

CONTENTS

1. Wednesday, January 27	1
2. Friday, January 29	4
3. Monday, February 1	8
Discussion Questions, February 3	10
4. Friday, February 5	12
5. Monday, February 8	15
6. Wednesday, February 10	17

1. WEDNESDAY, JANUARY 27

What is a number? Certainly the things used to count sheep, money, etc. are numbers: $1, 2, 3, \dots$. We will call these the *natural numbers* and write \mathbb{N} for the set of all natural numbers

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

Since we like to keep track of debts too, we'll allow negatives and 0, which gives us the *integers*:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}.$$

(The symbol \mathbb{Z} is used since the German word for number is *zahlen*.)

Fractions should count as numbers also, so that we can talk about eating one and two-thirds of a pizza last night. We define a *rational number* to be a number expressible as a quotient of two integers: $\frac{m}{n}$ for $m, n \in \mathbb{Z}$ with $n \neq 0$. For example

$$\frac{5}{3}, \frac{2}{7}, \frac{2019}{2020}$$

are rational numbers. Of course, we often talk about numbers such as “two and a fourth”, but that the same as $\frac{9}{4}$. Every integer is a rational number just by taking 1 for the denominator; for example, $7 = \frac{7}{1}$. The set of all rational numbers is written as \mathbb{Q} (for “quotient”).

You might not have thought about it before, but an expression of the form $\frac{m}{n}$ is really an “equivalence class”: the two numbers $\frac{m}{n}$ and $\frac{a}{b}$ are deemed equal if $mb = na$. For example $\frac{6}{9} = \frac{2}{3}$ because $6 \cdot 3 = 9 \cdot 2$.

We'll talk more about decimals later on, but recall for now that a decimal that terminates is just another way of representing a rational number. For example, 1.9881 is equal to $\frac{19881}{10000}$. Less obvious is the fact that a decimal that repeats also represents a rational number: For example, $1.333\dots$ is rational (it's equal to $\frac{4}{3}$) and so is $23.91278278278\dots$. We'll see why this is true later in the semester.

Are these all the numbers there are? Maybe no one in this class would answer “yes”, but the ancient Greeks believed for a time that every number was rational. Let’s convince ourselves, as the Greeks did eventually, that there must be numbers that are not rational. Imagine a square of side length 1. By the Pythagorean Theorem, the length of its diagonal, call this number c , must satisfy

$$c^2 = 1^2 + 1^2 = 2.$$

That is, there must be a some number whose square is 2 since certainly the length of the diagonal in such a square is representable as a number. Now, let’s convince ourselves that there is no *rational number* with this property. In fact, I’ll make this a theorem.

Theorem 1.1. *There is no rational number whose square is 2.*

Preproof Discussion 1. *Before launching a formal proof, let’s philosophize about how one shows something does not exist. To show something does not exist, one proves that its existence is not possible. For example, I know that there must not be large clump of plutonium sewn into the mattress of my bed. I know this since, if such a clump existed, I’d be dead by now, and yet here I am, alive and well!*

More generally and formally, one way to prove the falsity of a statement P is to argue that if we assume P to be true then we can deduce from that assumption something that is known to be false. If you can do this, then you have proven P is false. In symbols: If one can prove

$$P \implies \text{Contradiction}$$

then the statement P must in fact be false.

In the case at hand, letting P be the statement “there is a rational number whose square is 2”, the Theorem is asserting that P is false. We will prove this by assuming P is true and deriving an impossibility.

This is known as a proof by contradiction. (Some mathematicians would actually not consider this to be a proof by contradiction. For some, a proof by contradiction refers to when the truth of a statement P is established by assuming the statement “not P ” and deducing from that a falsity.)

Proof. By way of contradiction, assume there were a rational number q such that $q^2 = 2$. By definition of “rational number”, we know that q can be written as $\frac{m}{n}$ for some integers m and n such that $n \neq 0$. Moreover, we may assume that we have written q in reduced form so that m and n have no prime factors in common. In particular, we may assume that not both of m and n are even. (If they were both even, then we could simplify the fraction by factoring out common factors

of 2's.) Since $q^2 = 2$, $\frac{m^2}{n^2} = 2$ and hence $m^2 = 2n^2$. In particular, this shows m^2 is even and, since the square of an odd number is odd, it must be that m itself is even. So, $m = 2a$ for some integer a . But then $(2a)^2 = 2n^2$ and hence $4a^2 = 2n^2$ whence $2a^2 = n^2$. For the same reason as before, this implies that n must be even. But this contradicts the fact that m and n are not both even.

We have reached a contradiction, and so the assumption that there is a rational number q such that $q^2 = 2$ must be false. \square

A version of the previous proof was known even to the ancient Greeks.

Our first major mathematical goal in the class is to make a formal definition of the real numbers. Before we do this, let's record some basic properties of the rational numbers. I'll state this as a Proposition (which is something like a minor version of a Theorem), but we won't prove them; instead, we'll take it for granted to be true based on our own past experience with numbers.

For the rational numbers, we can do arithmetic ($+$, $-$, \times , \div) and we also have a notion of size ($<$, $>$). The first seven observations below describe the arithmetic, and the last three describe the notion of size.

