LECTURE 2

Proofs

1. Some Mathematical Terminology

A **definition** in mathematics is the laying down of the mathematical meaning of a particular term, in terms of mathematical objects or ideas that have been previously defined or shown to exist.

We have already run into several definitions; for example we have agreed what it means for the statement $P \Rightarrow Q$ to be true. Nothing says that this definition is correct. That is not the point at all; a good definition is simply one that communicates a useful idea. If an idea is not useful, then its definition is not needed.

For example, the definition of a prime number as "an integer greater than one that is not divisible by any positive integer other that 1 and itself" is an example of a useful definition because the concept of prime numbers is used repeatedly in mathematics (indeed, it is one of the cornerstones of Number Theory). Besides, it is easier to simply say "a prime number", rather than to say "an integer greater than one that is not divisible by any positive integer other that 1 and itself" all the time. Thus, a definition will also allow us to condense our language a bit.

An **axiom** is somewhere between a definition and a theorem. It is like a definition in that an axiom is to be accepted without proof (and even without certainty); but an axiom is also like a theorem in that it serves more to place limitations on the mathematical objects being considered rather than to introduce new objects. An example of an an axiom is

"Distinct parallel lines never meet."

which is one of the foundations of Euclidean geometry, but which is regarded as false in Riemannian geometry.

In mathematical literature, besides theorems, you also run across propositions, lemmas, and corollaries. A **proposition** is a true statement that you intend to prove.

Theorems, lemmas and corollaries are all examples of propositions; and the distinction between these terms is purely subjective.

Generally speaking, a **theorem** is some major result that you wish to prove. In doing so, however, the proof may be very long and tangled. In order to tidy up the presentation of a difficult proof, a mathematician may break it up into a series of "little propositions" or **lemmas**. Thus, a lemma is component proposition of a theorem. Once a theorem or lemma is proved, often several other results can be proved almost immediately. Such propositions are called **corollaries**.

2. Methods of Proof

Most mathematical theorems are conditional or biconditional statements; that is statements of the form

$$P \Rightarrow Q$$

or combinations thereof, like

$$P \Leftrightarrow Q\,.$$

And even if the statement of a theorem is not in a conditional form, it is often equivalent to one that is. For example, the statement

"Every integer greater than 1 is a product of primes."

is equivalent to the conditional statement

"If n is an integer and $n \geq 1$, then n is a product of primes."

The first step in proving a theorem is to identify the underlying hypothesis P and the conclusion Q. In order to prove the theorem "$P \Rightarrow Q$" one assumes that the hypothesis is true and then uses it, together with axioms, definitions, and previously proved theorems, to argue (logically) that the conclusion Q is necessarily true.

Below we outline some of the most common methods of proof.

2.1. Direct Proof. If R is a true statement and $R \Rightarrow S$ is a true conditional statement, then S is a true statement. To prove a theorem $P \Rightarrow Q$ by the direct method, one finds a series of statements P_1 , P_2 , $\ldots$, P_n and then verifies the each of the conditional statements

$$\begin{aligned} P &\Rightarrow P_1\,, \\ P_1 &\Rightarrow P_2\,, \\ &\vdots \\ P_{n-1} &\Rightarrow P_n\,, \\ P_n &\Rightarrow Q\,, \end{aligned}$$

are true. The assumption that P is true and the repeated application of the simple rule stated at the beginning of this paragraph show that Q is true.

2.2. The Forward-Backward Method. The method described above, while detailing very clearly the underlying logic of a proof, does not give one a clue as to how such a proof might be found. Indeed, one would have to be some sort of rare genius to simultaneously envision all the intermediary statements of a direct proof.

Mere mortals require a less ambituous approach. The idea behind the forward-backward approach is the point of the following allegory.

Suppose you're out 4-wheeling in the desert and you get a distress call on your CB radio. The caller is out of gas and does not know where he is. How can you find him?

Well, the first thing you would do is ask him what landmarks are near by. If you're lucky, he might point out something obvious like a nearby mountain which you can also see. Then with some other clues, e.g., his direction with respect to the mountain, you might find him quickly. If this is not the case, perhaps you both would be wise to search your relative vicinities to find some other common point of reference. Suppose you both find a river. Well, you might both drop a bottle in the river, then the one who receives the bottle would be the one down stream. Or maybe there's some other clever way of figuring out who is where and how to get there.

