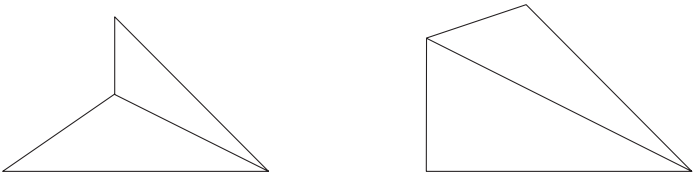
1

AN ANCIENT TRADITION

1.1. REDUCTION TO THE EVIDENT

The original idea of mathematical proofs was to make immediately evident that which is somehow hidden and beyond what can be directly seen. The immediately evident was given in the form of axioms that formed the basis of proofs of theorems. Examples from ancient Greek geometry are easily found: say, the sum of angles of any quadrangle makes a full circle. To make this evident, first check that any quadrangle can be divided into two triangles. For a convex quadrangle, just take any two opposite vertices and join them by a line. The same cutting into two triangles works also if the quadrangle has a cavity on one side:



Now take one of the triangles and draw a perpendicular through one of the vertices. This gives you two smaller right-angled triangles. Take one of these and draw another congruent triangle with the same hypothenuse, and you have a rectangle the angles of which add up to a circle:

The angles of each of the two triangles have to add up to half a circle. Now do the same with the bigger triangle that was one half of the

original quadrangle. Here, with some details filled in, we could add the famous *QED, quod erat demonstrandum* (as was to be proved).

Ancient Greek geometry was an attempt at determining explicitly what it is that makes proofs like the preceding one evident, namely the axioms of geometry and their combination step after step, as codified in Euclid's book *The Elements*. The preceding proof contains certain "auxiliary constructions" with specific properties, all detailed in Euclid.

1. First, the *connecting line* between two vertices of the quadrangle is drawn. *The Elements* contains a *construction postulate* by which the geometer assumes to have the capacity to produce lines that pass, with infinite precision one could say, through two given points. Therefore, it is justified to conclude that two triangles are produced.

2. In the second diagram, the auxiliary construction is the *perpendicular* to the base of the triangle, drawn through the opposite vertex. This could be produced by another construction postulate, but the organization in Euclid is different. He poses the construction of such a perpendicular or orthogonal line as a *problem*. Namely, his results are divided into theorems in which it is required to prove a result, and into problems in which it is required to produce a geometric object with some specific properties. The chosen conceptual order of things now requires a *definition* of perpendicularity that Euclid gives through the requirement that the two adjacent angles be equal. When this is the case, the angles are by definition *right*.

3. A third auxiliary construction is the triangle that has the same hypothenuse as the one produced by the perpendicular line. Principles of proof are required from which it follows that the two triangles have the same angles, and then the final result follows by some summing up of conclusions and angles.

In the end, the system of geometry becomes complicated, and one needs training in it. Mere mastery of the principles is not sufficient, for it cannot be determined in advance what auxiliary constructions are needed to solve a problem; their discovery comes from the ingenuity of the geometer.

Geometric proofs have been a constant part of higher education for more than two thousand years. Another part has been Aristotle's theory of logic, his syllogistic inferences. Here the basis is given by abstract

forms of language such as *Every A is B* and *Some A is B*. Consider the two inference patterns

Assumption α:	*Every A is B*	*Some A is B*
Assumption β:	*Some B is C*	*Every B is C*
Conclusion:	*Some A is C*	*Some A is C*

Strangely enough, the first suggested inference is incorrect, but the second is correct. Where does the latter come from? Aristotle gives an explanation of the quantifiers *Every* and *Some* and thereby justifies the second inference. For the first, we can give a *counterexample*; say, let A, B, and C be, respectively, *number divisible by four, number divisible by two, a prime number.* Now we get, for assumption α, *Every number divisible by four is a number divisible by two*, and for assumption β, *Some number divisible by two is a prime number*. Both are obviously correct, the latter because 2 is divisible by 2. The conclusion, however, is *Some number divisible by four is a prime number*, which is a falsity. In producing the example, we had to make a little adjustment, by adding of the indefinite article in the first assumption.