Proposition 1.2. *The set of rational numbers form an “ordered field”. This means that the following ten properties hold:*

- (1) *There are operations $+$ and \cdot defined on \mathbb{Q} , so that if p, q are in \mathbb{Q} , then so are $p + q$ and $p \cdot q$.*
- (2) *Each of $+$ and \cdot is a commutative operation (i.e., $p + q = q + p$ and $p \cdot q = q \cdot p$ hold for all rational numbers p and q).*
- (3) *Each of $+$ and \cdot is an associative operation (i.e., $(p + q) + r = p + (q + r)$ and $(p \cdot q) \cdot r = p \cdot (q \cdot r)$ hold for all rational numbers p , q , and r).*
- (4) *The number 0 is an identity element for addition and the number 1 is an identity element for multiplication. This means that $0 + q = q$ and $1 \cdot q = q$ for all $q \in \mathbb{Q}$.*
- (5) *The distributive law holds: $p \cdot (q + r) = p \cdot q + p \cdot r$ for all $p, q, r \in \mathbb{Q}$.*
- (6) *Every number has an additive inverse: For any $p \in \mathbb{Q}$, there is a number $-p$ satisfying $p + (-p) = 0$.*
- (7) *Every nonzero number has a multiplicative inverse: For any $p \in \mathbb{Q}$ such that $p \neq 0$, there is a number p^{-1} satisfying $p \cdot p^{-1} = 1$.*
- (8) *There is a “total ordering” \leq on \mathbb{Q} . This means that*
 - (a) *For all $p, q \in \mathbb{Q}$, either $p \leq q$ or $q \leq p$.*
 - (b) *If $p \leq q$ and $q \leq p$, then $p = q$.*

- (c) For all $p, q, r \in \mathbb{Q}$, if $p \leq q$ and $q \leq r$, then $p \leq r$.
- (9) The total ordering \leq is compatible with addition: If $p \leq q$ then $p + r \leq q + r$.
- (10) The total ordering \leq is compatible with multiplication by non-negative numbers: If $p \leq q$ and $r \geq 0$ then $pr \leq qr$.

2. FRIDAY, JANUARY 29

Which of the properties from Proposition 1.2 does \mathbb{N} satisfy?

The commutativity, associativity, distributive law, multiplicative identity, and all of the ordering properties are true for \mathbb{N} . There is one other important property of \mathbb{N} , which we accept to be true without proof. Such a property is called an axiom.

Axiom 2.1 (Well-ordering axiom). *Every nonempty subset of \mathbb{N} has a smallest element (which we call its minimum).*

As we will discuss later, the well-ordering axiom is closely related to the principle of induction.

Example 2.2. For the set of all even multiples of 7, $S = \{7 \cdot (2n) \mid n \in \mathbb{N}\}$, we have $\min(S) = 14$.

We expect everything from Proposition 1.2 to be true for the real numbers. We will build them into our definition. To define the real numbers \mathbb{R} , we take the ten properties listed in the Proposition to be axioms. It turns out the set of real numbers satisfies one key additional property, called the *completeness axiom*, which I cannot state yet.

Axioms. *The set of all real numbers, written \mathbb{R} , satisfies the following eleven properties:*

- (Axiom 1) *There are operations $+$ and \cdot defined on \mathbb{R} , so that if $x, y \in \mathbb{R}$, then so are $x + y$ and $x \cdot y$.*
- (Axiom 2) *Each of $+$ and \cdot is a commutative operation.*
- (Axiom 3) *Each of $+$ and \cdot is an associative operation.*
- (Axiom 4) *The real number 0 is an identity element for addition and the real number 1 is an identity element for multiplication. This means that $0 + x = x$ and $1 \cdot x = x$ for all $x \in \mathbb{R}$.*
- (Axiom 5) *The distributive law holds: $x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in \mathbb{R}$.*
- (Axiom 6) *Every real number has an additive inverse: For any $x \in \mathbb{R}$, there is a number $-x$ satisfying $x + (-x) = 0$.*
- (Axiom 7) *Every nonzero real number has a multiplicative inverse: For any $x \in \mathbb{R}$ such that $x \neq 0$, there is a real number x^{-1} satisfying $x^{-1} \cdot x = 1$.*

- (Axiom 8) *There is a “total ordering” \leq on \mathbb{R} . This means that*
- (a) *For all $x, y \in \mathbb{R}$, either $x \leq y$ or $y \leq x$.*
 - (b) *If $x \leq y$ and $y \leq z$, then $x \leq z$.*
 - (c) *For all $x, y, z \in \mathbb{R}$, if $x \leq y$ and $y \leq z$, then $x \leq z$.*
- (Axiom 9) *The total ordering \leq is compatible with addition: If $x \leq y$ then $x + z \leq y + z$ for all z .*
- (Axiom 10) *The total ordering \leq is compatible with multiplication by non-negative real numbers: If $x \leq y$ and $z \geq 0$ then $zx \leq zy$.*
- (Axiom 11) *The completeness axiom holds. (I will say what this means later.)*

There are many other familiar properties that are consequences of this list of axioms. As an example we can deduce the following property:

“Cancellation of Addition”: If $x + y = z + y$ then $x = z$.

Let’s prove this carefully, using just the list of axioms: If $x + y = z + y$ then we can add $-y$ (which exists by Axiom 6) to both sides to get $(x+y)+(-y) = (z+y)+(-y)$. This can be rewritten as $x+(y+(-y)) = z+(y+(-y))$ (Axiom 3) and hence as $x+0 = z+0$ (Axiom 6), which gives $x = z$ (Axiom 4 and Axiom 2).

