Demonstration

Proof Beyond the Possibility of Doubt

DECEMBER 27, 2022

U(M) Mathematics

Please send corrections and comments to the Undergraduate Program Director at `math-updir@umich.edu`.

Contents

Introduction

The worksheets in this document were created to help University of Michigan students transition into mathematics courses that are more writing intensive.[1] 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 has shown that the most important quality a student needs in order to succeed is intellectual curiosity.[2]

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.[3]

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.

[1] "One doesn't really understand what mathematics is until at least halfway through college when one takes abstract math courses and learns about proofs."
–Karen Uhlenbeck '64

[2] 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.

[3] See, for example, how the authors of the works listed in *Some Suggestions for Further Reading* on page 67 describe why their books were written.

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 $2k$ for some integer k. So, for example, 42 is even because $42 = 2 \cdot 21$. An integer is *odd* provided that it can be written as one more than an even integer; that is, as $2\ell + 1$ for some integer ℓ. Thus, $-61 = 2 \cdot (-31) + 1$ is odd. Since zero can be written as $2 \cdot 0$, zero is even.

In many other languages, the words for even and odd are much more natural: *pair* and *impair* in French; *par* and *impar* in Spanish; *gerade* and *ungerade* in German; *pari* and *dispari* in Italian; ...

The second result students need to know is that the positive square root[4] 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. You may have learned that a rational number is a number whose decimal expansion terminates or repeats—this is equivalent[5] to saying it can be written as a ratio c/d of integers

[4] We say $\star$ is a *square root* of $\leftmoon$ provided that $\star^2 = \leftmoon$.

never divide by zero.

[5] You will establish this equivalency in Exercise 18.10 on page 46.

with $d \neq 0$. The fact that $\sqrt{2}$ is not rational needs to be demonstrated,[6] and there are at least nineteen known distinct proofs. Here is a proof that is very similar to the one that may be found in later versions of Euclid's *Elements* (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 and 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 and 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.

[6] "In the course of my law-reading I constantly came upon the word demonstrate. I thought, at first, that I understood its meaning, but soon became satisfied that I did not. I said to myself, 'What do I do when I demonstrate more than when I reason or prove? How does demonstration differ from any other proof?' I consulted Webster's Dictionary. That told of 'certain proof,' 'proof beyond the possibility of doubt;' but I could form no idea what sort of proof that was. I thought a great many things were proved beyond a possibility of doubt, without recourse to any such extraordinary process of reasoning as I understood 'demonstration' to be. I consulted all the dictionaries and books of reference I could find, but with no better results. You might as well have defined blue to a blind man. At last I said, 'LINCOLN, you can never make a lawyer if you do not understand what demonstrate means;' and I left my situation in Springfield, went home to my father's house, and staid there till I could give any propositions in the six books of Euclid at sight. I then found out what 'demonstrate' means, and went back to my law studies." – Abraham Lincoln, quoted in *Mr. Lincoln's Early Life; HOW HE EDUCATED HIMSELF*, The New York Times, September 4, 1864.

How these worksheets are intended to be used.

Around 2009 we noticed that more and more students were arriving at U(M) without having seen basic set theory and predicate logic. The handouts *Joy of Sets* and *Mathematical Hygiene*, both of which appear in the *Resources* part 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 worked in groups of four to six under the guidance of experienced students 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. In 2020 the handouts *More Joy of Sets* and *Complex Numbers*, were created in response to student suggestions. Feedback is most welcome! Please send your suggestions to `math-updir@umich.edu`.

The current form of these worksheets assumes that you will be working collaboratively[7] 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.

[7] Both (i) explaining your own reasoning to others and (ii) listening to the explanations of your peers provide mechanisms for you to share ideas, clarify differences, construct new understandings, and learn new problem solving skills. Studies consistently show that collaborative work results in improved persistence, increased retention, enhanced teamwork skills, better communication skills, higher future individual achievement, greater knowledge acquisition, ... Of course, the key word here is *collaborative*; you need to both listen and contribute.

Fundamentals

Set Theory

Set Theory lies at the heart of all things mathematical, so take some time to review the fundamentals.[8] In this worksheet you will work with some of the basic concepts: intersections, unions, complements, and set-builder notation.[9] 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" = $\{1, 2, \dots\}$.

$\mathbb{Z}$ = the set of integers = $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

$\mathbb{Q}$ = the set of rational numbers (fractions) = $\{c/d \mid c \in \mathbb{Z}, d \in \mathbb{N}\}$.

$\mathbb{R}$ = the set of real numbers. Often represented via the number line.

$\mathbb{C}$ = the set of complex numbers = $\{a + bi \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}$.

[8] See, for example, *The Joy of Sets* on page 49.

[9] Also called *comprehension notation*.

warning. Some people include 0 in the set of natural numbers; we do not.

When you are struggling to internalize a new mathematical idea, know that your struggle is natural and take some comfort from history. For example, while the use of zero as a placeholder can be traced back at least five thousand years to the Sumerians of ancient Mesopotamia, its first documented use as a number had to wait until the work of Brahmagupta in 628 AD. Similarly, while negative numbers were introduced around 200 BC in China and appear in Indian mathematics beginning around 600 AD, many mathematicians, especially in Europe, rejected the existence of negative numbers until well into the nineteenth century!

Exercises

1.1 Let's 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."

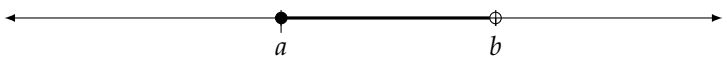
(a) $\{n \in \mathbb{Z} \mid n^2 > 5\}$.

(b) $\{n \in \mathbb{Z} \mid n = 2k + 1 \text{ for some } k \in \mathbb{Z}\}$

(c) $\{(x, y) \mid x, y \in S\}$, where S is a set.[10]

(d) $\{(x, y) \in \mathbb{R}^2 \mid x^2 = y\}$.

1.2 Fix $a, b \in \mathbb{R}$ with $a < b$. Write the interval $[a, b)$ in set-builder notation. (Why require $a < b$?)



1.3 Suppose $J = \{\star, \wr\}$ and $K = \{a, b, c\}$. Express $J \times K$ in set-builder notation.

[10] 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_1, 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. See page 59 for more on Cartesian products.

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

Set differences, e.g. $[0,1] \setminus \mathbb{Q}$, are discussed in Definition 6 on page 52.

When is one set a subset of another? For two sets A and B, we say A is a *subset* of B, abbreviated $A \subset B$ or $A \subseteq B$, provided that every element of A is an element of B. This is equivalent to saying $x \in A \Rightarrow x \in B$.

1.5 Suppose $\Xi = \{61, \{61\}\}$. Which of the following statements are true? Explain your answers.

- $61 \in \Xi$.
- $\{61\} \in \Xi$.
- $61 \subset \Xi$.
- $\{61\} \subset \Xi$.

In Exercise 1.5 the number 61 is to be treated as an object, not as a set.

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 $\mathbb{Z} \subseteq \mathbb{Q}$."

[11] Many students find that the remaining exercises on this worksheet are challenging. Don't panic; you can do this. Follow the proof templates to the left and below, use the many hints provided in the margin, and write in complete sentences.

1.6 Suppose L, M, N, and O are sets with $M \subset N$. Show[11] that if $L \subset M$, then $L \subset N$. If $O \subset N$, then is it true that $O \subset M$?

To show $P \subset K$, follow these steps:
(a) Let $p \in P$ be arbitrary.
(b) Use the properties of P to say something about p.
(c) Use what you learned in (b) to show p satisfies the properties of K.
(d) Conclude $p \in K$, but because p was arbitrary in P, $P \subset K$.

1.7 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 $C \subset D \cap E$.

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!

When people say "P if and only if Q" they mean "P is true exactly when Q is true". This is equivalent to saying "P implies Q and Q implies P". The latter interpretation is often the more useful.

1.8 Suppose X is a set and $I, J \subset X$. Show that $J \setminus I = J \cap I^c$.

Set complements, e.g. I^c, are discussed in Definition 7 on page 52.

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

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

Hint: given the pair $(x,y) \in \mathbb{R}^2$, let $a = -5x + 3y$ and $b = 2x - y$.

1.11 Let $B = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1\}$ and let $C = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$. Determine what $C \cup B$ is and prove it.

Do not be afraid to name things. For example, in Exercise 1.11 you may want to let D denote the unit disk centered at the origin in $\mathbb{R}^2$. This makes it easier to see that your job is to show $D = B \cup C$.

1.12 (*Review.*) True or False. Zero is an even number. Justify your answer.

"There is no math without courage."
–BR, 2017

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* $f\colon S \to T$ (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 $f(s) \in T$ is paired with a given $s \in S$.

A function $f\colon S \to T$ 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 requirement on a function is the equivalent of the vertical line test that you may have learned about in high school.

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

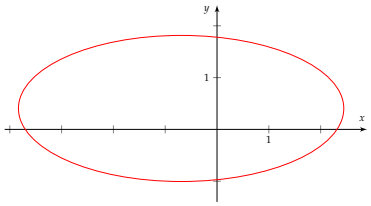


Figure 1: In red is a graph of pairs (x, y) satisfying

$$2(x + \ln(2))^2 + \pi^2(y - 23/57)^2 = 2\pi^2.$$

The rule that assigns $\dot{y} \in \mathbb{R}$ to $\dot{x} \in \mathbb{R}$ provided that $(\dot{x}, \dot{y})$ is on the red graph fails to define a function from $\mathbb{R}$ to $\mathbb{R}$.

For more on functions see *More Joy of Sets* on page 57.

Exercises

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

A discussion of the relationship between graphs and functions begins at the bottom of page 59.

2.2 Suppose S and T are sets. Describe all of the functions from S to T when (a) $|S| = |T| = 1$; (b) $|S| = 2$ and $|T| = 3$; and (c) $|S| = n$ and $|T| = m$ where $n, m \in \mathbb{N}$.

WE CAN BUILD FUNCTIONS using piece-wise notation. For example, consider the function $f\colon \mathbb{R} \to \mathbb{R}$ 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 $x < 0$.

Make sure you understand why this is actually a function; ask an experienced student of mathematics if you have any doubts.

2.3 Sketch a graph of $f\colon \mathbb{R} \to \mathbb{R}$ given by

$$f(x) = \begin{cases} x + 1 & \text{if } x \geq 0; \\ -x^2 - 2 & \text{if } x < 0. \end{cases}$$

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

2.4 Which of the following proposed functions actually defines a function? If it is not a function, explain why it isn't.

(a) $f\colon \mathbb{R} \to \mathbb{R}$ given by $f(x) = \begin{cases} x^2+1 & \text{if } x \geq 0; \\ x-1 & \text{if } x \leq 0. \end{cases}$

(b) $f\colon \mathbb{R} \to \mathbb{R}$ given by $f(x) = \begin{cases} x^2+x-4 & \text{if } x \geq 1; \\ x-3 & \text{if } x \leq 1. \end{cases}$

(c) $f\colon \mathbb{R} \to \mathbb{R}$ given by $f(x) = \begin{cases} 0 & \text{if } x \in \mathbb{Q}; \\ 1 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$

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

(d) $f\colon \mathbb{N} \to \mathbb{Q}$ given by $f(x) = \sqrt{x}$.

2.5 Let A be a set, and suppose you are given two functions $f\colon A \to \mathbb{R}$, $g\colon A \to \mathbb{R}$. Provide *brief* justifications for your answers.

(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) What if we send $a \in A$ to $(f+g)(a) = f(a) + g(a)$?

(c) Does sending $a \in A$ to $(f/g)(a) = f(a)/g(a)$ define a function?

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

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.

2.6 Rewrite the composition $f \circ g\colon \mathbb{R} \to \mathbb{R}$ of $f\colon \mathbb{R} \to \mathbb{R}$ and $g\colon \mathbb{R} \to \mathbb{R}$ as a polynomial or a simple piece-wise function.

(a) $g(x) = 2x+3$ and $f(x) = x^2 + 5x + 1$.

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

(b) $g(x) = 3$ and $f(x) = x + 5$.

(c) $g(x) = x^2$ and $f(x) = \sqrt{|x|}$.

The *absolute value* function $|\ |\colon \mathbb{R} \to \mathbb{R}$ is defined by

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

for $x \in \mathbb{R}$.

(d) $g(x) = \begin{cases} -1 & \text{if } x \in \mathbb{Q} \\ 1 & \text{if } x \in \mathbb{R} \setminus \mathbb{Q} \end{cases}$ and $f(x) = x^2$.

2.7 Let $X = \mathbb{R} \setminus \{0, 1\}$. The following functions have X as both their domain and codomain: $\mathrm{Id}_X(x) = x$, $f_1(y) = 1/(1-y)$, $f_2(z) = 1 - 1/z$, $g_1(u) = 1/u$, $g_2(v) = 1 - v$, and $g_3(w) = w/(w-1)$.

For a set S the *identity function on* S, denoted $\mathrm{Id}_S\colon S \to S$, is defined by $\mathrm{Id}_S(s) = s$ for all $s \in S$.

(a) Show[12] that $g_1 \circ g_1 = g_2 \circ g_2 = g_3 \circ g_3 = \mathrm{Id}_X$

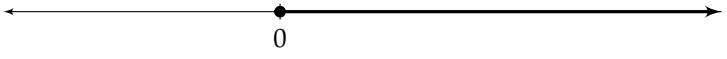
(b) Show that $f_1 \circ f_2 = f_2 \circ f_1 = \mathrm{Id}_X$.

(c) Show[13] that $g_1 \circ g_2 = f_1$, $g_2 \circ g_1 = f_2$, and $f_1 \neq f_2$.

[12] Two functions $f\colon S \to T$ and $\tilde{f}\colon \tilde{S} \to \tilde{T}$ are said to be equal provided that: (a) $S = \tilde{S}$; (b) $T = \tilde{T}$; and (c) $f(s) = \tilde{f}(s)$ for all $s \in S$.

[13] Since $f_1 \neq f_2$, this shows that function composition is not *commutative*. In Exercise 4.10 on page 16 you will show that function composition is associative.

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



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.