The discovery of non-Euclidean geometries in the nineteenth century changed the traditional picture of axioms as evident truths: If triangles are drawn on the surface of the Earth so that each side is a part of a great circle (one that passes through two opposite points of the globe), the geometry is elliptic, and the sum of the angles of triangles is greater than that of two right angles. Axioms are now just some postulates that we choose as a basis.

For some reason, today's logic did not first follow the lead of geometry, as a theory of hypothetical reasoning from axioms, but was formulated as a theory of logical truth on which even truth in mathematics was to be based. Here, then, is the essential tension of the following account: truth or proof?

1.2. ARISTOTLE'S DEDUCTIVE LOGIC

Aristotle's system of deductive logic, also known as the "theory of syllogisms," has been interpreted in various ways in the long time since it was conceived. The situation is no different from the reading

of other chapters of the formal sciences of antiquity, such as Euclid's geometry and the works of Archimedes. When Frege invented predicate logic, he finished the presentation proudly with a reconstruction of the Aristotelian forms of propositions, such as *Every A is B* that is interpreted as $\forall x(A(x) \supset B(x))$, with a universal quantification over some domain and the predicates A and B. Frege similarly reproduced Aristotelian inferences, such as the conclusion *Every A is C* obtained from the premisses *Every A is B* and *Every B is C*, in the way shown in Section 4.2. Frege's interpretation has become the most common one, but we can also consider Aristotle's logic in itself, without such interpretations, and see that it works to perfection.

(A) THE FORMS OF PROPOSITIONS. Aristotle's system of deductive logic is presented in his book *Prior Analytics*. It begins with four forms of propositions with a *subject A* and a *predicate B*, as shown in table 1.1.

Table 1.1. The Aristotelian forms of propositions

Universal affirmative:	*Every A is B*.
Universal negative:	*No A is B*.
Particular affirmative:	*Some A is B*.
Particular negative:	*Some A is not-B*.

There is also an *indefinite* form of proposition, *A is B*, not usually present in the rules of inference, even though it can so be (*cf.* 26a28).

Subjects and predicates together are *terms*. The indefinite form *A is B* has various other readings: *subject A has the predicate B, predicate B belongs to subject A, B belongs to A,* etc. The last one is preferred by Aristotle, and he writes the other forms similarly:

> *B belongs to every A, B belongs to no A, B belongs to some A, B does not belong to some A.*

Here the copula is written as one connected expression between the predicate and the subject, which underlines the formal character of the sentence construction.

A second reading is given to *B does not belong to some A*, namely *B does not belong to all A* (in 24a17). Another useful way of expressing

the Aristotelian propositions is:

Every A is B, No A is B, Some A is B, Not every A is B.

Now the indefinite form *A is B* is a constant part of the propositions, and the varying quantifier structure is singled out. It is seen clearly that the first and last are opposites, and that the second and third are likewise opposites.

The main principle in the formation of propositions is that subjects and predicates are treated symmetrically in the universal and particular propositions: Whenever *Every A is B* is a proposition, also *Every B is A* is one, and similarly for the universal negative and the particular forms. A formal structure is imposed that is not a natural feature of natural language, as in *Some man is wise*, the *converse* of which, *Some wise is a man*, would not be a natural expression but would have to be paraphrased, as in *Some wise being is a man.*

The *universal quantifier* of the Aristotelian form *Every A is B* is explained as follows in the *Prior Analytics* (24b28):

A thing is said of all of another when there is nothing to be taken of which the other could not be said.

Aristotle is saying that universality means the lack of a counterexample, a common idea in logic ever since. The other forms of quantification are explained similarly and are used in a justification of the Aristotelian rules. However, we do not need to go into the details, because it will turn out to be sufficient to treat the four Aristotelian forms as just atomic formulas with two terms but no further internal structure.

