Discrete Mathematics lecture notes 1-1

0. Introduction: What is truth?

Let us begin by something that surely must be true:

Theorem 1 (Pythagorean Theorem). *If a right triangle has legs of length a and b, and a hypotenuse of length c, then*

$$a^2 + b^2 = c^2.$$

What, beyond an appeal to nomenclature, allows us to assert that this Theorem is true? We could provide a proof, which is simply a fancy term for a rigorous argument in favor of the truth of our claim.[1] How rigorous is "rigorous," and how do we know that we've achieved it? Good questions. For answers, see the rest of this course, and several more math courses afterwards.

For now, I want to focus on a different problem: Even once we've given our perfect, rigorous proof of the Pythagorean Theorem, someone else can still come along and say:

"That's not right! and I know it's not right because I can produce right triangle with legs of length a and b and hypotenuse of length c [so this triangle satisfies the *hypotheses* of the Theorem], and yet it is not true that $a^2 + b^2 = c^2$.

"Start at the North Pole and walk due south (any south) until you hit the equator. Say you've traveled a miles at this point. Now turn east and walk along the equator until you've traveled a miles again. Finally, turn due note and walk until you return to the North Pole; because the North Pole is equidistant from every point on the equator, the last leg of the journey is again a miles. But now your trip has traced out a giant triangle on the face of the Earth, each side of which has length a, and this is a right triangle, since the turn from going due south to due east is 90°.[2] So if the Pythagorean Theorem were true, we'd have $a^2 + a^2 = a^2$, which is only true if $a = 0$... which is nonsense! Guess Pythagoras wasn't so hot after all."

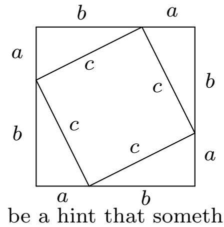
The fault is not in Pythagoras, but in ourselves: We misunderstood the nature of mathematical truth as being like those physical truths we encounter in our day-to-day lives. In fact, a Theorem can be either true or false depending on how we choose to interpret it. This is less a problem of *definition* ("triangle" always means something to the effect of "polygon with three sides"), than one of *axiom*: When we stated the Pythagorean Theorem, we were implicitly accepting—not as "true," but as a starting point for the discussion—Euclid's axioms for planar geometry, while our friend is conducting geometry on the surface of a sphere. In the Earth-walk situation, the notion of "line" still can be interpreted as "shortest path between two points," except now that means a great circle instead of something "straight." And indeed, in the spherical geometry world, the Pythagorean Theorem is false.[3]

For us in the course, we will investigate the roles of Axiom, Definition, and Theorem, and their interplay in the creation of mathematical truth. We will do this chiefly by example, starting now.

1. An axiom we can all agree on

Axiom. The natural numbers exist. We will denote them by $\mathbb{N}$.

Ok, this is actually pretty terrible as a starting axiom, because of the giant undefined term it is built around: What are these natural numbers that we assert exist? We could give a precise, axiomatic definition, but in the interests of not getting too bogged down with subtle details on the first day, let us simply assert:



[1] Can you use this picture to prove the Pythagorean Theorem?

[2] In fact, *every* angle of this triangle is a right angle, which should be a hint that something funny is about to happen.

[3] At least as stated here. . . .

Definition 2. The natural numbers $\mathbb{N}$ is a set $\{0, 1, 2, 3, \ldots\}$[4] that has certain *structure* and *properties.*

What is structure? What is a property? What's the difference, and which examples of both does $\mathbb{N}$ possess? I'll let you ponder the first two questions, and begin to answer the third with the following:

Axiom (Arithmetic structure of $\mathbb{N}$ [5])**.** The natural numbers possess two "internal laws of composition,"[6] called *addition* and *multiplication.* Addition is written $+$ and multiplication $\cdot$, so that for any natural numbers $a, b \in \mathbb{N}$[7] we can form new natural numbers $a + b$ and $a \cdot b$. These internal laws of composition are subject to the following axioms for all $a, b, c \in \mathbb{N}$:

- (Associativity for Addition) $a + (b + c) = (a + b) + c$.
- (Commutativity for Addition) $a + b = b + a$.
- (Identity for Addition) $a + 0 = a$.[8]
- (Cancelation for Addition) If $a + b = a + c$, then $a = c$.
- (Associativity for Multiplication) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- (Commutativity for Multiplication) $a \cdot b = b \cdot a$.
- (Identity for Multiplication) $a \cdot 1 = a$.[9]
- (Cancelation for Multiplication) If $a \cdot b = a \cdot c$ and $a \neq 0$, then $a = c$.
- (Distributivity) $a \cdot (b + c) = a \cdot b + a \cdot c$.

[Aside: $\mathbb{N}$ also possess a *unary operation* (meaning it only takes as input a single natural number instead of two) that we've encountered in passing: The successor function S. We will return to this guy when it comes time to talk about induction. It also possess an *order relation* $<$... Hopefully it is becoming clear that there's actually an awful lot of structure in the seemingly commonplace natural numbers.]

