbb{R} \mid x \in M_a \text{ and } x \geq a\}$.
We claim that A is an inductive set containing a.
Indeed, since $a \in M_a$ and $a \geq a$, we have $a \in A$.
Let $x \in \mathbb{R}$.
    Assume $x \in A$.
        Then since $x \in M_a$ and M_a is inductive, we have $x + 1 \in M_a$.
        Further, since $x \geq a$, we have $x + 1 \geq a + 1$.
        Since $x + 1 \geq a + 1$ and $a + 1 \geq a$, we have $x + 1 \geq a$ by transitivity.
        We have thus shown that $x + 1 \in M_a$ and $x + 1 \geq a$. Hence $x + 1 \in A$.
    Therefore, if $x \in A$ then $x + 1 \in A$.
Therefore, A is inductive.
Since $A \subseteq M_a$ for which $a \in A$ and A is inductive, we have $M_a \subseteq A$.
Let $x \in M_a$.
    Then $x \in A$ since $M_a \subseteq A$.
    Hence $x \geq a$.
Therefore, $\forall x \in M_a$, $x \geq a$. □

Proposition 1.2.25.

Let $a \in \mathbb{R}$, and let M_a be the smallest inductive set containing a. Then, $\forall x \in M_a$, if $x > a$ then $x - 1 \in M_a$.

Proof.
Let $A = \{x \in M_a \mid \text{if } x > a \text{ then } x - 1 \in M_a\}$.
Since $a > a$ is false, the statement if $a > a$ then $a - 1 \in M_a$ is true.
Let $x \in \mathbb{R}$.
    Assume $x \in A$.
        Assume $x + 1 > a$.
            Since $x \in A$, we have $x \in M_a$; hence $(x + 1) - 1 \in M_a$.
        Therefore, if $x + 1 > a$ then $(x + 1) - 1 \in M_a$.
        Therefore, $x + 1 \in A$.
    Therefore, if $x \in A$ then $x + 1 \in A$.
Hence, A is inductive.
It then follows from the definition of M_a, that $M_a \subseteq A$.
Therefore, $\forall x \in M_a$, if $x > a$ then $x - 1 \in M_a$. □

Notice the similarity between the next example and theorem 1.2.3.

Proposition 1.2.26.

Let $a \in \mathbb{R}$, and let M_a be the smallest inductive set containing a. Then, $\forall x, y \in M_a$, if $y < x$ then $y + 1 \leq x$.

Proof.
Let $a \in \mathbb{R}$, and let M_a be the smallest inductive set containing a.
Let $A = \{x \in M_a \mid \forall y \in M_a,$ if $y < x$ then $y + 1 \leq x\}$.
Let $y \in M_a$.
Suppose $y < a$ and $a < y + 1$.
By proposition 1.2.24, since $y \in M_a$, we have $a \leq y$.
Hence, we have the contradiction $y < a$ and $a \leq y$.
Therefore, if $y < a$ then $y + 1 \leq a$.
Therefore, $a \in A$.
Let $x \in \mathbb{R}$, and assume $x \in A$.
Let $y \in M_a$.
Assume $y < x + 1$.
In the case where $y = a$, we have by proposition 1.2.24 that $y \leq x$; hence $y + 1 \leq x + 1$.
In the case where $y \neq a$, we have that $a < y$; hence by the proposition 1.2.25, $y - 1 \in M_a$.
Since $y - 1 < x$ and $x \in A$, we then have $(y - 1) + 1 \leq x$.
Therefore, $y \leq x$; hence $y + 1 \leq x + 1$.
Therefore, if $y < x + 1$ then $y + 1 \leq x + 1$.
Hence $x + 1 \in A$.
Therefore, A is inductive.
Therefore, $M_a \subseteq A$.
Therefore, $\forall x, y \in M_a$, if $y < x$ then $y + 1 \leq x$. □

The following theorem shows that for any $a \in \mathbb{R}$, the smallest inductive set containing a satisfies the well-ordering property.

Theorem 1.2.27.

Let $a \in \mathbb{R}$, and let M_a be the smallest inductive set containing a. Then, if $S \subseteq M_a$ with $S \neq \emptyset$, then S has a smallest element. That is, $\exists c \in S, \forall x \in S, c \leq x$.

Proof.
Let $a \in \mathbb{R}$, and let M_a be the smallest inductive set containing a.
Assume $S \subseteq M_a$, with $S \neq \emptyset$.
Further, assume that S does not have a smallest element.
Let $A = \{c \in M_a \mid \forall x \in S,\ c \leq x\}$.
We claim that $a \in A$.
Indeed, let $x \in S$. Then $x \in M_a$, since $S \subseteq M_a$.
Therefore, $a \leq x$.
Therefore, $\forall x \in S, a \leq x$.
Therefore, $a \in A$.
Next, we claim that A is inductive.
Indeed, let $c \in A$.
Then $c \in M_a$; hence $c + 1 \in M_a$.
Let $x \in S$.
Then $c \leq x$.
Since S does not have a smallest element, we have $c \notin S$.
Hence, $c \neq x$.
Therefore, $c < x$; hence $c + 1 \leq x$.
Therefore, $\forall x \in S, c + 1 \leq x$.
Hence, $c + 1 \in A$.
Therefore, A is inductive.
Since $a \in A$ and A is inductive, we have $M_a \subseteq A$.
Since $S \neq \emptyset$, we have $\exists c \in M_a, c \in S$.
Since $c \in M_a$ and $M_a \subseteq A$, we have $c \in A$.
Therefore, $\forall x \in S, c \leq x$.
This is a contradiction, since $c \in S$, and S does not have a smallest element.
Therefore, if $S \subseteq M_a$ with $S \neq \emptyset$, then S has a smallest element. □

In fact, the inductive subsets of the real numbers provide an alternate construction of the integers. One can define the natural numbers to be M_1, the smallest inductive subset of $\mathbb{R}$ containing 1, and the integers to be $\{x \in \mathbb{R} \mid \exists m, n \in M_1,\ x = m - n\}$. Indeed, all of the defining axioms of the integers can be proven using this definition. The last axiom, the well-ordering property, was done above.

The Principle of Complete Induction

An objection that one might have to the principle of mathematical induction is that the one doing the counting has a very short memory. In only using the fact that $n \in A$ to prove $n + 1 \in A$, one forgets that all of the numbers from 1 through n have already been counted among the elements of A. In fact, in applying the counting process in the principle of mathematical induction, one does not know that $n \in A$ until having already established that $\{1, \ldots, n\} \subseteq A$. This information may be useful if we wish to prove that $n + 1 \in A$, and it does not need to be forgotten.

Notation

$\{1, \ldots, n\}$ means $\{k \in \mathbb{N} \mid k \leq n\}$.

We suggest a version of the principle of mathematical induction with a better memory: To prove that $n + 1 \in A$, we do not merely assume $n \in A$ but rather that $\{1, \ldots, n\} \subseteq A$. The statement of the principle of complete induction is as follows:

The Principle of Complete Induction

Let A be a set. If $1 \in A$ and $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$, then $\mathbb{N} \subseteq A$.

Using the well-ordering property, the proof of the principle of complete induction is very similar to that of the principle of mathematical induction.

Theorem 1.2.28 (The Principle of Complete Induction)**.**

Let A be a set. If $1 \in A$ and $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$, then $\mathbb{N} \subseteq A$.

Proof.
Let A be a set.
Assume $1 \in A$ and $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$.
    Suppose $\mathbb{N} \not\subseteq A$; hence $\exists x \in \mathbb{N}$, $x \notin A$.
        Let $S = \{x \in \mathbb{N} \mid x \notin A\}$. By our assumption, $S \neq \emptyset$.
            Since $S \subseteq \mathbb{N}$, we have that S is bounded below by 0.
        By the well-ordering property, $\exists a \in S$, $\forall x \in S$, $a \leq x$.
        Choose such an a.
        Since $a \in \mathbb{N}$, we have $a > 0$; hence $a \geq 1$.
        Further, since $1 \in A$, we have $1 \notin S$. Therefore, $a \neq 1$.
        Therefore, $a > 1$.
        Choose $n = a - 1$.
            We then have $n > 0$; hence $n \in \mathbb{N}$.
            Since $n + 1 = a$ and $a \notin A$, we have $n + 1 \notin A$.
            Therefore, $\{1, \ldots, n\} \not\subseteq A$.
            Therefore, $\exists x \in \mathbb{N}$, $x \in \{1, \ldots, n\}$ and $x \notin A$.
            For such an x, we have $x \in S$ and $x \leq n$.
            Since $n = a - 1$, we have $x < a$.
        Therefore, $\exists x \in S$, $x < a$
        This is a contradiction, since a is the smallest element of S.
    Therefore, $\mathbb{N} \subseteq A$.
Therefore, if $1 \in A$ and $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \in A$ then $n + 1 \in A$, then $\mathbb{N} \subseteq A$. □

Proofs Using the Principle of Complete Induction

Proofs using the principle of complete induction are very similar to those using the principle of mathematical induction. In both cases we define the set A as the set of all natural numbers for which the statement we are proving is true. In both cases we must demonstrate that $1 \in A$. The difference is in the inductive step. When using the principle of mathematical induction, we must prove the statement

$$\forall n \in \mathbb{N}, \text{ if } n \in A, \text{ then } n + 1 \in A.$$

When using the principle of complete induction, we prove the statement

$$\forall n \in \mathbb{N}, \text{ if } \{1, \ldots, n\} \subseteq A, \text{ then } n + 1 \in A.$$

The general form of a proof using the principle of complete induction is as follows:

Proof of $\forall x \in \mathbb{N}$, $P(x)$.

Proof.
Define A ▶ Let $A = \{x \in \mathbb{N} \mid P(x)\}$.
⋮
Demonstration
Demonstrate that $1 \in A$.
⋮
Therefore $1 \in A$.
Arbitrary element ▶ Let $n \in \mathbb{N}$.
Assumption ▶ Assume $\{1, \ldots, n\} \subseteq A$.
⋮
Demonstration
Demonstrate that $n + 1 \in A$.
⋮
Conclusion ▶ Therefore, $n + 1 \in A$.
Conclusion ▶ Therefore, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$.
Now, $1 \in A$ and $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$.
Apply PCI ▶ By the principle of complete induction, $\mathbb{N} \subseteq A$.
Therefore, $\forall x \in \mathbb{N}$, $x \in A$.
Conclusion ▶ Therefore, $\forall x \in \mathbb{N}$, $P(x)$. □

We demonstrate this technique by proving the following two properties of the natural numbers:

Proposition 1.2.29.

$\forall x \in \mathbb{N}, \exists m, y \in \mathbb{N}, x = 2^{m-1}(2y-1)$.

Proof.
Let $A = \{x \in \mathbb{N} \mid \exists m, y \in \mathbb{N},\ x = 2^{m-1}(2y-1)\}$.
Choose $m = 1$ and $y = 1$.
$1 = 2^0(2(1)-1) = 2^{m-1}(2y-1)$.
Therefore, $\exists m, y \in \mathbb{N}, 1 = 2^{m-1}(2y-1)$.
Hence, $1 \in A$.
Let $n \in \mathbb{N}$.
Assume $\{1, \ldots, n\} \subseteq A$.
$n+1$ is either even or odd, and we consider these possibilities in cases.
Case 1: $n+1$ is even.
The $\exists x \in \mathbb{N}, n+1 = 2x$.
Since $1 < 2$, we have $x < 2x$; hence $x < n+1$.
Therefore, $x \leq n$; hence $x \in \{1, \ldots, n\}$.
We then have that $x \in A$.
Therefore, $\exists k, y \in \mathbb{N}, x = 2^{k-1}(2y-1)$. Choose such k, y.
Choose $m = k+1$.
Then $n+1 = 2(2^{k-1})(2y-1) = 2^{m-1}(2y-1)$.
Therefore, $\exists m, y \in \mathbb{N}, n+1 = 2^{m-1}(2y-1)$.
Therefore, $n+1 \in A$.
Case 2: $n+1$ is odd.
Hence $\exists z \in \mathbb{N}, n+1 = 2z+1$.
Choose $m = 1$ and $y = z+1$.
$n+1 = 2z+1 = 2(y-1)+1 = 2y-1 = 2^0(2y-1) = 2^{m-1}(2y-1)$.
Therefore, $\exists m, y \in \mathbb{N}, n+1 = 2^{m-1}(2y-1)$.
Therefore, $n+1 \in A$.
In both cases, $n+1 \in A$.
Therefore, if $\{1, \ldots, n\} \subseteq A$, then $n+1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$, then $n+1 \in A$.
We now have $1 \in A$ and $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$, then $n+1 \in A$.
By the principle of complete induction, $\mathbb{N} \subseteq A$.
Therefore, $\forall x \in \mathbb{N}, \exists m, y \in \mathbb{N}, x = 2^{m-1}(2y-1)$. □

In our next example, we prove that every natural number other than 1 has a prime factor. However, since we have not yet seen any examples dealing with prime numbers, we will need define what it means for a natural number to be prime. The definition of a prime number that we will use is as follows:

Definition 1.2.10. Let $x \in \mathbb{N}$. x is prime means $x \neq 1$ and $\forall a, b \in \mathbb{N}$, if $x = ab$ then either $a = 1$ or $b = 1$.

Proposition 1.2.30.

$\forall x \in \mathbb{N}$, either $x = 1$ or $\exists p \in \mathbb{N}$, p is prime and p divides x.

Proof.
Let $A = \{x \in \mathbb{N} \mid \text{either } x = 1 \text{ or } \exists p \in \mathbb{N},\ p \text{ is prime and } p \text{ divides } x\}$.
$1 \in A$ is given explicitly in the definition of A.
Let $n \in \mathbb{N}$.
    Assume $\{1, \ldots, n\} \subseteq A$.
        Either $n + 1$ is prime or it is not.
        Case 1: $n + 1$ is prime.
            Choosing $p = n + 1$ gives us that p is prime and p divides $n + 1$.
            Therefore, $\exists p \in \mathbb{N}$, p is prime and p divides $n + 1$.
            Therefore, $n + 1 \in A$.
        Case 2: $n + 1$ is not prime.
            Therefore, $\exists a, b \in \mathbb{N}$, $n + 1 = ab$ and neither a nor b is equal to 1.
            Since $a \neq 1$, we have $a > 1$, hence $ab > b$.
            Therefore, $b < n + 1$, which then gives us $b \leq n$.
            Therefore, $b \in \{1, \ldots, n\}$; hence $b \in A$.
            Since $b \neq 1$, this means $\exists p \in \mathbb{N}$, p is prime and p divides b.
            Choosing such a p, since p divides b, we have $\exists t \in \mathbb{N}$, $b = tp$.
            Therefore, $n + 1 = (at)p$; hence p divides $n + 1$.
            Therefore, $\exists p \in \mathbb{N}$, p is prime and p divides $n + 1$.
            Therefore, $n + 1 \in A$.
        In both cases, we have $n + 1 \in A$.
    Therefore, if $\{1, \ldots, n\} \subseteq A$, then $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$, then $n + 1 \in A$.
We now have $1 \in A$ and $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$, then $n + 1 \in A$.
By the principle of complete induction, $\mathbb{N} \subseteq A$.
Therefore, $\forall x \in \mathbb{N}$, either $x = 1$ or $\exists p \in \mathbb{N}$, p is prime and p divides x. □

Recursive Definitions

There are many mathematical concepts that one comes to understand only by an inductive process. For example, when we first come to understand the concept of exponents, we identify x^1 as x, x^2 as $(x)x$, x^3 as $((x)x)x = (x^2)x$, and so on. The idea is known through a repetition of the operation of multiplication, where the exponent is a count of how many times the multiplication has been repeated. In a similar way, we can view multiplication (in the natural numbers) as repeated addition and division with remainder as repeated subtraction. The defining of concepts by a process of repetition (or recursion) can be made precise in a way that makes these definitions useable in formal proofs. We will explore several such definitions and show how they can be used in a proof.

Definition 1.2.11. For $x \in \mathbb{R}$, define $x^1 = x$ and for each $n \in \mathbb{N}$, define $x^{n+1} = (x^n)x$.

Note that we need not begin with the exponent 1. A compatible definition can be given in the case where $x \neq 0$, by defining $x^0 = 1$ and for each $n \in \mathbb{Z}_{\geq 0}$, $x^{n+1} = (x^n)x$. This is indeed compatible with the definition above since $x^1 = (x^0)x = (1)x = x$. Using this recursive definition, we will prove some well known properties of exponents.

Proposition 1.2.31.

$\forall x, y \in \mathbb{R}, \forall n \in \mathbb{N}, (xy)^n = x^n y^n$.

Proof.
Let $x, y \in \mathbb{R}$.
  Let $A = \{n \in \mathbb{N} \mid (xy)^n = x^n y^n\}$.
  Since $(xy)^1 = xy = x^1 y^1$, we have $1 \in A$.
  Let $n \in \mathbb{N}$.
    Assume $n \in A$.
      Then $(xy)^n = x^n y^n$.
      Now, $(xy)^{n+1} = (xy)^n xy = x^n y^n xy = (x^n)x(y^n)y = x^{n+1}y^{n+1}$.
      Hence, $n + 1 \in A$.
    Therefore, if $n \in A$ then $n + 1 \in A$.
  Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
  By the PMI, $\mathbb{N} \subseteq A$.
  Therefore, $\forall n \in \mathbb{N}, (xy)^n = x^n y^n$.
Therefore, $\forall x, y \in \mathbb{R}, \forall n \in \mathbb{N}, (xy)^n = x^n y^n$. □

Proposition 1.2.32.

$\forall x \in \mathbb{R}, \forall m, n \in \mathbb{N}, x^{m+n} = x^m x^n$.

Proof.
Let $x \in \mathbb{R}$.
  Let $A = \{n \in \mathbb{N} \mid \forall m \in \mathbb{N},\ x^{m+n} = x^m x^n\}$.
  Let $m \in \mathbb{N}$.
    Then $x^{m+1} = (x^m)x = x^m x^1$.
  Therefore, $\forall m \in \mathbb{N}, x^{m+1} = x^m x^1$.
  Therefore, $1 \in A$.
  Let $n \in \mathbb{N}$.
    Assume $n \in A$.
      Let $m \in \mathbb{N}$.
        Then $x^{m+n} = x^m x^n$.
        $x^{m+(n+1)} = x^{(m+n)+1} = (x^{m+n})x = x^m x^n x = x^m x^{n+1}$.
      Therefore, $\forall m \in \mathbb{N}, x^{m+(n+1)} = x^m x^{n+1}$.
      Hence, $n + 1 \in A$.
    Therefore, if $n \in A$ then $n + 1 \in A$.
  Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
  By the PMI, $\mathbb{N} \subseteq A$.
  Therefore, $\forall n \in \mathbb{N}, \forall m \in \mathbb{N}, x^{m+n} = x^m x^n$.
Therefore, $\forall x \in \mathbb{R}, \forall m, n \in \mathbb{N}, x^{m+n} = x^m x^n$. □

When giving a recursive definition, we are essentially describing a pattern that repeats indefinitely. We can make this idea yet more precise by introducing the notion of a **sequence**. Consider, for example, the pattern $1, 4, 9, 16, 25, 36, 49, \ldots$. If one recognizes this pattern, he or she will most likely infer that the next term in the pattern is 64, even though it has not been stated explicitly. However, our purpose throughout the course has been to remove all ambiguity and all dependence on the reader's intuition. To grasp the meaning of the notation $1, 4, 9, 16, 25, 36, 49, \ldots$, our reader must have some mathematical intuition to recognize the pattern, hence this notation is not precise enough for our purposes. A better way to describe this pattern is as the *sequence* $(k^2)_{k\in\mathbb{N}}$. In general, a sequence $(a_k)_{k\in\mathbb{N}}$ is a *correspondence* between the natural numbers $\mathbb{N}$ and the universe of discourse to which the terms of the sequence a_k belong. For us, this universe of discourse will usually be $\mathbb{R}$ or $\mathbb{Z}$. By *correspondence*, we mean that to each $k \in \mathbb{N}$ corresponds a *term* a_k. In our example, the *sequence* $(k^2)_{k\in\mathbb{N}}$ is the correspondence $k \mapsto k^2$. That is, to each $k \in \mathbb{N}$ corresponds the term k^2. We then know explicitly that the first term is $1^2 = 1$, the second term is $2^2 = 4$, and so on. Alternatively, one can view a *sequence* of say real numbers $(a_k)_{k\in\mathbb{N}}$ as a function $f : \mathbb{N} \to \mathbb{R}$, given by $f(k) = a_k$.

The concept of a **series** is very closely related to idea of sequences. A *series* is the accumulation of the terms of a sequence. For an example of what this means, imagine that a person deposits a certain amount of money into her bank account each week. Another way to say this is that to each week corresponds an amount of money she deposits. This can be viewed as a *sequence* $(a_k)_{k\in\mathbb{N}}$, where for each $k \in \mathbb{N}$, a_k represents the amount of money deposited in week k. Since this money will accumulate in her bank account, we can imagine another related sequence: That of her account balance in week k. This accumulation of the sequence $(a_k)_{k\in\mathbb{N}}$ is what we call a *series*. In this example, the first term in the series will be a_1, the second term will be $a_1 + a_2$, the third $a_1 + a_2 + a_3$, and so on. We make this idea precise by giving the following recursive definition:

Definition 1.2.12. For a sequence of real numbers $(a_k)_{k\in\mathbb{N}}$, define

$$\sum_{k=1}^{1} a_k = a_1,$$

and for each $n \in \mathbb{N}$, define

$$\sum_{k=1}^{n+1} a_k = \left(\sum_{k=1}^{n} a_k\right) + a_{n+1}.$$

Consider, as an example, the sum of all consecutive numbers from 1 to a certain ending point n. Although it may seem like the expression $1+2+3+\cdots+n$ is sufficient to express the idea of the sum of all consecutive numbers from 1 to n, it contains a flaw that the expression $\sum_{k=1}^{n} k$ does not: The dots are not categorically defined. That is, the dots '...' in $1+2+3+\cdots+n$ tell the reader that the observed pattern seen in the beginning $1+2+3$ is to continue until the ending point n. This leaves the recognition of the pattern to the reader's own intuition. Since the pattern is not given explicitly, the meaning of the dots is open to interpretation. In fact, there are many different patterns beginning with $1+2+3$: The reader may wish to verify that the first three terms of the sequence $(n^3-6n^2+12n-6)_{n\in\mathbb{N}}$ are 1, 2, and 3. Thus the expression $1+2+3+\cdots+n$, although it may seem clear enough in what it seeks to represent, depends on the reader for interpretation and hence does not have the precision required to be useable in a mathematical proof. On the other hand, the expression $\sum_{k=1}^{n} k$ is defined precisely and, provided the reader follows the definition with care, it can be interpreted in only one way.

The starting point of $k=1$ in the sum is somewhat arbitrary. One often sees sums starting at $k=0$, or other integers. To extend this definition to allow for other starting points, we need only a slight modification. First, we must allow sequences $(a_k)_{k\in\mathbb{Z}}$ indexed by the integers $\mathbb{Z}$ rather than the natural numbers $\mathbb{N}$. That is, the sequence $(a_k)_{k\in\mathbb{Z}}$ gives a correspondence between the *integers* $\mathbb{Z}$ and the universe of discourse to which the terms a_k belong. In fact, we can allow sequences to be indexed by other subsets of the integers as well. For example, the sequence $(3k+1)_{k\in\mathbb{Z}_{\geq -2}}$ gives a correspondence between the integers k that are greater than or equal to -2 and the terms $3k+1$. This sequence describes the pattern $-5,-2,1,4,7,10,13,\ldots$. Next, we must modify the definition of a *series* as follows:

Definition 1.2.13. Let $m\in\mathbb{Z}$. For a sequence of real numbers $(a_k)_{k\in\mathbb{Z}_{\geq m}}$, define

$$\sum_{k=m}^{m} a_k = a_m,$$

and for each $n\in\mathbb{Z}_{\geq m}$, define

$$\sum_{k=m}^{n+1} a_k = \left(\sum_{k=m}^{n} a_k\right) + a_{n+1}.$$

In fact, we can express a sum using any starting point, provided we alter the summand a_k accordingly. As a simple example of this, consider how one might express a sum beginning from $k=0$ as a sum beginning from $k=1$:

Proposition 1.2.33.

For a sequence of real numbers $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$, $\forall n \in \mathbb{Z}_{\geq 0}$, $\displaystyle\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1}$.

Proof.
Let $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$ be a sequence of real numbers.
Let $A = \left\{ x \in \mathbb{Z}_{\geq 0} \;\middle|\; \displaystyle\sum_{k=0}^{x} a_k = \sum_{k=1}^{x+1} a_{k-1} \right\}$
Since $\displaystyle\sum_{k=0}^{0} a_k = a_0 = a_{1-1} = \sum_{k=1}^{1} a_{k-1}$, we have that $0 \in A$.
Let $n \in \mathbb{Z}_{\geq 0}$.
Assume $n \in A$.
Then $\displaystyle\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1}$.

$$\begin{aligned}\sum_{k=0}^{n+1} a_k &= \left(\sum_{k=0}^{n} a_k\right) + a_{n+1} \\ &= \left(\sum_{k=1}^{n+1} a_{k-1}\right) + a_{n+1} \\ &= \left(\sum_{k=1}^{n+1} a_{k-1}\right) + a_{(n+2)-1} \\ &= \sum_{k=1}^{n+2} a_{k-1}.\end{aligned}$$

Therefore, $\displaystyle\sum_{k=0}^{n+1} a_k = \sum_{k=1}^{(n+1)+1} a_{k-1}$; hence $n+1 \in A$.
Therefore, if $n \in A$ then $n+1 \in A$.
Therefore, $\forall n \in \mathbb{Z}_{\geq 0}$, if $n \in A$ then $n+1 \in A$.
By the principle of mathematical induction, we have $\mathbb{Z}_{\geq 0} \subseteq A$.
Therefore, $\forall n \in \mathbb{Z}_{\geq 0}$, $\displaystyle\sum_{k=0}^{n} a_k = \sum_{k=1}^{n+1} a_{k-1}$. □

We see then that by increasing the range of the index by 1; which is to say by changing the range from $\{0, 1, \ldots, n\}$ to $\{1, 2, \ldots, n+1\}$, we need only compensate by decreasing the index in the summand by 1. That is, by changing the summand from a_k to a_{k-1}. In this case, the resulting sum is unchanged. This principle can be generalized quite easily to allow us to choose any starting point for our sum. Here is the general result:

Proposition 1.2.34.

For a sequence of real numbers $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$, $\forall m \in \mathbb{Z}$, $\forall n \in \mathbb{Z}_{\geq 0}$, $\displaystyle\sum_{k=0}^{n} a_k = \sum_{k=m}^{n+m} a_{k-m}$.

Proof.
Let $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$ be a sequence of real numbers.
Let $m \in \mathbb{Z}$.

Let $A = \left\{ x \in \mathbb{Z}_{\geq 0} \;\middle|\; \displaystyle\sum_{k=0}^{x} a_k = \sum_{k=m}^{x+m} a_{k-m} \right\}$

Since $\displaystyle\sum_{k=0}^{0} a_k = a_0 = a_{m-m} = \sum_{k=m}^{m} a_{k-m}$, we have that $0 \in A$.

Let $n \in \mathbb{Z}_{\geq 0}$.

Assume $n \in A$.

Then $\displaystyle\sum_{k=0}^{n} a_k = \sum_{k=m}^{n+m} a_{k-m}$.

$$\begin{aligned}\sum_{k=0}^{n+1} a_k &= \left(\sum_{k=0}^{n} a_k\right) + a_{n+1} \\ &= \left(\sum_{k=m}^{n+m} a_{k-m}\right) + a_{n+1} \\ &= \left(\sum_{k=m}^{n+m} a_{k-m}\right) + a_{(n+1+m)-m} \\ &= \sum_{k=m}^{n+1+m} a_{k-m}.\end{aligned}$$

Therefore, $\displaystyle\sum_{k=0}^{n+1} a_k = \sum_{k=m}^{(n+1)+m} a_{k-m}$; hence $n+1 \in A$.

Therefore, if $n \in A$ then $n+1 \in A$.

Therefore, $\forall n \in \mathbb{Z}_{\geq 0}$, if $n \in A$ then $n+1 \in A$.

By the principle of mathematical induction, we have $\mathbb{Z}_{\geq 0} \subseteq A$.

Therefore, $\forall n \in \mathbb{Z}_{\geq 0}$, $\displaystyle\sum_{k=0}^{n} a_k = \sum_{k=m}^{n+m} a_{k-m}$.

Therefore, $\forall m \in \mathbb{Z}$, $\forall n \in \mathbb{Z}_{\geq 0}$, $\displaystyle\sum_{k=0}^{n} a_k = \sum_{k=m}^{n+m} a_{k-m}$. □

Although sums are defined recursively, it is occasionally possible to find explicit formulas for certain sums. As an example, consider the problem of summing all consecutive natural numbers up to a certain number n. That is, consider the sum $1 + 2 + 3 + \cdots + n$, or more precisely: $\sum_{k=1}^{n} k$. An interesting observation can be made if we add this sum to itself in reverse order.

$$\begin{array}{cccccccccccc} & 1 & + & 2 & + & 3 & + & \ldots & + & (n-1) & + & n \\ + & n & + & (n-1) & + & (n-2) & + & \ldots & + & 2 & + & 1 \\ \hline & (n+1) & + & (n+1) & + & (n+1) & + & \ldots & + & (n+1) & + & (n+1) \end{array}$$

Note that each column adds to $n + 1$. Counting that there are n such columns gives us that the total of the two sums added together is $n(n+1)$. It then follows that $2\left(\sum_{k=1}^{n} k\right) = n(n+1)$; hence

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Although this argument may seem convincing enough, we should note that it relies on the reader's intuition in several places. First, as mentioned earlier, the expression $1 + 2 + 3 + \cdots + n$ relies on the reader's interpretation of the pattern beginning with 1, 2, and 3, to give meaning to the symbol '...'. Further, the argument that every column adds to $n + 1$ is only explicitly demonstrated for the first three columns and the last two columns. We then rely on the hope that our reader guesses the same pattern will continue. The intuition may be reasonable and correct that this pattern of $n + 1$ resulting in each column will continue. However, the reasoning involves more than just the definitions of the terms involved; hence this argument does not have the strength required of a mathematical demonstration. For a proper proof of this formula, we must turn to the recursive definition of the sum. The proof is as follows:

Proposition 1.2.35.

$\forall n \in \mathbb{N}, \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Proof.
Let $A = \left\{ x \in \mathbb{N} \;\middle|\; \sum_{k=1}^{x} k = \frac{x(x+1)}{2} \right\}$
$\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}$.
Therefore, $1 \in A$.
Let $n \in \mathbb{N}$.
Assume $n \in A$.
Then $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

$$\begin{aligned}\sum_{k=1}^{n+1} k &= \left(\sum_{k=1}^{n} k\right) + (n+1) \\ &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

Therefore, $n + 1 \in A$.
Therefore, if $n \in A$ then $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
By the PMI, $\mathbb{N} \subseteq A$.
Therefore, $\forall n \in \mathbb{N}, \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. □

An interesting application of explicit formulas for sums is to investigate the paradoxes of Zeno. In one such paradox, Zeno argues that for an object in motion to travel a certain distance, it must first travel half of that distance. To then travel the remaining distance, it must travel half of this remaining distance, and so on. Since the distance traveled by the object can be so divided into an infinite sequence of shorter distances, the object must traverse an infinite number of distances in order to reach its destination. Since admitting the possibility of completing an infinite number of tasks is not desirable, Zeno suggests that the completion of the journey is impossible. Further, since the total distance that the object had intended to travel was arbitrary, this suggests that no journey of any distance can be completed; hence motion is impossible. However, since it is abundantly evident that motion is possible, this is a paradox [2]. Zeno's paradoxes suggest a discrepancy between what we observe motion to be and one of the ways in which we reason about motion.

In addition to the philosophical challenges of Zeno's dichotomy paradox, the argument also presents some interesting mathematical ideas that are worth investigating. Suppose, with Zeno, that an object is to travel a certain distance. Since the units of measurement for distance can be arbitrarily assigned, we may assume without loss of generality that the object's intended distance is 1 unit. At the first stage of the journey, Zeno allows the object to travel a distance of $\frac{1}{2}$. At the second stage, it is allowed to travel an additional distance of $\frac{1}{4}$, bringing its total distance to $\frac{1}{2} + \frac{1}{4}$. In general, we have that the distance traveled after the n^{th} stage in Zeno's sequence is

$$\sum_{k=1}^{n} \frac{1}{2^k}.$$

There is in fact an explicit formula for this sum, which is given in the following proposition:

Proposition 1.2.36.

$\forall n \in \mathbb{N}, \sum_{k=1}^{n} \frac{1}{2^k} = 1 - \frac{1}{2^n}.$

Proof.
Let $A = \left\{ x \in \mathbb{N} \;\middle|\; \sum_{k=1}^{x} \frac{1}{2^k} = 1 - \frac{1}{2^x} \right\}$
$\sum_{k=1}^{1} \frac{1}{2^k} = \frac{1}{2} = 1 - \frac{1}{2^1}.$
Therefore, $1 \in A$.
Let $n \in \mathbb{N}$.
Assume $n \in A$.
Then $\sum_{k=1}^{n} \frac{1}{2^k} = 1 - \frac{1}{2^n}.$

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{2^k} &= \left(\sum_{k=1}^{n} \frac{1}{2^k} \right) + \frac{1}{2^{n+1}} \\
&= 1 - \frac{1}{2^n} + \frac{1}{2^{n+1}} \\
&= 1 - \left(\frac{1}{2^n} - \frac{1}{2^{n+1}} \right) \\
&= 1 - \frac{2-1}{2^{n+1}} \\
&= 1 - \frac{1}{2^{n+1}}.
\end{aligned}$$

Hence, $n + 1 \in A$.
Therefore, if $n \in A$ then $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
By the PMI, $\mathbb{N} \subseteq A$.
Therefore, $\forall n \in \mathbb{N}, \sum_{k=1}^{n} \frac{1}{2^k} = 1 - \frac{1}{2^n}.$ □

We may be able to shed some more light on Zeno's dichotomy paradox if we recall two earlier propositions. The first was given as an early example of a proof by induction: Proposition 1.2.20 tells us that $\forall n \in \mathbb{N}$, $n < 2^n$. This means that for all natural numbers n, $\frac{1}{2^n} < \frac{1}{n}$. Next, recall that the Archimedean property gives us that for any $\varepsilon \in \mathbb{R}$ with $\varepsilon > 0$, there exists a natural number n for which $\frac{1}{n} < \varepsilon$. The combination of these two propositions with the formula above yields the following:

Proposition 1.2.37.

$\forall \varepsilon > 0, \exists n \in \mathbb{N}, 1 - \sum_{k=1}^{n} \frac{1}{2^k} < \varepsilon.$

Proof.
Let $\varepsilon > 0$.
By the Archimedean property, $\exists n \in \mathbb{N}, \frac{1}{n} < \varepsilon$. Choose such an n.
By proposition 1.2.20, $n < 2^n$.
Therefore, $\frac{1}{2^n} < \frac{1}{n}$.
Since we also have $\frac{1}{n} < \varepsilon$, by transitivity $\frac{1}{2^n} < \varepsilon$.
Since $1 - \sum_{k=1}^{n} \frac{1}{2^k} = 1 - \left(1 - \frac{1}{2^n}\right) = \frac{1}{2^n}$,
We have $1 - \sum_{k=1}^{n} \frac{1}{2^k} < \varepsilon$.
Therefore, $\exists n \in \mathbb{N}, 1 - \sum_{k=1}^{n} \frac{1}{2^k} < \varepsilon$.
Therefore, $\forall \varepsilon > 0, \exists n \in \mathbb{N}, 1 - \sum_{k=1}^{n} \frac{1}{2^k} < \varepsilon$. □

The significance of this result can be seen if we appeal to an earlier result about real numbers. Proposition 1.1.14 tells us $\forall a, b \in \mathbb{R}$, if $\forall x > a$, $b \leq x$, then $b \leq a$. Choosing $a = 0$ and replacing the arbitrary variable x with ε, this proposition reads

$\forall b \in \mathbb{R}$, if $\forall \varepsilon > 0$, $b \leq \varepsilon$, then $b \leq 0$.

Suppose the actual distance traveled by Zeno's object is d units. Since the question of whether the object does or does not complete its total journey of 1 unit is open for debate, all that can be said is that $d \leq 1$. Further, for any $n \in \mathbb{N}$ the distance d cannot be less than the distance traveled at the n^{th} stage. That is, $\forall n \in \mathbb{N}, \sum_{k=1}^{n} \frac{1}{2^k} \leq d$; hence $\forall n \in \mathbb{N}$, $1 - d \leq 1 - \sum_{k=1}^{n} \frac{1}{2^k}$. Thus, for any $\varepsilon > 0$, since there is an $n \in \mathbb{N}$ with $1 - \sum_{k=1}^{n} \frac{1}{2^k} < \varepsilon$, we then have $1 - d < \varepsilon$. Therefore, $\forall \varepsilon > 0$, $1 - d \leq \varepsilon$. By proposition 1.1.14, we then have $1 - d \leq 0$; hence $1 \leq d$. Since $d \leq 1$ and $1 \leq d$, we must have $d = 1$ by trichotomy.

Although this analysis does not address all of the philosophical challenges presented by Zeno's paradox, it does provide the foundation for a proper and rigorous study of infinite sums. Such a study is now indispensable to modern math and physics.

The reduction of the sum to an explicit formula in the example above is a special case of a more general result concerning the sum of all powers of a given constant:

Proposition 1.2.38.

For all $a \in \mathbb{R}$, if $a \neq 1$ then $\sum_{k=1}^{n} a^k = \frac{a - a^{n+1}}{1 - a}$.

Proof.
Let $a \in \mathbb{R}$, and assume $a \neq 1$.
Let $A = \left\{ x \in \mathbb{N} \;\middle|\; \sum_{k=1}^{x} a^k = \frac{a - a^{n+1}}{1 - a} \right\}$
$\sum_{k=1}^{1} a^k = a = a\left(\frac{1 - a}{1 - a}\right) = \frac{a - a^{1+1}}{1 - a}$.
Therefore, $1 \in A$.
Let $n \in \mathbb{N}$.
Assume $n \in A$.
Then $\sum_{k=1}^{n} a^k = \frac{a - a^{n+1}}{1 - a}$.

$$\begin{aligned}
\sum_{k=1}^{n+1} a^k &= \left(\sum_{k=1}^{n} a^k\right) + a^{n+1} \\
&= \frac{a - a^{n+1}}{1 - a} + a^{n+1} \\
&= \frac{a - a^{n+1} + a^{n+1} - a^{n+2}}{1 - a} \\
&= \frac{a - a^{n+2}}{1 - a}.
\end{aligned}$$

Hence, $n + 1 \in A$.
Therefore, if $n \in A$ then $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.
By the PMI, $\mathbb{N} \subseteq A$.
Therefore, $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} a^k = \frac{a - a^{n+1}}{1 - a}$.
Therefore, $\forall a \in \mathbb{R}$, if $a \neq 1$ then $\sum_{k=1}^{n} a^k = \frac{a - a^{n+1}}{1 - a}$. □

This result can be made more general still:

Proposition 1.2.39.

For all $a, b \in \mathbb{R}$ and all $n \in \mathbb{N}$, $a^n - b^n = (a-b)\sum_{k=1}^{n} a^{n-k}b^{k-1}$.

Proof.
Let $a, b \in \mathbb{R}$.

Let $A = \left\{ x \in \mathbb{N} \;\middle|\; a^x - b^x = (a-b)\sum_{k=1}^{x} a^{x-k}b^{k-1} \right\}$

$a - b = (a-b)(1) = (a-b)(a^{1-1}b^{1-1}) = (a-b)\sum_{k=1}^{1} a^{1-k}b^{k-1}$.

Therefore, $1 \in A$.

Let $n \in \mathbb{N}$.

Assume $n \in A$.

Then $a^n - b^n = (a-b)\sum_{k=1}^{n} a^{n-k}b^{k-1}$.

$$\begin{aligned}
a^{n+1} - b^{n+1} &= a(a^n) - b(b^n) \\
&= a(a^n) - ab^n + ab^n - b(b^n) \\
&= a(a^n - b^n) + b^n(a-b) \\
&= a(a-b)\sum_{k=1}^{n} a^{n-k}b^{k-1} + b^n(a-b) \\
&= (a-b)\left(a\left(\sum_{k=1}^{n} a^{n-k}b^{k-1}\right) + b^n\right) \\
&= (a-b)\left(\left(\sum_{k=1}^{n} a^{n+1-k}b^{k-1}\right) + b^n\right) \\
&= (a-b)\left(\left(\sum_{k=1}^{n} a^{n+1-k}b^{k-1}\right) + a^{(n+1)-(n+1)}b^n\right) \\
&= (a-b)\sum_{k=1}^{n+1} a^{n+1-k}b^{k-1}.
\end{aligned}$$

Therefore, $n + 1 \in A$.

Therefore, if $n \in A$ then $n + 1 \in A$.

Therefore, $\forall n \in \mathbb{N}$, if $n \in A$ then $n + 1 \in A$.

By the PMI, $\mathbb{N} \subseteq A$.

Therefore, $\forall n \in \mathbb{N}$, $a^n - b^n = (a-b)\sum_{k=1}^{n} a^{n-k}b^{k-1}$.

Therefore, $\forall a, b \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $a^n - b^n = (a-b)\sum_{k=1}^{n} a^{n-k}b^{k-1}$. □

Definition 1.2.14. Define $0! = 1$, and for each $n \in \mathbb{N}$, define $n! = n(n-1)!$. Further, for $n, k \in \mathbb{N}$ with $n \geq k$, define the **binomial coefficient**

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

Proposition 1.2.40 (Pascal's Law)**.**

For all $n, k \in \mathbb{N}$ with $n > k$, $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

Proof.
Let $n, k \in \mathbb{N}$ with $n > k$.

The following calculation gives the desired result:

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \\
&= \frac{n!(k+1)}{(k+1)k!(n-k)!} + \frac{n!(n-k)}{(k+1)!(n-k)(n-k-1)!} \\
&= \frac{n!(k+1) + n!(n-k)}{(k+1)!(n-k)!} \\
&= \frac{n!(n+1)}{(k+1)!(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!(n+1-(k+1))!} \\
&= \binom{n+1}{k+1}
\end{aligned}$$

Therefore, $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

Therefore, for all $n, k \in \mathbb{N}$ with $n > k$, $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$. □

Proposition 1.2.41 (The Binomial Theorem)**.**

$\forall a, b \in \mathbb{R}$ with $a, b \neq 0$, $\forall n \in \mathbb{Z}_{\geq 0}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Proof.
Let $a, b \in \mathbb{R}$ with $a, b \neq 0$.

Let $A = \left\{ x \in \mathbb{N} \;\middle|\; (a+b)^x = \sum_{k=0}^{x} \binom{n}{k} a^k b^{x-k} \right\}$

$(a+b)^0 = 1 = \binom{0}{0} a^0 b^0 = \sum_{k=0}^{0} \binom{n}{k} a^k b^{0-k}$.

Therefore, $0 \in A$.

Let $n \in \mathbb{Z}_{\geq 0}$.

Assume $n \in A$.

Then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

$$
\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b) \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= a \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} + b \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \sum_{k=1}^{n+1} \binom{n}{k-1} a^k b^{n-(k-1)} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \left(\sum_{k=1}^{n} \binom{n}{k-1} a^k b^{n+1-k} \right) + a_{n+1} + b^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \binom{n+1}{0} b^{n+1} + \left(\sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k} \right) + \binom{n+1}{n+1} a^{n+1} \\
&= \binom{n+1}{0} b^{n+1} + \left(\sum_{k=1}^{n} \binom{n+1}{k} a^k b^{n+1-k} \right) + \binom{n+1}{n+1} a^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}
\end{aligned}
$$

Therefore, $n+1 \in A$.

Therefore, if $n \in A$ then $n+1 \in A$.

Therefore, $\forall n \in \mathbb{Z}_{\geq 0}$, if $n \in A$ then $n+1 \in A$.

By the PMI, $\mathbb{Z}_{\geq 0} \subseteq A$.

Therefore, $\forall n \in \mathbb{Z}_{\geq 0}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Therefore, $\forall a, b \in \mathbb{R}$ with $a, b \neq 0$, $\forall n \in \mathbb{Z}_{\geq 0}$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$. □

Definition 1.2.15. Define the **Fibonacci sequence** as follows: $f_1 = 1$, $f_2 = 1$, and for each $n \in \mathbb{N}$ with $n \geq 2$, $f_{n+1} = f_n + f_{n-1}$.

Proposition 1.2.42.

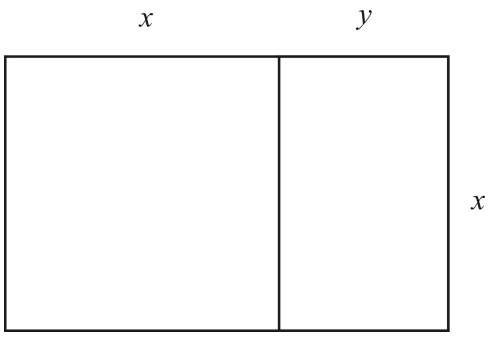
Let a and b be the two real solutions of the equation $x^2 = x + 1$. Then $\forall n \in \mathbb{N}$, $f_n = \frac{a^n - b^n}{a-b}$.