(B) THE PRINCIPLE OF INDIRECT PROOF. The two pairs *Every A is B*, *Some A is not-B* and *No A is B*, *Some A is B* form between themselves *contradictory opposites*. Furthermore, because from *No A is B* the weaker *Some A is not-B* follows, also *Every A is B* and *No A is B* together lead to a contradictory pair. We indicate the contradictory opposite of a proposition P by the orthogonality symbol, $P^{\perp}$. (Note that $P^{\perp\perp}$ is identical to P.) In general, if an assumption P has led to contradictory consequences Q and $Q^{\perp}$, $P^{\perp}$ can be concluded and the assumption P *closed*. The rule of indirect proof thus takes on the schematic form in table 1.2, with an *inference line* that separates the two premisses above it from the conclusion below.

Table 1.2. The scheme of indirect proof

$$\dfrac{\begin{array}{cc}\overset{1}{P^m} & \overset{1}{P^n}\\ \vdots & \vdots\\ Q & Q^\perp\end{array}}{P^\perp}\ RAA,1$$

This schematic proof figure is to be understood as follows. The assumption may appear among those that were used in the derivations of Q and $Q^\perp$, respectively. Any numbers $m, n \geqslant 0$ of occurrences of P in the two *subderivations* can be closed at the inference. The closed ones are indicated by a suitable label, such as a number, so that each instance of rule *RAA* (for *reductio ad absurdum*) clearly shows which occurrences of P are closed at the inference. It is typical of Aristotle's proofs that an assumption closed in indirect proof occurs just once: either $m = 1, n = 0$ or $m = 0, n = 1$. We then have one of:

Table 1.3. Aristotelian special cases of indirect proof

$$\dfrac{\begin{array}{cc}\overset{1}{P} & \\ \vdots & \\ Q & Q^\perp\end{array}}{P^\perp}\ RAA,1 \qquad \dfrac{\begin{array}{cc} & \overset{1}{P}\\ & \vdots\\ Q & Q^\perp\end{array}}{P^\perp}\ RAA,1$$

As mentioned, Aristotle's derivations have at most one instance of indirect proof, as a last rule. A rule of indirect proof in which the premisses of *RAA* are *Every A is B* and its *contrary No A is B* can be derived from the second of the following conversion rules.

(C) THE RULES OF CONVERSION AND SYLLOGISM. Aristotle's system of deductive logic begins properly with his *rules of conversion*:

$$\dfrac{\textit{No A is B}}{\textit{No B is A}}\ \textit{No-Conv} \qquad \dfrac{\textit{Every A is B}}{\textit{Some B is A}}\ \textit{Every-Conv} \qquad \dfrac{\textit{Some A is B}}{\textit{Some B is A}}\ \textit{Some-Conv}$$

The third rule of conversion is a *derivable rule*. Its conclusion is derivable from its premiss by the first conversion rule and the rule of indirect proof. Aristotle, in fact, notes the same (24a22): Given the premiss *Some A is B*, assume the contrary of the conclusion of *Some-Conv*, namely *No B is A*. Then, by *No-Conv*, *No A is B*, a contradiction, so that *Some B is A* follows.

Two more rules enter into Aristotle's deductive logic, the proper *syllogisms* as this word has been understood for a long time. Its meaning in Aristotle vacillates between a single syllogism and what today is called a deduction. The major part of the *Prior Analytics* deals with derivations that consist of a single syllogism, conversions, and a single step of indirect inference. The two syllogistic rules are (25b38–26a2):

Table 1.4. Aristotle's formulation of the syllogistic rules

When A of every B and B of every C, it is necessary that A is said of every C. For we have explained above what we mean by every.

Correspondingly also when A of no B, B instead of every C, then A will not belong to any C.

The added clause hints at a justification of the rule in terms of the meaning given to universal quantification, as discussed in detail in von Plato (2016).

We write the preceding two rules as

$$\frac{\textit{Every A is B} \quad \textit{Every B is C}}{\textit{Every A is C}}\ \textit{Every-Syll} \qquad \frac{\textit{Every A is B} \quad \textit{No B is C}}{\textit{No A is C}}\ \textit{No-Syll}$$

The order of the premisses, from left to right, is the reverse of that in Aristotle's proof texts. At some stage, it became customary to read the propositions with the subject first, so, to have the middle term in the middle, the order of the premisses was changed.