For another example, we can deduce the following fact from the axioms:

$$r \cdot 0 = 0 \text{ for any real number } r.$$

Let’s prove this carefully: Let r be any real number. We have $0+0 = 0$ (Axiom 4) and hence $r \cdot (0+0) = r \cdot 0$. But $r \cdot (0+0) = r \cdot 0 + r \cdot 0$ (Axiom 5) and so $r \cdot 0 = r \cdot 0 + r \cdot 0$. We can rewrite this as $0 + r \cdot 0 = r \cdot 0 + r \cdot 0$ (Axiom 4). Now apply the Cancellation of Addition property (which we previously deduced from the axioms) to obtain $0 = r \cdot 0$.

As I said, there are many other familiar properties of the real numbers that follow from these axioms, but I will not list them all. The great news is that all of these familiar properties follow from this short list of axioms. We will prove a couple, but for the most part, I’ll rely on your innate knowledge that facts such as $r \cdot 0 = 0$ hold.

I owe you a description of the very important Completeness Axiom, and it will take a bit of time to do so. Before we get to this, it will be helpful to review set notation, and some basics of proof-writing.

Often, sets are described as subsets of other larger sets, by specifying properties. For example, when I write

$$S = \{m \in \mathbb{Z} \mid m = a^2 \text{ for some } a \in \mathbb{Z}\}$$

I am specifying a subset of the set of all integers \mathbb{Z} . In words, S is: “the set of those integers that are equal to the square of some integer”. We

could also write this set out by listing its elements:

$$S = \{0, 1, 4, 9, 16, 25, 36, \dots\}.$$

It's safer in general to use the former description, since you don't have to worry about the reader getting the pattern.

The previous is an example of a subset of \mathbb{Z} , but we will mostly be concerned with subsets of \mathbb{R} . For example, we might consider the set

$$\{x \in \mathbb{R} \mid x^2 < 2\}.$$

We will also deal with “intervals” a lot. When I write $(0, 1)$ I mean the set $\{x \in \mathbb{R} \mid 0 < x < 1\}$. That is, it is all real numbers strictly between 0 and 1.

More generally, if a, b are real numbers and $a < b$, then

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$$

(What if $b \leq a$?) The set (a, b) is called an *open interval*.

We also have $[a, b]$, known as a *closed interval* and defined to be

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}.$$

We also have $[a, b)$, $(a, b]$, (a, ∞) , $[a, \infty)$, $(-\infty, b)$, and $(-\infty, b]$, all of which you probably have seen before.

We will also have need to consider sets defined in more complicated ways such as

$$S = \{1 - \frac{1}{n} \mid n \in \mathbb{N}\}.$$

The latter is a bit different than the previous examples. The previous ones had form $\{\text{element of a set} \mid \text{property holds}\}$, but this one has the form $\{\text{expression involving symbols} \mid \text{allowable values of these symbols}\}$. Explicitly, this example is the set $\{0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \dots\}$.

Recall also a few ways of making sets from others:

- union : $S \cup T = \{x \mid x \in S \text{ or } x \in T\}$
- intersection : $S \cap T = \{x \mid x \in S \text{ and } x \in T\}$
- set difference : $S \setminus T = \{x \mid x \in S \text{ and } x \notin T\}$.

Let's now talk a bit more about rules of logic, methods of proof, quantification, etc. Our book has a very nice treatment of these topics in Sections 1.4 and 1.5. Part of the next problem set will involve your reading these sections on your own and doing some of the exercises. Here, I'll just give some highlights.

Let me start with some rules of logic, and how that affects proofs. First, a *statement* is a sentence (or sometimes sequence of sentences) that is either true or false. Things like “Jack's shirt is ugly” is not a statement, nor is “Go Huskers!”. But “All odd numbers are prime” is a statement — it happens to be false. The sentence

“The digit 9 occurs infinitely often in the decimal expansion of π .”

is a statement, as it is surely either true or false. But, no one knows which!

An odder example is “This sentence is false”. Is it a statement? (Is it true? Is it false?) No!

If P and Q are any two statements, then we can form compound statements from them such as

- P and Q .
- P or Q .
- Not P .
- If P then Q .

The “truth values” for the first three are pretty clear, but be careful about the last.

- “ P and Q ” is a true statement when both P and Q are true statements.
- “ P or Q ” is a true statement when either P or Q is a true statement.
- “Not P ” is true when P is a false statement.
- “If P then Q ” is true when P is false or Q is true. In other words “If P then Q ” is logically equivalent to “not P or Q ”.

Which of the following are true?

- (1) If $1 + 1 = 1$, then I am the pope.
- (2) If 8 is prime then every real number is an integer.
- (3) If my name is Jack then I am the pope.
- (4) If it had been raining this morning then I would have brought an umbrella with me to class.

All but the third are true.

Most of the statements that we consider are, or can be framed as if-then statements: anything with hypotheses and a conclusion is an if-then statement. How do we prove such a statement? To give a “direct proof” of “if P then Q ” we:

- (1) Assume P ,
- (2) Do some stuff, then
- (3) Conclude Q .

