Examples of sets are to be found everywhere around us. For example, we can speak of the set of all living human beings, the set of all cities in the US, the set of all sentences of some language, the set of all prime numbers, and so on. Each living human being is an element of the set of all living human beings. Similarly, each prime number is an element of the set of all prime numbers, and so on.

If S is a set and s is an element of S, then we write $s \in S$. If it so happens that s is not an element of S, then we write $s \notin S$. If S is the set whose elements are s, t, and u, then we write $S = \{s, t, u\}$. The left brace and right brace visually indicate the "bounds" of the set, while what is written within the bounds indicates the elements of the set. For example, if $S = \{1, 2, 3\}$, then $2 \in S$, but $4 \notin S$.

Sets are determined by their elements. The order in which the elements of a given set are listed does not matter. For example, $\{1, 2, 3\}$ and $\{3, 1, 2\}$ are the same set. It also does not matter whether some elements of a given set are listed more than once. For instance, $\{1, 2, 2, 2, 3, 3\}$ is still the set $\{1, 2, 3\}$.

Many sets are given a shorthand notation in mathematics because they are used so frequently. A few elementary examples are the set of natural numbers,

$$\{0, 1, 2, \ldots\},$$

denoted by the symbol $\mathbb{N}$, the set of integers,

$$\{\ldots, -2, -1, 0, 1, 2, \ldots\},$$

denoted by the symbol $\mathbb{Z}$, the set of rational numbers, denoted by the symbol $\mathbb{Q}$, and the set of real numbers, denoted by the symbol $\mathbb{R}$.

A set may be defined by a property. For instance, the set of all planets in the solar system, the set of all even integers, the set of all polynomials with real coefficients, and so on. For a property P and an element s of a set S, we write $P(s)$ to indicate that s has the property P. Then the notation $A = \{s \in S : P(s)\}$ indicates that the set A consists of all elements s of S having the property P. The colon : is commonly read as "such that," and is also written as "$|$." So $\{s \in S \,|\, P(s)\}$ is an alternative notation for $\{s \in S : P(s)\}$. For a concrete example, consider $A = \{x \in \mathbb{R} : x^2 = 1\}$. Here the property P is "$x^2 = 1$." Thus, A is the set of all real numbers whose square is one.

Exercise 2.1. In the following sentences, identify the property, and translate the sentence to set notation.

1. The set of all even integers.
2. The set of all odd prime numbers.
3. The set of all cities with population more than one million people.

Exercise 2.2. Give an alternative description of the sets specified below.

1. $\{x \in \mathbb{R} : x^2 = 1\}$.
2. $\{x \in \mathbb{Z} : x > -2 \text{ and } x \leq 3\}$.
3. $\{x \in \mathbb{N} : x = 2y \text{ for some } y \in \mathbb{N}\}$.

2.1 Subset relation

For two sets, we may speak of whether or not one set is contained in the other. Here is how Dedekind defines this relation between sets. Note that Dedekind calls sets *systems*.

A system A is said to be *part* of a system S when every element of A is also an element of S. Since this relation between a system A and a system S will occur continually in what follows, we shall express it briefly by the symbol $A \prec S$. [10, p. 46]

Modern notation for $A \prec S$ is $A \subseteq S$, and we say that A is a *subset* of S. Thus,

$$A \subseteq S \text{ if, and only if, for all } x,\ \text{if } x \in A,\ \text{then } x \in S.$$

When A is not a subset of S, we write $A \nsubseteq S$.

Exercise 2.3. Describe what it means for $A \nsubseteq S$ that is similar to the description of $A \subseteq S$ given above.

Dedekind goes on to show that the subset relation satisfies the following properties.

Exercise 2.4.

1. Show that $A \subseteq A$.
2. Show that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

The first property is usually referred to as *reflexivity* and the second as *transitivity*. Thus, Exercise 2.4 establishes that the subset relation between sets is both reflexive and transitive. Dedekind also defines what it means for A to be a proper part of S.

A system A is said to be a *proper* part of S, when A is part of S, but...S is not a part of A, i.e., there is in S an element which is not an element of A. [10, p. 46]

Nowadays we say that A is a *proper subset* of S, and write $A \subset S$. If A is not a proper subset of S, then we write $A \not\subset S$.

Exercise 2.5.

1. Describe what it means for A to be a proper subset of S.
2. Describe what it means for A not to be a proper subset of S.
3. Show that if $A \subset S$, then $A \subseteq S$.
4. Does the converse hold? Justify your answer.
5. Show that $A \not\subset A$ for each set A.
6. Prove that if $A \subset B$ and $B \subset C$, then $A \subset C$.

The fifth property is usually referred to as *irreflexivity*. Thus, it follows from Exercise 2.5 that being a proper subset is an irreflexive and transitive relation.

As we have already seen, the subset relation $\subseteq$ is defined by means of the membership relation $\in$. However, the two behave quite differently.

Exercise 2.6.

1. Give an example of a set A such that there is a set B with $B \in A$ but $B \nsubseteq A$.
2. Give an example of a set A such that there is a set B with $B \subseteq A$ but $B \notin A$.

2.2 Set equality

We already discussed the membership and subset relations between sets. But when are two sets equal? Dedekind addresses this issue as follows.

...a system S...is completely determined when with respect to every thing it is determined whether it is an element of S or not.[2] The system S is hence the same as the system T, in symbols $S = T$, when every element of S is also element of T, and every element of T is also element of S. [10, p. 45]

Thus, two sets A and B are equal, in notation $A = B$, when they consist of the same elements; that is,

$$A = B \text{ if, and only if, for all } x,\ x \in A \text{ if, and only if, } x \in B.$$

Exercise 2.7. Prove that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

If two sets A and B are not equal, we write $A \neq B$.

Exercise 2.8. Let P be the property "is a prime number" and O be the property "is an odd integer." Consider the sets $A = \{x \in \mathbb{N} : P(x)\}$ and $B = \{x \in \mathbb{N} : O(x)\}$.

1. Examine A and B with respect to the subset relation. What can you conclude? Justify your answer.
2. Are A and B equal? Justify your answer.

Exercise 2.9. Consider the sets

$$A = \{x \in \mathbb{Z} : x = 2(y-2) \text{ for some } y \in \mathbb{Z}\}$$

and

$$B = \{x \in \mathbb{Z} : x = 2z \text{ for some } z \in \mathbb{Z}\}.$$

Are A and B equal? Justify your answer.