When one reads Aristotle's examples of syllogistic inference, the real deductive structure is somewhat hidden behind the convention of a linear sentence structure. Here is an example from *Prior Analytics* (27a10):

If M belongs to every N and to no X, then neither will N belong to any X. For if M belongs to no X, then neither does X belong to any M; but M belonged to every N; therefore, X will belong to no N (for the first figure has come about). And since the privative converts, neither will N belong to any X.

Let us number the sentences of this text in the succession in which they appear, rewritten so that each single purely syllogistic sentence

is identified (i.e., with the connectives and rhetorical expressions eliminated):

1. *M belongs to every N.*
2. *M belongs to no X.*
3. *N belongs to no X.*
4. *M belongs to no X.*
5. *X belongs to no M.*
6. *M belongs to every N.*
7. *X belongs to no N.*
8. *N belongs to no X.*

The *assumptions* in the syllogistic proof are 1 and 2. Line 3 states the *conclusion* of the proof. Line 4 *repeats* assumption 2, and line 5 gives the result of applying of a conversion rule to the premiss given by line 4. Line 6 repeats the assumption from line 1. Line 7 gives the conclusion of a syllogistic rule from the premisses given by lines 5 and 6. Line 8 gives the conclusion of a conversion rule applied to the premiss given by line 7. It is at the same time the sought-for conclusion expressed on line 3.

The formal nature of Aristotle's proof text is revealed by the repetition, twice, of assumptions or previous conclusions, on lines 4 and 6. These repetitions are made so that the application of a rule of inference in the proof text can follow a certain pattern: A one-premiss rule such as conversion is applied to a sentence in a way such that the conclusion immediately follows the sentence. A two-premiss rule such as a syllogism is applied to two premisses, given in succession in a predetermined order, so that the conclusion immediately follows the premisses. Let us collect these observations into a proof in which every step is justified in detail. The beginning of the proof is at the place where the word *For* occurs:

1. *M belongs to no X.*	assumption
2. *X belongs to no M.*	from 1 by *No-Conv*
3. *M belongs to every N.*	assumption
4. *X belongs to no N.*	from 2 and 3 by *No-Syll*
5. *N belongs to no X.*	from 4 by *No-Conv*

(D) THE DEDUCTIVE STRUCTURE OF SYLLOGISTIC PROOFS. The linearity of Aristotle's proofs texts hides a part of their true deductive structure. In the example, the assumptions are *independent* of each other: neither is derivable from the other by the rules. Leaving out the tentative statement of the conclusion from line 3, the *deductive dependences* on assumptions in Aristotle's proof are that line 4 depends on assumption 2, line 5 likewise on 2 through 4, line 6 on 1, line 7 on 1 and 2, and line 8 on 1 and 2.

Aristotle's linear derivations can be translated into a tree form by using the following two clauses:

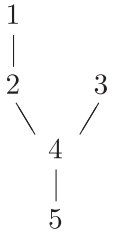
1. *Take the last sentence and draw a line above it, with the name of the rule that was used to conclude it next to the line. Write the sentences that correspond to the lines of the premisses of the last rule above the inference line.*

2. *Repeat the procedure until assumptions are arrived at.*

Here is what we get when the translation algorithm is applied to lines 1–5 of the preceding example:

$$\dfrac{\dfrac{1.\ M \text{ belongs to no } X}{2.\ X \text{ belongs to no } M}\ \textit{No-Conv} \qquad 3.\ M \text{ belongs to every } N}{\dfrac{4.\ X \text{ belongs to no } N}{5.\ N \text{ belongs to no } X}\ \textit{No-Conv}}\ \textit{No-Syll}$$

The *deductive dependences* in Aristotle's proof are now univocally determined, as can be seen from the derivation tree. They are as follows:



As the next example, consider the following indirect syllogistic derivation (from *Prior Analytics*, 28b17):

