Demonstration
Proof Beyond the Possibility of Doubt

April 21, 2020

U(M) Mathematics
Contents

PART I  MATHEMATICAL WRITING: FUNDAMENTALS

Set Theory  9
Functions (part one)  11
Existential Quantifiers  13
Universal Quantifiers  15
Combining Quantifiers  17
Functions (part two)  19
Negating Universal Quantifiers  21
Negating Existential Quantifiers  23
Negating Nested Quantifiers  25
Sets and Functions  27

PART II  MATHEMATICAL WRITING: PROOF TECHNIQUES

Uniqueness  31
Casework  33
Either/Or, Max/Min  35
Counterexamples  37
Contraposition  39
Contradiction  41
Proof by Induction  43
Direct Proof  45

PART III  MATHEMATICAL WRITING: BACK MATTER

The Joy of Sets  49
Mathematical Hygiene 53
More Joy of Sets 57
Some Suggestions for Further Reading 61
Index 63
Introduction

The worksheets in this document were created to help University of Michigan students transition into mathematics courses that are more writing intensive. The required math background is minimal. In terms of content students need to have seen high school algebra, high school geometry, and college level calculus (at the level of Math 115). Experience with these worksheets has shown that the most important quality a student needs in order to succeed is intellectual curiosity.¹

Throughout, an effort has been made to focus on the fundamentals of mathematical writing, rather than the mathematics itself. Thus, plenty of hints have been given. However, this doesn’t mean that these worksheets will be a walk in the park – most people find mathematical writing to be extremely challenging.

In the remainder of this introduction we discuss (a) two mathematical results students should know before starting these worksheets and (b) how these worksheets are intended to be used.

Two results students need to know

The first result students need to know is that the integer zero is even. The set of integers is \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}. By definition, an integer is even provided that it can be written as 2\(k\) for some integer \(k\). So, for example, 42 is even because \(42 = 2 \cdot 21\). Similarly, an integer is odd provided that it can be written as one more than an even integer; that is, of the form \(2\ell + 1\) for some integer \(\ell\). Thus, \(-17 = 2 \cdot (-9) + 1\) is odd. Since zero can be written as \(2 \cdot 0\), zero is even.

The second result students need to know is that the square root of 2, often written \(\sqrt{2}\), is not a rational number. A rational number is any number that can be written as a ratio \(a/b\) of two integers with \(b\) not zero.² You may have learned that a rational number is

¹ Thus, while it is good to be motivated to learn how to read and write mathematics for reasons like, for example, the well paying job that an actuarial, computer science, or statistics degree may bring you, we have found that in the absence of a desire to learn for the sake of learning, students with these other motivations tend to be unhappy while completing these worksheets.

² Never divide by zero.
a number whose decimal expansion terminates or repeats – this is equivalent to saying it can be written as a ratio $c/d$ of integers with $d \neq 0$. The fact that $\sqrt{2}$ is not rational needs to be demonstrated, and there are at least nineteen known distinct proofs. Here is a proof that is very nearly identical to the one Euclid wrote down over two thousand years ago (Proposition 117 of Book X):

Suppose for the sake of contradiction that $\sqrt{2}$ is rational. Then there exist integers $a$ and $b$ with $b \neq 0$ such that $\sqrt{2} = a/b$. After cancelling out factors of two, we may assume that **at most one of $a$ or $b$ is even**.

Since $\sqrt{2} = a/b$, we have $2b^2 = a^2$. This means $a^2$ is even. Since the square of an odd number is odd, it must be the case that $a$ is **even**.

Thus $a = 2k$ for some natural number $k$. Consequently $2b^2 = 4k^2$, so $b^2 = 2k^2$, and hence $b^2$ is even. Since the square of an odd number is odd, it must be the case that $b$ is **even**.

Since $a$ and $b$ are even, but at most one of $a$ or $b$ is even, we have arrived at a contradiction. Hence, our original assumption that $\sqrt{2}$ is rational must be false. Thus, $\sqrt{2}$ is not rational.

**How these worksheets are intended to be used.**

**Around 2009** we noticed that more and more students were arriving at the University of Michigan without having seen basic set theory and predicate logic. The handouts *Joy of Sets* and *Mathematical Hygiene*, both of which appear in the Back Matter of this document, were developed to help bridge this knowledge gap. Of course, if you were not exposed to these concepts in K-12, then you will not have practiced and internalized them. Thus, around 2015 we started developing worksheets to better help students get up to speed on these topics.

During 2019 students from Math 175, 185, 217, and 295 were invited to work on drafts of the worksheets. The students who showed up worked in groups of four to six under the guidance of an experienced student of mathematics. This scheme worked very well, and many improvements were made. For example, a great many hints were added, model proofs were added to most worksheets, and exercises that distracted more than aided were removed.

**The final form of these worksheets** assume that you will be working collaboratively with others under the guidance of an experienced student of mathematics. The pacing has been designed so that, on average, one worksheet can be completed per hour. While the first five worksheets should be done in order, after that there is some freedom to choose, with guidance from an experienced hand, an appropriate path through the worksheets.
Part I

Fundamentals
Set Theory

Set Theory lies at the heart of all things mathematical, so take some time to review the fundamentals. In this worksheet you will work with some of the basic concepts: intersections, unions, complements, and set-builder notation. You should know roughly what these terms mean. You should also be familiar with some basic sets that crop up often:

\( \mathbb{N} = \) the set of natural numbers = “counting numbers” = \{1, 2, 3, 4, \ldots \}.
\( \mathbb{Z} = \) the set of integers = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots \}.
\( \mathbb{Q} = \) the set of rational numbers (fractions) = \( \left\{ \frac{a}{b} \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{N} \right\} \).
\( \mathbb{R} = \) the set of real numbers. Often represented via the number line.

Exercises

1. First, we’ll practice set builder notation. Write out in plain English what the following sets are. For example, \( \{x \in \mathbb{R} \mid x^2 > 3\} \) is “the set of real numbers whose square is bigger than 3.”

   (a) \( \{(x, y) \mid x, y \in S\} \), where \( S \) is a set.
   (b) \( \{n \in \mathbb{Z} \mid n^2 > 5\} \).
   (c) \( \{(x, y) \in \mathbb{R}^2 \mid x^2 = y\} \).
   (d) \( \{n \in \mathbb{Z} \mid n = 2k + 1 \text{ for some } k \in \mathbb{Z}\} \)

2. Fix \( a, b \in \mathbb{R} \) with \( a < b \). Write the interval \([a, b)\) in set-builder notation.

3. Write \([0, 1] \setminus \mathbb{Q}\) with set-builder notation. Then write it as the intersection of \([0, 1]\) and another set.

\(^4\) See, for example, The Joy of Sets on page 49.

\(^5\) Also called comprehension notation.

\(^6\) The set \( \{(s, s') \mid s, s' \in S\} \) is the Cartesian Product of \( S \) with itself; it is often referred to as \( S \times S \), or \( S^2 \). This idea can be extended to \( S^3 \) where the elements look like \((s, s_2, s_3)\), and so on for \( S^n \). Common examples are \( \mathbb{R}^2 \), the plane, and \( \mathbb{R}^3 \), which is normal three-dimensional space.

Why \( a < b \)?
When is one set a subset of another? For two sets \( A \) and \( B \), we say \( A \) is a subset of \( B \), abbreviated \( A \subseteq B \), provided that every element of \( A \) is an element of \( B \). This is equivalent to saying \( a \in A \Rightarrow a \in B \) for every \( a \) in \( A \).

A proof that \( A \subseteq B \) often has the following structure: choose an element \( a \) of \( A \); show that \( a \) meets the requirements for belonging to \( B \); conclude that \( A \subseteq B \). So, for example, a proof that \( \mathbb{Z} \) is a subset of \( \mathbb{Q} \) might go like this: “Choose \( n \in \mathbb{Z} \). Note that \( n = n/1 \in \mathbb{Q} \). Thus \( \mathbb{Z} \subseteq \mathbb{Q} \).”

4. Show that

\[
A = \{ t(1,0,-1) \in \mathbb{R}^3 \mid t \in \mathbb{R} \}
\]

is a subset of

\[
B = \{ r(1,1,1) + s(3,2,1) \in \mathbb{R}^3 \mid r,s \in \mathbb{R} \}.
\]

5. Let \( C = \{ n \in \mathbb{Z} \mid n \text{ is a multiple of } 18 \} \), let \( E \) denote the set of even integers, and let \( D = \{ \ell \in \mathbb{Z} \mid \ell \text{ is a multiple of } 9 \} \). Show that \( C \subseteq D \cap E \).

When are two sets equal? Two sets \( X \) and \( Y \) are equal provided that every element of \( X \) is an element of \( Y \) and vice-versa. Thus, \( X = Y \) if and only if \( X \subseteq Y \) and \( Y \subseteq X \). When using this technique in a proof, label the sections that show \( X \subseteq Y \) and \( Y \subseteq X \) clearly!

6. Let \( F = \{ 5k - 7 \mid k \in \mathbb{Z} \} \) and let \( F = \{ 5\ell + 13 \mid \ell \in \mathbb{Z} \} \). Show that \( F = G \).

7. Let \( H = \{ a(1,2) + b(3,5) \mid a,b \in \mathbb{R} \} \). Show

\[
\mathbb{R}^2 = H.
\]

8. Suppose \( X \) is a set and \( I,J \subseteq X \). Show that \( J \setminus I = J \cap I^c \).

9. (Bonus) Let \( B = \{ (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1 \} \) and \( C = \{ (x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \} \). Determine what \( C \cup B \) is and prove it.
Functions (part one)

The concept of function is one of the more important mathematical ideas that you will encounter. Suppose $S$ and $T$ are sets. A function $f : S \rightarrow T$ (read as “$f$ is a function from $S$ to $T$”) is a rule that assigns a unique element $f(s) \in T$ to each element $s \in S$. Essentially, a function $f$ is a guide that tells you what object $f(s)$ is paired with a given $s \in S$.

A function $f : S \rightarrow T$ can assign only one $f(s) \in T$ to each $s \in S$, and it must assign an object $f(s) \in T$ to every $s \in S$. That first rule is the equivalent of the vertical line test that you may have learned about in high school.

For a function $g : S \rightarrow T$, we call $S$ the source, or domain, of the function, and $T$ the target, or codomain, of the function $g$.

Exercises

1. (Review.) Write $[0, \infty)$, the set of nonnegative real numbers, in set-builder notation. Show that $[0, \infty) = \mathbb{R} \setminus (-\infty, 0)$.

2. Observe that $2^2 = 4$ and $(-2)^2 = 4$. All positive real numbers have two real square roots. Knowing this, explain why the rule which assigns to each nonnegative $x$ a nonnegative square root of $x$ defines a function $r : [0, \infty) \rightarrow \mathbb{R}$.

3. Explain why the rule discussed in Figure 1 fails to define a function from $\mathbb{R}$ to $\mathbb{R}$.

We can build functions using piece-wise notation. For example, consider the function $f : \mathbb{R} \rightarrow \mathbb{R}$ given by

$$f(x) = \begin{cases} 
  x + 1 & \text{if } x \geq 0; \\
  0 & \text{if } x < 0.
\end{cases}$$

What this tells us is that $f(x) = x + 1$ if $x \geq 0$, and $f(x) = 0$ if $x < 0$.
4. Sketch a graph of \( f: \mathbb{R} \to \mathbb{R} \) given by
\[
f(x) = \begin{cases} 
  x + 1 & \text{if } x \geq 0; \\
  -x^2 - 2 & \text{if } x < 0.
\end{cases}
\]

5. Which of the following are functions? If it is not a function, explain why by telling which requirement for being a function it fails.
(a) \( f: \mathbb{R} \to \mathbb{R} \) given by \( f(x) = x^2 + 3x + 5 \).
(b) \( f: \mathbb{R} \to \mathbb{R} \) given by \( f(x) = \begin{cases} 
  x^2 + 1 & \text{if } x \geq 0; \\
  x - 1 & \text{if } x < 0.
\end{cases} \)
(c) \( f: \mathbb{R} \to \mathbb{R} \) given by \( f(x) = \begin{cases} 
  x^2 + x - 4 & \text{if } x \geq 1; \\
  x - 3 & \text{if } x < 1.
\end{cases} \)
(d) \( f: \mathbb{R} \to \mathbb{R} \) given by \( f(x) = \begin{cases} 
  0 & \text{if } x \in \mathbb{Q}; \\
  1 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q}.
\end{cases} \)
(e) \( f: \mathbb{N} \to \mathbb{Q} \) given by \( f(x) = \sqrt{x} \).

6. Let \( A \) be a set, and suppose you are given two functions \( f: A \to \mathbb{R} \), \( g: A \to \mathbb{R} \). Answer the following questions. You do not have to justify if something is a function.
(a) Does sending \( a \in A \) to \( (fg)(a) = f(a)g(a) \) define a function? What is the domain? What is the codomain?
(b) Does sending \( a \in A \) to \( (f + g)(a) = f(a) + g(a) \) define a function?
(c) Does sending \( a \in A \) to \( \left( \frac{f}{g} \right)(a) = f(a)/g(a) \) define a function?

Composing functions is another way to produce new functions from old ones. Suppose \( A, B, \) and \( C \) are sets and suppose you are given two functions \( f: B \to C \) and \( g: A \to B \). Then we can define the composition of two functions, \( f \circ g: A \to C \), by
\[
(f \circ g)(a) = f(g(a)).
\]
for \( a \in A \).

7. Rewrite the composition \( f \circ g: \mathbb{R} \to \mathbb{R} \) of \( f: \mathbb{R} \to \mathbb{R} \) and \( g: \mathbb{R} \to \mathbb{R} \) as a polynomial or a simple piece-wise function.
(a) \( g(x) = 2x + 3 \), \( f(x) = x^2 + 5x + 1 \).
(b) \( g(x) = \begin{cases} 
  -1 & \text{if } x \in \mathbb{Q}; \\
  1 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q}.
\end{cases} \), \( f(x) = x^2 \).
(c) \( g(x) = x^2 \), \( f(x) = \sqrt{|x|} \).
(d) \( g(x) = 3 \), \( f(x) = x + 5 \).

Notice how it’s like cutting and pasting two graphs together, where you change from one function to another at \( x = 0 \).

An element of \( \mathbb{R} \setminus \mathbb{Q} \) is called an irrational number.

What this does is send an element \( a \in A \) to an element \( g(a) \in B \), and then to an element \( f(g(a)) \in C \), so the function goes from \( A \) to \( B \) and then from \( B \) to \( C \).

For example, if \( g(x) = x + 1 \) and \( f(x) = x^2 \), then \( (f \circ g)(x) = x^2 + 2x + 1 \).

The absolute value function \( |\cdot|: \mathbb{R} \to \mathbb{R} \) is defined by
\[
|x| = \begin{cases} 
  x & \text{if } x \geq 0 \\
  -x & \text{if } x < 0
\end{cases}
\]
for \( x \in \mathbb{R} \).
Existential Quantifiers

The existential quantifier “there exists” is the first of our two major quantifiers. “There exists” (or alternatively, “there is”) is often abbreviated as $\exists$. This is a useful abbreviation for scratch work, but you should write out the actual words and avoid using the symbol $\exists$ in proofs in any formal writing. This quantifier is called existential because it declares the existence of a particular object.

A proof involving existential quantifiers generally involves finding or constructing a certain number/object that satisfies some conditions. For example, a proof that there exists a twice differentiable function $f : \mathbb{R} \to \mathbb{R}$ such that $f'' + 9f = 0$ might go something like this: “Let $g(t) = \sin(3t + 5)$. Since $g''(t) + 9g(t) = -9\sin(3t + 5) + 9\sin(3t + 5) = 0$, a function satisfying the differential equation $f'' + 9f = 0$ exists.”