[2] We give Dedekind's footnote in full, where he opposes Kronecker's point of view and sides with Cantor in his mathematical battles with Kronecker. "In what manner this determination is brought about, and whether we know a way of deciding upon it, is a matter of indifference for all that follows; the general laws to be developed in no way depend upon it; they hold under all circumstances. I mention this expressly because Kronecker not long ago (*Crelle's Journal*, Vol. 99, pp. 334–336) has endeavored to impose certain limitations upon the free formation of concepts in mathematics which I do not believe to be justified; but there seems to be no call to enter upon this matter with more detail until the distinguished mathematician shall have published his reasons for the necessity or merely the expediency of these limitations."

2.3 Set operations

So far we have studied the membership, subset, and equality relations between sets. But we can also define operations on sets that are somewhat similar to the operations of addition, multiplication, and subtraction of numbers that you are familiar with.

The sum of a collection of sets is obtained by combining the elements of the sets. Nowadays we call this operation *union*. This is how Dedekind defines it.

By the system *compounded* out of any systems $A, B, C, \ldots$ to be denoted $\mathfrak{M}(A, B, C, \ldots)$ we mean that system whose elements are determined by the following prescription: a thing is considered as element of $\mathfrak{M}(A, B, C, \ldots)$ when and only when it is element of some one of the systems $A, B, C, \ldots$, i.e., when it is element of A, *or* B, *or* $C, \ldots$ [10, pp. 46–47]

In the particular case of two sets A and B, the union of A and B is the set consisting of the elements that belong to either A or B. Modern notation for $\mathfrak{M}(A, B)$ is $A \cup B$. Thus,

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

Here the meaning of "or" is inclusive; that is, if it so happens that an element x belongs to both A and B, then x belongs to the union $A \cup B$.

Another useful operation on sets is taking their common part. Nowadays this operation is known as *intersection*. This is how Dedekind defines it.

A thing g is said to be *common* element of the systems $A, B, C, \ldots$, if it is contained in each of these systems (that is in A *and* in B *and* in $C \ldots$). Likewise a system T is said to be a *common part* of $A, B, C, \ldots$ when T is part of each of these systems; and by the *community* of the systems $A, B, C, \ldots$ we understand the perfectly determinate system $\mathfrak{G}(A, B, C, \ldots)$ which consists of all the common elements g of $A, B, C, \ldots$ and hence is likewise a common part of those systems. [10, pp. 48–49]

In the particular case of two sets A and B, the intersection of A and B is the set consisting of the elements of both A and B. Modern notation for $\mathfrak{G}(A, B)$ is $A \cap B$. Thus,

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

We may also define the difference of two sets A and B as the set consisting of those elements of A that do not belong to B. This operation is called *set complement* and is denoted by $-$. Thus,

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

The notations for the set operations $\cup, \cap, -$, for the membership relation $\in$, and for the subset relation $\subseteq$ that we use today were first introduced by the famous Italian mathematician Giuseppe Peano (1858–1932).[3]

[3]More on the life and work of Giuseppe Peano can be found in [13, 15, 18]. Also, our webpage `http://www.cs.nmsu.edu/historical-projects/` offers a variety of historical projects, including an historical project on Peano's work on natural numbers (see [3]).

Exercise 2.10. Let $A = \{2, 3, 5, 7, 11, 13\}$ and $B = \{A, 2, 11, 18\}$.

1. Find $A \cup B$.
2. Find $A \cap B$.
3. Find $A - B$.

Usually the sets that we work with are subsets of some ambient set. For instance, even numbers, odd numbers, and prime numbers are all subsets of the set of integers $\mathbb{Z}$. Such an ambient set is referred to as a *universal set* (or a *set of discourse*) and is denoted by U. In other words, a universal set is the underlying set that all the sets under examination are subsets of. We may thus speak of the set difference $U - A$, which is the set of those elements of U that do not belong to A. The set difference $U - A$ is usually denoted by A^c. Thus,

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

Exercise 2.11. Let $A = \{x \in \mathbb{R} : x^2 = 2\}$ and $B = \{x \in \mathbb{R} : x \geq 0\}$.

1. Find $A \cap B$.
2. Find $A \cup B$.
3. Find $A - B$.
4. For $U = \mathbb{R}$, find A^c and B^c.
5. Find $\mathbb{N} - B$.

2.4 Empty set

As we saw in Exercise 2.11, the set operations may yield a set containing no elements.

Exercise 2.12.

1. Let A be any set and let E be a set containing no elements. Prove that $E \subseteq A$.
2. Conclude that there is a unique set containing no elements.

We call the set containing no elements the *empty set* (or *null set*) and denote it by $\emptyset$.

Exercise 2.13. Give a definition of the empty set.

Exercise 2.14. Consider the following sets:

1. $A = \{x \in \mathbb{Q} : x^2 = 2\}$,
2. $B = \{x \in \mathbb{R} : x^2 + 1 = 0\}$,
3. $C = \{x \in \mathbb{N} : x^2 + 1 < 1\}$.

Can you give an alternative description of each of these sets? Justify your answer.

2.5 Set identities

There are a number of set identities that the set operations of union, intersection, and set difference satisfy. They are very useful in calculations with sets. Below we give a table of such set identities, where U is a universal set and A, B, and C are subsets of U.

Commutative Laws:	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative Laws:	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive Laws:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Idempotent Laws:	$A \cup A = A$	$A \cap A = A$
Absorption Laws:	$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$
Identity Laws:	$A \cup \emptyset = A$	$A \cap U = A$
Universal Bound Laws:	$A \cup U = U$	$A \cap \emptyset = \emptyset$
DeMorgan's Laws:	$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$
Complement Laws:	$A \cup A^c = U$	$A \cap A^c = \emptyset$
Complements of U and $\emptyset$:	$U^c = \emptyset$	$\emptyset^c = U$
Double Complement Law:	$(A^c)^c = A$	
Set Difference Law:	$A - B = A \cap B^c$	

Each of these laws asserts that the set on the right-hand side is equal to the set on the left-hand side. As we now know, this means that the two sets consist of the same elements. For example, to verify the de Morgan law $(A \cup B)^c = A^c \cap B^c$, we need to show that for each x, we have $x \in (A \cup B)^c$ if, and only if, $x \in A^c \cap B^c$. But $x \in (A \cup B)^c$ is equivalent to $x \notin A \cup B$. This is equivalent to $x \notin A$ and $x \notin B$, which is clearly equivalent to $x \in A^c$ and $x \in B^c$. Therefore, $x \in (A \cup B)^c$ is equivalent to $x \in A^c \cap B^c$. Thus, we have verified that $(A \cup B)^c$ and $A^c \cap B^c$ consist of the same elements, which means that $(A \cup B)^c = A^c \cap B^c$. Other set identities in the table can be verified by a similar argument. The next three exercises invite you to verify the remaining set identities in the table. The laws are grouped in these exercises according to the level of difficulty, from very simple to more difficult.

