

5 Digression: Theorems and Proofs

(c.f. Gemignani Ch. 1)

Comments on mathematical THEOREMS:

A *theorem* is a declarative assertion of a mathematical truth.

It generally has some initial statements, called *hypotheses*, which we assume are true just for this context of the theorem. These typically take forms such as: “Let p be a prime number...” or “If m and n are integers...” or “Suppose $x^2 + 2x + 1 = 0...$ ” (etc.)

Note that the hypotheses might assert something about some variables or other mathematical objects.

It ends with one or more statements, called *conclusions*.

Sometimes the statement of a theorem is hard to parse into hypotheses and conclusions.

Conceptually, the form is:

IF *hypotheses* THEN *conclusion(s)*.

The terms THEOREM, LEMMA, PROPOSITION, COROLLARY are all roughly synonymous; the difference is the depth or difficulty of the argument:

theorems are major assertions

lemmas are less major assertions, usually just used as tools in proving theorems

propositions are relatively simple assertions, sometimes nearly obvious

corollaries follow in a straightforward way either from the statement or proof of another statement (theorem, lemma, proposition, or other corollary)

Theorems are usually introduced with word ‘Theorem’ (or ‘Lemma’ etc) and are set off from the subsequent *proof* by means of space, different fonts, or some other way.

Comments on mathematical PROOF:

We will learn several kinds of proofs this term.

The simplest is *direct proof*

A direct proof takes the form of a sequence of assertions.

Sometimes these assertions are just a succession of sentences in English, sometimes they are equations or other statements expressible in purely mathematical notation, sometimes a mixture.

Every assertion should be either:

1. A hypothesis of the theorem.
2. A ‘basic’ fact of mathematics, property of arithmetic or geometry or logic, etc. (An *axiom*.)
3. Something that follows ‘logically’ from the earlier assertions.

The last assertion should be the theorem’s conclusion.

Most proofs are variants of direct proof.

6 Even more number theory

Corollary 6.1. *If N is composite then N has a prime factor $\leq \sqrt{N}$*

Proof. Class □

Lemma 6.1. *If p is a prime number and m, n are positive integers and $p|mn$ then either $p|m \vee p|n$*

(Note the new NOTATION: If P and Q are assertions [=“propositions”] then “ $P \vee Q$ ” means: either P is true OR Q is true *OR BOTH*.)

Proof. Class □