Proof.
Let a and b be the two real solutions of the equation $x^2 = x + 1$.
Let $A = \left\{ x \in \mathbb{N} \;\middle|\; f_x = \dfrac{a^x - b^x}{a-b} \right\}$
Since $\dfrac{a^1 - b^1}{a-b} = 1 = f_1$, we have $1 \in A$.
Let $n \in \mathbb{N}$.
Assume $\{1, \ldots, n\} \subseteq A$.
We consider the case $n = 1$ and the case $n \geq 2$.
Case 1: $n = 1$.
Then $\dfrac{a^{n+1} - b^{n+1}}{a-b} = \dfrac{a^2 - b^2}{a-b} = \dfrac{a + 1 - (b+1)}{a-b} = 1 = f_2 = f_{n+1}$.
Therefore, $n + 1 \in A$.
Case 2: $n \geq 2$.
Then $n - 1 \geq 1$.
We then have $n \in \{1, \ldots, n\}$ and $n - 1 \in \{1, \ldots, n\}$,
hence $n \in A$ and $n - 1 \in A$.
Therefore, $f_n = \dfrac{a^n - b^n}{a-b}$ and $f_{n-1} = \dfrac{a^{n-1} - b^{n-1}}{a-b}$.
We then have

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &= \frac{a^n - b^n}{a-b} + \frac{a^{n-1} - b^{n-1}}{a-b} \\ &= \frac{a^{n-1}(a+1) - b^{n-1}(b+1)}{a-b} \\ &= \frac{a^{n-1}a^2 - b^{n-1}b^2}{a-b} \\ &= \frac{a^{n+1} - b^{n+1}}{a-b} \end{aligned}$$

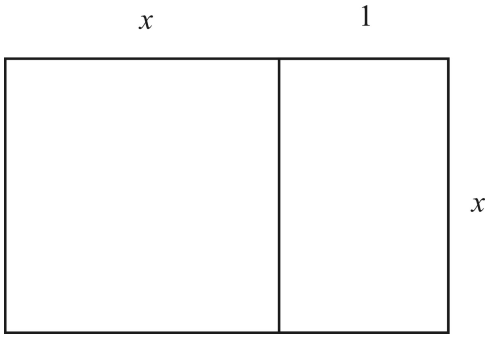
Therefore, $n + 1 \in A$.
In both cases, $n + 1 \in A$.
Therefore, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $\{1, \ldots, n\} \subseteq A$ then $n + 1 \in A$.
By the PCI, $\mathbb{N} \subseteq A$.
Therefore, $\forall n \in \mathbb{N}$, $f_n = \frac{a^n - b^n}{a-b}$. □

The roots of the equation $x^2 = x + 1$ are significant for another reason: Two lengths x and y are said to be in the **golden ratio** provided the ratio of the larger to the smaller is equal to the ratio of the total to the larger. That is, two lengths x and y with $x > y$ are in the *golden ratio* provided $\frac{x}{y} = \frac{x+y}{x}$. In this case, the *golden ratio* is the ratio of x to y; that is $\frac{x}{y}$. The diagram shows two similar rectangles whose side lengths are in the *golden ratio*.



$$\frac{x+y}{x} = \frac{x}{y}$$

Fixing the smaller of the two as one unit length, i.e. taking $y = 1$, we see that x is equal to the *golden ratio* provided $\frac{x}{1} = \frac{x+1}{x}$. Hence $x^2 = x + 1$.



$$\frac{x+1}{x} = \frac{x}{1} \Longrightarrow x^2 = x + 1$$

Exercises 1.2.

Prove the following propositions using the Well-Ordering Property.

1. $\forall x \in \mathbb{R}$, if $0 < x$, then $\exists n \in \mathbb{N}$, $n - 1 < x \leq n$.
2. $\forall x \in \mathbb{R}$, if $0 < x < 1$, then $\exists n \in \mathbb{N}$, $\frac{1}{n} < x \leq \frac{1}{n-1}$.
3. Let $S \subseteq \mathbb{N}$. Let $A = \{x \in \mathbb{R} \mid \frac{1}{x} \in S\}$. If $S \neq \emptyset$, then A has a largest element.
4. Let $S \subseteq \mathbb{N}$. Let $A = \{x \in \mathbb{R} \mid x^3 \in S\}$. If $S \neq \emptyset$, then A has a smallest element.
5. Let $a \in \mathbb{N}$. If $a \neq 1$, then the set $S = \{x \in \mathbb{N} \mid x \text{ divides } a \text{ and } x \neq a\}$ has a largest element.
6. Let $a \in \mathbb{N}$. If $a \neq 1$, then the set $S = \{x \in \mathbb{N} \mid x \text{ divides } a \text{ and } x \neq 1\}$ has a smallest element.
7. $\forall x \in \mathbb{N}$, $3^x \geq 1 + 2^x$.
8. $\forall a, b \in \mathbb{R}$, if $a \geq 0$ and $b \geq 0$, then $\forall x \in \mathbb{N}$, $(a + b)^x \geq a^x + b^x$.
9. $\forall x \in \mathbb{Z}$, if x is odd, then $\forall n \in \mathbb{N}$, x^n is odd.
10. $\forall x \in \mathbb{Z}$, if $\exists n \in \mathbb{N}$, x^n is odd, then x is odd.
11. $\forall x \in \mathbb{R}$, if $\exists n \in \mathbb{N}$, $x^n < 0$, then $x < 0$.
12. $\forall x \in \mathbb{R}$, if $\exists n \in \mathbb{N}$, $x^n < x$, then $x < 1$.
13. $\forall x \in \mathbb{R}$, if $1 < x$, then $\forall n \in \mathbb{N}$, $1 < x^n$.
14. $\forall x, y \in \mathbb{R}$, if $0 < x < y$, then $\forall n \in \mathbb{N}$, $x^n < y^n$.
15. $\forall x \in \mathbb{R}$, if $0 < x < 1$, then $\forall n \in \mathbb{N}$, $x^n < 1$.
16. $\forall x, y \in \mathbb{R}$, if $0 < x < 1$, then $\forall n \in \mathbb{N}$, $x^n < x$.
17. $\forall m, n \in \mathbb{N}$, if $m < n$, then $2^m < 2^n$.
18. $\forall m, n \in \mathbb{N}$, if $m < n$, then $\left(\frac{1}{2}\right)^n < \left(\frac{1}{2}\right)^m$.
19. $\forall x \in \mathbb{R}$, if $0 < x < 1$, then $\forall m, n \in \mathbb{N}$, if $m < n$, then $x^n < x^m$.
20. $\forall x \in \mathbb{R}$, if $1 < x$, then $\forall m, n \in \mathbb{N}$, if $m < n$, then $x^m < x^n$.

Prove the following propositions using theorem 1.2.3 or its corollary.

21. $\forall x \in \mathbb{Z}$, if $x < 0$, then $x \leq -1$.
22. $\forall x, y \in \mathbb{Z}$, if $x < y + 1$, then $x \leq y$.
23. $\forall x \in \mathbb{N}$, if x divides 2, then $x = 1$ or $x = 2$.
24. $\forall n \in \mathbb{N}$, if $\forall x \in \mathbb{N}$, $\exists t \in \mathbb{N}$, $2x = nt$, then $n = 1$ or $n = 2$.
25. $\forall x \in \mathbb{R}$, $\forall m, n \in \mathbb{Z}$, if $n \leq x < n + 1$ and $m \leq x < m + 1$, then $m = n$.
26. $\forall x, y, q_1, q_2, r_1, r_2 \in \mathbb{Z}$, if $x = yq_1 + r_1$ and $0 \leq r_1 < y$ and $x = yq_2 + r_2$ and $0 \leq r_2 < y$, then $q_1 = q_2$ and $r_1 = r_2$.
(That is, the quotient and remainder given by the division algorithm are unique.)

Prove the following propositions.

27. $\forall x \in \mathbb{Z}$, if x^2 is odd then x is odd.
28. $\forall x, y \in \mathbb{Z}$, if x is even and y is odd, then xy is even.
29. $\forall x, y \in \mathbb{Z}$, if x is even and $x + y$ is even, then y is even.
30. $\forall x, y \in \mathbb{Z}$, if x is odd and $x + y$ is odd, then y is even.
31. $\forall x, y \in \mathbb{Z}$, if x is odd and $x + y$ is even, then y is odd.
32. $\forall x, y \in \mathbb{Z}$, if x is even and $x + y$ is odd, then y is odd.
33. $\forall x, y \in \mathbb{Z}$, if x is odd and xy is odd, then y is odd.
34. $\forall x, y \in \mathbb{Z}$, if x is odd and xy is even, then y is even.
35. $\forall x, y \in \mathbb{Z}$, if xy is even, then x is even or y is even.
36. $\forall x, y \in \mathbb{Z}$, if xy is odd, then x is odd and y is odd.
37. $\forall x, y, z \in \mathbb{Z}$, if $x - y$ is even and $y - z$ is even, then $x - z$ is even.
38. $\forall x, y \in \mathbb{Z}$, if x divides $x + y$ then x divides y.
39. $\forall x, y, z \in \mathbb{Z}$, if x divides y and y divides z, then x divides z.
40. $\forall x, y \in \mathbb{Z}$, if x divides y and y divides x, then $x = y$ or $x = -y$.
41. $\forall x \in \mathbb{Z}$, if 3 divides x, then 3 divides $9 - x$.
42. $\forall x \in \mathbb{Z}$, if 3 divides $9 - x$, then 3 divides x.
43. $\forall x, y \in \mathbb{Z}$, if 5 divides $11x + 6y$, then 5 divides $x + y$.
44. $\forall x, y \in \mathbb{Z}$, if 5 divides $x + y$, then 5 divides $11x + 6y$.
45. $\forall x, y \in \mathbb{Z}$, if x divides y, then x divides $|y|$.
46. $\forall x, y \in \mathbb{Z}$, if x divides y, then $|x|$ divides y.
47. $\forall x, y \in \mathbb{Z}$, if $|x|$ divides y, then x divides y.
48. $\forall x, y \in \mathbb{Z}$, if x divides $|y|$, then x divides y.

49. $\forall x \in \mathbb{Z}$, if 3 divides x and 2 divides x, then 6 divides x.

50. $\forall x \in \mathbb{Z}$, if 6 divides x, then 3 divides x and 2 divides x.

51. $\forall x \in \mathbb{Z}$, if 30 divides x, then 5 divides x and 6 divides x.

52. $\forall x \in \mathbb{Z}$, if 5 divides x and 6 divides x, then 30 divides x.

Prove the following propositions about greatest common divisors and least common multiples.

53. $\forall x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\exists f \in \mathbb{Z}$, $f = \operatorname{lcm}(x, y)$.

54. $\forall a, x, y \in \mathbb{N}$, if x divides a and y divides a, then $\operatorname{lcm}(x, y)$ divides a. (Hint: use the division algorithm.)

55. $\forall a, x, y \in \mathbb{Z}$, if x divides y, then $\gcd(a, x)$ divides $\gcd(a, y)$.

56. $\forall a, x, y \in \mathbb{Z}$, if x divides y, then $\operatorname{lcm}(a, x)$ divides $\operatorname{lcm}(a, y)$.

57. $\forall a, b, x, y \in \mathbb{Z}$, if x divides y and a divides b, then $\gcd(a, x)$ divides $\gcd(b, y)$.

58. $\forall a, b, x, y \in \mathbb{Z}$, if x divides y and a divides b, then $\operatorname{lcm}(a, x)$ divides $\operatorname{lcm}(b, y)$.

59. $\forall m, n \in \mathbb{Z}$, if $m, n \neq 0$ and $\gcd(m, n) = 1$, then $\forall x \in \mathbb{Z}$, $\exists u, v \in \mathbb{Z}$, $x = mu + nv$.

60. $\forall m, n, x \in \mathbb{Z}$, if $m, n \neq 0$ and $\gcd(m, n)$ divides x, then $\exists u, v \in \mathbb{Z}$, $x = mu + nv$.

61. $\forall x, y, a \in \mathbb{Z}$, if $x, y \neq 0$ and x divides a and y divides a and $\gcd(x, y) = 1$, then xy divides a.

62. $\forall x, y, a \in \mathbb{Z}$, if if $a, x \neq 0$ and a divides xy and $\gcd(a, x) = 1$, then a divides y.

Prove the following propositions about rational and irrational numbers.

63. $\forall x, y \in \mathbb{R}$, if x is rational and y is rational, then $x + y$ is rational.

64. $\forall x, y \in \mathbb{R}$, if x is rational and y is irrational, then $x + y$ is irrational.

65. $\forall x, y \in \mathbb{R}$, if $x \neq 0$ and xy is rational and y is irrational, then x is irrational.

66. $\forall x, y \in \mathbb{R}$, if x is rational and $x \neq 0$ and y is irrational, then $\dfrac{x}{y}$ is irrational.

67. $\exists x, y \in \mathbb{R}$, x is irrational and y is irrational and xy is rational.

68. $\exists x, y \in \mathbb{R}$, x is irrational and y is irrational and $x + y$ is rational.

Prove the following propositions. They are analogous to lemma 1.2.14 and proposition 1.2.15.

69. $\forall x \in \mathbb{Z}$, if 3 divides x^2, then 3 divides x.

70. $\sqrt{3}$ is irrational.

Using the Well-Ordering Property, prove the following forms of the Principle of Mathematical Induction.

71. Let $a \in \mathbb{Z}$, and let $A \subseteq \mathbb{Z}$. If $a \in A$ and $\forall n \in \mathbb{Z}$, if $n \in A$ then $n - 1 \in A$, then $\mathbb{Z}_{\leq a} \subseteq A$.

72. Let $A \subseteq \mathbb{Z}$. If $0 \in A$ and $\forall n \in \mathbb{Z}$, if $n \in A$ then $n + 1 \in A$ and $n - 1 \in A$, then $A = \mathbb{Z}$.

73. Let $A \subseteq \mathbb{Z}$. If $A \neq \emptyset$ and $\forall n \in \mathbb{Z}$, if $n \in A$ then $n + 1 \in A$ and $n - 1 \in A$, then $A = \mathbb{Z}$.

74. Let $a \in \mathbb{Z}$, and let $A \subseteq \mathbb{Z}$. If $a \in A$ and $\forall n \in \mathbb{Z}_{\geq a}$, if $\{a, \ldots, n\} \subseteq A$ then $n + 1 \in A$, then $\mathbb{Z}_{\geq a} \subseteq A$.

Prove the following propositions using the Principle of Mathematical Induction.

75. $\forall x \in \mathbb{N}$, 5 divides $8^x + 2(3^{x-1})$.

76. $\forall x \in \mathbb{N}$, 3 divides $2^{2x+1} + 1$.

77. $\forall x, y \in \mathbb{Z}$, $\forall m \in \mathbb{N}$, $x - y$ divides $x^m - y^m$.

78. $\forall x \in \mathbb{Z}$, $\forall m \in \mathbb{N}$, $x^2 + x + 1$ divides $(x+1)^{2m-1} + x^{m+1}$.

79. $\forall x, y, a, b \in \mathbb{Z}$, if $x - y$ divides $a + b$, then $\forall k \in \mathbb{N}$, $x - y$ divides $ax^k + by^k$.

80. $\forall x \in \mathbb{N}$, $5^x \geq 2^x + 3^x$.

81. $\forall a, b \in \mathbb{R}$, if $a \geq 0$ and $b \geq 0$, then $\forall x \in \mathbb{N}$, $(a + b)^x \geq a^x + b^x$.

82. $\forall x \in \mathbb{Z}$, if x is odd, then $\forall n \in \mathbb{N}$, x^n is odd.

83. $\forall x \in \mathbb{Z}$, if $\exists n \in \mathbb{N}$, x^n is odd, then x is odd.

84. $\forall x \in \mathbb{R}$, if $\exists n \in \mathbb{N}$, x^n is irrational, then x is irrational.

85. $\forall x \in \mathbb{R}$, if $x > 1$, then $\forall n \in \mathbb{N}$, $x^n > 1$.

86. $\forall x \in \mathbb{R}$, if $\exists n \in \mathbb{N}$, $x^n < 0$, then $x < 0$.

87. $\forall x \in \mathbb{R}$, if $\exists n \in \mathbb{N}$, $x^n < x$, then $x < 1$.

88. $\forall x \in \mathbb{R}$, if $0 < x < 1$, then $\forall n \in \mathbb{N}$, $0 < x^n < 1$.

89. $\forall x, y \in \mathbb{R}$, if $0 < x < y$, then $\forall n \in \mathbb{N}$, $x^n < y^n$.

90. $\forall m, n \in \mathbb{N}$, if $m < n$, then $2^m < 2^n$.

91. $\forall m, n \in \mathbb{N}$, if $m < n$, then $\left(\frac{1}{2}\right)^n < \left(\frac{1}{2}\right)^m$.

92. $\forall x \in \mathbb{R}$, if $0 < x < 1$, then $\forall m, n \in \mathbb{N}$, if $m < n$, then $x^n < x^m$.

93. $\forall x \in \mathbb{R}$, if $1 < x$, then $\forall m, n \in \mathbb{N}$, if $m < n$, then $x^m < x^n$.

94. Let $a \in \mathbb{R}$ with $a > 1$. Then, $\forall n \in \mathbb{N}$, $\frac{a^{n+1}-1}{n+1} > \frac{a^n-1}{n}$.

95. Let $a \in \mathbb{R}$ with $0 < a < 1$. Then, $\forall n \in \mathbb{N}$, $\frac{a^{n+1}-1}{n+1} > \frac{a^n-1}{n}$.

96. (Bernoulli's Inequality) $\forall x \in \mathbb{R}$, if $-1 \leq x$, then $\forall n \in \mathbb{N}$, $1 + nx \leq (1 + x)^n$.

97. Every finite set of real numbers has a minimum element.

98. Let $f : \mathbb{Z} \to \mathbb{Z}$ be a function with the property that $\forall a \in \mathbb{Z}$, $f(a) < f(a + 1)$. Prove $\forall x, y \in \mathbb{Z}$, if $x < y$ then $f(x) < f(y)$. (Hint: Let $x \in \mathbb{Z}$, and let $A = \{k \in \mathbb{N} \mid f(x) < f(x + k)\}$. Prove by induction that $A = \mathbb{N}$, and use this to prove the desired result.)

99. Let $S \subseteq \mathbb{R}$. If S is closed under addition in the sense that $\forall x, y \in S$, $x + y \in S$, then $\forall a \in S$, $\forall n \in \mathbb{N}$, $na \in S$.

100. Let $S \subseteq \mathbb{R}$. If S is closed under multiplication in the sense that $\forall x, y \in S$, $xy \in S$, then $\forall a \in S$, $\forall n \in \mathbb{N}$, $a^n \in S$.

Prove the following propositions about inductive sets.

101. The set of rational numbers $\mathbb{Q}$ is an inductive subset of $\mathbb{R}$.

102. Let $A \subseteq \mathbb{R}$ be an inductive set. Then, $\forall a \in A$, $\forall n \in \mathbb{N}$, $a + n \in A$.

103. M_0 (the smallest inductive set containing 0) is closed under addition.

104. For all $a \in \mathbb{Z}$, M_a is closed under addition.

105. Let $a \in \mathbb{R}$, and let M_a be the smallest inductive set containing a. $\forall x, y \in M_a$, if $x < y$, then $y - x \in \mathbb{N}$.

106. Let $a \in \mathbb{Z}$, and let M_a be the smallest inductive set containing a. Then $M_a = \mathbb{Z}_{\geq a}$.

Prove the following propositions using the recursive definition of exponents.

107. $\forall x \in \mathbb{R} \setminus \{0\}$, $\forall n \in \mathbb{N}$, $(x^{-1})^n = (x^n)^{-1}$.

108. $\forall x \in \mathbb{R}$, $\forall y \in \mathbb{R} \setminus \{0\}$, $\forall n \in \mathbb{N}$, $\left(\frac{x}{y}\right)^n = \frac{x^n}{y^n}$.

109. $\forall x \in \mathbb{R}$, $\forall n, m \in \mathbb{N}$, $(x^n)^m = x^{nm}$.

110. $\forall x \in \mathbb{R} \setminus \{0\}$, $\forall n, m \in \mathbb{N}$ with $n > m$, $x^{n-m} = \frac{x^n}{x^m}$.

Prove the following properties of series.

111. $\forall a \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} a = na$.

112. For a sequence of real numbers $(a_k)_{k\in\mathbb{N}}$, $\forall c \in \mathbb{R}$, $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} ca_k = c \sum_{k=1}^{n} a_k$.

113. For sequences of real numbers $(a_k)_{k\in\mathbb{N}}$ and $(b_k)_{k\in\mathbb{N}}$, $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n}(a_k + b_k) = \left(\sum_{k=1}^{n} a_k\right) + \left(\sum_{k=1}^{n} b_k\right)$.

114. For a sequence of real numbers $(a_k)_{k\in\mathbb{Z}_{\geq 0}}$, $\forall n \in \mathbb{N}$, $\sum_{k=0}^{n} a_k = a_0 + \sum_{k=1}^{n} a_k$.

115. For a sequence of real numbers $(a_k)_{k\in\mathbb{N}}$, $\forall m, n \in \mathbb{N}$, if $m < n$, then $\sum_{k=1}^{m} a_k + \sum_{k=m+1}^{n} a_k = \sum_{k=1}^{n} a_k$.

116. For a sequence of real numbers $(a_k)_{k\in\mathbb{N}}$, $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} a_k = \sum_{k=1}^{n} a_{n+1-k}$.

117. For a sequence of real numbers $(a_k)_{k\in\mathbb{N}}$, $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n}(a_{k+1} - a_k) = a_{n+1} - a_1$. (Such a series is called a **telescoping sum**)

118. For a sequence of real numbers $(a_k)_{k\in\mathbb{N}}$, $\forall n \in \mathbb{N}$, $\left|\sum_{k=1}^{n} a_k\right| \leq \sum_{k=1}^{n} |a_k|$.

119. For a sequence of integers $(a_k)_{k\in\mathbb{N}}$, if $\forall k \in \mathbb{N}$, a_k is even, then $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} a_k$ is even.

120. For a sequence of real numbers $(a_k)_{k\in\mathbb{N}}$, if $\forall k \in \mathbb{N}$, a_k is rational, then $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} a_k$ is rational.

Prove the following propositions.

121. $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

122. $\forall n \in \mathbb{N}, \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

123. $\forall n \in \mathbb{N}, \sum_{k=1}^{n} k^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$.

124. $\forall n \in \mathbb{N}, \sum_{k=1}^{n} (k)(k!) = (n+1)! - 1$.

125. $\forall n \in \mathbb{N}, \sum_{k=1}^{n} \frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}$.

126. $\forall n \in \mathbb{N}, \sum_{k=1}^{n} 2k - 1 = n^2$.

For each of the following recursively defined functions, guess an explicit formula for $f(x)$ and prove that your formula is true for all $x \in \mathbb{N}$.

127. $f : \mathbb{N} \to \mathbb{N}$ given by: $f(1) = 2$ and for each $n \in \mathbb{N}$, $f(n+1) = f(n) + 2$.

128. $f : \mathbb{N} \to \mathbb{N}$ given by: $f(1) = 1$, $f(2) = 3$ and for each $n \geq 2$, $f(n+1) = 2f(n) - f(n-1)$.

129. $f : \mathbb{N} \to \mathbb{N}$ given by: $f(1) = 1$, $f(2) = 4$ and for each $n \geq 2$, $f(n+1) = 2(f(n)+1) - f(n-1)$.

130. $f : \mathbb{N} \to \mathbb{N}$ given by: $f(1) = 1$, $f(2) = 8$ and for each $n \geq 2$, $f(n+1) = 2(f(n)+3n) - f(n-1)$.

Let $n \in \mathbb{N}$ and let $\mathbb{N}|(n)$ be the set of divisors of n. That is,

$$\mathbb{N}|(n) = \{x \in \mathbb{N} \mid x \text{ **divides** } n\}.$$

Let $x, y, z \in \mathbb{N}|(n)$. Compare the following properties of the gcd **and** lcm **functions to the** *Boolean algebraic* **properties given in section 0.3.**

$\frac{n}{1} = n$ $\qquad$ $\frac{n}{n} = 1$

Idempotence
$\text{lcm}(x, x) = x$ $\qquad$ $\gcd(x, x) = x$

Commutativity
$\text{lcm}(x, y) = \text{lcm}(y, x)$ $\qquad$ $\gcd(x, y) = \gcd(y, x)$

Associativity
$\text{lcm}(x, \text{lcm}(y, z)) = \text{lcm}(\text{lcm}(x, y), z)$
$\gcd(x, \gcd(y, z)) = \gcd(\gcd(x, y), z)$

Absorption
$\text{lcm}(x, \gcd(x, y)) = x$ $\qquad$ $\gcd(x, \text{lcm}(x, y)) = x$

Distributivity
$\text{lcm}(x, \gcd(y, z)) = \gcd(\text{lcm}(x, y), \text{lcm}(x, z))$
$\text{lcm}(x, \gcd(y, z)) = \text{lcm}(\gcd(x, y), \gcd(x, z))$

Annihilator
$\text{lcm}(x, n) = n$ $\qquad$ $\gcd(x, 1) = 1$

Identity
$\text{lcm}(x, 1) = x$ $\qquad$ $\gcd(x, n) = x$

Double Negation
$$\frac{n}{\left(\frac{n}{x}\right)} = x$$

De Morgan's Laws
$\frac{n}{\gcd(x,y)} = \text{lcm}\left(\frac{n}{x}, \frac{n}{y}\right)$
$\frac{n}{\text{lcm}(x,y)} = \gcd\left(\frac{n}{x}, \frac{n}{y}\right)$

1. Prove the Idempotence properties for gcd and lcm.

2. Prove the Annihilator properties for gcd and lcm.

3. Prove the Identity properties for gcd and lcm.

4. Prove the Absorption properties for gcd and lcm.

5. Prove the Associativity properties for gcd and lcm. (Hint: use the result proven in exercise 54.)

6. Prove $\forall a, x, y \in \mathbb{N}|(n)$, both $\frac{n}{x}$ and $\frac{n}{y}$ divide $\frac{n}{a}$ if and only if a divides both x and y.

7. Prove $\forall a, x, y \in \mathbb{N}|(n)$, $\frac{n}{a}$ divides both $\frac{n}{x}$ and $\frac{n}{y}$ if and only if both x and y divide a.

8. Prove De Morgan's Laws for gcd and lcm.

9. Give an example of a value of $n \in \mathbb{N}$ and $x \in \mathbb{N}|(n)$ for which the analogous properties to Complementation: $\gcd(x, \frac{n}{x}) = 1$ and $\text{lcm}(x, \frac{n}{x}) = n$ do not hold.

Chapter 2

Sets

We began discussing the common notation used to describe sets and set related concepts in section 0.4. We now return to this topic with a view toward applying the proof techniques of chapter 1 to propositions involving sets. We will see in this chapter that the language of sets can be used to simplify and generalize a number of mathematical concepts. In one important example, the concepts of *greatest common divisor* and *least common multiple* can be viewed as simple operations on the *ideals* of $\mathbb{Z}$ defined in section 0.4 (definition 0.4.2). In fact, since the language and notation used in math can often become bulky and unwieldy as the theory develops, and sets offer us a convenient way to organize and simplify this language, their use has become indispensable in all areas of mathematics.

2.1 Relations and Operations

The primary concept with which the language of sets is concerned is the relation between *element* and *set*; that is, the relation '$\in$'. To explore the linguistic purpose served by this relation, recall the earlier discourse on sentence structure in chapter 0, section 0.1. We began then by identifying the subject x and predicate $P(x)$ in a given proposition. For example, in the proposition '2 is even,' the subject is 2 and the predicate is 'x is even.' Recall that when the subject is a free variable, the predicate 'x is even' is called an *open sentence*. Further, the possible subjects for which a given predicate is intelligible we called the *universe of discourse* (for the variable x in the open sentence 'x is even,' the universe of discourse is $\mathbb{Z}$).

Now, given any universe of discourse U and predicate $P(x)$, we can specify a set

$$A = \{x \in U \mid P(x)\}.$$

Having specified such a set, we see that for $x \in U$, the statements $P(x)$ and $x \in A$ have the same meaning. That is, if one is conversing about subjects that belong to a universe of discourse U (for example, when discussing real numbers or integers, the universe of discourse would be $\mathbb{R}$ or $\mathbb{Z}$ respectively), then any predicate $P(x)$ can be replaced with a predicate of the form $x \in A$ for an appropriate set A. For example, for $x \in \mathbb{Z}$, rather than saying 'x is even,' one can say $x \in \langle 2 \rangle$.

Recall that for $a \in \mathbb{Z}$, the **ideal** of $\mathbb{Z}$ generated by a is the set

$$\langle a \rangle = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = at\}.$$

Similarly, for $x \in \mathbb{R}$, rather than saying $x > 0$, one can say $x \in (0, \infty)$. In this way, all predicates can be phrased in terms of sets.

Consider now a statement involving a *universal quantifier*,

'$\forall x \in A$, $P(x)$,' or equivalently '$\forall x \in U$, if $x \in A$, then $P(x)$'.

By specifying $B = \{x \in U \mid P(x)\}$, this statement becomes

'$\forall x \in U$, if $x \in A$, then $x \in B$'. That is, '$A \subseteq B$'.

Hence statements with universal quantifiers can be phrased in terms of the *subset* relation. Similarly, for the same open sentence $P(x)$, the existentially quantified statement

'$\exists x \in U$, $P(x)$' can be written in the language of sets as '$B \neq \emptyset$'.

As an example, consider the statement '$\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$, $x < y$'. This can be written in set terms as '$\{x \in \mathbb{R} \mid (x, \infty) \neq \emptyset\} = \mathbb{R}$.' For a more extreme example, we can rewrite the statement '$\forall x \in \mathbb{R}$, if $\forall \varepsilon > 0$, $x < \varepsilon$, then $x \leq 0$' as '$\{x \in \mathbb{R} \mid (0, \infty) \subseteq (x, \infty)\} \subseteq (-\infty, 0]$.' It should be noted that these translations yield no new insight into the meaning or truth of the propositions in question. They simply say the same thing in different notation. In the examples given above, there is not necessarily any practical advantage to be gained from one notation or the other. The examples are only intended to illustrate that the element-set, set-subset, and equality of sets, relations comprise the core of the structure of mathematical language. Hence, these relations deserve further discussion.

Subsets and Set Equality

Recall that given two sets A and B, whose elements belong to a common universe of discourse U, to say that A is a *subset* of B means that all of the elements of A are also elements of B. More precisely:

For sets A and B whose elements belong to the universe of discourse U, A is a **subset** of B, denoted $A \subseteq B$, means

$$\forall x \in U,\ \text{if } x \in A, \text{ then } x \in B.$$

Equivalently, we may use the set A as the universe of discourse and write $A \subseteq B$ as

$$\forall x \in A,\ x \in B.$$

Notice that the relation $\subseteq$ is defined in terms of an implication:

'$\forall x \in U$, **if** $x \in A$**, then** $x \in B$.'

This means that to prove $A \subseteq B$, for given sets A and B, we must prove the implication

'if $x \in A$, then $x \in B$'

for an arbitrary constant x. Recall that we have three structures that can be used to prove implications. These are *direct proof*, *proof by contraposition*, and *proof by contradiction*. A proof that $A \subseteq B$ will hence follow one of these three structures. To examine some of the basic properties of the subset relation we will look at three fundamental results that hold for *every set*. First, when a set is defined using a universe of discourse and an open sentence:

$$\{x \in U \mid P(x)\},$$

we require that the universe of discourse U is itself a set. This leads to the very intuitive result that *every set is a subset of the universe of discourse* in which it is defined. Second, we have the similarly intuitive result that *every set is a subset of itself*. Third, we have the perhaps less intuitive result that the *empty set* $\emptyset$ *is a subset of every set*. We will use a direct proof for the first two and a proof by contradiction for the third.

Proposition 2.1.1.

Let A be a set whose elements belong to the universe U. Then

1. $A \subseteq U$,
2. $A \subseteq A$
3. $\emptyset \subseteq A$.

Proof.
(1) Let $x \in U$.
  Assume $x \in A$.
    Therefore, $x \in U$.
  Therefore, if $x \in A$, then $x \in U$.
Therefore, $\forall x \in U$, if $x \in A$, then $x \in U$.
Therefore, $A \subseteq U$.
(2) Let $x \in U$.
  Assume $x \in A$.
    Then $x \in A$.
  Therefore, if $x \in A$, then $x \in A$.
Therefore, $\forall x \in U$, if $x \in A$, then $x \in A$.
Therefore, $A \subseteq A$.
(3) Suppose $\exists x \in U$, $x \in \emptyset$ and $x \notin A$.
  Choose such an x.
  Then $x \in \emptyset$, which is a contradiction.
Therefore, $\forall x \in U$, if $x \in \emptyset$, then $x \in A$.
Therefore, $\emptyset \subseteq A$. □

All three proofs above are trivial in the sense that they do not involve an argument or demonstration. They are evident simply by their sentence structure. In the first case, since for any $x \in U$, the proposition $x \in U$ is true, the statement

'if $x \in A$, then $x \in U$' is of the form 'if P then $TRUE$'

which is a tautology (it is true regardless of the truth value of P). Similarly, in the second case, the statement

'if $x \in A$, then $x \in A$' is a tautology of the form 'if P, then P'.

Finally, since for any $x \in U$, the statement $x \in \emptyset$ is false, the third statement

'if $x \in \emptyset$, then $x \in A$' is of the form 'if $FALSE$, then P',

which again is true regardless of the truth or falsity of P. Hence all three propositions are true by virtue of their sentence structure, without regards to the meaning of the predicate $x \in A$.

Proofs of abstract statements that apply to all sets will generally exhibit this behaviour. Since the basic predicate $x \in A$ has no determined meaning when A is an arbitrary set, it is only the logical sentence structure of whatever proposition we are trying to prove that contributes to its proof. For this reason, proofs involving abstract sets give us a good opportunity to practice structuring our mathematical proofs, without the distraction of calculations or demonstrations. For another example of a proof that applies to all sets, we prove that the subset relation is *transitive*:

Proposition 2.1.2.

Let A, B, and C be sets whose elements belong to a common universe of discourse U. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof.
Assume $A \subseteq B$ and $B \subseteq C$.
    Let $x \in U$.
        Assume $x \in A$
            Since $x \in A$ and $A \subseteq B$, we have $x \in B$.
            Since $x \in B$ and $B \subseteq C$, we have $x \in C$.
            Therefore, $x \in C$.
        Therefore, if $x \in A$, then $x \in C$.
    Therefore, $\forall x \in U$, if $x \in A$, then $x \in C$.
    That is, $A \subseteq C$.
Therefore, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$ □

Recall from section 0.4 that equality of sets is given in terms of the subset relation:

For sets A and B whose elements belong to the universe of discourse U, $A = B$ means

$$A \subseteq B \text{ and } B \subseteq A.$$

This means that to prove sets A and B are equal, we prove that $A \subseteq B$ and that $B \subseteq A$. Thus a proof of equality is simply two proofs that a subset relation holds. We demonstrate this with two examples, one abstract and one more concrete. Both examples involve set complements, which were defined in section 0.4. So that the notation in these examples is understood, recall definition 0.4.4:

Let A be a set whose elements are in the universe of discourse U. We define the **complement** of A, denoted A^c, to be

$$A^c = \{x \in U \mid x \notin A\}.$$

Further, given any two sets A and B, we define the **complement of A relative to B**, denoted $B \setminus A$ to be

$$B \setminus A = \{x \in U \mid x \in B \text{ and } x \notin A\}.$$

Proposition 2.1.3.

Let A and B be sets within a common universe of discourse U. If $B \subseteq A^c$, then $A \setminus B = A$.

Proof.
Assume $B \subseteq A^c$.
    Let $x \in U$.
        Assume $x \in A \setminus B$.
            Then $x \in A$ and $x \notin B$.
            In particular, we have $x \in A$.
        Therefore, if $x \in A \setminus B$, then $x \in A$.
    Therefore, $A \setminus B \subseteq A$.
    Let $x \in U$.
        Assume $x \in A$.
            Suppose $x \in B$, seeking a contradiction.
                Since $x \in B$ and $B \subseteq A^c$, we have $x \in A^c$.
                Therefore, $x \notin A$.
                We now have the contradiction $x \in A$ and $x \notin A$.
            Therefore, $x \notin B$.
            Then $x \in A$ and $x \notin B$; hence $x \in A \setminus B$.
        Therefore, if $x \in A$, then $x \in A \setminus B$.
    Therefore, $A \subseteq A \setminus B$.
    Hence, we have $A \setminus B \subseteq A$ and $A \subseteq A \setminus B$.
    Therefore, $A = A \setminus B$.
Therefore, if $B \subseteq A^c$, then $A \setminus B = A$. □

Next, for a concrete example, we consider the relative complement of two real intervals: $(0, 2) \setminus (1, 3)$. If one can imagine these two sets drawn on a number line and consider those points on the line that lie within the interval $(0, 2)$ and outside of the interval $(1, 3)$, it will soon become clear that the set $(0, 2) \setminus (1, 3)$ is the interval $(0, 1]$. To confirm that our intuition is correct, we prove the equality of these sets:

Example 2.1.4.

$(0, 2) \setminus (1, 3) = (0, 1]$.

Proof.
Let $x \in \mathbb{R}$.
    Assume $x \in (0, 2) \setminus (1, 3)$.
        Then $x \in (0, 2)$ and $x \notin (1, 3)$.
        Since $x \in (0, 2)$, we have that $0 < x$ and $x < 2$.
        Since $x < 2$ and $2 < 3$, we have by transitivity, $x < 3$.
        Further, since $x \notin (1, 3)$, we have either $x \leq 1$ or $x \geq 3$.
        However, since $x < 3$, it is not the case that $x \geq 3$.
        Therefore, it must be the case that $x \leq 1$.
        We now have $0 < x$ and $x \leq 1$
        Therefore, $x \in (0, 1]$
    Therefore, if $x \in (0, 2) \setminus (1, 3)$, then $x \in (0, 1]$.
Therefore, $(0, 2) \setminus (1, 3) \subseteq (0, 1]$.
Let $x \in \mathbb{R}$.
    Assume $x \in (0, 1]$.
        Then $0 < x$ and $x \leq 1$.
        Since $x \leq 1$ and $1 < 2$, we have $x < 2$.
        We now have $0 < x$ and $x < 2$, hence $x \in (0, 2)$.
        Suppose $x \in (1, 3)$.
            Then $1 < x$ and $x < 3$.
            In this case, we have the contradiction $1 < x$ and $x \leq 1$.
        Therefore, $x \notin (1, 3)$
        We have thus shown that $x \in (0, 2)$ and $x \notin (1, 3)$.
        Therefore, $x \in (0, 2) \setminus (1, 3)$.
    Therefore, if $x \in (0, 1]$, then $x \in (0, 2) \setminus (1, 3)$.
Therefore, $(0, 1] \subseteq (0, 2) \setminus (1, 3)$.
Therefore, $(0, 2) \setminus (1, 3) = (0, 1]$. □

Binary Operations on Sets

In addition to the *relative complement*, we define two other binary operations on sets. Given two sets A and B, the **intersection** is the set of all elements common to both A and B, and the **union** is the set of elements that appear in at least one of A or B. The proper definitions are:

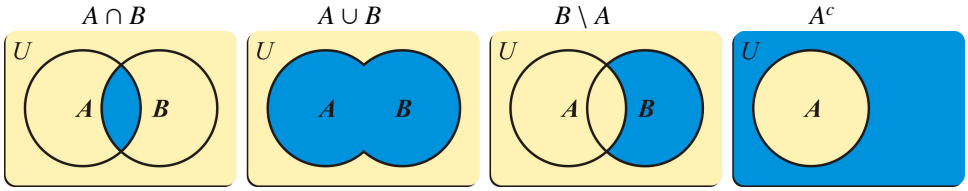
Definition 2.1.1. Let A and B be sets. We define the **intersection** of A and B, denoted $A \cap B$, to be

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

We define the **union** of A and B, denoted $A \cup B$ to be

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

Venn diagrams, **although not used in formal proofs**, can give us a convenient way of visualizing these binary operations. If we draw the universe of discourse as an all-encompassing rectangle and represent sets as circles within this universe, we can picture the regions captured by the definitions of *intersection*, *union*, *complement*, and *relative complement*.



One quick observation that we can see in the above diagram is that $A \cap B$ is in some sense *smaller* than each of A and B, while $A \cup B$ is in some sense *larger* than each of A and B. In fact, the sense in which these are smaller and larger is in terms of the *subset* relation. We have $A \cap B \subseteq A$ and $A \cap B \subseteq B$. Likewise, $A \subseteq A \cup B$ and $B \subseteq A \cup B$. However, since an appeal to the diagram does not constitute a mathematical proof, we should prove that these relations do in fact hold as stated.

Proposition 2.1.5.

Let A and B be sets. Then $A \cap B \subseteq A$ and $A \subseteq A \cup B$.

Proof.
Let $x \in A \cap B$.
    Then $x \in A$ and $x \in B$.
    In particular, $x \in A$.
Therefore, $A \cap B \subseteq A$.
Let $x \in A$.
    Then it is true that $x \in A$ or $x \in B$.
    Therefore, $x \in A \cup B$.
Therefore, $A \subseteq A \cup B$.
Therefore, $A \cap B \subseteq A$ and $A \subseteq A \cup B$. □

The binary operations $\cap$ and $\cup$ satisfy all of the same *Boolean algebraic* properties satisfied by the logical operators $\wedge$ and $\vee$ (see section 0.3). Thus, the family of sets in a given universe of discourse form a *boolean algebra*:

Boolean Algebraic Properties of Sets

For sets A, B, and C in a common universe of discourse U, the following are true:

$$U^c = \emptyset \qquad \emptyset^c = U$$

Idempotence

$$A \cap A = A \qquad A \cup A = A$$

Commutativity

$$A \cap B = B \cap A \qquad A \cup B = B \cup A$$

Associativity

$$A \cap (B \cap C) = (A \cap B) \cap C \qquad A \cup (B \cup C) = (A \cup B) \cup C$$

Absorption

$$A \cap (A \cup B) = A \qquad A \cup (A \cap B) = A$$

Distributivity

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Annihilator

$$A \cap \emptyset = \emptyset \qquad A \cup U = U$$

Identity

$$A \cap U = A \qquad A \cup \emptyset = A$$

Complementation

$$A \cap A^c = \emptyset \qquad A \cup A^c = U$$

Double Negation

$$(A^c)^c = A$$

De Morgan's Laws

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

Unlike the axioms of the real numbers, which establish an algebraic system by defining the real numbers as such, the algebraic properties of sets are not given by definition. Rather, each of the above properties can be deduced using the definitions of *intersection*, *union*, and *complement*. The proofs of the boolean algebraic properties of sets are all fairly straight forward and do not lead to any proof structures or techniques that we have not already discussed at length. It would therefore be tedious and of very little pedagogical value to recount all of their proofs here. However, the reader is certainly invited to attempt proofs of these properties at his or her leisure.

With all of our definitions in place, for the sake of practice we will give several examples of proofs involving intersections, unions, complements, subsets, and set equality. For each of the following examples, let A, B, C, and D be sets (if needed, assume that the elements of these sets belong to a common universe of discourse U).

Proposition 2.1.6.

If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.

Proof.
Assume $A \subseteq B$.
    Let $x \in A \cap C$.
        Then $x \in A$ and $x \in C$.
        Since $x \in A$ and $A \subseteq B$, we have $x \in B$.
        We now have $x \in B$ and $x \in C$.
        Therefore, $x \in B \cap C$.
    Therefore, $A \cap C \subseteq B \cap C$.
Therefore, if $A \subseteq B$, then $A \cap C \subseteq B \cap C$. □

Proposition 2.1.7.

If $A \subseteq B$ and $C \subseteq D$, then $A \cup C \subseteq B \cup D$.

Proof.
Assume $A \subseteq B$ and $C \subseteq D$.
    Let $x \in A \cup C$.
        Then $x \in A$ or $x \in C$.
        Case 1: $x \in A$.
            Since $x \in A$ and $A \subseteq B$, we have $x \in B$.
            Since $x \in B$ and $B \subseteq B \cup D$, we have $x \in B \cup D$.
        Case 2: $x \in C$.
            Since $x \in C$ and $C \subseteq D$, we have $x \in D$.
            Since $x \in D$ and $D \subseteq B \cup D$, we have $x \in B \cup D$.
        In both cases we have $x \in B \cup D$.
    Therefore, $A \cup C \subseteq B \cup D$.
Therefore, if $A \subseteq B$ and $C \subseteq D$, then $A \cup C \subseteq B \cup D$. □

Proposition 2.1.8.

If $A \subseteq B$, then $C \setminus B \subseteq C \setminus A$.

Proof.
Assume $A \subseteq B$.
Let $x \in U$.
Suppose $x \in C \setminus B$ and $x \notin C \setminus A$.
Since $x \in C \setminus B$, we have $x \in C$ and $x \notin B$.
Also, since $x \notin C \setminus A$, we have $x \notin C$ or $x \in A$.
Considering that $x \in C$, it must then be the case that $x \in A$.
Since $x \in A$ and $A \subseteq B$, we have $x \in B$.
This gives us the contradiction $x \in B$ and $x \notin B$.
Therefore, if $x \in C \setminus B$, then $x \in C \setminus A$.
Therefore, $C \setminus B \subseteq C \setminus A$.
Therefore, if $A \subseteq B$, then $C \setminus B \subseteq C \setminus A$. □

Proposition 2.1.9.

If $A \setminus B \subseteq C$, then $A \setminus C \subseteq B$.

Proof.
Suppose $A \setminus B \subseteq C$ and $A \setminus C \nsubseteq B$.
Since $A \setminus C \nsubseteq B$, we have that $\exists x \in U$, $x \in A \setminus C$ and $x \notin B$.
Choose such an x.
We then have $x \in A$ and $x \notin C$ and $x \notin B$.
Since $x \in A$ and $x \notin B$, we have $x \in A \setminus B$.
Therefore, $x \in C$, since $A \setminus B \subseteq C$.
We now have the contradiction $x \in C$ and $x \notin C$.
Therefore, if $A \setminus B \subseteq C$, then $A \setminus C \subseteq B$. □

Proposition 2.1.10.

If $A \cap B \subseteq C$, then $(A \setminus C) \cap B = \emptyset$.

Proof.
Suppose $A \cap B \subseteq C$ and $(A \setminus C) \cap B \neq \emptyset$.
Since $(A \setminus C) \cap B \neq \emptyset$, we can choose $x \in (A \setminus C) \cap B$.
For such an x, we have $x \in A$ and $x \notin C$ and $x \in B$.
Since $x \in A$ and $x \in B$, we have $x \in A \cap B$.
Therefore, $x \in C$, since $A \cap B \subseteq C$.
This gives us the contradiction $x \in C$ and $x \notin C$.
Therefore, if $A \cap B \subseteq C$, then $(A \setminus C) \cap B = \emptyset$. □

A remark about proving emptiness

Generally, for sets A and B, to prove $A = B$ we show $A \subseteq B$ and $B \subseteq A$. To prove $A = \emptyset$, this amounts to showing $\emptyset \subseteq A$, which is always true, and $A \subseteq \emptyset$, which presents some stylistic concerns: To show $A \subseteq \emptyset$ by a *direct proof* involves assuming $x \in A$ and demonstrating $x \in \emptyset$. Since $x \in \emptyset$ is categorically false, it is not likely that such a demonstration will be feasible. In fact, demonstrating that $x \in \emptyset$ amounts to finding a *contradiction*. Because of this, in practically all cases, the statement $A = \emptyset$ is best proved using a *proof by contradiction*. That is, we assume $A \neq \emptyset$, which allows us to choose a nonspecific constant $x \in A$. From this assumption, we then attempt to derive a contradiction.

For some more concrete examples, we will look at unions and intersections involving real intervals and ideals of $\mathbb{Z}$.

Example 2.1.11.

$(0, 1] \cap [2, 3) = \emptyset$.

Proof.
Suppose $(0, 1] \cap [2, 3) \neq \emptyset$.
We may then choose $x \in (0, 1] \cap [2, 3)$.
For such an x, we have $x \in (0, 1]$ and $x \in [2, 3)$.
This gives us four inequalities: $0 < x$, $x \leq 1$, $2 \leq x$, and $x < 3$.
Of particular interest are the inequalities $x \leq 1$ and $2 \leq x$.
Since $x \leq 1$ and $1 < 2$, we have $x < 2$, which contradicts $2 \leq x$.
We thus have a contradiction.
Therefore, $(0, 1] \cap [2, 3) = \emptyset$. □

Example 2.1.12.