> *If R belongs to every S but P does not belong to some, then it is necessary for P not to belong to some R. For if P belongs to every R and R to every S, then P will also belong to every S; But it did not belong.*

The translation into tree form gives

$$\dfrac{\dfrac{\overset{3}{\textit{Every } R \textit{ is } P} \quad \textit{Every } S \textit{ is } R}{\textit{Every } S \textit{ is } P}\,\textit{Every-Syll} \qquad \textit{Some } S \textit{ is not-} P}{\textit{Some } R \textit{ is not-} P}\,\textit{RAA},3$$

To finish this brief tour of Aristotle's logic, we show that his practice of making at most one last step of indirect inference is justified. The proof system consists of the five rules *Every-Conv, No-Conv, Every-Syll, No-Syll*, and *RAA*, and we have the following theorem.

Theorem. Normal form for derivations. *All derivations in Aristotle's deductive logic can be so transformed that the rule of indirect proof is applied at most once as a last rule.*

Proof. Consider an uppermost instance of *RAA* in a derivation. If it is followed by another instance of *RAA*, we have a part of derivation such as

$$\dfrac{\dfrac{\overset{1}{P} \quad \vdots \quad \vdots \qquad \overset{2}{R}}{Q \quad Q^{\perp}}\,\textit{RAA},1 \qquad \vdots}{P^{\perp} \qquad\qquad P}\,\textit{RAA},2$$
$$R^{\perp}$$

This derivation is transformed into

$$\dfrac{\overset{1}{R} \quad \vdots \quad \vdots}{P \quad \vdots \quad Q \quad Q^{\perp}}\,\textit{RAA},1$$
$$R^{\perp}$$

Two derivations have been *combined* in the transformation, when the derivation of P from R has been continued by the derivation of Q from P.

The preceding transformation is repeated until there is just one instance of *RAA*. If the conclusion $R^{\perp}$ is existential, it cannot be a premiss in any rule, and the claim of the theorem follows. If the

conclusion is universal, we have one of the following:

$$\dfrac{\begin{array}{cc}\overset{1}{\textit{Some A is not-B}} & \\ \vdots & \vdots \\ Q & Q^{\perp}\end{array}}{\textit{Every A is B}}\ \textit{RAA},1 \qquad \dfrac{\begin{array}{cc}\overset{1}{\textit{Some A is B}} & \\ \vdots & \vdots \\ Q & Q^{\perp}\end{array}}{\textit{No A is B}}\ \textit{RAA},1$$

There are by assumption no instances of *RAA* other than the ones shown. Therefore, because existential formulas can be premisses only in the instances of *RAA* shown, the derivations of the left premisses of *RAA* are degenerate, with *Some A is not-B* $\equiv Q$ and *Some A is B* $\equiv Q$, respectively. The derivations are therefore

$$\dfrac{\overset{1}{\textit{Some A is not-B}} \quad \begin{array}{c}\vdots \\ \textit{Every A is B}\end{array}}{\textit{Every A is B}}\ \textit{RAA},1 \qquad \dfrac{\overset{1}{\textit{Some A is B}} \quad \begin{array}{c}\vdots \\ \textit{No A is B}\end{array}}{\textit{No A is B}}\ \textit{RAA},1$$

The conclusion is equal to the right premiss in both, and therefore the instances of *RAA* can be removed. QED.

The proof depends crucially on a subtle property of Aristotle's minimal deductive system of five rules, namely that existential formulas are not premisses in rules other than *RAA*.

The formulas of Aristotle's deductive logic are atomic formulas in today's terminology, and his rules act only on such atomic formulas. The question of the derivability of an atomic formula from given atomic formulas used as assumptions is known as the *word problem*. The terminology stems from algebra where the word problem concerns the derivability of an equality from given equalities. The solution of this problem in Aristotle's deductive logic, i.e., the decidability of derivability by his rules, follows at once by the preceding result on normal form. It is sufficient to show that the terms in a derivation of P from the assumptions Γ can be restricted to those included in the assumptions and the conclusion. If the proof is direct, this is so because terms in any formula in the derivation can be traced up to assumptions. Otherwise, the last step is indirect, but the closed assumption is $P^{\perp}$, so that the terms in a derivation are as in the direct case. With a bounded number of terms, there are a bounded number of distinct formulas. The number of possible consecutive steps of inference in a

loop-free derivation, i.e., the height of a branch in a derivation tree, is bounded by the number of distinct formulas and we have the following theorem.