Everything that we've encountered so far should seem so natural as to almost not be worth mentioning... except now that we're trying to think about *why* mathematics works the way it does, we need to pay close attention to facts previously assumed without comment. For instance: We has from the axioms that $a \cdot 1 = a$ for all a, but what about the famous result $a \cdot 0 = 0$ for all a? That wasn't included in the axioms, so did we forget something?

In fact, we did not, because we do not need to axiomatically assert that $a \cdot 0 = 0$ for all a, as that *follows from the other axioms*:

Theorem 3. *If a is a natural number, then $a \cdot 0 = 0$.*

Proof. Because 0 is the additive identity, we can write $0 = 0 + 0$. If we multiply this equation through by a on both sides, we get a new equality[10] $a \cdot 0 = a \cdot (0 + 0)$. We can expand the right hand side via the Distribution Axiom, and the left hand side via another application of the Additive Identity Axiom, to get

$$(a \cdot 0) + 0 = a \cdot 0 + a \cdot 0.$$

Finally, use the Cancelation Axiom to conclude $0 = a \cdot 0$, and we get the desired result. □

[4] The ellipsis is shorthand for "you know what I mean," which should be taken as a warning sign that I'm not being fully honest here. In fact, the more formal approach begins: "$\mathbb{N}$ is a set. There is an element in $\mathbb{N}$ whose name is 0. For each element $x \in \mathbb{N}$, there is a *successor* $S(x)$ in $\mathbb{N}$ that is different from x..." and then more properties of S are recorded. The point is that, instead of thinking of $\mathbb{N}$ as $\{0, 1, 2, \ldots\}$, the more formal view takes the elements of $\mathbb{N}$ to be $\{0, S(0), S(S(0)), S(S(S(0))), \ldots\}$.

[5] Note that these axioms are not exactly standard in the mathematical world, as I'm basically giving you an *ad hoc* list of things that we will need to prove theorems about $\mathbb{N}$ without paying any attention to potential issues of redundancy or if a simpler list could be given.

[6] This is a fancy way of saying a way of combining two elements of the natural numbers to get a third.

[7] The symbol $\in$ is a variant of the Greek letter epsilon, for "element." It indicates that a and b are *elements* of the set $\mathbb{N}$.

[8] Good exercise: Why do we not need to write $0 + a = a$ as well? Prove that this result follows from the other axioms.

[9] What can we say about $1 \cdot a$? Prove it.

[10] In the truly formal version, what I'm asserting here must be taken as a new axiom.

And away we go. The point is that, with enough work and insight, any of the facts about the natural numbers which you've either accepted because you were indoctrinated with by your teachers or just seem obvious can be brought back to this (relatively) short list of Axioms, which we assert by fiat.

Moving on, we can construct new gadgets from ones whose existence we take to be axiomatic:

Definition 4. The *integers* are the set $\mathbb{Z}$ formed by taking $\mathbb{N}$ and adding, for each $x \in \mathbb{N}$, $x \neq 0$, a new formal symbol $-x$.[11] We can expand the internal laws of composition of $\mathbb{N}$—addition and multiplication—to $\mathbb{Z}$ by requiring

$$x + (-x) = 0 = (-x) + x$$

for all $x \in \mathbb{N}$. $-x$ will be called the *additive inverse of* x. Or, we can simply assert (as we choose to do) as another axiom that all of the Axioms that governed the arithmetic structure of $\mathbb{N}$ are still valid when a, b, c are allowed to be arbitrary integers.

Let's see how to use this new notion of the integers to prove a basic fact:

Theorem 5. $(-1) \cdot (-1) = 1$.

Proof. Consider: $0 = 1 + (-1)$, so multiplying both sides through by -1 gives

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

By the Multiplicative Identity Axiom, $(-1) \cdot 1 = -1$, and the same argument for $\mathbb{N}$ show that $(-1) \cdot 0 = 0$. We conclude $0 = -1 + (-1) \cdot (-1)$. Add 1 to each side, and use the definition of additive inverses, to conclude that $1 = 1 + (-1) + (-1) \cdot (-1) = 0 + (-1) \cdot (-1) = (-1) \cdot (-1)$, flip the order of equality[12], and we end up with the claim of the Theorem. □

We can keep playing this game,[13] but for now let's finish with the last few definitions from class.

Definition 6. Let a and b be in $\mathbb{Z}$. We say a *divides* b, written $a|b$, if there is some $c \in \mathbb{Z}$ such that $b = a \cdot c$.

Theorem 7. *If $a|b$ and $b|c$, then $a|c$.*

Proof. Do it. □

Theorem 8. *For all $a \in \mathbb{Z}$, $1|a$ and $a|0$. Conversely, if $0|a$ then $a = 0$, and if $a|1$ then $a = \pm 1$.*

Proof. Do it. □

Definition 9. A number $a \in \mathbb{Z}$ is *even* if $2|a$.

Question for you: How would you finish the statement "A number $a \in \mathbb{Z}$ is *odd* if...?"

[11] Be careful not to read this as "minus x" just yet; all that we're doing is introducing a new element to the set $\mathbb{Z}$, the *name* of this element is $-x$, which we should think of as a single symbol.

[12] That is, equality is *symmetric*: If $a = b$, then $b = a$. This is an axiom we assume for now, but will have cause to revisit shortly.

[13] And we will!