$(0, 2] \cup [1, 3) = (0, 3)$.

Proof.
Let $x \in (0, 2] \cup [1, 3)$.
Then $x \in (0, 2]$ or $x \in [1, 3)$.
Case 1: $x \in (0, 2]$.
In this case, we have $0 < x$ and $x \leq 2$.
Since $x \leq 2$ and $2 < 3$, we have $x < 3$.
This gives us $0 < x$ and $x < 3$; hence, $x \in (0, 3)$.
Case 2: $x \in [1, 3)$.
In this case, we have $1 \leq x$ and $x < 3$.
Since $0 < 1$ and $1 \leq x$, we have $0 < x$.
We then have $0 < x$ and $x < 3$; hence, $x \in (0, 3)$.
In both cases, $x \in (0, 3)$.
Therefore, $(0, 2] \cup [1, 3) \subseteq (0, 3)$.
Conversely, let $x \in (0, 3)$.
Then $0 < x$ and $x < 3$.
We consider two cases: $x \leq 2$ and $2 < x$.
Case 1: $x \leq 2$.
In this case, we have $0 < x$ and $x \leq 2$.
Therefore, $x \in (0, 2]$.
Therefore, $x \in (0, 2] \cup [1, 3)$, since $(0, 2] \subseteq (0, 2] \cup [1, 3)$.
Case 2: $2 < x$.
In this case, we have $1 < 2$ and $2 < x$, hence $1 < x$.
Therefore, $1 \leq x$.
We then have $1 \leq x$ and $x < 3$, hence $x \in [1, 3)$.
Therefore, $x \in (0, 2] \cup [1, 3)$.
In both cases, $x \in (0, 2] \cup [1, 3)$.
Therefore, $(0, 3) \subseteq (0, 2] \cup [1, 3)$.
Therefore, $(0, 2] \cup [1, 3) = (0, 3)$. □

Example 2.1.13.

$\langle 2\rangle \cap \langle 3\rangle = \langle 6\rangle$.

Proof.
Let $x \in \langle 2\rangle \cap \langle 3\rangle$.
Then $x \in \langle 2\rangle$ and $x \in \langle 3\rangle$.
This means, $\exists t \in \mathbb{Z}$, $x = 2t$ and $\exists s \in \mathbb{Z}$, $x = 3s$.
Choose such s and t, and set $r = t - s$.
$x = 3x - 2x = 3(2t) - 2(3s) = 6(t - s) = 6r$.
Therefore, $\exists r \in \mathbb{Z}$, $x = 6r$; hence, $x \in \langle 6\rangle$.
Therefore, $\langle 2\rangle \cap \langle 3\rangle \subseteq \langle 6\rangle$.
Conversely, let $x \in \langle 6\rangle$.
Then $\exists a \in \mathbb{Z}$, $x = 6a$. Choose such an a.
Put $b = 3a$.
$x = 6a = 2(3a) = 2b$.
Therefore, $\exists b \in \mathbb{Z}$, $x = 2b$; hence, $x \in \langle 2\rangle$.
Put $c = 2a$.
$x = 6a = 3(2a) = 3c$.
Therefore, $\exists c \in \mathbb{Z}$, $x = 3c$; hence, $x \in \langle 3\rangle$.
We now have $x \in \langle 2\rangle$ and $x \in \langle 3\rangle$; hence, $x \in \langle 2\rangle \cap \langle 3\rangle$.
Therefore, $\langle 6\rangle \subseteq \langle 2\rangle \cap \langle 3\rangle$.
Therefore, $\langle 2\rangle \cap \langle 3\rangle = \langle 6\rangle$. □

Extended Set Operations

Notice that both the union and the intersection are *associative* operations. That is, $A \cap (B \cap C) = (A \cap B) \cap C$, and $A \cup (B \cup C) = (A \cup B) \cup C$. For this reason, the notation $A \cup B \cup C$ can be used without ambiguity. Further, given a sequence of four sets A, B, C, and D, we can use the notation $A \cap B \cap C \cap D$ to denote $(A \cap B \cap C) \cap D$. The same is true for unions, and it is easy to see the idea of an intersection or union of any number of sets emerging from this convention. In fact, we can make this precise by using a *recursive definition*, as discussed in section 1.2. However, we will quickly run out of letters if we choose to denote our sets by uppercase letters A, B, C, etc. A better choice of notation would be something along the lines of A_1, A_2, A_3, etc. To make this notation more precise, we denote by $(A_k)_{k\in\mathbb{N}}$ a **sequence** of sets. Formally, this represents a *correspondence* between natural numbers and sets. That is, to each natural number k corresponds a set A_k. An example of such a sequence is given by: $\forall k \in \mathbb{N}$, $A_k = [0, k)$. In this case, to each $k \in \mathbb{N}$ corresponds the real interval $[0, k)$. Thus $A_1 = [0, 1)$, $A_2 = [0, 2)$, and so on. With this idea in mind, we can extend the definitions of union and intersection to any finite number of sets.

Definition 2.1.2. Let $(A_k)_{k\in\mathbb{N}}$ be a sequence of sets. Define

$$\bigcup_{k=1}^{1} A_k = A_1 \text{ and for each } n \in \mathbb{N}, \bigcup_{k=1}^{n+1} A_k = \left(\bigcup_{k=1}^{n} A_k\right) \cup A_{n+1}.$$

Define

$$\bigcap_{k=1}^{1} A_k = A_1 \text{ and for each } n \in \mathbb{N}, \bigcap_{k=1}^{n+1} A_k = \left(\bigcap_{k=1}^{n} A_k\right) \cap A_{n+1}.$$

Since these extensions of the union and intersection operations are defined recursively, proofs involving the union or intersection of a sequence of sets very often require induction. We give the following two proofs as examples.

Proposition 2.1.14.

Let $(A_k)_{k\in\mathbb{N}}$ be a sequence of sets. $\forall m, n \in \mathbb{N}$, if $n \leq m$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m} A_k$.

Proof.
Let $A = \{x \in \mathbb{N} \mid \forall n \in \mathbb{N}$, if $n \leq x$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{x} A_k\}$.
Let $n \in \mathbb{N}$.
    Assume $n \leq 1$.
        Then $n = 1$; so $\bigcup_{k=1}^{n} A_k = \bigcup_{k=1}^{1} A_k$, and hence $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{1} A_k$.
    Therefore, if $n \leq 1$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{1} A_k$.
Therefore, $\forall n \in \mathbb{N}$, if $n \leq 1$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{1} A_k$.
That is, $1 \in A$.
Let $m \in \mathbb{N}$ and assume $m \in A$.
    Then $\forall n \in \mathbb{N}$, if $n \leq m$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m} A_k$.
    Let $n \in \mathbb{N}$.
        Assume $n \leq m + 1$.
            We consider two cases: $n < m + 1$ and $n = m + 1$.
            Case 1: $n < m + 1$.
                In this case, $n \leq m$, hence $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m} A_k$.
                Since $\bigcup_{k=1}^{m} A_k \subseteq A_{m+1} \cup \bigcup_{k=1}^{m} A_k = \bigcup_{k=1}^{m+1} A_k$, we have
                $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m+1} A_k$ by transitivity.
            Case 2: $n = m + 1$.
                In this case, $\bigcup_{k=1}^{n} A_k = \bigcup_{k=1}^{m+1} A_k$; thus $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m+1} A_k$.
            In both cases, we have $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m+1} A_k$.
        Therefore, if $n \leq m + 1$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m+1} A_k$.
    Therefore, $\forall n \in \mathbb{N}$, if $n \leq m + 1$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m+1} A_k$.
    That is, $m + 1 \in A$.
Therefore, $\forall m \in \mathbb{N}$, if $m \in A$, then $m + 1 \in A$.
Hence, by the PMI, $\mathbb{N} \subseteq A$.
Therefore, $\forall m, n \in \mathbb{N}$, if $n \leq m$, then $\bigcup_{k=1}^{n} A_k \subseteq \bigcup_{k=1}^{m} A_k$. □

Proposition 2.1.15.

Let $(A_k)_{k\in\mathbb{N}}$ be a sequence of sets. $\forall m, n \in \mathbb{N}$, if $m \leq n$, then $\bigcap_{k=1}^{n} A_k \subseteq A_m$.

Proof.
Let $m \in \mathbb{N}$.
  Let $A = \{x \in \mathbb{Z}_{\geq m} \mid \bigcap_{k=1}^{x} A_k \subseteq A_m\}$.
  To show that $m \in A$, we consider two cases: $m = 1$ and $m > 1$.
  Case 1: $m = 1$.
    In this case, we have $\bigcap_{k=1}^{m} A_k = \bigcap_{k=1}^{1} A_k = A_1 = A_m$.
    Therefore, $\bigcap_{k=1}^{m} A_k \subseteq A_m$.
  Case 2: $m > 1$.
    Then $m - 1 > 0$; hence $m - 1 \in \mathbb{N}$.
    We then have $\bigcap_{k=1}^{m} A_k = A_m \cap \bigcap_{k=1}^{m-1} A_k$.
    Since $A_m \cap \bigcap_{k=1}^{m-1} A_k \subseteq A_m$, we have $\bigcap_{k=1}^{m} A_k \subseteq A_m$.
  In both cases, $\bigcap_{k=1}^{m} A_k \subseteq A_m$; hence $m \in A$.
  Let $n \in \mathbb{Z}_{\geq m}$.
    Assume $n \in A$.
      Then $\bigcap_{k=1}^{n} A_k \subseteq A_m$.
      Since $\bigcap_{k=1}^{n+1} A_k = A_{n+1} \cap \bigcap_{k=1}^{n} A_k \subseteq \bigcap_{k=1}^{n} A_k$,
      We have $\bigcap_{k=1}^{n+1} A_k \subseteq A_m$ by transitivity.
      Hence, $n + 1 \in A$.
    Therefore, if $n \in A$, then $n + 1 \in A$.
  Therefore, $\forall n \in \mathbb{Z}_{\geq m}$, if $n \in A$, then $n + 1 \in A$.
  Hence, by the PMI, $\mathbb{Z}_{\geq m} \subseteq A$.
Therefore, $\forall m, n \in \mathbb{N}$, if $m \leq n$, then $\bigcap_{k=1}^{n} A_k \subseteq A_m$. □

Exercises 2.1.

Let A, B, C, and D be sets (assume the elements of these sets belong to a common universe of discourse U). Prove the following propositions.

1. $U \setminus A = A^c$.
2. $A \setminus B = A \cap B^c$.
3. (a) If $A \subseteq B$, then $A \cap B = A$.
   (b) If $A \cap B = A$, then $A \cup B = B$.
   (c) If $A \cup B = B$, then $A \setminus B = \emptyset$.
   (d) If $A \setminus B = \emptyset$, then $A \subseteq B$.
4. (a) If $A \cap B = \emptyset$, then $A \subseteq B^c$.
   (b) If $A \subseteq B^c$, then $(A \cup B) \setminus B = A$.
   (c) If $(A \cup B) \setminus B = A$, then $B \subseteq A^c$.
   (d) If $B \subseteq A^c$, then $A \setminus B = A$.
   (e) If $A \setminus B = A$, then $B \setminus A = B$.
   (f) If $B \setminus A = B$, then $A \cap B = \emptyset$.
5. $(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)$.
6. $A \setminus (A \setminus B) = A \cap B$.
7. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
8. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
9. $A = (A \setminus B) \cup (A \cap B)$.
10. $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.
11. If $A \subseteq B$, then $A \cup C \subseteq B \cup C$.
12. If $A \subseteq B$, then $A \setminus C \subseteq B \setminus C$.
13. if $A \subseteq B$ then $C \setminus B \subseteq C \setminus A$.
14. If $A \subseteq B$ and $C \subseteq D$, then $A \cap C \subseteq B \cap D$.
15. If $A \subseteq B$ and $C \subseteq D$, then $A \setminus D \subseteq B \setminus C$.
16. (a) If $A \cap E \subseteq B \cap E$ for all sets E, then $A \subseteq B$.
    (b) If $A \cup E \subseteq B \cup E$ for all sets E, then $A \subseteq B$.
    (c) If $A \setminus E \subseteq B \setminus E$ for all sets E, then $A \subseteq B$.
    (d) If $E \setminus B \subseteq E \setminus A$ for all sets E, then $A \subseteq B$.
17. (a) If $A \cap E = \emptyset$ for all sets E, then $A = \emptyset$.
    (b) If $A \cap E = A$ for all sets E, then $A = \emptyset$.
    (c) If $A \cup E = E$ for all sets E, then $A = \emptyset$.
    (d) If $A \subseteq E$ for all sets E, then $A = \emptyset$.
18. (a) If $A \cup E = U$ for all sets E, then $A = U$.
    (b) If $A \cup E = A$ for all sets E, then $A = U$.
    (c) If $A \cap E = E$ for all sets E, then $A = U$.
    (d) If $E \subseteq A$ for all sets E, then $A = U$.
19. If $A \cap B = \emptyset$ and $A \cup B = U$, then $A = B^c$.
20. If $A \subseteq B \setminus A$, then $A = \emptyset$.
21. If $U \setminus A \subseteq A$, then $A = U$.
22. If $A \cap B \subseteq A \setminus B$, then $A \cap B = \emptyset$.
23. If $C \subseteq A \cup B$, then $C \setminus A \subseteq B$.
24. If $C \subseteq A \cup B^c$, then $(C \setminus A) \cap B = \emptyset$.
25. If $A \cap B \cap C = \emptyset$, then $C \subseteq A^c \cup B^c$.
26. If $A \subseteq B$ and $B \cap C = \emptyset$, then $A \cap C = \emptyset$.

Let $(A_k)_{k\in\mathbb{N}}$ be a sequence of sets, and let B be a set. Prove the following propositions.

27. $\forall m, n \in \mathbb{N}$, if $m \leq n$, then $A_m \subseteq \bigcup_{k=1}^{n} A_k$.
28. $\forall m, n \in \mathbb{N}$, if $n \leq m$, then $\bigcap_{k=1}^{m} A_k \subseteq \bigcap_{k=1}^{n} A_k$.
29. $\forall n \in \mathbb{N}$, $B \cup \bigcap_{k=1}^{n} A_k = \bigcap_{k=1}^{n} (B \cup A_k)$.
30. $\forall n \in \mathbb{N}$, $B \cap \bigcup_{k=1}^{n} A_k = \bigcup_{k=1}^{n} (B \cap A_k)$.
31. $\forall n \in \mathbb{N}$, $B \setminus \bigcup_{k=1}^{n} A_k = \bigcap_{k=1}^{n} (B \setminus A_k)$.
32. $\forall n \in \mathbb{N}$, $B \setminus \bigcap_{k=1}^{n} A_k = \bigcup_{k=1}^{n} (B \setminus A_k)$.
33. $\forall n \in \mathbb{N}$, $\left(\bigcup_{k=1}^{n} A_k\right)^c = \bigcap_{k=1}^{n} (A_k)^c$.
34. $\forall n \in \mathbb{N}$, $\left(\bigcap_{k=1}^{n} A_k\right)^c = \bigcup_{k=1}^{n} (A_k)^c$.
35. If $B \subseteq A_1$, then $\forall n \in \mathbb{N}$, $B \subseteq \bigcup_{k=1}^{n} A_k$.
36. If $A_1 \subseteq B$, then $\forall n \in \mathbb{N}$, $\bigcap_{k=1}^{n} A_k \subseteq B$.

37. If $\forall m \in \mathbb{N}$, $B \subseteq A_m$, then $\forall n \in \mathbb{N}$, $B \subseteq \bigcap_{k=1}^{n} A_k$.

38. If $\forall m \in \mathbb{N}$, $A_m \subseteq B$, then $\forall n \in \mathbb{N}$, $\bigcup_{k=1}^{n} A_k \subseteq B$.

39. If $\forall k \in \mathbb{N}$, $A_{k+1} \subseteq A_k$, then $\forall m, n \in \mathbb{N}$, if $m \leq n$, then $A_n \subseteq A_m$.

40. If $\forall k \in \mathbb{N}$, $A_k \subseteq A_{k+1}$, then $\forall m, n \in \mathbb{N}$, if $m \leq n$, then $A_m \subseteq A_n$.

41. If $\forall m \in \mathbb{N}$, $A_{m+1} \subseteq A_m$, then $\forall n \in \mathbb{N}$, $\bigcap_{k=1}^{n} A_k = A_n$.

42. If $\forall m \in \mathbb{N}$, $A_m \subseteq A_{m+1}$, then $\forall n \in \mathbb{N}$, $\bigcup_{k=1}^{n} A_k = A_n$.

43. If $\forall m \in \mathbb{N}$, $A_{m+1} \subseteq A_m$, then $\forall n \in \mathbb{N}$, $\bigcup_{k=1}^{n} A_k = A_1$.

44. If $\forall m \in \mathbb{N}$, $A_m \subseteq A_{m+1}$, then $\forall n \in \mathbb{N}$, $\bigcap_{k=1}^{n} A_k = A_1$.

Prove the following propositions.

45. $(-2, 1] \cup [0, 3) = (-2, 3)$.

46. $(-2, 1] \cap [0, 3) = [0, 1]$.

47. $(-2, 1] \setminus [0, 3) = (-2, 0)$.

48. $[0, 3) \setminus (-2, 1] = (1, 3)$.

49. $(-\infty, 3) \setminus (-2, 1] = (-\infty, -2] \cup (1, 3)$.

50. $(-\infty, 1) \cap (-2, 3] = (-2, 1)$.

51. $\langle 5 \rangle \cap \langle 6 \rangle = \langle 30 \rangle$.

52. $\langle 5 \rangle \cap \langle 2 \rangle = \langle 10 \rangle$.

53. $\forall a, b \in \mathbb{Z}$, if $\gcd(a, b) = 1$, then $\langle a \rangle \cap \langle b \rangle = \langle ab \rangle$.

54. $\langle 12 \rangle \cap \langle 18 \rangle = \langle 36 \rangle$.

55. Let $A = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z}, x = 15t + 7\}$, $B = \{x \in \mathbb{Z} \mid \exists s \in \mathbb{Z}, x = 3s + 1\}$, and $C = \{x \in \mathbb{Z} \mid \exists r \in \mathbb{Z}, x = 5r + 2\}$. Then $A = B \cap C$.

56. Let $A = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = 6t + 5\}$, $B = \{x \in \mathbb{Z} \mid \exists s \in \mathbb{Z},\ x = 8s + 3\}$, and $C = \{x \in \mathbb{Z} \mid \exists r \in \mathbb{Z},\ x = 24r + 11\}$. Then $A \cap B = C$.

57. $\forall n \in \mathbb{N}$, $\bigcup_{k=1}^{n} (0, k] = (0, n]$.

58. $\forall n \in \mathbb{N}$, $\bigcap_{k=1}^{n} (0, \frac{1}{k}] = (0, \frac{1}{n}]$.

2.2 Real Intervals

Our two most frequently used examples of sets are the real intervals and the ideals of the integers. The reason for this focus is to encourage practice with the techniques associated with the order relation in the real numbers and the divides relation in the integers. These relations and the techniques we use to study them are essential in many areas of mathematics and indispensable for any future student of analysis or algebra. To explore these two examples in more detail, we devote the current section to examining properties of real intervals and the section that follows to the ideals of the integers.

To begin, we distinguish between two types of real intervals: Those that are bounded, and those that are unbounded. We dealt briefly with upper and lower bounds in the section on the well-ordering property, since the well-ordering property states that sets of integers that are bounded below have and smallest element and those that are bounded above have a largest element. Although the well-ordering property does not hold in the real numbers, the concept of upper and lower bounds is still very useful. For the sake of building our inquiry on firm ground, we give the precise definition of a **bounded** set:

Definition 2.2.1. For a subset A of the real numbers $\mathbb{R}$, A is **bounded below** means

$$\exists a \in \mathbb{R},\ \forall x \in A,\ a \leq x.$$

A is **bounded above** means

$$\exists a \in \mathbb{R},\ \forall x \in A,\ x \leq a.$$

A is **bounded** means A is both bounded above and bounded below.

When a set is *bounded*, it will generally have more than one upper bound and more than one lower bound. This allows us some flexibility in selecting upper and lower bounds we wish to focus on, for any given bounded set. The following proposition shows that it is always possible to select the upper and lower bounds to be of the same magnitude. That is, if A is any bounded set, we may select $k \in \mathbb{R}$ such that A is *bounded above* by k and *bounded below* by $-k$. It is left as an exercise to show that due to the Archimedean property, we may also ask that such a k be a natural number.

Proposition 2.2.1.

For every subset A of $\mathbb{R}$, A is bounded if and only if $\exists k \in \mathbb{R}$, $\forall x \in A$, $|x| \leq k$.

Proof.
Let $A \subseteq \mathbb{R}$.
  Assume A is bounded.
    Choose $a \in \mathbb{R}$ such that $\forall x \in A$, $a \leq x$.
    Choose $b \in \mathbb{R}$ such that $\forall x \in A$, $x \leq b$.
    Choose $k = \max(-a, b)$.
    Then $-a \leq k$ and $b \leq k$.
    This can be written as $-k \leq a$ and $b \leq k$.
    Let $x \in A$.
      Then $-k \leq a \leq x \leq b \leq k$.
      By transitivity, $-k \leq x \leq k$; hence $|x| \leq k$.
    Therefore, $\exists k \in \mathbb{R}$, $\forall x \in A$, $|x| \leq k$.
  Conversely, assume $\exists k \in \mathbb{R}$, $\forall x \in A$, $|x| \leq k$.
    For such a k, we have $\forall x \in A$, $-k \leq x$ and $\forall x \in A$, $x \leq k$.
    Therefore, A is bounded below by $-k$ and above by k.
    Thus A is bounded.
  Therefore, A is bounded if and only if $\exists k \in \mathbb{R}$, $\forall x \in A$, $|x| \leq k$.
Therefore, for any $A \subseteq \mathbb{R}$, A is bounded if and only if $\exists k \in \mathbb{R}$, $\forall x \in A$, $|x| \leq k$. □

We classify the nine types of intervals into those that are bounded and those that are not bounded:

For $a, b \in \mathbb{R}$,

Bounded Intervals	**Unbounded Intervals**
$(a, b) = \{x \in \mathbb{R} \mid a < x \text{ and } x < b\}$	$(a, \infty) = \{x \in \mathbb{R} \mid a < x\}$
$(a, b] = \{x \in \mathbb{R} \mid a < x \text{ and } x \leq b\}$	$[a, \infty) = \{x \in \mathbb{R} \mid a \leq x\}$
$[a, b) = \{x \in \mathbb{R} \mid a \leq x \text{ and } x < b\}$	$(-\infty, b) = \{x \in \mathbb{R} \mid x < b\}$
$[a, b] = \{x \in \mathbb{R} \mid a \leq x \text{ and } x \leq b\}$	$(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$
	$(-\infty, \infty) = \mathbb{R}$.

We note that all of the *bounded* intervals can be viewed as intersections of the *unbounded* intervals. That is, $(a, b) = (a, \infty) \cap (-\infty b)$, $[a, b) = [a, \infty) \cap (-\infty, b)$, $(a, b] = (a, \infty) \cap (-\infty, b]$, and $[a, b] = [a, \infty) \cap (-\infty, b]$. The proofs of each of these are similar to one another, and so we only present the details for the first. To produce the other three results, the proof need only be modified by replacing $<$ by $\leq$ wherever appropriate.

Proposition 2.2.2.

$\forall a, b \in \mathbb{R}$, $(a, b) = (a, \infty) \cap (-\infty, b)$.

Proof.
Let $a, b \in \mathbb{R}$.
  Let $x \in (a, b)$.
    Then $a < x$ and $x < b$.
    Since $a < x$, we have $x \in (a, \infty)$.
    Since $x < b$, we have $x \in (-\infty, b)$.
    Therefore, $x \in (a, \infty) \cap (-\infty, b)$.
  Therefore, $(a, b) \subseteq (a, \infty) \cap (-\infty, b)$.
  Conversely, let $x \in (a, \infty) \cap (-\infty, b)$.
    Then $x \in (a, \infty)$ and $x \in (-\infty, b)$.
    Therefore, $a < x$ and $x < b$; hence $x \in (a, b)$.
  Thus, $(a, \infty) \cap (-\infty, b) \subseteq (a, b)$; hence $(a, b) = (a, \infty) \cap (-\infty, b)$.
Therefore, $\forall a, b \in \mathbb{R}$, $(a, b) = (a, \infty) \cap (-\infty, b)$. □

It is worth calling attention to the fact that the two directions in the above proof consist of exactly the same series of steps, performed in reverse order. In the rare occasions where this occurs, we can restructure the proof to execute both directions simultaneously. Here is an alternate version of the proof above:

Proof.
Let $a, b \in \mathbb{R}$.
  $x \in (a, b)$ if and only if $a < x$ and $x < b$.
  $a < x$ and $x < b$ if and only if $x \in (a, \infty)$ and $x \in (-\infty, b)$.
  $x \in (a, \infty)$ and $x \in (-\infty, b)$ if and only if $x \in (a, \infty) \cap (-\infty, b)$.
  Therefore, $x \in (a, b)$ if and only if $x \in (a, \infty) \cap (-\infty, b)$.
  Thus, $(a, b) = (a, \infty) \cap (-\infty, b)$.
Therefore, $\forall a, b \in \mathbb{R}$, $(a, b) = (a, \infty) \cap (-\infty, b)$. □

Here is another example of intervals of a certain type intersecting to form other intervals. In this proof, we use the following two theorems:

$$\forall x, y, a \in \mathbb{R},\ a < \min(x, y) \text{ if and only if } a < x \text{ and } a < y.$$

$$\forall x, y, a \in \mathbb{R},\ \max(x, y) < a \text{ if and only if } x < a \text{ and } y < a.$$

These are exercises 118 and 117 from section 1.1.

Proposition 2.2.3.

$\forall a, b, c, d \in \mathbb{R}$, $(a, b) \cap (-\infty, c) = (a, u)$ where $u = \min(b, c)$,
and $(a, b) \cap (d, \infty) = (v, b)$ where $v = \max(a, d)$.

Proof.
Let $a, b, c, d \in \mathbb{R}$.
Set $u = \min(b, c)$, and let $x \in \mathbb{R}$.
$x \in (a, b) \cap (-\infty, c)$ if and only if $a < x$ and $x < b$ and $x < c$.
$a < x$ and $(x < b$ and $x < c)$ if and only if $a < x$ and $x < \min(b, c) = u$.
$a < x$ and $x < u$ if and only if $x \in (a, u)$.
Therefore, $x \in (a, b) \cap (-\infty, c)$ if and only if $x \in (a, u)$.
Therefore, $(a, b) \cap (-\infty, c) = (a, u)$, where $u = \min(b, c)$.
Next, set $v = \max(a, d)$, and let $x \in \mathbb{R}$.
$x \in (a, b) \cap (d, \infty)$ if and only if $a < x$ and $x < b$ and $d < x$.
$(a < x$ and $d < x)$ and $x < b$ if and only if $v = \max(a, d) < x$ and $x < b$.
$v = \max(a, d) < x$ and $x < b$ if and only if $x \in (v, b)$.
Therefore, $x \in (a, b) \cap (d, \infty)$ if and only if $x \in (v, b)$.
Therefore, $(a, b) \cap (d, \infty) = (v, b)$, where $v = \max(a, d)$.
Now, $\forall a, b, c, d \in \mathbb{R}$, $(a, b) \cap (-\infty, c) = (a, u)$ where $u = \min(b, c)$,
and $(a, b) \cap (d, \infty) = (v, b)$ where $v = \max(a, d)$. □

It is left as an exercise to show that the intersection of any two intervals (no matter the type) will always produce another interval. However, the same cannot be said for the union or the relative complement. For example, $(0, 1) \cup [2, 3)$ is not an interval, and $(0, 3) \setminus [1, 2)$ is not an interval (actually, $(0, 1) \cup [2, 3) = (0, 3) \setminus [1, 2)$). For another example:

Proposition 2.2.4.

$\forall c, d \in \mathbb{R}$, $\mathbb{R} \setminus [c, d] = (-\infty, c) \cup (d, \infty)$.

Proof. Let $c, d \in \mathbb{R}$.
Let $x \in \mathbb{R} \setminus [c, d]$.
Then $x \notin [c, d]$.
This means that $x < c$ or $d < x$.
In case $x < c$, we have $x \in (-\infty, c)$; hence $x \in (-\infty, c) \cup (d, \infty)$.
In case $d < x$, we have $x \in (d, \infty$; so again $x \in (-\infty, c) \cup (d, \infty)$.
Therefore, $\mathbb{R} \setminus [c, d] \subseteq (-\infty, c) \cup (d, \infty)$.
Conversely, let $x \in (-\infty, c) \cup (d, \infty)$.
Then $x \in (-\infty, c)$ or $x \in (d, \infty)$.
That is, $x < c$ or $d < x$.
Therefore, it is not the case that $c \leq x$ and $x \leq d$.
Hence, $x \notin [c, d]$.
Therefore, $x \in \mathbb{R} \setminus [c, d]$.
Therefore, $\mathbb{R} \setminus [c, d] \subseteq (-\infty, c) \cup (d, \infty)$.
Thus, $\forall c, d \in \mathbb{R}$, $\mathbb{R} \setminus [c, d] = (-\infty, c) \cup (d, \infty)$. □

There are some situations, however, when the relative complement of two intervals does produce another interval. For example:

Proposition 2.2.5.

$\forall a, b, x, y \in \mathbb{R}$, if $x \in (a, b)$ and $b \in (x, y)$, then $(a, b) \setminus (x, y) = (a, x]$.

Proof.
Let $a, b, x, y \in \mathbb{R}$.
Assume $x \in (a, b)$ and $b \in (x, y)$.
Let $t \in (a, b) \setminus (x, y)$.
Then $t \in (a, b)$ and $t \notin (x, y)$.
Since $t \in (a, b)$, we have $t < b$.
Also, since $b \in (x, y)$, we have $b < y$.
With $t < b$ and $b < y$, we have by transitivity, $t < y$.
Now, since $t \notin (x, y)$, we have $t \leq x$ or $y \leq t$.
Since $t < y$, it is not the case that $y \leq t$.
Therefore, it is the case that $t \leq x$.
Finally, since $t \in (a, b)$, we have $a < t$.
Now, $a < t$ and $t \leq x$. Hence $t \in (a, x]$.
Therefore, $(a, b) \setminus (x, y) \subseteq (a, x]$.
Conversely, let $t \in (a, x]$.
Then $a < t$ and $t \leq x$.
Since $x \in (a, b)$, we have $x < b$.
Now, since $t \leq x$ and $x < b$, we have by transitivity, $t < b$.
We now have $a < t$ and $t < b$; hence $t \in (a, b)$.
Further, since $t \leq x$, it is not the case that $x < t$.
Therefore, $t \notin (x, y)$.
We then have $t \in (a, b)$ and $t \notin (x, y)$. Hence $t \in (a, b) \setminus (x, y)$.
Therefore, $(a, x] \subseteq (a, b) \setminus (x, y)$; hence $(a, b) \setminus (x, y) = (a, x]$.
Therefore, if $x \in (a, b)$ and $b \in (x, y)$, then $(a, b) \setminus (x, y) = (a, x]$.
Q.E.D. □

A remark about the use of Q.E.D.

Q.E.D. stands for the Latin 'quod erat demonstrandum,' meaning 'that which was to have been demonstrated.' Since it is understood that the last line of a proper formal proof is always an exact restatement of the theorem that was to be proven, the line Q.E.D. can stand as a substitute for this last line. When reading a proof that ends with Q.E.D., we mentally insert the exact statement of the theorem in place of the letters Q.E.D. (in the previous exercise this would be 'For all $a, b, x, y \in \mathbb{R}$, if $x \in (a, b)$ and $b \in (x, y)$, then $(a, b) \setminus (x, y) = (a, x]$.') We should then verify that this line follows from the proof that appears above it. You may also come across the acronym Q.E.F., which stands for 'quod erat faciendum' meaning 'that which was to have been done.' This is used in the same way as Q.E.D. but for proofs that are pure constructions, such as proposition 1.1.10. However, the preferred practice is always to include, as the last line of the proof, a full and exact restatement of the property being proven.

Let us consider in more detail the criteria under which the relative complement or union of two intervals is itself an interval. In fact, the case of relative complements is exactly the same as the case of unions. The reason is that the relative complement of two intervals is always equal to a union of two intervals. We will prove this in the special case $(a, b) \setminus [c, d]$. To simplify the proof, we will make use of some basic properties of sets from section 2.1. In particular, we will use the fact that $A \setminus B = A \cap B^c = A \cap (U \setminus B)$, as well as the distributive law $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proposition 2.2.6.

For all $a, b, c, d \in \mathbb{R}$, $(a, b) \setminus [c, d] = (a, u) \cup (v, b)$, where $u = \min\{b, c\}$ and $v = \max\{a, d\}$.

Proof.
Let $a, b, c, d \in \mathbb{R}$.
Set $u = \min\{b, c\}$ and $v = \max\{a, d\}$.

$$\begin{aligned}(a, b) \setminus [c, d] &= (a, b) \cap (\mathbb{R} \setminus [c, d]) \\ &= (a, b) \cap ((-\infty, c) \cup (d, \infty)) \text{ by proposition 2.2.4} \\ &= ((a, b) \cap (-\infty, c)) \cup ((a, b) \cap (d, \infty)) \\ &= (a, u) \cup (v, b) \text{ by proposition 2.2.3.}\end{aligned}$$

Therefore, $(a, b) \setminus [c, d] = (a, u) \cup (v, b)$, where $u = \min\{b, c\}$ and $v = \max\{a, d\}$.
Therefore, for all $a, b, c, d \in \mathbb{R}$, $(a, b) \setminus [c, d] = (a, u) \cup (v, b)$, where $u = \min\{b, c\}$ and $v = \max\{a, d\}$. □

Note that in the above proof, we could have one or both of the intervals (a, u) and (v, b) being empty. For example, the above proposition tells us that

$$(1, 3) \setminus [2, 5] = (1, 2) \cup (5, 3) = (1, 2) \cup \emptyset = (1, 2).$$

This is indeed the proper result.

We now consider the circumstances under which the *union* of two intervals is itself an interval. The answer is that the two intervals must overlap. We prove this in the case of bounded open intervals:

Proposition 2.2.7.

For all $a, b, c, d \in \mathbb{R}$, if $(a, b) \cap (c, d) \neq \emptyset$, then $(a, b) \cup (c, d) = (u, v)$, where $u = \min(a, c)$ and $v = \max(b, d)$.

Proof.
Let $a, b, c, d \in \mathbb{R}$.
Assume $(a, b) \cap (c, d) \neq \emptyset$.
Set $u = \min(a, c)$ and $v = \max(b, d)$, and let $x \in (a, b) \cup (c, d)$.
Then $x \in (a, b)$ or $x \in (c, d)$.
In case $x \in (a, b)$, we have $u \leq a < x < b \leq v$; hence $u < x < v$.
In case $x \in (c, d)$, we have $u \leq c < x < d \leq v$ and again $u < x < v$.
Therefore, $x \in (u, v)$.
Therefore, $(a, b) \cup (c, d) \subseteq (u, v)$
Conversely, let $x \in (u, v)$.
Since $(a, b) \cap (c, d) \neq \emptyset$, choose an element $t \in (a, b) \cap (c, d)$.
This gives us $a < t < b$ and $c < t < d$. Therefore, $c < b$ and $a < d$.
Case 1: $u = a$ and $v = b$
Then $x \in (a, b)$, so $x \in (a, b) \cup (c, d)$.
Case 2: $u = a$ and $v = d$
Then $a < x < d$.
If $x < b$, then $a < x < b$, in which case $x \in (a, b)$.
Hence, in the case where $x < b$, we have $x \in (a, b) \cup (c, d)$.
Otherwise, if $b \leq x$, then since $c < b$ we have $c < x$ by transitivity.
In this case, $c < x < d$, which means $x \in (c, d)$.
So, again $x \in (a, b) \cup (c, d)$.
Case 3: $u = c$ and $v = b$
Then $c < x < b$.
If $x < d$, then $c < x < d$; hence $x \in (c, d)$.
In this case, $x \in (a, b) \cup (c, d)$.
Otherwise, if $d \leq x$, then since $a < d$ we have $a < x$ by transitivity.
In this case, $a < x < b$; hence $x \in (a, b)$.
So, again $x \in (a, b) \cup (c, d)$.
Case 4: $u = c$ and $v = d$
Then $x \in (c, d)$, so $x \in (a, b) \cup (c, d)$.
Therefore, $(u, v) \subseteq (a, b) \cup (c, d)$; hence $(a, b) \cup (c, d) = (u, v)$.
Therefore, if $(a, b) \cap (c, d) \neq \emptyset$, then $(a, b) \cup (c, d) = (u, v)$, where $u = \min(a, c)$ and $v = \max(b, d)$.
Q.E.D. □

Nesting of Bounded Intervals

It is a fairly simple task to show that the four different types of bounded intervals are nested in the following ways:

$$(a,b) \subseteq (a,b] \subseteq [a,b] \text{ and } (a,b) \subseteq [a,b) \subseteq [a,b].$$

The proofs of these are left as exercises. It is also trivially true that

$$(a,b) \subseteq (a,b) \subseteq [a,b] \text{ and } (a,b) \subseteq [a,b] \subseteq [a,b].$$

Moreover, it is useful to note that the bounded intervals are the *only* sets nested between (a,b) and $[a,b]$. That is, the only sets J for which $(a,b) \subseteq J \subseteq [a,b]$ are the four bounded intervals (a,b), $(a,b]$, $[a,b)$, and $[a,b]$:

Theorem 2.2.8.

$\forall a, b \in \mathbb{R}$, If J is a non-empty subset of $\mathbb{R}$ and $(a, b) \subseteq J \subset [a, b]$, then $J = (a, b)$ or $J = (a, b]$ or $J = [a, b]$ or $J = [a, b)$.

Proof.
Let $a, b \in \mathbb{R}$.
Assume J is a non-empty subset of $\mathbb{R}$ and $(a, b) \subseteq J \subset [a, b]$.
Case 1: $a \notin J$ and $b \notin J$.
Let $x \in J$.
Then $x \in [a, b]$ since $J \subseteq [a, b]$; hence $a \leq x \leq b$.
Since $a, b \notin J$, we have $x \neq a$ and $x \neq b$.
Therefore, $a < x < b$; hence $x \in (a, b)$.
Therefore, $J \subseteq (a, b)$; hence $J = (a, b)$.
Case 2: $a, b \in J$.
Let $x \in [a, b]$.
Then either $x = a$, or $x = b$, or $x \in (a, b)$.
In all cases, $x \in J$, since $a \in J$, $b \in J$, and $(a, b) \subseteq J$.
Therefore, $[a, b] \subseteq J$; hence $J = [a, b]$.
Case 3: $a \in J$ and $b \notin J$.
For $x \in [a, b)$, we have either $x = a$ or $x \in (a, b)$.
In both of these cases, $x \in J$, since $a \in J$ and $(a, b) \subseteq J$.
Therefore, $[a, b) \subseteq J$.
Conversely, for $x \in J$, we have $x \in [a, b]$ and hence $a \leq x \leq b$.
Since $b \notin J$, we have $x \neq b$, hence $a \leq x < b$.
Therefore, $x \in [a, b)$.
Therefore, $J \subseteq [a, b)$; hence $J = [a, b)$.
Case 4: $a \notin J$ and $b \in J$.
Letting $x \in (a, b]$ gives us $x = b$ or $x \in (a, b)$.
In both of these cases, $x \in J$.
Therefore, $(a, b] \subseteq J$.
Conversely, letting $x \in J$, we have $x \in [a, b]$ and hence $a \leq x \leq b$.
Since $a \notin J$, $x \neq a$; hence $a < x \leq b$.
Therefore, $x \in (a, b]$.
So, in this case, $J = (a, b]$.
Therefore, if J is a non-empty subset of $\mathbb{R}$ and $(a, b) \subseteq J \subset [a, b]$,
then $J = (a, b)$ or $J = (a, b]$ or $J = [a, b]$ or $J = [a, b)$.
Q.E.D. □

We have results similar to the above for the unbounded intervals: Also true are:

$$\text{if } (a, \infty) \subseteq J \subseteq [a, \infty), \text{ then } J = (a, \infty) \text{ or } J = [a, \infty)$$

and

$$\text{if } (-\infty, b) \subseteq J \subseteq (-\infty, b], \text{ then } J = (-\infty, b) \text{ or } J = (-\infty, b).$$

The proofs of these are left as exercises.

Characterization of Intervals

One convenient characteristic of the intervals is that since both the $<$ relation and the $\leq$ relation satisfy the same axioms (transitivity, preserving addition, and preserving multiplication by positives), we see that the different types of intervals behave in essentially the same ways. That is, a result such as

$$\forall a, b, x, y \in \mathbb{R}, \text{ if } a \leq x \text{ and } y \leq b, \text{ then } (x, y) \subseteq (a, b).$$

also holds for other types of intervals. For example,

$$\forall a, b, x, y \in \mathbb{R}, \text{ if } a \leq x \text{ and } y \leq b, \text{ then } [x, y) \subseteq [a, b),$$

and

$$\forall a, b, x, y \in \mathbb{R}, \text{ if } a \leq x, \text{ then } [x, \infty) \subseteq [a, \infty)$$

are also true (the proofs of these are left as exercises).

One downside of this is that to prove these statements for all nine types of interval would require nine separate proofs, the details of which would be virtually identical to one another. To circumvent this monotony, we want a *characterization* of what it means to be an interval. That is, we look for one single property that is held by all nine types of intervals and no other sets. One such common property that is shared by all intervals, no matter the type, is that intervals (and no other sets) contain all of the real numbers that fall between any two of their elements. More precisely, for a subset $J \subseteq \mathbb{R}$, J is an interval if and only if

$$\forall x, y \in J, \ \forall z \in \mathbb{R}, \text{ if } x < z < y, \text{ then } z \in J.$$

The proof of this theorem is not trivial, and it will take a fair amount of discussion to bring to light.

However, it is quite easy to see how useful the above property can be. For example, consider the proposition 'the intersection of any two intervals (of any type) is itself an interval.' Immediately, we see that to prove this from the definition of an interval would require $(9)(9) = 81$ cases considering each of the different types that the two intervals might be. It gets worse: Even if the types of the two intervals are fixed, the intersection can be of several different types, depending on the circumstances. For example, $(0, 2] \cap [1, 3) = [1, 2]$, $(1, 3] \cap [0, 2) = (1, 2)$, $(0, 3] \cap [1, 2) = [1, 2)$, $(1, 2] \cap [0, 3) = (1, 2]$. We see that even in the case where the types of intervals are fixed as $(a, b] \cap [x, y)$, the intersection might be any of the four types of bounded interval. Hence, our 81 initial cases will contain further subcases. We have no intention of working through the proof as such, or even asking the reader to do so. Rather, to prove the proposition 'the intersection of any two intervals (of any type) is itself an interval,' we can choose merely to show that the intersection of any two sets satisfying the property

$$\forall x, y \in J, \ \forall z \in \mathbb{R}, \text{ if } x < z < y, \text{ then } z \in J$$

will itself satisfy this property. This is enough, to prove the desired proposition, since the intervals are exactly the sets that satisfy this property. Note: The proof that the intersection of intervals is an interval is left as an exercise. The reader is strongly encouraged to make use of the characterization of intervals as the sets satisfying the property $\forall x, y \in J$, $\forall z \in \mathbb{R}$, if $x < z < y$, then $z \in J$.

The remainder of the section will be devoted to proving the theorem: For a subset $J \subseteq \mathbb{R}$, J is an interval if and only if

$$\forall x, y \in J,\ \forall z \in \mathbb{R},\ \text{if } x < z < y, \text{ then } z \in J.$$

We begin with the forward direction: If J is an interval, then $\forall x, y \in J$, $\forall z \in \mathbb{R}$, if $x < z < y$, then $z \in J$. We make use of the nesting properties of intervals described in the preceding section.

Theorem 2.2.9.

If J is an interval of $\mathbb{R}$ (one of the nine types), then $\forall x, y \in J$, $\forall z \in \mathbb{R}$, if $x < z < y$, then $z \in J$.

Proof.
Let J be an interval of $\mathbb{R}$.
- Then J is one of 9 forms (a, b), $[a, b)$, etc.,
- We consider the four bounded intervals first:
- For some $a, b \in \mathbb{R}$, $J = [a, b]$, $J = (a, b]$, $J = [a, b)$, or $J = (a, b)$.
  - Choose $a, b \in \mathbb{R}$ so that J is given by one of the above four cases.
  - In all cases, we have $(a, b) \subseteq J \subseteq [a, b]$.
  - Let $x, y \in J$ and $z \in \mathbb{R}$. Assume $x < z < y$.
    - Since $J \subseteq [a, b]$, we have $x, y \in [a, b]$.
    - We then have $a \leq x < z < y \leq b$, so $a < z < b$ by transitivity.
    - Then $z \in (a, b)$; hence $z \in J$.
  - Therefore, $\forall x, y \in J$, $\forall z \in \mathbb{R}$, if $x < z < y$, then $z \in J$.
- Next, we consider the two types of interval bounded below:
- For some $a \in \mathbb{R}$, $J = (a, \infty)$ or $J = [a, \infty)$.
  - Choose $a \in \mathbb{R}$ for which J is one of these two intervals.
  - In either case, we have $(a, \infty) \subseteq J \subseteq [a, \infty)$.
  - Let $x, y \in J$ and $z \in \mathbb{R}$. Assume $x < z < y$.
    - Since $J \subseteq [a, \infty)$, we have $x \in [a, \infty)$.
    - Then $a \leq x < z < y$; hence $a < z$.
    - This means $z \in (a, \infty)$; hence $z \in J$.
  - Therefore, $\forall x, y \in J$, $\forall z \in \mathbb{R}$, if $x < z < y$, then $z \in J$.
- Next, if J is bounded above but not below:
- For some $b \in \mathbb{R}$, $J = (-\infty, b)$ or $J = (-\infty, b]$.
  - Choose such a $b \in \mathbb{R}$.
  - In either case, we have $(-\infty, b) \subseteq J \subseteq (-\infty, b]$.
  - Let $x, y \in J$ and $z \in \mathbb{R}$. Assume $x < z < y$.
    - Since $J \subseteq (-\infty, b]$, we have $y \leq b$.
    - Then $x < z < y \leq b$; hence $z < b$.
    - This means $z \in (-\infty, b)$; hence $z \in J$.
  - Therefore, $\forall x, y \in J$, $\forall z \in \mathbb{R}$, if $x < z < y$, then $z \in J$.
- Finally, if $J = (-\infty, \infty)$, then $J = \mathbb{R}$, and the result is trivially true.