Because the symbol $\exists$ is often followed by a predicate clause, in practice the string of symbols "$\exists x$" translates into English as "there exists x such that".

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 $f\colon \mathbb{R} \to \mathbb{R}$ such that $f'' + 9f = 0$ might go something like this:

> Let $g(t) = \sin(3t + 5)$. Since
>
> $$\begin{aligned} g''(t) + 9g(t) &= -9\sin(3t+5) + 9\sin(3t+5) \\ &= 0, \end{aligned}$$
>
> a function satisfying the differential equation $f'' + 9f = 0$ exists.

Exercises

3.1 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[14] by 8.

[14] 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.

3.2 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.[15]

[15] A natural number p is said to be *prime* provided that it has exactly two distinct positive integer factors.

(d) $\exists \ell \in \mathbb{N}$ such that $\ell^2 - 5\ell + 6 = 0$.

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

3.3 Rephrase the statement "$x^2 - 2x - 3$ has a real root" using the quantifier $\exists$.

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

3.4 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 $(\pm 1, 0)$).

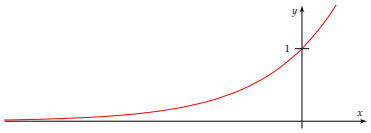
Hint: What's your favorite Pythagorean triple?

3.5 Suppose A is a set and $\ell \colon A \to \mathbb{R}$ is a function. Use the quantifier $\exists$ to define what it means for ℓ to be a nonzero function.[16]

[16] The *zero function* from A to $\mathbb{R}$ is the function that sends every element of A to 0. A *nonzero function* from A to $\mathbb{R}$ is any function that is not the zero function.

3.6 Prove your answer to question 3.3.

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



3.8 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.[17]

[17] 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 non-trivial solution other than $x = \pm 3$ and $y = \pm 2$. (Here the trivial solutions are $x = \pm 1$ and $y = 0$.)

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

3.9 (*Review.*) Show that $A = \{t(1, 0, -1) \in \mathbb{R}^3 \mid t \in \mathbb{R}\}$ is a subset of $B = \{r(1, 1, 1) + s(3, 2, 1) \in \mathbb{R}^3 \mid r, s \in \mathbb{R}\}$.

Hint: Given $(t, 0, -t) = t(1, 0, -1)$ in A, in order to show that it belongs to B try letting $r = -2t$ and $s = t$.

3.10 Use the quantifier $\exists$ to describe what it means for a set, let's call it H, to have at least three elements.

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

> 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 4.4 below, you need to first state something like "Fix a prime number p." and work from there.

4.1 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.

4.2 Rephrase the statement "$p + 7$ is composite[18] for any prime p" using the quantifier $\forall$.

[18] A natural number is called *composite* provided that (a) it is not one and (b) it is not prime.

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

(a) Every prime number is a Sophie Germain prime.[19]

(b) $\forall n \in \mathbb{Z}$, $n^2 \geq 0$.

(c) $\forall$ sets S, S has a finite number of elements.

(d) Every integer divides zero.

(e) $\forall x \in \mathbb{R}$, x has a real square root.

(f) $\forall a, b \in \mathbb{Z}$, $\frac{a}{b}$ is in $\mathbb{Q}$.

[19] 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: See sidenote 14.

NEVER divide by zero.

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

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

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

4.6 Rephrase the statement

> A^2 is upper triangular for any upper triangular 2×2 matrix A

using the quantifier $\forall$.

A two-by-two upper triangular matrix with entries in $\mathbb{R}$ looks like

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

with $a, b, d \in \mathbb{R}$.

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

4.8 True or False.

(a) For every negative natural number n we have that n is irrational.

(b) Every real solution to the equation $x^2 + 1 = 0$ is blue.

These are examples of *vacuous truths*.

4.9 (*Review*.) True or False. The positive square root of 2 is a rational number. Justify your answer.

4.10 (*Review*.) Show that function composition is *associative* . That is, if A, B, C, and D are sets and $f\colon A \to B$, $g\colon B \to C$, and $h\colon C \to D$ are functions, then show

$$h \circ (g \circ f)\colon A \to D \text{ is equal to } (h \circ g) \circ f\colon A \to D.$$

Hint: Two functions $\ell, m\colon A \to D$ are equal provided that $\ell(a) = m(a)$ for all $a \in A$.

4.11 (*Review*.) Suppose $A = \{6m \mid m \in \mathbb{Z}\}$, $B = \{15n \mid n \in \mathbb{Z}\}$, and $C = \{30\ell \mid \ell \in \mathbb{Z}\}$. Show that $A \cap B = C$.

Combining Quantifiers

Combining existential and universal quantifiers provides a way for us to form more complicated mathematical statements. For example, the Extreme Value Theorem[20] states that if $f\colon [a,b] \to \mathbb{R}$ 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[21] 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 $A \subset X$ such that for every set $B \subset X$ we have $A \cup B = B$ might go like this: "Let $A = \emptyset$. Fix $B \subset X$. 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 $A \subset X$ there is $B \subset X$ such that $X = A \cup B$ and $\emptyset = A \cap B$ might go something like this: "Fix $A \subset X$. Let $B = X \setminus A$. Note that $A \cup B = A \cup (X \setminus A) = X$ and $A \cap B = A \cap (X \setminus A) = \emptyset$."

[20] You are probably more familiar with this version: If $f\colon [a,b] \to \mathbb{R}$ is continuous, then f has both a maximum and a minimum on $[a,b]$.

[21] As with many things in mathematics, this result is probably named after the wrong person; Archimedes himself credited it to Eudoxus of Cnidus.

The mathematical statement $\exists y \forall x$ means that you present the reader of the proof with a y before they give you an x. Because the reader chooses x after you present them a y, the y you present **cannot** depend on x.

The mathematical statement $\forall x \exists y$ means that the reader of the proof hands you an x before you hand them a y. Because the x is presented to you before you choose y, your choice of y **can** depend on x.

Exercises

Remember the tips from the previous worksheets, especially from the *Universal Quantifiers* worksheet on page 15.

5.1 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 $0 < q < p$.

$\mathbb{R}_{>0} := \{s \in \mathbb{R} \mid s > 0\}$.

Recall that the *absolute value* function $|\ | : \mathbb{R} \to \mathbb{R}$ is defined by

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

for $x \in \mathbb{R}$.

$\mathbb{Q}_{>0} := \{r \in \mathbb{Q} \mid r > 0\}$.

5.2 Rephrase the statement "every positive real number has a square root" using quantifiers.

5.3 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 2π).

Hint: Don't be afraid to name things.

5.4 Prove that $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x^2 y + 2x = x$.

NEVER divide by zero.

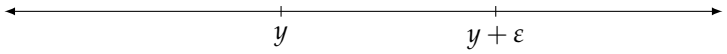
5.5 Prove that there is $n \in \mathbb{Z}$ such that for all $m \in \mathbb{Z}$, n divides m.

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

5.6 Provide a proof of Exercise 5.1g.

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

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



5.8 (*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.

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 $a = b = 0$.

5.9 (*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

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

5.10 (*Bonus*.) Provide a proof[22] of Exercise 5.1d.

[22] A rigorous proof will probably involve induction (see page 43).

5.11 (*Review*.) Show: $\{2n \mid n \in \mathbb{Z}\} = \{6a + 10b \mid a, b \in \mathbb{Z}\}$.

5.12 (*Review*.) In Exercise 2.7 on page 12 we introduced the functions $\mathrm{Id}_X(x) = x$, $f_1(y) = 1/(1-y)$, $f_2(z) = 1 - 1/z$, $g_1(u) = 1/u$, $g_2(v) = 1 - v$, and $g_3(w) = w/(w-1)$ all of which have domain and codomain $X = \mathbb{R} \setminus \{0, 1\}$.

(a) Show that $f_1 \circ f_1 = f_2$ and $f_2 \circ f_2 = f_1$.

(b) Since function composition is associative, both $f_1 \circ f_1 \circ f_1$ and $f_2 \circ f_2 \circ f_2$ make sense. Compute them.

The set of functions

$$G = \{\mathrm{Id}_X, f_1, f_2, g_1, g_2, g_3\}$$

is an example of a (noncommutative) group under function composition. You can can learn more about groups in Math 312, 412, or 493.

Functions (part two)

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 $f\colon S \to T$ 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.

If $g\colon A \to B$ is injective, some people will write

$$g\colon A \hookrightarrow B.$$

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 $f\colon \mathbb{N} \to \mathbb{N}$ 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

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

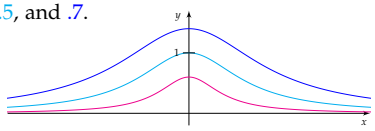
6.2 Fix $a \in \mathbb{R}_{>0}$. Prove that the function $w\colon \mathbb{R} \to \mathbb{R}^2$ given by $w(s) = (2as, 2a/(1 + s^2))$ is injective. Due to mistranslation, the curve described by w is often called the *Witch of Agnesi*.[23]

6.3 Prove that the function $d\colon \mathbb{Z} \to \mathbb{Z}$ given by $d(x) = 2x$ is injective.

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

6.5 (*Bonus.*) Prove that the function $j\colon \mathbb{Q}_{>0} \to \mathbb{N}$ given by $j(q) = 2^m 3^n$, where m, n are positive and $q = m/n$ in lowest terms[24], is injective.

[23] In 1748 Maria Gaetana Agnesi studied this curve, which she called *versiera*, in *Instituzioni analitiche ad uso della gioventù italiana*, the first textbook to cover both differential and integral calculus. Below are graphs of *versiera* for a equal to .3, .5, and .7.



[24] We say $q = m/n$ is in *lowest terms* provided that the only natural number that divides both m and n is 1.

Hint: No integer can be both odd and even. Also, by convention $\forall ☺$, $☺^0 = 1$.

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 $g\colon A \to B$ 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.

If $g\colon A \to B$ is surjective, some people will write

$$g\colon A \twoheadrightarrow B.$$

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 $f\colon \mathbb{R} \to \mathbb{R}$ 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[25] there is a $c \in [a, b] \subset \mathbb{R}$ for which $f(c) = t$."

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

–NB, 2018

Q: What did the citizens of the castle say as Sir Jective left the castle?
A: Bye, Jective.

–HB, 2020

[25] The Intermediate Value Theorem says that if $h\colon [a, b] \to \mathbb{R}$ is continuous and $d \in \mathbb{R}$ is between $h(a)$ and $h(b)$, then there exists $c \in [a, b]$ for which $h(c) = d$.

Exercises

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

6.7 Prove[26] that the function $\ell\colon \mathbb{R} \to \mathbb{R}$ defined by $\ell(x) = |x|$ is not surjective.

[26] Remember to write in complete sentences.

6.8 Prove that the function $g\colon \mathbb{Q} \to \mathbb{N}$ give by $g(q) = n$, where n is positive and $q = m/n$ in lowest terms[27], is surjective.

[27] By convention we represent 0 in lowest terms by $0/1$.

6.9 (*Bonus*.) Prove that any **nonzero** linear[28] transformation $f\colon \mathbb{R}^{61} \to \mathbb{R}$ is surjective. Is it necessary to assume f is nonzero?

[28] A function $g\colon \mathbb{R}^{61} \to \mathbb{R}$ is said to be linear provided that

- $g(\vec{x} + \vec{y}) = g(\vec{x}) + g(\vec{y})$ for all $\vec{x}, \vec{y} \in \mathbb{R}^{61}$ and
- $g(c\vec{x}) = cg(\vec{x})$ for all $c \in \mathbb{R}$ and $\vec{x} \in \mathbb{R}^{61}$.

6.10 (*Bonus*.) Use the Intermediate Value Theorem to show that if $f\colon \mathbb{R} \to \mathbb{R}$ is continuous, $\lim_{\bowtie\to\infty} f(\bowtie) = \infty$ and $\lim_{\star\to-\infty} f(\star) = -\infty$, 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.[29]

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

Exercises

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

Hint: If $(a, b) = (x + 2ky, 3x + y)$, then $x = \frac{a-2bk}{1-6k}$ and $y = \frac{b-3a}{1-6k}$. Also $1/6 \notin \mathbb{Z}$.

6.12 Prove that the function $g\colon \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$ is bijective. (Taking cube roots is not allowed until after this result is proved.)

Hint: You may assume $a^2 + ab + b^2 = 0$ if and only if $a = b = 0$; this will be proved in Exercise 12.5 of the *Casework* worksheet (see page 33). Also, thanks to the Intermediate Value Theorem (see Exercise 6.10 above), if $f\colon \mathbb{R} \to \mathbb{R}$ is continuous and $\lim_{\bowtie\to\infty} f(\bowtie) = \infty$ while $\lim_{\star\to-\infty} f(\star) = -\infty$, then for all $t \in \mathbb{R}$ there exists $s \in \mathbb{R}$ such that $f(s) = t$.

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.[30]

nb: the words "such that" are paired with the words "there exists".

[30] See, for example, *Mathematical Hygiene* on page 53.

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

7.1 Negate the following statements.

In order to negate a statement, you do not need to know the technical meaning of the words in the statement.

(a) All primes are odd.

(b) Every subgroup of S_5 is a normal subgroup of S_5.

To learn about groups, subgroups, and normal subgroups, please take Math 312, 412, or 493.

(c) $\forall x \in \mathbb{R}$, $x^2 = 1$.

(d) $\forall x \in \mathbb{R}$, $x^2 < 0$.

7.2 Which of the following statements are true? If a statement is false, negate it and prove[31] the negated version.

[31] Remember to write in complete sentences.

(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.

The notation $n!$ is read as "n factorial," and it is shorthand for the product $1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$. So, for example, 4! is 24.

Every odd number greater than 5 is the sum of three primes. This was proved in 2013 by Harald Helfgott. Goldbach's conjecture remains open.

7.3 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.

7.4 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.

7.5 (*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.

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 $a = b = 0$.

7.6 (*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.

A two-by-two matrix A with real entries is said to be *invertible* provided that there exists a two-by-two matrix B with real entries such that $AB = BA = \mathrm{Id}_2$. Here Id_2 is the two-by-two matrix $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.