Exercises

1. Write the following propositions in plain English.
   
   (a) $\exists n \in \mathbb{N}$ such that $n^2 = 9$.
   
   (b) $\exists m \in \mathbb{Z}$ such that $m < -\sqrt{2}$.
   
   (c) $\exists \ell, m \in \mathbb{N}$ such that $3\ell + 5m = 13$.
   
   (d) $\exists j \in \{3, 4, 7\}$ such that $j^3$ is divisible by 8.

2. Which of the following propositions are true? Justify.
   
   (a) $\exists \ell, m \in \mathbb{N}$ such that $3\ell + 5m = 13$.
   
   (b) $\exists x \in \mathbb{R}$ such that $x^2 = 0$.
   
   (c) $\exists k \in \mathbb{N}$ such that $k > 1$ and $k$ is not a prime.\(^9\)
   
   (d) $\exists \ell \in \mathbb{N}$ such that $\ell^2 - 5\ell + 6 = 0$.
   
   (e) $\exists q \in \mathbb{Q}$ such that $q^2 - 2 = 0$.

\(^8\) If $m$ and $n$ are integers, we say that $m$ divides $n$ provided that there is some integer $k$ such that $km = n$. When this happens, we say that $n$ is divisible by $m$ and $m$ is a factor of $n$.

\(^9\) A natural number $p$ is said to be prime provided that it has exactly two distinct positive integer factors.
3. Rephrase the statement “\(x^2 - 2x - 3\) has a real root” using the quantifier \(\exists\).

4. Prove there exists a non-trivial rational solution to \(x^2 + y^2 = 1\).
   (Here, non-trivial means different from the trivial solutions \((0, \pm 1)\) and \((\pm 1, 0)\)).

5. Suppose \(A\) is a set and \(\ell: A \to \mathbb{R}\) is a function. Use the quantifier \(\exists\) to define what it means for \(\ell\) to be a nonzero function.

6. Prove your answer to question 3.

7. Suppose \(c \in \mathbb{R}\) is not zero. Show that there is a nonzero differentiable function \(f: \mathbb{R} \to \mathbb{R}\) that satisfies \(f' - cf = 0\). Does your function also work when \(c = 0\)? Graph the function \(f\) you find for \(c = -\ln(2)\).

8. Diophantine equations are equations where only integer solutions are allowed. For example, the Diophantine equation \(x^2 + 2xy - 3y^2z - 17 = 0\) has solution \(x = 1, y = 2, z = -2\). On the other hand, the Diophantine equation \(x^2 + y^2 + 1 = 0\) has no solution for \(x, y\) integers.\(^{11}\)
   
   (a) Prove the Diophantine equation \(36x + 35y = 11\) has a solution.
   (b) Prove the Diophantine equation \(x^2 + y^2 + 1 = 0\) has no solution.
   (c) Prove that the Diophantine equation \(x^2 - 2y^2 = 1\) has a nontrivial solution other than \(x = \pm 3\) and \(y = \pm 2\).

9. Show there exists a positive integer which can be expressed as the sum of two cubes in two different ways.

   \(a \in \mathbb{R}\) is a root of a polynomial \(p\) provided that \(p(a) = 0\).

   Hint: What’s your favorite Pythagorean triple?

   \(\text{"The zero function from } A \text{ to } \mathbb{R} \text{ is the function that sends every element of } A \text{ to } 0. \text{ A nonzero function from } A \text{ to } \mathbb{R} \text{ is any function that is not the zero function."}\)

10. The tenth of David Hilbert’s influential list of twenty-three problems, which he published in 1900, asks if there is a general algorithm which can decide whether a given Diophantine equation has a solution or not. Thanks to the mid twentieth century work of Martin Davis, Yuri Matiyasevich, Hilary Putnam, and Julia Robinson we know the answer is no.

   (a) Prove the Diophantine equation \(36x + 35y = 11\) has a solution.
   (b) Prove the Diophantine equation \(x^2 + y^2 + 1 = 0\) has no solution.
   (c) Prove that the Diophantine equation \(x^2 - 2y^2 = 1\) has a nontrivial solution other than \(x = \pm 3\) and \(y = \pm 2\).

   Hint: 17/12 is approximately \(\sqrt{2}\).

I remember once going to see [Ramanujan] when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavourable omen. “No” he replied, “it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways.”

— G. H. Hardy
**Universal Quantifiers**

The universal quantifier “for all” is the second of our two major quantifiers. “For all” (or alternatively, “for every”) is often abbreviated as $\forall$. This quantifier is called **universal** because it talks about all objects, instead of a single one (contrast this with $\exists$).

A proof involving universal quantifiers generally involves proving that a property holds for all objects in a certain set. Because you cannot work with all elements of a set simultaneously, proving a statement $P(x)$ for all $x$ is done by picking an arbitrary $x$ and using the properties and theorems you know to deduce $P(x)$. Since your choice of $x$ was arbitrary at the beginning and could’ve been any $x$, you may deduce that $P(x)$ holds for all $x$. For example, a proof that every integer that is divisible by 14 is even might go something like this: “Fix an integer $n$ that is divisible by 14. Since $n$ is divisible by 14, there exists $k \in \mathbb{Z}$ for which $n = 14k$. Thus, $n = 2m$ where $m = 7k$; hence $n$ is even.”

**Exercises**

Remember to fix an element to work with in your proof and state at the very beginning that you are fixing such an element. For example, in Exercise 4 below, you need to first state something like “Fix a prime number $p$.” and work from there.

1. Write the following propositions in plain English.
   
   (a) $\forall$ even integers $n$, $n^2$ is divisible by 4.
   
   (b) $\forall n \in \mathbb{Z}$, $n^2 \geq 0$.
   
   (c) $\forall x \in \mathbb{R}$ with $|x| \geq 1$, we have that $x^2 \geq x$.
   
   (d) $\forall a, b, c \in \mathbb{Z}$ with $a^2 + b^2 = c^2$, we have that $a$ is even or $b$ is even.

2. Rephrase the statement “$p + 7$ is composite$^{12}$ for any prime $p$” provided that (a) it is not one and (b) it is not prime.

---

$^{12}$ A natural number is called **composite**.
using the quantifier $\forall$.

3. Which of the following propositions are true? If the proposition is false, explain why.

(a) $\forall a, b \in \mathbb{Z}, \frac{a}{b}$ is in $\mathbb{Q}$.
(b) $\forall n \in \mathbb{Z}, n^2 \geq 0$.
(c) Every prime number is a Sophie Germain prime.$^{13}$
(d) $\forall$ sets $S$, $S$ has a finite number of elements.
(e) $\forall x \in \mathbb{R}, x$ has a real square root.

4. Show that for all primes $p$, $p + 7$ is composite.

5. Prove that $\forall x, y \in \mathbb{R}$, we have that $x^2 + y^2 \geq 2xy$.

6. Rephrase the statement

“$A^2$ is upper triangular for any upper triangular $2 \times 2$ matrix $A$”

using the quantifier $\forall$.

7. Show that the square of every two-by-two upper triangular matrix is again an upper triangular matrix.

$^{13}$ A Sophie Germain prime is a prime $p$ such that $2p + 1$ is also prime. Germain used them in her work on Fermat’s Last Theorem (see page 41).

Hint: You may want to split the proof into two cases: odd and even primes.
Combining Quantifiers

Combining existential and universal quantifiers provides a way for us to form more complicated mathematical statements. For example, the Extreme Value Theorem\(^\text{14}\) states that if \(f: [a, b] \to \mathbb{R}\) is continuous, then

\[
\exists c, d \in [a, b] \text{ such that } \forall x \in [a, b], \ f(c) \leq f(x) \leq f(d),
\]

the Archimedean Property\(^\text{15}\) says

\[
\forall \varepsilon > 0 \ \exists n \in \mathbb{N} \text{ such that } 1/n < \varepsilon,
\]

and the fact that \(\mathbb{Q}\) is dense in \(\mathbb{R}\) may be written as

\[
\forall x, y \in \mathbb{R} \text{ with } x < y \ \exists q \in \mathbb{Q} \text{ such that } x < q < y.
\]

The order in which you list \(\forall, \exists\) is extremely important. Writing \(\forall x \exists y\) means that given any \(x\), you can find a \(y\) for it. Each \(x\) has its own \(y\). Writing \(\exists y \forall x\) means that there exists a \(y\) that works for every single \(x\). That is, the same \(y\) works for every \(x\).

**A proof of a \(\exists y \forall x\) statement** requires that you first produce a \(y\) and then show it works for all \(x\). For example, if \(X\) is a set, then a proof that there is a set \(A \subseteq X\) such that for every set \(B \subseteq X\) we have \(A \cup B = B\) might go like this: “Let \(A = \emptyset\). Fix \(B \subseteq X\). Note that \(A \cup B = \emptyset \cup B = B\).”

**A proof of a \(\forall x \exists y\) statement** requires that given any \(x\) you find a \(y\) that makes things work. For example, if \(X\) is a set, then a proof that for all \(A \subseteq X\) there is \(B \subseteq X\) such that \(X = A \cup B\) and \(\emptyset = A \cap B\) might go something like this: “Fix \(A \subseteq X\). Let \(B = X \setminus A\). Note that \(A \cup B = A \cup (X \setminus A) = X\) and \(A \cap B = A \cap (X \setminus A) = \emptyset\).”

**Exercises**

1. Write the following propositions in plain English.
(a) \( \forall x \in \mathbb{R}_{>0} \exists n \in \mathbb{N} \) such that \( \frac{1}{n} < x \).
(b) \( \forall p, q \in \mathbb{Q} \) with \( p < q \), \( \exists z \in \mathbb{R} \setminus \mathbb{Q} \) such that \( p < z < q \).
(c) \( \forall x \in \mathbb{R} \exists n \in \mathbb{N} \) such that \( |x| > n \).
(d) \( \exists n \in \mathbb{N} \forall m \in \mathbb{N}, n \leq m \).
(e) \( \forall m, n \in \mathbb{N} \exists \ell \in \mathbb{Z} \) such that \( m + \ell = n \).
(f) \( \forall x, y \in \mathbb{R} \) with \( x < y \) \( \exists q \in \mathbb{Q} \) such that \( x < q < y \).
(g) \( \forall p \in \mathbb{Q}_{>0} \exists q \in \mathbb{Q} \) such that \( 0 < q < p \).

2. Rephrase the statement “every positive real number has a square root” using quantifiers.

3. Suppose \( f : \mathbb{R} \to \mathbb{R} \). Use quantifiers to define what it means for \( f \) to be periodic (like \( \cos \) is periodic with period \( 2\pi \)).

4. Prove that \( \forall x \in \mathbb{R}, \exists y \in \mathbb{R} \) such that \( x^2 + 2x = y \).

5. Prove that there is \( n \in \mathbb{Z} \) such that for all \( m \in \mathbb{Z} \), \( n \) divides \( m \).

6. Provide a proof of Exercise 1g.

7. Prove that for any \( y \in \mathbb{R} \) and any \( \varepsilon \in \mathbb{R}_{>0} \), there exists a \( q \in \mathbb{Q} \) such that \( |q - y| < \varepsilon \).

8. (Bonus.) Show that for all matrices of the form \( \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \) with \( a, b \in \mathbb{R} \setminus \{0\} \), there exists a two-by-two matrix \( M \) such that \( \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \).

9. (Bonus.) Provide a proof of Exercise 1d.

10. (Bonus.) Prove that for every non-zero vector \( \vec{v} \in \mathbb{R}^2 \), there exists a vector \( \vec{w} \in \mathbb{R}^2 \) such that \( \vec{v} \) and \( \vec{w} \) are linearly independent.

Recall that the absolute value function \( |\cdot| : \mathbb{R} \to \mathbb{R} \) is defined by

\[ |x| = \begin{cases} \begin{array}{ll} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{array} \end{cases} \]

for \( x \in \mathbb{R} \).

\( \mathbb{Q}_{>0} := \{ r \in \mathbb{Q} | r > 0 \} \).

Hint: Don’t be afraid to name things.

Never divide by zero.

If \( k \) and \( \ell \) are integers, we say that \( k \) divides \( \ell \) provided that there is some integer \( j \in \mathbb{Z} \) such that \( \ell = jk \).

Hint: You may want to use that \( \mathbb{Q} \) is dense in \( \mathbb{R} \).

16 A rigorous proof will probably involve induction (see page 43).

Two vectors \( \vec{v} \) and \( \vec{w} \) in \( \mathbb{R}^2 \) are linearly independent provided that the only solution to \( a\vec{v} + b\vec{w} = \vec{0} \) is \( a = b = 0 \).
Injective, surjective, and bijective functions occur everywhere in mathematics.

A function is injective provided that different inputs map to different outputs. That is, for sets \( S \) and \( T \) a function \( f: S \to T \) is injective provided that for all \( a, b \in S \), if \( f(a) = f(b) \), then \( a = b \). Injective functions are also called one-to-one functions.

A proof that a function is injective often has the following structure: choose two elements \( s_1, s_2 \) of the source space that map to the same element in the target; then use the fact that they map to the same element in the target to show that \( s_1 = s_2 \). So, for example, a proof that the function \( f: \mathbb{N} \to \mathbb{N} \) defined by \( f(n) = 2n + 1 \) is injective might go like this: “Choose \( n_1, n_2 \in \mathbb{N} \) for which \( f(n_1) = f(n_2) \). Since \( f(n_1) = f(n_2) \), we have \( 2n_1 + 1 = 2n_2 + 1 \). Thus, \( 2n_1 = 2n_2 \) and so \( n_1 = n_2 \).”

Exercises

1. Formulate what it means for a function not to be injective. Have an experienced student of mathematics check your definition.

2. Prove that the function \( f: \mathbb{R} \to \mathbb{R} \) defined by \( f(x) = 2x \) is injective.

3. Fix \( a \in \mathbb{R}_{>0} \). Prove that the function \( w: \mathbb{R} \to \mathbb{R}^2 \) given by \( w(s) = (2as, 2a/(1 + s^2)) \) is injective. Due to mistranslation, the curve described by \( w \) is often called the Witch of Agnesi.\(^{17}\)

4. Prove that the function \( s: \mathbb{Z} \to \mathbb{Z} \) given by \( s(x) = x^2 \) is not injective.

5. (Bonus) Prove that the function \( j: \mathbb{Q}_{>0} \to \mathbb{N} \) given by \( j(q) = 2^m3^n \), where \( m, n \) are positive and \( q = m/n \) in lowest terms\(^{18}\), is injective.

\(^{17}\) In 1748 Maria Gaetana Agnesi studied this curve, which she called versiera, in *Instituzioni analitiche ad uso della gioventu italiana*, the first textbook to cover both differential and integral calculus. Below are graphs of versiera for \( a \) equal to 0.3, 0.5, and 0.7.

\(^{18}\) That is, the only positive common divisor of \( m \) and \( n \) is 1.
A function is surjective provided that every element in its target has something mapping to it from the source. That is, for sets $A$ and $B$ a function $g: A \to B$ is surjective provided that for every $b \in B$ there exists $a \in A$ such that $g(a) = b$. Surjective functions are also called onto functions.

A proof that a function is surjective often has the following structure: choose an element $t$ of the target space; produce $s$ in the source that maps to $t$; verify that $s$ is mapped to $t$. So, for example, a proof that the function $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 - x$ is surjective might go like this: “Choose $t \in \mathbb{R}$. Since $\lim_{x \to \infty} f(x) = \infty$, there is a $b \in \mathbb{R}$ for which $f(b) > t$. Since $\lim_{x \to -\infty} f(x) = -\infty$, there is an $a \in \mathbb{R}_{<b}$ for which $f(a) < t$. Since $f$ is continuous on $[a, b]$ and $f(a) < t < f(b)$, by the Intermediate Value Theorem there is a $c \in [a, b] \subset \mathbb{R}$ for which $f(c) = t$.”