Exercise 2.15.

1. Prove the commutative laws.
2. Prove the associative laws.
3. Prove the idempotent laws.
4. Prove the identity laws.
5. Prove the universal bound laws.

Exercise 2.16.

1. Prove the complement laws.
2. Prove the complement of U and $\emptyset$ laws.
3. Prove the double complement law.
4. Prove the difference law.

Exercise 2.17.

1. Prove the absorbtion laws.

2. Prove the second DeMorgan law.

3. Prove the distributive laws.

Exercise 2.18. Prove the following using only set identities:

1. $(A \cup B) - C = (A - C) \cup (B - C)$.

2. $(A \cup B) - (C - A) = A \cup (B - C)$.

3. $A \cap (((B \cup C^c) \cup (D \cap E^c)) \cap ((B \cup B^c) \cap A^c)) = \emptyset$.

2.6 Cartesian products and powersets

Next we introduce two more operations on sets. Both will play an important role in the second part of the project when we start developing the theory of finite and infinite sets. The first one plays an important role in defining the concept of function between sets, which is one of the key concepts in mathematics. The second one is of great importance in building sets of bigger and bigger sizes.

For two sets A and B, we define the *Cartesian product* of A and B to be the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. This operation on sets is somewhat similar to the product of two numbers. We denote the Cartesian product of A and B by $A \times B$. Thus,

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

Exercise 2.19. Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$.

1. Determine $A \times B$ and $B \times A$.

2. Are $A \times B$ and $B \times A$ equal? Justify your answer.

Exercise 2.20.

1. Let A consist of 4 elements and B consist of 5 elements. How many elements are in $A \times B$? Justify your answer.

2. More generally, let A consist of n elements and B consist of m elements. How many elements are in $A \times B$? Justify your answer.

Given a set A, we may speak of the set of all subsets of A. This is yet another operation on sets which, as we will see, is of great importance. We call the set of all subsets of A the *powerset* of A and denote it by $P(A)$. Thus,

$$P(A) = \{B : B \subseteq A\}.$$

For example, if $A = \{1, 2\}$, then the subsets of A are $\emptyset, \{1\}, \{2\}$, and A. Therefore, $P(A) = \{\emptyset, \{1\}, \{2\}, A\}$.

Exercise 2.21.

1. Determine $P(\emptyset)$.

Chapter 2

Basic Set Theory

> **A set is a Many that allows itself to be thought of as a One.**
> - *Georg Cantor*

This chapter introduces set theory, mathematical induction, and formalizes the notion of mathematical functions. The material is mostly elementary. For those of you new to abstract mathematics elementary does not mean *simple* (though much of the material is fairly simple). Rather, elementary means that the material requires very little previous education to understand it. Elementary material can be quite challenging and some of the material in this chapter, if not exactly rocket science, may require that you adjust you point of view to understand it. The single most powerful technique in mathematics is to adjust your point of view until the problem you are trying to solve becomes simple.

Another point at which this material may diverge from your previous experience is that it will require proof. In standard introductory classes in algebra, trigonometry, and calculus there is currently very little emphasis on the discipline of *proof.* Proof is, however, the central tool of mathematics. This text is for a course that is a students formal introduction to tools and methods of proof.

2.1 Set Theory

A *set* is a collection of distinct objects. This means that $\{1, 2, 3\}$ is a set but $\{1, 1, 3\}$ is not because 1 appears twice in the second collection. The second collection is called a *multiset.* Sets are often specified with curly brace notation. The set of even integers can be written:

$$\{2n : \text{n is an integer}\}$$

The opening and closing curly braces denote a set, $2n$ specifies the members of the set, the colon says "such that" or "where" and everything following the colon are conditions that explain or refine the membership. All correct mathematics can be spoken in English. The set definition above is spoken "The set of twice n where n is an integer".

The only problem with this definition is that we do not yet have a formal definition of the integers. The integers are the set of whole numbers, both positive and negative: $\{0, \pm 1, \pm 2, \pm 3, \ldots\}$. We now introduce the operations used to manipulate sets, using the opportunity to practice curly brace notation.

Definition 2.1 *The* **empty set** *is a set containing no objects. It is written as a pair of curly braces with nothing inside* $\{\}$ *or by using the symbol* $\emptyset$*.*

As we shall see, the empty set is a handy object. It is also quite strange. The set of all humans that weigh at least eight tons, for example, is the empty set. Sets whose definition contains a contradiction or impossibility are often empty.

Definition 2.2 *The* **set membership symbol** $\in$ *is used to say that an object is a member of a set. It has a partner symbol* $\notin$ *which is used to say an object is not in a set.*

Definition 2.3 *We say two sets are* **equal** *if they have exactly the same members.*

Example 2.1 *If*

$$S = \{1, 2, 3\}$$

then $3 \in S$ *and* $4 \notin S$. *The set membership symbol is often used in defining operations that manipulate sets. The set*

$$T = \{2, 3, 1\}$$

is equal to S *because they have the same members: 1, 2, and 3. While we usually list the members of a set in a "standard" order (if one is available) there is no requirement to do so and sets are indifferent to the order in which their members are listed.*

Definition 2.4 *The* **cardinality** *of a set is its* size. *For a finite set, the cardinality of a set is the number of members it contains. In symbolic notation the size of a set* S *is written* $|S|$. *We will deal with the idea of the cardinality of an infinite set later.*

Example 2.2 Set cardinality
For the set $S = \{1, 2, 3\}$ *we show cardinality by writing* $|S| = 3$

We now move on to a number of *operations* on sets. You are already familiar with several operations on numbers such as addition, multiplication, and negation.