7.7 (*Review.*) Decide whether each of the following functions is injective, surjective, and/or bijective. Justify your answers.

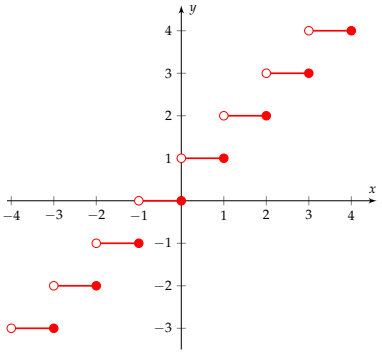
(a) $s \colon \mathbb{N} \to \mathbb{Z}$ defined by $s(n) = n^2$.

(b) The ceiling function $\lceil \cdot \rceil \colon \mathbb{R} \to \mathbb{Z}$.

(c) (*Bonus*) $t \colon \mathbb{N} \to \mathbb{Z}$ defined by

$$t(n) = \begin{cases} n/2 - 1 & \text{if } n \text{ is even} \\ -(n+1)/2 & \text{if } n \text{ is odd} \end{cases}$$

For $r \in \mathbb{R}$ we define $\lceil r \rceil := n$ where $n \in \mathbb{Z}$ and $n - 1 < r \leq n$.



7.8 (*Review.*) Each of the following statements is either true or false. Prove the statements that are true.

(a) $\forall x \in \mathbb{R}$ and $\forall y \in \mathbb{R}$ $\exists z \in \mathbb{R}$ such that $x + y = z$.

(b) $\forall x \in \mathbb{R}$ $\exists z \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$ we have $x + y = z$.

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."

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?

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.

8.1 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) There is a Cauchy sequence in $\mathbb{R}$ that doesn't converge.

In order to negate a statement, you do not need to know the technical meaning of the words in the statement.

To learn about Cauchy sequences, please take Math 351 or 451.

(d) $\exists x \in \mathbb{Q}$ such that $x^2 + 4x + 2 = 0$.

(e) $\exists a, b, c \in \mathbb{N}$ such that $a^3 + b^3 = c^3$.

(f) Some days are better than today.

(g) Some triangles are scalene.[32]

[32] A triangle is said to be *scalene* provided that all three sides have different lengths.

8.2 Which of the following statements are true? If a statement is false, negate it and prove[33] the negated version.

[33] Remember to write in complete sentences.

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

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

8.3 Prove that there does not exist a positive real number x such that $x + 1/x < 2$.

Hint: Multiplication by positive real numbers preserves inequalities.

8.4 Consider the statement

> There exist irrational $\alpha, \beta \in \mathbb{R}$ such that α^β is rational.

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

Hint: Consider $\sqrt{2}$, $\sqrt{2}^{\sqrt{2}}$, and $2 = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$.

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

Hint: Calculus or Completing the Square work equally well.

8.6 Consider the statement

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

$C^0(\mathbb{R})$ denotes the set of continuous functions from $\mathbb{R}$ to $\mathbb{R}$.

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

Hint: The Fundamental Theorem of Calculus states:

(i) Suppose $f \colon [a, b] \to \mathbb{R}$ is continuous and $F \colon [a, b] \to \mathbb{R}$ is differentiable with $F' = f$. We have

$$\int_a^b f = F(b) - F(a).$$

(ii) Suppose $g \colon [a, b] \to \mathbb{R}$ is continuous. If $c \in (a, b)$, then $G \colon [a, b] \to \mathbb{R}$ defined by

$$G(x) = \int_a^x g$$

is differentiable at c and $G'(c) = g(c)$.

8.7 (*Bonus*.) Prove that there do not exist invertible $n \times n$ matrices A and B such that AB is not invertible.

8.8 (*Review*.) Each of the following statements is either true or false. Prove the statements that are true and find a counterexample for the statements that are false.

(a) $\forall x \in \mathbb{R}\ \exists z, y \in \mathbb{R}$ such that $x + y = z$.

(b) $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$ and $\forall z \in \mathbb{R}$ we have $x + y = z$.

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

9.1 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."

9.2 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 $g\colon \mathbb{R} \to \mathbb{R}$ we have $g' - f \neq 0$.

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

(f) For every continuous, strictly increasing function $g\colon \mathbb{R} \to \mathbb{R}$ there exists $c \in \mathbb{R}$ such that $g(c) = 0$.

9.3 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 $\mathbb{R}$.

9.4 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.

Hint: The Fundamental Theorem of Arithmetic states that every $n \in \mathbb{N}$ with $n > 1$ has a *prime factorization*:

$$n = p_1^{m_1} p_2^{m_2} \cdots p_\ell^{m_\ell}$$

where $p_1, p_2, \ldots, p_\ell$ are the (unique) prime factors of n and $m_j \in \mathbb{N}$ for $1 \leq j \leq n$. For example, the prime factorization of $9,009$ is $3^2 \cdot 7 \cdot 11 \cdot 13$.

9.5 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.

9.6 A sequence[34] (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 $|a_m - L| < \varepsilon$.

[34] A *sequence* is a function $b\colon \mathbb{N} \to \mathbb{R}$. By convention, we denote $b(n)$ by b_n and use the shorthand (b_n) to denote the function $b\colon \mathbb{N} \to \mathbb{R}$. So, for example, the function $c\colon \mathbb{N} \to \mathbb{R}$ given by $c(\ell) = 2^\ell$ has $c_6 = 64$ and $(c_n) = (2, 4, 8, 16, \ldots)$.

(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

$$(a_n) = \left(\frac{1}{n}\right) = \left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right)$$

converges to 0.

Hint: You may want to use the Archimedean Property.

(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 $1/2$.

9.7 (*Bonus.*) Show that the vectors $(1, 0, 1)$ and $(1, 2, -1)$ do not span[35] $\mathbb{R}^3$.

[35] A collection of vectors $\vec{v}_1, \ldots, \vec{v}_n$ in $\mathbb{R}^3$ *spans* $\mathbb{R}^3$ provided that for every $\vec{w} \in \mathbb{R}^3$ there exist coefficients $c_1, \ldots, c_n \in \mathbb{R}$ such that

$$\vec{w} = c_1\vec{v}_1 + \cdots + c_n\vec{v}_n.$$

9.8 (*Review.*) Each of the following statements is either true or false. Prove the statements that are true and provide counterexamples for the statements that are false.

(a) $\forall x \in \mathbb{N}\ \exists y \in \mathbb{R}$ such that $y^2 = x$.

(b) $\exists x \in \mathbb{N}$ such that $\forall y \in \mathbb{R}$ we have $y^2 = x$.

(c) $\forall n \in \mathbb{N}\ \exists m \in \mathbb{N}$ such that $m^n = 1$.

(d) $\exists n \in \mathbb{Z}$ such that $\forall m \in \mathbb{N}$ we have $m^n = 1$.

(e) For all injective functions $f\colon \mathbb{R} \to \mathbb{R}$ there exists a surjective function $g\colon \mathbb{R} \to \mathbb{R}$ such that $g \circ f = \mathrm{Id}_{\mathbb{R}}$.

The function $\mathrm{Id}_{\mathbb{R}}\colon \mathbb{R} \to \mathbb{R}$ is defined by $\mathrm{Id}_{\mathbb{R}}(x) = x$ for all $x \in \mathbb{R}$.

9.9 (*Review.*) There are many functions of the form $s\colon A \to B$ where $A, B \subset \mathbb{R}$ and $s(x) = x^2$. Find choices for A and B so that

Hint: You should also make sure that your choices for A and B make sense. For example, if $A = \mathbb{R}$, then B cannot be $(-\infty, 0)$.

(a) $s\colon A \to B$ is neither injective nor surjective.

(b) $s\colon A \to B$ is injective but not surjective.

(c) $s\colon A \to B$ is surjective but not injective.

(d) $s\colon A \to B$ is bijective.

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.[36]

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$
$$\mathcal{P}(\{\bowtie\}) = \{\emptyset, \{\bowtie\}\}$$
$$\mathcal{P}(\{\square, \lozenge\}) = \{\emptyset, \{\square\}, \{\lozenge\}, \{\square, \lozenge\}\}$$

[36] One can visualize this by thinking of binary strings of length n – a subset $A \in \mathcal{P}(X)$ corresponds to the string whose kth digit is 1 if and only if the kth element of X belongs to A.

Functions on power sets occur in all branches of mathematics. Suppose X and Y are sets. If $f\colon X \to Y$ is a function, then we can define a new function, called the *induced set function*, $f\colon \mathcal{P}(X) \to \mathcal{P}(Y)$ 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 *direct image* or *forward image* of B. Similarly, we can define $f^{-1}\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ 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 *preimage* of D. You should verify that both $f^{-1}\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ and $f\colon \mathcal{P}(X) \to \mathcal{P}(Y)$ are functions.[37]

Using the notation f to denote both the function $f\colon X \to Y$ and the induced function $f\colon \mathcal{P}(X) \to \mathcal{P}(Y)$ may strike you as unwise. However, in practice it is always clear from context which function we are using, and it turns out to be extremely convenient to use the same notation for both.

[37] If S, T are sets, then a function $\mu\colon S \to T$ is a rule that assigns to every $s \in S$ a unique $\mu(s) \in T$.

Exercises

10.1 Find the power set of $\{\smile, \bowtie, \frown\}$.

10.2 Consider the map $g\colon \mathbb{R} \to \mathbb{R}$ defined by $g(x) = |x|$. Find the forward image of $A = (-\infty, -1] \cup (1, \infty)$ under g, and prove that your answer is correct.

Hint: Your proof may require some casework. Also, you may wish to review how to prove two sets are equal (see the *Set Theory* worksheet on page 9).

10.3 Consider the map $h\colon \mathbb{R} \to \mathbb{R}$ defined by $h(x) = x^2 + 3$. Find $h[\mathbb{R}]$ and prove your claim.

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

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

10.6 Suppose X and Y are sets. Let $f\colon X \to Y$ be a function. Suppose $A \subseteq X$ and $B \subseteq Y$.

(a) Show: $f[f^{-1}[B]] \subset B$.

(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: $A \subset f^{-1}[f[A]]$.

(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.

10.7 Suppose X and Y are sets. Let $f\colon X \to Y$ be a function. Is the function $f^{-1}\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ an inverse[38] of $f\colon \mathcal{P}(X) \to \mathcal{P}(Y)$?

10.8 (*Bonus.*) Suppose X and Y are sets. Let $f\colon X \to Y$ be a function. Suppose $A, C \subseteq X$ and $B, D \subseteq Y$.

(a) Is $f^{-1}[B \cap D] = f^{-1}[B] \cap f^{-1}[D]$? Does one set always contain the other? Justify your answers.

(b) Is $f[A \cap C] = f[A] \cap f[C]$? Does one set always contain the other? Justify your answers.

10.9 (*Bonus.*) Suppose X and Y are sets. Let $f\colon X \to Y$ be a function. Suppose $A, C \subseteq X$ and $B, D \subseteq Y$.

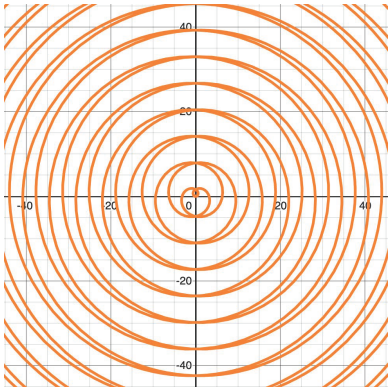
(a) Is $f[A \cup C] = f[A] \cup f[C]$? Does one set always contain the other? Justify your answers.

(b) Is $f^{-1}[B \cup D] = f^{-1}[B] \cup f^{-1}[D]$? Does one set always contain the other? Justify your answers.

10.10 (*Bonus.*) Suppose X and Y are sets. Let $f\colon X \to Y$ be a function. Suppose $A, C \subseteq X$ and $B, D \subseteq Y$.

(a) Is $f[A \setminus C] = f[A] \setminus f[C]$? Does one set always contain the other? Justify your answers.

(b) Is $f^{-1}[B \setminus D] = f^{-1}[B] \setminus f^{-1}[D]$? Does one set always contain the other? Justify your answers.



Hint: In all questions of this sort, it pays to consider the function $s\colon \mathbb{R} \to \mathbb{R}$ defined by $s(x) = x^2$.

[38] See sidenote 29.

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 $f\colon \mathbb{R} \to \mathbb{R}$ for which $f'(x) = 4x + 1$ and $f(2) = 42$ might go something like this: "Suppose $g, h\colon \mathbb{R} \to \mathbb{R}$ are differentiable functions for which $g'(x) = h'(x) = 4x + 1$ and $g(2) = h(2) = 42$. From the Mean Value Theorem,[39] 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."

Students of mathematics are appropriately prickly about the use of the pronouns "a" and "the". The definite article "the" specifies uniqueness, as in the statements "The smallest composite number is 4." and "The line passing through the points $(3, 2)$ and $(1, 4)$ intersects the y-axis." In the absence of uniqueness, we use the indefinite article "a" as in the statements "A positive composite number greater than 2 is 4." and "A non-vertical line passing through the point $(3, 2)$ intersects the y-axis."

[39] Suppose $a < b$. The Mean Value Theorem says that if $\ell\colon [a, b] \to \mathbb{R}$ is continuous on $[a, b]$ and differentiable on (a, b), then there exists a point $d \in (a, b)$ such that

$$\ell'(d) = \frac{\ell(b) - \ell(a)}{b - a}.$$

How are we using the Mean Value Theorem here?

Existence and uniqueness proofs are common throughout mathematics. For these proofs, you must show *both* that a solution exists *and* that there is at most one solution. So, for example, a proof that there exists a unique $f\colon \mathbb{R} \to \mathbb{R}$ 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.

11.1 Every element of $\mathbb{R}$ has a unique additive inverse. You have proba-

An element $\bowtie \in \mathbb{R}$ is an *additive inverse* of $\bigstar \in \mathbb{R}$ provided that $\bowtie + \bigstar = \bigstar + \bowtie = 0$. If an additive inverse of $\bigstar$ exists and is unique, it is often denoted $-\bigstar$.

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 $\bigstar \in \mathbb{R}$ is unique.