Exercises

1. Formulate what it means for a function not to be surjective. Have an experienced student of mathematics check your definition.

2. Prove that the function $\ell: \mathbb{R} \to \mathbb{R}$ defined by $\ell(x) = |x|$ is not surjective.

3. Prove that the function $g: \mathbb{Q} \to \mathbb{N}$ given by $g(q) = n$, where $n$ is positive and $q = m/n$ in lowest terms, is surjective.

4. (Bonus.) Prove that any nonzero linear transformation $f: \mathbb{R}^2 \to \mathbb{R}$ is surjective. Is it necessary to assume $f$ is nonzero?

5. (Bonus.) Use the Intermediate Value Theorem to show that if $f: \mathbb{R} \to \mathbb{R}$ is continuous and $\lim_{x \to \infty} f(\infty) = \infty$ while $\lim_{x \to -\infty} f(*) = -\infty$, then $f$ is surjective.

A function is bijective provided that every element in the target has exactly one element mapping to it. That is, a function is bijective provided that it is both injective and surjective. Bijective functions are important because they are invertible.

Exercises

1. Prove that for any $k \in \mathbb{Z}$, the function $f: \mathbb{R}^2 \to \mathbb{R}^2$ given by $f(x, y) = (x + 2ky, 3x + y)$ is bijective.

2. Prove that the function $g: \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$ is bijective.

By convention we represent 0 in lowest terms by 0/1.

A function $g: \mathbb{R}^2 \to \mathbb{R}$ is said to be linear provided that

$g(\vec{x} + \vec{y}) = g(\vec{x}) + g(\vec{y})$ for all $\vec{x}, \vec{y} \in \mathbb{R}^2$ and

$g(c\vec{x}) = cg(\vec{x})$ for all $c \in \mathbb{R}$ and $\vec{x} \in \mathbb{R}^2$.

Suppose $A$ and $B$ are sets. A function $h: A \to B$ is said to be invertible provided that there exists $g: B \to A$ such that $h \circ g(b) = b$ for all $b \in B$ and $g \circ h(a) = a$ for all $a \in A$. When $h: A \to B$ is invertible, the function $g: B \to A$ is called an inverse or inverse function of $h$.

Hint: If $(a, b) = (x + 2ky, 3x + y)$, then $x = \frac{b - 3y - 2k}{2y}$ and $y = \frac{b - 3x}{b - 2k}$. Also $1/6 \not\in \mathbb{Z}$.

Hint: You may assume $a^2 + ab + b^2 = 0$ if and only if $a = b = 0$; this will be proved in Exercise 5 of the Casework worksheet (see page 33). Also, thanks to the Intermediate Value Theorem (see Exercise 5 above), if $f: \mathbb{R} \to \mathbb{R}$ is continuous and $\lim_{x \to \infty} f(\infty) = \infty$ while $\lim_{x \to -\infty} f(*) = -\infty$, then for all $t \in \mathbb{R}$ there exists $s \in \mathbb{R}$ such that $f(s) = t$. 

Q: What do you call a knight who goes around the castle stabbing everyone?

A: Sir Jective.
Negating Universal Quantifiers

Negating quantifiers is challenging, but necessary if we want to prove that statements involving quantifiers are false. Given a set \( X \), if you want to show a property \( P \) does not hold for all \( x \in X \), you must show that \( P \) fails to hold for some \( x \) in \( X \). So, the negation of “\( \forall x, P(x) \) is true” is “\( \exists x \) such that \( P(x) \) is false.” Because negating statements can be tricky, you may want to spend some time reviewing elementary predicate logic.\(^{23}\)

A proof that involves negating a universal quantifier usually arises because we want to show that a statement is false. For example, to prove that the statement

Every natural number is prime.

is false, we could proceed as follows: “To show that the statement

‘Every natural number is prime.’ is false, it is enough to show that the statement’s negation, ‘There exists a natural number which is not prime.’, is true. Consider the natural number 42. Since 1, 2, 3, 6, 7, 14, 21, and 42 are positive divisors of 42, the number 42 has more than two distinct positive divisors and is therefore not prime.”

Exercises

1. Negate the following statements.
   (a) It rains every day.
   (b) All primes are odd.
   (c) \( \forall x \in \mathbb{R}, x^2 = 1 \).
   (d) \( \forall x \in \mathbb{R}, x^2 < 0 \).

2. Which of the following statements are true? If a statement is false, negate it and prove the negated version.
   (a) Every nonnegative real number has two distinct real square roots.
(b) \( \forall n \in \mathbb{N}, 2^n \leq n! \).

(c) \( \forall x \in \mathbb{R}, x^2 - 2x + 1 \geq 0 \).

(d) \( \forall x \in [0,1), \) it is true that \( x^2 < x \).

(e) Every odd number greater than 4 is the sum of two primes.

3. Consider the statement

For all irrational numbers \( x, y \), it is true that \( xy \) is irrational.

Is this statement true? If so, prove it. If not, negate it and prove the negated version.

4. Consider the statement

For all odd integers \( m, n \), it is true that \( mn \) is odd.

Is this statement true? If so, prove it. If not, negate it and prove the negated version.

5. (Bonus.) Consider the statement

For all \( m, n \in \mathbb{N} \), the vectors \( \begin{bmatrix} 2 \\ 3 \end{bmatrix} \) and \( \begin{bmatrix} 5m + 7 \\ n + 2 \end{bmatrix} \) are linearly independent.

Is this statement true? If so, prove it. If not, negate it and prove the negated version.

6. (Bonus.) Formulate and prove the negation of this statement

For all \( k \in \mathbb{Z} \), the matrix

\[
\begin{bmatrix}
1 & 2k \\
0 & k
\end{bmatrix}
\]

is invertible.
Negating Existential Quantifiers

Quantifier negation is challenging, but needed when showing that statements involving quantifiers are false. Given a set $X$, if you want to show there is no $x \in X$ having property $P$, then you need to show that the negation of $P$, written $\neg P$, holds for every $x \in X$. That is, the negation of “$\exists x$ such that $P(x)$ is true” is “$\forall x$, $\neg P(x)$” is true.

A proof that involves negating an existential quantifier usually arises because we want to show that a statement is false. For example, to prove that the statement

There exists even $n \in \mathbb{Z}$ such that $n^2$ is odd.

is false, we could proceed as follows: “To show that the statement ‘There exists even $n \in \mathbb{Z}$ such that $n^2$ is odd.’ is false, it is enough to show that the statement’s negation, ‘For every even integer $n$ we have that $n^2$ is even.’ is true. Fix an even integer $n$. Since $n$ is even, there is a $k \in \mathbb{Z}$ such that $n = 2k$. Note that

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2),$$

hence $n^2$ is even.”

Exercises

You may want to review the worksheet Universal Quantifiers on page 15 for tips on proving “for all” statements. In particular, remember that if you want to show something is true for all $x$ in a set $X$, then you need to fix an arbitrary $x$ in $X$ with which to work.

1. Negate the following statements.

   (a) It rained some day.

   (b) $\exists x \in \mathbb{R} \setminus \mathbb{Q}$ such that $x^2 \in \mathbb{Q}$.

   (c) $\exists x \in \mathbb{Q}$ such that $x^2 + 4x + 2 = 0$. More generally, the product of an even integer with any integer is even. Can you show this? Under what conditions on integers $a$ and $b$ is the product $ab$ odd?
(d) \( \exists a, b, c \in \mathbb{N} \) such that \( a^3 + b^3 = c^3 \).

(e) Some days are better than today.

(f) Some triangles are scalene.

2. Which of the following statements are true? If a statement is false, negate it and prove the negated version.

(a) There exists an integer greater than one with an odd number of positive factors.

(b) \( \exists \text{odd } n \in \mathbb{Z} \) such that \( n^2 \) is even.

(c) \( \exists a, b, c \in \mathbb{N} \) such that \( a^2 + b^2 = c^2 \).

(d) \( \exists q \in \mathbb{Q} \) such that \( q^2 - 2 = 0 \).

(e) \( \exists n \in \mathbb{N} \) such that \( n \) is even and \( n \) can be written as a sum of two primes in two different ways.

(f) \( \exists \text{odd } n, m \in \mathbb{Z} \) such that \( n + m \) is odd.

3. Prove that there does not exist a positive real number \( x \) such that \( x + \frac{1}{x} < 2 \).

4. Consider the statement

There exist irrational \( a, \beta \in \mathbb{R} \) such that \( a^\beta \) is rational.

Is this statement true? If so, prove it. If not, negate it and prove the negated version.

5. Prove that there does not exist \( x \in \mathbb{R} \) such that \( x^2 - 3x + 3 \leq 0 \).

6. Consider the statement

There exists \( f \in C^0(\mathbb{R}) \) that is not the derivative of any function \( g: \mathbb{R} \to \mathbb{R} \).

Is this statement true? If so, prove it. If not, negate it and prove the negated version.

7. (Bonus.) Prove that there do not exist invertible \( n \times n \) matrices \( A \) and \( B \) such that \( AB \) is not invertible.
Negating Nested Quantifiers

Negating complex statements that are composed of nested quantifiers is extremely challenging. Be especially careful with your writing for this worksheet!

Exercises

1. Using your prior experience with negating quantifiers and thinking through what the negation should be, figure out how to negate the following statements. Ask an experienced student of mathematics to check your work after you’re done. Here, $P(x, y)$ denotes that $P$ is a property of the objects $x, y$.

   (a) “$\forall x \exists y$ such that $P(x, y)$ is true.”
   (b) “$\exists y \forall x P(x, y)$ is true.”

2. Which of the following statements are true? If a statement is false, negate it and prove the negated version.

   (a) For all $x \in \mathbb{R}$ there exists $n \in \mathbb{N}$ such that $n < x$.
   (b) There exists $m \in \mathbb{Z}$ such that $rm \in \mathbb{Q}$ for all $r \in \mathbb{R}$.
   (c) For all $x \in \mathbb{R}$ there exists $y \in \mathbb{R}$ such that $x + y = 42$.
   (d) There exists $u \in \mathbb{R}$ such that for all $v \in \mathbb{R}$ we have $u + v = 42$.
   (e) There exists $f \in C^0(\mathbb{R})$ such that for all differentiable $g: \mathbb{R} \to \mathbb{R}$ we have $g' - f \neq 0$.
   (f) For every continuous, strictly increasing function $g: \mathbb{R} \to \mathbb{R}$ there exists $c \in \mathbb{R}$ such that $g(c) = 0$.

   Hint: You may want to use the Fundamental Theorem of Calculus.

3. A set $S \subseteq \mathbb{R}$ is said to be bounded above provided that there exists $M \in \mathbb{R}$ such that for all $x \in S$ we have $x \leq M$. Use the Archimedean Property to show that $\mathbb{N}$ is not bounded above in $\mathbb{R}$.
4. Consider the following statement: “there exists \( n \in \mathbb{N} \) such that every prime divides \( n \).” Negate this statement and then prove the negated statement.

5. Consider the following statement: “for all even \( n \in \mathbb{N} \) there exists \( m \in \mathbb{N} \) such that \( nm \) is odd.” Negate this statement and then prove the negated statement.

6. A sequence\(^{24}\) \((a_n)\) is said to converge to \( L \in \mathbb{R} \) provided that for all \( \varepsilon > 0 \) there exists \( N \in \mathbb{N} \) such that \( m > N \) implies \(|a_m - L| < \varepsilon\).

(a) Explain what this definition means intuitively. You may write a geometric interpretation for this, if you find it helpful.

(b) Use the definition given above of what it means for a sequence to converge to prove that the sequence \((a_n) = (\frac{1}{n}) = (1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots)\) converges to 0.

(c) Use the definition given above of what it means for a sequence to converge to prove that the sequence \((a_n) = ((-1)^n) = (-1, 1, -1, 1, \ldots)\) does not converge to \( \frac{1}{2} \).

7. (Bonus.) Show that the vectors \((1, 0, 1)\) and \((1, 2, -1)\) do not span\(^{25}\) \(\mathbb{R}^3\).
Sets and Functions

Building new objects from existing ones is a common theme in mathematics. As an example, consider power sets. The power set, \( \mathcal{P}(X) \), of a set \( X \) is defined to be

\[
\mathcal{P}(X) := \{ A \mid A \subseteq X \}.
\]

That is, \( \mathcal{P}(X) \) is the set of all subsets of \( X \). The power set of a set can be quite large – how many subsets are there of \( \mathbb{N} \)? of \( \mathbb{R} \)? of \( \mathcal{P}(\mathbb{R}) \)?

In fact, the power set always has greater cardinality than the original set. For example, if \( X \) is a finite set with \( n \) elements, then \( \mathcal{P}(X) \) has \( 2^n \) elements.\(^{26}\)

Functions on power sets occur in all branches of mathematics. Suppose \( X \) and \( Y \) are sets. If \( f: X \rightarrow Y \) is a function, then we can define a new function, called the induced set function, \( f: \mathcal{P}(X) \rightarrow \mathcal{P}(Y) \) by:

\[
f[A] = \{ f(x) \mid x \in A \}
\]

for \( A \subset X \). For \( B \in \mathcal{P}(X) \), the subset \( f[B] \) of \( Y \) is called the image of \( B \). Similarly, we can define \( f^{-1}: \mathcal{P}(Y) \rightarrow \mathcal{P}(X) \) by

\[
f^{-1}[C] = \{ x \in X \mid f(x) \in C \}
\]

for \( C \subset Y \). For \( D \in \mathcal{P}(Y) \), the subset \( f^{-1}[D] \) of \( X \) is called the inverse image of \( D \). You should verify that both \( f^{-1}: \mathcal{P}(Y) \rightarrow \mathcal{P}(X) \) and \( f: \mathcal{P}(X) \rightarrow \mathcal{P}(Y) \) are functions.\(^{27}\)

Exercises

1. Find the power set of \( \{ \emptyset, \infty, \odot \} \).

2. Consider the map \( g: \mathbb{R} \rightarrow \mathbb{R} \) defined by \( g(x) = |x| \). Find the image of \( A = (-\infty, -1] \cup (1, \infty) \) under \( g \), and prove that your answer is correct.
3. Consider the map \( h: \mathbb{R} \to \mathbb{R} \) defined by \( h(x) = x^2 + 3 \). Find \( h[\mathbb{R}] \) and prove your claim.

4. Consider the map \( \ell: \mathbb{R} \to \mathbb{R} \) defined by \( \ell(x) = 2x + 1 \). Find the inverse image of \([-3, 5]\) under this map, and prove that your answer is correct.

5. Is the function \( p: \mathbb{R} \to \mathbb{R}^2 \) given by \( p(\theta) = (\theta \cos(\theta), \theta \sin(\theta)) \) injective? Justify your answer. What is \( p[\mathbb{R}] \)? What is \( p^{-1}[\mathbb{R}^2] \)?

6. Suppose \( X \) and \( Y \) are sets. Let \( f: X \to Y \) be a function. Suppose \( A \subseteq X \) and \( B \subseteq Y \).
   
   (a) Show: \( f[f^{-1}[B]] \subseteq B \).

   (b) Is \( f[f^{-1}[B]] \) always equal to \( B \)? If yes, prove it. If not, provide an example of a function where they are not equal.

   (c) Show: \( A \subseteq f^{-1}[f[A]] \).

   (d) Is \( f^{-1}[f[A]] \) always equal to \( A \)? If yes, prove it. If not, provide an example of a function where they are not equal.

7. Suppose \( X \) and \( Y \) are sets. Let \( f: X \to Y \) be a function. Is the function \( f^{-1}: \mathcal{P}(Y) \to \mathcal{P}(X) \) an inverse\(^{28}\) of \( f: \mathcal{P}(X) \to \mathcal{P}(Y) \)?

