Contents

1. Wednesday, January 27

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

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

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

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

(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, $1.333\ldots$ is rational (it's equal to $\frac{4}{3}$) and so is $23.91278278278\ldots$. 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

$$P \Longrightarrow \textit{Contradiction}$$

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 is 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 nonnegative 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 { element of a set | property holds }, but this one has the form { expression involving symbols | 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 : $S \cup T = \{x \mid x \in S \text{ and } x \in T\}$
- 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."