Suppose $\bowtie, \bowtie' \in \mathbb{R}$ are additive inverses of $\bigstar$. Note that

$$\bowtie = 0 + \bowtie = (\bowtie' + \bigstar) + \bowtie = \cdots \qquad \cdots = \bowtie' .$$

Hence if an additive inverse of $\bigstar \in \mathbb{R}$ exists, then it is unique.

Hint: if you find yourself writing $-\bigstar$, then you are probably assuming what you are trying to prove!

11.2 Similarly, every nonzero $r \in \mathbb{R}$ has a unique multiplicative inverse.[40] Since you've probably never shown that a multiplicative inverse of a nonzero $r \in \mathbb{R}$ is unique, do so now.

[40] An element $s \in \mathbb{R}$ is a *multiplicative inverse* of r provided that $rs = sr = 1$.

Hint: The role of zero in Exercise 11.1 will now be played by one. If you find yourself writing $1/r$ or r^{-1}, then you are probably assuming what you are trying to prove!

11.3 Suppose A and B are sets and $h\colon A \to B$ is invertible (see sidenote 29). Show that h has a unique inverse function.

Hint: If $g\colon B \to A$ and $f\colon B \to A$ are inverses of $h\colon A \to B$, then you need to show $g(b) = f(b)$ **for all** $b \in B$.

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 $\pentagon$ is denoted by $-\pentagon$. 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 a multiplicative inverse of an object $\sun$ exists and is unique, it is often denoted $\sun^{-1}$.

11.4 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.

Recall that $\star$ is a square root of $\moon$ provided that $\star^2 = \moon$.

If a nonnegative square root of $\moon \in \mathbb{R}$ exists and is unique, it is denoted $\sqrt{\moon}$.

11.5 For the objects you claimed to be unique in Exercise 11.4, prove that they are unique.

Hint: if you find yourself writing $\sqrt{x}$, then you are probably assuming what you are trying to prove!

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

11.7 Show that there is a unique real number solution to the equation $x^3 = 1$.

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

11.8 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.

Hint: Complete the square: $ax^2 + bx + c = a[(x + \smiley)^2 + (c/a - \smiley^2)]$; what's $\smiley$?

11.9 (*Bonus.*) Show that 0 is the unique element of $\mathbb{R}$ such that $s + 0 = 0 + s = s$ for all $s \in \mathbb{R}$. Similarly, show that 1 is the unique element of $\mathbb{R}$ such that $s \cdot 1 = 1 \cdot s = s$ for all $s \in \mathbb{R}$.

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

Hint: Don't think too much. Maybe try something like $A = A\,\mathrm{Id}_n = \cdots = \mathrm{Id}_n$ where the stuff in the middle follows from the given information and Id_n is the n-by-n matrix with ones on the diagonal and zeroes elsewhere. Also, since A is invertible, there exists a (unique) $n \times n$ matrix B so that $AB = BA = \mathrm{Id}_n$.

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.[41] 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 4.2 on page 15).

[41] This makes sense because this is a problem about divisibility by two.

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
>
> $$\frac{n(n+1)}{2} = \frac{(2k)(2k+1)}{2} = k(2k+1).$$
>
> - n is odd: In this case we can write $n = 2k+1$ with $k \in \mathbb{Z}$. We have
>
> $$\frac{n(n+1)}{2} = \frac{(2k+1)(2k+2)}{2} = (2k+1)(k+1).$$
>
> Since the result holds in each case, the claim is proved.

Exercises

Remember to label the separate cases of your proof to avoid confusion.

12.1 Prove[42] that 7 divides $x^2 + x + 12$ for $x \in \{1, 5, 8\}$.

[42] Remember to write in complete sentences.

12.2 Prove that 5, 13, and 25 can all be written as the sum of two squares (of integers).

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

Vertical lines are lines too.

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

Hint: This is a problem about divisibility by three.

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

Hint: $b^2 = b^2/4 + 3b^2/4$.

12.6 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.

The numbers $\binom{n}{k}$ have been studied for millennia. The formula discussed in this problem was known to Acharya Pingala in the second century BC.

Hint: Suppose that $(n+1)$ objects are lined up in order, and consider two cases – one where you pick the first element, and one where you do not.

12.7 (*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.)

12.8 (*Bonus*.) Determine which 2×2 matrices A with two entries of 0 and two entries of 1 satisfy $A^2 = A$.

Hint: The number of ways to choose two objects from a set of four is $\binom{4}{2} = \frac{4!}{(4-2)!2!} = 6$.

12.9 (*Review*.) Suppose A and B are sets. Show that if $A \subset B$, then $\mathcal{P}(A) \subset \mathcal{P}(B)$.

12.10 (*Bonus*.) Show that the converse of Exercise 12.9 is also true.

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

13.1 If p is a prime number and b is an integer such that p does not divide[43] b, then the only positive integer that divides both p and b is 1.

13.2 Let A be a 2×2 matrix such that $A^2 = \mathrm{Id}_2$. Then the top left entry or the bottom left entry of A is nonzero.

13.3 Suppose $a, b \in \mathbb{R}$. If $ab = 0$ then $a = 0$ or $b = 0$.

[43] Recall that if m and n are integers, we say that m *divides* n provided that there is some integer k such that $km = n$. A natural number p is prime if and only if p has exactly two distinct positive divisors.

Hint: When asked to prove something that appears obvious, you usually need to go back to first principles.

FOR MAX/MIN PROOFS, it's important to know how to interpret statements about a maximum of a set or a minimum of a set.[44] Relations between a number $x \in \mathbb{R}$ and a 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 $\min S \leq x$, you just need that *there exists* some element in S that is

[44] If $A \subset \mathbb{R}$, then M is a *maximum* for A provided that **both** $M \in A$ **and** $M \geq a$ for all $a \in A$. Similarly, m is a *minimum* for A provided that **both** $m \in A$ **and** $m \leq a$ for all $a \in A$.

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[45] $x \in \mathbb{R}$. 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 $\min\{x(x-2) \mid x \in \mathbb{R}\} \geq -1$.

[45] Remember that a proof that shows that something is true "for all $s \in S$" will almost always use the words "Fix $s \in S$."

Exercises

13.4 Suppose $B \subset \mathbb{R}$. Show[46] 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.

[46] Remember to write in complete sentences.

13.5 Does every subset of $\mathbb{R}$ have a maximum? A minimum?

13.6 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) $\emptyset$

13.7 Let S, T be subsets of $\mathbb{R}$, let $x \in \mathbb{R}$, and suppose that $\max S$, $\min S$, and $\min T$ all exist. Rewrite the statements below using quantifiers[47].

[47] Remember, these are phrases like *for every*, *there exists*, *for all*.

(a) $\max S \leq x$.

(b) $\max S \geq x$.

(c) $\min S \leq \min T$.

(d) $\min S \geq \min T$.

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

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

Hint: You may want to use calculus here. Also, you may need to remember how to complete the square.

Counterexamples

Counterexamples help us understand the boundaries of truth.[48] 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.[49] 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: $a = b = \sqrt{2}$).

[48] "Every good theorem must have a good counterexample." (Francesco Severi as quoted in *American Mathematical Monthly*, June, 1976)

[49] Consider, for example, the statements: "All birds can fly." "All prime numbers are odd." and " Subtraction is commutative."

Exercises

14.1 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.

(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 $a, b, c \in \mathbb{R}$.

Hint: Consider
$$(a-b)^2 + (a-c)^2 + (b-c)^2.$$

(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.

Hint: Try some primes less than 15.

(i) Suppose n is the product of three consecutive integers 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 14.1g 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 14.1e you might want to check what happens to zero.

14.2 Prove[50] all of your answers to Exercise 14.1, making sure to give an example/counterexample where applicable.

[50] Remember to write in complete sentences.

14.3 (*Bonus*.) True or False. Justify your answer.

(a) The set of invertible 2×2 matrices is a subspace[51] of the vector space $\mathbb{R}^{2\times 2}$ of 2×2 matrices.

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

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

[51] If V is a vector space, then $W \subset V$ 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 $k\vec{x} \in W$.

Contrapostive

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

> Any real number x that satisfies $|x| < \varepsilon$ for all $\varepsilon > 0$ must be zero.

might proceed as follows:

> Fix $x \in \mathbb{R}$. We are trying to show
>
> $$\forall \epsilon > 0,\ |x| < \varepsilon \Rightarrow x = 0.$$
>
> We will prove this by contraposition. The contrapositive is
>
> $$x \neq 0 \Rightarrow \exists \epsilon > 0 \text{ such that } |x| \geq \varepsilon.$$
>
> Suppose $x \neq 0$. Let $\varepsilon = |x|/2 > 0$. Note that $|x| > |x|/2 = \varepsilon$, so $|x| \geq \varepsilon$.

[52] The truth table for $P \Rightarrow Q$ is

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

and the truth table for $\neg Q \Rightarrow \neg P$ is

P	Q	$\neg Q$	$\neg P$	$\neg Q \Rightarrow \neg P$
T	T	F	F	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

Exercises

15.1 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 $\neg B$.

15.2 Suppose P and Q are statements. Use truth tables to verify DeMorgan's laws:

$$\neg(P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q) \quad \text{and} \quad \neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q).$$

These laws were observed by Aristotle two millennia before DeMorgan was born.

The symbol $\Leftrightarrow$ is shorthand for "if and only if".

15.3 (*Review.*) Suppose A and B are subsets of a set X. Show

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

Hint: If your proof does not make use of DeMorgan's laws, then it is probably wrong.

15.4 Find the contrapositive of each of the following statements.

(a) Suppose $n \in \mathbb{Z}$. If $n^2 + 3n - 7$ is even, then n is odd.

(b) Suppose $m \in \mathbb{N}$. If the remainder of m upon dividing by 4 is 2 or 3, then m is not a perfect square.[53]

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

[53] An integer ℓ is called a *perfect square* provided that there exists $k \in \mathbb{Z}$ such that $\ell = k^2$.

15.5 Prove[54] that if $x^{61} - x^7 + x^2 \neq 1$, then $x \neq 1$.

[54] Remember to write in complete sentences.

15.6 Prove the statement of Exercise 15.4a.

15.7 Prove the statement of Exercise 15.4b.

Hint: A natural number is either even or odd.

15.8 Prove the statement of Exercise 15.4c.

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

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

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

15.11 (*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.

"I am a linearly independent woman – all of my relationships are trivial."
–NJ, 2020

Contradiction

Proof by contradiction has been described as "one of a mathematician's finest weapons."[55] 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 $r \wedge \neg r$ for some statement r. That this is logically equivalent to showing $P \Rightarrow Q$ is verified in the truth table below. The

P	Q	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$r \wedge \neg r$	$\neg(P \Rightarrow Q) \Rightarrow (r \wedge \neg r)$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	F	T
F	F	T	F	F	T

statement r is not given to you, but usually arises naturally from the problem under consideration. In the proof that the positive square root of 2 is not rational on page 6 of the *Introduction* the statement r is "At most one of a and 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 $n > 2$."

[55] "*. . . reductio ad absurdum*, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers *the game*." – G. H. Hardy, *A Mathematician's Apology*, 1940, italics in original.

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;[56] 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[57] 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."

[56] Instead of writing $\neg(P \Rightarrow Q)$, we often write the logically equivalent $P \wedge \neg Q$.

P	Q	$P \wedge \neg Q$
T	T	F
T	F	T
F	T	F
F	F	F

[57] 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.

Exercises

16.1 Prove[58] by contradiction: If $s \in \mathbb{R}$ and $s^2 = 3$, then $s \notin \mathbb{Q}$.

[58] Remember to write in complete sentences.

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

16.3 Prove by contradiction: If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and $q \in \mathbb{Q}$, then $\alpha - q \in \mathbb{R} \setminus \mathbb{Q}$.

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

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

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

Hint: Rolle's Theorem, which was stated by Bhāskara II five centuries before Michel Rolle lived, might be useful here. Suppose $a < b$. Rolle's Theorem says that if $f\colon [a, b] \to \mathbb{R}$ 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 $f'(d) = 0$.

16.6 Show: There are no integers a, b such that $21a + 35b = 1$.

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

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

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.

The Principle of Mathematical Induction states:

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

This is an axiom – that is, it is one of our basic, unprovable assumptions about the nature of the natural numbers.

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

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= [1 + 2 + \cdots + k] + (k+1) \\ &\qquad \text{(since } G(k) \text{ is assumed to be true)} \\ &= \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}; \end{aligned}$$

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."

This is the result Carl Friedrich 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.

Exercises

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

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

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

(e) If $a, c \in \mathbb{R}_{\geq 0}$ with $a < c$, then $a^n < c^n$ for all $n \in \mathbb{N}$.

17.2 Suppose $r \in \mathbb{R} \setminus \{1\}$. Show $1 + r + \cdots + r^n = (1 - r^{n+1})/(1 - r)$.

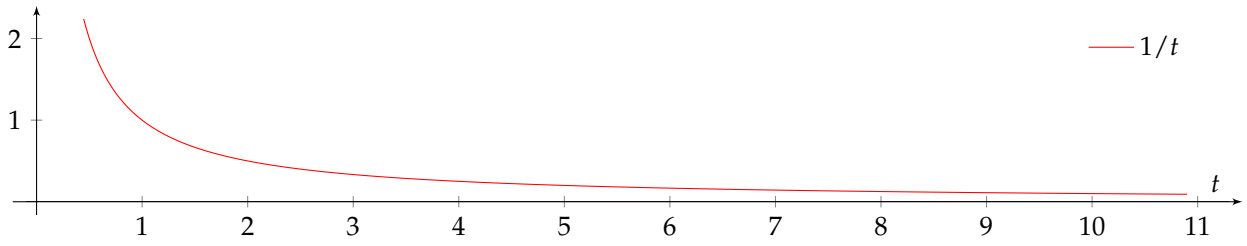
17.3 Prove statements (17.1a) and (17.1e).

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

17.5 For all $n \geq 2$:

$$\ln(n) \;\geq\; \frac{1}{2} + \cdots + \frac{1}{n}.$$

Hint: For $x > 0$, $\ln(x) = \int_1^x \frac{1}{t}\, dt$.