Theorem. Termination of proof search in Aristotle's deductive logic. *The derivability of a formula P from given formulas Γ used as assumptions is decidable.*

The only thing that has been added to Aristotle's proofs as he wrote them is the tree form that keeps track of what depends on what within a proof.

1.3. INFINITY AND INCOMMENSURABILITY

I shall give two ancient proofs about numbers. The first is Euclid's famous proof of the infinity of prime numbers, and the second is the Pythagorean proof of the irrationality of the square root of 2, as given by Aristotle. Both proofs have been the source of infinite misunderstandings. In particular, both have been described as *indirect proofs* which they are not. Furthermore, the first one is a clear proof by induction, in contrast to repeated claims that such proofs surfaced only with the work of Pascal in the seventeenth century. One's natural question is: How could there have been an ancient arithmetic without this crucial principle of proof? There wasn't, but a mere reading of the ancient texts may not be sufficient for seeing it.

(A) THE INFINITY OF PRIMES. Euclid's *Elements* contains 13 "books" as they were called, with books VII to IX being dedicated to arithmetic instead of geometry. The last of these includes Euclid's famous proof of the infinitude of prime numbers, theorem 20:

> *The prime numbers are more than any proposed multiplicity of prime numbers.*

The proof goes as follows, in my translation from Fabio Acerbi's formidable 2007 Greek-Italian edition of all of Euclid in one 2720-page volume! It can be read with some effort exactly as it was written some time around 200 B.C.—no explanations and the considerable delight of figuring from the context the meaning of Euclid's notation, with just the

modest hint that the letters as they appear come from their alphabetical order in Greek:

> Let the prime numbers proposed be A, B, Γ. I say that there are more prime numbers than A, B, Γ.
>
> Assume the least number to have been taken that is divisible by A, B, Γ, and let it be ΔE, and let a unit ΔZ have been summed to ΔE. Then EZ is in any case either prime or not. Let it be in the first place prime. Then more prime numbers than A, B, Γ have been found, namely A, B, Γ, EZ.
>
> But now, let EZ not be prime, so then it is divisible by a certain prime number. Let it be divisible by prime H. I say that H is not the same one of any of the A, B, Γ. If that should be possible, let it so be. And A, B, Γ divide ΔE, so then even H divides ΔE. And it divides also EZ; it divides also the unit ΔZ that remains because H is a number, which is absurd. So there is not the case that H is the same as just one of the A, B, Γ. And it was assumed to be prime. It then results that more prime numbers have been found, A, B, Γ, H, than the proposed multiplicity A, B, Γ, which was to be proved.

The same proof in today's terminology is: Let n prime numbers $p_1, \ldots p_n$ be given. Form the product $p_1 \times \cdots \times p_n$, add one to it, and denote this number by p. If p is prime, we have $n + 1$ primes. If p instead is divisible, it has at least one prime divisor q. This divisor is distinct from each of the previous p_i, because each of them leaves a rest if used to divide p. So we have $n + 1$ primes.

If we add to this the fact that 2 is a prime number, we have the base case:

2 *is a prime number.*

The step case is

If there are n prime numbers, there are $n + 1$ *prime numbers.*

Euclid's conclusion is that *the prime numbers are more than any proposed multiplicity of prime numbers*. It should be kept in mind how the Ancients saw the concept of infinity, as something that can be extended beyond any bound rather than as a finished totality. Euclid uses precisely this notion in his proof: He does not write that *all* numbers have a property but instead gives a procedure of extension

beyond any given number. In this light, it seems rather foolhardy to maintain that Euclid did not give an inductive proof, especially as his result cannot be proved without induction or equivalent.