8. (Bonus) Suppose \( X \) and \( Y \) are sets. Let \( f: X \to Y \) be a function. Suppose \( A, C \subseteq X \) and \( B, D \subseteq Y \).

   (a) Is \( f^{-1}[B \cap D] = f^{-1}[B] \cap f^{-1}[D] \)? If not, provide an example where it fails. Does one set always contain the other?

   (b) Is \( f[A \cap C] = f[A] \cap f[C] \)? If not, provide an example where it fails. Does one set always contain the other?

9. (Bonus) Suppose \( X \) and \( Y \) are sets. Let \( f: X \to Y \) be a function. Suppose \( A, C \subseteq X \) and \( B, D \subseteq Y \).

   (a) Is \( f[A \cup C] = f[A] \cup f[C] \)? If not, provide an example where it fails.

   (b) Is \( f^{-1}[B \cup D] = f^{-1}[B] \cup f^{-1}[D] \)? If not, provide an example where it fails.

   (c) Is \( f[A \setminus C] = f[A] \setminus f[C] \)? If not, provide an example where it fails.

---

\(^{28}\) See sidenote 22.
Part II

Proof Techniques
Uniqueness

Showing that there is at most one object possessing a given property $P$ is a common mathematical task; such proofs are called uniqueness proofs.

A proof of uniqueness will generally involve assuming there are two objects $x,y$ that satisfy $P$, and then showing that $x$ and $y$ must in fact be the same object; that is, having the property $P$ forces $x,y$ to be the same. So, for example, a proof that there is at most one differentiable function $f : \mathbb{R} \to \mathbb{R}$ for which $f'(x) = 4x + 1$ and $f(2) = 42$ might go something like this: “Suppose $g,h : \mathbb{R} \to \mathbb{R}$ are differentiable functions for which $g'(x) = h'(x) = 4x + 1$ and $g(2) = h(2) = 42$. From the Mean Value Theorem, there is a constant $C$ so that $g(t) = h(t) + C$ for all $t \in \mathbb{R}$. Plugging in 2 for $t$ we have

$$C = g(2) - h(2) = 42 - 42 = 0.$$  

Consequently, $g = h$ and so if a solution exists, then it is unique.”

Existence and uniqueness proofs are common throughout mathematics. For these proofs, you must show both that a solution exists and that the solution is unique. So, for example, a proof that there exists a unique $f : \mathbb{R} \to \mathbb{R}$ for which $f'(x) = 4x + 1$ and $f(2) = 42$ might go something like this: “Define $f(x) = 2x^2 + x + 32$. Since $f'(x) = 4x + 1$ and $f(2) = 2 \cdot 2^2 + 2 + 32 = 42$, a solution exists. To show that $2x^2 + x + 32$ is the unique solution, please see the paragraph above.”

Exercises

For uniqueness proofs, make sure to state that you are supposing two $x,y$ exist satisfying whatever properties the objects $x$ and $y$ are supposed to satisfy.

1. Every element of $\mathbb{R}$ has a unique additive inverse. You have proba-
bly never seen a proof of the uniqueness of additive inverses, so let us remedy this now. Complete the following proof that an additive inverse of \( q \in \mathbb{R} \) is unique.

Suppose \( p, p' \in \mathbb{R} \) are additive inverses of \( q \). Note that

\[
p = 0 + p = (p' + q) + p = \cdots = p'.
\]

Hence if an additive inverse of \( q \in \mathbb{R} \) exists, then it is unique.

2. Similarly, every nonzero \( r \in \mathbb{R} \) has a unique multiplicative inverse.\(^{30}\) Since you’ve probably never shown that a multiplicative inverse of a nonzero \( r \in \mathbb{R} \) is unique, do so now.

3. Suppose \( A \) and \( B \) are sets and \( h: A \to B \) is invertible (see side-note 22). Show that \( h \) has a unique inverse function.

Inverses often have specialized notation. For example, in situations where it is known that additive inverses exist and are unique, the additive inverse of an object \( \circ \) is denoted by \( -\circ \). So, for example, additive inverses of matrices exist and are unique, and the additive inverse of a matrix \( A \) is denoted \( -A \). Similarly, when it is known that the multiplicative inverse of an object \( \diamond \) exists and is unique, it is often denoted \( \diamond^{-1} \).

4. Which of the following are unique?

(a) A square root of a positive real number.

(b) A complex square root of a real number.

(c) A positive square root of a positive real number.

5. For the objects you claimed to be unique in Exercise 4, prove that they are unique.

6. Show there is a unique differentiable function \( \text{ellen}: \mathbb{R}_{>0} \to \mathbb{R} \) for which \( \text{ellen}'(s) = 1/s \) for all \( s \in \mathbb{R}_{>0} \) and \( \text{ellen}(1) = 0 \).

7. Show that there is a unique real number solution to the equation \( x^3 = 1 \).

8. Let \( ax^2 + bx + c \) be a degree two polynomial such that \( b^2 - 4ac = 0 \). Show, without using the quadratic formula, that \( ax^2 + bx + c = 0 \) has a unique solution.

9. (Bonus.) Is there a unique invertible \( n \times n \) matrix \( A \) such that \( A^2 = A \)?

\[\text{Hint: if you find yourself writing } -q, \text{ then you are probably assuming what you are trying to prove!}\]

\[\text{Hint: if you find yourself writing } 1/r \text{ or } r^{-1}, \text{ then you are probably assuming what you are trying to prove!}\]

\[\text{Hint: if you find yourself writing } 1/\sqrt{x}, \text{ then you are probably assuming what you are trying to prove!}\]

\[\text{We say } \star \text{ is a square root of } \sqrt{x} \text{ provided that } \star^2 = x.\]

\[\text{If a nonnegative square root of } \sqrt{x} \in \mathbb{R} \text{ exists and is unique, it is denoted } \sqrt{x}.\]

\[\text{Hint: You may assume that for } a, b \in \mathbb{R} \text{ we have } a^2 + ab + b^2 = 0 \text{ if and only if } a = b = 0.\]

\[\text{Hint: Complete the square: } ax^2 + bx + c = a[(x + \alpha)^2 + (c/a - \alpha^2)]; \text{ what’s } \alpha?\]

\[\text{Hint: Don’t think too much. Maybe try something like } A = A \text{ Id}_n = \cdots = \text{ Id}_n, \text{ where the stuff in the middle follows from the given information. Also, since } A \text{ is invertible, there exists a (unique) } n \times n \text{ matrix } B \text{ so that } AB = BA = \text{ Id}_n,\]
**Casework**

Using casework in a proof is a pretty intuitive idea – sometimes you want to prove a property $P$ is true for a set of objects $S$, but the proof varies for different types of elements in $S$.

A common example of using casework involves proving something for a few objects by checking them individually. For example, if you wanted to prove that 1, 2 and 3 are roots of $x^3 - 6x^2 + 11x - 6$, you could just check these numbers individually. Another way to use casework is to split up an infinite set by some relevant property. For example, if you wanted to prove that for an integer $n$ the number $n(n + 1)/2$ is always an integer, it makes sense to split into the cases when $n$ is even and when $n$ is odd. Casework can also be used to deal with fringe cases; for example, when proving something about primes, you may have to split into the $p = 2$ and $p \neq 2$ cases or deal with small primes like 2, 3, 5 individually (see Exercise 2 on page 15).

A proof involving casework usually has the following structure: begin by specifying what the cases will be; explain why these are the only cases; prove the result in each case. For example, a proof that for every integer $n$, $n(n + 1)/2$ is an integer might go something like this: “Suppose $n$ is an integer. Since every integer is either even or odd, we have two cases:

- $n$ is even: In this case we can write $n = 2k$ with $k \in \mathbb{Z}$. We have $n(n + 1)/2 = (2k)(2k + 1)/2 = k(2k + 1)$.

- $n$ is odd: In this case we can write $n = 2k + 1$ with $k \in \mathbb{Z}$. We have $n(n + 1)/2 = (2k + 1)(2k + 2)/2 = (2k + 1)(k + 1)$.

Since the result holds in each case, the claim is proved.”

**Exercises**

Remember to label the separate cases of your proof to avoid confusion.
1. Prove that 7 divides $x^2 + x + 12$ for $x = 1, 5, 8$.

2. Prove that 5, 13, and 25 can all be written as the sum of two squares.

3. Prove that any non-horizontal line in $\mathbb{R}^2$ intersects the $x$-axis.

4. Show that every perfect cube is a multiple of 9 or has the from $9m \pm 1$ for some $m \in \mathbb{Z}$.

5. Suppose $a, b \in \mathbb{R}$. Show that $a^2 + ab + b^2 = 0$ if and only if $a = b = 0$.

6. The notation $\binom{n}{k}$, or $n$ choose $k$, denotes the number of ways to pick $k$ elements from a set of $n$ elements (ignoring order). Prove that

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

using casework style logic. Do not prove it algebraically.

7. (Bonus.) Determine which $2 \times 2$ matrices $A$ with two entries of 0 and two entries of 1 satisfy $A^2 = A$.

8. (Bonus.) Find the number of three digit positive integers (that is, integers between 0 = 000 and 999) whose second digit is the average of its first and third digits. (For instance, 630 is one such number, since 3 is the average of 6 and 0.)
Either/Or, Max/Min

A proof involving either/or looks very much like a casework proof. Either/or methods will generally involve splitting your proof into two cases by breaking it up by inequality conditions. For example, if you assume \( x \neq 0 \), you might state next that "either \( x > 0 \) or \( x < 0 \)" and deal with each situation separately. A proof of the proposition

If \( x^2 - 5x + 6 \geq 0 \), then either \( x \leq 2 \) or \( x \geq 3 \)

might go something like this: “Factoring the polynomial, we have that \( (x - 2)(x - 3) \geq 0 \). So, because of the sign, either \( x - 2 \leq 0 \) and \( x - 3 \leq 0 \), or \( x - 2 \geq 0 \) and \( x - 3 \geq 0 \). In the former case we have \( x \leq 2 \) and \( x \leq 3 \), so \( x \leq 2 \). In the latter case, we have \( x \geq 2 \) and \( x \geq 3 \), so \( x \geq 3 \). Thus, we must have \( x \leq 2 \) or \( x \geq 3 \).”

Exercises

1. If \( p \) is a prime number and \( b \) is an integer such that \( p \) does not divide \( b \), then the only positive integer that divides both \( p \) and \( b \) is 1.

2. Let \( A \) be a \( 2 \times 2 \) matrix such that \( A^2 = \text{Id}_2 \). Then the top left entry or the bottom left entry of \( A \) is nonzero.

3. Suppose \( a, b \in \mathbb{R} \). If \( ab = 0 \) then \( a = 0 \) or \( b = 0 \).

For Max/Min proofs, it’s important to know how to interpret statements about the maximum of a set or the minimum of a set. Relations between a number \( x \in \mathbb{R} \) and the max or min of a set \( S \subseteq \mathbb{R} \) tells you about the relative positioning of \( x \) to the set \( S \) on the number line.

Bounding a minimum above is easier, while bounding it below is harder. The reverse is true for maximums (bounding below is easy, bounding above is hard). For example, if you want to show

\[33\text{ Recall that if } m \text{ and } n \text{ are integers, we say that } m \text{ divides } n \text{ provided that there is some integer } k \text{ such that } km = n. \text{ A natural number } p \text{ is prime if and only if } p \text{ has exactly two distinct positive divisors.}

\[3\text{ If } A \subseteq \mathbb{R}, \text{ then } M \text{ is a maximum for } A \text{ provided that both } M \in A \text{ and } M \geq a \text{ for all } a \in A. \text{ Similarly, } m \text{ is a minimum for } A \text{ provided that both } m \in A \text{ and } m \leq a \text{ for all } a \in A.

\]
min $S \leq x$, you just need that there exists some element in $S$ that is less than or equal to $x$. But if you want $\min S \geq x$, then you need that every element of $S$ is greater than or equal to $x$. (Take a moment to think on the difference).

A proof involving max/min requires careful attention to the use of the quantifiers “for all” and “there exists”. For example, a proof that $\min \{x(x-2) \mid x \in \mathbb{R}\} \geq -1$ might go something like this: “To show $\min \{x(x-2) \mid x \in \mathbb{R}\} \geq -1$, we need to show that for all $x \in \mathbb{R}$ we have $x(x-2) \geq -1$. Fix $x \in \mathbb{R}$. Note that $x(x-2) \geq -1$ if and only if $x^2 - 2x + 1 \geq 0$, and this is true if and only if $(x-1)^2 \geq 0$. Since the square of a real number is always nonnegative, we conclude $(x-1)^2 \geq 0$ and so $\min \{x(x-2) \mid x \in \mathbb{R}\} \geq -1$.”

**Exercises**

1. Suppose $B \subset \mathbb{R}$. Show that $B$ has at most one maximum and at most one minimum. That is, show that if they exist, then maximums and minimums are unique.

2. Does every subset of $\mathbb{R}$ have a maximum? a minimum?

3. Find, if possible, the max and min for each of the following sets.
   
   (a) $\{x \in [e, \pi] \mid x \geq \sqrt{2}\}$
   
   (b) $(3, 5)$
   
   (c) $\{q \in \mathbb{Q} \mid q^2 \leq 2\}$
   
   (d) $\emptyset$

4. Let $S, T$ be subsets of $\mathbb{R}$, and suppose that $\max S, \min S, \min T$ all exist. Rewrite the statements below using quantifiers35.
   
   (a) $\max S \leq x$.
   
   (b) $\max S \geq x$.
   
   (c) $\min S \leq \min T$.
   
   (d) $\min S \geq \min T$.

5. Prove that $\max \{-x(x-1) \mid x \in \mathbb{R}\} \geq 1/4$.

6. Let $S = \{(x-2)(x-3) \mid x \in \mathbb{R}\}$ and $T = \{(x-1)(x-5) \mid x \in \mathbb{R}\}$. Show that $\min T \leq \min S$.

---

34 Remember that a proof that shows that something is true “for all $s \in S$” will almost always use the words “Fix $s \in S$.”

35 Remember, these are phrases like for every, there exists, for all.
Counterexamples

Counterexamples help us understand the boundaries of truth.\(^{36}\) They are also useful for disproving universal statements – to disprove a “for all” statement, you need only find a single instance of the statement failing. Sometimes, finding counterexamples requires little effort.\(^{37}\) However, the further one travels into mathematics, the more challenging finding counterexamples becomes. As with art, pretty much the only way to get better is by practicing.

When determining whether or not a counterexample may be warranted, pay attention to wording. In particular, it’s usually difficult to derive a strong conclusion from little information. You may want to ask yourself: how are the given information and the conclusion related? is there any reason the hypotheses should imply the conclusion? how can we relate the hypothesis with the conclusion given the tools at hand? For example, consider the statement “if \(a, b\) are irrational numbers, then \(ab\) is also irrational.” How would you be able to translate the information about the irrationality of \(a, b\), into facts about \(ab\)? If the word irrational were replaced with rational, then we’d know what to do. However, as stated, there’s no clear way to get from information about \(a, b\) to information about \(ab\). Indeed, it turns out that this statement is false (counterexample: \(a = b = \sqrt{2}\)).

Exercises

1. True or False? In this exercise, you do not have to provide justification. However, don’t answer without mentally checking the thought process behind your answer (that is, be confident in your answer).

   (a) All birds can fly.

   (b) All prime numbers are odd.

   (c) Subtraction in \(\mathbb{Z}\) is commutative.

\(^{36}\) “Every good theorem must have a good counterexample.” (Francesco Severi as quoted in American Mathematical Monthly, June, 1976)

\(^{37}\) Consider, for example, the statements: “All birds can fly.” “All prime numbers are odd.” and “Subtraction is commutative.”
(d) $x + y \geq x$ for all $x, y \in \mathbb{R}$.

(e) The only real number $r$ satisfying $r^2 = r$ is one.