Thus, if J is an interval of $\mathbb{R}$, then $\forall x, y \in J$, $\forall z \in \mathbb{R}$, if $x < z < y$, then $z \in J$. □

The following quick but useful corollary is one half of a proposition stating that if I is an interval and $b \notin I$, then b is either an upper or lower bound of I. Hence, all real numbers will fall into at least one of these three categories: the upper bounds of I, the lower bounds of I, and I itself. We give the upper bound case here. The lower bound case is an exercise.

Corollary 2.2.10.

Let $I \subseteq \mathbb{R}$ be an interval. For all $b \in \mathbb{R}$, if $b \notin I$ and $\exists a \in I$, $a < b$, then $\forall x \in I$, $x < b$.

Proof.
Let $b \in \mathbb{R}$.
    Suppose $b \notin I$, $\exists a \in I$, $a < b$, and $\exists x \in I$, $b \leq x$.
        Choose $a \in I$ with $a < b$ and $x \in I$ with $b \leq x$.
        Since $x \in I$ and $b \notin I$, we have $b \neq x$.
        Therefore, $a < b < x$.
        Since $a, x \in I$, we then have $b \in I$ by theorem 2.2.9.
        We now have the contradiction $b \in I$ and $b \notin I$.
    Therefore, if $b \notin I$ and $\exists a \in I$, $a < b$, then $\forall x \in I$, $x < b$.
Therefore, for all $b \in \mathbb{R}$, if $b \notin I$ and $\exists a \in I$, $a < b$, then $\forall x \in I$, $x < b$. □

Recall that our goal in this section is to characterize the intervals as follows: For $J \subseteq \mathbb{R}$,

$$J \text{ is an interval if and only if } \forall x, y \in J,\ \forall z \in \mathbb{R},\ \text{if } x < z < y, \text{ then } z \in J.$$

Theorem 2.2.9 gives us one direction of this theorem, and so it only remains to show that the converse also holds:

Theorem 2.2.11.

If J is a subset of $\mathbb{R}$ such that $\forall x, y \in J$, $\forall z \in \mathbb{R}$, $x < z < y$ implies $z \in J$, then J is an interval. (This is the converse of Theorem 2.2.9.)

In the exercises that follow, the reader is expected to know and understand the statements of both theorems 2.2.9 and 2.2.11 and to use these results to prove statements about intervals. However, the *proof* of theorem 2.2.11 involves techniques that we have not sufficiently practiced (in particular its use of the completeness axiom). As such, the reproduction of this proof is beyond the expectations of a student in this course. Nevertheless, we have no intention of leaving the reader speculating about a mysterious and supposedly difficult proof. We include the proof here along with an explanation of the steps involved. The reader is invited to read and verify the proof, paying close attention to the use of completeness. The techniques involved can be compared to those used to prove the Archimedean property (theorem 1.1.34) which also makes use of completeness.

The Proof of Theorem 2.2.11

We of course begin the proof by assuming J is a subset of $\mathbb{R}$ satisfying the property that $\forall x, y \in J, \forall z \in \mathbb{R}, x < z < y$ implies $z \in J$. We must then show that J is an interval of one of the nine types. Which type will naturally depend on whether J is bounded or unbounded, and so we consider several different cases depending on the boundaries of the set J:

Proof.
Let J be a subset of $\mathbb{R}$ such that $\forall x, y \in J, \forall z \in \mathbb{R}, x < z < y$ implies $z \in J$.
Then, there are 5 cases:

1. $J = \emptyset$.
2. J is non-empty and bounded above and below.
3. J is non-empty and bounded below, unbounded above.
4. J is non-empty and bounded above, unbounded below.
5. J is non-empty and unbounded above and below.

We then exhaust these five cases one by one. The first case is easy:

Case 1: $J = \emptyset$.
Then J can be viewed as the degenerate interval $(0, 0)$.
That is, since $(0, 0) = \emptyset$, we have $J = (0, 0)$.
Therefore, J is an interval.

The second case requires more work. Since there are four types of bounded interval ((a, b), $(a, b]$, $[a, b)$, and $[a, b]$), in the case where J is non-empty and bounded, we must prove that J is of one of these four types. Due to the nesting of bounded intervals given in theorem 2.2.8, we can prove that J must be one of these four types by showing that

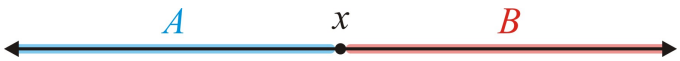
$$(a, b) \subseteq J \subseteq [a, b]$$

for some $a, b \in \mathbb{R}$. The task then becomes to find real numbers a and b for which $(a, b) \subseteq J \subseteq [a, b]$. To find such a and b, we turn to the completeness axiom.

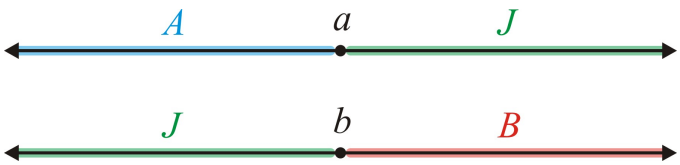
The completeness axiom

If A and B are non-empty subsets of $\mathbb{R}$ such that for all $a \in A$ and all $b \in B$, $a < b$, then there is an element $x \in \mathbb{R}$ such that for all $a \in A$, $a \leq x$ and for all $b \in B$, $x \leq b$.

Recall that the completeness axiom ensures that if we cut the real line into two pieces A and B, the cut must fall on a real number. That is, there is a real number x lying between all the points in piece A and the points in piece B.



To prove the existence of real numbers a and b for which $(a,b) \subseteq J \subseteq [a,b]$, we make two cuts: One separating J from its lower bounds, and another separating J from its upper bounds. That is, if A is the set of all lower bounds of J and B is the set of all upper bounds of J, we apply the completeness axiom to create the following pictures:



Combining these pictures, we have

For the a and b chosen in this way, we can then prove that $(a,b) \subseteq J \subseteq [a,b]$; hence J must be an interval of one of the four bounded types. The details of this case are as follows:

Case 2: J is non-empty and bounded above and below.
Let A be the set of lower bounds of J
and let B be the set of upper bounds of J; that is, let

$$A = \{\ell \in \mathbb{R} : \forall x \in J, \ell \leq x\} \text{ and } B = \{u \in \mathbb{R} : \forall x \in J, x \leq u\}.$$

Then, for all $\ell \in A$ and all $x \in J$, $\ell \leq x$.
Therefore, by completeness we can choose $a \in \mathbb{R}$ such that

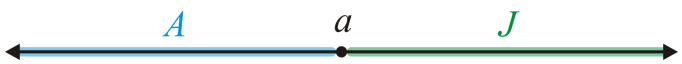
$$\forall \ell \in A,\ \ell \leq a \text{ and } \forall x \in J,\ a \leq x.$$

In the same way, $\forall x \in J$, $\forall u \in B$, $x \leq u$, so we can choose $b \in \mathbb{R}$ such that

$$\forall x \in J,\ x \leq b \text{ and } \forall u \in B,\ b \leq u.$$

We will prove that $(a, b) \subseteq J \subseteq [a, b]$.
Indeed, we established that $\forall x \in J,\ a \leq x$ and $\forall x \in J, x \leq b$,
so $\forall x \in J, a \leq x \leq b$; that is, $J \subset [a, b]$.
It remains to show that $(a, b) \subseteq J$.
To this end, let $t \in (a, b)$.
Then $a < t$ and $t < b$.
But, $\forall \ell \in A$, $\ell \leq a$, so $t \notin A$.
Since t is not a lower bound for J, we can choose $x \in J$ with $x < t$,
Similarly, since $t < b$, t is not an upper bound for J,
so we can choose $y \in J$ with $t < y$.
Thus, $x < t < y$, with $x, y \in J$; hence, by hypothesis $t \in J$.
This shows for all $t \in (a, b)$, $t \in J$. In other words, $(a, b) \subseteq J$.
In summary, $(a, b) \subseteq J \subseteq [a, b]$.
Therefore, $J = (a, b)$ or $J = (a, b]$ or $J = [a, b]$ or $J = [a, b)$, by theorem 2.2.8.
Therefore, J is an interval.

Case 3 (J is non-empty and bounded below, unbounded above) is somewhat similar to case 2. In this case, we find a real number a for which $(a, \infty) \subseteq J \subseteq [a, \infty)$; hence $J = (a, \infty)$ or $J = [a, \infty)$. To find such an a, we apply completeness, making a cut between J and the set A consisting of all lower bounds of J.



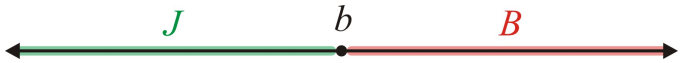
The details of this case are as follows:

Case 3: J is non-empty and bounded below, unbounded above.
As in Case 2, put $A = \{\ell \in \mathbb{R} : \forall x \in J, \ell \leq x\}$.
Then, for all $\ell \in A$ and all $x \in J$, $\ell \leq x$.
By completeness we can choose $a \in \mathbb{R}$ such that

$$\forall \ell \in A,\ \ell \leq a \text{ and } \forall x \in J,\ a \leq x.$$

We will show $(a, \infty) \subseteq J \subseteq [a, \infty)$.
Indeed, since $\forall x \in J$, $a \leq x$, we have $J \subseteq [a, \infty)$.
Next, let $t \in (a, \infty)$; that is, $a < t$.
As before, we have $t \notin A$, so we may choose $x \in J$, with $x < t$.
But J is not bounded above, so we can choose $y \in J$ with $t < y$.
Thus, $x, y \in J$ and $x < t < y$, so $t \in J$ by hypothesis.
Therefore, $(a, \infty) \subseteq J$.
We have shown $(a, \infty) \subseteq J \subseteq [a, \infty)$.
It follows that $J = (a, \infty)$ or $J = [a, \infty)$.
Thus, in case J is non-empty, bounded below and not above, J is an interval.

Case 4 (J is non-empty and bounded above, unbounded below) is very similar to case 3, only using the set B of upper bounds of J to obtain a b such that $J = (-\infty, b)$ or $J = (-\infty, b]$.



Case 4: J is non-empty and bounded above, unbounded below.
This time, put $B = \{u \in \mathbb{R} : \forall x \in J, x \leq u\}$.
Then, for all $x \in j$ and all $u \in B$, $x \leq u$.
By completeness we can choose $b \in \mathbb{R}$ such that

$$\forall x \in J,\ x \leq b \text{ and } \forall u \in B,\ b \leq x.$$

We will show $(-\infty, b) \subseteq J \subseteq (-\infty, b]$.
Indeed, since $\forall x \in J$, $x \leq b$, we have $J \subseteq (-\infty, b]$.
Next, let $t \in (-\infty, b)$; hence, $t < b$.
We then have $t \notin B$, so we may choose $y \in J$, with $t < y$.
Further, since J is not bounded below, we can choose $x \in J$ with $x < t$.
Thus, $x, y \in J$ and $x < t < y$, so $t \in J$ by hypothesis.
Therefore, $(-\infty, b) \subseteq J$.
We have shown $(-\infty, b) \subseteq J \subseteq (-\infty, b]$.
It follows that $J = (-\infty, b)$ or $J = (-\infty, b]$.
Therefore, J is an interval.

Finally, the case in which J is neither bounded above nor below is somewhat easier, in that it does not require completeness. The details are as follows:

Case 5: In case J is non-empty and neither bounded above nor bounded below, let $t \in (-\infty, +\infty) = \mathbb{R}$.

Since J is not bounded below, we can choose $x \in J$ with $x < t$.

Since J is not bounded above, we can choose $y \in J$ with $t < y$.

Then, $x, y \in J$ and $x < t < y$, so $t \in J$ also.

This shows that $t \in (-\infty, \infty) \subseteq J$.

But J is a subset of $\mathbb{R} = (-\infty, +\infty)$, so $J = (-\infty, \infty)$, an interval.

Thus, in all 5 cases J is an interval.

Therefore, if J is a subset of $\mathbb{R}$ such that $\forall x, y \in J$, $\forall z \in \mathbb{R}$, $x < z < y$ implies $z \in J$, then J is an interval. □

Exercises 2.2.

Prove the following propositions.

1. For every subset A of $\mathbb{R}$, A is bounded above if and only if $\exists k \in \mathbb{N}, \forall x \in A,\ x \leq k$.
2. For every subset A of $\mathbb{R}$, A is bounded if and only if $\exists k \in \mathbb{N}, \forall x \in A,\ |x| \leq k$.
3. $\forall a, b \in \mathbb{R}, (a, b) \subseteq (a, b] \subset [a, b]$.
4. $\forall a, b \in \mathbb{R}, (a, b) \subseteq [a, b) \subset [a, b]$.
5. $\forall a, b \in \mathbb{R}$, if $b \leq a$, then $(a, b] = \emptyset$. (So the empty set is an interval.)
6. $\forall a, b \in \mathbb{R}$, if $b < a$, then $[a, b] = \emptyset$.
7. $\forall a, b \in \mathbb{R}$, if $a = b$, then $[a, b] = \{a\}$.
8. $\forall a, b \in \mathbb{R}$, if $a \leq b$, then $[a, b] = (a, b) \cup \{a, b\}$.
9. $\forall x, y \in \mathbb{R}$, if $(-\infty, x) = (-\infty, y)$, then $x = y$.
10. $\forall x, y \in \mathbb{R}$, if $[x, \infty) = [y, \infty)$, then $x = y$.
11. $\forall a, b, x, y \in \mathbb{R}$, if $a \leq x$ and $y \leq b$, then $(x, y) \subseteq (a, b)$.
12. $\forall a, x \in \mathbb{R}$, if $a \leq x$, then $[x, \infty) \subseteq [a, \infty)$.
13. $\forall a, b \in \mathbb{R}_{\geq 0}$, if $[0, a) \subseteq [0, b)$, then $a \leq b$.
14. $\forall a \in \mathbb{R}$, if $(0, \infty) \subseteq [a, \infty)$, then $a \leq 0$.
15. $\forall a, b \in \mathbb{R}_{\geq 0}$, if $[0, a] = [0, b]$, then $a = b$.
16. $\forall a, b \in \mathbb{R}_{\geq 0}$, if $[0, a) = [0, b)$, then $a = b$.
17. $\forall a \in \mathbb{R}$, if $(0, \infty) \subseteq [a, \infty)$, then $(0, \infty) \subseteq (a, \infty)$.
18. $\forall a, b, c, d \in \mathbb{R}$, if $(a, b) \subseteq [c, d]$, then $(a, b) \subseteq (c, d)$.

Prove the following propositions about unions, intersections, and complements of intervals.

19. $\forall a, b, x, y \in \mathbb{R}$, if $x \in (a, b)$ and $b \in (x, y)$, then $(a, b) \cap (x, y) = (x, b)$.
20. $\forall a, b, x, y \in \mathbb{R}$, if $x \in (a, b)$ and $b \in (x, y)$, then $(a, b) \cup (x, y) = (a, y)$.
21. $\forall a, b, c, d \in \mathbb{R}$, $(a, b) \cap (c, d) = (e, f)$, where $e = \max(a, c)$ and $f = \min(b, d)$.
22. $\forall a, b, c, d \in \mathbb{R}$, $[a, b] \cap [c, d] = [e, f]$, where $e = \max(a, c)$ and $f = \min(b, d)$.
23. $\forall a, b \in \mathbb{R}$, $(a, \infty) \cap (b, \infty) = (c, \infty)$, where $c = \max(a, b)$.
24. $\forall a, b \in \mathbb{R}$, $(-\infty, a) \cap (-\infty, b) = (-\infty, c)$, where $c = \min(a, b)$.
25. $\forall a \in \mathbb{R}, \mathbb{R} \setminus (a, \infty) = (-\infty, a]$.
26. $\forall a, b \in \mathbb{R}, \mathbb{R} \setminus (a, b) = (-\infty, a] \cup [b, \infty)$.
27. $\forall a, b, c \in \mathbb{R}$, $[a, b] \cap (-\infty, c] = [a, u]$, where $u = \min(b, c)$.
28. $\forall a, b, c \in \mathbb{R}$, $[a, b] \cap [c, \infty) = [v, b]$, where $v = \max(a, c)$.
29. $\forall a, b, c, d \in \mathbb{R}$, $[a, b] \setminus (c, d) = [a, u] \cup [v, b]$, where $u = \min(b, c)$ and $v = \max(a, d)$.
30. $\forall a, b \in \mathbb{R}$, $[a, \infty) \setminus (b, \infty) = [a, b]$.
31. $\forall a, b, c \in \mathbb{R}$, if $(-\infty, a) \cap (b, c) \neq \emptyset$, then $(-\infty, a) \cup (b, c) = (-\infty, u)$, where $u = \max(a, c)$.
32. $\forall a, b, c \in \mathbb{R}$, if $(a, b) \cap (c, \infty) \neq \emptyset$, then $(a, b) \cup (c, \infty) = (v, b)$, where $v = \min(a, c)$.
33. $\forall a \in \mathbb{R}$, if $J \subseteq \mathbb{R}$ with $(a, \infty) \subseteq J \subseteq [a, \infty)$, then $J = (a, \infty)$ or $J = [a, \infty)$.
34. $\forall b \in \mathbb{R}$, if $J \subseteq \mathbb{R}$ with $(-\infty, b) \subseteq J \subseteq (-\infty, b]$, then $J = (-\infty, b)$ or $J = (-\infty, b]$.

Prove the following propositions using theorems 2.2.9 and 2.2.11.

35. Let I be an interval of $\mathbb{R}$. For all $a \in \mathbb{R}$, if $a \notin I$ and $\exists b \in I,\ a < b$, then $\forall x \in I,\ a < x$.
36. Let A and B be intervals in $\mathbb{R}$ with $A \cap B = \emptyset$. If $\exists a \in A, \exists b \in B,\ a < b$, then $\forall x \in A, \forall y \in B,\ x < y$.
37. The intersection of any two intervals is an interval.
38. Let $(I_k)_{k \in \mathbb{N}}$ be a sequence of intervals. Then $\forall n \in \mathbb{N}$, $\bigcap_{k=1}^{n} I_k$ is an interval.

Prove the following propositions characterizing bounded intervals.

39. $\forall a, b \in \mathbb{R}$, if $a < b$, then $(a, b) = \{x \in \mathbb{R} \mid \exists t \in (0, 1),\ x = (1 - t)a + tb\}$.
40. $\forall a, b \in \mathbb{R}$, if $a \leq b$, then $[a, b] = \{x \in \mathbb{R} \mid \exists t \in [0, 1],\ x = (1 - t)a + tb\}$.
41. $\forall a, b \in \mathbb{R}$, if $a \neq b$, then $(a, b) \cup (b, a) = \{x \in \mathbb{R} \mid \exists t \in (0, 1),\ x = (1 - t)a + tb\}$.
42. $\forall a, b \in \mathbb{R}$, $[a, b] \cup [b, a] = \{x \in \mathbb{R} \mid \exists t \in [0, 1],\ x = (1 - t)a + tb\}$.
43. $\forall a, b \in \mathbb{R}$, if $a < b$, then $(a, b] = \{x \in \mathbb{R} \mid \exists t \in (0, 1],\ x = (1 - t)a + tb\}$.
44. $\forall a, b \in \mathbb{R}$, if $a < b$, then $[a, b) = \{x \in \mathbb{R} \mid \exists t \in [0, 1),\ x = (1 - t)a + tb\}$.

2.3 Ideals of the Integers

Recall that for $a \in \mathbb{Z}$, the ideal of $\mathbb{Z}$ generated by a is the *set of multiples of a*. That is,

For $a \in \mathbb{Z}$:
$$\langle a \rangle = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = at\}.$$

These sets provide a convenient notation for expressing ideas related to the integers, including such ideas as the *greatest common divisor*, *least common multiple*, and the distinction between *prime* and *composite* integers. In many cases, the notation becomes less cumbersome and the ideas become more lucid and manageable when expressed in terms of ideals.

We first note that the set of *all* integers is an ideal. In fact, $\mathbb{Z}$ is the ideal generated by 1.

Proposition 2.3.1.

$\mathbb{Z} = \langle 1 \rangle$.

Proof.
Since $\mathbb{Z}$ is the universe of discourse in which the ideals are defined, we have $\langle 1 \rangle \subseteq \mathbb{Z}$.
Conversely, let $x \in \mathbb{Z}$.
    Put $t = x$.
        Then $x = (1)x = (1)t$.
    Therefore, $\exists t \in \mathbb{Z}$, $x = (1)t$.
    Hence, $x \in \langle 1 \rangle$.
Therefore, $\mathbb{Z} \subseteq \langle 1 \rangle$.
Hence $\mathbb{Z} = \langle 1 \rangle$. □

One particular complication that is avoided by speaking in terms of ideals is the distinction between positive and negative integers. Notice that $\gcd(15, 20)$ is the same as $\gcd(-15, 20)$, $\gcd(-15, -20)$, and so on. The same is true for the least common multiple. Likewise, we see that 5 is prime and -5 is also prime, in fact for $a \in \mathbb{Z}$, a is prime if and only if $-a$ is prime. In general, we see that the concepts of prime, composite, gcd, and lcm are unaffected by the *sign* of the integer. Considering positive and negative integers as different cases will then only add needless repetition to our proofs. The reader may already be familiar with the following notation:

Notation

The notation '$x = \pm y$' means '$x = y$ or $x = -y$'.

This is often used when one wants to speak about results that are true for an integer and its corresponding negative. For example, one may write 'if $x = \pm y$, then $x^2 = y^2$,' rather than 'if $x = y$ or $x = -y$ then $x^2 = y^2$.' Another common way of simplifying this notation is to write $|x| = |y|$, which we have seen is true if and only if $x = \pm y$. Our example could then be written as 'if $|x| = |y|$, then $x^2 = y^2$.' This notation may get us out of writing a long series of disjunctions when we express the *result*, but to ensure that the result holds for both the number and its negative will still require multiple cases in its *proof*. Thus it is only a shorthand notation used to *state* the result; it does not add clarity to an argument in support of the result. On the other hand, when we speak in terms of ideals, the issue of positives and negatives is avoided altogether. This is due to the following theorem:

Theorem 2.3.2.

For all $x, y \in \mathbb{Z}$, $\langle x \rangle = \langle y \rangle$ if and only if $x = \pm y$.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume $\langle x \rangle = \langle y \rangle$.
Since $x = 1(x)$, we have $x \in \langle x \rangle$.
Therefore, $x \in \langle y \rangle$.
Similarly, we have $y \in \langle x \rangle$.
It follows that $\exists a \in \mathbb{Z}$, $x = ay$ and $\exists b \in \mathbb{Z}$, $y = bx$.
Therefore, $x = abx$; hence $x(1 - ab) = 0$
By axiom FZ, we then have either $x = 0$ or $1 - ab = 0$.
Case 1: $x = 0$.
Then $y = bx = b(0) = 0$.
In this case, we have $x = y$; hence $x = \pm y$.
Case 2: $1 - ab = 0$.
Therefore, $ab = 1$; hence $|a| \leq 1$ by proposition 1.2.8.
Further, since $ab = 1 \neq 0$, we have $a \neq 0$ and hence $|a| \neq 0$.
We now have, $0 < |a| \leq 1$; hence $|a| = 1$.
Therefore, $a = 1$ or $a = -1$.
Since $x = ay$, we then have either $x = (1)y$ or $x = (-1)y$.
Therefore, $x = \pm y$.
Therefore, if $\langle x \rangle = \langle y \rangle$, then $x = \pm y$.
Conversely, assume $x = \pm y$.
In the case $x = y$ we have $\langle x \rangle = \langle y \rangle$,
hence it only remains to consider the case $x = -y$.
Let $a \in \langle x \rangle$.
Then $\exists t \in \mathbb{Z}$, $a = xt$. Choose such a t.
Put $s = -t$.
$a = xt = (-y)t = (-t)y = sy$.
Therefore, $\exists s \in \mathbb{Z}$, $a = sy$.
Therefore, $a \in \langle y \rangle$.
Hence, $\langle x \rangle \subseteq \langle y \rangle$.
Similarly, since $y = -x$, we have $\langle y \rangle \subseteq \langle x \rangle$.
Therefore, $\langle x \rangle = \langle y \rangle$.
Therefore, if $x = \pm y$, then $\langle x \rangle = \langle y \rangle$.
Therefore, for all $x, y \in \mathbb{Z}$, $\langle x \rangle = \langle y \rangle$ if and only if $x = \pm y$. □

A remark about the word 'similarly'

The use of the word 'similarly' in a mathematical proof indicates a very particular circumstance: 'Similarly' means that the proof of the statement is *exactly the same* as the proof above, with only a suitable alteration of the notation. In the example above, since the fact that $x = -y$ implies that $y = -x$, the letters x and y can be interchanged without affecting the truth of the assumption. Hence there is no logical difference between the role of x and the role of y in our proof; there is only a notational difference. The word 'similarly' indicates that if the roles of x and y are reversed in the argument that $x = -y$ implies $\langle x \rangle \subseteq \langle y \rangle$, the result will be a correct proof of the statement that $y = -x$ implies $\langle y \rangle \subseteq \langle x \rangle$. The careful reader should verify that this is the case, whenever the word 'similarly' is encountered in a mathematical proof.

The previous proposition shows that there is no difference between the ideal generated by a positive number and that generated by its corresponding negative. That is, $\langle x \rangle = \langle -x \rangle$. Further, the ideal is generated *only* by this pair. Therefore, to speak of an ideal $\langle a \rangle$ is to speak simultaneously about a and $-a$.

The ideals also have a convenient property: that membership in the set implies a subset relation. Hence, any idea that can be expressed in terms of membership in an ideal can also be expressed in terms of subsets, and vice versa.

Theorem 2.3.3.

For all $x, y \in \mathbb{Z}$, $x \in \langle y \rangle$ if and only if $\langle x \rangle \subseteq \langle y \rangle$.

Proof.
Let $x, y \in \mathbb{Z}$.
    Assume $x \in \langle y \rangle$.
        Then $\exists t \in \mathbb{Z}$, $x = ty$.
        Let $a \in \langle x \rangle$.
            Then $\exists s \in \mathbb{Z}$, $a = sx$.
            Put $r = st$.
                Then $a = sx = sty = ry$.
            Hence, $\exists r \in \mathbb{Z}$, $a = ry$.
            Therefore, $a \in \langle y \rangle$.
        Therefore, $\langle x \rangle \subseteq \langle y \rangle$.
    Therefore, if $x \in \langle y \rangle$, then $\langle x \rangle \subseteq \langle y \rangle$.
    Conversely, assume $\langle x \rangle \subseteq \langle y \rangle$.
        Since $x = (1)x$, we have $x \in \langle x \rangle$.
        Since $x \in \langle x \rangle$ and $\langle x \rangle \subseteq \langle y \rangle$, we have $x \in \langle y \rangle$.
    Therefore, if $\langle x \rangle \subseteq \langle y \rangle$, then $x \in \langle y \rangle$.
Therefore, for all $x, y \in \mathbb{Z}$, $x \in \langle y \rangle$ if and only if $\langle x \rangle \subseteq \langle y \rangle$. □

This means that **for ideals** the *element-set* relation $x \in \langle y \rangle$ can always be expressed as a *subset* relation $\langle x \rangle \subseteq \langle y \rangle$; hence all concepts that are expressible in terms of ideals can be expressed simply by the subset relations between the ideals themselves. To examine the significance of such subset relations in the integers, we look at an example of two integers for which this relation holds.

Proposition 2.3.4.

$\langle 6 \rangle \subseteq \langle 3 \rangle$.

Proof.
Let $x \in \langle 6 \rangle$.
    Then $\exists t \in \mathbb{Z}$, $x = 6t$.
    Put $s = 2t$.
        $x = 6t = 3(2t) = 3s$.
    Therefore, $\exists s \in \mathbb{Z}$, $x = 3s$.
    Hence, $x \in \langle 3 \rangle$.
Therefore, $\langle 6 \rangle \subseteq \langle 3 \rangle$. □

Many students find this counter-intuitive at first, since the order of the ideals is an inversion of the order of the numbers generating them. That is $\langle 6 \rangle \subseteq \langle 3 \rangle$ looks like a reversal of the well-known ordering $3 \leq 6$. This is in fact almost always the case. Indeed, if $\langle y \rangle \subseteq \langle x \rangle$ and $y \neq 0$, then $|x| \leq |y|$. The reason for this is in part due to the following theorem:

Theorem 2.3.5.

For all $x, y \in \mathbb{Z}$, x divides y if and only if $\langle y \rangle \subseteq \langle x \rangle$.

Proof.
Let $x, y \in \mathbb{Z}$.
    Assume x divides y.
        Then $\exists t \in \mathbb{Z}$, $y = xt$.
        Hence, $y \in \langle x \rangle$.
        Therefore, $\langle y \rangle \subseteq \langle x \rangle$ by theorem 2.3.3.
    Therefore, if x divides y then $\langle y \rangle \subseteq \langle x \rangle$.
    Conversely, assume $\langle y \rangle \subseteq \langle x \rangle$.
        Then $y \in \langle x \rangle$ by theorem 2.3.3.
        That is, $\exists t \in \mathbb{Z}$, $y = xt$.
        Hence, x divides y.
    Therefore, if $\langle y \rangle \subseteq \langle x \rangle$, then x divides y.
Therefore, for all $x, y \in \mathbb{Z}$, x divides y if and only if $\langle y \rangle \subseteq \langle x \rangle$. □

Recall from proposition 1.2.8 that if x divides y and $y \neq 0$, then $|x| \leq |y|$. We then see that since the statement about ideals '$\langle y \rangle \subseteq \langle x \rangle$,' being equivalent to the statement 'x divides y,' must also imply that $|x| \leq |y|$ in the case where $y \neq 0$. Hence, in all but the case where $y = 0$, we have that $\langle y \rangle \subseteq \langle x \rangle$ implies $|x| \leq |y|$. Thus it is a common occurrence that the ordering of the ideals is contrary to the ordering of the numbers that generate them.

The above theorem is important for another reason: It shows that the set theoretic statement $\langle y \rangle \subseteq \langle x \rangle$ means the same thing as the statement x divides y in the integers. Hence, when speaking about integers dividing other integers, which is the fundamental concept behind such ideas as prime numbers, composite numbers, gcd, lcm , and factorization, we can use the language of ideals.

Algebraic Characterization of Ideals

Ideals, in addition to their descriptive power, have a number of other properties that make them particularly easy to work with. For example, they are closed under addition; that is,

$$\forall a, x, y \in \mathbb{Z}, \text{ if } x \in \langle a \rangle \text{ and } y \in \langle a \rangle, \text{ then } x + y \in \langle a \rangle.$$

They are also closed under the unary operation given by $x \mapsto -x$, in the sense that

$$\forall a, x \in \mathbb{Z}, \text{ if } x \in \langle a \rangle, \text{ then } -x \in \langle a \rangle.$$

Further, since $x \in \langle a \rangle$ implies $\langle x \rangle \subseteq \langle a \rangle$, we see that the ideals contain *all multiples of their elements*. That is,

$$\forall x, a \in \mathbb{Z}, \text{ if } x \in \langle a \rangle, \text{ then } \forall t \in \mathbb{Z}, \ xt \in \langle a \rangle.$$

The proofs of the above three properties are left as exercises. However, we will show here that these three properties completely characterize the ideals of the integers, in the sense that any non-empty set satisfying these properties must be equal to $\langle a \rangle$ for some $a \in \mathbb{Z}$.

To begin, we will show that the third property discussed above follows from the first two. That is, if a non-empty subset of the integers is closed under addition and negation, then it necessarily contains all multiples of its elements. To prove this, we recall a form of the principle of mathematical induction that was proved as an exercise in section 1.2: For a subset $A \subseteq \mathbb{Z}$,

$$\text{if } 0 \in A \text{ and } \forall n \in \mathbb{Z}, \ n \in A \Rightarrow n + 1 \in A \text{ and } n - 1 \in A, \text{ then } A = \mathbb{Z}.$$

Proposition 2.3.6.

Let $S \subseteq \mathbb{Z}$, with $S \neq \emptyset$. If $\forall x, y \in S$, $x + y \in S$ and $\forall x \in S$, $-x \in S$, then $\forall x \in S$, $\forall a \in \mathbb{Z}$, $ax \in S$.

Proof.
Let $S \subseteq \mathbb{Z}$, with $S \neq \emptyset$.
Assume $\forall x, y \in S$, $x + y \in S$ and $\forall x \in S$, $-x \in S$.
    Let $x \in S$.
        Let $A = \{a \in \mathbb{Z} \mid ax \in S\}$.
            Since $x \in S$, we have $-x \in S$; hence $x + (-x) \in S$.
            This gives us $0x \in S$; hence $0 \in A$.
            Let $n \in \mathbb{Z}$, and assume $n \in A$.
                Then $nx \in S$.
                Since $x \in S$ as well, we have $nx + x \in S$.
                Hence, $(n + 1)x \in S$, which means $n + 1 \in A$.
                Further, since $x \in S$, we have $-x \in S$.
                Therefore, $nx + (-x) \in S$; hence $(n - 1)x \in S$.
                This gives us $n - 1 \in A$.
            Therefore, $\forall n \in \mathbb{Z}$, if $n \in A$, then $n + 1 \in A$ and $n - 1 \in A$.
        Therefore, by the PMI, $A = \mathbb{Z}$.
        Therefore, $\forall a \in \mathbb{Z}$, $ax \in S$.
    Therefore, $\forall x \in S$, $\forall a \in \mathbb{Z}$, $ax \in S$.
Q.E.D. □

The above proposition refers to a certain abstract type of subset of the integers. The subset S in question, being closed under addition and negation (and hence also containing all multiples of its elements), in some sense contains much of the algebraic structure of the integers themselves. Yet, at this point the set is merely a hypothetical entity. Exactly what such sets look like remains to be determined. Applying the same argument that was used to prove Bezout's identity (theorem 1.2.11), we can show that any such set must be an ideal $\langle a \rangle$ for some $a \in \mathbb{Z}$. The proof, as in the case of Bezout's identity, uses the well-ordering property to select the smallest element of the set S, then uses the division algorithm to show that S is exactly the ideal generated by its smallest element.

Theorem 2.3.7.

Let $S \subseteq \mathbb{Z}$, with $S \neq \emptyset$. If $\forall x, y \in S$, $x + y \in S$ and $\forall x \in S$, $-x \in S$, then $\exists g \in \mathbb{Z}$, $S = \langle g \rangle$.

Proof.
Let $S \subseteq \mathbb{Z}$, with $S \neq \emptyset$.
Assume $\forall x, y \in S$, $x + y \in S$ and $\forall x \in S$, $-x \in S$.
    First consider the case where $S = \{0\}$.
        Letting $x \in \langle 0 \rangle$ gives us that $\exists t \in \mathbb{Z}$, $x = 0t$.
            In this case, $x = 0$; hence $x \in S$.
        Therefore, $\langle 0 \rangle \subseteq S$.
        Conversely, letting $x \in \{0\}$ gives us $x = 0$; hence $x \in \langle 0 \rangle$.
        Therefore, $S \subseteq \langle 0 \rangle$.
        Therefore, in this case, we have $S = \langle 0 \rangle$.
    Next, we consider the case where $S \neq \{0\}$.
        Since $S \neq \emptyset$ and $S \neq \{0\}$, we may choose $x \in S$ with $x \neq 0$.
        If $x > 0$, then $x \in S \cap \mathbb{N}$.
        If $x < 0$, then $-x \in S \cap \mathbb{N}$.
        In both cases, we have $S \cap \mathbb{N} \neq \emptyset$.
        Applying the well-ordering property,
        choose g to be the smallest element of $S \cap \mathbb{N}$.
        We claim that $S = \langle g \rangle$.
        Indeed, let $x \in S$.
            Applying the division algorithm, choose $q, r \in \mathbb{Z}$ with $x = qg + r$
            and $0 \leq r < g$.
            Since $g \in S$, we have $-qg \in S$ by proposition 2.3.6.
            Since $x \in S$ as well, we have $x + (-qg) \in S$.
            Since $r = x - qg$, this means that $r \in S$.
            Since $r < g$ and g is the smallest element of $S \cap \mathbb{N}$, we have $r \notin S \cap \mathbb{N}$.
            Therefore, either $r \notin S$ or $r \notin \mathbb{N}$.
            Since we have shown that $r \in S$, it must be the case that $r \notin \mathbb{N}$.
            Therefore, $r \leq 0$.
            Since $0 \leq r$ and $r \leq 0$, we have that $r = 0$.
            Therefore, $x = qg + 0$; hence $\exists q \in \mathbb{Z}$, $x = qg$.
            Therefore, $x \in \langle g \rangle$.
        Therefore, $S \subseteq \langle g \rangle$.
        Conversely, let $x \in \langle g \rangle$.
            Then, $\exists t \in \mathbb{Z}$, $x = gt$.
            Since $g \in S$ and $t \in \mathbb{Z}$, we have $gt \in S$ by proposition 2.3.6.
            Therefore, $x \in S$.
        Hence, $\langle g \rangle \subseteq S$.
        Therefore, $S = \langle g \rangle$.
    In both cases, $\exists g \in \mathbb{Z}$, $S = \langle g \rangle$.
Therefore, if $\forall x, y \in S$, $x + y \in S$ and $\forall x \in S$, $-x \in S$, then $\exists g \in \mathbb{Z}$, $S = \langle g \rangle$. □

Set Operations on Ideals

An example in section 2.1 (example 2.1.13) showed that $\langle 2 \rangle \cap \langle 3 \rangle = \langle 6 \rangle$. Hence, the intersection of the ideals $\langle 2 \rangle$ and $\langle 3 \rangle$ yields another ideal. For another such example, consider the following:

Example 2.3.8.

$\langle 9 \rangle \cap \langle 15 \rangle = \langle 45 \rangle$.

Proof.
Let $x \in \langle 9 \rangle \cap \langle 15 \rangle$.
Then $x \in \langle 9 \rangle$ and $x \in \langle 15 \rangle$.
Choose $a \in \mathbb{Z}$ with $x = 9a$ and choose $b \in \mathbb{Z}$ with $x = 15b$.
Put $c = 2b - a$.
$x = 6x - 5x = 6(15b) - 5(9a) = 45(2b) - 45a = 45(2b - a) = 45c$.
Therefore, $\exists c \in \mathbb{Z}$, $x = 45c$.
Hence $x \in \langle 45 \rangle$.
Therefore, $\langle 9 \rangle \cap \langle 15 \rangle \subseteq \langle 45 \rangle$.
Conversely, let $x \in \langle 45 \rangle$.
Choose $s \in \mathbb{Z}$ with $x = 45s$.
Put $t = 5s$.
$x = 45s = 9(5s) = 9t$.
Therefore, $\exists t \in \mathbb{Z}$, $x = 9t$.
Hence, $x \in \langle 9 \rangle$.
Put $r = 3s$.
$x = 45s = 15(3s) = 15r$.
Therefore, $\exists t \in \mathbb{Z}$, $x = 15r$.
Therefore, $x \in \langle 15 \rangle$.
We now have $x \in \langle 9 \rangle$ and $x \in \langle 15 \rangle$.
Therefore, $x \in \langle 9 \rangle \cap \langle 15 \rangle$.
Therefore, $\langle 45 \rangle \subseteq \langle 9 \rangle \cap \langle 15 \rangle$.
Therefore, $\langle 9 \rangle \cap \langle 15 \rangle = \langle 45 \rangle$. □

It is in fact always true that the intersection of two ideals is an ideal. This can be shown quite easily if we appeal to the algebraic characterization of ideals as those sets that are closed under addition and negation and contain the multiples of all of their elements.

Proposition 2.3.9.

For all $x, y \in \mathbb{Z}$, $\exists g \in \mathbb{Z}$, $\langle x \rangle \cap \langle y \rangle = \langle g \rangle$.

Proof.
Let $x, y \in \mathbb{Z}$.
  Let $a, b \in \langle x \rangle \cap \langle y \rangle$.
    Then $a \in \langle x \rangle$ and $a \in \langle y \rangle$ and $b \in \langle x \rangle$ and $b \in \langle y \rangle$.
    Choose $q, r, s, t \in \mathbb{Z}$ with $a = qx$, $a = ry$, $b = sx$, and $b = ty$.
    Put $u = q + s$.
      Then $a + b = qx + sx = (q + s)x = ux$.
    Therefore, $a + b \in \langle x \rangle$.
    Put $v = r + t$.
      Then $a + b = ry + ty = (r + t)y = vy$.
    Therefore, $a + b \in \langle y \rangle$.
    Hence, $a + b \in \langle x \rangle \cap \langle y \rangle$.
  Therefore, $\forall a, b \in \langle x \rangle \cap \langle y \rangle$, $a + b \in \langle x \rangle \cap \langle y \rangle$.
  Next, let $a \in \langle x \rangle \cap \langle y \rangle$.
    Once again, choose $q, r \in \mathbb{Z}$ with $a = qx$ and $a = ry$.
    This time, put $u = -q$.
      Then $-a = -qx = ux$.
    Hence $-a \in \langle x \rangle$.
    Put $v = -r$.
      Then, $-a = -ry = vy$.
    Hence, $-a \in \langle y \rangle$.
    Therefore, $-a \in \langle x \rangle \cap \langle y \rangle$.
  Therefore, $\forall a \in \langle x \rangle \cap \langle y \rangle$, $-a \in \langle x \rangle \cap \langle y \rangle$.
  By theorem 2.3.7, we then have $\exists g \in \mathbb{Z}$, $\langle x \rangle \cap \langle y \rangle = \langle g \rangle$. □

In the above proposition, the existence of the integer a that generates the intersection $\langle x \rangle \cap \langle y \rangle$ is ultimately known only via the well-ordering property. That is, the only clue we have as to the identity of a, in relation to x and y, is that it is the *smallest non-negative* element of $\langle x \rangle \cap \langle y \rangle$. We can do better than this. If we look closely at the connection between ideals and '*division*' in the integers, we see that elements of the intersection $\langle x \rangle \cap \langle y \rangle$ are elements of both $\langle x \rangle$ and $\langle y \rangle$. We also know that the elements of $\langle x \rangle$ are the *multiples* of x and that the elements of $\langle y \rangle$ are the *multiples* of y. Hence, the elements of $\langle x \rangle \cap \langle y \rangle$ must be the *common multiples* of both x and y. The generator a in the proposition above, being the smallest non-negative such element, must then be the *least common multiple* of x and y. Recall the definition of the *least common multiple* (definition 1.2.5):

For $x, y, f \in \mathbb{Z}$, with $x \neq 0$ and $y \neq 0$, f is the **least common multiple** of x and y means

1. $f > 0$,
2. x divides f and y divides f, and
3. $\forall a \in \mathbb{Z}$, if x divides a and y divides a, then $f \leq |a|$.

We denote that g is the least common multiple of x and y by $f = \operatorname{lcm}(x, y)$.

Theorem 2.3.10.

For all $x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\langle x \rangle \cap \langle y \rangle = \langle \operatorname{lcm}(x, y) \rangle$.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume $x \neq 0$ and $y \neq 0$.
Then $\langle x \rangle \cap \langle y \rangle \neq \{0\}$, since $xy \in \langle x \rangle \cap \langle y \rangle$, and $xy \notin \{0\}$.
By the previous proposition, we have $\exists g \in \mathbb{Z}$, $\langle x \rangle \cap \langle y \rangle = \langle g \rangle$.
Since for every $a \in \mathbb{Z}$, we have $\langle a \rangle = \langle -a \rangle$, we may choose $f \in \mathbb{Z}$ with $\langle x \rangle \cap \langle y \rangle = \langle f \rangle$ and $f \geq 0$.
In fact, since $\langle x \rangle \cap \langle y \rangle \neq \{0\}$, we have $f > 0$. (1)
Since $f \in \langle x \rangle \cap \langle y \rangle$, we have $f \in \langle x \rangle$ and $f \in \langle y \rangle$.
Therefore, x divides f and y divides f. (2)
Let $a \in \mathbb{Z}$, and assume x divides a and y divides a.
Then $a \in \langle x \rangle$ and $a \in \langle y \rangle$.
Hence, $a \in \langle x \rangle \cap \langle y \rangle$.
Therefore, $a \in \langle f \rangle$.
This means that f divides a; hence $|f| \leq |a|$.
Since $f > 0$, this means $f \leq |a|$.
Therefore, $\forall a \in \mathbb{Z}$, if x divides a and y divides a, then $f \leq |a|$. (3)
By (1), (2), and (3), we have that $f = \operatorname{lcm}(x, y)$.
Therefore, $\langle x \rangle \cap \langle y \rangle = \langle \operatorname{lcm}(x, y) \rangle$.
Therefore, if $x \neq 0$ and $y \neq 0$, then $\langle x \rangle \cap \langle y \rangle = \langle \operatorname{lcm}(x, y) \rangle$.
Therefore, for all $x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\langle x \rangle \cap \langle y \rangle = \langle \operatorname{lcm}(x, y) \rangle$. □

Unlike the intersection, the union of two ideals is not necessarily an ideal. For example, consider the union $\langle 2 \rangle \cup \langle 3 \rangle$. It is easy to see that $2 \in \langle 2 \rangle \cup \langle 3 \rangle$ and $3 \in \langle 2 \rangle \cup \langle 3 \rangle$, but $5 \notin \langle 2 \rangle \cup \langle 3 \rangle$. This shows that the union $\langle 2 \rangle \cup \langle 3 \rangle$ is not closed under addition. However, all ideals are closed under addition (the proof of this is an exercise). It follows that $\langle 2 \rangle \cup \langle 3 \rangle$ cannot possibly be an ideal. There is however another way to combine ideals that will always result in an ideal:

Definition 2.3.1. For $a, b \in \mathbb{Z}$, we define the **sum of ideals** $\langle a \rangle + \langle b \rangle$ to be the set

$$\langle a \rangle + \langle b \rangle = \{x \in \mathbb{Z} \mid \exists y \in \langle a \rangle, \exists z \in \langle b \rangle,\ x = y + z\}.$$

We can view the set $\langle a \rangle + \langle b \rangle$ as the collection of all sums of elements from $\langle a \rangle$ and $\langle b \rangle$. That is, the set of all numbers that can be expressed as the sum of a multiple of a and a multiple of b. It should be noted that unlike the intersection, the sum of ideals is not *purely* set-theoretic. That is, it cannot be defined for arbitrary sets, since it makes use of the *addition* operation that is defined for the integers. In fact, it is the *elements* of the sets that are actually being added, not the sets themselves. Hence, it is only because we can add integers together that we can have a sensible definition of the addition of ideals of the integers. We could not for example extend the notion of addition of sets to collections of apples or people, since we do not have the binary operation of addition defined on such objects. The *intersection* and *union* of sets, on the other hand, are defined for all sets regardless of the universe of discourse.

That the sum of two ideals is itself an ideal can be shown using the algebraic characterization of ideals given in theorem 2.3.7. That is, any set that is closed under addition and negation is an ideal $\langle a \rangle$ for some integer a.

Proposition 2.3.11.

For all $x, y \in \mathbb{Z}$, $\exists g \in \mathbb{Z}$, $\langle x \rangle + \langle y \rangle = \langle g \rangle$.