17.6 Let $f(x) = \ln(1 + x)$, and let $f^{(m)}(x)$ denote the m-th derivative of f. Prove that for all m in $\mathbb{N}$

$$f^{(m)}(x) = (-1)^{m+1} \frac{(m-1)!}{(1+x)^m}.$$

By convention, $0! = 1$.

17.7 For all $n \in \mathbb{N}$:

$$\int_0^\infty x^n e^{-x}\, dx \;=\; n!$$

Hint: $\int u\, dv = uv - \int v\, du$; recall the definition of $\int_0^\infty$; set $u = x^{n+1}$ and $v = -e^{-x}$.

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

By convention, $\forall ☺$, $☺^0 = 1$.

17.9 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.

Hint: Fix $y_0 \in Y$. Let $Y' = Y \setminus \{y_0\}$. If A is a subset of Y', then we have $A \subset Y$, $A \cup \{y_0\} \subset Y$, and $A \neq A \cup \{y_0\}$.

17.10 Suppose you contribute P dollars at the end of each year to an ordinary annuity with an annual rate of return I. Show that the future value of your annuity at the end of n years is given by $F(n) = P \cdot \frac{(1+I)^n - 1}{I}$.

I is sometimes called the interest or discount rate.

17.11 (*Bonus.*) The determinant[59] of an upper triangular $n \times n$ matrix is the product of the diagonal entries.

[59] Developed to help solve systems of equations, determinants were independently introduced in the late seventeenth century by Seki Takakazu and Gottfried Wilhelm Leibniz.

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 18.7 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 18.1 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[60] as well as what happens at each step.[61]
- Write in complete sentences, with correct grammar, punctuation, and capitalization.
- Cite the results that you use.[62]
- 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.

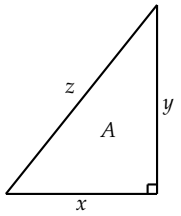
[60] For example: "We will split the problem into two cases and prove that the statement holds in each case."

[61] For example: "Multiplying by two on both sides, we see that . . . "

[62] For example: "By theorem 1.10 we know that..." or "By the lemma from class stating that every matrix satisying . . . has the property . . . , we conclude . . . "

Exercises

18.1 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.



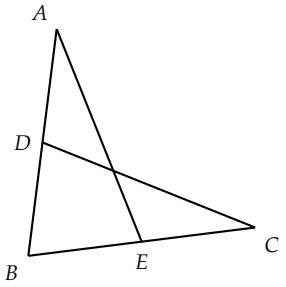
The right triangle of Exercise 18.1

18.2 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:

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

For more on complex numbers see *Complex Numbers* on page 61.

18.3 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".)



The diagram for Exercise 18.3

18.4 Suppose S, T, and U are sets, $f\colon S \to T$ is a function, and $g\colon T \to U$ is a function.

(a) Show[63] that if f and g are injective, then $g \circ f\colon S \to U$ is injective.

(b) Show that if f and g are surjective, then $g \circ f\colon S \to U$ is surjective.

[63] Remember to write in complete sentences.

18.5 If $n \in \mathbb{N}$ is not prime, then $2^n - 1$ is not prime.

Hint: If $n = ab$, find an expression for $(2^n - 1)/(2^a - 1)$.

18.6 Suppose $a, b, c, d \in \mathbb{Z}$.

(a) (Rule of 3) If $a + b = c$ and d divides both a and b, then d divides c.

(b) (Transitivity of divisibility) If a divides b and b divides c, then a divides c.

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

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

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

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

18.9 (*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 does it mean that M is invertible?

18.10 (*Bonus*.) Suppose that $\alpha \in \mathbb{R}$. Show that α has a terminating or repeating decimal expansion if and only if $\alpha \in \mathbb{Q}$.

Hint: The remainder at each step in the long division $d\overline{)c}$ belongs to $\{0, 1, 2, \ldots, (d-1)\}$.

Resources

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*.

[1] 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.

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.

[2] Paul Halmos, *Naive Set Theory*, Springer–Verlag, NY 1974.

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 $x \in S$ if x is an element of S and $x \notin S$ 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 $x \in S$ or $x \notin S$, but not both.

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

Math 582, *Introduction to Set Theory*, provides a rigorous treatment of $\mathbb{N}$.

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

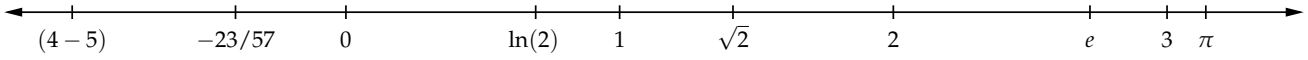
The symbol $\mathbb{Z}$ is derived from *Zahlen*, the German word for numbers.

NEVER divide by zero.

In Math 412, *Introduction to Modern Algebra*, $\mathbb{Q}$ is rigorously defined.

Approximately 1.41, $\sqrt{2}$ 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 $\mathbb{Q}$.

Introductory analysis courses, including Math 351 and Math 451, provide in-depth treatments of $\mathbb{R}$.



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 $|A|$.

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

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

$$\{n \in \mathbb{N} \mid n \text{ has exactly two distinct positive divisors}\},$$

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.

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

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,∞), $(-\infty,a)$, and $(-\infty,a]$ are defined similarly.

PRACTICE: Test your understanding of set notation using Doug Ensley's material at `math.lsa.umich.edu/courses/101/sets.html`.

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.

$$\begin{aligned}\{T,O,M,M,A,R,V,O,L,O,R,I,D,D,L,E\} \\ &= \{I,A,M,L,O,R,D,V,O,L,D,E,M,O,R,T\} \\ &= \{A,D,E,I,L,M,O,R,T,V\}.\end{aligned}$$

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.

[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:

$$\begin{aligned}0 &= 0^2+0^2+0^2+0^2\\ 1 &= 1^2+0^2+0^2+0^2\\ 2 &= 1^2+1^2+0^2+0^2\\ 3 &= 1^2+1^2+1^2+0^2\\ 4 &= 1^2+1^2+1^2+1^2\\ &= 2^2+0^2+0^2+0^2\\ 5 &= 2^2+1^2+0^2+0^2\end{aligned}$$

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?

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.*

WARNING: Some people say "A contains a" to mean "$a \in A$."

WARNING: Some people write "$A \subset B$" to mean "$A \subseteq B$, 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 $1 \in \{1, \sqrt{2}\} \subset (\sqrt{2}/2, \sqrt{2}] \subset [\ln(2), e) \subset [\ln(2), e]$ and the obvious[5] 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 $Y \subset X$. □

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

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

The symbol □ 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*.

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.

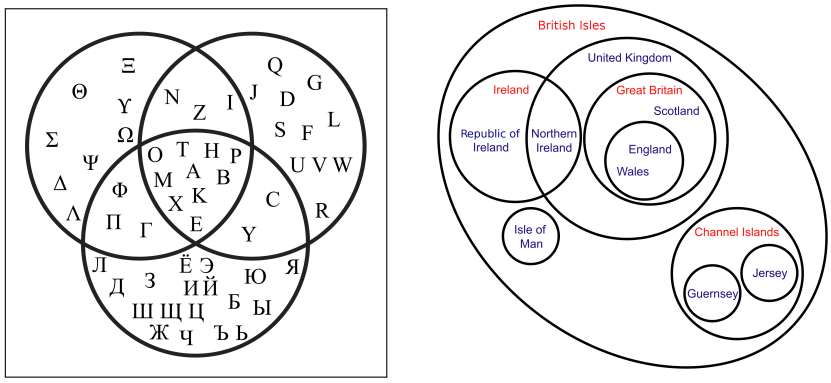


Figure 1: The left Venn diagram illustrates relationships among upper case letters in the Greek, Latin, and Russian alphabets. The universe consists of all upper case letters in these alphabets, and each language is represented by one of the circles. The Venn diagram on the right describes the geographical 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.

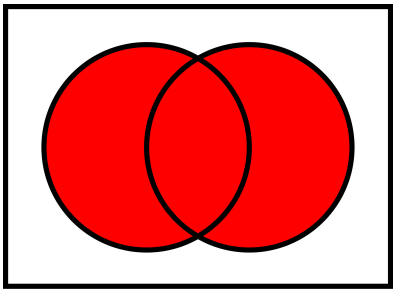
CAUTION. Because many statements about sets are intuitive and/or obvious, figuring out how to prove them can be difficult. While Venn diagrams are excellent tools for illustrating many of these statements, the diagrams are not substitutes for their proofs.

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

PRACTICE: Use Doug Ensley's materials to gain basic familiarity with set operations at `math.lsa.umich.edu/courses/101/venn2.html` and `math.lsa.umich.edu/courses/101/venn3.html`.

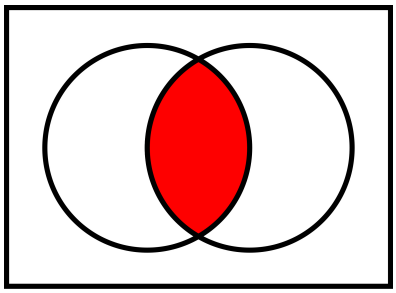
by the circle to the right, and the box represents a universe that contains both A and B.



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

$$\{\☺ \mid (\☺ \in A) \text{ or } (\☺ \in B)\}.$$

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 $\{\varepsilon, \delta, \alpha\}$ and $\{\delta, \beta, \rho, \phi\}$ is the set $\{\alpha, \beta, \delta, \varepsilon, \rho, \phi\}$, the union of $\mathbb{Z}$ and $\mathbb{Q}$ is $\mathbb{Q}$, and $[\ln(2), \sqrt{2}] \cup (\sqrt{2}/2, e]$ is $[\ln(2), e]$. Note that $S \cup \emptyset = S$ for all sets S.

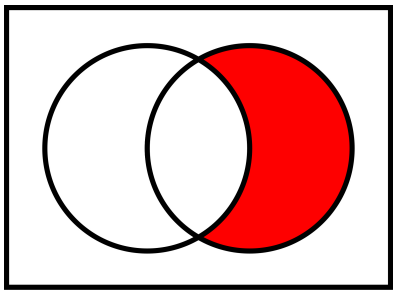


Definition 4. *The* intersection *of sets A and B, written $A \cap B$, is the set*

$$\{\☹ \mid (\☹ \in A) \text{ and } (\☹ \in B)\}.$$

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 $\{\varepsilon, \delta, \alpha\}$ and $\{\delta, \beta, \rho, \phi\}$ is the *singleton* $\{\delta\}$, the intersection of $\mathbb{Z}$ and $\mathbb{Q}$ is $\mathbb{Z}$, 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.

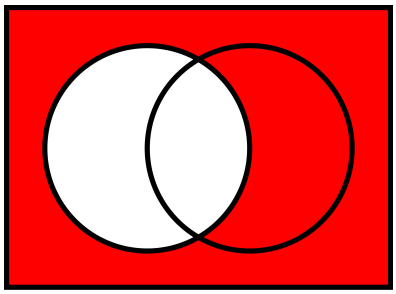
Remark 5. *For S and T sets, $S \cap T \subset S \subset S \cup T$ and $S \cap T \subset T \subset S \cup T$.*



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

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

Note that, like subtraction, the difference operator is not symmetric. For example, $\{\varepsilon, \delta, \alpha\} \setminus \{\delta, \beta, \rho, \phi\}$ is $\{\alpha, \varepsilon\}$ while $\{\delta, \beta, \rho, \phi\} \setminus \{\varepsilon, \delta, \alpha\}$ 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, $A^{\complement}$, $\bar{A}$, 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 $[-1, \pi)^{\complement}$, then from context the set U is $\mathbb{R}$ and $[-1, \pi)^{\complement} = (-\infty, -1) \cup [\pi, \infty)$.

Note that $A^{\complement} \cup A$ is U, and $A^{\complement} \cap A = \emptyset$. 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[6] them. They say

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

[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*.

[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)

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 $\boxed{1+2+3=1\cdot 2\cdot 3.}$, $\boxed{5+4=8.}$, and $\boxed{\text{In terms of future career satisfaction, math is a top-ranked degree.}}$ are all statements. However, the sentences $\boxed{\text{This sentence is false.}}$, $\boxed{x=\pi+34.}$, $\boxed{\text{When does Michigan play today?}}$, and $\boxed{\text{Go Blue!}}$ are all NOT statements.

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

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.

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

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 (The Michigan Math Club meets on Thursdays at 4PM in the Nesbitt Commons Room, East Hall.) is T.

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`.

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, $\neg$(All mathematicians are left-handed.) is (Not all mathematicians are left-handed.) rather than (All mathematicians are not left-handed.).

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

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.

P	$\neg P$
T	F
F	T

Table 1: The truth table for negation.

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.).

[2] *Euclid's Elements*, Book I, Propositions 47 and 48.

When statements P and Q are equivalent, we write $P \Leftrightarrow Q$. 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 $\neg(\neg P) \Leftrightarrow P$. As expected, $\neg(\neg P)$ and P have the same truth values:

P	$\neg P$	$\neg(\neg P)$
T	F	T
F	T	F

"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)

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 ($P \wedge Q$). Note that the statement ($P \wedge Q$) is true when both P and Q are true and is false otherwise.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

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 ($P \vee Q$). Note that the statement ($P \vee Q$) is false when both P and Q are false and is true otherwise.

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.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

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:

$$\neg(P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q) \quad \text{and} \quad \neg(P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q).$$

[3] $A^{\complement} = \{x \mid \neg(x \in A)\}$
$A \cap B = \{\text{☺} \mid (\text{☺} \in A) \wedge (\text{☺} \in B)\}$
$A \cup B = \{\text{☺} \mid (\text{☺} \in A) \vee (\text{☺} \in B)\}$

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-

PRACTICE: To gain familiarity with compound statements and conditionals, use Doug Ensley's materials at `math.lsa.umich.edu/courses/101/imply.html`, `math.lsa.umich.edu/courses/101/tt1.html`, and `math.lsa.umich.edu/courses/101/tt2.html`.

bined the statements r = (You're not part of the solution.) and s = (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.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

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." *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.