For example, the Goldbach Conjecture posits that if n is an even integer greater than 2, then n is a sum of two primes. (A conjecture is a statement that people believe to be true based on some evidence, but is not proven.) I can’t prove this conjecture, but I can tell you the

first and last sentence of a proof: “Assume that n is an even integer. . . . Thus, n is a sum of two primes.”

3. MONDAY, FEBRUARY 1

As I said earlier, “If P then Q ” is the same as “not P or Q ”. It follows that “If not Q then not P ” is the same as “not not Q or not P ” and hence is the same as “not P or Q ”. That is:

“If P then Q ” is logically equivalent to “If not Q then not P ”.

“If not Q then not P ” is known as the *contrapositive* of “If P then Q ”. So, an if-then statement and its contrapositive are logically equivalent.

Often when proving an if-then statement, it works a bit better to give a “direct” proof of the contrapositive. That is, in a proof of “If P then Q ” *by contraposition* we:

- (1) Assume not Q ,
- (2) Do some stuff, then
- (3) Conclude not P .

Example 3.1. An *irrational number* is a real number that is not rational. Consider the following assertion:

Let r be any rational number and let x be any real number. If x is irrational then $x + r$ is irrational.

This is logically equivalent to:

Let r be any rational number and let x be any real number. If $x + r$ is rational then x is rational.

Let us prove the latter statement “directly”: Let r be any rational number and let x be any real number. Suppose $x + r$ is rational. Then since r is rational, $-r$ is also rational (by Proposition 1.2, part (6)). It follows that $(x + r) + (-r)$ is also rational (by Proposition 1.2, part (1)) and hence $(x + r) + (-r) = x + (r + (-r)) = x + 0 = x$ is rational.

Never, ever, ever, ever confuse the contrapositive of an if-then statement with its *converse*. The converse of “If P then Q ” is “If Q then P ”.

Example 3.2. Give examples of statements that are true whose converses are false.

Recall that when we say “ P if and only if Q ” we mean “If P then Q , and if Q then P ”. In other words, an “if and only if” statement includes both an if-then statement and its converse. The statement “ P if and only if Q ” is true when either P and Q are both true or P and Q are both false, and it is false in the other two cases, when one

is true and the other is false. A proof of such a statement generally has two parts, one where we prove P implies Q (either directly or by contraposition) and one where we prove Q implies P (again either directly or by contraposition).

Let me also say a bit about quantification: This refers to usage of “for every” or “there exists”. For example, “For every real number x , x^2 is strictly positive” and “There exists an even integer that is prime”.

“For every” statements are sometimes better cast as if-then statements. For example, the first one above is equivalent to “If x is a real number, then x^2 is strictly positive”. So, be aware that sometimes, as in this example, there is an implicit “For every” clause lurking about even if you don’t see those words written.

The negation of a “for every” clause usually involves “there exists”. For example the negation of “For every real number x , x^2 is strictly positive.” is “There is a real number x such that x^2 is not strictly positive”.

The negation of a “there exists” statement usually involves “for every”. For example, the negation of “There is an even integer that is prime” is “For every even integer n , n is not prime” or better “If n is an even integer, then n is not prime”.

In general,

- the negation of “For every $x \in S$, P ” is “There exists $x \in S$ such that not P ”;
- the negation of “There exists $x \in S$ such that P ” for some statement P is “For every $x \in S$, not P ”.

How do we prove statements with quantifiers? To prove “For every $x \in S$, P ” , we

- (1) Take an arbitrary $x \in S$,
- (2) Do some stuff, then
- (3) Conclude that P holds for x .

In the first step we specify one element of S , but we *don’t get to decide which one*. In particular, its name should be a variable, rather than the name of any specific element in S .

To *disprove* “For every $x \in S$, P ” we can give a counterexample. That means that we get to choose an element of S , and show that P fails for our choice.

To prove “There exists $x \in S$ such that P ” , we just need to give an example: we can choose any element of S and show that P holds for that element.

Things get harder when we combine “for every” and “there exist” clauses in one statement. One very important point here is that order matters a lot. For example,

“For every $n \in \mathbb{N}$ there is an $m \in \mathbb{N}$ such that $n < m$ ”

and

“There is an $m \in \mathbb{N}$ such that for every $n \in \mathbb{N}$, $n < m$ ”

have very different meanings. In fact, the first is clearly true (since given an n one could, for example, take $m = n + 1$) and the second is false.

Never interchange the positions of “for every” and “there exist” unless you intend to change the meaning!

When we combine “for every” and “there exist” clauses with a negation things can also get confusing. For example: the negation of “For every integer m there is an integer n such that $n > m$ ” is “There exists an integer m such that for every integer n , $n \leq m$.”

Using symbols sometimes helps focus attention on the underlying logic. We write \forall and \exists in place of “for every” and “there exists”, sometimes. For example the negation of “ $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}$ such that $n > x$ ” is “ $\exists x \in \mathbb{R}$ such that $\forall n \in \mathbb{N}, n \leq x$ ”

DISCUSSION QUESTIONS, FEBRUARY 3

- Write the contrapositive, and the converse of each statement. Is the statement true or false? Is the converse true or false? Explain why (but don’t write a full proof). For each statement below, a, b are real numbers.

◇ If a is irrational, then $1/a$ is irrational.

Contrapositive: “If $1/a$ is rational, then a is rational.