Proof.
Let $x, y \in \mathbb{Z}$.
  Let $a, b \in \langle x \rangle + \langle y \rangle$.
    Choose $q, r, s, t \in \mathbb{Z}$ with $a = qx + ry$, $b = sx + ty$.
    Put $u = q + s$ and $v = r + t$.
      Then $a + b = qx + ry + sx + ty = (q + s)x + (r + t)y = ux + vy$.
    Therefore, $a + b \in \langle x \rangle + \langle y \rangle$.
  Therefore, $\forall a, b \in \langle x \rangle + \langle y \rangle$, $a + b \in \langle x \rangle + \langle y \rangle$.
  Next, let $a \in \langle x \rangle + \langle y \rangle$.
    Once again, choose $q, r \in \mathbb{Z}$ with $a = qx + ry$.
    This time, put $u = -q$ and $v = -r$.
      Then, $-a = -(qx + ry) = -qx + (-ry) = ux + vy$.
    Hence, $-a \in \langle x \rangle + \langle y \rangle$.
  Therefore, $\forall a \in \langle x \rangle + \langle y \rangle$, $-a \in \langle x \rangle + \langle y \rangle$.
  By theorem 2.3.7, we then have $\exists g \in \mathbb{Z}$, $\langle x \rangle + \langle y \rangle = \langle g \rangle$. □

Just as we did for the intersection of two ideals, by examining the relationship between ideals and the concept of *division* in the integers, we can determine the identity of the generator a in the above proposition. The result is quite nice; the sum of ideals $\langle x\rangle + \langle y\rangle$ is generated by the *greatest common divisor* of x and y. Recall the definition (definition 1.2.4):

For $x, y, g \in \mathbb{Z}$, with $x \neq 0$ and $y \neq 0$, g is the **greatest common divisor** of x and y means

1. $g > 0$,
2. g divides x and g divides y, and
3. $\forall a \in \mathbb{Z}$, if a divides x and a divides y, then $g \geq a$.

We denote that g is the greatest common divisor of x and y by $g = \gcd(x, y)$.

Theorem 2.3.12.

For all $x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\langle x\rangle + \langle y\rangle = \langle \gcd(x, y)\rangle$.

Proof.
Let $x, y \in \mathbb{Z}$.
Assume $x \neq 0$ and $y \neq 0$.
Then $\langle x\rangle + \langle y\rangle \neq \{0\}$, since $x = (1)x + (0)y \in \langle x\rangle + \langle y\rangle$, and $x \notin \{0\}$.
By the previous proposition, we have $\exists g \in \mathbb{Z}$, $\langle x\rangle + \langle y\rangle = \langle g\rangle$.
Since for every $a \in \mathbb{Z}$, we have $\langle a\rangle = \langle -a\rangle$, we may choose $g \in \mathbb{Z}$ with $\langle x\rangle + \langle y\rangle = \langle g\rangle$ and $g \geq 0$.
Since $\langle x\rangle + \langle y\rangle \neq \{0\}$, we have $g > 0$. (1)
Since $x = (1)x + (0)y$, we have $x \in \langle x\rangle + \langle y\rangle$.
Therefore, $x \in \langle g\rangle$ and hence g divides x.
Similarly, $y \in \langle x\rangle + \langle y\rangle$, which means $y \in \langle g\rangle$ and hence g divides y.
Therefore, g divides x and g divides y. (2)
Let $a \in \mathbb{Z}$, and assume a divides x and a divides y.
Choose $s, t \in \mathbb{Z}$ with $x = as$ and $y = at$.
Since $g \in \langle g\rangle$, we have $g \in \langle x\rangle + \langle y\rangle$.
Therefore, we can choose $q, r \in \mathbb{Z}$, $g = xq + yr$.
Then $g = asq + atr = a(sq + tr)$; hence $g \in \langle a\rangle$.
Therefore, a divides g; hence $|a| \leq |g|$.
Since $a \leq |a|$ and $g = |g|$, this gives us $a \leq g$.
Therefore, $\forall a \in \mathbb{Z}$, if a divides x and a divides y, then $a \leq g$. (3)
By (1), (2), and (3), we have that $g = \gcd(x, y)$.
Therefore, $\langle x\rangle + \langle y\rangle = \langle \gcd(x, y)\rangle$.
Therefore, if $x \neq 0$ and $y \neq 0$, then $\langle x\rangle + \langle y\rangle = \langle \gcd(x, y)\rangle$.
Therefore, for all $x, y \in \mathbb{Z}$, if $x \neq 0$ and $y \neq 0$, then $\langle x\rangle + \langle y\rangle = \langle \gcd(x, y)\rangle$. □

Characterization of Prime Numbers

Recall the definition of a prime natural number (definition 1.2.10):

For $x \in \mathbb{N}$, x is prime means $x \neq 1$ and $\forall a, b \in \mathbb{N}$, if $x = ab$, then either $a = 1$ or $b = 1$.

Since we have already seen that $\langle 1 \rangle = \mathbb{Z}$, the statement $x \neq 1$ can be written as $\langle x \rangle \neq \mathbb{Z}$. Further, it is fairly clear that in the event that $x = ab$, to say $b = 1$ is equivalent to saying $a = x$ in the case where $x \neq 0$. That is, the characterization of x being prime given above could be equivalently expressed as

$$\langle x \rangle \neq \mathbb{Z} \text{ and } \forall a, b \in \mathbb{Z}, \text{ if } x = ab, \text{ then } \langle a \rangle = \mathbb{Z} \text{ or } \langle a \rangle = \langle x \rangle.$$

The expression $x = ab$ also has an interpretation in terms of ideals. Since it indicates that x is a multiple of a, the equation $x = ab$ implies that $\langle x \rangle \subseteq \langle a \rangle$. This suggests the following interpretation of the statement 'x is prime':

$$\langle x \rangle \neq \mathbb{Z} \text{ and } \forall a \in \mathbb{Z}, \text{ if } \langle x \rangle \subseteq \langle a \rangle, \text{ then } \langle a \rangle = \mathbb{Z} \text{ or } \langle a \rangle = \langle x \rangle.$$

For example, consider the following proposition:

Proposition 2.3.13.

$\forall a \in \mathbb{Z}$, if $\langle 2 \rangle \subseteq \langle a \rangle$, then $\langle a \rangle = \mathbb{Z}$ or $\langle a \rangle = \langle 2 \rangle$.

Proof.
Let $a \in \mathbb{Z}$.
    Assume $\langle 2 \rangle \subseteq \langle a \rangle$.
        Since $2 \in \langle 2 \rangle$, we then have $2 \in \langle a \rangle$.
        Therefore, a divides 2; hence $|a| \leq 2$.
        Therefore, $a = \pm 1$ or $a = \pm 2$.
        Case 1: $a = \pm 1$.
            In this case, $\langle a \rangle = \langle 1 \rangle = \mathbb{Z}$.
            Therefore, $\langle a \rangle = \mathbb{Z}$ or $\langle a \rangle = \langle 2 \rangle$.
        Case 2: $a = \pm 2$.
            In this case, $\langle a \rangle = \langle 2 \rangle$.
            Therefore, $\langle a \rangle = \mathbb{Z}$ or $\langle a \rangle = \langle 2 \rangle$.
    Therefore, if $\langle 2 \rangle \subseteq \langle a \rangle$, then $\langle a \rangle = \mathbb{Z}$ or $\langle a \rangle = \langle 2 \rangle$.
Therefore, $\forall a \in \mathbb{Z}$, if $\langle 2 \rangle \subseteq \langle a \rangle$, then $\langle a \rangle = \mathbb{Z}$ or $\langle a \rangle = \langle 2 \rangle$. □

The fact that the only divisors of 2 are -1, 1, -2, and 2 (that is, 2 is prime) certainly plays a key role in the above proof, and one may be able to see that the truth of the set-theoretic concept in the above proposition is in some way related to the primeness of 2. It can be somewhat enlightening to examine exactly what the statement

$$\forall a \in \mathbb{Z}, \text{, if } \langle 2\rangle \subseteq \langle a\rangle, \text{ then } \langle a\rangle = \mathbb{Z} \text{ or } \langle a\rangle = \langle 2\rangle.$$

indicates about the ideal $\langle 2\rangle$. Essentially, this is saying that the ideal $\langle 2\rangle$ is not contained in any strictly larger ideal, except the all encompassing ideal that is $\mathbb{Z}$ itself. That is, one *cannot* fit an ideal $\langle a\rangle$ between $\langle 2\rangle$ and $\mathbb{Z}$ in the sense that $\langle 2\rangle \subsetneq \langle a\rangle \subsetneq \mathbb{Z}$. In this way, $\langle 2\rangle$ is as *large* as an ideal can be without being all of $\mathbb{Z}$; the next larger ideal is the entire set $\mathbb{Z}$. The proof that this *maximality* of ideals is entwined with the notion of *prime* in the integers is no more difficult than the proof of the special case $\langle 2\rangle$ given above:

Proposition 2.3.14.

$\forall x \in \mathbb{Z}$, if x is prime, then $\forall a \in \mathbb{Z}$, if $\langle x\rangle \subseteq \langle a\rangle$, then $\langle a\rangle = \mathbb{Z}$ or $\langle a\rangle = \langle x\rangle$.

Proof.
Let $x \in \mathbb{Z}$.
    Assume x is prime.
        Let $a \in \mathbb{Z}$.
            Assume $\langle x\rangle \subseteq \langle a\rangle$.
                Since $x \in \langle x\rangle$, we then have $x \in \langle a\rangle$.
                Therefore, $\exists b \in \mathbb{Z}$, $x = ab$. Choose such a b.
                Therefore, $a = \pm 1$ or $b = \pm 1$, since x is prime.
                Case 1: $a = \pm 1$.
                    In this case, $\langle a\rangle = \langle 1\rangle = \mathbb{Z}$.
                    Therefore, $\langle a\rangle = \mathbb{Z}$ or $\langle a\rangle = \langle x\rangle$.
                Case 2: $b = \pm 1$.
                    In this case, $a = \pm x$; hence $\langle a\rangle = \langle x\rangle$.
                    Therefore, $\langle a\rangle = \mathbb{Z}$ or $\langle a\rangle = \langle x\rangle$.
            Therefore, if $\langle x\rangle \subseteq \langle a\rangle$, then $\langle a\rangle = \mathbb{Z}$ or $\langle a\rangle = \langle x\rangle$.
        Therefore, $\forall a \in \mathbb{Z}$, if $\langle x\rangle \subseteq \langle a\rangle$, then $\langle a\rangle = \mathbb{Z}$ or $\langle a\rangle = \langle x\rangle$.
    Therefore, if x is prime, then $\forall a \in \mathbb{Z}$, if $\langle x\rangle \subseteq \langle a\rangle$, then $\langle a\rangle = \mathbb{Z}$ or $\langle a\rangle = \langle x\rangle$.
Hence, $\forall x \in \mathbb{Z}$, if x is prime, then $\forall a \in \mathbb{Z}$, if $\langle x\rangle \subseteq \langle a\rangle$, then $\langle a\rangle = \mathbb{Z}$ or $\langle a\rangle = \langle x\rangle$. □

The converse of the above proposition is true in the case where $x \neq \pm 1$ and $x \neq 0$. The proof of this is left as an exercise.

Exercises 2.3.

Prove the following propositions.

1. $\forall a, x, y \in \mathbb{Z}$, if $x \in \langle a \rangle$ and $y \in \langle a \rangle$, then $x + y \in \langle a \rangle$.
2. $\forall a, x \in \mathbb{Z}$, if $x \in \langle a \rangle$, then $-x \in \langle a \rangle$.
3. $\forall a, x \in \mathbb{Z}$, if $x \in \langle a \rangle$, then $\forall t \in \mathbb{Z}$, $xt \in \langle a \rangle$.
4. $\forall a, x, y \in \mathbb{Z}$, if $x + y \in \langle a \rangle$ and $y \in \langle a \rangle$, then $x \in \langle a \rangle$.
5. $\langle 4 \rangle \cap \langle 6 \rangle = \langle 12 \rangle$.
6. $\langle 4 \rangle + \langle 6 \rangle = \langle 2 \rangle$.
7. $\forall a \in \mathbb{Z}$, $\langle a \rangle + \langle a \rangle = \langle a \rangle$.
8. $\forall a, b \in \mathbb{Z}$, $\langle b \rangle \subseteq \langle a \rangle + \langle b \rangle$.
9. $\forall a, b \in \mathbb{Z}$, if $\langle a \rangle + \langle b \rangle = \langle b \rangle$, then $\langle a \rangle \subseteq \langle b \rangle$.
10. $\forall a, b \in \mathbb{Z}$, if $\langle a \rangle \subseteq \langle b \rangle$, then $\langle a \rangle + \langle b \rangle = \langle b \rangle$.
11. $\forall a, b \in \mathbb{Z}$, $\langle a \rangle \cap (\langle a \rangle + \langle b \rangle) = \langle a \rangle$.
12. $\forall a, b \in \mathbb{Z}$, $\langle a \rangle + (\langle a \rangle \cap \langle b \rangle) = \langle a \rangle$.
13. $\forall a, b, c \in \mathbb{Z}$, if $\langle c \rangle \subseteq \langle a \rangle$, then $\langle a \rangle \cap (\langle b \rangle + \langle c \rangle) = (\langle a \rangle \cap \langle b \rangle) + \langle c \rangle$.
14. $\forall a, x, y \in \mathbb{Z}$, if $\langle x \rangle \subseteq \langle a \rangle$ and $\langle y \rangle \subseteq \langle a \rangle$, then $\langle x \rangle + \langle y \rangle \subseteq \langle a \rangle$.
15. $\forall a, x, y \in \mathbb{Z}$, if $\langle x \rangle \subseteq \langle y \rangle$, then $\langle a \rangle + \langle x \rangle \subseteq \langle a \rangle + \langle y \rangle$.
16. $\forall a, b, x, y \in \mathbb{Z}$, if $\langle x \rangle \subseteq \langle y \rangle$ and $\langle a \rangle \subseteq \langle b \rangle$, then $\langle a \rangle + \langle x \rangle \subseteq \langle b \rangle + \langle y \rangle$.
17. $\forall x, y \in \mathbb{Z} \setminus \{0\}$, $\gcd(x, y) = 1$ if and only if $\langle x \rangle + \langle y \rangle = \mathbb{Z}$.
18. $\forall a, x, y \in \mathbb{Z} \setminus \{0\}$, if $\langle a \rangle \subseteq \langle x \rangle$ and $\langle a \rangle \subseteq \langle y \rangle$ and $\gcd(x, y) = 1$, then $\langle a \rangle \subseteq \langle xy \rangle$.
19. $\forall a, x, y \in \mathbb{Z} \setminus \{0\}$, if $xy \in \langle a \rangle$ and $\gcd(a, x) = 1$, then $y \in \langle a \rangle$.
20. $\forall a, b, n \in \mathbb{Z}$, $\langle b \rangle \subseteq \langle a \rangle + \langle n \rangle$ if and only if $\exists x \in \mathbb{Z}$, $b - ax \in \langle n \rangle$.
21. $\forall a \in \mathbb{Z}$, if a is prime, then $\forall x \in \mathbb{Z}$, $\langle a \rangle + \langle x \rangle = \mathbb{Z}$ or $\langle a \rangle + \langle x \rangle = \langle a \rangle$.
22. $\forall x \in \mathbb{Z} \setminus \{-1, 0, 1\}$, if $\forall a \in \mathbb{Z}$, if $\langle x \rangle \subseteq \langle a \rangle$, then $\langle a \rangle = \mathbb{Z}$ or $\langle a \rangle = \langle x \rangle$, then x is prime.
23. (Euclid's Lemma) $\forall a \in \mathbb{Z}$, if a is prime, then $\forall x, y \in \mathbb{Z}$, if $xy \in \langle a \rangle$, then $x \in \langle a \rangle$ or $y \in \langle a \rangle$. (Hint: Combine the result of problem 21, with those of problems 9 and 19.)
24. $\forall a \in \mathbb{Z} \setminus \{0\}$, if $\langle a \rangle \neq \mathbb{Z}$ and $\forall x, y \in \mathbb{Z}$, if $xy \in \langle a \rangle$, then $x \in \langle a \rangle$ or $y \in \langle a \rangle$, then a is prime.

Let $(I_k)_{k \in \mathbb{N}}$ be a sequence of ideals. That is, for each $k \in \mathbb{N}$, $\exists a_k \in \mathbb{Z}$, $I_k = \langle a_k \rangle$. Prove the following propositions.

25. $\forall x \in \mathbb{Z}$, if $\forall k \in \mathbb{N}$, $a_k \in \langle x \rangle$, then $\forall n \in \mathbb{N}$, $\sum_{k=1}^{n} a_k \in \langle x \rangle$.
26. $\forall n \in \mathbb{N}$, $\exists g \in \mathbb{Z}$, $\bigcap_{k=1}^{n} I_k = \langle g \rangle$. (Hint: use proposition 2.3.9).

2.4 Families of Sets

We begin this section by drawing a distinction between statements about the members of a set and statements about the set itself. For example, when we say 'humans are mortal,' the statement is about each individual human. That is, we are speaking about the *members* of the class of humans. On the other hand, statements such as 'humans are diverse,' 'humans are widespread throughout the world,' or 'humans are numerous,' refer to humans *collectively* rather than individually. These are statements about the *set* of humans rather than about the individual members of that set. For an example in mathematics, consider the statements 'the natural numbers are positive' and 'the natural numbers are infinite.' The former statement refers to the members of the set $\mathbb{N}$, while the latter refers to the set $\mathbb{N}$ itself. To make this precise, consider these statements in terms of their subjects and predicates: in the one case, when saying the natural numbers are positive, we use the predicate '$x > 0$' where the subject x is ranges over the elements of the set $\mathbb{N}$. In the other case, when saying the natural numbers are infinite, we use the predicate 'X is infinite' with the subject being the set $\mathbb{N}$ itself.

In fact, there are many predicates whose subjects are the sets themselves rather than the elements of those sets. Two further examples are 'S has a smallest element' and 'S is bounded above.' Recall that for a universe of discourse U and a predicate $P(x)$, the notation

$$\{x \in U \mid P(x)\}$$

is used to define the set of all subjects x for which the statement $P(x)$ is true. Since it is common to have predicates whose subjects are sets, it is just as common to see sets whose elements are sets themselves. To indicate that a set has sets as elements, we will often call a set of sets a **family of sets**. To illustrate the concept of a *family of sets*, consider the fact that some subsets of the real numbers have smallest elements, while others do not. For example, the interval $[0, 1)$ has a smallest element but the interval $(0, 1)$ does not. There may be situations in which we want to speak about the subsets of $\mathbb{R}$ that do have smallest elements. In such a situation, we would be speaking about the family of sets

$$\mathcal{S} = \{S \subseteq \mathbb{R} \mid S \text{ has a smallest element}\}.$$

Another example was encountered in the previous section: We found that any subset of the integers that is closed under addition and negation is an ideal. In this case, we saw that

$$\{S \subseteq \mathbb{Z} \mid S \neq \emptyset \text{ and } \forall x, y \in S,\ x + y \in S \text{ and } -x \in S\} = \{S \subseteq \mathbb{Z} \mid \exists g \in \mathbb{Z},\ S = \langle g \rangle\}.$$

These are all examples in which the members of a set are sets themselves.

The Powerset

The notation used above ($\{S \subseteq \mathbb{R} \mid S \text{ has a smallest element}\}$) is not quite proper and ought to be corrected. The reason is that set specification notation $\{x \in U \mid P(x)\}$ requires that we indicate the *universe of discourse* U to which the elements of the set belong. Saying that $S \subseteq \mathbb{R}$ indicates that the element S is a subset of $\mathbb{R}$, but this is not quite the same thing as identifying the universe of discourse to which S belongs. To be proper, the universe of discourse in this case should be the *set of all subsets of* $\mathbb{R}$, which we call the **powerset** of $\mathbb{R}$:

Definition 2.4.1. Let A be a set. The **powerset** of A, denoted $\mathcal{P}(A)$ is the set of all subsets of A. That is, $X \in \mathcal{P}(A)$ means $X \subseteq A$.

Example 2.4.1.

For a simple example, list all elements of the powerset of $A = \{0, 1\}$.

$\mathbf{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

In practice, when working with the *powerset*, we keep in mind that the statements $X \in \mathcal{P}(A)$ and $X \subseteq A$ are interchangeable. Hence, to prove $X \in \mathcal{P}(A)$, one must prove $X \subseteq A$. Likewise, if we assume $X \in \mathcal{P}(A)$, then it is known that $X \subseteq A$. Keep this in mind when examining the structure of the following proof:

Proposition 2.4.2.

Let A and B be sets whose elements belong to a common universe of discourse U. Then $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof.
Assume $A \subseteq B$.
    Let $X \in \mathcal{P}(U)$.
        Assume $X \in \mathcal{P}(A)$.
            Then $X \subseteq A$.
            Let $x \in U$.
                Assume $x \in X$.
                    Then $x \in A$, since $X \subseteq A$.
                    Hence $x \in B$, since $A \subseteq B$.
                Therefore, if $x \in X$, then $x \in B$.
            Therefore, $X \subseteq B$.
            Equivalently, $X \in \mathcal{P}(B)$.
        Therefore, if $X \in \mathcal{P}(A)$, then $X \in \mathcal{P}(B)$.
    Therefore, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
Therefore, if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
Conversely, assume $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
    Since $A \subseteq A$, we have $A \in \mathcal{P}(A)$.
    Therefore, $A \in \mathcal{P}(B)$, since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
    Hence, $A \subseteq B$.
Therefore, if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, then $A \subseteq B$.
Therefore, $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. □

A common error when working with powersets is to confuse the element relation $\in$ with the subset relation $\subseteq$. For example, $X \subseteq A \cup B$ does NOT mean $X \subseteq A$ or $X \subseteq B$. The union $A \cup B$ is defined in terms of elements rather than subsets. That is, $x \in A \cup B$ means $x \in A$ or $x \in B$. To replace the $\in$ symbol with the $\subseteq$ symbol is not valid and in this case results in a statement that is not true. A particularly frustrating aspect of this error is the fact that, in the case of intersections, the crime is committed without penalty. In fact, $X \subseteq A \cap B$ does imply that $X \subseteq A$ and $X \subseteq B$. The converse is also true. This property can be phrased as follows:

Proposition 2.4.3.

Let A and B be sets whose elements belong to a common universe of discourse U. Then $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

Proof.
Let $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.
    Then $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$.
    That is, $X \subseteq A$ and $X \subseteq B$.
    Let $x \in X$.
        Then $x \in A$, since $X \subseteq A$.
        Likewise, $x \in B$, since $X \subseteq B$.
        We now have $x \in A$ and $x \in B$; hence $x \in A \cap B$.
    Therefore, if $x \in X$, then $x \in A \cap B$.
    Therefore, $X \subseteq A \cap B$.
    Then $X \in \mathcal{P}(A \cap B)$.
Therefore, if $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$, then $X \in \mathcal{P}(A \cap B)$.
Therefore, $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.
Conversely, let $X \in \mathcal{P}(A \cap B)$.
    Then $X \subseteq A \cap B$.
    Since $X \subseteq A \cap B$ and $A \cap B \subseteq A$, we have $X \subseteq A$ by transitivity.
    Therefore, $X \in \mathcal{P}(A)$.
    Similarly, since $X \subseteq A \cap B$ and $A \cap B \subseteq B$, we know $X \subseteq B$.
    Therefore, $X \in \mathcal{P}(B)$.
    We now have $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$, hence $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.
Therefore, if $X \in \mathcal{P}(A \cap B)$, then $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.
Hence $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.
Therefore, $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$. □

Despite this convenient property of intersections, the reader is cautioned that the same does not hold for unions, complements, or relative complements. That is, $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$, $\mathcal{P}(A) \setminus \mathcal{P}(B) \neq \mathcal{P}(A \setminus B)$, and $(\mathcal{P}(A))^c \neq \mathcal{P}(A^c)$. The connections between these sets will be further investigated in the exercises.

When working with sets, sets of sets, and even sets of sets of sets, it can be important to keep track of the different levels in which our mathematical objects sit. To do this, we will try wherever possible to denote elements at the lowest level of our discourse (such as individual real numbers or integers) using lowercase letters (such as a), sets containing these elements using uppercase letters (such as A), and sets containing these sets using calligraphic letters (such as $\mathcal{A}$). Hence, we will usually see notation such as $a \in A$, $A \subseteq B$, $A \in \mathcal{A}$, and $\mathcal{A} \subseteq \mathcal{B}$. There is no formal rule in mathematics saying that sets must be denoted by uppercase letters and their elements by lowercase letters. In fact, one often encounters the notation $x \in y$, where the letter y is used to denote a set and the letter x is used to denote one of its elements. However, in the interest of avoiding confusion, we will stick to our notational convention wherever we can.

To practice identifying the levels in which our mathematical objects sit, the reader is invited to try the following example first without looking at the answers:

Example 2.4.4.

Decide which of the following are true and which are false:

1. $\mathbb{Z} \subseteq \mathcal{P}(\mathbb{Z})$.
2. $\mathbb{Z} \in \mathcal{P}(\mathbb{Z})$
3. $1 \in \mathcal{P}(\mathbb{Z})$
4. $\{1\} \subseteq \mathcal{P}(\mathbb{Z})$
5. $\{1\} \in \mathcal{P}(\mathbb{Z})$
6. $\emptyset \in \mathcal{P}(\mathbb{Z})$
7. $\emptyset \in \mathbb{Z}$
8. $\emptyset \subseteq \mathcal{P}(\mathbb{Z})$
9. $\{\emptyset\} \in \mathcal{P}(\mathbb{Z})$
10. $\{\emptyset\} \subseteq \mathcal{P}(\mathbb{Z})$

Answers: 1. False; 2. True; 3. False; 4. False; 5. True; 6. True; 7. False; 8. True; 9. False; 10. True.

Set Operations

In section 2.1, we defined the operations $\cap$ and $\cup$. These operations combine two sets into one. Using a recursive definition, we extended these operations to allow the combination of any finite number of sets into one set: $\bigcap_{k=1}^{n} A_k$ in the case of intersection and $\bigcup_{k=1}^{n} A_k$ for union. With the concept of a *family of sets* in place, we can extend these operations even further.

First, let us consider the intersection of a sequence of sets $\bigcap_{k=1}^{n} A_k$ in another way: the sequence of sets (A_k) can be viewed as a family of sets $\{A_k \mid 1 \leq k \leq n\}$. We have seen that even though it is defined recursively, the intersection $\bigcap_{k=1}^{n} A_k$ can be thought of intuitively as consisting of those elements that belong to every set A_k for $1 \leq k \leq n$. In other words, the intersection consists of those elements that belong to *every set* in the family $\{A_k \mid 1 \leq k \leq n\}$. Likewise, the union $\bigcup_{k=1}^{n} A_k$ can be thought of as consisting of all elements that belong to *at least one set* in the family $\{A_k \mid 1 \leq k \leq n\}$.

Now, consider the family of sets $\mathcal{I} = \{\langle k \rangle \mid k \in \mathbb{Z}\}$. Since this family consists of an infinite number of sets, our current definitions are insufficient if we want to talk about the intersection or union of the sets in this family. However, the idea given above, which says the intersection consists of those elements that are common to all sets in the family and the union consists of those elements that appear in at least one set in the family, can easily be extended to the family of sets $\mathcal{I}$. In fact, the only integer that is common to every ideal is 0, and every integer appears in at least one ideal. It seems reasonable then to say that the intersection of all of the ideals is the set $\{0\}$, and the union of all of the ideals is $\mathbb{Z}$.

In general, we define the union and intersection of a family of sets as follows:

Definition 2.4.2. Let $\mathcal{A} \subseteq \mathcal{P}(U)$ be a family of sets. The **intersection** of the family of sets $\mathcal{A}$ is defined to be

$$\bigcap_{S \in \mathcal{A}} S = \{x \in U \mid \forall S \in \mathcal{A},\ x \in S\}.$$

The **union** of $\mathcal{A}$ is defined to be

$$\bigcup_{S \in \mathcal{A}} S = \{x \in U \mid \exists S \in \mathcal{A},\ x \in S\}.$$

This definition is consistent with our earlier definitions, since the intersection $A \cap B$ can be viewed as consisting of those elements that are common to all sets in the family $\{A, B\}$. Likewise, the union of two sets $A \cup B$ can be viewed as those elements appearing in at least one set in the family $\{A, B\}$. Moreover, as mentioned earlier, the intersection and union of a sequence of sets $\bigcap_{k=1}^{n} A_k$ and $\bigcup_{k=1}^{n} A_k$ can be viewed as the intersection and union of the family of sets $\{A_k \mid 1 \leq k \leq n\}$.

Indexed Families of Sets

Notice that in some of our examples, such as any sequence of sets $\{A_k \mid 1 \leq k \leq n\}$, the sets in the family are labeled with an index. In this case, the index is the variable k which ranges in value from 1 through n. That is, to each number $k \in \{1, \ldots, n\}$, there corresponds a set A_k in our family if sets. In general, we say a family of sets $\mathcal{A}$ is **indexed** by a set I provided to each element $k \in I$, there corresponds a set in the family $\mathcal{A}$. In this way, the sequence of sets $\{A_k \mid 1 \leq k \leq n\}$ is *indexed* by the set $\{1, \ldots, n\}$.

Likewise, we can say that the family of ideals $\mathcal{I} = \{\langle k \rangle \mid k \in \mathbb{Z}\}$ is *indexed* by the set $\mathbb{Z}$. This is because to each element $k \in \mathbb{Z}$, there corresponds a set $\langle k \rangle$ in the family $\mathcal{I}$. When a family of sets is *indexed*, we often adjust the notation used to describe the intersection and union by referring to the sets by their index. A restatement of the definition of the intersection and union of an *indexed* family of sets, using this alternate notation, is as follows:

Definition 2.4.3. Let $\mathcal{A} = \{S_k \mid k \in I\}$ be a family of sets indexed by the set I. The **intersection** of $\mathcal{A}$ is defined to be

$$\bigcap_{k \in I} S_k = \{x \in U \mid \forall k \in I,\ x \in S_k\}.$$

The **union** of $\mathcal{A}$ is defined to be

$$\bigcup_{k \in I} S_k = \{x \in U \mid \exists k \in I,\ x \in S_k\}.$$

$\bigcap_{k \in I} S_k$ is often read as 'the intersection of the sets S_k over I', similarly for the union.

For a slightly more involved example of the intersection and union of a family of sets, for each $n \in \mathbb{N}$ let

$$S_n = \left\{ x \in \mathbb{R} \;\middle|\; \exists m \in \mathbb{Z},\ x = \frac{m}{n} \right\}.$$

Let $\mathcal{A} = \{S_n \mid n \in \mathbb{N}\}$. In this case, $\mathcal{A}$ is a family of sets indexed by $\mathbb{N}$. That is, to each $n \in \mathbb{N}$, there corresponds a set S_n in the family $\mathcal{A}$. Writing down the first few members of this family:

$$S_1 = \left\{ \ldots, \frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1}, \frac{4}{1}, \ldots \right\}$$

$$S_2 = \left\{ \ldots, \frac{-3}{2}, \frac{-2}{2}, \frac{-1}{2}, \frac{0}{2}, \frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \frac{4}{2}, \ldots \right\}$$

$$S_3 = \left\{ \ldots, \frac{-3}{3}, \frac{-2}{3}, \frac{-1}{3}, \frac{0}{3}, \frac{1}{3}, \frac{2}{3}, \frac{3}{3}, \frac{4}{3}, \ldots \right\}$$

$$\vdots$$

we can guess that the union of this family will be the set of all rational numbers and that the intersection will be the set of all integers. Indeed, since we have a precise definition of the intersection and union over a family of sets, we can prove that this is the case:

Example 2.4.5.

For each $n \in \mathbb{N}$, let $S_n = \{x \in \mathbb{R} \mid \exists m \in \mathbb{Z},\ x = \frac{m}{n}\}$. Then $\bigcup_{n \in \mathbb{N}} S_n = \mathbb{Q}$.

Proof.
Let $x \in \bigcup_{n \in \mathbb{N}} S_n$.
    Then $\exists n \in \mathbb{N}$, $x \in S_n$. Choose such an n.
    We then have $\exists m \in \mathbb{Z}$, $x = \frac{m}{n}$. Choose such an m.
    Since $n \in \mathbb{N}$, we have $n \neq 0$.
    We have $nx = m$ and $n \neq 0$; hence $x \in \mathbb{Q}$.
Therefore, $\bigcup_{n \in \mathbb{N}} S_n \subseteq \mathbb{Q}$.
Conversely, let $x \in \mathbb{Q}$. By proposition 1.2.13, choose $a, b \in \mathbb{Z}$, $bx = a$ and $b > 0$.
    Since $b > 0$, we have $b \in \mathbb{N}$.
    Further, since $x = \frac{a}{b}$, we have $x \in S_b$.
    Therefore, $\exists n \in \mathbb{N}$, $x \in S_n$.
    Hence, $x \in \bigcup_{n \in \mathbb{N}} S_n$
Therefore, $\mathbb{Q} \subseteq \bigcup_{n \in \mathbb{N}} S_n$.
Therefore, $\bigcup_{n \in \mathbb{N}} S_n = \mathbb{Q}$. □

Example 2.4.6.

For each $n \in \mathbb{N}$, let $S_n = \{x \in \mathbb{R} \mid \exists m \in \mathbb{Z},\ x = \frac{m}{n}\}$. Then $\bigcap_{n\in\mathbb{N}} S_n = \mathbb{Z}$.

Proof.
Let $x \in \bigcap_{n\in\mathbb{N}} S_n$.
  Then $\forall n \in \mathbb{N}$, $x \in S_n$.
  Since $1 \in \mathbb{N}$, we have $x \in S_1$.
  Therefore, $\exists m \in \mathbb{Z}$, $x = \frac{m}{1} = m$; hence $x \in \mathbb{Z}$.
Therefore, $\bigcap_{n\in\mathbb{N}} S_n \subseteq \mathbb{Z}$.
Conversely, let $x \in \mathbb{Z}$.
  Let $n \in \mathbb{N}$.
    Put $m = xn$.
      Then $x = \frac{xn}{n} = \frac{m}{n}$.
    Therefore, $\exists m \in \mathbb{Z}$, $x = \frac{m}{n}$; thus, $x \in S_n$.
  Therefore, $\forall n \in \mathbb{N}$, $x \in S_n$.
  That is, $x \in \bigcap_{n\in\mathbb{N}} S_n$
Therefore, $\mathbb{Z} \subseteq \bigcap_{n\in\mathbb{N}} S_n$.
Therefore, $\bigcap_{n\in\mathbb{N}} S_n = \mathbb{Z}$. □

For practice, here are two more examples of proofs involving indexed families of sets:

Example 2.4.7.

$$\bigcup_{n\in\mathbb{N}} \left(0, 1 - \frac{1}{n}\right] = (0, 1).$$

Proof.
Let $x \in \bigcup_{n\in\mathbb{N}}(0, 1 - \frac{1}{n}]$.
  Then $\exists n \in \mathbb{N}$, $x \in (0, 1 - \frac{1}{n}]$. Choose such an n.
  We then have $0 < x$ and $x < 1 - \frac{1}{n}$.
  Since $n > 0$, we have $\frac{1}{n} > 0$; hence $-\frac{1}{n} < 0$. Therefore, $1 - \frac{1}{n} < 1$.
  Since $x < 1 - \frac{1}{n}$ and $1 - \frac{1}{n} < 1$, we have $x < 1$.
  Therefore, $0 < x$ and $x < 1$; hence $x \in (0, 1)$.
Therefore, $\bigcup_{n\in\mathbb{N}}(0, 1 - \frac{1}{n}] \subseteq (0, 1)$.
Conversely, let $x \in (0, 1)$.
  Then $0 < x$ and $x < 1$.
  Since $x < 1$, we have $0 < 1 - x$.
  By the Archimedean property, we can choose $n \in \mathbb{N}$ with $\frac{1}{n} \leq 1 - x$.
    For such an n, we have $x \leq 1 - \frac{1}{n}$; hence $x \in (0, 1 - \frac{1}{n}]$.
  Therefore, $\exists n \in \mathbb{N}$, $x \in (0, 1 - \frac{1}{n}]$.
  That is, $x \in \bigcup_{n\in\mathbb{N}}(0, 1 - \frac{1}{n}]$.
Therefore, $(0, 1) \subseteq \bigcup_{n\in\mathbb{N}}(0, 1 - \frac{1}{n}]$.
Therefore, $\bigcup_{n\in\mathbb{N}}(0, 1 - \frac{1}{n}] = (0, 1)$. □

Example 2.4.8.

$$\bigcap_{a\in(0,\infty)} [0, a] = \{0\}.$$

Proof.
Let $x \in \bigcap_{a\in(0,\infty)}[0, a]$.
Then $\forall a \in (0, \infty)$, we have $x \in [0, a]$.
Since $1 \in (0, \infty)$, we have $x \in [0, 1]$; hence $0 \leq x$.
Suppose $x > 0$.
Taking $a = \frac{x}{2}$ gives us $a \in (0, \infty)$; hence $x \in [0, a]$.
Then $x \leq a$, which means $x \leq \frac{x}{2}$.
Therefore, $2x \leq x$; hence $x \leq 0$ which is a contradiction.
Therefore, $x \leq 0$, and since $0 \leq x$, it must be the case that $x = 0$; hence $x \in \{0\}$.
Therefore, $\bigcap_{a\in(0,\infty)}[0, a] \subseteq \{0\}$.
Conversely, let $x \in \{0\}$.
Then $x = 0$; hence $0 \leq x$.
Let $a \in (0, \infty)$.
Then $0 < a$, which means $x < a$. Hence, $x \leq a$.
We now have $0 \leq x \leq a$; hence $x \in [0, a]$.
Therefore, $\forall a \in (0, \infty)$, $x \in [0, a]$.
That is, $x \in \bigcap_{a\in(0,\infty)}[0, a]$.
Therefore, $\{0\} \subseteq \bigcap_{a\in(0,\infty)}[0, a]$.
Hence, $\bigcap_{a\in(0,\infty)}[0, a] = \{0\}$. □

Exercises 2.4.

Let A, B, and C be sets whose elements belong to a common universe of discourse U. Prove the following propositions.

1. If $\mathcal{P}(A) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$, then $A \subseteq B$.
2. if $\mathcal{P}(A) \cap \mathcal{P}(B^c) = \{\emptyset\}$, then $A \subseteq B$.
3. (a) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
   (b) Give examples of sets A and B for which $\mathcal{P}(A) \cup \mathcal{P}(B) \neq \mathcal{P}(A \cup B)$.
   (c) if $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$, then $A \subseteq B$ or $B \subseteq A$.
   (d) if $A \subseteq B$ or $B \subseteq A$, then $\mathcal{P}(A \cup B) \subseteq \mathcal{P}(A) \cup \mathcal{P}(B)$.
4. (a) There are no sets A and B for which $\mathcal{P}(A \setminus B) \subseteq \mathcal{P}(A) \setminus \mathcal{P}(B)$.
   (b) if $A \cap B^c = \emptyset$, then $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$.
   (c) if $A \cap B = \emptyset$, then $\mathcal{P}(A) \setminus \mathcal{P}(B) \subseteq \mathcal{P}(A \setminus B)$.
   (d) if $A \cap B^c \neq \emptyset$ and $A \cap B \neq \emptyset$, then $\mathcal{P}(A) \setminus \mathcal{P}(B) \nsubseteq \mathcal{P}(A \setminus B)$.
5. If $(\mathcal{P}(A))^c \subseteq \mathcal{P}(A^c)$, then $A = U$ or $A = \emptyset$.
6. $\mathcal{P}(A^c) \nsubseteq (\mathcal{P}(A))^c$.
7. Let $\mathcal{S} = \{A, B\}$. Then $\bigcap_{S \in \mathcal{S}} S = A \cap B$.
8. Let $\mathcal{S} = \{A, B\}$. Then $\bigcup_{S \in \mathcal{S}} S = A \cup B$.

Let $\mathcal{A} = \{S_k \mid k \in I\}$ be a family of sets with index set $I \neq \emptyset$, and let B be a set. Prove the following propositions.

9. $B \cap \bigcup_{k \in I} S_k = \bigcup_{k \in I} (B \cap S_k)$.
10. $B \cup \bigcap_{k \in I} S_k = \bigcap_{k \in I} (B \cup S_k)$.
11. $B \setminus \bigcup_{k \in I} S_k = \bigcap_{k \in I} (B \setminus S_k)$.
12. $B \setminus \bigcap_{k \in I} S_k = \bigcup_{k \in I} (B \setminus S_k)$.
13. $\left(\bigcup_{k \in I} S_k\right)^c = \bigcap_{k \in I} (S_k)^c$.
14. $\left(\bigcap_{k \in I} S_k\right)^c = \bigcup_{k \in I} (S_k)^c$.
15. If $\bigcup_{k \in I} S_k = \emptyset$, then $\forall m \in I, S_m = \emptyset$.
16. If $\exists m \in I, S_m = \emptyset$, then $\bigcap_{k \in I} S_k = \emptyset$.
17. $\forall J \in \mathcal{P}(I), \bigcup_{k \in J} S_k \subseteq \bigcup_{k \in I} S_k$.
18. $\forall J \in \mathcal{P}(I), \bigcap_{k \in I} S_k \subseteq \bigcap_{k \in J} S_k$.
19. For all $n \in \mathbb{N}$, if $I = \{k \in \mathbb{N} \mid k \leq n\}$, then $\bigcap_{k \in I} S_k = \bigcap_{k=1}^{n} S_k$.
20. For all $n \in \mathbb{N}$, if $I = \{k \in \mathbb{N} \mid k \leq n\}$, then $\bigcup_{k \in I} S_k = \bigcup_{k=1}^{n} S_k$.
21. If $\forall k \in I$, $S_k \subseteq \mathbb{R}$ is an interval, then $\bigcap_{k \in I} S_k$ is an interval. (Hint: Use theorems 2.2.9 and 2.2.11).
22. If $\forall k \in I$, $S_k \subseteq \mathbb{Z}$ is an ideal, then $\bigcap_{k \in I} S_k$ is an ideal. (Hint: Use theorem 2.3.7).
23. Let $(S_k)_{k \in \mathbb{N}}$ be a sequence of ideals of $\mathbb{Z}$. If $\forall k \in \mathbb{N}$, $S_k \subseteq S_{k+1}$, then $\bigcup_{k \in \mathbb{N}} S_k$ is an ideal.
24. Let $(S_k)_{k \in \mathbb{N}}$ be a sequence of intervals of $\mathbb{R}$. If $\forall k \in \mathbb{N}$, $S_k \subseteq S_{k+1}$, then $\bigcup_{k \in \mathbb{N}} S_k$ is an interval.

Prove the following propositions.

25. $\bigcup_{k \in \mathbb{Z}} \langle k \rangle = \mathbb{Z}$.
26. $\bigcap_{k \in \mathbb{Z}} \langle k \rangle = \{0\}$.
27. $\bigcap_{n \in \mathbb{N}} [n, \infty) = \emptyset$.
28. $\bigcup_{n \in \mathbb{N}} [n, \infty) = [1, \infty)$.
29. $\bigcup_{n \in \mathbb{N}} [0, n) = [0, \infty)$.
30. $\bigcap_{n \in \mathbb{N}} [0, n) = [0, 1)$.
31. $\bigcap_{x \in \mathbb{R}} (-\infty, x) = \emptyset$.

32. $\bigcup_{x\in\mathbb{R}}(-\infty, x) = \mathbb{R}$.

33. $\bigcup_{n\in\mathbb{N}}[1, 3n) = [1, \infty)$.

34. $\bigcap_{n\in\mathbb{N}}[1, n+1) = [1, 2)$.

35. $\bigcap_{n\in\mathbb{N}}\left(-\infty, \frac{1}{n}\right] = (-\infty, 0]$.

36. $\bigcup_{n\in\mathbb{N}}(-\infty, n) = \mathbb{R}$.

37. $\bigcup_{a\in(-\infty,1)}[0, 2+a) = [0, 3)$.

38. $\bigcap_{a\in(0,\infty)}[0, 2+a) = [0, 2]$.

39. $\bigcap_{a\in(-\infty,1)}[0, 2-a] = [0, 1]$.

40. $\bigcup_{a\in(0,\infty)}[0, 2-a] = [0, 2)$.

41. $\bigcup_{a\in(0,\infty)}[a, 2] = (0, 2]$.

42. $\bigcap_{a\in(-\infty,1)}[a, 2] = [1, 2]$.

43. $\bigcap_{a\in(0,\infty)}(1-a, 2] = [1, 2]$.

44. $\bigcup_{a\in(-\infty,1)}(1-a, 2] = (0, 2]$.

45. $\bigcup_{a\in(-\infty,1)}(1-a, 2+a) = (0, 3)$.

46. $\bigcap_{a\in(0,\infty)}(1-a, 2+a) = [1, 2]$.

47. $\bigcap_{a\in(-\infty,1)}[a, 2-a] = \{1\}$.

48. $\bigcup_{a\in(0,\infty)}[a, 2-a] = (0, 2)$.

49. $\bigcup_{a\in(0,1)}[a, 2+a) = (0, 3)$.

50. $\bigcap_{a\in(0,1)}[a, 2+a) = [1, 2]$.

51. $\bigcap_{a\in(0,1)}(1-a, 2-a] = \{1\}$.

52. $\bigcup_{a\in(0,1)}(1-a, 2-a] = (0, 2)$.

53. $\bigcup_{n\in\mathbb{N}}\left[0, 2+\frac{1}{n}\right) = [0, 3)$.

54. $\bigcap_{n\in\mathbb{N}}\left[0, 2+\frac{1}{n}\right) = [0, 2]$.

55. $\bigcap_{n\in\mathbb{N}}\left[0, 2-\frac{1}{n}\right] = [0, 1]$.

56. $\bigcup_{n\in\mathbb{N}}\left[0, 2-\frac{1}{n}\right] = [0, 2)$.

57. $\bigcup_{n\in\mathbb{N}}\left[\frac{1}{n}, 2\right] = (0, 2]$.

58. $\bigcap_{n\in\mathbb{N}}\left[\frac{1}{n}, 2\right] = [1, 2]$.

59. $\bigcap_{n\in\mathbb{N}}\left(1-\frac{1}{n}, 2\right] = [1, 2]$.

60. $\bigcup_{n\in\mathbb{N}}\left(1-\frac{1}{n}, 2\right] = (0, 2]$.

61. $\bigcup_{n\in\mathbb{N}}\left(1-\frac{1}{n}, 2+\frac{1}{n}\right) = (0, 3)$.

62. $\bigcap_{n\in\mathbb{N}}\left(1-\frac{1}{n}, 2+\frac{1}{n}\right) = [1, 2]$.

63. $\bigcap_{n\in\mathbb{N}}\left[\frac{1}{n}, 2-\frac{1}{n}\right] = \{1\}$.

64. $\bigcup_{n\in\mathbb{N}}\left[\frac{1}{n}, 2-\frac{1}{n}\right] = (0, 2)$.