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 π is that the function be differentiable at π.

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.

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 $\neg(P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q$. 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 π, then f is continuous at π.) is (f is differentiable at π, and f is not continuous at π.).

P	Q	$P \wedge \neg Q$	$\neg(P \Rightarrow Q)$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	F	F

Predicates

The sentence $\boxed{y > 4.}$ 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 $\boxed{y > 4.}$ 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 $\boxed{2 < e^x < e}$ and $Q(\☺, \☹)$ might denote the predicate $\boxed{\☺^2 + \☹^2 = 34.}$.

PRACTICE: To gain familiarity with predicates, use Doug Ensley's material at `math.lsa.umich.edu/courses/101/predicate.html`.

As with statements, a predicate can be negated. For example, suppose $Q(\☺, \☹) = \boxed{\☺^2 + \☹^2 = 34.}$ and $r(y) = \boxed{y > 4.}$, then $\neg Q(\☺, \☹)$ is $\boxed{\☺^2 + \☹^2 \neq 34.}$ and $\neg r(y)$ is $\boxed{y \leq 4.}$.

PRACTICE: To gain familiarity with negating predicates, use Doug Ensley's material at `math.lsa.umich.edu/courses/101/np1.html` and `math.lsa.umich.edu/courses/101/np2.html`.

Quantifiers

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

$$\text{(There exists a real number } y \text{ such that } y > 4.) \tag{1}$$

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

$$\text{(For all real numbers } y\text{, we have } y > 4.) \tag{2}$$

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 $(\forall n \in \mathbb{Z},\ n$ is even.) and the statement (Some integers are even.) is equivalent to $(\exists m \in \mathbb{Z}\ m$ 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

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

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, ¬(Everyone 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

$$\neg(\forall x, P(x)) \text{ is } \exists z\ \neg P(z) \quad \text{and} \quad \neg(\exists w\ P(w)) \text{ is } \forall v, \neg P(v).$$

Thus, the negation of (Every triangle is isosceles.) is (Some triangle is not isosceles.) and ¬(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.).

PRACTICE: To gain familiarity with quantifiers, use Doug Ensley's material at `math.lsa.umich.edu/courses/101/quantifiers.html`.

We have used the phrase "such that" rather than the incorrect "so that." See the comments of former Michigan mathematics professor J.S. Milne at `www.jmilne.org/math/words.html`.

"For all" is called a *universal* quantifier and "there exists" is called an *existential* quantifier.

... cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

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

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

Thus, as you should verify, a function f is NOT continuous at a provided that

$$\exists \varepsilon > 0\ \forall \delta > 0, \exists x \in \mathbb{R}$$
$$(|x - a| < \delta) \wedge (|f(x) - f(a)| \geq \varepsilon).$$

"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)

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[3] *source* of f, and the set Y is called the *codomain* or[3] *target space* of f. Sometimes it is useful to have notation for this, so we might write $\mathrm{dom}(f)$ for the domain of the function f and $\mathrm{cod}(f)$ for its codomain.

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

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 $\mathrm{im}(f)$, is the set

$$\mathrm{im}(f) := \{f(x) : x \in X\}$$

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

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

and we define the *preimage* of B under f to be the set

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

These operations have friendly properties that are fun to prove.[5]

Example. For any set X, the *identity function* $\mathrm{Id}_X : X \to X$ is defined by the rule $\mathrm{Id}_X(x) = x$ 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.

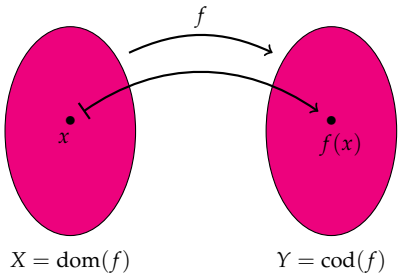


Figure 1: The function $f : X \to Y$.

[1] 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.

[2] 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.)

"$f : X \to Y$" 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 "$\mapsto$" and write "$x \mapsto f(x)$."

[3] Variety is the spice of life.

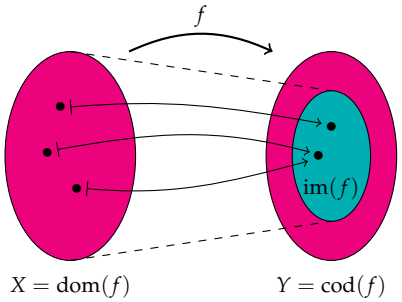


Figure 2: $\mathrm{im}(f) = f[X] \subseteq \mathrm{cod}(f)$.

[4] Some folks use *range* to mean image, but others use it to mean codomain, so we avoid the term altogether.

[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 $s : \mathbb{R} \to \mathbb{R}$ is defined by the rule $s(x) = x^2$ 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[6] 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 $h \circ (g \circ f) = (h \circ g) \circ f$.

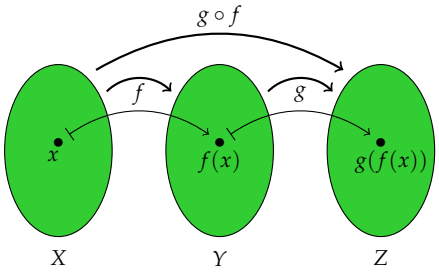


Figure 3: The function $g \circ f : X \to Z$.

[6] 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!)

Definition. If $f : X \to Y$ is a function, then an *inverse* of f is a function $g : Y \to X$ such that $g \circ f = \mathrm{Id}_X$ and $f \circ g = \mathrm{Id}_Y$. 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.

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.

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

Try proving that $f : X \to Y$ is injective if and only if there is $g : Y \to X$ such that $g \circ f = \mathrm{Id}_X$ and surjective if and only if there is $g : Y \to X$ such that $f \circ g = \mathrm{Id}_Y$.

***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 $\mathrm{dom}(f)$ or $\mathrm{cod}(f)$.

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 $f \restriction A$ or[3] $\mathrm{res}_A f$.

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

While you're at it, also prove this: for any functions $f : X \to Y$ and $g : Y \to Z$,
(i) If f and g are injective, so is $g \circ f$;
(ii) If f and g are surjective, so is $g \circ f$;
(iii) If f and g are bijective, so is $g \circ f$;
(iv) If $g \circ f$ is injective, then so is f;
(v) If $g \circ f$ is surjective, then so is g.

For any function $f : X \to Y$, the function $g : X \to \mathrm{im}(f)$ 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.

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

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 kth element is x_k. Two lists are *equal* if they have the same length and the same elements, in the same order.

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.

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.

Although named for René Descartes, Nicole Oresme came up with the idea of using rectangular coordinates in both two and three dimensions more than half a millennium before Descartes was born.

You are faimilar with the *summation* symbol, which is the capital Greek letter sigma: $\sum$. 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 $\vec{x} \in \mathbb{R}^n$ being both an n-tuple and a vector. It's a bit like the fact that you are both a leader and the best.

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

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

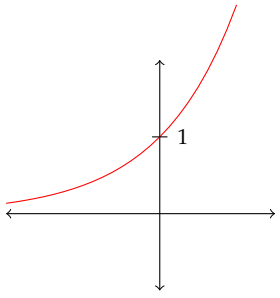


Figure 4: The graph of the exponential function $y = e^x$.

Now that we have defined Catesian products in general, there is nothing to stop us from doing this with *any* function. That is, for any function $f : X \to Y$, we define the *graph* of f to be the set

$$\text{graph}(f) \;:=\; \{(x,y) \in X \times Y \,:\, f(x) = y\} \;\subseteq\; X \times Y.$$

When X and Y are arbitrary sets, we cannot really "draw" the graph of a function $f : X \to Y$ 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.

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 $f, g : \mathbb{R} \to \mathbb{R}$ defined by

$$f(x) = \sqrt{x^2} \qquad \text{and} \qquad g(x) = \begin{cases} -x & \text{if } x < 0; \\ x & \text{if } x \geq 0. \end{cases}$$

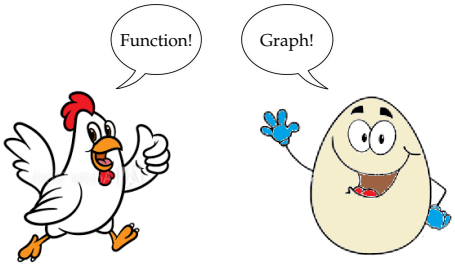
"In mathematics rigor is not everything, but without it there is nothing." *–Henri Poincaré*

"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 $f(14)$?

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 $(x,y) \in f$.

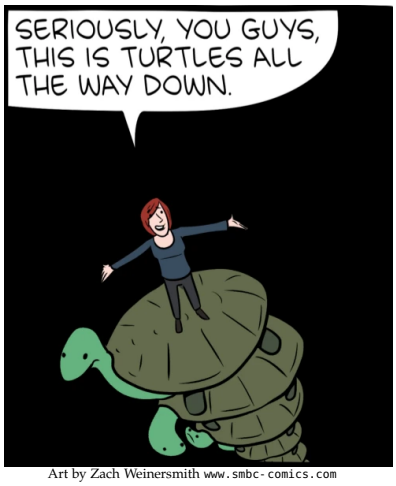
Of course, "$(x,y) \in f$" is a bit of set-theoretic folderol that will never appear again outside this definition, since it just means "$y = f(x)$."

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[7] is a set.



Art by Zach Weinersmith www.smbc-comics.com

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

Complex Numbers

While you should already be somewhat familiar with the number systems $\mathbb{N}$ of natural numbers, $\mathbb{Z}$ of integers, $\mathbb{Q}$ of rational numbers, and $\mathbb{R}$ of real numbers, you may feel less acquainted with the number system $\mathbb{C}$ of complex numbers. This handout provides a friendly introduction.

What are complex numbers?

Intuitively, a complex number is a number of the form

$$z = a + bi,$$

where a and b are real numbers and $i^2 = -1$. The set of complex numbers is denoted $\mathbb{C}$. When $b = 0$, the complex number $a + bi$ is real, so $\mathbb{R} \subseteq \mathbb{C}$. For any complex number $z = a + bi$, the real numbers $\mathrm{Re}(z) = a$ and $\mathrm{Im}(z) = b$ are called the *real* and *imaginary* parts of z, respectively. Addition, subtraction, and multiplication are defined by

$$\begin{aligned} (a+bi) + (c+di) &= (a+c) + (b+d)i, \\ (a+bi) - (c+di) &= (a-c) + (b-d)i, \\ \text{and} \qquad (a+bi)(c+di) &= (ac-bd) + (ad+bc)i. \end{aligned}$$

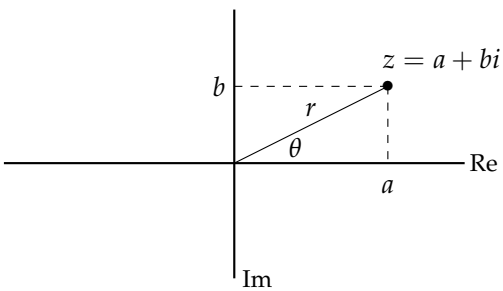
Division is a bit trickier, but we can do that too:

$$\frac{a+bi}{c+di} = \left(\frac{ac+bd}{c^2+d^2}\right) + \left(\frac{bc-ad}{c^2+d^2}\right) i. \tag{1}$$

The fact that you can add, subtract, multiply, and divide in $\mathbb{C}$ makes $\mathbb{C}$ a *field*, just like $\mathbb{Q}$ and $\mathbb{R}$; we will have more to say about this later.

Ok, but what do they look like?

You may have noticed that complex numbers are basically just pairs[1] of real numbers, which makes them seem a lot like elements of $\mathbb{R}^2$. This analogy between $\mathbb{C}$ and $\mathbb{R}^2$ is quite useful for visualizing complex numbers. If we let the horizontal axis represent the real part of a complex number, and the vertical axis the imaginary part, then we can plot a complex number $z = a + bi$ in the *complex plane* (also called an *Argand diagram*) like so:



While x and y are the go-to variables for real numbers, we tend to use z and w to represent complex numbers.

Thus $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Note that "complex" does not necessarily mean "nonreal." π, $\sqrt{2}$, and 217 are complex numbers too!

The easy way to remember the multiplication rule is that you just expand everything and collect like terms, using the fact that $i^2 = -1$.

Whenever we say "divide," of course, we mean division by a *nonzero* number. It is a cardinal rule in math that you are NEVER allowed to divide by zero.

There is no need to memorize the division rule; just remember that you can eliminate the imaginary part of the denominator by multiplying by its *complex conjugate* (see below).

[1] In fact, we can rigorously define $\mathbb{C}$ by setting $\mathbb{C} = \mathbb{R}^2$ as sets. We then define zero in $\mathbb{C}$ to be $(0,0)$, one in $\mathbb{C}$ to be $(1,0)$, addition in $\mathbb{C}$ by

$$(a,b) + (c,d) = (a+c, b+d),$$

and multiplication in $\mathbb{C}$ by

$$(a,b) \cdot (c,d) = (ac - bd, ad + bc).$$

We set $i = (0,1)$.

We can also represent complex numbers using 2×2 matrices. If we define the map $\varphi : \mathbb{C} \to \mathbb{R}^{2\times 2}$ by

$$\varphi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix},$$

then for all $z, w \in \mathbb{C}$ we have $\varphi(z+w) = \varphi(z) + \varphi(w)$ and $\varphi(zw) = \varphi(z)\varphi(w)$.

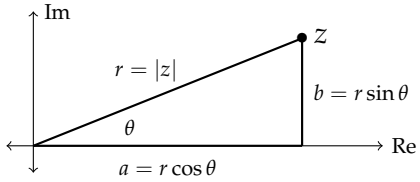
"I'm sorry, the number you have dialed is imaginary. Please rotate your phone 90 degrees and try again."

Converting to polar coordinates, we can express the complex number $z = a + bi$ in *polar form* as

$$z \;=\; r\cos\theta + (r\sin\theta)i \;=\; re^{i\theta},$$

where the second equality follows from *Euler's formula*:

$$e^{i\theta} \;=\; \cos\theta + i\sin\theta.$$



The best way to verify Euler's formula is using the Taylor series expansions at 0 of e^x, $\cos x$, and $\sin x$. Try it!

