

# Basic Notions of Mathematical Proofs

by Dr. Frank Luger, DSPE

Elementary mathematical proofs rest upon the basic principles of mathematical logic, which, in turn, is a direct application of classical Aristotelian logic to mathematics. Classical logic was used in Euclid's *Elements*, on which all traditional geometry and mathematics was built, using propositional logic or the logic of propositions. The essence of propositional logic was laid down in the three famous "laws of thought" by Aristotle (384-322 BCE), namely, the Law of Identity ( $A = A$ ), the Law of Non-Contradiction ( $A$  never equals non- $A$ ), and the Law of the Excluded Middle (either  $A$  or non- $A$ ). They can also be expressed in symbolic logic as follows:

If  $p$ , then  $p$  ( $p$  implies  $p$  by the Law of Identity).

Not both  $p$  and not- $p$  ( $\sim[p \text{ and } \sim p]$ , by the Law of Non-Contradiction, where the tilde [ $\sim$ ] means negation).

Either  $p \vee \sim p$  by the Law of the Excluded Middle, where  $\vee$  means the exclusive "or."

These "laws of thought" have remained essentially unchanged ever since. In propositional logic, these basic principles take the following form (the Law of Identity is so basic that it is taken for granted, so it isn't even mentioned).

**First Principle - Law of the Excluded Middle:**  
For any proposition,  $p$ , the proposition, "either  $p$  or not- $p$ " is true.

**Second Principle - Law of Contradiction:**  
For any proposition,  $p$ , the proposition " $p$  and not- $p$ " is false.

**Third Principle - Law of Transitivity of Implication:**  
For any propositions,  $p$ ,  $q$ ,  $r$ , the proposition, "if  $p$  implies  $q$  and  $q$  implies  $r$ , then  $p$  implies  $r$ ," is true.

By definition, a *general proposition* is a proposition expressible in one of the following forms for a specific designation of  $x$  and  $y$ :

- (a) All  $x$ 's are  $y$ 's.
- (b) No  $x$ 's are  $y$ 's.
- (c) Some  $x$ 's are  $y$ 's.
- (d) Some  $x$ 's are not  $y$ 's.

Propositions are, many times, stated in the form of hypotheses and conclusions. But one must be careful, because the conclusion being true provides no information in itself about the truth or falsity of the hypothesis.

There are certain relationships between implications involving the same two statements or their negatives that occur sufficiently often to make special terminology helpful, as follows. For a *given* implication, " $p$  implies  $q$ " or "if  $p$  then  $q$ " or " $p$  only if  $q$ " is evident from what has been said above. The *converse* is the implication " $q$  implies  $p$ " or "if  $q$  then  $p$ " or " $q$  only if  $p$ ," while the *inverse* is the implication "not- $p$  implies not- $q$ " or "if not- $p$  then not- $q$ " or "not- $p$  only if not- $q$ ."

Finally, the *contrapositive* is the implication, "not- $q$  implies not- $p$ ," or "if not- $q$  then not- $p$ " or "not- $q$  only if not- $p$ ." It is noteworthy that a given implication and its contrapositive are *logically equivalent*. The concept of logical equivalence applies in general to pairs of propositional forms. We say that *two propositional forms are logically equivalent, provided they have the same set of meaningful values and the same set of truth values*; that is, each has the same true-false classification as the other for all possible choices of the variables. For a *true implication*, "if  $p$  then  $q$ ," where  $p$  and  $q$  are propositional forms,  $p$  is said to be a *sufficient condition* for  $q$ , and  $q$

is said to be a *necessary condition* for  $p$ ; i.e.,  $q$  necessarily follows from  $p$ .

The purpose of the foregoing was as an introductory “warm-up” to enable us to apply logical principles to finding and proving new mathematical results. Mathematics is an abstract science in the sense that it consists of a system of undefined terms about which certain statements are assigned a true classification (these are the axioms and the postulates), which, together with basic defined terms, are used to develop additional propositions. These, in turn, are then shown to be true or false according to the rules of logic that have so far been considered (such true propositions being called *theorems*).

Many of the new results in such a system are proved by *direct* methods that involve primary applications of the Law of Transitivity for Implications mentioned above. However, *indirect* methods of proof are also used frequently, both in mathematical developments and in everyday reasoning, with compelling, even necessarily true, results. When a child asks, “Has Daddy gone to work?” and Mother answers, “See if the car is in the garage,” it is likely that the thought pattern involves, “If Daddy has gone to work, then the car is gone.” When the child finds the car in the garage, he concludes, “If the car has not gone, then Daddy has not gone to work,” thus utilizing the contrapositive to arrive at a “No” answer to his original question.

Direct proofs, both in their *forward* (reasoning from premises to conclusion) and *backward* (reasoning from conclusion to premises) varieties, are quite straightforward and, as such, need not be treated here. However, while a direct proof may often be given where an indirect method is employed, the latter is often clearer, more forceful, and shorter. This is such an important phase of reasoning that it will be worthwhile to consider a general analysis and some further examples. There are essentially two forms in which indirect reasoning may appear, frequently interchangeably.

## Form I of Indirect Reasoning

Form I consists of proving the contrapositive and, thereby, the desired implication. To show “ $p$  implies  $q$ ” is true, we show that “not- $q$  implies not- $p$ ” is true. For example, we assume simple properties of integers and also the definition that a prime number is a positive integer which is divisible by no other integers than itself and 1.

*Proposition:* If an integer greater than 2 is prime, then it is an odd number.