65. $\bigcup_{n\in\mathbb{N}}\left[\frac{1}{n}, 2+\frac{1}{n}\right) = (0, 3)$.

66. $\bigcap_{n\in\mathbb{N}}\left[\frac{1}{n}, 2+\frac{1}{n}\right) = [1, 2]$.

67. $\bigcap_{n\in\mathbb{N}}\left(1-\frac{1}{n}, 2-\frac{1}{n}\right] = \{1\}$.

68. $\bigcup_{n\in\mathbb{N}}\left(1-\frac{1}{n}, 2-\frac{1}{n}\right] = (0, 2)$.

69. $\bigcup_{k\in\langle 6\rangle}\langle k\rangle = \langle 6\rangle$.

70. $\bigcap_{k\in\{n\in\mathbb{Z}\mid 6\in\langle n\rangle\}}\langle k\rangle = \langle 6\rangle$.

71. $\bigcap_{k\in\mathbb{Z}}(-\infty, k] \cup [k+1, \infty) = \mathbb{Z}$.

72. $\bigcup_{k\in\mathbb{Z}}(-\infty, k+1) \cap (k, \infty) = \mathbb{R} \setminus \mathbb{Z}$.

Let U and V be sets. Let $\mathcal{A} = \{A_y \mid y \in V\}$ be a family of subsets of U, indexed by V. For each $x \in U$, let $B_x = \{y \in V \mid x \in A_y\}$, and let $\mathcal{B} = \{B_x \mid x \in U\}$.

73. Prove $\forall x \in U$, $x \in \bigcap_{y\in V} A_y$ if and only if $B_x = V$.

74. Prove $\forall x \in U$, $x \in \bigcup_{y\in V} A_y$ if and only if $B_x \neq \emptyset$.

75. Prove $\forall y \in V$, $y \in \bigcup_{x\in U} B_x$ if and only if $A_y \neq \emptyset$.

76. Prove $\forall y \in V$, $y \in \bigcap_{x\in U} B_x$ if and only if $A_y = U$.

Prove the following propositions about families of inductive sets.

77. Let $\mathcal{A} = \{A \in \mathcal{P}(\mathbb{R}) \mid 1 \in A \text{ and } A \text{ is inductive}\}$.

    (a) $\bigcap_{A\in\mathcal{A}} A$ is inductive.

    (b) $\mathbb{N} \cap \bigcap_{A\in\mathcal{A}} A$ is inductive.

    (c) $\bigcap_{A\in\mathcal{A}} A = \mathbb{N}$.

78. Let $a \in \mathbb{R}$. Let $\mathcal{M} = \{A \in \mathcal{P}(\mathbb{R}) \mid a \in A \text{ and } A \text{ is inductive}\}$.

    (a) $\mathcal{M}$ is non-empty.

    (b) $\bigcap_{A\in\mathcal{M}} A$ is inductive.

    (c) $\bigcap_{A\in\mathcal{M}} A$ is the smallest inductive set containing a (See definition 1.2.9).

Chapter 3

Relations

Relations are statements about *two* subjects. For example, statements such as 'x causes y', 'x precedes y', 'x is beside y', or for math related examples, '$x > y$', '$x = y$', 'x divides y', '$x \in Y$', etc. are all examples of statements relating two objects. In fact, the predicates '*causes*', '*precedes*', '*is beside*', are only sensible when applied to *two* subjects.

To deal with *relations* in a set theoretic way, we must accept that the *truth set* of a relation is not a collection of *single* elements. Rather, it is a collection of *pairs* of elements. The proposition $0 < 1$ is not a statement about the subject 0 or the subject 1 individually; it is a statement about *both* subjects 0 and 1 simultaneously. That is, it is a statement about the pair $(0, 1)$. A very simple way of dealing with this is as follows: Suppose $P(x, y)$ is an open sentence with two variables (for example, one can imagine that P is the relation $<$, in which case $P(x, y)$ represents the statement '$x < y$'). We view the two subjects x and y as being *one pair* of subjects. That is, we view P as a predicate requiring a single subject that is an *ordered pair* (x, y). In doing so, we can specify the truth set of such a predicate as $\{(x, y) \mid P(x, y)\}$. In the case where $P(x, y)$ is the statement '$x < y$', our set is $\{(x, y) \mid x < y\}$. This set would contain for example the ordered pair $(0, 1)$, meaning that $0 < 1$. To make this precise, we turn to a familiar mathematical construction: The Cartesian plane.

Definition 3.0.1. Let A and B be sets. The **Cartesian product** of A and B, denoted $A \times B$, is the set consisting of all ordered pairs (x, y) for which $x \in A$ and $y \in B$. That is,

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$$

For a set A, we denote $A \times A$ by A^2.

Under this definition, the familiar Cartesian plane is the set $\mathbb{R} \times \mathbb{R}$, which is more commonly denoted as $\mathbb{R}^2$. We naturally extend this concept not only to sets of ordered *pairs* but to sets of ordered *triples*, *quadruples*, or any other number of objects:

Definition 3.0.2. Let A be a set. Define $A^1 = A$, and for each $n \in \mathbb{N}$ define $A^{n+1} = A^n \times A$.

With this in mind, we can begin to discuss relations in a set theoretic way. As a starting point, we state the definition of a *relation* in these terms:

Definition 3.0.3. Let A and B be sets. A **relation R from A to B** is any non-empty subset of $A \times B$. A non-empty subset of $A \times A$ is called a **relation on A**. When R is a relation from A to B, for $a \in A$ and $b \in B$, we use the notation aRb to denote $(a, b) \in R$.

In this sense, the relation $<$ is viewed as a *set* of ordered pairs; formally, $< \subseteq \mathbb{R} \times \mathbb{R}$. For $a, b \in \mathbb{R}$, we use the notation $a < b$ to indicate that $(a, b) \in <$.

3.1 Equivalence Relations

Equivalence relations are those relations that indicate two subjects are *the same* in some way. For example, 'x is of the same colour as y' and 'x has the same shape as y' are both examples of predicates that define *equivalence relations*. Different equivalence relations merely describe different senses in which two things can be the same. Equivalence relations are characterized by three properties: First, every object is the same as itself in every sense of the word 'same'. For example, every object is of the same colour as itself, and every object has the same shape as itself. Second, if the object x is the same as the object y, then we can also say that the object y is the same as the object x. That is, the order in which the subjects are mentioned does not change the meaning of the statement 'x is the same as y'. Again, this is true for any sense of the word 'same'. Third, x being the same as y is a *transitive* relation, in the sense that if x and y are the same and y and z are the same, then we can expect x to be the same as z. We take these three properties together to be the definition of an equivalence relation.

Definition 3.1.1. For a relation R on a set U:

1. R is **reflexive** means $\forall x \in U$, xRx.
2. R is **symmetric** means $\forall x, y \in U$, if xRy, then yRx.
3. R is **transitive** means $\forall x, y, z \in U$, if xRy and yRz, then xRz.

A relation that is reflexive, symmetric, and transitive is called an **equivalence relation**.

For a math example of an equivalence relation, consider the *parity* relation. By parity, we mean whether a number is even or odd. Odd numbers are said to have *odd parity* and even numbers are said to have *even parity*. The relation 'x is of the same parity as y' is an equivalence relation on the integers. This relation can be described formally as follows:

$$\equiv_2 = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \in \langle 2 \rangle\}.$$

That is, for $x, y \in \mathbb{Z}$, $x \equiv_2 y$ if and only if $x - y \in \langle 2 \rangle$. To prove that this is an equivalence relation, we must show that $\equiv_2$ is *reflexive*, *symmetric*, and *transitive*. That is, we must prove

1. $\forall x \in \mathbb{Z}$, $x \equiv_2 x$.
2. $\forall x, y \in \mathbb{Z}$, if $x \equiv_2 y$, then $y \equiv_2 x$.
3. $\forall x, y, z \in \mathbb{Z}$, if $x \equiv_2 y$ and $y \equiv_2 z$, then $x \equiv_2 z$.

Proposition 3.1.1.

$\equiv_2$ is an equivalence relation.

Proof.
Let $x \in \mathbb{Z}$.
    Since $x - x = 0 = (0)(2) \in \langle 2 \rangle$, we have $x \equiv_2 x$.
Therefore, $\forall x \in \mathbb{Z}$, $x \equiv_2 x$.
Hence, $\equiv_2$ is reflexive.
Next, let $x, y \in \mathbb{Z}$.
    Assume $x \equiv_2 y$.
        Then $x - y \in \langle 2 \rangle$.
        Choose $a \in \mathbb{Z}$ such that $x - y = 2a$.
        Then $y - x = -2a = 2(-a) \in \langle 2 \rangle$.
        Therefore, $y \equiv_2 x$.
    This shows that if $x \equiv_2 y$, then $y \equiv_2 x$.
Therefore, $\equiv_2$ is symmetric.
Finally, let $x, y, z \in \mathbb{Z}$.
    Assume $x \equiv_2 y$ and $y \equiv_2 z$.
        That is, $x - y \in \langle 2 \rangle$, and $y - z \in \langle 2 \rangle$.
        Choose $a, b \in \mathbb{Z}$ such that $x - y = 2a$ and $y - z = 2b$.
        Then $x - z = (x - y) + (y - z) = 2a + 2b = 2(a + b) \in \langle 2 \rangle$.
        Therefore, $x \equiv_2 z$.
    Therefore, if $x \equiv_2 y$ and $y \equiv_2 z$, then $x \equiv_2 z$.
Thus $\equiv_2$ is transitive.
Since $\equiv_2$ is reflexive, symmetric, and transitive, $\equiv_2$ is an equivalence relation. □

Equivalence Classes

To see precisely how the equivalence relation $\equiv_2$ corresponds to the partition of the integers into evens and odds, we notice that every equivalence relation on a set A implies a grouping of the elements of A into classes of like objects. For example, consider the following set of nine coloured shapes:

$$\{●, ●, ■, ●, ▲, ■, ▲, ▲, ■\}$$

The equivalence relation given by 'x **is of the same colour as** y' suggests the following grouping of the elements in A:

$$\{\{●, ▲\}, \{●, ■\}, \{■, ●, ▲\}, \{■, ▲\}\}$$

On the other hand, the equivalence relation given by 'x **has the same shape as** y' implies we partition the set A into classes of shapes as follows:

$$\{\{●, ●, ●\}, \{■, ■, ■\}, \{▲, ▲, ▲\}\}$$

To make precise this idea of grouping elements of a set into classes of similar elements, we give the following definition:

Definition 3.1.2. For an equivalence relation R on a set U, for each $a \in U$, we define the **equivalence class** of a relative to R to be the set

$$[a]_R = \{x \in U \mid xRa\}.$$

We denote by U/R, the family of equivalence classes:

$$U/R = \{[a] \mid a \in U\}.$$

In practice, it is not always necessary to include a reference to the equivalence relation R in the notation denoting the equivalence class $[a]_R$. If there is no ambiguity and the reader of our proof can reasonably be expected to know the equivalence relation relative to which the class $[a]_R$ is defined, then we can denote the equivalence class of a simply by $[a]$. Other common notation for the equivalence class of a includes $\overline{a}$ and $\dot{a}$. In summary:

Notation

When the relation R is understood in the context in which we are working, we commonly denote the **equivalence class** of a relative to R by $[a]$, $\overline{a}$, or $\dot{a}$.

For an example of equivalence classes, we return to the relation $\equiv_2$. Recall that this relation on $\mathbb{Z}$ is given by: $x \equiv_2 y$ if and only if $x - y \in \langle 2 \rangle$. We can now show that the equivalence classes relative to this relation are the even integers and the odd integers.

Proposition 3.1.2.

For the equivalence relation $\equiv_2$, $[0] = \mathbb{E}$ and $[1] = \mathbb{O}$.

Proof.
Let $x \in \mathbb{Z}$.
$x \in [0]$ if and only if $x \equiv_2 0$.
$x \equiv_2 0$ if and only if $x - 0 \in \langle 2 \rangle$.
$x - 0 \in \langle 2 \rangle$ if and only if $\exists a \in \mathbb{Z}$, $x = 2a$.
$\exists a \in \mathbb{Z}$, $x = 2a$ if and only if $x \in \mathbb{E}$.
Therefore, $x \in [0]$ if and only if $x \in \mathbb{E}$.
Therefore, $[0] = \mathbb{E}$.
To show that $[1] = \mathbb{O}$, we again let $x \in \mathbb{Z}$.
$x \in [1]$ if and only if $x \equiv_2 1$.
$x \equiv_2 1$ if and only if $x - 1 \in \langle 2 \rangle$.
$x - 1 \in \langle 2 \rangle$ if and only if $\exists a \in \mathbb{Z}$, $x - 1 = 2a$.
$\exists a \in \mathbb{Z}$, $x - 1 = 2a$ if and only if $\exists a \in \mathbb{Z}$, $x = 2a + 1$.
$\exists a \in \mathbb{Z}$, $x = 2a + 1$ if and only if $x \in \mathbb{O}$.
Therefore, $x \in [1]$ if and only if $x \in \mathbb{O}$.
Therefore, $[1] = \mathbb{O}$. □

Although we speak about the equivalence class of a single object $[a]$, the choice of which object represents its equivalence class is arbitrary. Any element in the equivalence class can stand as its representative. For example, in the case of the equivalence relation given by 'x is the same shape as y' partitioning the set of coloured shapes into classes:

$$\{\{●, ●, ●\}, \{■, ■, ■\}, \{▲, ▲, ▲\}\}$$

The class of triangles could be represented by any of the three triangles. That is, the equivalence class of the red triangle is the same as the equivalence class of the green triangle, as well as that of the blue triangle. That any two related objects can stand as representatives for the same equivalence class is the main point of the following theorem:

Theorem 3.1.3.

Let R be an equivalence relation on a set U. Let $a, b \in U$. The following statements are equivalent:

1. aRb
2. $a \in [b]$
3. $[a] \subseteq [b]$
4. $[a] = [b]$
5. $[a] \cap [b] \neq \emptyset$.

Proof.
Let $a, b \in U$.
(1) $\iff$ (2) is the definition so we use them interchangeably.
We will prove (1) $\Rightarrow$ (3), (3) $\Rightarrow$ (4), (4) $\Rightarrow$ (5), and (5) $\Rightarrow$ (1).
(1) $\Rightarrow$ (3):
    Assume aRb.
        Let $x \in [a]$.
            Then xRa.
            Since xRa and aRb, we have xRb by transitivity.
            Hence, $x \in [b]$.
        Therefore, $[a] \subseteq [b]$.
    Therefore, if aRb, then $[a] \subseteq [b]$.
(3) $\Rightarrow$ (4):
    Assume $[a] \subseteq [b]$.
        Since R is reflexive, $a \in [a]$; hence $a \in [b]$.
        Then aRb, and so bRa by symmetry.
        Thus, $[b] \subseteq [a]$, since (1) $\Rightarrow$ (3).
        Now, $[a] \subseteq [b]$ and $[b] \subseteq [a]$, which means $[a] = [b]$.
    Therefore, if $[a] \subseteq [b]$, then $[a] = [b]$.
(4) $\Rightarrow$ (5):
    Assume $[a] = [b]$.
        Then, $[a] \cap [b] = [a] \neq \emptyset$, since $a \in [a]$, by reflexivity.
    Therefore, if $[a] = [b]$, then $[a] \cap [b] \neq \emptyset$.
(5) $\Rightarrow$ (1):
    Assume $[a] \cap [b] \neq \emptyset$.
        Choose $x \in [a] \cap [b]$.
        Then, $x \in [a]$ and $x \in [b]$, so xRa and xRb.
        But R is symmetric, so aRx and xRb.
        Hence, aRb by transitivity.
    Therefore, if $[a] \cap [b] \neq \emptyset$, then aRb.
Q.E.D. □

Returning to our example $\equiv_2$, recall that $[0] = \mathbb{E}$ and $[1] = \mathbb{O}$. The point of the theorem above is that the class of even integers need not be represented by 0, it could in fact be represented by any even integer. Likewise, the class of odd integers could be represented by any odd integer; not only the odd integer 1. We make this precise as follows:

Proposition 3.1.4.

For the equivalence relation $\equiv_2$, $\forall x \in \mathbb{Z}$, if x is even, then $[x] = \mathbb{E}$, and if x is odd, then $[x] = \mathbb{O}$.

Proof.
Let $x \in \mathbb{Z}$.
Assume x is even.
Then $x \in [0]$, since $[0] = \mathbb{E}$.
Therefore, $[x] = [0]$; hence $[x] = \mathbb{E}$.
Therefore, if x is even, then $[x] = \mathbb{E}$.
Assume x is odd.
Then $x \in [1]$, since $[1] = \mathbb{O}$.
Therefore, $[x] = [1]$; hence $[x] = \mathbb{O}$.
Therefore, if x is odd, then $[x] = \mathbb{O}$.
Therefore, $\forall x \in \mathbb{Z}$, if x is even, then $[x] = \mathbb{E}$, and if x is odd, then $[x] = \mathbb{O}$. □

Partitions

To examine in more detail this separation of the underlying set into classes, we can make the sense in which we use the word *partition* more precise:

Definition 3.1.3. Let U be a set. A family of sets $\mathcal{A} \subseteq \mathcal{P}(U)$ is called a **partition** of U provided:

1. $\forall S \in \mathcal{A}, S \neq \emptyset$.
2. $\forall S, T \in \mathcal{A}$, if $S \neq T$, then $S \cap T = \emptyset$.
3. $\bigcup_{S \in \mathcal{A}} S = U$.

In the event that our family of sets is *indexed*, we restate this definition using the indexed form:

Definition 3.1.4. Let U be a set. An indexed family of sets $\mathcal{A} = \{S_k \mid k \in I\} \subseteq \mathcal{P}(U)$ is called a **partition** of U provided:

1. $\forall k \in I, S_k \neq \emptyset$.
2. $\forall j, k \in I$, if $S_j \neq S_k$, then $S_j \cap S_k = \emptyset$.
3. $\bigcup_{k \in I} S_k = U$.

It is in this sense of the word *partition* that equivalence classes form a partition of underlying set:

Theorem 3.1.5.

Let R be an equivalence relation on a set U. The family of equivalence classes relative to R, denoted $U/R = \{[x] \mid x \in U\}$, is a partition of U.

Proof.
Let $x \in U$.
  Since R is reflexive, we have xRx; hence $x \in [x]$.
  Therefore, $[x] \neq \emptyset$.
Therefore, $\forall x \in U$, $[x] \neq \emptyset$.
Let $x, y \in U$.
  Assume $[x] \cap [y] \neq \emptyset$.
    Then $[x] = [y]$ by theorem 3.1.3.
  Therefore, if $[x] \cap [y] \neq \emptyset$, then $[x] = [y]$.
Therefore, $\forall x, y \in U$, if $[x] \neq [y]$, then $[x] \cap [y] = \emptyset$.
Since U is the universe of discourse, we have $\bigcup_{a \in U}[a] \subseteq U$.
Conversely, let $x \in U$.
  Then, since R is reflexive, we have $x \in [x]$.
  Therefore, $\exists a \in U$, $x \in [a]$; hence $x \in \bigcup_{a \in U}[a]$.
Therefore, $\bigcup_{a \in U}[a] = U$.
Therefore, $U/R = \{[x] \mid x \in U\}$ is a partition of U. □

Although at first it may seem like a novel way of thinking, in some sense the converse of theorem 3.1.5 is also true. Where theorem 3.1.5 says that whenever one has an equivalence relation, one also has a partition; it is also true that whenever one has a partition, one acquires an equivalence relation. In fact, the possible partitions of a set and the possible equivalence relations on that set are in one-to-one correspondence with one another. For an example of an equivalence relation derived from a partition, consider that due to the high enrollment in first year calculus at many universities, it is necessary to offer several sections of the same course to accommodate all of the students. We thus *partition* the set of all first year calculus students into different first year calculus *classes*. The grouping of students into these classes may be completely arbitrary, in that the students in a particular class may not share any other similarity than just that they happen to have been placed in the same class. However, by thus being placed into the same class, the students *acquire* the similarity of *belonging to the same class*. This is true in general; as soon as one partitions any set into classes, the elements of each class acquire the relation of *belonging to the same class*. This relation is an equivalence relation.

For a partition $\mathcal{A}$ of a set U, define the relation $\sim_{\mathcal{A}}$ on U by

$$\sim_{\mathcal{A}} = \{(x, y) \in U \times U \mid \exists S \in \mathcal{A},\ x \in S \text{ and } y \in S\}.$$

That is, for $x, y \in U$, $x \sim_{\mathcal{A}} y$ if and only if $\exists S \in \mathcal{A}$, $x \in S$ and $y \in S$.

We first verify that for a partition $\mathcal{A}$, the relation $\sim_{\mathcal{A}}$ is an *equivalence* relation:

Theorem 3.1.6.

Let $\mathcal{A}$ be a partition of a set U. Then $\sim_{\mathcal{A}}$ is an equivalence relation.

Proof.
Let $x \in U$.
  Since $\bigcup_{S \in \mathcal{A}} S = U$, we have $\exists S \in \mathcal{A}$, $x \in S$.
  Therefore, $\exists S \in \mathcal{A}$, $x \in S$ and $x \in S$, which means $x \sim_{\mathcal{A}} x$.
Therefore, $\sim_{\mathcal{A}}$ is reflexive.
Let $x, y \in U$.
  Assume $x \sim_{\mathcal{A}} y$.
    Then $\exists S \in \mathcal{A}$, $x \in S$ and $y \in S$.
    Therefore, $\exists S \in \mathcal{A}$, $y \in S$ and $x \in S$,
    and so $y \sim_{\mathcal{A}} x$.
  Therefore, if $x \sim_{\mathcal{A}} y$, then $y \sim_{\mathcal{A}} x$.
Therefore, $\sim_{\mathcal{A}}$ is symmetric.
Let $x, y, z \in U$.
  Assume $x \sim_{\mathcal{A}} y$ and $y \sim_{\mathcal{A}} z$.
    Choose $S \in \mathcal{A}$ such that $x \in S$ and $y \in S$.
    Choose $T \in \mathcal{A}$ such that $y \in T$ and $z \in T$.
    Then $y \in S \cap T$; hence $S \cap T \neq \emptyset$.
    Therefore, $S = T$; hence $z \in S$.
    Therefore, $\exists S \in \mathcal{A}$, $x \in S$ and $z \in S$, hence $x \sim_{\mathcal{A}} z$.
  Therefore, if $x \sim_{\mathcal{A}} y$ and $y \sim_{\mathcal{A}} z$, then $x \sim_{\mathcal{A}} z$.
Therefore, $\sim_{\mathcal{A}}$ is transitive.
Thus, $\sim_{\mathcal{A}}$ is an equivalence relation. □

Together, theorems 3.1.5 and 3.1.6 tell us that to each equivalence relation corresponds a partition and to each partition corresponds an equivalence relation. In fact, the correspondences are inverses of one another, in the following sense:

Theorem 3.1.7.

Let $\mathcal{A}$ be a partition of a set U, and let $\sim$ be $\sim_{\mathcal{A}}$, the corresponding equivalence relation. Then $U/\sim = \mathcal{A}$.

Proof.
First notice that for all $a \in U$ and $S \in \mathcal{A}$, if $a \in S$, then $S = [a]$.
Indeed, let $S \in \mathcal{A}$, assume $a \in S$.
  Let $x \in S$.
    Then $a, x \in S$, so $x \sim a$
    Hence, $x \in [a]$.
  Thus, $S \subseteq [a]$.
  Conversely, let $x \in [a]$.
    Then, $x \sim a$, so we can choose $T \in \mathcal{A}$ with $x, a \in T$.
    But now $a \in S \cap T$, so $S = T$, by property 2 of partition.
    Therefore, $x \in S$.
  Thus, $[a] \subseteq S$, and we have $S = [a]$.
Therefore, for all $a \in U$ and $S \in \mathcal{A}$, if $a \in S$, then $S = [a]$.

Now, to prove $U/\sim = \mathcal{A}$,
let $S \in \mathcal{A}$.
  Then $S \neq \emptyset$, so we can choose $a \in U$ with $a \in S$;
  Hence $S = [a]$ as shown above, so $S \in U/\sim$.
Therefore, $\mathcal{A} \subseteq U/\sim$.
Conversely, let $S \in U/\sim$.
  Choose $a \in U$ so that $S = [a]$.
  Since U is the union of $\mathcal{A}$, we choose $T \in \mathcal{A}$ with $a \in T$,
  so that again $S = [a] = T \in \mathcal{A}$,
Thus, the families $U/\sim$ and $\mathcal{A}$ are equal. □

Modular Arithmetic

To put the theory of equivalence relations and their classes in a more concrete setting, we draw attention to one specific type of equivalence relation on the integers. Modular arithmetic is a very common and useful bit of mathematics, and some students may already have some exposure to this concept. However, familiarity with modular arithmetic is not necessary for this section. Our purpose here is not to develop a comprehensive theory of modular math. That would take too long and take us too far off course. Rather, we are only interested in considering modular arithmetic as an example of equivalence relations and to show how the theory of modular arithmetic is built on the foundation laid by the theory of equivalence relations.

Definition 3.1.5. For $n \in \mathbb{Z}$, we define the relation **congruence modulo** n to be

$$\equiv_n = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \in \langle n \rangle\}.$$

That is, for $x, y \in \mathbb{Z}$, we say x and y are **congruent modulo** n, denoted $x \equiv_n y$, if and only if $x - y \in \langle n \rangle$.

Notation

For $x, y, n \in \mathbb{Z}$, the notation $x \equiv y \pmod{n}$ is often used to denote $x \equiv_n y$.

Proposition 3.1.8.

For each $n \in \mathbb{Z}$, $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

Proof.
Let $n \in \mathbb{Z}$.
- Let $x \in \mathbb{Z}$.
  - Since $x - x = 0 = (0)(n) \in \langle n \rangle$, we have $x \equiv_n x$.
- Hence, $\equiv_n$ is reflexive.
- Next, let $x, y \in \mathbb{Z}$.
  - Assume $x \equiv_n y$.
    - Then $x - y \in \langle n \rangle$.
    - Choose $a \in \mathbb{Z}$ such that $x - y = na$.
    - Then $y - x = -na = n(-a) \in \langle n \rangle$.
    - Therefore, $y \equiv_n x$.
  - This shows that if $x \equiv_n y$, then $y \equiv_n x$.
- Therefore, $\equiv_n$ is symmetric.
- Finally, let $x, y, z \in \mathbb{Z}$.
  - Assume $x \equiv_n y$ and $y \equiv_n z$.
    - That is, $x - y \in \langle n \rangle$ and $y - z \in \langle n \rangle$.
    - Choose $a, b \in \mathbb{Z}$ such that $x - y = na$ and $y - z = nb$.
    - Then $x - z = (x - y) + (y - z) = na + nb = n(a + b) \in \langle n \rangle$.
    - Therefore, $x \equiv_n z$.
  - Therefore, if $x \equiv_n y$ and $y \equiv_n z$, then $x \equiv_n z$.
- Thus $\equiv_n$ is transitive.
- Since $\equiv_n$ is reflexive, symmetric, and transitive, $\equiv_n$ is an equivalence relation.

Therefore, for all $n \in \mathbb{Z}$, $\equiv_n$ is an equivalence relation on $\mathbb{Z}$. □

Proposition 3.1.9.

For all $n, a \in \mathbb{Z}$, the equivalence class of a relative to the relation $\equiv_n$ is

$$[a]_{\equiv_n} = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = a + nt\}.$$

Proof.
Let $n, a \in \mathbb{Z}$.
To simplify notation, let $A = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = a + nt\}$.
Let $x \in \mathbb{Z}$.
$x \in [a]_{\equiv_n}$ if and only if $x \equiv_n a$.
$x \equiv_n a$ if and only if $x - a \in \langle n \rangle$.
$x - a \in \langle n \rangle$ if and only if $\exists t \in \mathbb{Z}$, $x - a = nt$.
$\exists t \in \mathbb{Z}$, $x - a = nt$ if and only if $\exists t \in \mathbb{Z}$, $x = a + nt$.
$\exists t \in \mathbb{Z}$, $x = a + nt$ if and only if $x \in A$.
Therefore, $x \in [a]_{\equiv_n}$ if and only if $x \in A$.
Therefore, $[a]_{\equiv_n} = A$.
Therefore, for all $n, a \in \mathbb{Z}$, $[a]_{\equiv_n} = \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = a + nt\}$. □

Notation

When working with congruence modulo n, we often allow ourselves the following notation:

$$\text{for } n, a \in \mathbb{Z},\ a + \langle n \rangle \text{ is defined to be } \{x \in \mathbb{Z} \mid \exists t \in \mathbb{Z},\ x = a + nt\}.$$

The notation $a + \langle n \rangle$ is not in any way meant to indicate that an integer can be added to a set. It is simply meant as notation representing the set indicated.

Also, when the relation is congruence modulo n, we will simplify the notation for the equivalence class of a as follows:

$$\text{for } n, a \in \mathbb{Z},\ [a]_n \text{ is defined to be } [a]_{\equiv_n}.$$

Using this notation, proposition 3.1.9 becomes: For all $n, a \in \mathbb{Z}$, $[a]_n = a + \langle n \rangle$.

Theorem 3.1.10.

Let $n, a, b \in \mathbb{Z}$. The following are equivalent:

1. $a - b \in \langle n \rangle$
2. $a \in b + \langle n \rangle$
3. $a + \langle n \rangle \subseteq b + \langle n \rangle$
4. $a + \langle n \rangle = b + \langle n \rangle$
5. $(a + \langle n \rangle) \cap (b + \langle n \rangle) \neq \emptyset$.

Proof.
For the relation $\equiv_n$, by theorem 3.1.3, we have equivalence of the propositions

1. $a \equiv_n b$
2. $a \in [b]$
3. $[a]_n \subseteq [b]_n$
4. $[a]_n = [b]_n$
5. $[a]_n \cap [b]_n = \emptyset$.

Since $[a]_n = a + \langle n \rangle$, $[b]_n = b + \langle n \rangle$, and $a \equiv_n b$ means $a - b \in \langle n \rangle$, we have equivalence of the propositions

1. $a - b \in \langle n \rangle$
2. $a \in b + \langle n \rangle$
3. $a + \langle n \rangle \subseteq b + \langle n \rangle$
4. $a + \langle n \rangle = b + \langle n \rangle$
5. $(a + \langle n \rangle) \cap (b + \langle n \rangle) \neq \emptyset$.

□

We have already seen that for the relation $\equiv_2$, $[0]_2 = \mathbb{E}$ and $[1]_2 = \mathbb{O}$. Further, this is a complete list of distinct equivalence classes, since for any even x, $[x]_2 = [0]_2$ and for any odd x, $[x]_2 = [1]_2$. In general, for any $n \in \mathbb{N}$, there will be n distinct equivalence classes relative to the relation $\equiv_n$. In fact, $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$ is a complete list of equivalence classes relative to $\equiv_n$. The proof of this claim uses the division algorithm:

Theorem 3.1.11.

For all $n \in \mathbb{N}$, $\mathbb{Z}/\equiv_n = \{[x]_n \mid 0 \leq x < n\}$.

Proof.
Let $n \in \mathbb{N}$.
$\{[x]_n \mid 0 \leq x < n\} \subseteq \mathbb{Z}/\equiv_n$,
since $\mathbb{Z}/\equiv_n$ is the universe of discourse in which $\{[x]_n \mid 0 \leq r < n\}$ is defined.
Next, let $A \in \mathbb{Z}/\equiv_n$. That is, $A = [a]_n$ for some $a \in \mathbb{Z}$.
Choose such an $a \in \mathbb{Z}$.
Applying the division algorithm, choose $q, r \in \mathbb{Z}$, $a = qn + r$ and $0 \leq r < n$.
Then $a - r = qn \in \langle n \rangle$; hence $a \equiv_n r$.
Therefore, $[a]_n = [r]_n$.
Since $0 \leq r < n$, we have $[r]_n \in \{[x]_n \mid 0 \leq x < n\}$.
Therefore, $[a]_n \in \{[x]_n \mid 0 \leq x < n\}$.
Therefore, $\mathbb{Z}/\equiv_n \subseteq \{[x]_n \mid 0 \leq x < n\}$.
Therefore, for all $n \in \mathbb{N}$, $\mathbb{Z}/\equiv_n = \{[x]_n \mid 0 \leq x < n\}$. □

In fact, not only is $\{[x]_n \mid 0 \leq x < n\}$ a complete list of all equivalence classes relative to $\equiv_n$, but these equivalence classes are also distinct. That is, if $0 \leq r_1 < n$ and $0 \leq r_2 < n$ and $r_1 \neq r_2$, then $[r_1]_n \neq [r_2]_n$. The reason is that the quotient and remainder given by the division algorithm are unique for a given numerator and denominator. The proof of this uniqueness was included as an exercise in section 1.2 (exercise 26). We prove this result again in this setting:

Theorem 3.1.12.

For all $n \in \mathbb{N}$, if $0 \leq r_1 < n$ and $0 \leq r_2 < n$ and $r_1 \neq r_2$, then $[r_1]_n \neq [r_2]_n$. Where the equivalence classes are relative to $\equiv_n$.

Proof.
Let $n \in \mathbb{N}$
Suppose $0 \leq r_1 < n$ and $0 \leq r_2 < n$ and $r_1 \neq r_2$ and $[r_1]_n = [r_2]_n$.
Then $r_1 \equiv_n r_2$, which means $r_1 - r_2 \in \langle n \rangle$.
Therefore, n divides $r_1 - r_2$.
Now, since $r_1 \neq r_2$, we have $r_1 - r_2 \neq 0$.
Therefore, by Proposition 1.2.8, we have $n \leq |r_1 - r_2|$.
Also, by Proposition 1.1.30, we have $|r_1 - r_2| \leq \max(r_1, r_2)$.
By transitivity, we now have $n \leq \max(r_1, r_2)$.
However, this presents a problem: since $r_1 < n$ and $r_2 < n$, we have $\max(r_1, r_2) < n$.
Thus, have the contradiction $n \leq \max(r_1, r_2)$ and $\max(r_1, r_2) < n$.
Therefore, if $0 \leq r_1 < n$ and $0 \leq r_2 < n$ and $r_1 \neq r_2$, then $[r_1]_n \neq [r_2]_n$.
Therefore, for all $n \in \mathbb{N}$, if $0 \leq r_1 < n$ and $0 \leq r_2 < n$ and $r_1 \neq r_2$, then $[r_1]_n \neq [r_2]_n$. □

Definition 3.1.6. For $n \in \mathbb{N}$, we denote by $\mathbb{Z}_n$ the set of equivalence classes relative to the relation $\equiv_n$. That is,

$$\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \{[x]_n \mid 0 \leq x < n\}.$$

For example, consider the relation $\equiv_5$ and its equivalence classes $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. Recall that $[a]_5$ denotes the *set* of all integers congruent to a modulo 5. That is,

$$[0]_5 = \{\ldots, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\}$$

$$[1]_5 = \{\ldots, -14, -9, -4, 1, 6, 11, 16, 21, \ldots\}$$

$$[2]_5 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}$$

$$[3]_5 = \{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}$$

$$[4]_5 = \{\ldots, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}$$

The equivalence classes relative to $\equiv_n$ have an interesting property that is not necessarily shared by equivalence classes relative to other relations; they preserve addition and multiplication. What we mean by this can be seen in the following example: Select any element from the equivalence class $[2]_5$ and any element from the equivalence class $[4]_5$, say $-8 \in [2]_5$ and $14 \in [4]_5$. If we add these numbers together, we get $-8 + 14 = 6$, which is in the equivalence class $[1]_5$. We claim that this result is independent of the choice of elements -8 and 14. That is, had we chosen say $17 \in [2]_5$ and $-1 \in [4]_5$, we have $17 + (-1) = 16$, which is still in the equivalence class $[1]_5$. Trying a few more examples, we begin to suspect that for any $x \in [2]_5$ and any $y \in [4]_5$, we will have $x + y \in [1]_5$. Multiplication of elements from two equivalence classes is similarly independent of the choice of which elements to multiply. For example, taking $-3 \in [2]_5$ and $4 \in [4]_5$ gives us $(-3)(4) = -12 \in [3]_5$. Selecting different elements, $7 \in [2]_5$ and $-1 \in [4]_5$ gives us $(7)(-1) = -7 \in [3]_5$. In general, we find that for any $x \in [2]_5$ and any $y \in [4]_5$, we will have $xy \in [3]_5$. This works for equivalence classes relative to $\equiv_n$, for any n:

Theorem 3.1.13.

Let $n \in \mathbb{Z}$. For all $a, b, x, y \in \mathbb{Z}$, if $x \in [a]_n$ and $y \in [b]_n$, then $x+y \in [a+b]_n$ and $xy \in [ab]_n$.

Proof.
Let $n \in \mathbb{Z}$.
Let $a, b, x, y \in \mathbb{Z}$, and assume $x \in [a]_n$ and $y \in [b]_n$.
Then $x \equiv_n a$ and $y \equiv_n b$.
That is, $x - a \in \langle n \rangle$ and $y - b \in \langle n \rangle$.
Choose $s, t \in \mathbb{Z}$ such that $x - a = ns$ and $y - b = nt$.
Then $(x + y) - (a + b) = x - a + y - b = ns + nt = n(s + t) \in \langle n \rangle$.
Therefore, $(x + y) \equiv_n (a + b)$; hence $x + y \in [a + b]_n$.
Also, $xy - ab = xy - ay + ay - ab = (x - a)y + a(y - b) = nsy + nta$.
Thus, $xy - ab = n(sy + ta) \in \langle n \rangle$.
Therefore, $xy \equiv_n ab$; hence $xy \in [ab]_n$.
Therefore, for all $a, b, x, y \in \mathbb{Z}$, if $x \in [a]_n$ and $y \in [b]_n$, then $x + y \in [a + b]_n$ and $xy \in [ab]_n$. Where the equivalence classes are relative to the relation $\equiv_n$.
Q.E.D. □

Notice that given the equivalence of the statement $x \in [a]_n$ to the statement $[x]_n = [a]_n$, the above theorem may be rewritten as

For all $a, b, x, y \in \mathbb{Z}$, if $[x]_n = [a]_n$ and $[y]_n = [b]_n$, then $[x+y]_n = [a+b]_n$ and $[xy]_n = [ab]_n$.

That is, the result of addition and multiplication is independent of the choice of representative for the equivalence class. This enables us to define addition and multiplication of the equivalence classes themselves. For example, since modulo 5 we see that any element of $[2]_5$ added to any element of $[4]_5$ results in an element of $[1]_5$, we can define without ambiguity $[2]_5 + [4]_5 = [1]_5$. Similarly, since any element of $[2]_5$ multiplied by any element of $[4]_5$ produces an element of $[3]_5$, we may define $[2]_5[4]_5 = [3]_5$. In general, we define the following addition and multiplication of equivalence classes:

Definition 3.1.7. For $n \in \mathbb{N}$, relative to the relation $\equiv_n$, we define for $x, y \in \mathbb{Z}$, $[x]_n + [y]_n = [x + y]_n$ and $[x]_n[y]_n = [xy]_n$.

We encourage caution when working with addition and multiplication of equivalence classes, since the addition and multiplication as defined here do not necessarily satisfy all of the same axioms that addition and multiplication in the integers of real numbers satisfy. For example, in the integers, if we know that $2x = 6$, we can deduce that $x = 3$. The same deduction cannot be made in, for example, in the integers modulo 8. The integers modulo 8 have the following multiplication table:

$\mathbb{Z}_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$
$[1]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[2]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[3]_8$	$[0]_8$	$[3]_8$	$[6]_8$	$[1]_8$	$[4]_8$	$[7]_8$	$[2]_8$	$[5]_8$
$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$
$[5]_8$	$[0]_8$	$[5]_8$	$[2]_8$	$[7]_8$	$[4]_8$	$[1]_8$	$[6]_8$	$[3]_8$
$[6]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$
$[7]_8$	$[0]_8$	$[7]_8$	$[6]_8$	$[5]_8$	$[4]_8$	$[3]_8$	$[2]_8$	$[1]_8$

We see that $[2]_8[x]_8 = [6]_8$ has two solutions: $[x]_8 = [3]_8$ and $[x]_8 = [7]_8$. The reason we cannot solve linear equations in the integers modulo 8 is that $\mathbb{Z}_8$ does not satisfy the factors of zero axiom. In the integers, we have that $\forall x, y \in \mathbb{Z}$, if $xy = 0$, then $x = 0$ or $y = 0$. Whereas in $\mathbb{Z}_8$, there are many non-zero equivalence classes that multiply to produce the zero equivalence class. For example, $[2]_8[4]_8 = [0]_8$, $[4]_8[4]_8 = [0]_8$, and $[4]_8[6]_8 = [0]_8$.

Exercises 3.1.

Let A and B be sets in a universe of discourse U, and let X and Y be sets in a universe of discourse V. Let S and T be subsets of $U \times V$. Prove the following propositions.

1. If $A \subseteq B$, then $A \times X \subseteq B \times X$.
2. If $A \subseteq B$ and $X \subseteq Y$, then $A \times X \subseteq B \times Y$.
3. $(A \times X) \cap (B \times Y) = (A \cap B) \times (X \cap Y)$.
4. $(A \times X) \cup (B \times Y) = (A \cup B) \times (X \cup Y)$.
5. If $S \subseteq A \times X$ and $T \subseteq B \times Y$, then $S \cap T \subseteq (A \cap B) \times (X \cap Y)$.
6. If $S \subseteq A \times X$ and $T \subseteq B \times Y$, then $S \cup T \subseteq (A \cup B) \times (X \cup Y)$.
7. $(A \setminus B) \times X = (A \times X) \setminus (B \times X)$.
8. $A \times (X \setminus Y) = (A \times X) \setminus (A \times Y)$.
9. $(A \setminus B) \times (X \setminus Y) \subseteq (A \times X) \setminus (B \times Y)$.
10. $A^c \times X^c \subseteq (A \times X)^c$.
11. $(A \times X)^c = (U \times X^c) \cup (A^c \times V)$.
12. $(A \times X) \setminus (B \times Y) = (A \times (X \setminus Y)) \cup ((A \setminus B) \times X)$.

Prove that each of the following are equivalence relations. Describe the equivalence classes.

13. The relation R on the set $\mathbb{R} \setminus \{0\}$ given by: $\forall x, y \in \mathbb{R} \setminus \{0\}$, xRy if and only if $xy > 0$.
14. The relation $\equiv_{\mathbb{Z}}$ on the set $\mathbb{R}$ given by: $\forall x, y \in \mathbb{R}$, $x \equiv_{\mathbb{Z}} y$ if and only if $x - y \in \mathbb{Z}$.
15. The relation $\equiv_{\mathbb{Q}}$ on the set $\mathbb{R}$ given by: $\forall x, y \in \mathbb{R}$, $x \equiv_{\mathbb{Q}} y$ if and only if $x - y \in \mathbb{Q}$.
16. The relation $\equiv_{\mathbb{Q}^*}$ on the set $\mathbb{R} \setminus \{0\}$ given by: $\forall x, y \in \mathbb{R} \setminus \{0\}$, $x \equiv_{\mathbb{Q}^*} y$ means $\dfrac{x}{y} \in \mathbb{Q}$.
17. The relation R on the set $\mathbb{Z}$ given by: $\forall x, y \in \mathbb{Z}$, xRy if and only if $x^2 = y^2$.
18. The relation R on the set $\mathbb{Z}$ given by: $\forall x, y \in \mathbb{Z}$, xRy if and only if $\exists a, b \in \mathbb{O}$, $ax = by$.
19. The relation R on the set $\mathbb{Z}$ given by: $\forall x, y \in \mathbb{Z}$, xRy if and only if $\exists n \in \mathbb{Z}$, $x = 2^n y$.
20. The relation R on the set $\mathbb{R}$ given by: $\forall x, y \in \mathbb{R}$, xRy if and only if $\exists n \in \mathbb{Z}$, $n - 1 < x \leq n$ and $n - 1 < y \leq n$.
21. The relation R on the set $\mathbb{R}^2$ given by: $\forall (x_1, x_2), (y_1, y_2) \in \mathbb{R}^2$, $(x_1, x_2) R (y_1, y_2)$ if and only if $y_2 + 2x_1 = x_2 + 2y_1$.
22. The relation R on the set $U = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_2 \neq 0\}$ given by $\forall (x_1, x_2), (y_1, y_2) \in U$, $(x_1, x_2) R (y_1, y_2)$ if and only if $\det \begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix} = 0$.
23. The relation R on the set $\mathbb{R}^3$ given by $\forall (x_1, x_2, x_3), (y_1, y_2, y_3) \in \mathbb{R}^3$, $(x_1, x_2, x_3) R (y_1, y_2, y_3)$ if and only if $\exists t \in \mathbb{R} \setminus \{0\}$, $(x_1, x_2, x_3) = (ty_1, ty_2, ty_3)$.
24. The relation R on the set $U = \{A \mid A \text{ is an invertible } 2 \times 2 \text{ matrix}\}$ given by: $\forall A, B \in U$, ARB if and only if $\exists P \in U$, $AP = PB$.

Prove the following propositions. These are analogous to theorem 3.1.13.

25. For the relation $\equiv_{\mathbb{Q}}$ defined in question 15, prove $\forall a, b, x, y \in \mathbb{R}$, if $x \in [a]_{\equiv_{\mathbb{Q}}}$ and $y \in [b]_{\equiv_{\mathbb{Q}}}$, then $x + y \in [a + b]_{\equiv_{\mathbb{Q}}}$.
26. For the relation $\equiv_{\mathbb{Z}}$ defined in question 14, $\forall a, b, x, y \in \mathbb{R}$, if $x \in [a]_{\equiv_{\mathbb{Z}}}$ and $y \in [b]_{\equiv_{\mathbb{Z}}}$, then $x + y \in [a + b]_{\equiv_{\mathbb{Z}}}$.

Prove the following propositions about partitions.

27. Let $A, B \subseteq \mathbb{Z}$ with $A \neq B$. Let $\mathcal{P} = \{A, B\}$. If $\mathcal{P}$ is a partition of $\mathbb{Z}$, then $B \neq \mathbb{Z}$.
28. Let $A, B \subseteq \mathbb{Z}$ with $A \neq B$. Let $\mathcal{P} = \{A, B\}$. If $\mathcal{P}$ is a partition of $\mathbb{Z}$, then $A = \mathbb{Z} \setminus B$.
29. For each $n \in \mathbb{N}$, let $S_n = \{x \in \mathbb{R} \mid n - 1 \leq x^2 < n\}$. Then $\mathcal{A} = \{S_n \mid n \in \mathbb{N}\}$ is a partition of $\mathbb{R}$.
30. $\mathcal{A} = \{(k - 1, k] \mid k \in \mathbb{Z}\}$ is a partition of $\mathbb{R}$.
31. For each $y \in \mathbb{R}$, let $A_y = \{x \in \mathbb{R} \mid y = x^2\}$. Then $\mathcal{A} = \{A_y \mid y \in [0, \infty)\}$ is a partition of $\mathbb{R}$.
32. For the sets A_y as defined in exercise 31, is $\mathcal{B} = \{A_y \mid y \in \mathbb{R}\}$ a partition of $\mathbb{R}$? Prove or disprove.
33. The family of sets $\mathcal{A} = \{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$ is a partition of $\mathbb{Z}$.
34. For each $n \in \mathbb{N}$, the family of sets $\mathcal{A} = \{r + \langle n \rangle \mid r \in \mathbb{Z} \text{ and } 0 \leq r < n\}$ is a partition of $\mathbb{Z}$.
35. $\mathcal{A} = \{\langle 4 \rangle, 2 + \langle 4 \rangle\}$ is a partition of $\langle 2 \rangle$.
36. $\mathcal{A} = \{\langle 6 \rangle, 3 + \langle 6 \rangle\}$ is a partition of $\langle 3 \rangle$.