Definition 2.5 *The* **intersection** *of two sets* S *and* T *is the collection of all objects that are in both sets. It is written* $S \cap T$. *Using curly brace notation*

$$S \cap T = \{x : (x \in S) \text{ and } (x \in T)\}$$

The symbol *and* in the above definition is an example of a Boolean or logical operation. It is only true when both the propositions it joins are also true. It has a symbolic equivalent $\wedge$. This lets us write the formal definition of intersection more compactly:

$$S \cap T = \{x : (x \in S) \wedge (x \in T)\}$$

Example 2.3 Intersections of sets
Suppose $S = \{1, 2, 3, 5\}$,
$T = \{1, 3, 4, 5\}$, *and* $U = \{2, 3, 4, 5\}$.
Then:

$S \cap T = \{1, 3, 5\}$,

$S \cap U = \{2, 3, 5\}$, *and*

$T \cap U = \{3, 4, 5\}$

Definition 2.6 *If* A *and* B *are sets and* $A \cap B = \emptyset$ *then we say that* A *and* B *are* disjoint, *or* disjoint sets.

Definition 2.7 *The* **union** *of two sets* S *and* T *is the collection of all objects that are in either set. It is written* $S \cup T$. *Using curly brace notion*

$$S \cup T = \{x : (x \in S) \text{ or } (x \in T)\}$$

The symbol *or* is another Boolean operation, one that is true if either of the propositions it joins are true. Its symbolic equivalent is $\vee$ which lets us re-write the definition of union as:

$$S \cup T = \{x : (x \in S) \vee (x \in T)\}$$

Example 2.4 Unions of sets.
Suppose $S = \{1, 2, 3\}$, $T = \{1, 3, 5\}$, *and* $U = \{2, 3, 4, 5\}$.
Then:

$S \cup T = \{1, 2, 3, 5\}$,

$S \cup U = \{1, 2, 3, 4, 5\}$, *and*

$T \cup U = \{1, 2, 3, 4, 5\}$

When performing set theoretic computations, you should declare the domain in which you are working. In set theory this is done by declaring a universal set.

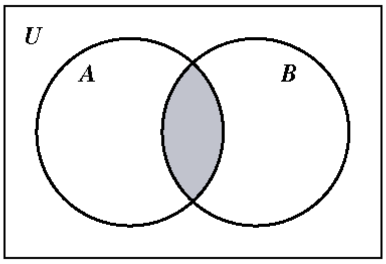
Definition 2.8 *The* **universal set**, *at least for a given collection of set theoretic computations, is the set of all possible objects.*

If we declare our universal set to be the integers then $\{\frac{1}{2}, \frac{2}{3}\}$ is not a well defined set because the objects used to define it are not members of the universal set. The symbols $\{\frac{1}{2}, \frac{2}{3}\}$ do define a set if a universal set that includes $\frac{1}{2}$ and $\frac{2}{3}$ is chosen. The problem arises from the fact that neither of these numbers are integers. The universal set is commonly written $\mathcal{U}$. Now that we have the idea of declaring a universal set we can define another operation on sets.

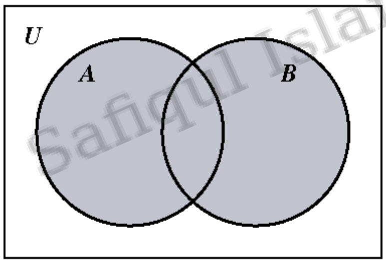
2.1.1 Venn Diagrams

A Venn diagram is a way of depicting the relationship between sets. Each set is shown as a circle and circles overlap if the sets intersect.

Example 2.5 *The following are Venn diagrams for the intersection and union of two sets. The shaded parts of the diagrams are the intersections and unions respectively.*



$A \cap B$



$A \cup B$

Notice that the rectangle containing the diagram is labeled with a U representing the universal set.

Definition 2.9 *The* **compliment** *of a set S is the collection of objects in the universal set that are not in S. The compliment is written S^c. In curly brace notation*

$$S^c = \{x : (x \in \mathcal{U}) \wedge (x \notin S)\}$$

or more compactly as

$$S^c = \{x : x \notin S\}$$

however it should be apparent that the compliment of a set always depends on which universal set is chosen.

There is also a Boolean symbol associated with the complementation operation: the *not* operation. The notation for not is $\neg$. There is not much savings in space as the definition of compliment becomes

$$S^c = \{x : \neg(x \in S)\}$$

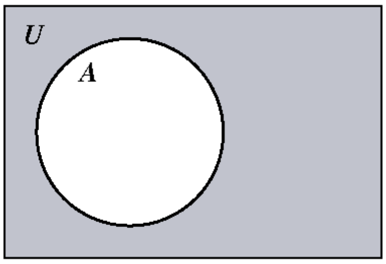
Example 2.6 Set Compliments

(i) Let the universal set be the integers. Then the compliment of the even integers is the odd integers.

(ii) Let the universal set be $\{1, 2, 3, 4, 5\}$, then the compliment of $S = \{1, 2, 3\}$ is $S^c = \{4, 5\}$ while the compliment of $T = \{1, 3, 5\}$ is $T^c = \{2, 4\}$.

(iii) Let the universal set be the letters $\{a, e, i, o, u, y\}$. Then $\{y\}^c = \{a, e, i, o, u\}$.

The Venn diagram for A^c is



A^c

We now have enough set-theory operators to use them to define more operators quickly. We will continue to give English and symbolic definitions.

Definition 2.10 *The* **difference** *of two sets S and T is the collection of objects in S that are not in T. The difference is written $S - T$. In curly brace notation*

$$S - T = \{x : x \in (S \cap (T^c))\},$$

or alternately

$$S - T = \{x : (x \in S) \wedge (x \notin T)\}$$

Notice how intersection and complementation can be used together to create the difference operation and that the definition can be rephrased to use Boolean operations. There is a set of rules that reduces the number of parenthesis required. These are called **operator precedence rules**.

(i) Other things being equal, operations are performed left-to-right.

(ii) Operations between parenthesis are done first, starting with the innermost of nested parenthesis.

(iii) All complimentations are computed next.

(iv) All intersections are done next.

(v) All unions are performed next.