[True]

Converse: “If $1/a$ is irrational, then a is irrational.

[True]

◇ If a and b are both irrational, then ab is irrational.

Contrapositive: “If ab is rational, then either a or b is rational. [False]

Converse: “If ab is irrational, then a and b are both irrational. [False]

◇ If $x > 3$ then $x^2 > 9$.

Contrapositive: “If $x^2 \leq 9$, then $x \leq 3$. [True]
 Converse: “If $x^2 > 9$, then $x > 3$. [False]”

- Write the negation of each statement. Is the statement true or false? Explain why (but don’t write a full proof).

◇ $\exists x \in \mathbb{Q}: x^2 = 2$.

Negation: $\forall x \in \mathbb{Q}, x^2 \neq 2$. [The original is false.]

◇ $\forall x \in \mathbb{Q}, x^2 > 0$.

Negation: $\exists x \in \mathbb{Q}, x^2 \leq 0$. [The original is false.]

◇ $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}: xy = 1$.

Negation: $\exists x \in \mathbb{R} : \forall y \in \mathbb{R}, xy \neq 1$. [The original is false.]

◇ $\exists x \in \mathbb{R}: \forall y \in \mathbb{R}, e^y < x$.

Negation: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : e^y \geq x$. [The original is false.]

◇ $\exists x \in \mathbb{R}: \forall y \in \mathbb{R}, \sin(y) < x$.

Negation: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R} : \sin(y) \geq x$. [The original is true.]

- Prove the following statements using the axioms of \mathbb{R} and facts we have proven in class.

◇ Let x be a real number. If there is a real number y such that $xy = 1$, then x is nonzero.¹

We argue the contrapositive. Let x be zero. Then, for any $y \in \mathbb{R}$, we have $xy = 0$, by a fact we proved in class. In particular, we have $xy \neq 1$, as required.

◇ If x is a nonzero real number, then x^2 is also nonzero.²

¹Hint: Consider the contrapositive of this statement.

²Hint: Use x^{-1} and the previous statement.

Let x be a nonzero real number. By Axiom 7, there is an element $x^{-1} \in \mathbb{R}$ such that $xx^{-1} = 1$. Then $x^2 \cdot (x^{-1})^2 = (xx^{-1})(xx^{-1}) = 1$, using Axioms 2 and 3 in the first equality and Axiom 5 in the second. By the previous fact (using $y = (x^{-1})^2$) we conclude that $x^2 \neq 0$.

◇ For any real number x , $x \geq 0$ if and only if $-x \leq 0$.³

Let $x \geq 0$. Adding $(-x)$ to both sides (which exists by Axiom 6), we obtain $0 = x + (-x) \geq 0 + (-x) = -x$ (by Axiom 9 and Axiom 5). Conversely, let $-x \leq 0$. Adding x to both sides, we obtain $0 = x + (-x) \leq x + 0 = x$ (by Axiom 9 and Axiom 5).

◇ $0 \leq 1$.⁴

To obtain a contradiction, suppose that $1 < 0$. Then $0 = -1 + 1 < -1 + 0 = -1$. By the previous fact, we then have $1 > 0$, which contradicts the hypothesis.

◇ For any real number x , $(-1) \cdot x = -x$.

Observe that

$$x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 + -1) \cdot x = 0 \cdot x = 0.$$

We also have $x + (-x) = 0$, so $x + (-1)x = x + (-x)$. By cancellation of addition, we conclude that $(-1)x = -x$.

◇ The product of two negative real numbers is nonnegative.

4. FRIDAY, FEBRUARY 5

Definition 4.1. Let S be any subset of \mathbb{R} . A real number b is called an *upper bound* of S provided that for every $s \in S$, we have $s \leq b$.

For example, the number 1 is an upper bound for the set $(0, 1)$. The number 182 is also an upper bound of this set and so is π . It is pretty clear that 1 is the “best” (i.e., smallest) upper bound for this set, in the sense that every other upper bound of $(0, 1)$ must be at least as big as 1. Let’s make this official:

³Hint: Add something to both sides.

⁴Hint: Try a proof by contradiction and use the previous fact.

Proposition 4.2. *If b is an upper bound of the set $(0, 1)$, then $b \geq 1$.*

I will prove this claim using just the axioms of the real numbers (in fact, I will only use the first 10 axioms):

Proof. Suppose b is an upper bound of the set $(0, 1)$. By way of contradiction, suppose $b < 1$. (Our goal is to derive a contradiction from this.)

Consider the number $y = \frac{b+1}{2}$ (the average of b and 1). I will argue that $b < y$ and $b \geq y$, which is not possible.

Since we are assuming $b < 1$, we have $\frac{b}{2} < \frac{1}{2}$ and hence

$$b = \frac{2b}{2} = \frac{b}{2} + \frac{b}{2} < \frac{b}{2} + \frac{1}{2} = \frac{b+1}{2} = y.$$

So, $b < y$.

Similarly,

$$1 = \frac{1+1}{2} > \frac{b+1}{2} = y$$

so that

$$y < 1.$$

Since $\frac{1}{2} \in S$ and b is an upper bound of S , we have $\frac{1}{2} \leq b$. Since we already know that $b < y$, it follows that $\frac{1}{2} < y$ and hence $0 < y$. We have proven that $y \in (0, 1)$. But, remember that b is an upper bound of $(0, 1)$, and so we get $y \leq b$ by definition.