37. For each $n \in \mathbb{Z}_{\geq 0}$, let $A_n = 2^n + \langle 2^{n+1} \rangle$. Then $\mathcal{A} = \{A_n \mid n \in \mathbb{Z}_{\geq 0}\}$ is a partition of $\mathbb{Z} \setminus \{0\}$.

38. For each $k \in \mathbb{Z}$, let $A_k = \{x \in \mathbb{Z} \mid \exists n \in \mathbb{Z}_{\geq 0},\ x = 2^n + 2^{n+1}k\}$. Then $\mathcal{A} = \{A_k \mid k \in \mathbb{Z}\}$ is a partition of $\mathbb{Z} \setminus \{0\}$.

The following exercises investigate multiplication of congruence classes.

39. Write a complete multiplication table for the family of equivalence classes $\mathbb{Z}_5$.

40. Write a complete multiplication table for the family of equivalence classes $\mathbb{Z}_4$.

41. Write a complete multiplication table for the family of equivalence classes $\mathbb{Z}_6$.

42. Decide whether the following statement is true or false: $\forall x, y \in \mathbb{Z}$, if $[x]_5[y]_5 = [0]_5$, then $[x]_5 = [0]_5$ or $[y]_5 = [0]_5$. To which axiom of the integers is this similar?

43. Prove your answer to exercise 42.

44. Decide whether the following statement is true or false: $\forall x, y \in \mathbb{Z}$, if $[x]_6[y]_6 = [0]_6$, then $[x]_6 = [0]_6$ or $[y]_6 = [0]_6$.

45. Prove your answer to exercise 44.

46. Decide whether the following statement is true or false: $\forall x \in \mathbb{Z}$, if $[x]_5 \neq [0]_5$, then $\exists y \in \mathbb{Z}$, $[x]_5[y]_5 = [1]_5$. To which axiom of the real numbers is this similar?

47. Prove your answer to exercise 46.

48. Decide whether the following statement is true or false: $\forall x \in \mathbb{Z}$, if $[x]_6 \neq [0]_6$, then $\exists y \in \mathbb{Z}$, $[x]_6[y]_6 = [1]_6$.

49. Prove your answer to exercise 48.

50. Use the statement in exercise 42 to prove $\forall x, y, z \in \mathbb{Z}$, if $[x]_5[z]_5 = [y]_5[z]_5$ and $[z]_5 \neq [0]_5$, then $[x]_5 = [y]_5$.

51. Use the statement in exercise 46 to prove $\forall x, y, z \in \mathbb{Z}$, if $[x]_5[z]_5 = [y]_5[z]_5$ and $[z]_5 \neq [0]_5$, then $[x]_5 = [y]_5$.

52. Disprove the statement $\forall x, y, z \in \mathbb{Z}$, if $[x]_6[z]_6 = [y]_6[z]_6$ and $[z]_6 \neq [0]_6$, then $[x]_6 = [y]_6$.

Prove the following propositions about congruence classes.

53. Let $n \in \mathbb{N}$. $\forall x, y, z \in \mathbb{Z}$, $x - y \in [z]_n$ if and only if $x \in [y + z]_n$.

54. $\forall n, m \in \mathbb{Z}$, $(x + \langle n \rangle) \cap (x + \langle m \rangle) = x + \langle n \rangle \cap \langle m \rangle$.

55. $\langle 2 \rangle \setminus \langle 4 \rangle = 2 + \langle 4 \rangle$.

56. $\langle 2 \rangle \setminus (2 + \langle 4 \rangle) = \langle 4 \rangle$.

57. $\langle 3 \rangle \setminus (3 + \langle 6 \rangle) = \langle 6 \rangle$.

58. $\langle 3 \rangle \setminus \langle 6 \rangle = 3 + \langle 6 \rangle$.

59. Let $n \in \mathbb{N}$. $\forall a, x \in \mathbb{Z}$, if $a \in [x]_n$, then $-a \in [-x]_n$.

60. Let $n \in \mathbb{N}$. $\forall a, x \in \mathbb{Z}$, if $a \in [x]_n$, then $\forall m \in \mathbb{N}$, $a^m \in [x^m]_n$.

61. $\forall n \in \mathbb{N}$, if $n \neq 1$ and n is not prime, then $\exists x, y \in \mathbb{Z}$, $[x]_n[y]_n = [0]_n$ but $[x]_n \neq [0]_n$ and $[y]_n \neq [0]_n$.

62. $\forall n \in \mathbb{N}$, if n is prime, then $\forall x, y \in \mathbb{Z}$, if $[x]_n[y]_n = [0]_n$, then $[x]_n = [0]_n$ or $[y]_n = [0]_n$. (Hint: use the result proven in exercise 23 of section 2.3).

3.2 Order Relations

Order relations are those that express, in some sense, that one element of a set is *smaller* than another element in a set, or that one element *precedes* another element. Simple examples of order relations in everyday life are 'object x is no heavier than object y,' 'event x occurred no later than event y,' 'statement x implies statement y,' 'event x caused event y,' and so on. Each of these expresses a different notion of something being smaller than or preceding something else. For common examples of order relations in mathematics, we have the relation $\leq$ on the set $\mathbb{R}$ as well as on the set $\mathbb{Z}$, and the relation $\subseteq$ on the power set of any set U.

To study order relations in general, we look for properties that are common to all order relations and study all relations having those properties. Consider, for example, the relations $\leq$ on $\mathbb{R}$ and $\subseteq$ on $\mathcal{P}(U)$ for some set U. We notice that both relations are *reflexive*:

$$\forall x \in \mathbb{R},\ x \leq x \text{ and } \forall A \in \mathcal{P}(U),\ A \subseteq A.$$

Likewise, both relations are *transitive*:

$$\forall x, y, z \in \mathbb{R},\ \text{if } x \leq y \text{ and } y \leq z, \text{ then } x \leq z$$

$$\text{and } \forall A, B, C \in \mathcal{P}(U),\ \text{if } A \subseteq B \text{ and } B \subseteq C, \text{ then } A \subseteq C.$$

Moreover, although neither relation is symmetric, both fail to be symmetric in the same way: the only time $x \leq y$ and $y \leq x$ is when $x = y$. Likewise, the only time $A \subseteq B$ and $B \subseteq A$ is when $A = B$. This lack of symmetry in all cases except when the two subjects are equal is called **antisymmetry**:

Definition 3.2.1. Let R be a relation on a set U. R is **antisymmetric** means

$$\forall x, y \in U,\ \text{if } xRy \text{ and } yRx, \text{ then } x = y.$$

Thus, we say that the relations $\leq$ and $\subseteq$ are both *antisymmetric*. To study these two relations simultaneously (along with any other similar order relations), we define the class of relations satisfying these properties:

Definition 3.2.2. Let R be a relation on a set U. R is a **partial ordering** means R is reflexive, antisymmetric, and transitive.

There is one important difference between our two motivating examples $\leq$ and $\subseteq$: There are sets A and B for which neither $A \subseteq B$ nor $B \subseteq A$. For example, $\{0\} \not\subseteq \{1\}$ and $\{1\} \not\subseteq \{0\}$. This is actually a very common occurrence for order relations. For example, consider the common relation 'event x caused event y.' It is possible that events can be so remote that neither event can be said to have caused the other. That is, there are events x and y for which x did not cause y and y did not cause x. However, no such analogy exists for the relation $\leq$ on $\mathbb{R}$. In fact, by trichotomy, we have for all $x, y \in \mathbb{R}$, at least one of $x \leq y$ or $y \leq x$ is always true. To make this distinction, we refer to the relation $\leq$ and others like it as **total orderings**.

Definition 3.2.3. Let R be a relation on a set U. R is a **total ordering** means R is a partial ordering that also satisfies the property

$$\forall x, y \in U,\ xRy \text{ or } yRx.$$

The phrase **linear ordering** is often used as a synonym for *total ordering*.

The 'divides' relation

Another very common example of a partial ordering in mathematics is the *divides* relation on the natural numbers:

Let $|$ denote the relation on $\mathbb{N}$ given by $\forall a, b \in \mathbb{N}$, $a|b$ if and only if $\exists t \in \mathbb{N}$, $b = at$. (that is, a divides b).

Proposition 3.2.1.

The divides relation | on $\mathbb{N}$ is a partial ordering.

Proof.
Let $x \in \mathbb{N}$.
    Putting $t = 1$ gives us $x = xt$; hence $x|x$.
Therefore, | is reflexive.
Let $x, y \in \mathbb{N}$.
    Assume $x|y$ and $y|x$.
        Choose $s, t \in \mathbb{N}$ such that $y = xs$ and $x = yt$.
        Then $x = xst$. Since $x \neq 0$, we then have $st = 1$.
        Since t divides 1, we have $t \leq 1$; hence $t = 1$ since $t \in \mathbb{N}$.
        Therefore, $x = y(1)$, which means $x = y$.
    Therefore, if $x|y$ and $y|x$, then $x = y$.
Hence, | is antisymmetric.
Let $x, y, z \in \mathbb{N}$.
    Assume $x|y$ and $y|z$.
        Choose $s, t \in \mathbb{N}$ such that $y = xs$ and $z = yt$.
        Then $z = x(st)$; hence $x|z$.
    Therefore, if $x|y$ and $y|z$, then $x|z$.
Therefore, | is transitive.
Since | is reflexive, symmetric, and transitive, | is a partial ordering. □

Notice that | is not a total ordering, since for example $2 \nmid 3$ and $3 \nmid 2$.

The divides relation remains a partial ordering if we allow 0 to be in the set. That is, the divides relation is also a partial ordering on the set $\mathbb{Z}_{\geq 0}$. However, if we include negative numbers, the relation fails to be antisymmetric. That is, the divides relation is not a partial ordering on the set $\mathbb{Z}$. The proofs of these facts are left as exercises.

Extreme Elements of a Set

When working with different partial orderings, it is often useful to identify certain extreme elements of a set. In fact, we will see that many common concepts in mathematics (including unions, intersections, greatest common divisors, and least common multiples) are simply the extreme elements of sets considered under different partial orderings. We begin the the most obvious type of extreme elements: the greatest and least elements of the set (if they exist).

Note: throughout this section, we will use the symbol $\preccurlyeq$ to denote an arbitrary partial ordering.

Definition 3.2.4. Let $\preccurlyeq$ be a partial ordering on a set U, and let A be a subset of U. For $a \in U$, a is the **least element** of A means

$$a \in A \text{ and } \forall x \in A,\ a \preccurlyeq x.$$

a is the **greatest element** of A means

$$a \in A \text{ and } \forall x \in A,\ x \preccurlyeq a.$$

It is important to note that not every set has a least or greatest element. For example, the real interval $(0, 1)$ has neither a greatest nor least element under the usual ordering $\leq$. Under the divides relation, the number 1 is the least element of the set $\mathbb{N}$, since $1 \in \mathbb{N}$ and $\forall x \in \mathbb{N}$, $1|x$. Yet, $\mathbb{N}$ has no greatest element under the partial ordering $|$, since there is no natural number a for which $\forall x \in \mathbb{N}$, $x|a$. However, if we extend the divides relation to allow 0 (that is if it is considered as a relation on the set $\mathbb{Z}_{\geq 0}$), then the set $\mathbb{Z}_{\geq 0}$ has both a least and greatest element under the relation $|$.

Proposition 3.2.2.

Under the partial ordering $|$, 1 is the least element of $\mathbb{Z}_{\geq 0}$, and 0 is the greatest element of $\mathbb{Z}_{\geq 0}$.

Proof.
Both 0 and 1 belong to the set $\mathbb{Z}_{\geq 0}$, so it only remains to show:
$\forall x \in \mathbb{Z}_{\geq 0}$, $1|x$, and $\forall x \in \mathbb{Z}_{\geq 0}$, $x|0$.
To this end, let $x \in \mathbb{Z}_{\geq 0}$.
Since $x = x(1)$, we have that 1 divides x.
Since $0 = 0(x)$, we have that x divides 0.
Therefore, $\forall x \in \mathbb{Z}_{\geq 0}$, $1|x$, and $\forall x \in \mathbb{Z}_{\geq 0}$, $x|0$.
Hence, 1 is the least element of $\mathbb{Z}_{\geq 0}$, and 0 is the greatest element of $\mathbb{Z}_{\geq 0}$. □

To see how to interpret the idea of greatest element and least element under different partial orderings, we give a few more examples.

Proposition 3.2.3.

Let U be a set. Under the partial ordering $\subseteq$, $\emptyset$ is the least element of $\mathcal{P}(U)$, and U is the greatest element of $\mathcal{P}(U)$.

Proof.
Since $\emptyset \subseteq U$, we have $\emptyset \in \mathcal{P}(U)$.
Let $X \in \mathcal{P}(U)$.
    Then $\emptyset \subseteq X$.
Therefore, $\forall X \in \mathcal{P}(U)$, $\emptyset \subseteq X$.
Hence, $\emptyset$ is the least element of $\mathcal{P}(U)$.
Since $U \subseteq U$, we have $U \in \mathcal{P}(U)$.
Further, for any $X \in \mathcal{P}(U)$, we have $X \subseteq U$.
Therefore, U is the greatest element of $\mathcal{P}(U)$. □

Proposition 3.2.4.

Under the partial ordering $\subseteq$ on the family of sets $\mathcal{I} = \{\langle n \rangle \mid n \in \mathbb{Z}\}$, $\langle 0 \rangle$ is the least element of $\mathcal{I}$, and $\langle 1 \rangle$ is the greatest element of $\mathcal{I}$.

Proof.
Since $0 \in \mathbb{Z}$, $\langle 0 \rangle \in \{\langle n \rangle \mid n \in \mathbb{Z}\} = \mathcal{I}$.
Let $X \in \mathcal{I}$.
    Then $X = \langle n \rangle$ for some $n \in \mathbb{Z}$. Choose such an n.
    Let $x \in \langle 0 \rangle$.
        Since we can choose $t \in \mathbb{Z}$ with $x = 0t$, we have $x = 0$.
        Therefore, $x = 0(n) \in \langle n \rangle$.
    Therefore, $\langle 0 \rangle \subseteq \langle n \rangle$.
Therefore, $\forall X \in \mathcal{I}$, $\langle 0 \rangle \subseteq X$.
Hence, $\langle 0 \rangle$ is the least element of $\mathcal{I}$.
Likewise, since $1 \in \mathbb{Z}$, we have $\langle 1 \rangle \in \{\langle n \rangle \mid n \in \mathbb{Z}\} = \mathcal{I}$.
Again, let $X \in \mathcal{I}$ and choose $n \in \mathbb{Z}$ with $X = \langle n \rangle$.
    Let $x \in \langle n \rangle$.
        Then $x = (x)(1) \in \langle 1 \rangle$.
    Therefore, $\langle n \rangle \subseteq \langle 1 \rangle$.
Now, $\forall X \in \mathcal{I}$, $X \subseteq \langle 1 \rangle$,
which together with the fact that $\langle 1 \rangle \in \mathcal{I}$ means
$\langle 1 \rangle$ is the greatest element of $\mathcal{I}$. □

Supremum and Infimum of a Set

Besides the greatest and least elements of a set, there are other notions of extreme elements that have important applications. We begin by relaxing the requirement that an extreme element must itself be in the set.

Definition 3.2.5. Let $\preccurlyeq$ be a partial ordering on a set U, and let A be a subset of U. For $a \in U$, a is a **lower bound** of A means

$$\forall x \in A,\ a \preccurlyeq x.$$

a is an **upper bound** of A means

$$\forall x \in A,\ x \preccurlyeq a.$$

The definitions of lower bounds and upper bounds appear similar to those of least and greatest elements, in that both require the extreme element a to satisfy $\forall x \in A,\ a \preccurlyeq x$ and $\forall x \in A,\ x \preccurlyeq a$ respectively. The difference is in the fact that in the case of least and greatest elements, the extreme element a must itself be a member of the set A, whereas to be a lower or upper bound, a need not be in the set A.

For example, the real number 0 is a lower bound of the set $(0, 1)$, but since 0 itself is not in the set, it is not the least element. For another example, under the partial ordering $|$, the natural number 12 is an upper bound of the set $\{1, 2, 3, 4, 6\}$, but again it is not called the greatest element since 12 is not in the set. Likewise, even though $0 \notin \mathbb{N}$, 0 is still an upper bound of the set $\mathbb{N}$ under the partial ordering $|$, since for all $x \in \mathbb{N}$, $x|0$.

Much like least and greatest elements, there are sets for which lower and upper bounds do not exist. For example, the set $\mathbb{R}$ has no upper bounds and no lower bounds under the usual ordering $\leq$. However, unlike least and greatest elements, upper and lower bounds (if they do exist) are not necessarily unique. That is, one set can have multiple lower bounds and multiple upper bounds. For example, for the real interval $(0, 1)$, the numbers 1 and 2 are both upper bounds, since $\forall x \in (0, 1)$, $x \leq 1$ and $\forall x \in (0, 1)$, $x \leq 2$. In fact, any number that is greater than or equal to 1 is an upper bound of $(0, 1)$. Likewise, any number that is less than or equal to 0 is a lower bound of $(0, 1)$. For another example, under the partial ordering $|$, both 36 and 72 are upper bounds of the set $\{6, 12, 18\}$, and both 2 and 3 are lower bounds of the set $\{6, 12, 18\}$. In fact, for the set $\{6, 12, 18\}$, any multiple of 36 is an upper bound, and any divisor of 6 is a lower bound. In situations where there are many lower or upper bounds, the lower bound that is greatest among all other lower bounds, and likewise the upper bound that is least among all other upper bounds, are often of interest. We take the time to distinguish these particular lower and upper bounds:

Definition 3.2.6. Let R be a partial ordering on a set U, and let A be a subset of U. For $a \in U$, a is the **infimum** of A, denoted $a = \inf(A)$, means a is a lower bound of A and $\forall x \in U$, if x is a lower bound of A, then xRa. The *infimum* is often called by the more descriptive name **the greatest lower bound** of A.

a is the **supremum** of A, denoted $a = \sup(A)$, means a is an upper bound of A and $\forall x \in U$, if x is an upper bound of A, then aRx. The *supremum* is often referred to as **the least upper bound** of A.

Consider the following examples of suprema and infima for sets of real numbers under the usual ordering $\leq$.

Example 3.2.5.

$1 = \inf(1, 3)$, under the partial ordering $\leq$.

Proof.
For any $x \in (1, 3)$, we have $1 < x$; hence $1 \leq x$.
Therefore, $\forall x \in (1, 3)$, $1 \leq x$, which means 1 is a lower bound of the set $(1, 3)$.
Now, let x be any lower bound of the set $(1, 3)$.
    Suppose $1 < x$.
        Since, for example, $2 \in (1, 3)$, we have $x \leq 2$ which means $x < 3$.
        Choosing $y = \frac{1+x}{2}$ gives us $1 < y < x < 3$.
        Then $y \in (1, 3)$. Since x is a lower bound of $(1, 3)$, this means $x \leq y$.
        This gives us the contradiction $y < x$ and $x \leq y$.
    Therefore, $x \leq 1$.
Therefore, if x is a lower bound of $(1, 3)$, then $x \leq 1$.
Therefore, 1 is the greatest lower bound of $(1, 3)$.
That is, $1 = \inf(1, 3)$. □

Example 3.2.6.

$3 = \sup(1, 3)$, under the partial ordering $\leq$.

Proof.
We first prove that 3 is an upper bound of $(1, 3)$:
Let $x \in (1, 3)$.
    Then $x < 3$, which implies $x \leq 3$.
Therefore, $\forall x \in (1, 3)$, $x \leq 3$.
Hence, 3 is an upper bound of $(1, 3)$.
Next we will show that if x is an upper bound of $(1, 3)$, then $3 \leq x$.
To this end, suppose x is an upper bound of $(1, 3)$ but $x < 3$.
    Put $y = \frac{x+3}{2}$, so that $x < y < 3$.
    Since $2 \in (1, 3)$ and x is an upper bound of $(1, 3)$, we have $2 \leq x$.
    By transitivity, $1 < x$; hence $1 < x < y < 3$.
    Therefore, $y \in (1, 3)$, which implies $y \leq x$, since x is an upper bound.
    Then $x < y$ and $y \leq x$, which is a contradiction.
Therefore, if x is an upper bound of $(1, 3)$, then $3 \leq x$.
Thus, $3 = \sup(1, 3)$. □

Example 3.2.7.

$0 = \inf\{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{1}{n}\}$, under the partial ordering $\leq$.

Proof.
To simplify notations, let $A = \{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{1}{n}\}$.
We first prove that 0 is a lower bound of A:
Let $x \in A$.
Choose $n \in \mathbb{N}$ with $x = \frac{1}{n}$.
Since $0 < n$, we have $0 < \frac{1}{n}$; hence $0 \leq x$.
Therefore, $\forall x \in A$, $0 \leq x$.
That is, 0 is a lower bound of A.
Next we will show that if x is a lower bound of A, then $x \leq 0$.
Indeed, suppose x is a lower bound of A but $0 < x$.
By the Archimedean property, choose $n \in \mathbb{N}$ with $\frac{1}{n} < x$.
Then $\frac{1}{n} \in A$, which is a contradiction since x is a lower bound of A.
Therefore, if x is a lower bound of A, then $x \leq 0$.
Thus, $0 = \inf A$. □

Note that even in cases where a set has upper and lower bounds, it is not necessary that an infimum or supremum of the set exist. For example, the set $\{x \in \mathbb{Q} \mid x^2 < 2\}$ has many upper and lower bounds, but it has neither an infimum nor a supremum in $\mathbb{Q}$. The proofs of these statements are left as exercises. However, when the infimum or supremum of a set do exist, they are unique. That is, if there is an infimum, then there is only one. Likewise, if there is a supremum, then there is only one. We give the proof for infimum and leave the similar proof for supremum as an exercise.

Proposition 3.2.8.

Let $\preccurlyeq$ be a partial ordering on a set U, and let $A \subseteq U$. If a and b are both infima of the set A, then $a = b$.

Proof.
Assume both a and b are infima of the set A.
That is, a is a lower bound of A and $\forall x \in U$, if x is a lower bound of A, then $x \preccurlyeq a$.
Likewise, b is a lower bound of A and $\forall x \in U$, if x is a lower bound of A, then $x \preccurlyeq b$.
Now, since b is a lower bound of A and $\forall x \in U$, if x is a lower bound of A, then $x \preccurlyeq a$,
we have $b \preccurlyeq a$.
Similarly, since a is a lower bound of A and $\forall x \in U$, if x is a lower bound of A, then $x \preccurlyeq b$,
we have $a \preccurlyeq b$.
Now, $a \preccurlyeq b$ and $b \preccurlyeq a$; hence $a = b$ by antisymmetry.
Therefore, if a and b are both infima of the set A, then $a = b$. □

Suprema and Infima for Common Orderings

Many common mathematical concepts can be viewed as suprema and infima under different orderings. We give a few examples here and leave some others as exercises.

Proposition 3.2.9.

Let U be a set. Under the partial ordering $\subseteq$ on the set $\mathcal{P}(U)$, $\forall A, B \in \mathcal{P}(U)$, $A \cap B = \inf\{A, B\}$.

Proof.
Let $A, B \in \mathcal{P}(U)$.
    Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$,
    we have that $A \cap B$ is a lower bound of the set $\{A, B\}$.
    Now, suppose C is a lower bound of the set $\{A, B\}$.
        Then $C \subseteq A$ and $C \subseteq B$.
        Let $x \in C$.
            Since $C \subseteq A$, we have $x \in A$.
            Since $C \subseteq B$, we have $x \in B$.
            Since $x \in A$ and $x \in B$, we have $x \in A \cap B$.
        Therefore, $C \subseteq A \cap B$.
    Therefore, if C is a lower bound of the set $\{A, B\}$, then $C \subseteq A \cap B$.
    Therefore, $A \cap B = \inf\{A, B\}$.
Therefore, $\forall A, B \in \mathcal{P}(U)$, $A \cap B = \inf\{A, B\}$. □

Proposition 3.2.10.

Let U be a set. Under the partial ordering $\subseteq$ on the set $\mathcal{P}(U)$, $\forall A, B \in \mathcal{P}(U)$, $A \cup B = \sup\{A, B\}$.

Proof.
Let $A, B \in \mathcal{P}(U)$.
    Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$,
    we have that $A \cup B$ is an upper bound of the set $\{A, B\}$.
    Now, suppose C is an upper bound of the set $\{A, B\}$.
        Then $A \subseteq C$ and $B \subseteq C$.
        Then $A \cup C \subseteq C \cup C = C$ and $A \cup B \subseteq A \cup C$.
        By transitivity, we have $A \cup B \subseteq C$.
    Therefore, if C is an upper bound of the set $\{A, B\}$, then $A \cap B \subseteq C$.
    Therefore, $A \cup B = \sup\{A, B\}$.
Therefore, $\forall A, B \in \mathcal{P}(U)$, $A \cup B = \sup\{A, B\}$. □

Proposition 3.2.11.

Under the partial ordering | on the set $\mathbb{N}$, $\forall a, b \in \mathbb{N}$, $\gcd(a, b) = \inf\{a, b\}$.

Proof.
Let $a, b \in \mathbb{N}$, and let $g = \gcd(a, b)$.
By the definition of $\gcd(a, b)$ (definition 1.2.4), we have $g|a$ and $g|b$.
Therefore, g is a lower bound of the set $\{a, b\}$.
Next, let x be any lower bound of the set $\{a, b\}$.
Hence, $x|a$ and $x|b$.
Then, again by the definition of $\gcd(a, b)$, we have that $x|g$.
Therefore, if x is a lower bound of $\{a, b\}$, then $x|g$.
Thus, g is the greatest lower bound of the set $\{a, b\}$.
Therefore, $\forall a, b \in \mathbb{N}$, $\gcd(a, b) = \inf\{a, b\}$. □

Proposition 3.2.12.

Under the partial ordering | on the set $\mathbb{N}$, $\forall a, b \in \mathbb{N}$, $\operatorname{lcm}(a, b) = \sup\{a, b\}$.

Proof.
Let $a, b \in \mathbb{N}$, and let $f = \operatorname{lcm}(a, b)$.
By the definition of $\operatorname{lcm}(a, b)$ (definition 1.2.5), we have $a|f$ and $b|f$.
Therefore, f is an upper bound of the set $\{a, b\}$.
Now, let x be any upper bound of the set $\{a, b\}$.
This means $a|x$ and $b|x$.
Then, by the definition of $\operatorname{lcm}(a, b)$, we have that $f|x$.
Therefore, if x is an upper bound of $\{a, b\}$, then $f|x$.
Thus, f is the least upper bound of the set $\{a, b\}$.
Therefore, $\forall a, b \in \mathbb{N}$, $\operatorname{lcm}(a, b) = \sup\{a, b\}$. □

Maximal and Minimal Elements of a Set

There is one final notion of an extreme element of a set that warrants some discussion. To illustrate what we intend to mean by 'maximal' or 'minimal' elements of a set, we will begin with some non-mathematical examples. First, imagine a river that flows East to West and a city that occupies the Southern shore of the river. In this way, if a person in the city travels due North from any point, he or she is bound to eventually reach the river. A partial ordering can be defined on the locations in the city by saying $x \preccurlyeq y$ provided $x = y$ or location x is directly South of location y. Thus, a path due North toward the river is an increasing path under this ordering. Now, the points that lie at the edge of the river bank are extreme points in some sense, because they are the furthest points one can reach under this partial ordering. However, they are neither greatest elements nor upper bounds. This is because no point along the river bank is greater than any other point along the river bank, as these points lie East or West of one another. Rather, the points on the edge of the river bank are greatest in the sense that one can go no further than these points; there are no points beyond them.

For another example, consider the partial ordering on humans given by $x \preccurlyeq y$ means $x = y$ or x is a direct descendant of y. That is, under this relation, a person is ordered below his or her mother and father, grandmother and grandfather, great-grandmother and great-grandfather, and so on, but does not stand in any order relation with his or her cousins, aunts, uncles, nephews, siblings, etc. The individuals that are without children are in some sense extreme elements under this relation. It is at these people that each family tree ends. However, since they are not related to their siblings, they are not greatest or least elements of their family trees, nor are they upper or lower bounds. Rather, people without descendants are extreme elements in the sense that there are none beneath them under this ordering.

The extreme elements described in the two preceding paragraphs are examples of elements that can either not be increased or not be decreased. In other words, they are either nonextensible or irreducible. This is what we mean by **maximal** and **minimal** elements. The definitions is as follows.

Definition 3.2.7. Let $\preccurlyeq$ be a partial ordering on a set U, and let A be a subset of U. For $a \in U$, a is a **minimal** element of A means

$$a \in A \text{ and } \forall x \in A, \text{ if } x \preccurlyeq a, \text{ then } x = a.$$

a is a **maximal** element of A means

$$a \in A \text{ and } \forall x \in A, \text{ if } a \preccurlyeq x, \text{ then } x = a.$$

Note that to say a is *minimal* means that there are no elements other than a itself for which $x \preccurlyeq a$. That is, there is nothing strictly smaller than a. Likewise, to say a is *maximal* means that there are no elements but a itself for which $a \preccurlyeq x$. In this way, there is nothing strictly larger than a.

The notions of maximal and minimal are particularly well suited for describing irreducible or nonextensible mathematical objects. For example, the reader who is familiar with linear algebra may know that a basis for a vector space is not contained in any strictly larger linearly independent set and does not contain and strictly smaller spanning sets. Thus, though the proof is beyond the scope of this book, a basis for a vector space may be described as a maximal linearly independent set or as a minimal spanning set. For an example that is within the scope of this course, the following two propositions show that the minimal elements of $\mathbb{N}$ under the divides relation are what we commonly think of as *irreducible* numbers.

Proposition 3.2.13.

For the partial ordering | on the set $\mathbb{N}$ and the subset $A = \{n \in \mathbb{N} \mid n \geq 2\}$, $\forall a \in A$, if a is minimal in A, then a is prime.

Proof.
Let $a \in A$, and assume a is minimal in A.
Let $p, q \in \mathbb{N}$, and assume $a = pq$.
Then $p|a$.
If $p \geq 2$, then $p \in A$, in which case $p = a$ since a is minimal in A.
Thus, if $p \geq 2$, then $p = a$ and hence $q = 1$.
Otherwise, if $p < 2$, then $p = 1$ since $p \in \mathbb{N}$.
Therefore, either $q = 1$ or $p = 1$.
This shows, if $a = pq$, then either $q = 1$ or $p = 1$, which means a is prime.
Therefore, $\forall a \in A$, if a is minimal in A, then a is prime. □

The converse of the above proposition is also true:

Proposition 3.2.14.

For the partial ordering | on the set $\mathbb{N}$ and the subset $A = \{n \in \mathbb{N} \mid n \geq 2\}$, $\forall a \in A$, if a is prime, then a is minimal in A.

Proof.
Let $a \in A$, and assume a is prime.
Since $a \neq 1$, we have $a \geq 2$; hence $a \in A$.
Next, let $x \in A$, and assume $x|a$.
Choose $y \in \mathbb{N}$ such that $a = xy$.
Since a is prime, we have either $x = 1$ or $y = 1$.
In fact, since $x \in A$, it is not the case that $x = 1$,
hence it must be the case that $y = 1$.
Therefore, $a = x(1)$.
Therefore, $\forall x \in A$, if $x|a$, then $a = x$.
Thus, a is minimal in A.
Therefore, $\forall a \in A$, if a is prime, then a is minimal in A. □

Exercises 3.2.

For each of the following, prove that the relation is a partial ordering. If the relation is also a total ordering, prove it. Otherwise, prove that it is not a total ordering.

1. The relation $\preccurlyeq$ on $\mathbb{Q}$ given by: $\forall x, y \in \mathbb{Q}$, $x \preccurlyeq y$ if and only if $y - x \in \mathbb{Z}_{\geq 0}$.
2. The relation $\preccurlyeq$ on $\mathbb{R}$ given by: $\forall x, y \in \mathbb{R}$, $x \preccurlyeq y$ if and only if $y - x \in \mathbb{Q}_{\geq 0}$.
3. The relation $\preccurlyeq$ on $\mathbb{Z}$ given by: $\forall x, y \in \mathbb{Z}$, $x \preccurlyeq y$ if and only if $\exists a \in \mathbb{Z}_{\geq 0}$, $y = x + 3a$.
4. The relation $\preccurlyeq$ on $\mathbb{Z}$ given by: $\forall x, y \in \mathbb{Z}$, $x \preccurlyeq y$ if and only if $\exists n \in \mathbb{Z}_{\geq 0}$, $y = 2^n x$.
5. The relation $\preccurlyeq$ on $\mathbb{R}^2$ given by: $\forall (x_1, x_2), (y_1, y_2) \in \mathbb{R}^2$, $(x_1, x_2) \preccurlyeq (y_1, y_2)$ if and only if $x_1 \leq y_1$ and $x_2 \leq y_2$.
6. The relation $\preccurlyeq$ on $\mathbb{R}^2$ given by: $\forall (x_1, x_2), (y_1, y_2) \in \mathbb{R}^2$, $(x_1, x_2) \preccurlyeq (y_1, y_2)$ if and only if $x_1 < y_1$ or ($x_1 = y_1$ and $x_2 \leq y_2$). (Note: This is known as **lexicographic order** because it is analogous to the ordering used to arrange words in a dictionary.)
7. The relation $\preccurlyeq$ on $\mathbb{R} \times (\mathbb{R} \setminus \{0\})$ given by: $\forall (x_1, x_2), (y_1, y_2) \in \mathbb{R} \times (\mathbb{R} \setminus \{0\})$, $(x_1, x_2) \preccurlyeq (y_1, y_2)$ if and only if $x_1 y_2 = x_2 y_1$ and $x_2 \leq y_2$.
8. The relation $\preccurlyeq$ on $\mathbb{R} \times (\mathbb{R} \setminus \{0\})$ given by: $\forall (x_1, x_2), (y_1, y_2) \in \mathbb{R} \times (\mathbb{R} \setminus \{0\})$, $(x_1, x_2) \preccurlyeq (y_1, y_2)$ if and only if $x_1 y_2 \leq x_2 y_1$ and $x_2 = y_2$.

Prove the following propositions about extensions of the divides relation.

9. The relation $|$ on $\mathbb{Z}$, given by: $\forall x, y \in \mathbb{Z}$, $x|y$ if and only if $\exists q \in \mathbb{Z}$, $y = xq$, is not a partial ordering.
10. The relation $|$ on $\mathbb{Z}_{\geq 0}$, given by: $\forall x, y \in \mathbb{Z}_{\geq 0}$, $x|y$ if and only if $\exists q \in \mathbb{Z}_{\geq 0}$, $y = xq$, is a partial ordering.

Prove the following propositions where the ordering is the usual ordering $\leq$ on $\mathbb{R}$.

11. The set $A = \{x \in \mathbb{Q} \mid x^2 < 2\}$ has both an upper bound and a lower bound in $\mathbb{Q}$.
12. The set $A = \{x \in \mathbb{Q} \mid x^2 < 2\}$ has neither a supremum nor an infimum in $\mathbb{Q}$.
13. $\forall a, b \in \mathbb{R}$, if $a < b$, then $\inf(a, b) = a$.
14. $\forall a, b \in \mathbb{R}$, if $a < b$, then $\sup(a, b) = b$.
15. $\sup\{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{n-1}{n}\} = 1$.
16. $\inf\{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{n+1}{n}\} = 1$.
17. $\inf\{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{2^n+1}{2^n}\} = 1$.
18. $\sup\{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{2^n-1}{2^n}\} = 1$.
19. $\sup\{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{3n-2}{n}\} = 3$.
20. $\inf\{x \in \mathbb{R} \mid \exists n \in \mathbb{N},\ x = \frac{3n+2}{n}\} = 3$.
21. $\sup\{x \in \mathbb{R} \mid \exists a \in (-\infty, 0),\ x = 1 + a\} = 1$.
22. $\inf\{x \in \mathbb{R} \mid \exists a \in (0, \infty),\ x = 1 + a\} = 1$.
23. $\inf\{x \in \mathbb{R} \mid \exists a \in (-\infty, 0),\ x = 1 - a\} = 1$.
24. $\sup\{x \in \mathbb{R} \mid \exists a \in (0, \infty),\ x = 1 - a\} = 1$.
25. $\sup\{x \in \mathbb{R} \mid \exists a \in (-2, 2),\ x = a^2\} = 4$.
26. $\inf\{x \in \mathbb{R} \mid \exists a \in (2, \infty),\ x = a^2\} = 4$.
27. $\inf\{x \in \mathbb{R} \mid \exists a \in [0, 1),\ x^2 = a\} = -1$.
28. $\sup\{x \in \mathbb{R} \mid \exists a \in [0, 1),\ x^2 = a\} = 1$.

Prove the following propositions about the subset ordering.

29. For a family of sets $\mathcal{A} \subseteq \mathcal{P}(U)$, $\bigcap_{S \in \mathcal{A}} S = \inf(\mathcal{A})$ under the partial ordering $\subseteq$.
30. For a family of sets $\mathcal{A} \subseteq \mathcal{P}(U)$, $\bigcup_{S \in \mathcal{A}} S = \sup(\mathcal{A})$ under the partial ordering $\subseteq$.
31. Under the partial ordering $\subseteq$ on the family of sets $\mathcal{I} = \{\langle n \rangle \mid n \in \mathbb{Z}\}$, $\forall a, b \in \mathbb{Z}$, $\langle a \rangle + \langle b \rangle = \sup\{\langle a \rangle, \langle b \rangle\}$.
32. Under the partial ordering $\subseteq$ on the family of sets $\mathcal{I} = \{\langle n \rangle \mid n \in \mathbb{Z}\}$, $\forall a, b \in \mathbb{Z}$, $\langle a \rangle \cap \langle b \rangle = \inf\{\langle a \rangle, \langle b \rangle\}$.

Let $\preccurlyeq$ be a partial ordering on a set U for which $\sup\{x, y\}$ and $\inf\{x, y\}$ exist for all $x, y \in U$. Prove the following propositions.

33. (Idempotence) $\forall x \in U$, $\sup\{x, x\} = x$.
34. (Idempotence) $\forall x \in U$, $\inf\{x, x\} = x$.
35. (Associativity) $\forall x, y, z \in U$, $\inf\{\inf\{x, y\}, z\} = \inf\{x, \inf\{y, z\}\}$.

36. (Associativity) $\forall x, y, z \in U$, $\sup\{\sup\{x, y\}, z\} = \sup\{x, \sup\{y, z\}\}$.
37. (Absorption) $\forall x, y \in U$, $\sup\{x, \inf\{x, y\}\} = x$.
38. (Absorption) $\forall x, y \in U$, $\inf\{x, \sup\{x, y\}\} = x$.
39. (Identity) If b is the greatest element of U, then $\forall x \in U$, $\inf\{x, b\} = x$.
40. (Identity) If a is the least element of U, then $\forall x \in U$, $\sup\{x, a\} = x$.
41. (Annihilator) If b is the greatest element of U, then $\forall x \in U$, $\sup\{x, b\} = b$.
42. (Annihilator) If a is the least element of U, then $\forall x \in U$, $\inf\{x, a\} = a$.
43. $\forall a, x, y \in U$, if $x \preccurlyeq y$, then $\inf\{a, x\} \preccurlyeq \inf\{a, y\}$.
44. $\forall a, x, y \in U$, if $x \preccurlyeq y$, then $\sup\{a, x\} \preccurlyeq \sup\{a, y\}$.
45. If $\preccurlyeq$ is a total ordering, then $\forall x, y \in U$, $\sup\{x, y\} = x$ or $\sup\{x, y\} = y$.
46. If $\preccurlyeq$ is a total ordering, then $\forall x, y \in U$, $\inf\{x, y\} = x$ or $\inf\{x, y\} = y$.

Let $\preccurlyeq$ be a partial ordering on a set U, and let A and B be subsets of U for which $\sup A$, $\inf A$, $\sup B$, and $\inf B$ exist. Prove the following propositions.

47. $\forall a, b \in U$, if a and b are both greatest elements of A, then $a = b$.
48. $\forall a, b \in U$, if a and b are both least elements of A, then $a = b$.
49. $\forall a \in U$, if $a \in A$ and $a = \sup A$, then a is the greatest element of A.
50. $\forall a \in U$, if $a \in A$ and $a = \inf A$, then a is the least element of A.
51. $\forall a \in U$, if a is the least element of A, then $a = \inf A$.
52. $\forall a \in U$, if a is the greatest element of A, then $a = \sup A$.
53. If $\inf A \notin A$, then A does not have a least element.
54. If $\sup A \notin A$, then A does not have a greatest element.
55. If $A \subseteq B$, then $\sup A \preccurlyeq \sup B$.
56. If $A \subseteq B$, then $\inf B \preccurlyeq \inf A$.
57. If $A \neq \emptyset$, then $\inf A \preccurlyeq \sup A$.
58. $\forall a, b \in U$, if a and b are both suprema of A, then $a = b$.
59. $\forall a \in U$, if $\preccurlyeq$ is a total ordering and a is maximal in A, then a is the greatest element of A.
60. $\forall a \in U$, if $\preccurlyeq$ is a total ordering and a is minimal in A, then a is the least element of A.
61. If $\forall x \in B$, $\forall y \in A$, $x \preccurlyeq y$, then $\sup B \preccurlyeq \inf A$.
62. If $\sup B \preccurlyeq \inf A$, then $\forall x \in B$, $\forall y \in A$, $x \preccurlyeq y$.

For the partial ordering $\preccurlyeq_{\mathbb{Z}}$ on the set $\mathbb{Q}$, defined in exercise 1, prove the following propositions.

63. $\frac{1}{2}$ is a maximal element of the set $A = \{x \in \mathbb{Q} \mid 0 \leq x \leq 1\}$.
64. $\frac{1}{2}$ is a minimal element of the set $A = \{x \in \mathbb{Q} \mid 0 \leq x \leq 1\}$.

Let U be a non-empty set with at least two elements, and let $\mathcal{A} = \mathcal{P}(U) \setminus \{\emptyset, U\}$. That is, $\mathcal{A}$ is the family of non-empty, non-trivial subsets of U. Prove the following propositions for the partial ordering $\subseteq$.

65. $\forall a \in U$, $\{a\}$ is a minimal element of $\mathcal{A}$.
66. $\forall a \in U$, $U \setminus \{a\}$ is a maximal element of $\mathcal{A}$.
67. $\forall S \in \mathcal{A}$, if S is a maximal element of $\mathcal{A}$, then $\exists a \in U$, $S = U \setminus \{a\}$.
68. $\forall S \in \mathcal{A}$, if S is a minimal element of $\mathcal{A}$, then $\exists a \in U$, $S = \{a\}$.

3.3 Functions

Functions are often described as rules that relate each element of one set to exactly one element of another set. Informally, we can think of functions as describing a sense in which the elements of one set can be made to correspond to certain elements of another set. For example, the fact that 5-cent candies cost 5 cents each gives us a correspondence between amounts of candies and amounts of money. The different amounts of candy one can purchase can be thought of as the set of natural numbers $\mathbb{N}$ (if we allow the number 1 to represent one candy and so on). Likewise, different amounts of money can be thought of as elements in the set of all real numbers having up to two digits after the decimal. After a moment's thought, we may think to describe this set as $M = \{x \in \mathbb{R} \mid 100x \in \mathbb{N}\}$. Now, the fact that 5-cent candies cost 5 cents tells us that to each number of candies $x \in \mathbb{N}$ corresponds an amount of money $0.05x \in M$. The relation thus described between the elements of $\mathbb{N}$ and the elements of M is an example of a function.

Formally, we define a *function* as a type of *relation*; that is, as a non-empty set of ordered pairs. More specifically, a function is a relation for which each element of the first set is related to one and only one element of the second set. The formal definition is as follows:

Definition 3.3.1. Let A and B be sets. A **function** f from A to B, denoted $f : A \to B$, is defined to be a non-empty subset of $A \times B$ satisfying the properties

1. $\forall x \in A, \exists y \in B, (x, y) \in f$.
2. $\forall x \in A, \forall y_1, y_2 \in B$, if $(x, y_1) \in f$ and $(x, y_2) \in f$, then $y_1 = y_2$.

In this case, we denote $(x, y) \in f$ by $f(x) = y$. We call the set A the **domain** of f and the set B the **codomain** of f.

Notice that the first property

$$\forall x \in A,\ \exists y \in B,\ (x, y) \in f$$

tells us that every element of A is related to some element of B. The second property

$$\forall x \in A,\ \forall y_1, y_2 \in B,\ \text{if } (x, y_1) \in f \text{ and } (x, y_2) \in f, \text{ then } y_1 = y_2$$

tells us that no element of A is related to more than one element of B. Taken together, these two properties say that every element of A is related to one and only one element of B. Because of this, for $x \in A$ and $y \in B$, the notation $y = f(x)$ (indicating that $(x, y) \in f$) makes sense. Indeed, in this case, since $x \in A$, there is exactly one element of B that is related to x, and that element is y. Thus, what we mean by $y = f(x)$ is that y is the one and only one element that f relates to x. In this sense, for any element $x \in A$, we can think of the symbol $f(x)$ as representing that one and only one element in the set B that the function f relates to x. To make sense of this notation, consider the following simple example:

Example 3.3.1.

Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4, 5\}$. The relation $f = \{(1, 1), (2, 3), (3, 5)\} \subseteq A \times B$ is a function, since each element of A is related to one and only one element of B. In function notation, we can describe the pairs in f as: $f(1) = 1$, $f(2) = 3$, and $f(3) = 5$.

Once we understand the definition of a function, the next step is learning to use it. For example, if we want to prove that a given relation is a function, we are required to prove that the two defining properties of a function are true for that relation. For an example of this, we will prove that the relation $f = \{(x, n) \in \mathbb{R} \times \mathbb{Z} \mid n \leq x < n + 1\}$ is a function.

Example 3.3.2.

The relation $f : \mathbb{R} \to \mathbb{Z}$ given by $f = \{(x, n) \in \mathbb{R} \times \mathbb{Z} \mid n \leq x < n + 1\}$ is a function.