The notion of potential infinity applies even in the geometrical parts of the *Elements*. One of the construction postulates is *to extend a given line segment indefinitely.* Euclid's lines are not actually infinite in both directions but just rather extensible beyond any point.

Once it is accepted that Euclid gives an inductive proof expressed in the language of his notion of potential infinity, other results in Euclid's arithmetic should be found as evidence for the permanence of his proof pattern. Namely:

1. It is known that there is at least one number a such that some property $P(a)$ holds for a.
2. Assuming that there are n such numbers, there are more than n.
3. Conclusion: Such numbers "are more than any proposed multiplicity."

In Euclid's proof, the inductive step is produced by a construction process from a given n to $n+1$. Many inductive proofs are so simple that we step silently over them, perhaps with the added word "obviously." However, "obviously" is no recognized step in a proof that stands on its own feet.

(B) THE IRRATIONALITY OF THE SQUARE ROOT OF 2. Aristotle reports in §23 of the *Prior Analytics* the following proof of the Pythagorean theorem about the "incommensurability of the side and diagonal of the square." The proof, in modern notation and reading, is as follows. Assume $\sqrt{2}$ is rational. Then there are n, m such that $\sqrt{2} = n/m$, and let these be relatively prime, i.e., assume that n and m have no common divisors. With both sides squared, we get $2 = n^2/m^2$, so $n^2 = 2m^2$. But now, if n^2 is even, n itself has to be even, so there is some k such that $n = 2k$. By $n^2 = 2m^2$, we get $2^2k^2 = 2m^2$, and dividing both sides by 2, we get $2n^2 = m^2$, by which m also is even, so 2 divides both n and m against the assumption that n and m are relatively prime. Therefore, the assumption that $\sqrt{2}$ is rational led to a contradiction, by which it is irrational.

There is no limit to the number of books, from textbooks for schoolchildren to advanced books written by otherwise competent logicians, that declare the preceding proof to be a *proof by contradiction, a proof*

by reductio ad absurdum, an indirect proof. The logically minded reader who keeps things in a conceptual order can only despair and repeat the basics: What is it that we are proving? We are proving the claim that $\sqrt{2}$ is an irrational number. What does it mean to be an irrational number? It means that there do *not* exist two integers n, m such that n/m is equal to the number. At this point, says our logician, the *direct* way to prove a negative statement such as $\neg A$ is to assume A, to derive a contradiction, and to conclude $\neg A$. In an indirect proof, a negative assumption such as $\neg A$ is made, a contradiction is derived, and a positive claim A is concluded. The most typical example is: Assume there does not exist a number x such that $P(x)$, derive a contradiction, and conclude indirectly that there exists an x such that $P(x)$. The pattern of proof is different from the earlier Pythagorean proof of a negative proposition.

The logical notation and rules of proof of formal logic were invented for the purpose of making steps in mathematical proofs explicit. Let us use some of this notation and steps of proof to see that there is no step of indirect inference in the proof of irrationality of $\sqrt{2}$. We start with implication $A \supset B$. The principle of proof is that if A is *assumed* and B *derived under assumption* A, then $A \supset B$ can be concluded with no assumption A left. The neatest way to treat negation $\neg A$ is to use a constant *false proposition* $\perp$ and to define $\neg A$ as $A \supset \perp$. A proof of a negation is obtained if $\perp$ is derived from the assumption A. This is a *direct* proof of a negative proposition. In arithmetic, we can use $0 = 1$ for $\perp$.

In the Pythagorean proof, the task is to prove $\neg\exists x \exists y(\sqrt{2} = x/y)$. To prove this, assume $\exists x \exists y(x/y = \sqrt{2})$, just a formal notation for the previous "there are n, m such that $\sqrt{2} = n/m$," and try to derive a contradiction. The existential quantifiers of an assumption are treated through *instantiation by eigenvariables*; that is, fresh symbols n and m in place of x and y and the assumption $n/m = \sqrt{2}$, with the further property that n and m are relatively prime. None of the simple arithmetic steps up to the contradiction is indirect, though one step is in itself quite interesting: *If n^2 is even, n itself has to be even.* The definition in logical notation is $Even(x) \equiv \exists y(x = 2 \cdot y)$, a *finitary* definition despite the quantifier, because, given x, there is a bounded number of possible values for y. As "obviously" is not allowed for a

step of proof, an attempt to cover the "interesting step" will lead to the realization that the only way is the inductive one.