To summarize: given an upper bound b of $(0, 1)$, starting with the assumption that $b < 1$, we have deduced the existence of a number y such that both $b < y$ and $y \leq b$ hold. As this is not possible, it must be that $b < 1$ is false, and hence $b \geq 1$. \square

This claim proves the (intuitively obvious) fact that 1 is “least upper bound” of the set $(0, 1)$. The notion of “least upper bound” will be an extremely important one in this class.

Definition 4.3. A subset S of \mathbb{R} is called *bounded above* if there exists at least one upper bound for S . That is, S is bounded above provided there is a real number b such that $s \leq b$ for all $s \in S$.

For example, $(0, 1)$ is bounded above, by for example 50.

The subset \mathbb{N} of \mathbb{R} is not bounded above — there is no real number that is larger than every natural number. This fact is surprisingly non-trivial to deduce just using the axioms; in fact, one needs the Completeness Axiom to show it. But of course our intuition tells us that it is obviously true.

Let’s give a more interesting example of a subset of \mathbb{R} that is bounded above.

Example 4.4. Define S to be those real numbers whose squares are less than 2:

$$S = \{x \in \mathbb{R} \mid x^2 < 2\}.$$

I claim S is bounded above. In fact, I'll prove 2 is an upper bound: Suppose $x \in S$. If $x > 2$, then $x \cdot x > x \cdot 2$ and $x \cdot 2 > 2 \cdot 2$, and hence $x^2 > 4 > 2$. This contradicts the fact that $x \in S$. So, we must have $x \leq 2$.

A nearly identical argument shows that 1.5 is also an upper bound (since $1.5^2 = 2.25 > 2$) and similarly one can show 1.42 is an upper bound. But 1.41 is not an upper bound. For note that $1.411^2 = 1.99091$ and so $1.41 \in S$ but $1.411 > 1.41$.

Question: What is the smallest (or least) upper bound for this set S ? Clearly, it ought to be $\sqrt{2}$ (i.e., the positive number whose square is equal to exactly 2), but there's a catch: how do we know that such real number exists?

Definition 4.5. Suppose S is subset of \mathbb{R} that is bounded above. A *supremum* (also known as a *least upper bound*) of S is a number ℓ such that

- (1) ℓ is an upper bound of S (i.e., $s \leq \ell$ for all $s \in S$) and
- (2) if b is any upper bound of S , then $\ell \leq b$.

Example 4.6. 1 is a supremum of $(0, 1)$. Indeed, it is clearly an upper bound, and in the "Claim" above, we proved that if b is any upper bound of $(0, 1)$ then $b \geq 1$. Note that this example shows that a supremum of S does not necessarily belong to S .

Example 4.7. I claim 1 is a supremum of $(0, 1] = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$. It is by definition an upper bound. If b is any upper bound of $(0, 1]$ then, since $1 \in (0, 1]$, by definition we have $1 \leq b$. So 1 is the supremum of $(0, 1]$.

The subset \mathbb{N} does not have a supremum since, indeed, it does not have any upper bounds at all.

Can you think of an example of a set that is bounded above but has no supremum? There is only one such example and it is rather silly: the empty set is bounded above. Indeed, every real number is an upper bound for the empty set. So, there is no least upper bound.

Having explained the meaning of the term "supremum", I can finally state the all-important completeness axiom:

Axiom (Completeness Axiom). *Every nonempty, bounded-above subset of \mathbb{R} has a supremum.*

5. MONDAY, FEBRUARY 8

Note that I keep saying *a* supremum of a set, but in fact, when they exist, there is only one possible supremum of a given set.

Proposition 5.1. *If a subset of \mathbb{R} has a supremum, then it is unique.*

Preproof Discussion 2. *The proposition has the general form “If a thing with property P exists, then it is unique”.*

How do we prove a statement such as “If a thing with property P exists, then it is unique”? We argue that if two things x and y both have property P , then x and y must be the same thing.

Proof. Suppose both x and y are both suprema of the same subset S of \mathbb{R} . Then, since y is an upper bound of S and x is a supremum of S , by part (2) of the definition of “supremum” we have $y \geq x$. Likewise, since x is an upper bound of S and y is a supremum of S , we have $x \geq y$ by definition. Since $x \leq y$ and $y \leq x$, we conclude $x = y$. \square

From now on we will speak of *the* supremum of a set (when it exists).

Let us now explore consequences of the completeness axiom. First up, we show that it implies that $\sqrt{2}$ really exists:

Proposition 5.2. *There is a positive real number whose square is 2.*

Proof. Define S to be the subset

$$S = \{x \in \mathbb{R} \mid x^2 < 2\}.$$

S is nonempty since, for example, $1 \in S$, and it is bounded above, since, for example, 2 is an upper bound for S , as we showed earlier. So, by the Completeness Axiom, S has a least upper bound, and we know it is unique from the proposition above. Let us call it ℓ . I will prove $\ell^2 = 2$.

We know one of $\ell^2 > 2$, $\ell^2 < 2$ or $\ell^2 = 2$ must hold. We prove $\ell^2 = 2$ by showing that both $\ell^2 > 2$ and $\ell^2 < 2$ are impossible.