(vi) Tests of set membership and computations, equality or inequality are performed last.

Special operations like the set difference or the symmetric difference, defined below, are not included in the precedence rules and thus always use parenthesis.

Example 2.7 Operator precedence
Since complementation is done before intersection the symbolic definition of the difference of sets can be rewritten:

$$S - T = \{x : x \in S \cap T^c\}$$

If we were to take the set operations

$$A \cup B \cap C^c$$

and put in the parenthesis we would get

$$(A \cup (B \cap (C^c)))$$

Definition 2.11 *The* **symmetric difference** *of two sets S and T is the set of objects that are in one and only one of the sets. The symmetric difference is written $S\Delta T$. In curly brace notation:*

$$S\Delta T = \{(S - T) \cup (T - S)\}$$

Example 2.8 Symmetric differences
Let S be the set of non-negative multiples of two that are no more than twenty four. Let T be the non-negative multiples of three that are no more than twenty four. Then

$$S\Delta T = \{2, 3, 4, 8, 9, 10, 14, 15, 16, 20, 21, 22\}$$

Another way to think about this is that we need numbers that are positive multiples of 2 or 3 (but not both) that are no more than 24.

Another important tool for working with sets is the ability to compare them. We have already defined what it means for two sets to be equal, and so by implication what it means for them to be unequal. We now define another comparator for sets.

Definition 2.12 *For two sets S and T we say that S* **is a subset of** *T if each element of S is also an element of T. In formal notation $S \subseteq T$ if for all $x \in S$ we have $x \in T$.*

If $S \subseteq T$ then we also say T contains S which can be written $T \supseteq S$. If $S \subseteq T$ and $S \neq T$ then we write $S \subset T$ and we say S is a *proper* subset of T.

Example 2.9 Subsets
If $A = \{a, b, c\}$ then A has eight different subsets:

$$\emptyset \quad \{a\} \quad \{b\} \quad \{c\}$$

$$\{a, b\} \quad \{a, c\} \quad \{b, c\} \quad \{a, b, c\}$$

Notice that $A \subseteq A$ and in fact each set is a subset of itself. The empty set $\emptyset$ is a subset of every set.

We are now ready to prove our first proposition. Some new notation is required and we must introduce an important piece of mathematical culture. If we say "A if and only if B" then we mean that either A and B are both true or they are both false in any given circumstance. For example: "an integer x is even if and only if it is a multiple of 2". The phrase "if and only if" is used to establish *logical equivalence*. Mathematically, "A if and only if B" is a way of stating that A and B are simply different ways of saying the same thing. The phrase "if and only if" is abbreviated iff and is represented symbolically as the double arrow $\Leftrightarrow$. Proving an iff statement is done by independently demonstrating that each may be deduced from the other.

Proposition 2.1 *Two sets are equal if and only if each is a subset of the other. In symbolic notation:*

$$(A = B) \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

Proof:

Let the two sets in question be A and B. Begin by assuming that $A = B$. We know that every set is a subset of itself so $A \subseteq A$. Since $A = B$ we may substitute into this expression on the left and obtain $B \subseteq A$. Similarly we may substitute on the right and obtain $A \subseteq B$. We have thus demonstrated that if $A = B$ then A and B are both subsets of each other, giving us the first half of the iff.

Assume now that $A \subseteq B$ and $B \subseteq A$. Then the definition of subset tells us that any element of A is an element of B. Similarly any element of B is an element of A. This means that A and B have the same elements which satisfies the definition of set equality. We deduce $A = B$ and we have the second half of the iff. □

A note on mathematical grammar: the symbol □ indicates the end of a proof. On a paper turned in by a student it is usually taken to mean "I think the proof ends here". Any proof should have a □ to indicate its end. The student should also note the lack of calculations in the above proof. If a proof cannot be read back in (sometimes overly formal) English then it is probably incorrect. Mathematical symbols should be used for the sake of brevity or clarity, not to obscure meaning.

Proposition 2.2 De Morgan's Laws *Suppose that S and T are sets. DeMorgan's Laws state that*

(i) $(S \cup T)^c = S^c \cap T^c$*, and*

(ii) $(S \cap T)^c = S^c \cup T^c$*.*

Proof:

Let $x \in (S \cup T)^c$; then x is not a member of S or T. Since x is not a member of S we see that $x \in S^c$. Similarly $x \in T^c$. Since x is a member of both these sets we see that $x \in S^c \cap T^c$ and we see that $(S \cup T)^c \subseteq S^c \cap T^c$. Let $y \in S^c \cap T^c$. Then the definition of intersection tells us that $y \in S^c$ and $y \in T^c$. This in turn lets us deduce that y is not a member of $S \cup T$, since it is not in either set, and so we see that $y \in (S \cup T)^c$. This demonstrates that $S^c \cap T^c \subseteq (S \cup T)^c$. Applying Proposition 2.1 we get that $(S \cup T)^c = S^c \cap T^c$ and we have proven part (i). The proof of part (ii) is left as an exercise. □

In order to prove a mathematical statement you must prove it is always true. In order to disprove a mathematical statement you need only find a single instance where it is false. It is thus possible for a false mathematical statement to be "true most of the time". In the next chapter we will develop the theory of prime numbers. For now we will assume the reader has a modest familiarity with the primes. The statement "Prime numbers are odd" is false once, because 2 is a prime number. All the other prime numbers are odd. The statement is a false one. This very strict definition of what makes a statement true is a convention in mathematics. We call 2 a *counter example*. It is thus necessary to find only one counter-example to demonstrate a statement is (mathematically) false.

Example 2.10 Disproof by counter example
Prove that the statement $A \cup B = A \cap B$ *is false.*

Let $A = \{1, 2\}$ *and* $B = \{3, 4\}$*. Then* $A \cap B = \emptyset$ *while* $A \cup B = \{1, 2, 3, 4\}$*. The sets A and B form a counter-example to the statement.*

Problems

Problem 2.1 *Which of the following are sets? Assume that a proper universal set has been chosen and answer by listing the names of the collections of objects that are sets. Warning: at least one of these items has an answer that, while likely, is not 100% certain.*

(i) $A = \{2, 3, 5, 7, 11, 13, 19\}$

(ii) $B = \{A, E, I, O, U\}$

(iii) $C = \{\sqrt{x} : x < 0\}$

(iv) $D = \{1, 2, A, 5, B, Q, 1, V\}$

(v) E is the list of first names of people in the 1972 phone book in Lawrence Kansas in the order they appear in the book. There were more than 35,000 people in Lawrence that year.