*Proof:*

- (1) If an integer greater than 2 is not odd, it is even, by definition.
- (2) If an integer greater than 2 is even, it is divisible by 2, by definition.
- (3) If an integer greater than 2 is divisible by 2, it is not prime.
- (4) Hence, if an integer greater than 2 is not odd, it is not prime, by the Transitive Property of Implications (*vide supra*).
- (5) Therefore, if an integer greater than 2 is prime, then it is an odd number, since step 4 states the truth of the contrapositive.

## QED

QED is a standard abbreviation from Latin, *quod erat demonstrandum* (that which was to be proved); but in the case of as-yet unproven theorems, it reads *quod est demonstrandum* (that which is to be proved). This is the Latin rendering of the original Greek phrases which Euclid used to finish or start his proofs, and both of these have become habitual expressions in the classical mathematical literature of most countries.

## Form II of Indirect Reasoning

Form II essentially follows the pattern below:

- (a) To prove true:  $p$  implies  $q$ , where  $p$  has a true classification.
- (b) Show:  $p$  and not- $q$  imply  $r$ , where  $r$  is known to be false.
- (c) A false conclusion indicates a false hypothesis; hence, not- $q$  is false.
- (d) Not- $q$  being false shows that  $q$  is true. This is the desired result.

For example, assume the usual terminology of plane geometry and the proposition, "From a point not on a straight line, one perpendicular, and only one, can be drawn to the line." Prove the proposition.

*Proposition:* Two straight lines in the same plane perpendicular to the same line are parallel.

*Notation:* Let  $L$  be the given line through distinct points  $A$  and  $C$ , with  $AB$  perpendicular to  $L$  at  $A$  and  $CD$  perpendicular to  $L$  at  $C$ .

*Restatement:* If  $AB$  and  $CD$  are each perpendicular to  $L$ , then  $AB$  and  $CD$  are parallel.

*Proof:* Assume  $p$  ( $AB$  is perpendicular to  $L$  and  $CD$  is perpendicular to  $L$ ) and not- $q$  ( $AB$  and  $CD$  are *not* parallel).

- (1)  $AB$  and  $CD$  not parallel imply that  $AB$  and  $CD$  intersect in a unique point  $P$ , by definition of parallel lines.

(2)  $AB$  and  $CD$  are distinct lines through point  $P$  not on  $L$ , both perpendicular to  $L$ , by hypothesis  $p$ .

(3) This is false by the proposition quoted for reference.

(4) Hence, not- $q$  is false, since a false conclusion requires a false hypothesis in a true implication.

(5) Therefore,  $AB$  and  $CD$  are parallel ( $q$  is true).

Indirect methods of reasoning are sometimes called "proof by contradiction" (or *reductio ad absurdum*) due to the property of arriving at the negative, or contradiction, of a known true proposition. By virtue of the laws of thought cited above, (self-)contradictions are absurd and may, therefore, be safely discarded.

When the *deductive* aspect of inquiry, which has been emphasized above, is applied to mathematics or to other scientific fields, it frequently is preceded by an *inductive* aspect. The latter is concerned with the search for facts or information by observation and experimental procedure. Once the available facts have been assimilated, the scientist proceeds by *induction* to the formulation of a hypothesis or premise of a general nature to explain the particular facts observed and the relationships among them. The *deductive* aspect involves logical reasoning leading from this hypothesis to new statements or principles, which then may be checked against the facts already available. This use of inductive and deductive procedures to complement, reinforce, and check each other in the formulation of scientific knowledge comprises the main part of what is called *the scientific method*.

## SUGGESTED READINGS

### 1. Elementary treatments of the subject matter.

Händel, A. and K. A. Kneist. *A Brief Sketch of Logic* (in German). Berlin: VEB Deutscher Verlag der Wissenschaften, 1960.

---

Klaus, G. *Introduction to Formal Logic* (in German). Berlin: VEB Deutscher Verlag der Wissenschaften, 1959.

Klenk, V. *Understanding Symbolic Logic*. 3rd ed. Englewood Cliffs, NJ: Prentice-Hall, 1994.

Polya, G. *How to Solve It*. 5th ed. Princeton, NJ: Princeton University Press, 1948.

Polya, G. *Mathematical Discovery*. 3rd ed. New York: John Wiley, 1981.

Solow, D. *How to Read and Do Proofs*. 2nd ed. New York: John Wiley, 1990.

## **2. Intermediate treatments of the subject matter.**

Copi, I. *Symbolic Logic*. 5th ed. New York: Macmillan, 1979.

Filkorn, V. *Pre-Dialectical Logic* (in English). Bratislava: Slovak Academy of Sciences, 1963.

Frege, G. *Logic, Semantics, and Mathematics: Selected Essays* in P. Geach and M. Black, editors, *The Philosophical Writings of Gottlob Frege*. Oxford: Blackwell, 1960. There are over three dozen original Frege works well worth exploring.

Polya, G. *Mathematics and Plausible Reasoning*. Vols. I-II. 2nd ed. Princeton, NJ: Princeton University Press, 1968.

Quine, W. *Mathematical Logic*. 2nd rev. ed. New York: Harper, 1951.

Ruzsa, I. *Introduction to Metalogic* (in English). Budapest: Aron Publishers, 1997.

Tarski, A. *Logic, Semantics, Metamathematics*. Oxford: Clarendon, (1956) 1974.

## **3. Advanced treatments of the subject matter.**

Bell, J. and M. Machover. *A Course in Mathematical Logic*. Amsterdam: Elsevier, 1977.

Bethem, J. *Exploring Logical Dynamics*. Stanford, CA: CSLI, 1996. [Ω](#)