The nonnegative real number $r = \sqrt{a^2+b^2}$ is called the *modulus* of the complex number $z = a + bi$, usually written $|z|$. The angle $\theta \in (-\pi, \pi]$ is called the *argument* of z, written $\mathrm{Arg}(z)$. Multiplying, dividing, and taking powers of complex numbers becomes far easier in polar form, since the usual rules of exponents allow us to write:

$$\text{(i)}\quad (re^{i\theta})^n \;=\; r^n e^{in\theta},$$
$$\text{(ii)}\quad r_1 e^{i\theta_1}\cdot r_2 e^{i\theta_2} \;=\; r_1 r_2 e^{i(\theta_1+\theta_2)},$$
$$\text{and (if } r_2 \neq 0)\quad \text{(iii)}\quad (r_1 e^{i\theta_1})/(r_2 e^{i\theta_2}) \;=\; (r_1/r_2)e^{i(\theta_1-\theta_2)}.$$

For all $z, w \in \mathbb{C}$, we have $|zw| = |z||w|$ and $|z+w| \leq |z| + |w|$.

Technically this θ is called the *principal argument* of z, while any number differing from it by an integer multiple of 2π is an argument of z.

For instance, using polar form we can quickly compute $\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^6$, since

$$\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^6 \;=\; \left(1e^{\frac{\pi i}{3}}\right)^6 \;=\; e^{2\pi i} \;=\; 1.$$

In fact, the 6 sixth roots of 1 in $\mathbb{C}$ are just $e^{\frac{2\pi k i}{6}}$, where $k \in \{0,1,2,3,4,5\}$.

What is complex conjugation?

The easiest way to understand the rule for dividing complex numbers given in (1) is to remember that the imaginary part of the denominator in $\frac{a+bi}{c+di}$ can be eliminated by multiplying the numerator and denominator by $c - di$. The complex number $c - di$ is called the *complex conjugate* of $w = c + di$, and is usually written $\bar{w}$. Geometrically, complex conjugation is just reflection over the real axis. Complex conjugation has the following properties:

Remember: NEVER divide by zero.

You used a similar method in high school to rationalize denominators.

$\bar{w}$ is pronounced "w-bar."

- $\overline{z+w} = \bar{z} + \bar{w}$
- $\overline{z/w} = \bar{z}/\bar{w}$
- $\mathrm{Re}(z) = \frac{1}{2}(z + \bar{z})$
- $\overline{zw} = \bar{z}\bar{w}$
- $|z|^2 = z\bar{z}$
- $\mathrm{Im}(z) = \frac{1}{2i}(z - \bar{z})$.

NEVER divide by zero.

Note that for all $z \in \mathbb{C}$, we have that $z \in \mathbb{R}$ if and only if $z = \bar{z}$.

What's so special about $\mathbb{C}$*?*

The complex number system $\mathbb{C}$ is an example of an algebraic structure called a *field*. Roughly speaking, a field is a set of numbers that you can add, subtract, multiply, and divide (except by zero). $\mathbb{N}$ is not a field because you can't subtract, and $\mathbb{Z}$ is not a field because you can't divide, but $\mathbb{Q}$ is a field.

However, while you can add, subtract, multiply, and divide in $\mathbb{Q}$, there are two more things you might want to do but cannot: take limits of certain sequences, and solve certain polynomial equations. For instance,

3.1, 3.14, 3.141, 3.1415, 3.14159, 3.141592, 3.1415926, 3.14159265, ...

The field axioms, which you do not need to memorize (yet), are:

1. $\forall x, y, z,\ (x+y)+z = x+(y+z)$;
2. $\forall x,\ x+0 = 0+x = x$;
3. $\forall x\ \exists y$ such that $x+y=0$;
4. $\forall x, y,\ x+y = y+x$;
5. $\forall x, y, z,\ (xy)z = x(yz)$;
6. $0 \neq 1$ and $\forall x,\ 1\cdot x = x\cdot 1 = x$;
7. $\forall x \neq 0,\ \exists y$ such that $xy = 1$;
8. $\forall x, y,\ xy = yx$;
9. $\forall x, y, z,\ x(y+z) = xy + xz$.

A *field* is any system of numbers that can be added and multiplied, includes the special numbers zero and one, and satisfies these nine axioms.

is a sequence in $\mathbb{Q}$ that "should" converge but does not (in $\mathbb{Q}$) because π is irrational. Likewise, $x^2 - 2 = 0$ and $x^2 + 1 = 0$ are two perfectly good polynomial equations which "should" have solutions but do not (in $\mathbb{Q}$) since neither 2 nor -1 has a rational square root.

To fix the first problem, we extend $\mathbb{Q}$ to $\mathbb{R}$, i.e., we use real numbers: any sequence in $\mathbb{R}$ that "should" converge *does* converge. Introducing $\mathbb{R}$ solves much of the second problem too; for instance, we get $\sqrt{2} \in \mathbb{R}$, a solution of $x^2 - 2 = 0$. But there are still some polynomial equations that cannot be solved in $\mathbb{R}$, like $x^2 + 1 = 0$. To fix *this* problem, we extend $\mathbb{R}$ to $\mathbb{C}$, i.e., we use complex numbers. The fact that $\mathbb{C}$ really does solve the second problem is an important fact:

The sequences $(a_n)_{n\in\mathbb{N}}$ that "should converge" are called *Cauchy sequences*, and are defined by the property that for every $\epsilon > 0$ there is $N \in \mathbb{N}$ such that $|a_m - a_n| < \epsilon$ whenever $m, n \geq N$. You may encounter these in Math 351 or 451.

The technical term for this is that $\mathbb{R}$ is *complete*. In general, any space in which both the notion of Cauchy sequence makes sense and every Cauchy sequence converges to an element of the space is called complete.

Theorem (The Fundamental Theorem of Algebra)**.** *For every nonconstant polynomial $p(x) = \sum_{k=0}^{n} a_k x^k$ with coefficients in $\mathbb{C}$, the equation $p(x) = 0$ has at least one solution in $\mathbb{C}$.*

The Fundamental Theorem of Algebra is usually attributed to Gauss, who proved it in his PhD thesis, although, as is often the case in math, the full history is a bit more complicated.

But do "imaginary" numbers really exist?

We have said that

$$\mathbb{C} = \{a + bi \,:\, a, b \in \mathbb{R}\},$$

where $i^2 = -1$. But how do we know that -1 should have a square root? Are we really allowed to make up a new symbol, i, and say that $i^2 = -1$? The whole thing feels like cheating. If we can just introduce a new symbol for whatever nonexistent thing we want, what's to stop us from "defining" j to be $\frac{1}{0}$ and suddenly declaring division by 0 to be possible?

I Shrink by Craig Snodgrass
notsohumblepi.com

The field axioms are what is stopping us! It is impossible to prove, using the field axioms, that "there does not exist x such that $x^2 = -1$." But it *is* possible to prove that "there does not exist x such that $0 \cdot x = 1$."

In fact, there is no more reason to be skeptical of i than there is to be skeptical of $\sqrt{2}$, and any queasiness you might have about i probably stems from your relative familiarity with $\mathbb{R}$ as compared to $\mathbb{C}$, perhaps along with the fact that when we measure lengths in the real world we use real numbers, giving us a sort of built-in geometric intuition for them.

But the analogy between $\sqrt{2}$ and i is quite strong. If you are working in $\mathbb{Q}$, then *there is no number* whose square is 2, making $\sqrt{2}$ just as "imaginary" as i is from the perspective of $\mathbb{Q}$. But it is perfectly legal to introduce a new symbol, $\sqrt{2}$, and declare its square to be 2. In fact, there is a smallest field containing both $\mathbb{Q}$ and $\sqrt{2}$, and you can do math in this number system without breaking any rules. Similarly, if you are working in $\mathbb{R}$, then *there is no number* whose square is -1, but it is again perfectly legal to introduce a new symbol, i, and declare its square to be -1. There is then a smallest field containing both $\mathbb{R}$ and i, and in fact this field is $\mathbb{C}$. The theory of how all this works is called the theory of *field extensions*, which you can learn about in a future abstract algebra course.

"Legal" in the sense that it does not contradict the field axioms.

The smallest field containing $\mathbb{Q}$ and $\sqrt{2}$ is written $\mathbb{Q}(\sqrt{2})$, and it consists of numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$. We say that $\mathbb{Q}(\sqrt{2})$ is obtained from $\mathbb{Q}$ by *adjoining* a square root of 2.

One significant difference between $\mathbb{R}$ and $\mathbb{C}$ is that real numbers can be *ordered* to produce the familiar real number line. In contrast, there is no way to arrange complex numbers in a line in a way that is compatible with the algebraic operations.

Polynomials and complex numbers

For any number system $\mathbb{F}$ (like $\mathbb{R}$ or $\mathbb{C}$), a *polynomial over* $\mathbb{F}$ *in the variable* x is an expression of the form

$$\sum_{k=0}^{n} a_k x^k$$

where $n \in \mathbb{N}$ and $a_k \in \mathbb{F}$ for each k. We write $\mathbb{F}[x]$ for the set of all polynomials over $\mathbb{F}$. Polynomials can be used to define *polynomial functions*; in fact, each polynomial $p = \sum_{k=0}^{n} a_k x^k \in \mathbb{F}[x]$ defines a function from $\mathbb{F}$ to $\mathbb{F}$ by the rule $p(c) = \sum_{k=0}^{n} a_k c^k$ for all $c \in \mathbb{F}$.

Technically, it is more convenient to define a polynomial p to be an *infinite* sequence of coefficients $(a_k)_{k\geq 0}$, where we demand that $a_k = 0$ for all but finitely many integers k. Then the largest n for which $a_n \neq 0$ is called the *degree* of p, and we write $\sum_{k=0}^{n} a_k x^k$ to represent $(a_k)_{k\geq 0}$ (By convention, the degree of the zero polynomial is $-\infty$.)

The function $c \mapsto p(c)$ is so closely connected to the polynomial p that the two are often given the same name.

The numbers a_k are called *coefficients*, and the largest k such that $a_k \neq 0$ is called the *degree* of the polynomial p, written $\deg(p)$. If $\sum_{k=0}^{n} a_k x^k$ is a polynomial of degree n, then a_n is called the *leading coefficient* of p, and p is called *monic* if $a_n = 1$.

Usually when we write $p = \sum_{k=0}^{n} a_k x^k$, we implicitly mean that $a_n \neq 0$, so that $n = \deg(p)$.

Polynomials can be added and multiplied together in the usual way, and writing p as a product of polynomials of smaller degree is called *factoring* p. For any $c \in \mathbb{F}$, the (degree one) polynomial $x - c$ is a factor of p if and only if c is a *root* of p, meaning that $p(c) = 0$.

Historically significant polynomials you may encounter include $x^2 - 2$, $x^2 + 1$, $8x^3 - 6x - 1$, and $x^5 - x - 1$.

Polynomials of degree 1, 2, and 3 are called *linear*, *quadratic*, and *cubic*, respectively. By the well-known quadratic formula, the complex roots of the quadratic polynomial $q(x) = ax^2 + bx + c$ are

$$r_{\pm} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

This was first proved by Descartes.

Warning: this meaning of the term "linear" is not the same as its usual meaning in a linear algebra course! A "linear" (i.e., degree one) polynomial is usually *not* a linear transformation from $\mathbb{R}$ to $\mathbb{R}$. (In fact, when is it?)

These roots are real if and only if $b^2 - 4ac \geq 0$, in which case q factors (over $\mathbb{R}$) into a product $q(x) = (x - r_+)(x - r_-)$ of linear terms, where r_+ and r_- are the real roots of q. If $b^2 - 4ac < 0$, q is called *irreducible* and cannot be factored (over $\mathbb{R}$) into a product of linear terms. Here are some important facts about polynomials with real coefficients:

The quantity $b^2 - 4ac$ is called the *discriminant* of $ax^2 + bx + c$.

- Every polynomial $p \in \mathbb{R}[x]$ of odd degree has a real root.

This follows from the Intermediate Value Theorem.

- For every polynomial $p \in \mathbb{R}[x]$ and complex number $z \in \mathbb{C}$, z is a root of p if and only if $\bar{z}$ is a root of p.

Here's the proof idea: $p(\bar{z}) = \sum a_k \bar{z}^k = \sum a_k \overline{z^k} = \sum \overline{a_k z^k} = \overline{\sum a_k z^k} = \overline{p(z)}$.

- Every polynomial $p \in \mathbb{R}[x]$ factors into a product of linear terms and irreducible quadratic terms.

Can you prove this using the previous fact and the Fundamental Theorem of Algebra?

Complex vector spaces

In many introductory linear algebra courses, it is built into the definition of *vector space* that scalars are always real numbers. But, in fact, it makes sense to define vector spaces using scalars that belong to other fields, like $\mathbb{C}$ or $\mathbb{Q}$. You might see a fuller treatment of complex vector spaces and of linear algebra over other fields in courses like Math 296, 297, 420, or 493.

Vector spaces that use real scalars are called *real vector spaces*, or *vector spaces over* $\mathbb{R}$, while vector spaces that use complex scalars are called *complex vector spaces*, or *vector spaces over* $\mathbb{C}$.

What is the dimension of $\mathbb{C}$ considered as a vector space over $\mathbb{R}$? Over $\mathbb{C}$? Over (warning: this may hurt your head) $\mathbb{Q}$?

Notation

We list[1] here some of the common notation you will encounter in both these worksheets and your undergraduate mathematics courses.

[1] If this document were a book, this section would be printed on the endpaper.

Set theory is the basis of most things mathematical. Suppose A, B, and C are sets while x is an object. The commonly used symbols of set theory are described below.

The basics of set theory are discussed in *The Joy of Sets* on page 49.

$x \in A$	x is an element of A
$x \notin A$	x is not an element of A
$B \subset C$	B is a subset of C
$B \subseteq C$	B is a subset of C
$A \subsetneq C$	A is a proper subset of C
$A \cap B$	the intersection of A and B
$A \cup B$	the union of A and B
$A \setminus B$	the set difference of A and B
A^c	the complement of A
$\emptyset$	the emptyset

Quantifiers allow us to specify the "quantity" of objects under consideration. The existential and universal quantifiers appear throughout mathematics.