(f) $(a + b + c)^2 \leq 3(a^2 + b^2 + c^2)$ for all $a, b, c \in \mathbb{R}$.

(g) $\sqrt{x} \leq x$ for all $x \in \mathbb{R}_{\geq 0}$.

(h) If $p$ is prime, then $2^p - 1$ is also prime.

(i) Suppose $n$ is the product of 3 consecutive numbers and 7 divides $n$. Then 6, 28, and 42 all divide $n$.

To find a counterexample, try to think of how the statement could fail. For example, in Exercise 1g the basic idea is that squaring big numbers results in very big numbers, so perhaps small numbers are a natural place to look for a counterexample.

It is also often a good idea to think about simple things. For example, in a problem like Exercise 1e you might want to check what happens to zero.

2. Prove all of your answers to Exercise 1, making sure to give an example/counterexample where applicable.

3. (Bonus.) True or False. Justify your answer.

(a) The set of invertible $2 \times 2$ matrices is a subspace of the vector space $\mathbb{R}^{2 \times 2}$ of $2 \times 2$ matrices.

(b) The set of $3 \times 3$ matrices with trace equal to zero is a subspace of $\mathbb{R}^{3 \times 3}$.

(c) There is a $2 \times 3$ matrix $Q$ such that $QQ^T = \begin{bmatrix} 6 & 0 \\ 0 & 3 \end{bmatrix}$.

* If $V$ is a vector space, then $W \subseteq V$ is called a subspace provided that $W$ contains $\vec{0}$ and is closed under addition and scalar multiplication. That is, a subspace of $V$ is a subset $W \subseteq V$ such that
  i. $\vec{0} \in W$;
  ii. if $\vec{x}, \vec{y} \in W$, then also $\vec{x} + \vec{y} \in W$;
  iii. if $\vec{x} \in W$ and $k$ is any scalar, then also $k\vec{x} \in W$.
Contraposition

The contrapositive of the statement \( p \Rightarrow q \) is the statement \( \neg q \Rightarrow \neg p \). The technique of proof by contraposition or taking the contrapositive employs the logical equivalence\(^\text{39}\) of \( p \Rightarrow q \) and \( \neg q \Rightarrow \neg p \). It often happens that the contrapositive is considerably easier to prove than the original statement!

A proof by contraposition usually has the following structure: begin by stating that this is a proof by contraposition; then prove the contrapositive. So, for example, a proof of the statement

Any real number \( x \) that satisfies \( |x| < \epsilon \) for all \( \epsilon > 0 \) must be zero.

might proceed as follows: “Suppose \( x \in \mathbb{R} \). We are trying to show

\[ \forall \epsilon > 0 \; |x| < \epsilon \Rightarrow x = 0. \]

We will prove this by contraposition. The contrapositive is

\[ x \neq 0 \Rightarrow \exists \epsilon > 0 \text{ such that } |x| \geq \epsilon. \]

Suppose \( x \neq 0 \). Let \( \epsilon = |x|/2 > 0 \). Note that \( |x| > |x|/2 = \epsilon \); so \( |x| \geq \epsilon \).”

Exercises

1. Suppose \( A \) and \( B \) are statements. Negate the following statements.
   (a) \( A \) or \( B \).
   (b) \( A \) and \( B \).
   (c) \( A \) and \( \neg B \).
   (d) \( \neg A \) and \( \neg B \).

2. Suppose \( p \) and \( q \) are statements. Use truth tables to verify DeMorgan’s laws:

\[ \neg (p \lor q) \iff (\neg p) \land (\neg q) \quad \text{and} \quad \neg (p \land q) \iff (\neg p) \lor (\neg q). \]

The symbol \( \iff \) is shorthand for “if and only if”.

\[ \begin{array}{c|c|c|c}
   p & q & p \Rightarrow q \\
   \hline
   T & T & T \\
   T & F & F \\
   F & T & T \\
   F & F & T \\
\end{array} \]

and the truth table for \( \neg q \Rightarrow \neg p \) is

\[ \begin{array}{c|c|c|c|c|c}
   p & q & \neg q & \neg p & \neg q \Rightarrow \neg p \\
   \hline
   T & T & F & F & T \\
   T & F & T & F & F \\
   F & T & F & T & T \\
   F & F & T & T & T \\
\end{array} \]
3. (Review.) Suppose $A$ and $B$ are subsets of a set $X$. Show

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \quad \text{and} \quad X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B).$$

4. Find the contrapositive of each of the following statements.

(a) If $n \in \mathbb{Z}$ is odd, then $n^2$ is odd.

(b) Suppose $a, b \in \mathbb{R}$. If $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

(c) Suppose $a, b \in \mathbb{R}$. If $(a + b)^2 = a^2 + b^2$, then $a = 0$ or $b = 0$.

5. Prove that if $x^{17} - x^7 + x^2 \neq 1$, then $x \neq 1$.

6. Prove the statement of Exercise 4b.

7. Prove the statement of Exercise 4c.

8. Prove: If 3 does not divide $ab$, then 3 does not divide $a$ and 3 does not divide $b$.

9. Prove: If the equation $ax^2 + bx + c = 0$ has no solution, then the equation $5ax^2 + 5bx + 5c = 0$ has no solution.

10. (Bonus.) Use proof by contrapositive to show that for all vectors $\vec{u}, \vec{v} \in \mathbb{R}^2$, we have that if $\vec{u}, \vec{v}$ are linearly independent then $\vec{u} + \vec{v}, \vec{u} - \vec{v}$ are linearly independent.

Remember that if $m$ and $n$ are integers, then we say that $m$ divides $n$ provided that there is some integer $k$ such that $km = n$.

Remember that two vectors $\vec{v}$ and $\vec{w}$ in $\mathbb{R}^2$ are linearly independent provided that the only solution to $a\vec{v} + b\vec{w} = \vec{0}$ is $a = b = 0$. 
Contradiction

Proof by contradiction has been described as “one of a mathematician’s finest weapons.”

A proof by contradiction works by assuming that a statement is false, and then shows that this assumption leads to a contradiction. More precisely, if \( p \Rightarrow q \) is the statement to be proved, then a proof by contradiction proceeds by showing that \( \neg(p \Rightarrow q) \) implies \( r \land \neg r \) for some statement \( r \). That this is logically equivalent to showing \( p \Rightarrow q \) is verified in the truth table below. The statement \( r \) is not given to you, but usually arises naturally from the problem under consideration. In the proof that the square root of 2 is not rational on page 6 of the Introduction the statement \( r \) is “At most one of \( a \) or \( b \) is even.” In the proof that \( 2^{1/3} \) is not rational given below, the statement \( r \) is “\( a^n + b^n = c^n \) has no solution in \( \mathbb{N} \) for \( n > 2 \).”

A proof by contradiction usually has the following structure: begin by stating that this is a proof by contradiction; write down what you are assuming; derive a contradiction; finish by stating what has been achieved. For example, a proof that \( 2^{1/3} \) is irrational might go something like this: “Suppose \( 2^{1/3} \) is rational. Then there exists \( m, n \in \mathbb{N} \) such that \( 2^{1/3} = m/n \). Thus \( 2n^3 = m^3 \), or \( n^3 + n^3 = m^3 \). But from Fermat’s Last Theorem we know that \( a^3 + b^3 = c^3 \) has no natural number solutions, a contradiction. Thus, it must be the case that \( 2^{1/3} \) is irrational.”

Exercises

1. Reformulate the statement “\( 2^{1/3} \) is irrational.” in the form \( p \Rightarrow q \).

\[
\begin{array}{c|c|c|c|c}
 p & q & p \Rightarrow q & \neg(p \Rightarrow q) & (r \land \neg r) \\
 T & T & T & F & T \\
 T & F & F & T & F \\
 F & T & T & F & T \\
 F & F & T & F & T \\
\end{array}
\]

\[
\begin{array}{c|c|c}
p & q & p \land \neg q \\
 T & T & F \\
 T & F & T \\
 F & T & F \\
 F & F & T \\
\end{array}
\]

\text{Instead of writing } \neg(p \Rightarrow q), \text{ we often write the logically equivalent } p \land \neg q.

\text{Fermat’s Last Theorem (1637) says} \( (\exists a, b, c \in \mathbb{N} \ a^n + b^n = c^n) \Rightarrow (n \leq 2) \).

It was proved by Andrew Wiles in 1995.
2. Prove by contradiction: The sum of two odd integers is always even.

3. Prove by contradiction: Suppose \( a \in \mathbb{N} \). Show that if \( a^3 \) is even, then \( a \) is even.

4. Prove by contradiction: If \( a \in \mathbb{R} \setminus \mathbb{Q} \) and \( q \in \mathbb{Q} \), then \( a - q \in \mathbb{R} \setminus \mathbb{Q} \).

5. Prove by contradiction: For every \( t \in [0, \pi/2] \) we have \( \sin(t) + \cos(t) \geq 1 \).

6. Prove that the function \( f(x) = 3x^9 + 4x^3 + 42x + 4 \) cannot have more than one root.

7. Show: There are no integers \( a, b \) such that \( 21a + 35b = 1 \).

8. (Bonus.) The vectors \( \begin{bmatrix} 3 \\ 2 \end{bmatrix} \) and \( \begin{bmatrix} 2 \\ -2 \end{bmatrix} \) are linearly independent.

9. (Bonus.) Show: For all integers \( a, b, c \), if \( a^2 + b^2 = c^2 \), then \( a \) is even or \( b \) is even.

Hint: Both \( \sin \) and \( \cos \) are nonnegative on \([0, \pi/2]\). Also, if \( 0 \leq y < 1 \), then \( 0 \leq y^2 < 1 \).

Hint: Rolle’s Theorem (which is a special case of the Mean Value Theorem) might be useful here. Suppose \( a < b \). Rolle’s Theorem says that if \( f: [a,b] \to \mathbb{R} \) is continuous on \([a,b]\), differentiable on \((a,b)\), and \( f(a) = f(b) \), then there exists a point \( d \in (a,b) \) such that \( f'(d) = 0 \).

Hint: Suppose \( k \in \mathbb{Z} \). What are the possible remainders when we divide \( k^2 \) by 4?
**Proof by Induction**

**Mathematical induction** is a common method of proof when showing that a statement $S(n)$, which depends on $n$, is true for all $n$ in $\mathbb{N}$. In general, induction is useful in contexts where the statement $S(\ell + 1)$ is easily relatable to the statement $S(\ell)$. Thus, for example, statements about indexed sums and products are often proved by induction, statements about square matrices can sometimes be proved by induction on their size, and statements about vector spaces can sometimes be proved by induction on their dimension.

A **proof by induction** follows a fairly standard template: show the base case, $S(1)$, is true; show that the inductive step ($S(k)$ true $\Rightarrow$ $S(k + 1)$ true) is valid; invoke the Principle of Mathematical Induction to conclude that $S(n)$ is true for all $n \in \mathbb{N}$. For example, a proof that the statement

$$G(n) := 1 + 2 + \cdots + n = \frac{n(n + 1)}{2}$$

holds for all $n \in \mathbb{N}$ might go something like this: “We will prove this by induction. Since $1 = 1(1 + 1)/2$, the base case $G(1)$ is valid. For the inductive step we assume $k \in \mathbb{N}$ and that $G(k)$ is true. We have

$$1 + 2 + \cdots + k + (k + 1) = [1 + 2 + \cdots + k] + (k + 1)$$

(since $G(k)$ is assumed to be true)

$$= \frac{k(k + 1)}{2} + (k + 1) = \frac{(k + 1)(k + 2)}{2};$$

that is, $G(k)$ true implies $G(k + 1)$ is true. Therefore, the statement $G(m)$ holds for all $m \in \mathbb{N}$ by induction.”

**Exercises**

1. For which of the following statements is proof by induction applicable? If it is not applicable, give a short explanation why.

   (a) $\forall r \in \mathbb{R}_{\geq 0}$, there exists some $s$ such that $s^2 - 1 = r$.  

   The Principle of Mathematical Induction states:

   $$[S(1) \land (\forall k \in \mathbb{N}, S(k) \Rightarrow S(k + 1))] \Rightarrow (\forall m \in \mathbb{N}, S(m)).$$

   This is the result Gauss may or may not have formulated when he was in kindergarten.

   Some tips to follow when writing induction proofs:
   - State at the start of your proof that you are doing a proof by induction.
   - Label the base case and inductive step clearly.
   - State where you use the inductive hypothesis.
   - Write some variation of “therefore the statement holds for all $n$ by induction” at the end of your proof.

   If words like “show for all $n \in \mathbb{N}$” occur in the statement of a problem, then a correct solution will likely involve a proof by induction.
(b) \( \forall n \in \mathbb{N}, 1 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1. \)

(c) \( \exists m \in \mathbb{N} \) such that 7 divides \( m^2 + m - 2. \)

(d) \( \forall k \in \mathbb{N}, k! + 10 > k^2. \)

2. For all \( \ell \in \mathbb{N}, \) show that
\[
1 + 2 + 2^2 + \cdots + 2^\ell = 2^{\ell+1} - 1.
\]

3. \( \forall j \in \mathbb{N}, 1 + 3 + 5 + \cdots + (2j - 1) = j^2. \)

4. For all \( n \geq 2: \)
\[
\ln(n) \geq \frac{1}{2} + \cdots + \frac{1}{n}.
\]

5. For every integer \( \ell \geq 0 \) and for all \( x \geq -1, \) \( (1 + x)^\ell \geq 1 + \ell x. \)

6. Suppose \( Y \) is a finite set with \( n \) elements. The power set of \( Y, \) denoted \( \mathcal{P}(Y), \) is the set of all subsets of \( Y. \) (Power sets were introduced on the worksheet Sets and Functions on page 27.) Show that \( \mathcal{P}(Y) \) has \( 2^n \) elements.
Direct Proof

While we’ve spent much time covering some of the popular, alternative proof techniques, we end with a refresher on straightforward, direct proof writing. For a statement \( p \Rightarrow q \), there are a few standard ways to start constructing a direct proof. You can look at the conclusion \( q \), and think about what could imply it (this could correspond to the penultimate steps in your proof). For example, in Exercise 5 below, you know that you are going to need an integer to plug into the final equation. You can also look at the given \( p \), determine some properties you can quickly derive from \( p \), and then see if these properties move you any closer to proving \( q \). For example, in Exercise 1 below, you might start by writing down the area of \( A \) in terms of \( x \) and \( y \).

We close with a few tips that apply to all of your future mathematical writing.

- Justify each step of your proof. Explain what you’re trying to do at the beginning of major sections in your proof\(^{43}\) as well as what happens at each step.\(^{44}\)
- Write in complete sentences, with correct grammar, punctuation, and capitalization.
- Cite the results that you use.\(^ {45}\)
- When writing proofs, be clear and precise with your language. Write with enough detail that you could hand your proof to a classmate and they could easily follow along.

Exercises

1. Suppose the right triangle \( A \) has legs \( x, y \) and hypotenuse \( z \), and that \( A \) has area \( z^2/4 \). Prove that \( x = y \); that is, prove that \( A \) is isosceles.

\(^{43}\) For example: “We will split the problem into two cases and prove that the statement holds in each case.”

\(^{44}\) For example: “Multiplying by two on both sides, we see that …”

\(^{45}\) For example: “By theorem 1.10 we know that…” or “By the lemma from class stating that every matrix satisfying … has the property …, we conclude …”
2. Let $a + bi$ be a nonzero complex number. Explicitly calculate the multiplicative inverse of $a + bi$ and write it in standard form. That is, find $c, d \in \mathbb{R}$ such that:

$$(a + bi)(c + di) = 1.$$ 

3. Consider the diagram to the right. Prove that if $\angle A \cong \angle C$ and $\overline{AB} \cong \overline{BC}$, then $\overline{AD} \cong \overline{EC}$. (Here “$\cong$” means “congruent”.)