(vi) F is a list of the weight, to the nearest kilogram, of all people that were in Canada at any time in 2007.

(vii) G is a list of all weights, to the nearest kilogram, that at least one person in Canada had in 2007.

Problem 2.2 *Suppose that we have the set* $U = \{n : 0 \leq n < 100\}$ *of whole numbers as our universal set. Let* P *be the prime numbers in* U*, let* E *be the even numbers in* U*, and let* $F = \{1, 2, 3, 5, 8, 13, 21, 34, 55, 89\}$*. Describe the following sets either by listing them or with a careful English sentence.*

(i) E^c,

(ii) $P \cap F$,

(iii) $P \cap E$,

(iv) $F \cap E \cup F \cap E^c$, and

(v) $F \cup F^c$.

Problem 2.3 *Suppose that we take the universal set* $\mathcal{U}$ *to be the integers. Let* S *be the even integers, let* T *be the integers that can be obtained by tripling any one integer and adding one to it, and let* V *be the set of numbers that are whole multiples of both two and three.*

(i) Write S, T, and V using symbolic notation.

(ii) Compute $S \cap T$, $S \cap V$ and $T \cap V$ and give symbolic representations that do not use the symbols S, T, or V on the right hand side of the equals sign.

Problem 2.4 *Compute the cardinality of the following sets. You may use other texts or the internet.*

(i) Two digit positive odd integers.

(ii) Elements present in a sucrose molecule.

(iii) Isotopes of hydrogen that are not radioactive.

(iv) Planets orbiting the same star as the planet you are standing on that have moons. Assume that Pluto is a minor planet.

(v) Elements with seven electrons in their valence shell. Remember that Ununoctium was discovered in 2002 so be sure to use a relatively recent reference.

(vi) Subsets of $S = \{a, b, c, d\}$ with cardinality 2.

(vii) Prime numbers whose base-ten digits sum to ten. Be careful, some have three digits.

Problem 2.5 *Find an example of an infinite set that has a finite complement, be sure to state the universal set.*

Problem 2.6 *Find an example of an infinite set that has an infinite complement, be sure to state the universal set.*

Problem 2.7 *Add parenthesis to each of the following expressions that enforce the operator precedence rules as in Example 2.7. Notice that the first three describe sets while the last returns a logical value (true of false).*

(i) $A \cup B \cup C \cup D$

(ii) $A \cup B \cap C \cup D$

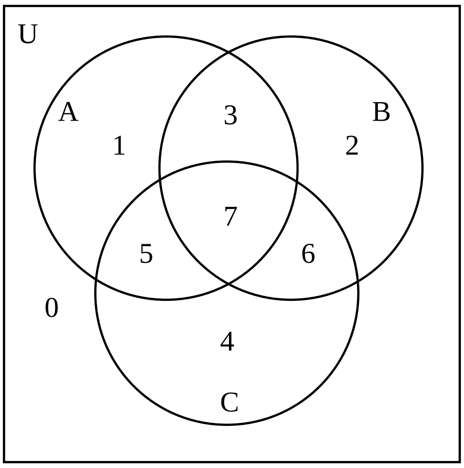
(iii) $A^c \cap B^c \cup C$

(iv) $A \cup B = A \cap C$

Problem 2.8 *Give the Venn diagrams for the following sets.*

(i) $A - B$ (ii) $B - A$ (iii) $A^c \cap B$

(iv) $A \Delta B$ (v) $(A \Delta B)^c$ (vi) $A^c \cup B^c$



Problem 2.9 *Examine the Venn diagram above. Notice that every combination of sets has a unique number in common. Construct a similar collection of four sets.*

Problem 2.10 *Read Problem 2.9. Can a system of sets of this sort be constructed for any number of sets? Explain your reasoning.*

9.5 Equivalence Relations

You know from your early study of fractions that each fraction has many equivalent forms. For example,

$$\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{-1}{-2}, \frac{-3}{-6}, \frac{15}{30}, \ldots$$

are all different ways to represent the same number. They may look different; they may be called different names; but they are all equal. The idea of grouping together things that "look different but are really the same" is the central idea of equivalence relations.

A partition of a set S is a finite or infinite collection of nonempty, mutually disjoint subsets whose union is S.

Definition 1. *A partition of a set S is a collection of disjoint nonempty subsets of S that have S as their union. In other words, the collection of subsets $A_i, i \in I$ (where I is an index set) forms a partition of S if and only if*

(i) $A_i \neq \emptyset$ *for* $i \in I$,

(ii) $A_i \cap A_j = \emptyset$ *when* $i \neq j$, *and*

(iii)

$$\bigcup_{i \in I} A_i = S.$$

(Here the notation $\bigcup_{i \in I}$ represents the union of the sets A_i for all $i \in I$.)

Definition 2. *A relation on a set A is called an equivalence relation if it is reflexive, symmetric, and transitive.*

Recall:

1. R is reflexive if, and only if, $\forall x \in A, x\,R\,x$.
2. R is symmetric if, and only if, $\forall x, y \in A$, if $x\,R\,y$ then $y\,R\,x$.
3. R is transitive if, and only if, $\forall x, y, z \in A$, if $x\,R\,y$ and $y\,R\,z$ then $x\,R\,z$.

Definition 3. *Two elements a and b that are related by an equivalence relation are called equivalent. The notation $a \sim b$ is often used to denote that a and b are equivalent elements with respect to a particular equivalence relation.*

Example 1. *Are these equivalence relations on* $\{0, 1, 2\}$*?*

(a) $\{(0,0), (1,1), (0,1), (1,0)\}$

(b) $\{(0,0), (1,1), (2,2), (0,1), (1,2)\}$

(c) $\{(0,0), (1,1), (2,2), (0,1), (1,2), (1,0), (2,1)\}$

(d) $\{(0,0), (1,1), (2,2), (0,1), (0,2), (1,0), (1,2), (2,0), (2,1)\}$

(e) $\{(0,0), (1,1), (2,2)\}$

Solution. (a) R is not reflexive: $(2,2) \notin R$. Thus, by definition, R is not an equivalence relation.

