Math 117 Fall 2014 Lecture 12 (Sept. 22, 2014)

Reading: 314 Notes: Proof and Logic §1.

- Steps to approach a (proof) problem.

  1. Check the definitions involved.
  2. Identify the logical structure:
     - Is it "prove" or "disprove"?
     - What are the hypotheses, that is what are given?
     - What are the conclusions that need to be proved (or disproved)?
  3. (For harder problems) Gain understanding through examples.
     - (To prove) Why should the conclusion hold?
     - (To disprove) What could go wrong in the conclusion?
  4. Apply appropriate proof strategies.

- To prove.

  - Direct proof.

    For simpler problems, it suffices to start from the hypotheses, explore their consequences, and then reach the conclusions.

  - Forward-backward proof.

    For most problems, quite a few intermediate conclusions are needed to reach the final conclusion and it is hard to get them all starting from the hypotheses. In such cases it is a good idea to start from the hypothesis, go as far as one could; Then start from the conclusion and see what **implies** the conclusion, and try to meet in the middle.

    Example 1. Let A, B, C be sets. Assume $A \subseteq B$. Prove that $C - B \subseteq C - A$.

    We follow the four steps.

    1. Check all definitions:
       - sets;
       - $A \subseteq B$ means for every $x \in A$, $x \in B$;
       - $C - B = \{x | x \in C, x \notin B\}$.
    2. Identify logical structure.
       - To prove;
       - Hypotheses: A, B, C sets, $A \subseteq B$.
       - Conclusion: $C - B \subseteq C - A$.
    3. Examples? Anyone not sure about the conclusion could draw a Venn diagram and be convinced.
    4. Proof.
       - Forward: If $A \subseteq B$ then every $x \in A$, $x \in B$.
       - Backward: $C - B \subseteq C - A$ is implied by

$$\text{For every } x \in C - B,\ x \in C - A.$$

- Backward: "For every $x \in C - B$, $x \in C - A$" is implied by

$$\text{For every } x \in C \text{ but } x \notin B,\ x \in C \text{ but } x \notin A.$$

- Backward: We notice that $x \in C$ implies $x \in C$, therefore "For every $x \in C$ but $x \notin B$, $x \in C$ but $x \notin A$." is implied by

$$\text{For every } x \notin B,\ x \notin A.$$

Exercise 1. Show that "For every $x \in C$ but $x \notin B$, $x \in C$ but $x \notin A$." does not imply "For every $x \notin B$, $x \notin A$."

- Forward: We prove "every $x \in A$, $x \in B$" implies "every $x \notin B$, $x \notin A$". Assume the contrary. Then there is $x \notin B$ but $x \in A$. Since every $x \in A$, $x \in B$, we have $x \in B$ contradicting $x \notin B$.

Thus we see that the "forward" and "backward" steps meet in the middle and the proof ends.

5. Write the proof.

The above is a legitimate proof but is really hard to read. Therefore it is a good idea to rewrite it.

Proof. Take an arbitrary $x \in C - B$. By definition $x \in C$ and $x \notin B$. Now we prove that $x \notin B$ implies $x \notin A$ by contradiction.

Assume the contrary. Then there is $x \notin B$ but $x \in A$. Since every $x \in A$, $x \in B$, we have $x \in B$ contradicting $x \notin B$.

Thus we have $x \in C$ and $x \notin A$ which by definition is $x \in C - A$.

Summarizing, we have shown that every $x \in C - B$, $x \in C - A$. By definition this means $C - B \subseteq C - A$ and the proof ends. □

- Proof by contradiction.

If from

$$\text{"Mathematical facts"} + \text{"Hypotheses"} + \text{"Contrary of the Conclusion"}$$

we can derive absurdity, then something must be false in these three. The only possible thing in these three that could be false is "contrary of the conclusion" and therefore the conclusion holds.

Example 2. Prove that all of the following

$$\sqrt{5},\ \sqrt{5\sqrt{5}},\ \sqrt{5\sqrt{5\sqrt{5}}}, \ldots \tag{1}$$

are irrational.

Proof. (by contradiction) Assume the contrary. Then there is at least one $\sqrt{5\sqrt{5\cdots}} \in \mathbb{Q}$. Among such numbers there must be one with minimal number of square roots. We denote it

$$\alpha := \sqrt{5\sqrt{5\cdots}} \tag{2}$$

and denote by m the number of square roots in it.

There are two cases.

i. $m = 1$. In this case $\alpha = \sqrt{5}$ which we know is not rational. Contradiction.

ii. $m > 1$. Then as $\alpha \in \mathbb{Q}$ we have $\frac{\alpha^2}{5} \in \mathbb{Q}$. But

$$\frac{\alpha^2}{5} = \sqrt{5\sqrt{5\cdots}} \tag{3}$$

where there are only $m-1$ square roots in the right hand side. This contradicts the minimality of m.

Thus the proof ends. $\square$

Remark 3. As many observed during the lecture, this could also be proved directly through induction.

Exercise 2. Does the limit of the sequence $\sqrt{5}, \sqrt{5\sqrt{5}}, \sqrt{5\sqrt{5\sqrt{5}}}, \ldots$ exist? If so what is it?

- To disprove.
  - Find a counterexample.

Example 4. Prove or disprove:

$$A, B, C \text{ are sets. } A \subset B \text{ then } C - B \subset C - A. \tag{4}$$

Disprove. Let $A = \{1\}, B = \{1, 2\}, C = \{3, 4, 5\}$. Then $A \subset B$ but $C - B = C - A = \varnothing$.