Proof.
Let $x \in \mathbb{R}$.
    Let $S = \{n \in \mathbb{Z} \mid n \leq x\}$.
        By the Archimedean property, choose $k \in \mathbb{N}$ with $-x \leq k$.
        Then $-k \leq x$; hence $-k \in S$. Thus, $S \neq \emptyset$.
        Also, by the Archimedean property, we can choose $m \in \mathbb{N}$ with $x < m$.
        Now, for any $s \in S$, we have $s \leq x < m$; hence $s < m$.
        Therefore, S is bounded above by m.
        Applying the well-ordering property, choose $n \in \mathbb{Z}$ to be the largest element of S.
        Since $n \in S$, we have $n \leq x$.
        Since $n + 1 \notin S$, we have $x < n + 1$.
        Therefore, $n \leq x < n + 1$; hence $(x, n) \in f$.
    Therefore, $\exists n \in \mathbb{Z}, (x, n) \in f$.
Therefore, $\forall x \in \mathbb{R}, \exists n \in \mathbb{Z}, (x, n) \in f$.
Next, let $x \in \mathbb{R}$, let $n_1, n_2 \in \mathbb{Z}$, and assume $(x, n_1) \in f$ and $(x, n_2) \in f$.
    Then $n_1 \leq x < n_1 + 1$ and $n_2 \leq x < n_2 + 1$.
    Now, $n_1 < n_2 + 1$ and $n_2 < n_1 + 1$ by transitivity.
    Therefore, $n_1 \leq n_2$ and $n_2 \leq n_1$.
    Thus, $n_1 = n_2$.
Therefore, $\forall x \in \mathbb{R}, \forall n_1, n_2 \in \mathbb{Z}$, if $(x, n_1) \in f$ and $(x, n_2) \in f$, then $n_1 = n_2$.
Therefore, f is a function. □

Since functions are defined to be sets of ordered pairs, to say two functions f and g are equal means $f \subseteq g$ and $g \subseteq f$. However, the following theorem proves that functions are completely determined by the elements corresponding to each $x \in A$. That is, two functions f and g are the same function if and only if they relate each element of A to the same element of B. That is, if and only if $\forall x \in A$, $f(x) = g(x)$.

Theorem 3.3.3.

Let $f : A \to B$ and $g : A \to B$ be functions. $f = g$ if and only if $\forall x \in A$, $f(x) = g(x)$.

Proof.
Assume $f = g$, and let $x \in A$.
Since f and g are functions, by property (1), choose $y_1, y_2 \in B$ with $(x, y_1) \in f$ and $(x, y_2) \in g$.
That is, $f(x) = y_1$ and $g(x) = y_2$.
Since $f = g$ and $(x, y_2) \in g$, we have $(x, y_2) \in f$.
Therefore, $(x, y_1) \in f$ and $(x, y_2) \in f$. So, by property (2), $y_1 = y_2$.
That is, $f(x) = g(x)$.
Therefore, if $f = g$, then $\forall x \in A$, $f(x) = g(x)$.
Conversely, assume $\forall x \in A$, $f(x) = g(x)$.
Let $(x, y) \in f$.
Then $y = f(x)$; hence $y = g(x)$ since $f(x) = g(x)$.
Hence, $(x, y) \in g$.
Therefore, $f \subseteq g$.
Similarly, if $(x, y) \in g$, then $y = g(x)$ so $y = f(x)$; hence $(x, y) \in f$.
Therefore, $g \subseteq f$.
Therefore, if $\forall x \in A$, $f(x) = g(x)$, then $f = g$.
Thus, $f = g$ if and only if $\forall x \in A$, $f(x) = g(x)$. □

The above theorem may seem obvious, but it says something very important about functions: If we know the values $f(x)$ for all $x \in A$, then we know the function, because the function is uniquely determined by these values. We can therefore describe a function simply by stating the value of $f(x)$ for each $x \in A$. Consider, for example, the function $f : \mathbb{R} \to \mathbb{R}$ defined by

$$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 4x\}.$$

Rather than describing this function explicitly as sets of ordered pairs (as we have done here), we could also describe it simply by stating $\forall x \in \mathbb{R}$, $f(x) = 4x$. Indeed, this statement completely determines the function.

Another interesting observation due to the theorem above is that two functions f and g could be described in different ways, for example using two different formulas, and yet if those formulas happen to result in the same value $f(x) = g(x)$ for every choice of $x \in A$, then the two functions will be equal. Consider the following two examples:

Example 3.3.4.

Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be given by $\forall x \in \mathbb{R}$, $f(x) = 4x$, and $\forall x \in \mathbb{R}$, $g(x) = (x+1)^2 - (x-1)^2$. Then $f = g$.

Proof.
Let $x \in \mathbb{R}$.
Then $g(x) = (x+1)^2 - (x-1)^2 = (x^2 + 2x + 1) - (x^2 - 2x + 1) = 4x = f(x)$.
Therefore, $\forall x \in \mathbb{R}$, $f(x) = g(x)$.
Therefore, $f = g$. □

Example 3.3.5.

Let $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$ be given by $\forall n \in \mathbb{N}$, $f(n) = \sum_{k=1}^{n} 2^{k-1}$, and $\forall n \in \mathbb{N}$, $g(n) = 2^n - 1$. Then $f = g$.

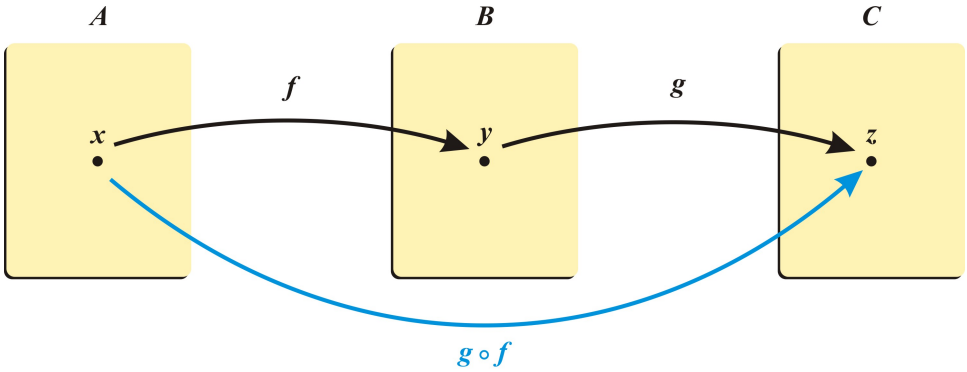
Proof.
Let $A = \{n \in \mathbb{N} \mid f(n) = g(n)\}$.
Since $f(1) = \sum_{k=1}^{1} 2^{k-1} = 2^0 = 1 = 2^1 - 1 = g(1)$, we have $1 \in A$.
Let $n \in \mathbb{N}$ and assume $n \in A$.
Then $f(n) = g(n)$.

$$\begin{aligned} f(n+1) &= \sum_{k=1}^{n+1} 2^{k-1} \\ &= \sum_{k=1}^{n} 2^{k-1} + 2^{(n+1)-1} \\ &= f(n) + 2^n \\ &= g(n) + 2^n \\ &= 2^n - 1 + 2^n \\ &= 2^{n+1} - 1 \\ &= g(n+1) \end{aligned}$$

Therefore, $n + 1 \in A$.
Therefore, $\forall n \in \mathbb{N}$, if $n \in A$, then $n + 1 \in A$.
By the principle of mathematical induction, $\forall n \in \mathbb{N}$, $f(n) = g(n)$.
Therefore, $f = g$. □

Composition of Functions

The **composition** of two functions can be thought of intuitively as the application of two functions in succession. That is, the result of applying one function after another. To make this clear, suppose A, B, and C are sets, and that $f : A \to B$ is a function from A to B, and $g : B \to C$ is a function from B to C. The composition of f and g, denoted $g \circ f$, is the function that results by applying f and g in succession.



Beginning with an element $x \in A$, we can apply the function f resulting in an element $y = f(x) \in B$. We then apply the function g to this element $y \in B$, resulting in an element $z = g(y) \in C$. The net result of this process is a relation between the element $x \in A$ and the element $z \in C$.

Definition 3.3.2. Let $f : A \to B$ and $g : B \to C$ be functions. The **composition** of f and g, denoted $g \circ f$, is the function from A to C given by $\forall x \in A$, $g \circ f(x) = g(f(x))$. In set notation:

$$g \circ f = \{(x, z) \in A \times C \mid \exists y \in B,\ (x, y) \in f \text{ and } (y, z) \in g\}.$$

It often happens that the domain and codomain of a function are the same, meaning $f : A \to A$ for some set A. In this case, it is possible to consider the composition of the function f with itself. i.e. $f \circ f$, which is again a function from A to A. In this case, we can recursively define "powers" of the function f as follows:

Definition 3.3.3. Let $f : A \to A$ be a function. We define $f^1 = f$ and for each $n \in \mathbb{N}$, $f^{n+1} = f^n \circ f$.

Algebra of Functions

Notice that the composition of two functions $g \circ f$ is another function. This means that the composition $\circ$ can be viewed as a *binary operation* on functions. Just as the binary operations + and $\cdot$ each combine two real numbers into another real number, and the binary operations $\cap$ and $\cup$ each combine two sets into another set, the binary operation $\circ$ combines two functions into another function.

The composition operation shares some characteristics with other binary operations we have studied. For example, the operation $\circ$ is associative:

Given functions $f : A \to B$, $g : B \to C$, and $h : C \to D$, we have

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

Indeed, for any $x \in A$, we have

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

However, $\circ$ is not generally commutative. That is, it is not always the case that $f \circ g = g \circ f$. In fact, when $g \circ f$ is defined (i.e. when the codomain of f is equal to the domain of g) the function $f \circ g$ may not be defined, because the codomain of g may not be the same as the domain of f.

There are also functions that play the role of an *identity* under composition. Recall that in the real numbers, we have $\forall x \in \mathbb{R}$, $x + 0 = x$ and $0 + x = x$, making 0 an identity element under the binary operation +. Similarly, the number 1 is an identity under multiplication, since $\forall x \in \mathbb{R}$, $x1 = x$ and $1x = x$. We have also seen that $\emptyset$ and the universe of discourse U are identity elements in $\mathcal{P}(U)$ under the operations $\cup$ and $\cap$ respectively. Indeed, for any $A \in \mathcal{P}(U)$, we have $A \cup \emptyset = A$ and $A \cap U = A$. In the case of composition, the following function fills this role:

Definition 3.3.4. For a set A, the **identity function** on A, $i_A : A \to A$, is the function given by $\forall x \in A$, $i_A(x) = x$.

Proposition 3.3.6.

Let $f : A \to B$ be a function. Then $f \circ i_A = f$ and $i_B \circ f = f$.

Proof.
Let $x \in A$.
Then $f \circ i_A(x) = f(i_A(x)) = f(x)$.
Likewise, $i_B \circ f(x) = i_B(f(x)) = f(x)$
Therefore, $\forall x \in A$, $f \circ i_A(x) = f(x)$, and $i_B \circ f(x) = f(x)$.
It follows from theorem 3.3.3 that $f \circ i_A = f$ and $i_B \circ f = f$. □

Some functions (not all) also have inverses under composition. Recall that in the real numbers, to each $x \in \mathbb{R}$ corresponds an additive inverse $-x$, with the property that $x+(-x) = 0$ and $(-x) + x = 0$. Similarly, to each non-zero $x \in \mathbb{R}$ corresponds a multiplicative inverse x^{-1}, with the property that $xx^{-1} = 1$ and $x^{-1}x = 1$. The analogous idea for a function $f : A \to B$ under the composition operation would be a function whose composition with f results in the identity function. This suggests the following definition:

Definition 3.3.5. For a function $f : A \to B$, f is **invertible** means there is a function $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$. In this case, we write $g = f^{-1}$ and call g the **inverse** of f.

Notice that the definition of *invertibility* requires the *existence* of a function that serves as an inverse in the appropriate way. Thus, if we are to use the definition to prove that a given function is invertible, we must prove the existence of such an inverse function. This means our proof must include a construction of the inverse function. For example:

Example 3.3.7.

The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \dfrac{x-1}{2}$ is invertible.

Proof.
Define the function $g : \mathbb{R} \to \mathbb{R}$ by $\forall x \in \mathbb{R}$, $g(x) = 2x + 1$.
Let $x \in \mathbb{R}$.

$$\begin{aligned} g \circ f(x) &= g(f(x)) \\ &= g\left(\frac{x-1}{2}\right) \\ &= 2\left(\frac{x-1}{2}\right) + 1 \\ &= (x-1) + 1 \\ &= x \\ &= i_{\mathbb{R}}(x) \end{aligned}$$

Therefore, $\forall x \in \mathbb{R}$, $g \circ f(x) = i_{\mathbb{R}}(x)$, which means $g \circ f = i_{\mathbb{R}}$. □

Proofs like the example above are not always obvious since an easily visible formula for the inverse of a function is not always apparent. With a view toward developing our knowledge of invertibility and the tools available for proofs of invertibility, we prove the following theorems.

Theorem 3.3.8.

For any set A, i_A is invertible and $(i_A)^{-1} = i_A$.

Proof.
By proposition 3.3.6, $i_A \circ i_A = i_A$, which means $i_A = (i_A)^{-1}$. □

Theorem 3.3.9.

Let $f : A \to B$ be a function. If f is invertible, then f^{-1} is invertible and $(f^{-1})^{-1} = f$.

Proof. Let $f : A \to B$ be a function.
Assume f is invertible.
Then $f^{-1} : B \to A$ is a function for which $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.
Put another way, f is a function for which $f \circ f^{-1} = i_B$ and $f^{-1} \circ f = i_A$,
which by definition makes f^{-1} invertible and $(f^{-1})^{-1} = f$.
Therefore, if f is invertible, then f^{-1} is invertible and $(f^{-1})^{-1} = f$. □

Theorem 3.3.10.

Let $f : A \to B$ and $g : B \to C$ be functions. If f and g are invertible, then $g \circ f$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. Let $f : A \to B$ and $g : B \to C$ be functions.
Assume f and g are invertible.
Then $f^{-1} : B \to A$ is a function for which $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.
Likewise, $g^{-1} : C \to B$ is a function for which $g^{-1} \circ g = i_B$ and $g \circ g^{-1} = i_C$.
Let $x \in A$.

$$\begin{aligned}(f^{-1} \circ g^{-1}) \circ (g \circ f)(x) &= f^{-1} \circ g^{-1}(g \circ f(x)) \\ &= f^{-1}(g^{-1}(g(f(x)))) \\ &= f^{-1}(g^{-1} \circ g(f(x))) \\ &= f^{-1}(i_B(f(x)) \\ &= f^{-1}(f(x)) \\ &= i_A(x)\end{aligned}$$

Therefore, $\forall x \in A$, $(f^{-1} \circ g^{-1}) \circ (g \circ f)(x) = i_A(x)$. Hence, $(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A$.
Let $z \in C$.

$$\begin{aligned}(g \circ f) \circ (f^{-1} \circ g^{-1})(x) &= g(f(f^{-1}(g^{-1}(z)))) \\ &= g(f \circ f^{-1}(g^{-1}(z))) \\ &= g(i_B(g^{-1}(z))) \\ &= g(g^{-1}(z) \\ &= i_C(z)\end{aligned}$$

Therefore, $\forall z \in C$, $(g \circ f) \circ (f^{-1} \circ g)(z) = i_C(z)$. Hence, $(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_C$.
Now, since $(f^{-1} \circ g^{-1}) \circ (g \circ f) = i_A$ and $(g \circ f) \circ (f^{-1} \circ g^{-1}) = i_C$, we have that $g \circ f$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. □

Criteria for Invertibility

The following two properties together give a necessary and sufficient condition for a function to be invertible.

Definition 3.3.6. For a function $f : A \to B$, f is **injective** (or one-to-one) means

$$\forall x_1, x_2 \in A, \text{ if } f(x_1) = f(x_2), \text{ then } x_1 = x_2.$$

f is **surjective** (or onto) means

$$\forall y \in B, \ \exists x \in A, \ f(x) = y.$$

f is **bijective** means f is both injective and surjective.

Example 3.3.11.

The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \dfrac{x-1}{2}$ is bijective.

Proof.
Let $x_1, x_2 \in \mathbb{R}$, and assume $f(x_1) = f(x_2)$.
Then $\dfrac{x_1 - 1}{2} = \dfrac{x_2 - 1}{2}$.
Multiplying by 2 gives us $x_1 - 1 = x_2 - 1$.
Adding 1 gives us $x_1 = x_2$.
Therefore, $\forall x_1, x_2 \in \mathbb{R}$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.
That is, f is injective.
Next, let $y \in \mathbb{R}$.
Put $x = 2y + 1$.
Then $f(x) = \dfrac{x-1}{2} = \dfrac{(2y+1)-1}{2} = \dfrac{2y}{2} = y$.
Therefore, $\exists x \in \mathbb{R}$, $f(x) = y$.
Therefore, $\forall y \in \mathbb{R}$, $\exists x \in \mathbb{R}$, $f(x) = y$.
That is, f is surjective.
Since f is both injective and surjective, f is bijective. □

Theorem 3.3.12.

Let $f : A \to B$ be a function. f is invertible if and only if f is bijective.

Proof. Let $f : A \to B$ be a function.
Assume f is invertible.
Then there is a function $f^{-1} : B \to A$ for which $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.
Let $x_1, x_2 \in A$, and assume $f(x_1) = f(x_2)$.
Then $f^{-1}(f(x_1)) = f^{-1}(f(x_2))$; hence $f^{-1} \circ f(x_1) = f^{-1} \circ f(x_2)$.
This means $i_A(x_1) = i_A(x_2)$; hence $x_1 = x_2$.
Therefore, $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.
Hence, f is injective.
Next, let $y \in B$.
Put $x = f^{-1}(y)$.
Then $f(x) = f(f^{-1}(y)) = f \circ f^{-1}(y) = i_B(y) = y$.
Therefore, $\exists x \in A$, $f(x) = y$.
Therefore, f is surjective; thus f is bijective.
Conversely, assume f is bijective.
Let $g = \{(y, x) \in B \times A \mid y = f(x)\}$. We will prove that $g : B \to A$ is a function.
Let $y \in B$.
Since f is surjective, we can choose $x \in A$ with $y = f(x)$.
For such an x, we have $(y, x) \in g$.
Therefore, $\forall y \in B$, $\exists x \in A$, $(y, x) \in B$.
Next, let $y \in B$ and $x_1, x_2 \in A$, and assume $(y, x_1) \in g$ and $(y, x_2) \in g$.
Then $y = f(x_1)$ and $y = f(x_2)$.
Since $f(x_1) = f(x_2)$ and f is injective, we have $x_1 = x_2$.
Therefore, $\forall y \in B$, $\forall x_1, x_2 \in A$, if $(y, x_1) \in g$ and $(y, x_2) \in g$, then $x_1 = x_2$.
Therefore, g is a function.
Now, for any $x \in A$, letting $y = f(x)$ gives us $g(y) = x$.
Then $g \circ f(x) = g(f(x)) = g(y) = x = i_A(x)$.
Thus, $g \circ f = i_A$.
Likewise, for any $y \in B$, letting $x = g(y)$ gives us $y = f(x)$.
Then $f \circ g(y) = f(g(y)) = f(x) = y = i_B(y)$.
Thus, $f \circ g = i_B$.
Therefore, f is invertible and $g = f^{-1}$.
Therefore, f is invertible if and only if f is bijective. □

The theorem above suggests an alternate approach to proving a function is invertible. Rather than finding a formula for the inverse function, as we did previously (and which is sometimes difficult), we can instead prove a function is invertible by proving it is bijective. Consider, for example, the following function (the inverse of which would be very difficult to describe with a formula).

Example 3.3.13.

The function $f : \mathbb{N}^2 \to \mathbb{N}$ given by $f(m, n) = 2^{m-1}(2n - 1)$ is invertible.

Proof. We will show that f is bijective.
Let $(m_1, n_1), (m_2, n_2) \in \mathbb{N}^2$.
Suppose $f(m_1, n_1) = f(m_2, n_2)$ and $m_1 \neq m_2$.
Then $2^{m_1-1}(2n_1 - 1) = 2^{m_2-1}(2n_2 - 1)$.
Without loss of generality, assume $m_1 < m_2$. Then $0 < m_2 - m_1$.
Now, $2n_1 - 1 = 2^{m_2-m_1}(2n_2 - 1)$, which is a contradiction, since the left side is odd and the right is even.
Therefore, if $f(m_1, n_1) = f(m_2, n_2)$, then $m_1 = m_2$.
Therefore, f is injective.
Next, let $A = \{y \in \mathbb{N} \mid \exists (m, n) \in \mathbb{N}^2,\ f(m, n) = y\}$.
Since $f(1, 1) = 2^{1-1}(2(1) - 1) = 1$, we have $1 \in A$.
Let $y \in \mathbb{N}$, and assume $\{1, \ldots, y\} \subseteq A$.
Case 1: $y + 1$ is odd.
Choose $n \in \mathbb{N}$ with $y + 1 = 2n - 1$.
$f(1, n) = 2^{1-1}(2n - 1) = (1)(y + 1) = y + 1$.
Therefore, $y + 1 \in A$.
Case 2: $y + 1$ is even.
Choose $q \in \mathbb{N}$ with $y + 1 = 2q$.
Since $1 \leq q \leq y$, we have $q \in \{1, \ldots, y\}$; hence $q \in A$.
Choose $(m, n) \in \mathbb{N}^2$ with $f(m, n) = q$; that is, $2^{m-1}(2n - 1) = q$.
Now, $f(m + 1, n) = 2^{(m+1)-1}(2n - 1) = 2(2^{m-1})(2n - 1) = 2q = y + 1$.
Therefore, $y + 1 \in A$.
Therefore, if $\{1, \ldots, y\} \subseteq A$, then $y + 1 \in A$.
By the principle of complete induction, $\mathbb{N} \subseteq A$.
Therefore, $\forall y \in \mathbb{N}$, $\exists (m, n) \in \mathbb{N}^2$, $f(m, n) = y$.
Therefore, f is surjective; thus f is bijective.
Now, since f is bijective, it is invertible. □

A remark about 'without loss of generality'

In general, if one introduces an assumption P into a proof, it affects the proposition that is ultimately proven. That is, our conclusion will then only be valid *if* P is true. This means that we can only make an assumption that is consistent with the implication we wish to prove. There is, however, one very important exception to this rule: When our assumption only refers to the *notation* used to express our proposition and has no bearing on the *meaning* of our proposition, then such an assumption can be introduced *without loss of generality*. For example, in the previous proof, we have arbitrary constants m_1 and m_2 and the knowledge that $m_1 \neq m_2$. By trichotomy, this means that either $m_1 < m_2$ or $m_2 < m_1$. However, there is no logical distinction between the natural number denoted by m_1 and the natural number denoted by m_2. The only discernable difference is in the notation that we have chosen to represent them. Hence the assumption that we have chosen to denote the smaller of the numbers by m_1 and the larger by m_2, is an assumption about our *notation* only; it does not interfere with the meaning of the proposition. In fact m_1 and m_2 can be interchanged in the proposition with no impact on its meaning. This means that the additional assumption that $m_1 < m_2$ is only an assumption about our choice of notation and can therefore be made *without loss of generality*. This is so common that one often simply writes 'WLOG, assume...', in place of 'without loss of generality, assume...'.

Images and Pre-Images

We now consider not only how a function $f : A \to B$ relates elements of the domain A to elements of the codomain B, but also how f relates the subsets of the domain A to subsets of the codomain B.

Definition 3.3.7. Let $f : A \to B$ be a function, and let $S \subseteq A$. The **image** of the set S under the function f is the set

$$f(S) = \{y \in B \mid \exists x \in S,\ f(x) = y\}.$$

The set $f(A)$ is called the **image** (or range) of f.

Caution

The notation $f(S)$ is not meant to suggest that the function f is applied to the set S in the same sense that it is applied to an element x. It should be noted that the notation $f(S)$ when $S \subseteq A$ stands for a very different concept than the notation $f(x)$ when $x \in A$. Indeed, when $S \subseteq A$, $f(S)$ is a set; it is $\{y \in B \mid \exists x \in S,\ f(x) = y\}$. On the other hand, when $x \in A$, you will recall from the beginning of this section that $f(x)$ stands for the unique element $y \in B$ for which $(x, y) \in f$. Thus, we must be cautious to consider the context when interpreting this notation.

Proposition 3.3.14.

Let $f : A \to B$ be a function. f is surjective if and only if $f(A) = B$.

Proof. Let $f : A \to B$ be a function.
Assume f is surjective.
    Since B is the universe of discourse in which $f(A)$ is defined, we have $f(A) \subseteq B$.
    Let $y \in B$.
        Since f is surjective, $\exists x \in A$, $f(x) = y$.
        That is, $y \in f(A)$.
    Therefore, $B \subseteq f(A)$; thus $f(A) = B$.
Conversely, assume $f(A) = B$.
    Let $y \in B$.
        Then $y \in f(A)$, since $f(A) = B$.
        That is, $\exists x \in A$, $f(x) = y$.
    Therefore, $\forall y \in B$, $\exists x \in A$, $f(x) = y$.
    Therefore, f is surjective.
Therefore, f is surjective if and only if $f(A) = B$. □

Example 3.3.15.

Let $f : \mathbb{R} \to \mathbb{R}$ be the function given by $\forall x \in \mathbb{R}$, $f(x) = x^2$. Then $f((-1, 2)) = [0, 4)$.

Proof.
Let $y \in f((-1, 2))$.
Then $\exists x \in (-1, 2)$, $y = f(x)$. For such an x, we have $y = f(x) = x^2$ and $-1 < x < 2$.
Now, since $0 \leq x^2$, we have $0 \leq y$.
Since $-2 < -1 < x$, we have $-2 < x$. Then $-2 < x < 2$, and by exercise 127 in section 1.1, we then have $x^2 < 4$.
Now, $0 \leq y$ and $y < 4$, so $y \in [0, 4)$.
Therefore, $f((-1, 2)) \subseteq [0, 4)$.
Conversely, let $y \in [0, 4)$.
Putting $x = \sqrt{y}$, gives us $y = x^2 = f(x)$. Then $0 \leq x^2 < 4$.
Now, since $x = \sqrt{y}$, we have $0 \leq x$; hence $-1 < x$.
Suppose $2 \leq x$.
Then $4 \leq 2x$ and $2x \leq x^2$; hence $4 \leq x^2$.
Since this is a contradiction, we must have $x < 2$.
Therefore, $x \in (-1, 2)$.
Therefore, $\exists x \in (-1, 2)$, $y = f(x)$, which means $y \in f((-1, 2))$.
Therefore, $[0, 4) \subseteq f((-1, 2))$. Thus, $f((-1, 2)) = [0, 4)$. □

Example 3.3.16.

Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ given by

$$\forall x \in \mathbb{Z},\ f(x) = \begin{cases} x & \text{if } x \text{ is even} \\ 2x & \text{if } x \text{ is odd} \end{cases}.$$

Then $f(\langle 3 \rangle) = \langle 6 \rangle$.

Proof.
Let $y \in f(\langle 3 \rangle)$.
Accordingly, choose $x \in \langle 3 \rangle$ with $y = f(x)$, and choose $t \in \mathbb{Z}$ with $x = 3t$.
In the case where x is odd, we have $y = f(x) = 2x = 6t \in \langle 6 \rangle$.
In the case where x is even, choose $s \in \mathbb{Z}$ with $x = 2s$.
Then $y = f(x) = x = 3x - 2x = 3(2s) - 2(3t) = 6(s - t) \in \langle 6 \rangle$.
Thus, in both cases, $y \in \langle 6 \rangle$.
Therefore, $f(\langle 3 \rangle) \subseteq \langle 6 \rangle$.
Conversely, let $y \in \langle 6 \rangle$.
Choose $q \in \mathbb{Z}$ with $y = 6q$.
Put $x = y$.
Since $x = y = 6q = 2(3q)$, we have that x is even.
Thus, $f(x) = x = y$.
Moreover, $x = 6q = 3(2q) \in \langle 3 \rangle$.
Therefore, $\exists x \in \langle 3 \rangle$, $y = f(x)$; hence $y \in f(\langle 3 \rangle)$.
Therefore, $\langle 6 \rangle \subseteq f(\langle 3 \rangle)$, and so $f(\langle 3 \rangle) = \langle 6 \rangle$. □

Another relationship between subsets of the domain and codomain is given by what we call the *pre-image*.

Definition 3.3.8. Let $f : A \to B$ be a function, and let $V \subseteq B$. The **pre-image** of the set V under the function f is the set

$$f^{-1}(V) = \{x \in A \mid f(x) \in V\}.$$

Example 3.3.17.

Let $f : \mathbb{R} \to \mathbb{R}$ be the function given by $\forall x \in \mathbb{R}$, $f(x) = x^2$. Then $f^{-1}([0, 4)) = (-2, 2)$.

Proof.
Let $x \in f^{-1}([0, 4))$.
Then $f(x) \in [0, 4)$, which means $0 \leq x^2 < 4$.
Therefore, $|x| < 2$ by exercise 128 of section 1.1.
Therefore, $-2 < x < 2$ by proposition 1.1.27.
Thus, $x \in (-2, 2)$.
Therefore, $f^{-1}([0, 4)) \subseteq (-2, 2)$.
Conversely, let $x \in (-2, 2)$
Since $0 \leq x^2$, we have $0 \leq f(x)$.
Since $-2 < x < 2$, by exercise 127 in section 1.1, we have $x^2 < 4$.
Therefore, $0 \leq f(x) < 4$; hence $f(x) \in [0, 4)$.
Therefore, $x \in f^{-1}([0, 4))$.
Therefore, $(-2, 2) \subseteq f^{-1}([0, 4))$. □

Caution

The notation $f^{-1}(V)$ is not meant to suggest that the function f is invertible, or that the inverse of the function f, as discussed previously, is involved in any way. The notation $f^{-1}(V)$ when $V \subseteq B$ stands only for the pre-image of the set V as defined. This notation is also not meant to suggest that the image a pre-image cancel one another out. In many cases, when $S \subseteq A$, $f^{-1}(f(S)) \neq S$. Likewise, when $V \subseteq B$, we often have $f(f^{-1}(V)) \neq V$.

For an example illustrating the fact that for a subset $S \subseteq A$, $f^{-1}(f(S))$ need not be equal to S (thus the pre-image and image are not inverse operations), recall that for $f : \mathbb{R} \to \mathbb{R}$ given by $\forall x \in \mathbb{R}$, $f(x) = x^2$, we have $f((-1, 2)) = [0, 4)$ (see example 3.3.15) and $f^{-1}([0, 4)) = (-2, 2)$ (see example 3.3.18). Combining these, we have

$$f^{-1}(f((-1, 2))) = f^{-1}([0, 4)) = (-2, 2) \neq (-1, 2).$$

For an example of a situation in which $f(f^{-1}(V)) \neq V$ for a subset $V \subseteq B$, consider the following:

Example 3.3.18.

Let $f : \mathbb{R} \to \mathbb{R}$ be the function given by $\forall x \in \mathbb{R}$, $f(x) = x^2$. Then $f(f^{-1}((-4, 4))) = [0, 4)$.

Proof.
Let $y \in f(f^{-1}((-4, 4)))$.
  Then $\exists x \in f^{-1}((-4, 4))$, $y = f(x)$. Choose such an x.
  Since $x \in f^{-1}((-4, 4))$, we have $f(x) \in (-4, 4)$. Thus, $y \in (-4, 4)$.
  In particular, we have $y < 4$.
  Moreover, since $y = f(x) = x^2$, we have $0 \leq y$.
  Thus, $y \in [0, 4)$.
Therefore, $f(f^{-1}((-4, 4))) \subseteq [0, 4)$
Conversely, let $y \in [0, 4)$
  Put $x = \sqrt{y}$.
    Then $y = x^2 = f(x)$; hence $0 \leq f(x) < 4$, since $y \in [0, 4)$.
    Now, since $-4 < 0 \leq f(x)$, we have $-4 < f(x)$; thus, $-4 < f(x) < 4$.
    We now have $f(x) \in (-4, 4)$, which means $x \in f^{-1}((-4, 4))$.
  Therefore, $\exists x \in f^{-1}((-4, 4))$, $y = f(x)$.
  Therefore, $y \in f(f^{-1}((-4, 4)))$.
Therefore, $[0, 4) \subseteq f(f^{-1}((-4, 4)))$.
Thus, $f(f^{-1}((-4, 4))) = [0, 4)$. □

It should be noted that the above examples are made possible by the fact that the function $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = x^2$, is neither injective nor surjective. For a bijective function $f : A \to B$, we indeed have $f^{-1}(f(S)) = S$ whenever $S \subseteq A$, and $f(f^{-1}(V)) = V$ whenever $V \subseteq B$. This fact is demonstrated in the following two theorems.

Theorem 3.3.19.

Let $f : A \to B$ be a function, and let $S \subseteq A$. If f is injective, then $f^{-1}(f(S)) = S$.

Proof.
Assume f is injective.
  Let $a \in f^{-1}(f(S))$.
    Then $f(a) \in f(S)$.
    Therefore, $\exists x \in S$, $f(a) = f(x)$. Choose such an x.
    Since f is injective, we have $a = x$; hence $a \in S$.
  Therefore, $f^{-1}(f(S)) \subseteq S$.
  Conversely, let $a \in S$.
    Then $f(a) \in f(S)$.
    Thus, $a \in f^{-1}(f(S))$.
  Therefore, $S \subseteq f^{-1}(f(S))$.
  Thus, $f^{-1}(f(S)) = S$.
Therefore, if f is injective, then $f^{-1}(f(S)) = S$. □

Theorem 3.3.20.

Let $f : A \to B$ be a function, and let $V \subseteq B$. If f is surjective, then $f(f^{-1}(V)) = V$.

Proof.
Assume f is surjective.
    Let $y \in f(f^{-1}(V))$.
        Then $\exists x \in f^{-1}(V)$, $y = f(x)$.
        Since $x \in f^{-1}(V)$, we have $f(x) \in V$; hence $y \in V$.
    Therefore, $f(f^{-1}(V)) \subseteq V$.
    Conversely, let $y \in V$.
        Since f is surjective, $\exists x \in A$, $y = f(x)$. Choose such an x.
        Since $f(x) = y \in V$, we have $x \in f^{-1}(V)$.
        Therefore, $\exists x \in f^{-1}(V)$, $y = f(x)$; hence $y \in f(f^{-1}(V))$.
    Therefore, $V \subseteq f(f^{-1}(V))$.
    Thus, $f(f^{-1}(V)) = V$.
Therefore, if f is surjective, then $f(f^{-1}(V)) = V$. □

Exercises 3.3.

For each of the following, prove that the relation f is a function. State the domain and codomain of f.

1. $f = \{(x, n) \in (0, 1] \times \mathbb{N} \mid \frac{1}{n+1} < x \leq \frac{1}{n}\}$.
2. $f = \{(x, n) \in \mathbb{R} \times \mathbb{Z} \mid n - 1 < x \leq n\}$.
3. Let $S = \{x \in \mathbb{Z} \mid 0 \leq x < 5\}$.
   $f = \{(x, r) \in \mathbb{N} \times S \mid \exists q \in \mathbb{Z},\ x = 5q + r\}$.
4. Let $n \in \mathbb{N}$ and let $S = \{x \in \mathbb{Z} \mid 0 \leq x < n\}$.
   $f = \{(x, r) \in \mathbb{N} \times S \mid \exists q \in \mathbb{Z},\ x = nq + r\}$.

For each of the following, find expressions for the functions $g \circ f$ and $f \circ g$.

5. $f : \mathbb{Z} \to \mathbb{Z}$, given by $\forall x \in \mathbb{Z},\ f(x) = 2x + 1$.
   $g : \mathbb{Z} \to \mathbb{Z}$, given by
   $$\forall x \in \mathbb{Z},\ g(x) = \begin{cases} x + 1 & \text{if } x \text{ is even} \\ x - 1 & \text{if } x \text{ is odd} \end{cases}.$$
6. $f : \mathbb{Z} \to \mathbb{Z}$, given by $\forall x \in \mathbb{Z},\ f(x) = x^2 - 2x + 1$.
   $g : \mathbb{Z} \to \mathbb{Z}$, given by
   $$\forall x \in \mathbb{Z},\ g(x) = \begin{cases} x - 1 & \text{if } x \text{ is even} \\ x + 1 & \text{if } x \text{ is odd} \end{cases}.$$

Let A, B, and C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. Prove the following.

7. If $\alpha : B \to A$ and $\beta : B \to A$ are functions for which $\alpha \circ f = i_A$ and $f \circ \beta = i_B$, then $\alpha = \beta$. (Thus, the inverse of a function is unique).
8. If f is invertible, then $\forall x \in A$, $\forall y \in B$, $f(x) = y$ if and only if $f^{-1}(y) = x$.
9. Suppose $A = B$, so that $f : A \to A$. If $f \circ f$ is invertible, then f is invertible.
10. Suppose $A = B$, so that $f : A \to A$. If f is invertible, then $f \circ f$ is invertible.
11. If $g \circ f$ is invertible and g is invertible, then f is invertible.
12. If $g \circ f$ is invertible and f is invertible, then g is invertible.

For each of the following, prove the function is bijective.

13. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = \dfrac{5x - 7}{2}$.
14. $f : \mathbb{Q} \to \mathbb{Q}$, given by $\forall x \in \mathbb{Q}$, $f(x) = 6x - 5$.
15. $f : \mathbb{R}^2 \to \mathbb{R}^2$, given by
    $$\forall (x_1, x_2) \in \mathbb{R}^2,\ f(x_1, x_2) = (x_1 + x_2, x_1 - x_2).$$
16. $f : \mathbb{Z}^3 \to \mathbb{Z}^3$, given by
    $$\forall (x_1, x_2, x_3) \in \mathbb{Z}^3, f(x_1, x_2, x_3) = (x_1 + x_2 + x_3, x_2 + x_3, x_3).$$

Let A be a set, and let $f : A \to A$ be a function. Prove the following.

17. If $f \circ f$ is injective, then f is injective.
18. If $f \circ f$ is surjective, then f is surjective.
19. If f is surjective, then $f \circ f$ is surjective.
20. If f is injective, then $f \circ f$ is injective.
21. If f is injective, then $\forall n \in \mathbb{N}$, f^n is injective.
22. If f is surjective, then $\forall n \in \mathbb{N}$, f^n is surjective.
23. If $\exists n \in \mathbb{N}$, f^n is surjective, then f is surjective.
24. If $\exists n \in \mathbb{N}$, f^n is injective, then f is injective.

Let A, B, and C be sets, and let $f : A \to B$ and $g : B \to C$ be functions. Prove the following.

25. If $g \circ f$ is injective, then f is injective.
26. If $g \circ f$ is surjective, then g is surjective.
27. If f and g are surjective, then $g \circ f$ is surjective.
28. If f and g are injective, then $g \circ f$ is injective.
29. If $g \circ f$ is injective and f is surjective, then g is injective.
30. If $g \circ f$ is surjective and g is injective, then f is surjective.

For the given function f and set S, find $f(S)$. Prove your result.

31. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = 2x + 1$.
    (a) $S = [-1, 1)$.
    (b) $S = (-3, 5]$.
32. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = 1 - 2x$.
    (a) $S = (-3, 5]$.

(b) $S = [-1, 1)$.

33. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = x^2$.

(a) $S = [-1, 1)$.

(b) $S = (-3, 5]$.

34. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = 1 - x^2$.

(a) $S = (-3, 5]$.

(b) $S = [-1, 1)$.

35. $f : \mathbb{Z}^2 \to \mathbb{Z}$, given by $\forall x, y \in \mathbb{Z}$, $f(x, y) = x + y$.

(a) $S = \mathbb{E}^2$.

(b) $S = \mathbb{O}^2$.

36. $f : \mathbb{Z}^3 \to \mathbb{Z}^3$, given by

$$\forall (x_1, x_2, x_3) \in \mathbb{Z}^3,\ f(x_1, x_2, x_3) = (x_1 + x_2 + x_3, x_2 + x_3, x_3).$$

(a) $S = \mathbb{O}^3$.

(b) $S = \mathbb{N}^3$.

37. $f : \mathbb{Z} \to \mathbb{Z}$, given by

$$\forall x \in \mathbb{Z},\ f(x) = \begin{cases} x - 1 & \text{if } x \text{ is even} \\ x + 1 & \text{if } x \text{ is odd} \end{cases}.$$

(a) $S = \langle 3 \rangle$.

(b) $S = \mathbb{Z}$.

38. $f : \mathbb{Z} \to \mathbb{Z}$, given by

$$\forall x \in \mathbb{Z},\ f(x) = \begin{cases} 2x - 2 & \text{if } x \text{ is even} \\ 2x & \text{if } x \text{ is odd} \end{cases}.$$

(a) $S = \mathbb{Z}$.

(b) $S = \langle 3 \rangle$.

39. $f : \mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$, given by

$$\forall (m, n) \in \mathbb{Z} \times \mathbb{N},\ f(m, n) = \frac{m}{n}.$$

(a) $S = \mathbb{E} \times (\mathbb{E} \cap \mathbb{N})$.

(b) $S = \mathbb{O} \times (\mathbb{E} \cap \mathbb{N})$.

40. $f : \mathbb{Z} \to \mathbb{Z}_6$, given by $\forall x \in \mathbb{Z}$, $f(x) = [x]_6$.

(a) $S = \langle 3 \rangle$.

(b) $S = \langle 2 \rangle$.

For the given function f and set V, find $f^{-1}(V)$. Prove your result.

41. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = 2x + 1$.

(a) $V = (0, 3]$.

(b) $V = [-1, 5)$.

42. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = 1 - 2x$.

(a) $V = (0, 3]$.

(b) $V = [-1, 5]$.

43. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = x^2$.

(a) $V = (0, 9]$.

(b) $V = [0, 4) \cup (9, 16]$.

44. $f : \mathbb{R} \to \mathbb{R}$, given by $\forall x \in \mathbb{R}$, $f(x) = 1 - x^2$.

(a) $V = (1, 2]$.

(b) $V = [-3, 2)$.

45. $f : \mathbb{Z}^2 \to \mathbb{Z}$, given by $\forall x, y \in \mathbb{Z}$, $f(x, y) = x + y$.

(a) $V = \mathbb{E}$.

(b) $V = \mathbb{O}$.

46. $f : \mathbb{Z} \to \mathbb{Z}$, given by

$$\forall x \in \mathbb{Z},\ f(x) = \begin{cases} x - 1 & \text{if } x \text{ is even} \\ x + 1 & \text{if } x \text{ is odd} \end{cases}.$$

(a) $V = \langle 4 \rangle$.

(b) $V = \langle 3 \rangle$.

47. $f : \mathbb{Z} \to \mathbb{Z}$, given by

$$\forall x \in \mathbb{Z},\ f(x) = \begin{cases} 2x - 2 & \text{if } x \text{ is even} \\ 2x & \text{if } x \text{ is odd} \end{cases}.$$

(a) $V = \{6, 12\}$.

(b) $V = 6 + \langle 8 \rangle$.

48. $f : \mathbb{Z} \to \mathbb{Z}_{15}$, given by $\forall x \in \mathbb{Z}$, $f(x) = [x]_{15}$.

(a) $V = \{[0]_{15}\}$.

(b) $V = \{[0]_{15}, [5]_{15}, [10]_{15}\}$.

Let $f : A \to B$ be a function. Let S and T be subsets of A, and let V and W be subsets of B. Prove the following.

49. $f(S \cup T) \subseteq f(S) \cup f(T)$.

50. $f(S) \cup f(T) \subseteq f(S \cup T)$.

51. $f(S \cap T) \subseteq f(S) \cap f(T)$. Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ and subsets S and T of $\mathbb{R}$ for which $f(S) \cap f(T) \not\subseteq f(S \cap T)$.

52. If f is injective, then $f(S) \cap f(T) \subseteq f(S \cap T)$.

53. If f is injective, then $f(S \setminus T) \subseteq f(S) \setminus f(T)$.

54. $f(S) \setminus f(T) \subseteq f(S \setminus T)$. Give an example of a function $f : \mathbb{R} \to \mathbb{R}$ and subsets S and T of $\mathbb{R}$ for which $f(S \setminus T) \not\subseteq f(S) \setminus f(T)$.

55. If f is injective, then $f(S^c) \subseteq (f(S))^c$.

56. If f is surjective, then $(f(S))^c \subseteq f(S^c)$.

57. $f^{-1}(V \cup W) = f^{-1}(V) \cup f^{-1}(W)$.

58. $f^{-1}(V \cap W) = f^{-1}(V) \cap f^{-1}(W)$.

59. $f^{-1}(V \setminus W) = f^{-1}(V) \setminus f^{-1}(W)$.

60. $f^{-1}(V^c) = (f^{-1}(V))^c$.

61. If $\forall E \in \mathcal{P}(B)$, $E \subseteq f(f^{-1}(E))$, then f is surjective.

62. If $\forall Z \in \mathcal{P}(A)$, $f^{-1}(f(Z)) \subseteq Z$, then f is injective.

63. If f is bijective, then $f(S) = V$ if and only if $f^{-1}(V) = S$.

64. If f is invertible, then

$$\{x \in A \mid f(x) \in V\} = \{x \in A \mid \exists y \in V,\ x = f^{-1}(y)\}.$$

(Hence when f is invertible, the notation $f^{-1}(V)$ is not ambiguous).

The following exercises combine the topics in this section with those in the section 3.1.

65. Let $f : A \to B$ be a function. Let R be the relation on A given by: For all $a, b \in A$, aRb if and only if $f(a) = f(b)$. Prove R is an equivalence relation.

66. Let R be an equivalence relation on a set A. Let $f : A \to A/R$ be the function given by $\forall x \in A$, $f(x) = [x]_R$. Prove $\forall a, b \in A$, aRb if and only if $f(a) = f(b)$.

67. Let $f : A \to B$ be a function. Let R be the relation on A given by: For all $a, b \in A$, aRb if and only if $f(a) = f(b)$. Prove the relation

$$g = \{([x]_R, f(x)) \in A/R \times B \mid x \in A\}$$

is an injective function.

68. Let R be an equivalence relation on a set A. Let $f : A \to A/R$ be the function given by $\forall x \in A$, $f(x) = [x]_R$. Let $g : A/R \to B$ be an injective function. Prove $\forall a, b \in A$, aRb if and only if $g \circ f(a) = g \circ f(b)$.

69. Let $f : A \to B$ be a function, and let $\mathcal{P}$ be a partition of A. Let $\mathcal{Q} = \{f(S) \mid S \in \mathcal{P}\}$. Prove if f is bijective, then $\mathcal{Q}$ is a partition of B.

70. Let $f : A \to B$ be a function, and let $\mathcal{Q}$ be a partition of B. Let $\mathcal{P} = \{f^{-1}(V) \mid V \in \mathcal{Q}\}$. Prove if f is surjective, then $\mathcal{P}$ is a partition of A.

Bibliography

[1] L. Carroll, H. Haughton, and J. Tenniel. *Alice's Adventures in Wonderland and Through the Looking Glass*. Penguin classics. Penguin Books Limited, 1998.

[2] H.W. Eves. *An introduction to the history of mathematics*. The Saunders series. Saunders College Pub., 1983.