4. Suppose you want to show that two lines, $\ell$ and $\ell'$, in $\mathbb{R}^2$ are parallel. Which of the following methods are valid? Prove your answer.

(a) Show that both of $\ell$ and $\ell'$ are parallel to a third line.

(b) Show that either $\ell$ and $\ell'$ have the same slope or they are both vertical.

(c) Show that each of $\ell$ and $\ell'$ is perpendicular to a third line.

(d) Show that $\ell$ and $\ell'$ are on opposite sides of a quadrilateral.

(e) For each line choose a nonzero vector parallel to the line, then show that the two resulting vectors have a dot product of zero.

5. If $n$ is an integer satisfying $2n^2 - 7n + 6 = 0$, then $3n^2 - 5n = 2$.

6. Let $a, b$ be the legs of a right triangle, and $c$ the hypotenuse. For $n > 2$, prove that $c^n > a^n + b^n$.

7. (Bonus.) Prove that for an invertible matrix $n$-by-$n$ matrix $M$, $\det(M^{-1}) = (\det M)^{-1}$. You may use the fact that $\det(A) \det(B) = \det(AB)$ for all $n \times n$ matrices $A$ and $B$. 

Hint: What are the last steps leading up to “$3n^2 - 5n = 2$”? 

Hint: You may want to consult Euclid’s *The Elements*: Book I, Proposition 27 

Hint: $c > a$ and $c > b$. Why? 

Hint: $\det(A) \det(B) = \det(AB)$ for all $n \times n$ matrices $A$ and $B$. Look at some immediate consequences of invertibility.
Part III

Back Matter
The Joy of Sets

The study of modern mathematics requires a basic familiarity with the notions and notation of set theory.¹ For a rigorous treatment of set theory, you may wish to take Math 582, Introduction to Set Theory.

What is a set?

A colony of beavers, an unkindness of ravens, a murder of crows, a team of oxen, . . . each is an example of a set of things. Rather than define what a set is, we assume you have the “ordinary, human, intuitive (and frequently erroneous) understanding”² of what a set is.

Sets have elements, often called members. The elements of a set may be flies, beavers, words, sets, vectors, . . . . If x is some object and S is a set, we write x ∈ S if x is an element of S and x ∉ S if x is not a member of S. For us, the most important property a set S has is this: if x is an object, then either x ∈ S or x ∉ S, but not both.

The sets N, Z, Q, and R are well-known to you, though you may not know their names. The set of natural numbers is denoted by N, and its elements are the numbers 1, 2, 3, 4, . . . . Note that if n, m ∈ N, then n + m ∈ N; that is, N is closed under addition. However, N is not closed under subtraction. For example, (4 − 5) ∉ N. To overcome this inconvenience we consider Z, the set of integers, which has as its elements the numbers 0, ±1, ±2, ±3, . . . . While Z is closed under addition, subtraction, and multiplication, it is not closed under division. For example, (−23)/57 ∉ Z. To surmount this difficulty, we form the set of rational numbers, Q. Intuitively, Q is the set of all numbers that can be expressed as a fraction n/m with n ∈ Z and m ∈ N. While closed under multiplication, division, addition, and subtraction, Q is missing important numbers like √2. There are many ways to overcome this inconvenience; the most common approach is to introduce R, the set of real numbers. R is usually depicted as a line that extends forever in both directions.

A way to specify a finite set is by listing all of its elements; this is sometimes called the roster method. The cardinality of a finite set is the number of elements that the set contains. For example, the sets

\[ \{\pi, \sqrt{2}, 32, -5.4\} \quad \text{and} \quad \{\pi, -2, e, \{\pi, \sqrt{2}, 32, -5.4\}\} \]

both have cardinality four. The cardinality of a set A is denoted |A|.

The most common way to specify a set is by using set-builder or comprehension notation. For example, the set of primes could be written

\[ \{x \in \mathbb{N} : \text{prime}(x)\} \]

³ In 1960 Grace Chisholm Young and her spouse William published their highly influential How to Find the First Million Prime Numbers. It was the first textbook on set theory.

Math 582, Introduction to Set Theory, provides a rigorous treatment of N.

Warning: Some people consider zero to be a natural number.

The symbol Z is derived from Zahlen, the German word for numbers.

Never divide by zero.

In Math 412, Introduction to Modern Algebra, Q is rigorously defined.

Approximately 1.41, √2 is the ratio of a square’s diagonal to one of its sides. Historians believe it was the first number understood not to belong to Q.

Introductory analysis courses, including Math 351 and Math 451, provide in-depth treatments of R.

Approximately 3.14, π is the ratio of a circle’s circumference to its diameter.

Approximately 2.72, e is \( \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n \).

The first four primes are: 2, 3, 5, and 7. In particular, 1 is not a prime number.


² In 1906 Grace Chisholm Young and her spouse William published their highly influential The Theory of Sets of Points. It was the first textbook on set theory.

³ In 1960 Grace Chisholm Young and her spouse William published their highly influential How to Find the First Million Prime Numbers. It was the first textbook on set theory.
\{n \in \mathbb{N} \mid n \text{ has exactly two distinct positive divisors}\},

the open interval \((\ln(2), 1)\) could be written
\[\{x \in \mathbb{R} \mid 2 < e^x < e\},\]
and the set of non-negative integers, \(\mathbb{Z}_{\geq 0}\), could be written
\[\{m \in \mathbb{Z} \mid m \geq 0\} .\]

Russell’s paradox provides a non-example of a set. Consider
\[\{S \text{ is a set} \mid S \notin S\} .\]

Call this candidate for set-hood \(T\). As you should verify, we have both \(T \in T\) and \(T \notin T\). Thus, \(T\) does not have the most important property, and so is not a set.

**Set relations: Equality**

One can’t do mathematics for more than ten minutes without grappling, in some way or other, with the slippery notion of equality. Slippery, because the way in which objects are presented to us hardly ever, perhaps never, immediately tells us — without further commentary — when two of them are to be considered equal.\(^3\)

**Definition 1.** Two sets are defined to be equal when they have precisely the same elements. When the sets \(A\) and \(B\) are equal, we write \(A = B\).

That is, the sets \(A\) and \(B\) are equal if every element of \(A\) is an element of \(B\), and every element of \(B\) is an element of \(A\). For example, thanks to Lagrange’s four-square theorem (1770),\(^4\) we have
\[\mathbb{Z}_{\geq 0} = \{n \in \mathbb{Z} \mid n \text{ is the sum of four squares of integers}\} .\]

The next example shows that order and inefficiency do not matter.
\[
= \{I, A, M, L, O, R, D, V, O, L, D, E, M, O, R, T\} \\
= \{A, D, E, I, L, M, O, R, T, V\} .
\]

Since two sets are the same provided that they have precisely the same elements, there is exactly one set with cardinality zero; it is called the empty set or null set and is denoted \(\emptyset\). Beware: The set \(\emptyset\) has zero elements, but the set \(\{\emptyset\}\) has cardinality one.

**Set relations: Subset**

**Definition 2.** If \(A\) and \(B\) are sets, then we say that \(A\) is a subset of \(B\) (or \(A\) is contained in \(B\), or \(B\) contains \(A\), or \(A\) is included in \(B\), or \(B\) includes \(A\)), and write \(A \subset B\) or \(A \subseteq B\), provided that every element of \(A\) is an element of \(B\).

Approximately \(.69, \ln(2) = \sum_{i=0}^{\infty} \frac{(-1)^i}{i+1}\).

For \(a, b \in \mathbb{R}\) with \(a \leq b\) we define
\[
[a,b] := \{x \in \mathbb{R} \mid a \leq x \leq b\}, \\
(a,b] := \{x \in \mathbb{R} \mid a < x \leq b\}, \\
[a,b) := \{x \in \mathbb{R} \mid a \leq x < b\}, \\
(a, b) := \{x \in \mathbb{R} \mid a < x < b\},\]
and
\([a,\infty) := \{x \in \mathbb{R} \mid x \geq a\} .\]

The sets \((a,\infty), (-\infty, a),\) and \((-\infty, a]\) are defined similarly.

**Practice:** Test your understanding of set notation using Doug Ensley’s material at http://www.math.lsa.umich.edu/courses/181/sets.html.

\(^3\) Barry Mazur, *When is one thing equal to some other thing?*, Proof and other dilemmas, 2008.

The notations “\(=\)” and “\(:=\)” do not mean the same thing. The latter means: this is the definition of the object on the left.

\(^4\) When you encounter a new mathematical statement, work examples:
\begin{align*}
0 &= 0^2 + 0^2 + 0^2 + 0^2 \\
1 &= 1^2 + 0^2 + 0^2 + 0^2 \\
2 &= 1^2 + 1^2 + 0^2 + 0^2 \\
3 &= 1^2 + 1^2 + 1^2 + 0^2 \\
4 &= 1^2 + 1^2 + 1^2 + 1^2 \\
5 &= 2^2 + 0^2 + 0^2 + 0^2 \\
6 &= 2^2 + 1^2 + 0^2 + 0^2
\end{align*}

Also try to formulate new questions based on your understanding of the statement. For example, you could ask: which numbers can, like 4, be written as a sum of four squares in more than one way?

**Warning:** Some people say “\(A\) contains \(a\)” to mean “\(a \in A\).”

**Warning:** Some people write “\(A \subset B\)” to mean “\(A \subset B\), but \(A \neq B\).” We will write “\(A \subsetneq B\)” for this.
For example, $\mathbb{N} \subset \mathbb{Z} \subseteq \mathbb{Q} \subset \mathbb{R}$; to emphasize that each inclusion is proper, we could write $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$. We also have $1 \in \{1, \sqrt{2}\} \subset (\sqrt{\pi}/2, \sqrt{2}] \subseteq [\ln(2), e) \subset [\ln(2), e]$ and the obvious inclusion $\{n \in \mathbb{N} \mid n \text{ is even and the sum of two primes}\} \subset \{2m + 2 \mid m \in \mathbb{N}\}$.

Note that for any set $A$ we have $\emptyset \subset A \subset A$.

**Unreasonably Useful Result.** Suppose that $X$ and $Y$ are sets.

$$X = Y \text{ if and only if } X \subset Y \text{ and } Y \subset X.$$  

**Proof.** By Definition 1, to say that $X$ and $Y$ are equal means that every element of $X$ is an element of $Y$ and every element of $Y$ is an element of $X$. In other words, by Definition 2, to say $X = Y$ means that $X \subset Y$ and $Y \subset X$. \[\square\]

**Venn diagrams**

Representing sets using Venn diagrams can be a useful tool for visualizing the relationships among them. In a Venn diagram a larger figure, often a rectangle, is used to denote a set of objects called the universe (for example the universe could be $\mathbb{R}$) and smaller figures, usually circles, within the diagram represent subsets of the universe — points inside a circle are elements of the corresponding subset.

![Venn Diagrams](image)

**CAUTION.** Because many statements about sets are intuitive and/or obvious, figuring out how to prove them can be difficult. While Venn diagrams are excellent tools for illustrating many of these statements, the diagrams are not substitutes for their proofs.

**Set operations: Complement, union, and intersection**

In the Venn diagrams illustrating the definitions of this section, the set $A$ is represented by the circle to the left, the set $B$ is represented

---

5 If you can demonstrate the reverse inclusion, you will have proved the Goldbach conjecture, one of the older unsolved problems in mathematics.

\begin{align*}
4 &= 2 + 2 \\
6 &= 3 + 3 \\
8 &= 3 + 5 \\
10 &= 7 + 3 \\
&= 5 + 5 \\
\vdots
\end{align*}

The symbol $\square$ is called a tombstone or halmos, after former Michigan mathematics professor Paul Halmos. It means: my proof is complete, stop reading. It has replaced the initialism Q.E.D. which stands for *quod erat demonstrandum*; a phrase that means *that which was to be demonstrated*.

**Figure 1:** The left Venn diagram illustrates relationships among upper case letters in the Greek, Latin, and Russian alphabets. The universe consists of all upper case letters in these alphabets, and each language is represented by one of the circles. The Venn diagram on the right describes the geographical areas (red) and political entities (blue) that make up the British Isles. With the exception of the United Kingdom, items labeled in blue are the elements of the universe. The remaining words describe the rule for membership in their respective circles.

**Practice:** Use Doug Ensley’s materials to gain basic familiarity with set operations at www.math.lsa.umich.edu/courses/101/venn2.html and www.math.lsa.umich.edu/courses/101/venn3.html.
by the circle to the right, and the box represents a universe that contains both $A$ and $B$.

**Definition 3.** The union of sets $A$ and $B$, written $A \cup B$, is the set

$$\{ \varnothing | (\varnothing \in A) \text{ or } (\varnothing \in B) \}.$$ 

In other words, for an object to be an element of the union of two sets, it need only be a member of one or the other of the two sets. For example, the union of the sets $\{e, \delta, \alpha\}$ and $\{\delta, \beta, \rho, \phi\}$ is the set $\{\delta, \beta, \rho, \epsilon, \rho, \phi\}$, the union of $Z$ and $Q$ is $Q$, and $[\ln(2), \sqrt{2}] \cup (\sqrt{2}/2, e]$ is $[\ln(2), e]$. Note that $S \cup \emptyset = S$ for all sets $S$.

**Definition 4.** The intersection of sets $A$ and $B$, written $A \cap B$, is the set

$$\{ \varnothing | (\varnothing \in A) \text{ and } (\varnothing \in B) \}.$$ 

Thus, for an object to be a member of the intersection of two sets, it must be an element of both of the sets. For example, the intersection of the sets $\{e, \delta, \alpha\}$ and $\{\delta, \beta, \rho, \phi\}$ is the singleton $\{\delta\}$, the intersection of $Z$ and $Q$ is $Z$, and $[\ln(2), \sqrt{2}] \cap (\sqrt{2}/2, e]$ is $(\sqrt{2}/2, \sqrt{2}]$. Note that $T \cap \emptyset = \emptyset$ for all sets $T$.

**Remark 5.** For $S$ and $T$ sets, $S \cap T \subset S \subset S \cup T$ and $S \cap T \subset T \subset S \cup T$.

**Definition 6.** Suppose $A$ and $B$ are sets. The difference of $B$ and $A$, denoted $B \setminus A$ or $B - A$, is the set

$$\{ b \in B | b \notin A \}.$$ 

Note that, like subtraction, the difference operator is not symmetric. For example, $\{e, \delta, \alpha\} \setminus \{\delta, \beta, \rho, \phi\}$ is $\{\alpha, \epsilon\}$ while $\{\delta, \beta, \rho, \phi\} \setminus \{e, \delta, \alpha\}$ is $\{\beta, \rho, \phi\}$. As another example, we have $[\ln(2), e] \setminus (\sqrt{2}/2, \sqrt{2}]$ is $[\ln(2), \sqrt{2}/2] \cup (\sqrt{2}, e]$ and $(\sqrt{2}/2, \sqrt{2}] \setminus [\ln(2), e] = \emptyset$.

**Definition 7.** Let $U$ denote a set that contains a subset $A$. The complement of $A$ (with respect to $U$), often written $A^c$, $\overline{A}$, $\bar{A}$, or $A'$, is the set $U \setminus A$.

**Warning:** It is common practice to suppress reference to the set $U$ occurring in the definition of complement. Relying on the reader to implicitly identify the set $U$ can cause confusion, but context often clarifies. For example, if asked to find $[-1, \pi]^C$, then from context the set $U$ is $\mathbb{R}$ and $[-1, \pi]^C = (-\infty, -1) \cup [\pi, \infty)$.

Note that $A^c \cup A$ is $U$, and $A^c \cap A = \emptyset$. Two sets with empty intersection are said to be disjoint.