We start by observing that $1 \leq \ell \leq 2$. The inequality $1 \leq \ell$ holds since $1 \in S$ and ℓ is an upper bound of S , and the inequality $\ell \leq 2$ holds since 2 is an upper bound of S and ℓ is the least upper bound of S .

Suppose $\ell^2 < 2$. We show this leads to a contradiction by showing that ℓ is not an upper bound of S in this case. We will do this by constructing a number that is ever so slightly bigger than ℓ and belongs to S . Let $\varepsilon = 2 - \ell^2$. Then $0 < \varepsilon \leq 1$ (since $\ell^2 < 2$ and $\ell^2 \geq 1$). We will now show that $\ell + \varepsilon/5$ is in S : We have

$$(\ell + \varepsilon/5)^2 = \ell^2 + \frac{2}{5}\ell\varepsilon + \frac{\varepsilon^2}{25} = \ell^2 + \varepsilon\left(\frac{2\ell}{5} + \frac{\varepsilon}{25}\right).$$

Now, using $\ell \leq 2$ and $0 < \varepsilon \leq 1$, we deduce

$$0 < \frac{2\ell}{5} + \frac{\varepsilon}{25} \leq \frac{4}{5} + \frac{\varepsilon}{25} < 1.$$

Putting these equations and inequalities together yields

$$(\ell + \frac{\varepsilon}{5})^2 < \ell^2 + \varepsilon = 2.$$

So, $\ell + \frac{\varepsilon}{5} \in S$ and yet $\ell + \frac{\varepsilon}{5} > \ell$, contradicting the fact that ℓ is an upper bound of S . We conclude $\ell^2 < 2$ is not possible.

Assume now that $\ell^2 > 2$. Our strategy will be to construct a number even so slightly smaller than ℓ , which therefore cannot be an upper bound of S , and use this to arrive at a contradiction. Let $\delta = \ell^2 - 2$. Then $0 < \delta \leq 2$ (since $\ell \leq 2$ and hence $\ell^2 - 2 \leq 2$). Since $\delta > 0$, we have $\ell - \frac{\delta}{5} < \ell$. Since ℓ is the least upper bound of S , $\ell - \frac{\delta}{5}$ must not be an upper bound of S . By definition, this means that there is $r \in S$ such that $\ell - \frac{\delta}{5} < r$. Since $\delta \leq 2$ and $\ell \geq 1$, it follows that $\ell - \frac{\delta}{5}$ is positive and hence so is r . We may thus square both sides of $\ell - \frac{\delta}{5} < r$ to obtain

$$(\ell - \frac{\delta}{5})^2 < r^2.$$

Now

$$(\ell - \frac{\delta}{5})^2 = \ell^2 - \frac{2\ell\delta}{5} + \frac{\delta^2}{25} = \delta + 2 - \frac{2\ell\delta}{5} + \frac{\delta^2}{25}$$

since $\ell^2 = \delta + 2$. Moreover,

$$\delta + 2 - \frac{2\ell\delta}{5} + \frac{\delta^2}{25} = 2 + \delta(1 - \frac{2\ell}{5} + \frac{\delta}{25}) \geq 2 + \delta(1 - \frac{4}{5} + \frac{\delta}{25})$$

since $\ell \leq 2$. We deduce that

$$\delta + 2 - \frac{2\ell\delta}{5} + \frac{\delta^2}{25} \geq 2 + \delta(\frac{1}{5}) \geq 2.$$

Putting these inequalities together gives $r^2 > 2$, contrary to the fact that $r \in S$. We conclude that $\ell^2 > 2$ is also not possible.

Since $\ell^2 < 2$ and $\ell^2 > 2$ are impossible, we must have $\ell^2 = 2$. \square

The collection of rational numbers does not satisfy the completeness axiom and indeed it is precisely the completeness axiom that differentiates \mathbb{R} from \mathbb{Q} .

Example 5.3. Within the set \mathbb{Q} the subset $S = \{x \in \mathbb{Q} \mid x^2 < 2\}$ does not have a supremum. That is, no matter which rational number you pick that is an upper bound for S , you may always find an even smaller one that is also an upper bound of S .

It is precisely the completeness axiom that assures us that everything that ought to be a number (like the length of the hypotenuse in an isosceles right triangles of side length 1) really is a number. It gives us that there are “no holes” in the real number line — the real numbers are *complete*.

For example, we can use it to prove that $\sqrt[8]{147}$ exists: Let $S = \{x \in \mathbb{R} \mid x^8 < 147\}$. Then S is nonempty (e.g., $0 \in S$) and bounded above (e.g., 50 is an upper bound) and so it must have a supremum ℓ . A proof similar to (but even messier than) the proof of Proposition 5.2 above shows that ℓ satisfies $\ell^8 = 147$.

The completeness axiom is also at the core of the Intermediate Value Theorem and many of the other major theorems we will cover in this class.

6. WEDNESDAY, FEBRUARY 10

We now discuss a few consequence of the completeness axiom.

Theorem 6.1. *If x is any real number, then there exists a natural number n such that $n > x$.*

This looks really stupid at first. How could it be false? But consider: there are examples of ordered fields, i.e. situations in which Axioms 1–10 hold, in which this Theorem is not true! So, its proof must rely on the Completeness Axiom.