(b) R is not symmetric: $(1,2) \in R$ but $(2,1) \notin R$. Thus R is not an equivalence relation.

(c) R is not transitive: $(0,1), (1,2) \in R$, but $(0,2) \notin R$. Thus R is not an equivalence relation.

(d) R is reflexive, symmetric, and transitive. Thus R is an equivalence relation.

(e) R is reflexive, symmetric, and transitive. Thus R is an equivalence relation. $\square$

Example 2. *Which of these relations on the set of all functions on $\mathbb{Z} \to \mathbb{Z}$ are equivalence relations?*

(a) $R = \{(f, g) \mid f(1) = g(1)\}$.

(b) $R = \{(f, g) \mid f(0) = g(0) \text{ or } f(1) = g(1)\}$.

Solution. (a) $f(1) = f(1)$, so R is reflexive. If $f(1) = g(1)$, then $g(1) = f(1)$, so R is symmetric. If $f(1) = g(1)$ and $g(1) = h(1)$, then $f(1) = h(1)$, so R is transitive. R is reflexive, symmetric, and transitive, thus R is an equivalence relation.

(b) $f(1) = f(1)$, so R is reflexive. If $f(1) = g(1)$ or $f(0) = g(0)$, then $g(1) = f(1)$ or $g(0) = f(0)$, so R is symmetric. However, R is not transitive: if $f(0) = g(0)$ and $g(1) = h(1)$, it does not necessarily follow that $f(1) = h(1)$ or that $f(0) = h(0)$. Thus R is not an equivalence relation. $\square$

Example 3. *Let R be the relation on $\mathbb{Z} \times \mathbb{Z}$ such that*

$$((a, b), (c, d)) \in R \Leftrightarrow a + d = b + c.$$

Show that R is an equivalence relation.

Solution. R is reflexive: Suppose (a, b) is an ordered pair in $\mathbb{Z} \times \mathbb{Z}$. [We must show that $(a, b)\, R\, (a, b)$.] We have $a + b = a + b$. Thus, by definition of R, $(a, b)\, R\, (a, b)$.

R is symmetric: Suppose (a, b) and (c, d) are two ordered pairs in $\mathbb{Z} \times \mathbb{Z}$ and $(a, b)\, R\, (c, d)$. [We must show that $(c, d)\, R\, (a, b)$.] Since $(a, b)\, R\, (c, d)$, $a + d = b + c$. But this implies that $b + c = a + d$, and so, by definition of R, $(c, d)\, R\, (a, b)$.

R is transitive: Suppose $(a, b), (c, d)$, and (e, f) are elements of $\mathbb{Z} \times \mathbb{Z}$, $(a, b)\, R\, (c, d)$, and $(c, d)\, R\, (e, f)$. [We must show that $(a, b)\, R\, (e, f)$.] Since $(a, b)\, R\, (c, d)$, $a + d = b + c$, which means $a - b = c - d$, and since $(c, d)\, R\, (e, f)C$, $c + f = d + e$, which means $c - d = e - f$. Thus $a - b = e - f$, which means $a + f = b + e$, and so, by definition of R, $(a, b)\, R\, (e, f)$. $\square$

Definition 4. *Suppose A is a set and R is an equivalence relation on A. For each element a in A, the equivalence class of a, denoted $[a]$ and called the class of a for short, is the set of all elements x in A such that x is related to a by R.*

In symbols,

$$[a] = \{x \in A \mid x\, R\, a\}.$$

The procedural version of this definition is

$$\forall x \in A, \quad x \in [a] \Leftrightarrow x\, R\, a.$$

When several equivalence relations on a set are under discussion, the notation $[a]_R$ is often used to denote the equivalence class of a under R.

Theorem 1. *Let R be an equivalence relation on a set A. Let $a, b \in A$. The following are equivalent (TFAE):*

(i) $a\, R\, b$

(ii) $[a] = [b]$

(iii) $[a] \cap [b] \neq \emptyset$.

Proof. [(i) ⇒ (ii)]: Assume that $a\,R\,b$. We will prove that $[a] = [b]$ by showing $[a] \subseteq [b]$ and $[b] \subseteq [a]$. Suppose $c \in [a]$. Then $a\,R\,c$. Because $a\,R\,b$ and R is symmetric, we know that $b\,R\,a$. Furthermore, because R is transitive and $b\,R\,a$ and $a\,R\,c$, it follows that $b\,R\,c$. Hence, $c \in [b]$. This shows that $[a] \subseteq [b]$. The proof that $[b] \subseteq [a]$ is similar.

[(ii) ⇒ (iii)]: Assume that $[a] = [b]$. It follows that $[a] \cap [b] \neq \emptyset$ because $[a]$ is nonempty (because $a \in [a]$ because R is reflexive).

[(iii) ⇒ (i)]: Suppose that $[a] \cap [b] \neq \emptyset$. Then there is an element c with $c \in [a]$ and $c \in [b]$. In other words, $a\,R\,c$ and $b\,R\,c$. By the symmetric property, $c\,R\,b$. Then by transitivity, because $a\,R\,c$ and $c\,R\,b$, we have $a\,R\,b$.

Because (i) implies (ii), (ii) implies (iii), and (iii) implies (i), the three statements, (i), (ii), and (iii), are equivalent. □

Corollary. *If A is a set, R is an equivalence relation on A, and a and b are elements of A, then*

$$\textit{either } [a] \cap [b] = \emptyset \textit{ or } [a] = [b].$$

That is, any two equivalence classes of an equivalence relation are either mutually disjoint or identical.

Theorem 2. *Let R be an equivalence relation on a set A. Then the equivalence classes of R form a partition of A. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set A, there is an equivalence relation R that has the sets $A_i, i \in I$, as its equivalence classes.*

The proof of Theorem 2 is divided into two parts: first, a proof that A is the union of the equivalence classes of R and second, a proof that the intersection of any two distinct equivalence classes is empty. The proof of the first part follows from the fact that the relation is reflexive. The proof of the second part follows from the corollary above.

Proof. Suppose A is a set and R is an equivalence relation on A. For notational simplicity, we assume that R has only a finite number of distinct equivalence classes, which we denote

$$A_1, A_2, \ldots, A_n,$$

where n is a positive integer. (When the number of classes is infinite, the proof is identical except for notation.)