DeMorgan’s Laws relate the set operations. You should use the definition of equality to verify them. They say

$$(A \cup B)^c = A^c \cap B^c \quad \text{and} \quad (A \cap B)^c = A^c \cup B^c.$$  

---

© The University of Michigan, 2019

---

6 Mathematics is not a spectator sport. In order to understand math, you need to do math; now is a good time to start.
Mathematical Hygiene

These notes are designed to expose you to elementary logic, the grammar of mathematical communication. Once internalized, this material will help keep your mathematics “healthy and strong.”¹ For a rigorous treatment of logic, you may wish to take Math 481, Introduction to Mathematical Logic.

Statements

Ambiguity is accepted, maybe even welcomed, in certain methods of discourse. As Definition 1 suggests, it is generally avoided in math.

Definition 1. A statement, also called a proposition, is a sentence that is either true or false, but not both.

For example, the sentences 
\[1 + 2 + 3 = 1 \cdot 2 \cdot 3,\]
\[5 + 4 = 8,\]
\[x = \pi + 34,\]
\[\text{This sentence is false.}\]
\[\text{When does Michigan play today?}\]
\[\text{and Go Blue!}\]

are all statements. However, the sentences
\[(\text{This sentence is false.})\]
\[(\text{When does Michigan play today?})\]
\[(\text{and Go Blue!})\]

are all not statements.

To help distinguish between examples and the running text, statements will often be placed in parentheses. For example, for a fixed object \(x\) and a fixed set \(S\) both \((x \in S)\) and \((x \notin S)\) are statements.

In math, the symbols \(p\) and \(q\) are often used as short hand for statements. If \(p\) is a statement, then its truth value is \(T\) if \(p\) is true and \(F\) if \(p\) is false. For example, the truth value of the statement \((3 \cdot 4 = 13)\) is \(F\), while the the truth value of both \((1001 = 7 \cdot 11 \cdot 13)\) and \((\text{The Michigan Math Club meets on Thursdays at 4PM in the Nesbitt Commons Room, East Hall.})\) is \(T\).

Negation and truth tables

The negation of a statement \(p\) is written \(\neg p\) and read “not \(p\).” The negation can usually be formed by inserting the word not into the original statement. For example, the negation of \((1000009\) is prime.) is \((1000009\) is not prime.). We require that \(\neg p\) have the opposite truth value of \(p\), and so, for example, \((\text{All mathematicians are left-handed.})\) is \((\text{Not all mathematicians are left-handed.})\) rather than \((\text{All mathematicians are not left-handed.})\).

A truth table is a tabulation of the possible truth values of a logical operation. For example, the truth table for negation appears in Table 1. For each possible input (the truth value of \(p\) is either \(T\) or \(F\)) the table records the output of the negation operation.

<table>
<thead>
<tr>
<th>(p)</th>
<th>(\neg p)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(T)</td>
<td>(F)</td>
</tr>
<tr>
<td>(F)</td>
<td>(T)</td>
</tr>
</tbody>
</table>

Table 1: The truth table for negation.

¹ “Logic is the hygiene that the mathematician practices to keep his ideas healthy and strong.” (Hermann Weyl, quoted in American Mathematical Monthly, November 1992)

See www.math.lsa.umich.edu/career/ for information about careers for students of math.

For a fixed value of \(x\) the sentence \(x = \pi + 34\) is either true or false. However, as a value for \(x\) has not been specified, the sentence is neither true nor false.

The phrase “mind your p’s and q’s” becomes especially relevant in this part of mathematics.

Math Club events feature an engaging math talk and free pizza and pop. See www.math.lsa.umich.edu/mathclub.

By writing it as a sum of two squares in two different ways, Euler deduced that \(1000009 = 293 \cdot 3413\).
Equivalent statements

Suppose the edges of a triangle $T$ have lengths $a$, $b$, and $c$ with $a \leq b \leq c$. Thanks to Pythagoras and others we know\(^2\) that the statement $(a^2 + b^2 = c^2)$ is equivalent to the statement ($T$ is a right triangle). Similarly, (Not all mathematicians are left-handed.) is equivalent to (Some mathematicians are not left-handed.).

When statements $p$ and $q$ are equivalent, we write $p \iff q$. We remark that equivalent statements have the same truth values.

In the standard interpretation of English, two negatives make a positive. The same is true in logic: for all statements $p$ we have $\neg(\neg p) \iff p$. As expected, $\neg(\neg p)$ and $p$ have the same truth values:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\neg p$</th>
<th>$\neg(\neg p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Compound statements: Conjunctions and Disjunctions

Mathematics and English agree about the meaning of “and.” The conjunction of statements $p$ and $q$ is the statement ($p$ and $q$), often written $(p \land q)$. Note that the statement $(p \land q)$ is true when both $p$ and $q$ are true and is false otherwise.

However, Mathematics and English disagree when it comes to the meaning of the word “or.” For example, if your mathematics instructor says

“As a prize, you may have a t-shirt or a keychain,”

then the standard interpretation of this statement is “As a prize, you may have a t-shirt or a keychain, but not both.” This is not the mathematical meaning of the statement. The mathematical meaning is “As a prize, you may have a t-shirt, a keychain, or both.” The disjunction of statements $p$ and $q$ is the statement ($p$ or $q$), often written $(p \lor q)$. Note that the statement $(p \lor q)$ is false when both $p$ and $q$ are false and is true otherwise.

The operations of negation, conjunction, and disjunction correspond\(^3\) to the set operations of complement, intersection, and union, respectively. It is therefore not surprising that relations among negation, conjunction, and disjunction are encapsulated in DeMorgan’s Laws:

$\neg(p \lor q) \iff (\neg p) \land (\neg q)$ and $\neg(p \land q) \iff (\neg p) \lor (\neg q)$.

Conditional Statements

When Bruce Willis’ character in Die Hard expounds “If you’re not part of the solution, [then] you’re part of the problem,” he has com-

\(^2\) Euclid’s Elements, Book I, Propositions 47 and 48.

“The English linguistics professor J.L. Austin was lecturing one day. ‘In English,’ he said, ‘a double negative forms a positive. In some languages though, such as Russian, a double negative is still a negative. However,’ he pointed out, ‘there is no language wherein a double positive can form a negative.’ From the back of the room, the voice of philosopher Sydney Morgenbesser piped up, ‘Yeah, right.’” (The Times, September 8, 2004)

Michigan Math t-shirts are available for purchase in the Undergraduate Office, 2082 East Hall.

In the table below, the first row of truth values reflects the difference between mathematics and English.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \land q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

\(^3\) $A^C = \{x | \neg(x \in A)\}$

$A \cap B = \{x | (\in A) \land (\in B)\}$

$A \cup B = \{x | (\in A) \lor (\in B)\}$

bined the statements \( r = \text{(You're not part of the solution.)} \) and \( s = \text{(You're part of the problem.)} \) to form the conditional statement (If \( r \), then \( s \)).

For statements \( p \) and \( q \) the conditional statement (If \( p \), then \( q \)) is often written \( (p \Rightarrow q) \) and read “\( p \) implies \( q \).” The statement \( p \) is called the hypothesis (or antecedent or premise) and the statement \( q \) is called the conclusion (or consequent). Mathematically, the statement \( (p \Rightarrow q) \) is false when \( p \) is true and \( q \) is false and is true otherwise.

Note that \( p \Rightarrow q \) is false exactly once: when a true hypothesis implies a false conclusion. Does this agree with our ordinary understanding of implication? Consider Almira Gulch’s threat to Dorothy:

“If you don’t hand over that dog, then I’ll bring a damage suit that’ll take your whole farm.”

\[ \text{The Wizard of Oz, 1939} \]

Suppose that Dorothy hands over that dog, Toto, thus failing to carry out the hypothesis. In this case, Ms. Gulch’s statement is true independent of whether or not she fulfills the conclusion by bringing a damage suit. Should Dorothy choose to fulfill the hypothesis by not handing over the dog, then Ms. Gulch’s statement is false unless she files suit. So, it appears mathematics and English agree for this example. On the other hand, the mathematically correct statement (If \( 3 = 7 \), then \( 8 = 4 + 4 \)) sounds bizarre, even to a mathematician.

As with all statements, the statement \( p \Rightarrow q \) may be negated. Since the negation of \( (p \Rightarrow q) \) is required to be true when \( p \) is true and \( q \) is false, and false otherwise, we must have \( \neg(p \Rightarrow q) \Leftrightarrow p \land \neg q \). Thus, the negation of (If you’re not part of the solution, then you’re part of the problem.) is (You are not part of the solution and yet you are not part of the problem.), and for a function \( f \) on the real numbers, the negation of (If \( f \) is differentiable at \( \pi \), then \( f \) is continuous at \( \pi \)) is \( (f \) is differentiable at \( \pi \), and \( f \) is not continuous at \( \pi \)).

Predicates

The sentence \( y > 4 \) is not a statement because, depending on the value of the variable \( y \), the sentence may be either true or false. Since sentences such as \( y > 4 \) arise very often, we give them their own name, predicate. We often use notation like \( p(x) \) to denote a predicate that depends on a variable \( x \). So, for example, \( p(x) \) might denote the predicate \( 2 < e^x < e^2 \) and \( q(\odot, \ominus) \) might denote the predicate \( \odot^2 + \ominus^2 = 34 \).

As with statements, a predicate can be negated. For example, suppose \( q(\odot, \ominus) = \odot^2 + \ominus^2 = 34 \) and \( r(y) = y > 4 \), then \( \neg q(\odot, \ominus) \) is \( \odot^2 + \ominus^2 \neq 34 \) and \( \neg r(y) \) is \( y \leq 4 \).

| \begin{array}{c|c|c|c} p & q & p \Rightarrow q \\ \hline T & T & T \\ T & F & F \\ F & T & T \\ F & F & T \end{array} |

| \begin{array}{c|c|c|c} p & q & p \land \neg q & \neg(p \Rightarrow q) \\ \hline T & T & F & F \\ T & F & T & T \\ F & T & F & F \\ F & F & F & F \end{array} |

When \( p \Rightarrow q \) is true, we say that \( p \) is a sufficient condition for \( q \). For example, a sufficient condition for a function on the real numbers to be continuous at \( \pi \) is that the function be differentiable at \( \pi \).

When \( p \Rightarrow q \) is true, we say that \( q \) is a necessary condition for \( p \). For example, \( \lim_{n \to \infty} a_n = 0 \) is a necessary condition for the series \( \sum_{n=1}^{\infty} a_n \) to converge.

Practice: To gain familiarity with predicates, use Doug Ensley’s material at [www.math.lsa.umich.edu/courses/101/predicate.html](http://www.math.lsa.umich.edu/courses/101/predicate.html).

Practice: To gain familiarity with negating predicates, use Doug Ensley’s material at [www.math.lsa.umich.edu/courses/101/np1.html](http://www.math.lsa.umich.edu/courses/101/np1.html) and [www.math.lsa.umich.edu/courses/101/np2.html](http://www.math.lsa.umich.edu/courses/101/np2.html).
Quantifiers

By quantifying the variable that occurs in a predicate, we can create statements. For example,

(There exists a real number \( y \) such that \( y > 4 \).) \hspace{1cm} (1)

is true (and, since it is not false, is therefore a statement), and

(For all real numbers \( y \), we have \( y > 4 \).) \hspace{1cm} (2)

is false (and, since it is not true, is therefore a statement). The words *there exists* and *for all* in statements (1) and (2) are called quantifiers. While the words “for all” and “there exists . . . such that” don’t take long to write out, they appear so frequently that the following shorthand has been adopted: the symbol \( \forall \) translates as “for all” and the symbol \( \exists \) translates as “there exists . . . such that.” Thus, statement (1) is equivalent to \( (\exists y \in \mathbb{R} \ r(y)) \), and statement (2) is equivalent to \( (\forall y \in \mathbb{R}, r(y)) \).

Often, quantifiers are hidden. For example, the statement (Every integer is even.) can be written \( (\forall n \in \mathbb{Z}, n \text{ is even}) \) and the statement (Some integers are even.) is equivalent to \( (\exists m \in \mathbb{Z} \ m \text{ is even}) \). Ferreting out hidden quantifiers can be more than half the battle.

Here are two final examples that may be familiar to you. Fermat’s Last Theorem says

\[
\forall n \in \mathbb{N}, (\exists a, b, c \in \mathbb{N} a^n + b^n = c^n) \Rightarrow (n \leq 2)
\]

and, for a predicate \( S \), the Principle of Mathematical Induction states

\[
[S(1) \land (\forall n \in \mathbb{N}, S(n) \Rightarrow S(n + 1))] \Rightarrow (\forall m \in \mathbb{N}, S(m)).
\]

Negation and quantifiers

Recall that if \( p \) is a statement, then the symbol \( \neg p \) denotes the negation of \( p \). With the addition of quantifiers to the mix, negation can be more challenging. For example, \( \neg(\text{Everybody remembers how to negate statements.}) \) is (Somebody does not remember how to negate statements.) and the negation of (Some integers are even.) is (Every integer is odd.). The negation of statement (1) is (For all real numbers \( w, w \leq 4 \).), and the negation of statement (2) is (There exists a real number \( z \) such that \( z \leq 4 \)). Do you see the pattern? For a predicate \( p(x) \) we have

\[
\neg(\forall x, p(x)) \text{ is } \exists z \: \neg p(z) \text{ and } \neg(\exists w \: p(w)) \text{ is } \forall \nu, \neg p(\nu).
\]

Thus, the negation of (Every triangle is isosceles.) is (Some triangle is not isosceles.) and \( \neg(\text{There is a positive real number that is greater than its square.}) \) is (Every positive real number is less than or equal to its square.).

In Calculus, a function \( f \) is said to be continuous at \( a \) provided that

\[
\forall \epsilon > 0, \exists \delta > 0 \forall x \in \mathbb{R}, (|x - a| < \delta) \Rightarrow (|f(x) - f(a)| < \epsilon).
\]

Thus, as you should verify, a function \( f \) is not continuous at \( a \) provided that

\[
\exists \epsilon > 0 \forall \delta > 0, \exists x \in \mathbb{R}, (|x - a| < \delta) \land (|f(x) - f(a)| \geq \epsilon).
\]

"Don’t just read it; fight it! Ask your own questions, look for your own examples, discover your own proofs."
(Paul Halmos, *I Want to be a Mathematician*, 1985)

© The University of Michigan, 2019
More Joy of Sets

In this handout we continue our summary of basic set theory begun in The Joy of Sets, with a special emphasis on functions.

Functions

If X and Y are sets, a function from X to Y is a rule\(^1\) that assigns to each element \(x\) in the set \(X\) a unique element \(y\) in the set \(Y\). A good name for a function is \(f\). (You can probably guess why). If \(f\) is a function from \(X\) to \(Y\) and \(x \in X\), the unique element \(y \in Y\) that \(f\) associates to \(x\) is called the value of \(f\) at \(x\), usually written\(^2\) \(f(x)\). To indicate that \(f\) is a function from \(X\) to \(Y\), we write \(f : X \to Y\). In math, the words map or mapping are synonymous\(^3\) with function.

If \(f : X \to Y\) is a function from \(X\) to \(Y\), the set \(X\) is called the domain or source of \(f\), and the set \(Y\) is called the codomain or target space of \(f\). Sometimes it is useful to have notation for this, so we might write \(\text{dom}(f)\) for the domain of the function \(f\) and \(\text{cod}(f)\) for its codomain.

It often helps to picture functions using “blobs and arrows” as in Figure 1. If you picture \(\text{dom}(f)\) as one blob (on the left) and \(\text{cod}(f)\) as another blob (on the right), then you can represent \(f\) using arrows that transform inputs in \(\text{dom}(f)\) into outputs in \(\text{cod}(f)\).

Functions are often defined using rules that specify how to convert an input \(x\) into an output \(y = f(x)\). When variables are used in this manner to define a function via a rule, the input variable (often, but not always, \(x\)) is called the independent variable, and the output variable (often, but not always, \(y\)) is called the dependent variable.

