MAT 200 OUTLINE, PART 1

I'm preparing a lecture outline for the benefit of those who are unable to make it to class due to illness or other reasons. See the course textbook for additional details about most of these items.

2/3

- What is math? How would you define it to a friend? Wikipedia: "it has non generally accepted definition." But here is one possibility: a method of establishing truth by formulating **conjectures** and then either **proving** the conjecture or giving a counterexample
- Conjecture, proof, theorem, counterexample, axiom
- Proposition, predicate, statement
- Five logical connectives: or ($\vee$), and ($\wedge$), not ($-$), if... then ($\Longrightarrow$), if and only if ($\Longleftrightarrow$)
- Truth tables
- In principle, everything we do in this class can be made completely "rigorous" by working explicitly with axioms. This would entail the following:
  - Make an "alphabet" of symbols that can be used to make statements
  - Make a list of acceptable "primitive" or "atomic" statements
  - Describe the acceptable ways to make more complicated statements out of existing statements
  - Give a list of axioms expressed symbolically (see "axiomatic set theory" or "Zermelo–Fraenkel set theory")
  - Describe the exact rules of logical inference to establish theorems
  - Every new definition must be stated in terms of existing symbols

  In this way, mathematics becomes a sort of mechanical manipulation of symbols, something like a computer program. As you might imagine, this would take a lot of tedious work, probably beyond both the patience of most students here and the time we have available in this class.
- Instead, we stick to common practice by being more informal about some of these technical or logical issues. We take certain things like arithmetic for granted. It is helpful to be aware that the more formal approach exists

2/5

- Why is "$4 > 3 \Longrightarrow 4 \geq 0$" a true statement? In what way does the conditional $\Longrightarrow$ not correspond to our English usage of the term?
- Universal implication
- How do you prove $1 + 1 = 2$? In a vacuum, you can't. It makes sense to talk about proof only after you've agreed on **definitions** for the relevant terms and **axioms** or facts accepted as true. Back in the early 1900s, mathematicians were very interested in the foundations of the subject. For example, Bertrand Russell in *Principia Mathematica* famously needed hundreds of pages before proving $1 + 1 = 2$. Needless to say, such a proof is very dependent on the choice of definitions and axioms. Arguably, no proof is needed for a statement as fundamental as $1 + 1 = 2$.
- Thus, we need to fix a starting point. In Prop. 2.3.1 and Axiom 3.1.2, the book lists specific properties of the real numbers that we can take for granted when

writing proofs (commutative property, associative property, distributive property, zero, unity, subtraction, division, trichotomy, addition law, multiplication law, transitive law)
- There are two broad steps for writing proofs: (1) work out the steps involved on scrap paper (2) write out a polished argument in English following principles of good mathematical writing
- Prove: for any positive real numbers a, b, $a < b \implies a^2 < b^2$.

2/8

- Three methods of proof (so far): direct proof, proof by cases, proof by contradiction
- divide (i.e., one integer divides another integer), even, odd
- Prove: 101 is an odd number
- Often the same proposition can be proved in multiple ways. It's usually considered bad style to use proof by contradiction when a direct proof is available

2/10

- Prove: $0 \cdot a = a \cdot 0 = 0$ for all real numbers a
- Prove: if a, b, c are integers such that $a > b$, then $ac \leq bc \implies c \leq 0$.
- The previous proof can be done by contradiction. But it is simpler to use the logically equivalent **proof by contrapositive**
- Prove: if a, b are real numbers, then $ab = 0 \iff a = 0$ or $b = 0$
- To prove biconditional statements, we usually split the proof into two parts: the forwards implication $\implies$ and the backwards implication $\impliedby$

2/12

- Equivalence of propositional statements, e.g. $-(P \wedge Q) \iff -P \vee -Q$ and $-(P \vee Q) \iff -P \wedge -Q$ (DeMorgan's laws), $(P \implies Q) \iff (-Q \implies -P)$ (contrapositive)
- When writing a proof, it's fine to switch from the original form of the proposition to another form which is logically equivalent. One example of this is proof by contrapositive.
- The induction principle, which is an **axiom** about the integers
- base case, inductive step
- Prove: for all positive integers n, $n \leq 2^n$
- Prove: For all integers n such that $n \geq 4$, $n^2 \leq 2^n$
- Note that the base case can be any integer (of course, the proposition is not proved for any number smaller than the base case)