($A = A_1 \cup A_2 \cup \cdots \cup A_n$): [We must show that $A \subseteq A_1 \cup A_2 \cup \cdots \cup A_n$ and $A_1 \cup A_2 \cup \cdots \cup A_n \subseteq A$.]

To show that $A \subseteq A_1 \cup A_2 \cup \cdots \cup A_n$, suppose x is an arbitrary element of A. [We must show that $x \in A_1 \cup A_2 \cup \cdots \cup A_n$.] By reflexivity of R, $x\,R\,x$. But this implies that $x \in [x]$ by definition of class. Since x is in some equivalence class, it must be in one of the distinct equivalence classes $A_1, A_2, \ldots,$ or A_n. Thus $x \in A_i$ for some index i, and hence $x \in A_1 \cup A_2 \cup \cdots \cup A_n$ by definition of union [as was to be shown].

To show that $A_1 \cup A_2 \cup \cdots \cup A_n \subseteq A$, suppose $x \in A_1 \cup A_2 \cup \cdots \cup A_n$. [We must show that $x \in A$.] Then $x \in A_i$ for some $i = 1, 2, \ldots, n$, by definition of union. But each A_i is an equivalence class of R. And equivalence classes are subsets of A. Hence $A_i \subseteq A$ and so $x \in A$ [as was to be shown].

Since $A \subseteq A_1 \cup A_2 \cup \cdots \cup A_n$ and $A_1 \cup A_2 \cup \cdots \cup A_n \subseteq A$, then by definition of set equality, $A = A_1 \cup A_2 \cup \cdots \cup A_n$.

(The distinct classes of R are mutually disjoint): Suppose that A_i and A_j are any two distinct equivalence classes of R. [We must show that A_i and A_j are disjoint.] Since A_i and A_j are distinct, then $A_i \neq A_j$. And since A_i and A_j are equivalence classes of R, there must exist elements a and b in A such that $A_i = [a]$ and $A_j = [b]$. By the corollary to theorem 1,

$$\text{either } [a] \cap [b] = \emptyset \text{ or } [a] = [b].$$

But $[a] \neq [b]$ because $A_i \neq A_j$. Hence $[a] \cap [b] = \emptyset$. Thus $A_i \cap A_j = \emptyset$, and so A_i and A_j are disjoint [as was to be shown]. □

There are m different congruence classes modulo m, corresponding to the m different remainders possible when an integer is divided by m. The m congruence classes are also denoted by $[0]_m, [1]_m, \ldots, [m-1]_m$. They form a partition of the set of integers.

$$[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}.$$

Example 4. *What is equivalence class of* $1, 2$ *for congruence modulo* 5*? Let* $R = \{(a, b) \mid a \equiv b \pmod 5\}$.

Solution. For each integer a,

$$\begin{aligned}
[a] &= \{x \in \mathbb{Z} \mid x\, R\, a\} \\
&= \{x \in \mathbb{Z} \mid 5 \mid (x - a)\} \\
&= \{x \in \mathbb{Z} \mid x - a = 5k, \text{ for some integer } k\}.
\end{aligned}$$

Therefore,

$$[a] = \{x \in \mathbb{Z} \mid x = 5k + a, \text{ for some integer } k\}.$$

In particular,

$$\begin{aligned}
[1] &= \{x \in \mathbb{Z} \mid x = 5k + 1, \text{ for some integer } k\} \\
&= \{\ldots, -14, -9, -4, 1, 6, 11, 16, 21, \ldots\}
\end{aligned}$$

and

$$\begin{aligned}
[2] &= \{x \in \mathbb{Z} \mid x = 5k + 2, \text{ for some integer } k\} \\
&= \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}.
\end{aligned}$$

□

Example 5. *How many distinct equivalence classes are there modulo* 5*?*

Solution. There are five distinct equivalence classes, modulo 5: $[0], [1], [2], [3]$, and $[4]$. □

The last examples above illustrate a very important property of equivalence classes, namely that an equivalence class may have many different names. In the above example, for instance, the class of 0, $[0]$, may also be called the class of 5, $[5]$, or the class of -10, $[-10]$. But what the class is, is the set

$$\{x \in \mathbb{Z} \mid x = 5k, \text{ for some integers } k\}.$$

Definition 5. *Suppose* R *is an equivalence relation on a set* A *and* S *is an equivalence class of* R*. A representative of the class* S *is any element* a *such that* $[a] = S$.

If a is any element of an equivalence class S, then $S = [a]$. Hence every element of an equivalence class is a representative of that class.

Example 6. *Let* A *be the set of all ordered pairs of integers for which the second element of the pair is nonzero. Symbolically,*

$$A = \mathbb{Z} \times (\mathbb{Z} - \{0\}).$$

Define a relation R *on* A *as follows:* $\forall (a, b), (c, d) \in A$,

$$(a, b)\, R\, (c, d) \Leftrightarrow ad = bc.$$

The fact is that R *is an equivalence relation. Describe the distinct equivalence classes of* R.

Solution. There is one equivalence class for each distinct rational number. Each equivalence class consists of all ordered pairs (a, b) that, if written as fractions $\frac{a}{b}$, would equal each other. The reason for this is that the condition for two rational numbers to be equal is the same as the condition for two ordered pairs to be related. For instance, the class of $(1, 2)$ is

$$[(1,2)] = \{(1,2), (-1,-2), (2,4), (-2,-4), (3,6), (-3,-6), \ldots\}$$

because

$$\frac{1}{2} = \frac{-1}{-2} = \frac{2}{4} = \frac{-2}{-4} = \frac{3}{6} = \frac{-3}{-6} = \cdots .$$

It is possible to expand this result to define operations of addition and multiplication on the equivalence classes of R that satisfy all the same properties as the addition and multiplication of rational numbers. It follows that the rational numbers can be defined as equivalence classes of ordered pairs of integers. $\square$

Courtesy (Contents are sourced from) **: ---**

1. An Introduction to Elementary Set Theory by Guram Bezhanishvili and Eachan Landreth, https://www.maa.org/sites/default/files/images/upload_library/46/Pengelley_projects/Project-5/set_theory_project.pdf

2. https://www.math.uh.edu/~dlabate/settheory_Ashlock.pdf

3. https://math.berkeley.edu/~arash/55/9_5.pdf