For any function \(f : X \to Y\), the image\(^4\) of \(f\), written \(\text{im}(f)\), is the set

\[
\text{im}(f) := \{f(x) : x \in X\}
\]

of all values that \(f\) takes on (see Figure 2). More generally, if \(f : X \to Y\) is any function, then for subsets \(A \subseteq X\) and \(B \subseteq Y\) we define the direct image or\(^3\) forward image of \(A\) under \(f\) to be the set

\[
f[A] := \{f(a) \in Y : a \in A\} \subseteq \text{cod}(f),
\]

and we define the inverse image or\(^3\) preimage of \(B\) under \(f\) to be the set

\[
f^{-1}[B] := \{x \in X : f(x) \in B\} \subseteq \text{dom}(f).
\]

These operations have friendly properties that are fun to prove.\(^5\)

Example. For any set \(X\), the identity function \(\text{id}_X : X \to X\) is defined by the rule \(\text{id}_X(x) = x\) for all \(x \in X\). Identity functions may seem kind of boring, but you will encounter them frequently and find them to be quite useful.

\(^1\) Some folks use range to mean image, but others use it to mean codomain, so we avoid the term altogether.

\(^2\) If you are worried about what exactly a “rule” is or suspect that this definition is not entirely rigorous, have patience! We will remedy this below.

\(^3\) Thanks, Euler! (For those who read left-to-right, it would have been better\(^6\) to write \((x)f\) instead of \(f(x)\). Oh well.)

\(^4\) “\(f : X \to Y\)” is read “\(f\) maps \(X\) to \(Y\).” Note that the arrow “\(\to\)” goes between the domain \(X\) and codomain \(Y\); for individual elements in \(X\) and \(Y\), we use the arrow “\(\to\)” and write “\(x \mapsto f(x)\)”.

\(^5\) If \(f : X \to Y\) is a function, then for all \(A, B \subseteq X\) and \(C, D \subseteq Y\) we have:

(i) \(f[f^{-1}[C]] \subseteq C\)

(ii) \(f^{-1}[f[A]] \supseteq A\)

(iii) \(f[A \cup B] = f[A] \cup f[B]\)

(iv) \(f[A \cap B] \subseteq f[A] \cap f[B]\)

(v) \(f[A \setminus B] \supseteq f[A] \setminus f[B]\)

(vi) \(f^{-1}[C \cup D] = f^{-1}[C] \cup f^{-1}[D]\)

(vii) \(f^{-1}[C \cap D] = f^{-1}[C] \cap f^{-1}[D]\)

(viii) \(f^{-1}[C \setminus D] = f^{-1}[C] \setminus f^{-1}[D]\)
Example. The squaring function \( f : \mathbb{R} \to \mathbb{R} \) is defined by the rule \( f(x) = x^2 \) for all \( x \in \mathbb{R} \).

Example. The power set of a set \( X \) is the collection of all subsets of \( X \). Viewed as a function \( \mathcal{P} : V \to V \) on the universe \( V \) of all sets, \( \mathcal{P} \) is defined by the rule \( \mathcal{P}(X) = \{ Y : Y \subseteq X \} \).

Functions can be iterated with each other to produce new functions in a process called composition (see Figure 3). Specifically, if \( X \), \( Y \), and \( Z \) are sets and \( f : X \to Y \) and \( g : Y \to Z \) are functions, the composite function \( g \circ f : X \to Z \) is defined\(^\circ\) by \( (g \circ f)(x) = g(f(x)) \) for all \( x \in X \). Composition of functions is associative; that is, for any sets \( W \), \( X \), \( Y \), and \( Z \) and functions \( f : W \to X \), \( g : X \to Y \), and \( h : Y \to Z \), we have \( h \circ (g \circ f) = (h \circ g) \circ f \).

Definition. If \( f : X \to Y \) is a function, then an inverse of \( f \) is a function \( g : Y \to X \) such that \( g \circ f = \text{id}_X \) and \( f \circ g = \text{id}_Y \). The function \( f : X \to Y \) is said to be invertible if it has an inverse.

If \( f \) is invertible, then its inverse is unique and is denoted \( f^{-1} \). Fortunately, there is a handy way of checking\(^*\) whether a function is invertible without having to know much about its inverse.

Definition. Let \( f : X \to Y \) be a function. Then \( f \) is:

- **injective** if for all \( x, x' \in X \), \( x \neq x' \) implies \( f(x) \neq f(x') \);
- **surjective** if for all \( y \in Y \) there is \( x \in X \) such that \( y = f(x) \);
- **bijective** if \( f \) is both injective and surjective.

Can you explain (see Figure 2!) how to think of injectivity and surjectivity in terms of the “blobs and arrows” picture?

\(^*\)Theorem. For any function \( f \), \( f \) is invertible if and only if \( f \) is bijective.

Note that for two functions to be equal to each other they must have the same domain and codomain. We can obtain new functions from a given function \( f : X \to Y \) by changing \( \text{dom}(f) \) or \( \text{cod}(f) \).

Definition. If \( f : X \to Y \) is a function and if \( A \subseteq X \), the restriction of \( f \) to \( A \) is the function \( g : A \to Y \) defined by the rule \( g(x) = f(x) \) for all \( x \in A \). The restriction of \( f \) to \( A \) is often denoted \( f \upharpoonright A \) or \( \text{res}_Af \).

Example. Let \( f : \mathbb{R} \to \mathbb{R} \) be the squaring function. Then \( f \) is neither injective nor surjective, but \( f \upharpoonright [0, \infty) \) is injective, and the function \( g : [0, \infty) \to [0, \infty) \) defined by \( g(x) = x^2 \) is bijective (thus invertible).

Lists

Recall from *The Joy of Sets* that sets do not care about order or repetition; for instance, \( \{N, A, S, A\} = \{N, S, A\} = \{S, A, N, S\} \). If we want

---

\(^*\) Note that composition is read backwards: “\( g \circ f \)” means first apply \( f \), then apply \( g \). If we wrote \((x)f\), then we could compose functions the same way we read: from left to right. (Try it!)

The terms injective and surjective have synonyms\(^3\) that you might have heard of: namely, one-to-one and onto, respectively.

A function \( f : \mathbb{R} \to \mathbb{R} \) is injective if and only if every horizontal line meets the graph of \( f \) at most once, and surjective if and only if every horizontal line meets the graph of \( f \) at least once.

Try proving that \( f : X \to Y \) is injective if and only if there is \( g : Y \to X \) such that \( g \circ f = \text{id}_Y \) and surjective if and only if there is \( g : Y \to X \) such that \( f \circ g = \text{id}_Y \).

While you’re at it, also prove this: for any functions \( f : X \to Y \) and \( g : Y \to Z \),

1. If \( f \) and \( g \) are injective, so is \( g \circ f \);
2. If \( f \) and \( g \) are surjective, so is \( g \circ f \);
3. If \( f \) and \( g \) are bijective, so is \( g \circ f \);
4. If \( g \circ f \) is injective, then so is \( f \);
5. If \( g \circ f \) is surjective, then so is \( g \).

For any function \( f : X \to Y \), the function \( g : X \to \text{im}(f) \) defined by \( g(x) = f(x) \) for all \( x \in X \) is surjective, which shows that any function can be converted into a surjective one simply by shrinking its codomain.
to distinguish between NASA, the NSA, and a useful bit of Latin, we will need to use finite ordered lists rather than sets.

As in our notation for sets, we can name a list by writing out its elements separated by commas, but in order to distinguish lists from sets we will enclose the elements between parentheses rather than between braces. The crucial difference between lists and finite sets is that order and repetition do matter for lists. So, for instance,

\[(N, A, S, A) \neq (N, A, S) \quad \text{and} \quad (N, A, S) \neq (N, S, A).\]

The length of a list is the number of elements in it. It is often convenient to index the elements of a list of length \(n\) using the natural numbers from 1 to \(n\). That is, we might write

\[L = (x_1, \ldots, x_n) \quad \text{or} \quad L = (x_k : 1 \leq k \leq n)\]

if \(L\) is a list of length \(n\) whose \(k\)th element is \(x_k\). Two lists are equal if they have the same length and the same elements, in the same order.

**Cartesian Products**

Of special importance are lists of length two, which are called ordered pairs. In the past you have probably used ordered pairs \((a, b)\) of real numbers to represent points in the Cartesian plane. More generally, for any sets \(X\) and \(Y\), the Cartesian product of \(X\) and \(Y\) is the set

\[X \times Y := \{(x, y) : x \in X \text{ and } y \in Y\}\]

consisting of all ordered pairs whose first element belongs to \(X\) and whose second element belongs to \(Y\).

More generally still, we can form the Cartesian product of any finite list of sets \((X_1, \ldots, X_n)\), namely

\[X_1 \times \cdots \times X_n := \{(x_1, \ldots, x_n) : x_k \in X_k \text{ for each } 1 \leq k \leq n\}.\]

As you might guess, we can also use exponential shorthand for repeated products: e.g., \(X \times X = X^2\), \(Y \times Y \times Y = Y^3\), etc. Thus

\[\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(a, b) : a \in \mathbb{R} \text{ and } b \in \mathbb{R}\},\]

and, in general, \(\mathbb{R}^n\) is the set of all \(n\)-tuples of real numbers.

**The Graph of a Function**

In calculus, one of the best ways to get a visual representation of a function is to draw its graph. For instance, consider the exponential function \(\exp : \mathbb{R} \to \mathbb{R}\) defined by \(\exp(x) = e^x\) for all \(x \in \mathbb{R}\). Its graph is a certain subset of \(\mathbb{R}^2\), namely

\[\text{graph}(\exp) = \{(x, y) \in \mathbb{R}^2 : e^x = y\} \subseteq \mathbb{R}^2.\]

For us, a list is by definition a finite ordered set. Of course, infinite sets can be ordered as well, and an infinite ordered set that is ordered like \(\mathbb{N}\) is called a sequence.

Thus \((N, A, S, A)\) is a list, while \(\{N, A, S, A\}\) is a set.

In linear algebra, bases are sets but finite ordered bases are lists. And sometimes we really do need to use ordered bases, such as when we define coordinate vectors.

Lists of length \(n\) are often called \(n\)-tuples, particularly when their elements are numbers.

Repetition is allowed in lists: \((1, 1, 1) \neq (1, 1)\), since these lists do not even have the same length.

You are familiar with the summation symbol, which is the capital Greek letter sigma: \(\Sigma\). The corresponding symbol for products is a capital pi: \(\prod\). So we might write \(X_1 \times \cdots \times X_n = \prod_{k=1}^{n} X_k\).

In linear algebra, we often refer to the \(n\)-tuples in \(\mathbb{R}^n\) as vectors. This is because the Cartesian product \(\mathbb{R}^n\) becomes a vector space once we introduce the addition and scalar multiplication operations on it, so it is natural to think of its elements as vectors. There is no contradiction in \(\mathbb{R}^n\) being both a Cartesian product and a vector space, or in \(\mathbb{R}\) being both an \(n\)-tuple and a vector. It’s a bit like the fact that you are both a leader and the best.

**Figure 4:** The graph of the exponential function \(y = e^x\).
Now that we have defined Cartesian products in general, there is nothing to stop us from doing this with any function. That is, for any function \( f : X \rightarrow Y \), we define the graph of \( f \) to be the set
\[
\text{graph}(f) := \{(x, y) \in X \times Y : f(x) = y\} \subseteq X \times Y.
\]

**Rigorous Definition of Function**

Earlier we defined a function to be a “rule,” and informally this can be a useful way to think about functions, but it has some serious drawbacks that make it untenable as an official definition. Chief among them: what is a rule? “Rule” is not a precise mathematical notion. Furthermore, consider the functions \( f, g : \mathbb{R} \rightarrow \mathbb{R} \) defined by
\[
f(x) = \sqrt{x^2} \quad \text{and} \quad g(x) = \begin{cases} -x & \text{if } x < 0; \\ x & \text{if } x \geq 0. \end{cases}
\]

The functions \( f \) and \( g \) are defined by different rules, but we are inclined to say that they are the same function. This is because they have the same domain and codomain and their values agree on every input. In other words, they have the same graph.

In fact, the graph of a function encodes all the information we need to know about it, and is already a well-defined mathematical object. So we elect to bypass the idea of a “rule” altogether and just define a function to be its graph.

**Definition.** A function \( f \) from \( X \) to \( Y \) is a subset \( f \subseteq X \times Y \) with the property that for every element \( x \in X \) there is exactly one element \( y \in Y \) such that \((x, y) \in f\).

Of course, “\((x, y) \in f\)” is a bit of set-theoretic folderol that will never appear again outside this definition, since it just means “\( y = f(x) \).”

**Sets All the Way Down**

One of the goals — and one of the great achievements — of set theory is to represent literally every mathematical object as a set. In defining a function to be its graph, which is a set of ordered pairs, we have reduced the notion of function to that of ordered pair. This is enough to satisfy everyone but the set theorists, and now to satisfy them as well we show how to represent ordered pairs as sets. Given elements \( x \) and \( y \), define the ordered pair \((x, y)\) to be the set
\[
(x, y) := \{\{x\}, \{x, y\}\}.
\]
Then for all \( a, b, c, d \) we have \((a, b) = (c, d)\) if and only if \( a = c \) and \( b = d \), which is all we ever needed from ordered pairs to begin with. There — now everything is a set.

When \( X \) and \( Y \) are arbitrary sets, we cannot really “draw” the graph of a function \( f : X \rightarrow Y \) the way we would for a function from \( \mathbb{R} \) to \( \mathbb{R} \), but the set of points \((x, y) \in X \times Y \) such that \( f(x) = y \) still makes good sense as a set.

“In mathematics rigor is not everything, but without it there is nothing.” – Henri Poincaré

“Everything is vague to a degree you do not realize till you have tried to make it precise.” – Bertrand Russell

For instance, does the rule \( f(n) = \) the least natural number that cannot be described in fewer than \( n \) words” define a function? If so, what is \( f(14) \)?

7 Thanks, Bourbaki! (Essentially all mathematical objects can be represented as sets. To get a feel for how this is done, take Math 582.)
Some Suggestions for Further Reading


Index

$C^{0}(\mathbb{R})$, 24
$n$ choose $k$, 34
absolute value, 12, 18
additive inverse, 31
Archimedean Property, 17
bijective, 20
bounded above, 25
Cartesian Product, 9
casework, 33
codomain, 11
complete the square, 32
composite, 15
composition, 12
comprehension notation, 9
contrapositive, 39
converge, 26
dense, 17
Diophantine equation, 14
divides, 13, 18
divisible, 13
domain, 11
equal, 10
even, 5
equation and uniqueness, 31
existential quantifier, 13
Extreme Value Theorem, 17
factor, 13
factorial, 22
Fermat’s Last Theorem, 41
for all, 15
for every, 15
function, 11
Fundamental Theorem of Calculus, 24
if and only if, 10, 39
image, 27
induced set function, 27
injective, 19
integers, 9
Intermediate Value Theorem, 20
inverse function, 20
inverse image, 27
invertible, 20
invertible matrix, 22
irrational number, 12
linear, 20
linearly independent, 18, 22
maximum, 35
Mean Value Theorem, 31
minimum, 35
multiplicative inverse, 32
natural numbers, 9
nonzero function, 14
odd, 5
one-to-one, 19
onto, 20
piece-wise, 11
power set, 27
prime, 13
prime factorization, 26
rational numbers, 9
real numbers, 9
Rolle’s Theorem, 42
root, 14
sequence, 26
set builder notation, 9
Sophie Germain prime, 16
source, 11
span, 26
subset, 10
subspace, 38
surjective, 20
target, 11
there exists, 13
there is, 13
uniqueness, 31
universal quantifier, 15
upper triangular, 16
verseira, 19
zero function, 14