Proof. Let x be any real number. By way of contradiction, suppose there is no natural number n such that $n > x$. That is, suppose that for all $n \in \mathbb{N}$, $n \leq x$. Then \mathbb{N} is a bounded above (by x). Since it is also clearly nonempty, by the Completeness Axiom, \mathbb{N} has a supremum, call it ℓ . Consider the number $y := \ell - 1$. Since $y < \ell$ and ℓ is the supremum of \mathbb{N} , y cannot be an upper bound of \mathbb{N} . So, there must be some $m \in \mathbb{N}$ such that $\ell - 1 < m$. But then by adding 1 to both sides of this inequality we get $\ell < m + 1$ and, since $m + 1 \in \mathbb{N}$, this contradicts that assumption that ℓ is the supremum of \mathbb{N} .

We conclude that, given any real number x , there must exist a natural number n such that $n > x$. \square

Corollary 6.2 (Archimedean Principle). *If $a \in \mathbb{R}$, $a > 0$ and $b \in \mathbb{R}$, then for some natural number n we have $na > b$.*

“No matter how small a is and how large b is, if we add a to itself enough times, we can overtake b .”

Proof. We apply Theorem 6.1 to the real number $x = \frac{b}{a}$. It gives that there is a natural number n such that $n > x = \frac{b}{a}$. Since $a > 0$, upon multiplying both sides by a we get $n \cdot a > b$. \square

Corollary 6.3 (Density of the Rational Numbers). *Between any two distinct real numbers there is a rational number; more precisely, if $x, y \in \mathbb{R}$ and $x < y$, then there exists $q \in \mathbb{Q}$ such that $x < q < y$.*

Proof. We will prove this by consider two cases: $x \geq 0$ and $x < 0$.

Let us first assume $x \geq 0$. We apply the Archimedean Principle using $a = y - x$ and $b = 1$. (The Principle applies as $a > 0$ since $y > x$.) This gives us that there is a natural number $n \in \mathbb{N}$ such that

$$n \cdot (y - x) > 1$$

and thus

$$0 < \frac{1}{n} < y - x.$$

Since $\frac{1}{n} > 0$, using the Archimedean principle again, there is at least one natural number p such that $p \cdot \frac{1}{n} > x$. By the Well Ordering Axiom, there is a smallest natural number such that $m \cdot \frac{1}{n} > x$; call it m .

We claim that $\frac{m-1}{n} \leq x$. Indeed, if $m > 1$, then $m - 1 \in \mathbb{N} \setminus S$ (because $m - 1$ is less than the minimum), so $\frac{m-1}{n} \leq x$; if $m = 1$, then $m - 1 = 0$, so $\frac{m-1}{n} = 0 \leq x$.

So, we have

$$\frac{m-1}{n} \leq x < \frac{m}{n}$$

By adding $\frac{1}{n}$ to both sides of $\frac{m-1}{n} \leq x$ and using that $\frac{1}{n} < y - x$, we get

$$\frac{m}{n} \leq x + \frac{1}{n} < x + (y - x) = y$$

and hence

$$x < \frac{m}{n} < y.$$

Since $\frac{m}{n}$ is clearly a rational number, this proves the result in this case (when $x \geq 0$).

We now consider the case $x < 0$. The idea here is to simply “shift” up to the case we’ve already proven. By Theorem 6.1, we can find a natural number j such that $j > -x$ and thus $0 < x + j < y + j$. Using the first case, which we have already proven, applied to the number $x + j$ (which is positive), there is a rational number q such that $x + j < q < y + j$. We deduce that $x < q - j < y$, and, since $q - j$ is also rational, this proves the corollary in this case. \square

Let me say a bit more about the density of the rationals: it is a consequence of this result that between any two distinct real numbers there are *infinitely many* rational numbers: For if $x, y \in \mathbb{R}$ and $x < y$, then by the Corollary there is a rational number q_1 with $x < q_1 < y$. But then we can apply the Corollary again using x and q_1 , to obtain the existence of a rational number q_2 with $x < q_2 < q_1$, and yet again using x and q_2 to obtain $q_3 \in \mathbb{Q}$ with $x < q_3 < q_2$, and so on forever.

A real number is called *irrational* if it is not rational. For example, $\sqrt{2}$ is irrational, a fact we have proven: we proved it exists as a real number, using the axioms, and earlier we showed that it cannot be rational.

Corollary 6.4 (Density of the Irrational Numbers). *Between any two distinct real numbers there is an irrational number; more precisely, if $x, y \in \mathbb{R}$ and $x < y$, then there exists an irrational number z such that $x < z < y$.*

Proof. We will prove this by using the Density of the Rational Numbers along with the fact that we know of at least one irrational number: $\sqrt{2}$.

Suppose $x, y \in \mathbb{R}$ and $x < y$. Then $x - \sqrt{2} < y - \sqrt{2}$ and, by the Density of Rational Numbers, there is a rational number q such that $x - \sqrt{2} < q < y - \sqrt{2}$. By adding though by $\sqrt{2}$ we obtain

$$x < q + \sqrt{2} < y.$$

As we showed earlier, the sum of a rational and an irrational number is always irrational. In particular, $q + \sqrt{2}$ is irrational. By letting $z = q + \sqrt{2}$ we have proven the Corollary. \square

As with rational numbers, between any two distinct real numbers there are in fact infinitely many irrational numbers. (In particular, there are infinitely many irrational numbers, which is not something we've proven up until this point.)