Every branch of mathematics has the following four elements in it:

Definitions, Axioms, Theorems, Proofs.

Example 1.

Definition: Two lines are said to be **parallel** if they have no points in common.

Axiom: If L_1 and L_2 are parallel, and L_2 and L_3 are parallel, then L_1 and L_3 are parallel.

Theorem: If L_1 and L_2 are parallel, and L_2 and L_3 are parallel, and L_3 and L_4 are parallel, then L_1 and L_4 are parallel.

Proof: Since L_1 and L_2 are parallel, and L_2 and L_3 are also parallel, it follows from the above axiom that L_1 and L_3 are parallel. Now, since L_1 and L_3 are parallel, and L_3 and L_4 are also parallel, it follows from the above axiom that L_1 and L_4 are parallel.

We prove theorems using axioms. Axioms are accepted without proof. (We have to have something to start with; we can't prove things from nothing.)

This course is about making these concepts precise. What is a "proof?" What makes a proof valid or invalid? Are there things (other than axioms) that can neither be proved nor disproved? (Yes!) Are there things (other than axioms) that are true but cannot be proved to be true? (Yes!)

Here is a very brief answer to some of the above questions, followed by a concrete but over-simplified example. In a formal system, we agree on a set of axioms, and certain rules of inference. Then, a *proof* is defined to be a list of statements such that each statement is either an axiom, or follows from the preceding statements according to the given rules of inference. The last statement in the list should be what we aim to prove, and is called a *theorem*.

Example 2. A formal system: We have an imaginary language whose alphabet has only four symbols: $a, b, =, +$. A **word** or **expression** is any sequence of letters, e.g., $abb = + + abbb+$.

But we are only interested in expressions of the form

$$a \cdots a + a \cdots a = b \cdots b$$

i.e., a string of one or more a's, followed by one $+$, followed by another string of one or more a's, followed by one $=$, followed by a string of one or more b's.

We'll refer to expression of this form as **formulas**.

We have one **axiom**:

$$a + a = bb$$

(Think of this as just a formula who happens to be a "celebrity.")

From just this one axiom, we'd like to be able to prove theorems, using rules of inference. We have two **rules of inference**:

R1: Given any formula, we are allowed to add one a to the first string of a's on the left, and one b on the right.

R2: Given any formula, we are allowed to switch the order of the two strings of a's.

Example: From the formula $a + aaa = bb$, using R1, we can infer $aa + aaa = bbb$; and, using R2, we can infer $aaa + a = bb$.

Q: Which of the following formulas can we infer from the axiom $a + a = bb$, using repeated applications of R1 and R2?

(i) $aaa + a = bbbb$ (ii) $aa + aa = bbbb$ (iii) $aa + aaa = bbbb$

A: Only the first two, but not the third one. How can we prove this claim? Proving that the first two can be inferred from the axiom is easy. (How?) But proving that the third one cannot be inferred from the axiom takes more work (see below). But first, some more terminology:

Any formula that can be inferred from the axiom (using repeated applications of R1 and R2) is called a **theorem**.

General definition:

Definition 1. To **prove** a formula A means to write a sequence or list of formulas such that: (1) each formula is either an axiom or is inferred from the previous formulas using one of the rules of inference; (2) the last formula in the list is A. The formula A is called a **theorem**, and the list of formulas is called a **proof** for the theorem.

Back to our specific example:

Claim 1. Every formula that has a proof has the same total number of a's and b's.

Proof. First observe that if a formula F has the same number of a's as b's, then any formula derived from F using R1 or R2 will also have the same number of a's as b's. Why? Because R1 increases both numbers by one. And R2 does not change either number.

Now, by def, a proof always starts with the axiom $a + a = bb$. This formula has the same number of a's as b's (two of each). So the second formula in the proof must also have the same number of a's as b's, because by def it is derived from the axiom using R1 or R2. Similarly for the third statement, fourth, and so on, until the last one. (Note: The proper way to phrase all this is to use induction.) □

Challenge: Prove that the axiom $a + a = bb$ and the two rules of inference, R1 and R2, are enough to provide a proof for any formula that has the same number of a's as b's.

In every branch of mathematics, we start with certain axioms. Then an important question arises: Have we included enough axioms to be able to prove everything that's true?

Example: In arithmetic, we have just a few very simple axioms, such as: $x + 0 = x$; $x(y + 1) = xy + x$; etc. (We'll talk about all the axioms of arithmetic in detail later.) Now, one may wonder: If Goldbach's Conjecture is really true (every even number ≥ 4 is the sum of two prime numbers), do we have enough axioms to prove it?

Kurt Gödel proved that no matter how many axioms we include in mathematics, there will always be lots of statements that are true but not provable from those axioms!

HW # 1, due Mon 29 Jan
Read Section 1.3. Do: p. 11: 1-4.