The basics of working with quantifiers, including how to negate statements involving quantifiers, are discussed in *Mathematical Hygiene* on page 53.

$\exists$	existential quantifier	there exists
$\forall$	universal quantifier	for all

nb: the words "such that" are often paired with the words "there exists".

Some sets are so common that people often forget to properly introduce them when they appear. Here is a partial list of such sets.

$\mathbb{N}$	the set of natural numbers
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{C}$	the set of complex numbers
$\mathcal{P}(A)$	the power set of a set A
2^A	the power set of a set A
$A \times B$	the Cartesian product of sets A and B

Power sets and Cartesian products are discussed in *More Joy of Sets* on page 57.

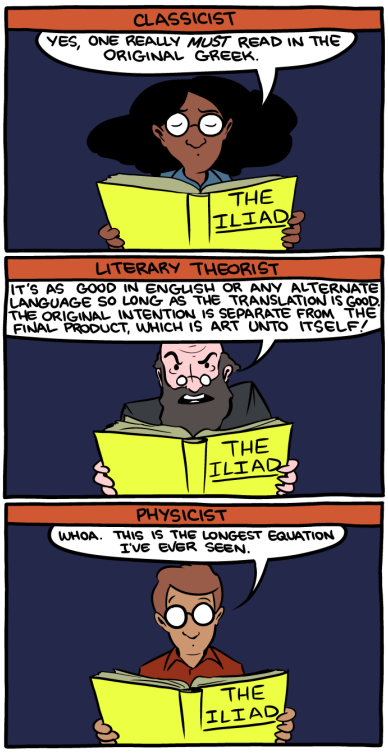
THE NOTATIONAL CONVENTIONS FOR FUNCTIONS are not universally agreed upon. We list here some popular conventions. Suppose S, T, and U are sets and $f\colon S \to T$ and $g\colon T \to U$ are functions.

Functions are discussed in *More Joy of Sets* on page 57.

S	the source or domain of f
$\mathrm{dom}(f)$	the source or domain of f
T	the target or codomain of f
$\mathrm{cod}(f)$	the target or codomain of f
$\mathrm{im}(f)$	the forward image of f
$g \circ f$	the composition of g with f
$f[A]$	the forward image of a set $A \subset S$
$f^{-1}[B]$	the preimage of a set $B \subset T$

THE ENGLISH LANGUAGE HAS 26 LETTERS; this is too limiting for math, science, and engineering. The Greek alphabet, whose elements are listed below, is a common source of additional symbols.

A	α	alpha	N	ν	nu
B	β	beta	Ξ	ξ	xi
Γ	γ	gamma	O	o	omicron
Δ	δ	delta	Π	π	pi
E	ε	epsilon	P	ρ	rho
Z	ζ	zeta	Σ	σ	sigma
H	η	eta	T	τ	tau
Θ	θ	theta	Υ	υ	upsilon
I	ι	iota	Φ	φ	phi
K	κ	kappa	X	χ	chi
Λ	λ	lambda	Ψ	ψ	psi
M	μ	mu	Ω	ω	omega



An *SMBC* comic by Zach Weinersmith
www.smbc-comics.com

Some Suggestions for Further Reading

Lara Alcock. *How to Study as a Mathematics Major*. Oxford University Press, 2013.

> "Every year, thousands of students declare mathematics as their major. Many of these students are extremely intelligent and hardworking. However, even the best struggle with the demands of making the transition to advanced mathematics. Some struggles are down to the demands of increasingly independent study. Others, however, are more fundamental: the mathematics shifts in focus from calculation to proof, and students are thus expected to interact with it in different ways. These changes need not be mysterious – mathematics education research has revealed many insights into the adjustments that are necessary – but they are not obvious and they do need explaining.
> This book aims to offer such explanation for a student audience . . . " (page v).

Jeremy Avigad, Robert Y. Lewis, and Floris van Doorn. *Logic and Proof*. `https://leanprover.github.io/logic_and_proof/index.html`, 2021.

Ethan D. Bloch. *Proofs and Fundamentals*. Springer, 2011.

> "This book is designed to bridge the large conceptual gap between computational courses such as calculus, usually taken by first and second year college students, and more theoretical courses such as linear algebra, abstract algebra and real analysis, which feature rigorous definitions and proofs of a type not usually found in calculus and lower level courses. . . .
> Though we emphasize proofs in this book, serious mathematics (contrary to a popular misconception) is not 'about' proofs and logic any more than serious literature is 'about' grammar, or music is 'about' notes. Mathematics is the study of some fascinating ideas and insights concerning such topics as numbers, geometry, counting, etc. Ultimately, intuition and imagination are as valuable in mathematics as rigor. Both mathematical intuition and facility with writing proofs can be developed with practice, just as artists and musicians develop their creative skills through training and practice." (page xiii).

Gary Chartrand, Albert D. Polimeni, and Ping Zhang. *Mathematical Proofs: A Transition to Advanced Mathematics*. Pearson, 2018.

> "As the teaching of calculus in many colleges and universities has become more problem oriented with added emphasis on the use of calculators and computers, the theoretical gap between the material presented in calculus and the mathematical background expected (or at least hoped for) in advanced calculus and other more advanced courses has widened. In an attempt to narrow this gap and to better prepare students for the more abstract mathematics courses to follow, many colleges and universities have introduced courses that are now commonly called 'transition courses.' In these courses, students are introduced to problems whose solution involves mathematical reasoning and a knowledge of proof

techniques, where writing clear proofs is emphasized. . . . This textbook has been written for such a course." (page viii).

Daniel W. Cunningham. *A Logical Introduction to Proof*. Springer, 2012.

"Each student of mathematics needs to learn how to find and write mathematical proofs. These are probably two of the most difficult skills that a mathematics major has to develop. Students often fail to construct a proof of a mathematical statement because they lack confidence or just do not know how to get started. This text is designed to increase students confidence . . . Even with a guide, the work required to find a proof can be quite challenging. Professional mathematicians also have difficulty finding proofs; however, mathematicians know that persistence often pays off and thus, they do easily not give up." (page vi).

Antonella Cupillari. *The Nuts and Bolts of Proofs*. Academic Press, 2001.

"The purpose of these notes is to help the reader to gain a better understanding of the basic logic of mathematical proofs and to become familiar with some of the basic steps needed to construct proofs. Thus the mathematical statements to be proved have been kept simple with these goals in mind. It is just like learning where the chords are, before being able to play a nice piece of music!" (page xi).

Ulrich Daepp and Pamela Gorkin. *Reading, Writing, and Proving: A Closer Look at Mathematics*. Springer, 2003.

"In our experience, students beginning this course have little training in rigorous mathematical reasoning; they need guidance. At the end, they are where they should be; on their own. Our aim is to teach the students to read, write, and do mathematics independently, and to do it with clarity, precision, and care. If we can maintain the enthusiasm they have for the subject, or even create some along the way, our book has done what it was intended to do." (page vii).

Larry J. Gerstein. *Introduction to Mathematical Structures and Proofs*. Springer, 2012.

"Students who are new to higher mathematics are often startled to discover that mathematics is a subject of *ideas*, and not just formulaic rituals, and that they are now expected to understand and create mathematical proofs. . . .
Students need experience in working with abstract ideas at a nontrivial level if they are to achieve the sophisticated blend of knowledge, discipline, and creativity that we call 'mathematical maturity.' I don't believe that 'theorem-proving' can be taught any more than 'question-answering' can be taught. Nevertheless, I have found that it is possible to guide students gently into the process of mathematical proof in such a way that they become comfortable with the experience and begin asking themselves questions that will lead them in the right direction. As with learning to swim or ride a bicycle, there are usually anxieties to be overcome; and . . . it takes a while for students to come to believe that they may be capable of solving a problem even when no instantaneous solution presents itself. " (page vii).

Richard Hammack. *Book of Proof - Third Edition*. `http://www.people.vcu.edu/~rhammack/BookOfProof/`, 2013.

"Until this point in your education, mathematics has probably been presented as a primarily computational discipline. You have learned to solve equations, compute derivatives and integrals, multiply matrices and find determinants; and you have seen how these things can answer practical questions about the real world. In this setting your primary goal in using mathematics has been to compute answers.

But there is another side of mathematics that is more theoretical than computational. Here the primary goal is to understand mathematical structures, to prove mathematical statements, and even to invent or discover new mathematical theorems and theories. The mathematical techniques and procedures that you have learned and used up until now are founded on this theoretical side of mathematics. For example, in computing the area under a curve, you use the fundamental theorem of calculus. It is because this theorem is true that your answer is correct. However, in learning calculus you were probably far more concerned with how that theorem could be applied than in understanding why it is true. But how do we know it is true? How can we convince ourselves or others of its validity? Questions of this nature belong to the theoretical realm of mathematics. This book is an introduction to that realm. " (page viii).

Kevin Houston. *How to Think Like a Mathematician: A Companion to Undergraduate Mathematics*. Cambridge University Press, 2009.

"The aim of this book is to divulge the secrets of how a mathematician actually thinks. As I went through my mathematical career, there were many instances when I thought, 'I wish someone had told me that earlier.' This is a collection of such advice. Well, I hope it is more than such a collection. I wish to present an attitude – a way of thinking and doing mathematics that works – not just a collection of techniques (which I will present as well!)" (page 4).

Tamara J. Lakins. *The tools of mathematical reasoning*. American Mathematical Society, Providence, RI, 2016.

"... this type of course is usually a completely new experience for students. It is normal to feel a bit disoriented at first. It is important to persevere. It is especially important to study *actively*, by reading the textbook equipped with pencil and paper, by writing lots of proofs, and by discussion the mathematics with your instructor and fellow students. You should never expect to simply write down a proof immediately after reading the statement to be proved. ... " (page xii).

Joseph J. Rotman. *Journey into Mathematics: An Introduction to Proofs*. Dover Publications, 2007.

"Instructors have observed, when teaching junior level [math] courses . . . that many students have difficulty out of proportion to the level of difficulty of the material. . . . The cause of this problem is plain when one considers the previous mathematics courses. . . .
My solution is a one semester intermediate course between calculus and the first courses in abstract algebra and real variables. This is not a new idea. There are many such 'transition courses' designed to prepare students for junior-level courses, but they emphasize the elements of logic (from modus ponens and truth tables through quantifiers) and set theory (from Boolean operations through relations and functions). I find this material rather dull and uninspiring, and I imagine that this feeling is shared by most students. Of course, these things should be learned eventually . . . " (page vii).

Carol Schumacher. *Chapter Zero: Fundamental Notions of Abstract Mathematics*. Pearson, 2000.

"This is a book about mathematical reasoning. That is, it is a book about the kind of thinking that mathematicians do when they are doing mathematics. Most mathematics courses through the level of elementary calculus teach students how to *use* established mathematical techniques to solve problems. This is a very good beginning, but a complete mathematical education cannot stop there. A student of mathematics must learn to discover and prove mathematical facts on her own. It takes a long time to learn how to create new mathematics. This book is designed for the beginning of the journey." (page 1) .

Douglas Smith, Maurice Eggen, and Richard St. Andre. *A Transition to Advanced Mathematics*. Thomson, 2006.

> " 'I understand mathematics but I just can't do proofs.'
> Our experience has led us to believe that the remark above, though contradictory, expresses the frustration many students feel as they pass from beginning calculus to a more rigorous level of mathematics. This book developed from a series of lecture notes for a course at Central Michigan University that was designed to address this lament." (page vi).

Daniel Solow. *How to Read and Do Proofs: An Introduction to Mathematical Thought Processes*. Wiley, 2013.

> "After finishing my undergraduate degree, I began to wonder why learning theoretical mathematics had been so difficult. As I progressed through my graduate work, I realized that mathematics possessed many of the aspects of a game – a game in which the rules had been partially concealed. Imagine trying to play chess before you know how all the pieces move! It is no wonder that so many students have trouble with abstract mathematics.
> This book describes some of the rules by which the game of theoretical mathematics is played. It has been my experience that virtually anyone who is motivated and who has a knowledge of high school mathematics can learn these rules. Doing so greatly reduces the time (and frustration) involved in learning mathematics. I hope this book serves that purpose for you." (page vii).

Ted Sundstrom. *Mathematical Reasoning: Writing and Proof*. `https://scholarworks.gvsu.edu/books/9/`, 2021.

> "[This book] is designed to be a text for the first course in the college mathematics curriculum that introduces students to the processes of constructing and writing proofs ...
> This type of course has now become a standard part of the mathematics major at many colleges and universities. It is often referred to as a 'transition course' from the calculus sequence to the upper-level courses in the major. The transition is from the problem-solving orientation of calculus to the more abstract and theoretical upper-level courses. This is needed today because many students complete their study of calculus without seeing a formal proof or having constructed a proof of their own. This is in contrast to many upper-level mathematics courses, where the emphasis is on the formal development of abstract mathematical ideas, and the expectations are that students will be able to read and understand proofs and be able to construct and write coherent, understandable mathematical proofs." (page viii).

Daniel J. Velleman. *How to Prove It: A Structured Approach*. Cambridge University Press, 2019.

> "Students of mathematics and computer science often have trouble the first time they're asked to work seriously with mathematical proofs, because they don't know the 'rules of the game.' What is expected of you if you are asked to prove something? What distinguishes a correct proof from an incorrect one? This book is intended to help students learn the answers to these questions by spelling out the underlying principles involved in the construction of proofs." (page ix).

Dave Witte Morris and Joy Morris. *Mathematical Proofs: A Transition to Advanced Mathematics*. `https://people.uleth.ca/~dave.morris/books/proofs+concepts.html`, 2016.

> "Unlike in earlier courses, success in advanced undergraduate mathematics classes (and beyond) does not depend nearly so much on being able to find the right answer to a question as it does on being able to provide a convincing explanation that the answer is correct. (Mathematicians call this explanation a **proof**.) This textbook is designed to help students acquire this essential skill ..." (from the preface).

Index