2/15

- Definition by induction (recursive definition) for $\sum_{i=1}^{n} a_n$, x^n, $n!$
- Addition and multiplication of natural numbers can be defined by induction using the fundamental operation of "successor" (see "Peano arithmetic")
- Strong induction
- the Fibonacci sequence $u_0 = 0$, $u_1 = 1$, $u_{i+1} = u_i + u_{i-1}$
- Prove: $u_n = (\alpha^n - \beta^n)/\sqrt{5}$, where $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$. Note that α is the golden ratio.
- set: any well-defined collection of objects
- Examples of sets: $\mathbb{Z}, \mathbb{Z}^+, \mathbb{Z}^{\geq}, \mathbb{Q}, \mathbb{R}, \mathbb{R}^+, \mathbb{R}^{\geq}, \mathbb{C}$
- $x \in E$, $x \notin E$

2/17

- Three ways to specify a set:
  1. list the elements, e.g. $\{1, 3, \pi, -14\}$
  2. conditional definition, e.g. $\{n \in \mathbb{Z} : 0 < n < 6\}$
  3. constructive definition, e.g. $\{n^2 : n \in \mathbb{Z}\}$ or $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, b \neq 0\}$
- equality of sets: $A = B$ means $x \in A \iff x \in B$ for all x. This is an axiom about the nature of sets. For example, $\{1, 3, \pi, -14\} = \{3, 1, 1, -14, -14, \pi\}$
- empty set ϕ
- subset relation $A \subseteq B$, proper subset $A \subsetneq B$
- set operations
  - intersection $A \cap B = \{x : x \in A \text{ and } x \in B\}$
  - union $A \cup B = \{x : x \in A \text{ or } x \in B\}$
  - difference $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$
  - complement $A^c = \{x \in U : x \notin A\}$, where U is some universal set depending on the problem
- Prove: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Two approaches for this proof and similar proofs: show $\iff$ all at once (good when the proof is simple), or show $\implies$ and $\impliedby$ separately (good when the proof is more complicated)

2/19

- Thm. 6.3.4: standard properties of set operations
- Prove: $(A \cup B) \cap (C \cup D) = (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D)$ using these standard set properties
- power set $\mathcal{P}(X)$
- universal quantifier “for all” $(\forall a \in A, P(a))$
- existential quantifier “there exists” $(\exists a \in A, P(a))$
- dummy variable
- ambiguity in English meaning of “any”, “not”. Try to avoid these ambiguities when writing
- For multiple quantifiers, the order affects the meaning significantly. Compare:
  - $\forall a \in A, \forall b \in B, P(a, b)$
  - $\exists a \in A, \exists b \in B, P(a, b)$
  - $\forall a \in A, \exists b \in B, P(a, b)$
  - $\exists b \in B, \forall a \in A, P(a, b)$
  - $\forall b \in B, \exists a \in A, P(a, b)$
  - $\exists a \in A, \forall b \in B, P(a, b)$
- Which of the above are true for $A = B = \mathbb{Z}^+$, $P(a, b) = a \leq b$?

2/22

- How to prove/disprove statements of the form $\forall a \in A, P(a)$ and $\exists a \in A, P(a)$
- Decide which are true and which are false. Try writing out proofs.
  - $\forall x, y \in \mathbb{R}$, $xy = x$
  - $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$, $xy = x$
  - $\exists x \in \mathbb{R}$, $\forall y \in \mathbb{R}$, $xy = x$
  - $\exists x, y \in \mathbb{R}$, $xy = x$
- $X \times Y$, the Cartesian product of two sets X and Y
- ordered pair (x, y). Contrast this with $\{x, y\}$.
- Sketch $\{(m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : m < n\}$. How does this relate to propositions like $(\forall m \in \mathbb{Z}^+, \exists n \in \mathbb{Z}^+, m < n)$ and $(\forall n \in \mathbb{Z}^+, \exists m \in \mathbb{Z}^+, m < n)$?
- Properties of the Cartesian product:

- $A \times (C \cup D) = (A \times C) \cup (B \times D)$
- $A \times (C \cap D) = (A \times C) \cap (B \times D)$
- $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$
- $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$