The point of this story is the following. In trying to prove a proposition like $P \Rightarrow Q$ by the direct method, you need to find a "path" of intermediary statements $P_i \Rightarrow P_{i+1}$ that starts at P and ends at Q and a way to do this is to mimic the story above. You try to first identify "landmarks" (i.e., propositions) that can be reached from P and "landmarks" from which Q can be reached; then you try to find a way of getting from a landmark in the reachable from P to one from which Q can be reached.

Let's now consider a mathematical example.

DEFINITION 2.1. *An integer n is **even** if it can be written as $n = 2k$ for some $k \in \mathbb{Z}$. An integer n is **odd** if it can be written as $n = 2k + 1$ for some $k \in \mathbb{Z}$.*

PROPOSITION 2.2. *If n is an even integer, then n^2 is an even integer.*

To prove this proposition we shall use the forward-backward method. The hypothesis P is the statement that n is an even integer. The conclusion Q we wish to reach is that n^2 is an even integer.

Well, let's first look backward from Q and ask "How can I show n^2 is even?" Well, according to the definition of even given above if n^2 is even, then it must be 2 times some other integer, say k.

(Q_{-1}) $$n^2 = 2k \quad .$$

So if we can show that n^2 is twice some integer we are done.

Working forward from the hypothesis, we assume that since n is even,

(P_1) $$n = 2s \quad .$$

However, if $n = 2s$, then

(P_2) $$n^2 = 4s^2 = 2(2s^2)$$

And so now we have shown that n^2 is twice $2s^2$ (which is equivalent to the statement Q_{-1}).

Putting this all together we have

$$P \Rightarrow P_1 \Rightarrow P_2 \Rightarrow Q_{-1} \Rightarrow Q$$

and we are done.

Formal Proof: By hypothesis, $n = 2k$ for som $k \in \mathbb{Z}$. Thus, $n^2 = (2k)^2 = 2(2k^2)$. Since $2k^2$ is an integer if k is an integer, we can conclude that n^2 is even. ∎

2.3. Proof by Contradiction. Consider the proposition

"If n is an integer and n^2 is even, then n is even."

which is the converse of the proposition proved in the example above. The forward-backward method does not work so well in this example. Let's take a moment to see why.

Working backward from the conclusion "n is even", we can infer

(Q_{-1}) There is an integer k such that $n = 2k$.

Working forward from the premise "n is an integer and n^2 is even", we can deduce

(P_1) $$n^2 = 2p$$

or

(P_2) $$n = \pm\sqrt{2p} \quad .$$

The problem then is to show that $\pm\sqrt{2p}$ can be written as $2k$. There is no obvious way to do this.

So we need another method of proof. The proof by contradiction method is based on the following fact:

Suppose you presume the truth of a statement R and you then make a valid argument that $R \Rightarrow S$. If the statement S is in fact false, there is only one possible conclusion: the original statement must have been false.

To make use of this reasoning in a proof, say, of a statement $P \Rightarrow Q$, one can try to prove, using P and previously proven results, that not-Q implies a statement S which is known to be false. Since not-Q is false exactly when Q is true, the original statement is then proved.

Diagramatically,

$$\left.\begin{array}{r} P \text{ is true} \\ \text{“}P \text{ and not-}Q\text{”} \Rightarrow S \\ S \text{ is false} \end{array}\right\} \Rightarrow \text{not-}Q \text{ is false} \Rightarrow Q \text{ is true} \quad .$$

Let's now return to the example above where we are trying to prove that if n is an integer and n^2 is an even integer, then n is even.

proof. Suppose that n is an integer, n^2 is an even integer and n is odd. Since n is odd, $n-1$ is even, and hence we have

$$n - 1 = 2k \quad ; \quad k \in \mathbb{Z} \quad .$$

or

$$n = 2k + 1 \quad .$$

Similarly, we have by hypothesis,

$$n^2 = 2p \quad ; \quad p \in \mathbb{Z} \quad .$$

But then

$$\begin{aligned} n^2 &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

But $2(2k^2 + 2k)$ is obviously even, so $2(2k^2 + 2k) + 1$ is odd. Hence our hypothesis is violated. So n must be even. To make contact with the notation of the diagram preceding this example, we set

$$\begin{aligned} P = S &= \text{“}n^2 \text{ is even”} \\ Q &= \text{“}n \text{ is even”} \\ \text{not-}Q &= \text{“}n \text{ is odd”} \end{aligned}$$