Indirect inference can be formulated as the following rule: from $\neg\neg A$ to conclude A. If our logic is classical, these two are equated. Therefore, our principles of proof have to be formulated so that such equating does not creep in unwanted. We can put the matter overall as:

> *In the Pythagorean proof, the distinction between being rational and not being irrational is precisely what is needed to have a separate notion of indirect proof.*

Observations similar to those about the Pythagorean proof apply to Euclid's proof. A proof could begin with the assumption that there is only a finite number of prime numbers, and let this number be n. Now a contradiction is derived. Thus, it is not the case that the number of primes is finite, and we have a direct proof of a negative claim. Euclid's claim, though, is formulated in positive terms, and his proof gives an algorithm by which, given any number of primes, one more can be effectively produced. Euclid's algorithm does not necessarily produce a prime greater than the given ones, and it leaves enormous gaps. If we start from 2, Euclid's method gives three primes in succession, first $2 + 1 = 3$, then $2 \times 3 + 1 = 7$, then $2 \times 3 \times 7 + 1 = 43$, until $2 \times 3 \times 7 \times 43 + 1 = 1807$ is reached. This number has the prime 13 as a factor, so now we get $2 \times 3 \times 7 \times 13 \times 43 + 1 = 23479$, with the prime 53 as a factor. The algorithm keeps producing composite numbers, with the prime divisors 5 and 89, so there are at least four in succession after the first four primes produced.

Let us look a bit more closely at the logic of Euclid's proof. The first essential step in it is the phrase *Then EZ is in any case either prime or not,* an instance of the law of excluded middle $A \vee \neg A$. This would in general qualify for a genuinely classical, indirect step: Assume the premiss of an indirect inference, namely $\neg\neg A$, and the second of the possibilities in excluded middle is contradicted, with just the first one left, namely A as concluded from $\neg\neg A$. However, the property of being a prime number is *decidable* in a bounded number of steps, and the instance of excluded middle does not have the effect of producing genuinely classical, i.e., undecidable case distinctions. More

generally, it can be shown that all results about the natural numbers that don't require the use of quantifiers (*for all* and *there exists*, or ∀ and ∃) for their expression have finitary proofs, appearances to the contrary.

The structure of a mathematical proof must in principle be visible from the way the proof is written. When pressed enough, a mathematician should be able to produce a proof composed in a transparent way of such simple parts that no one competent in mathematics can doubt it. When something in a proof is assumed to be false, a level of understanding is imported that has no place there. Such aspects belong to the background knowledge that guides what we try to prove. An assumption is just an assumption; it can turn out false at some point in the sense that a contradiction is reached, and then its negation can be concluded. In fact, in the presence of more than one assumption, it is the assumptions together that lead to a contradiction. The negation of any one of the assumptions can be concluded with the rest kept in place. Similarly, if a negative assumption is made, indirect proof leads to the positive conclusion.

Explicit rules of proof leave no place for a second level of consideration of truth inside a proof, beyond the level of formal inference. At most, we can say: *If* the assumptions are true, *if* the proof is correct, *then* even the conclusion is true.

1.4. DEDUCTIVE AND MARGINAL NOTIONS OF TRUTH

(A) LOGICAL TRUTH. Today's logic had its beginnings in the work of Frege, Peano, and Russell. In Russell's work, logic had taken the same form as traditional geometry: There were as starting points logical axioms, and just two rules of logical inference. Frege and Russell advocated a doctrine, called *logicism*, by which the axioms express the most basic logical truths, and the rules just make evident other such truths. The scheme even included that first arithmetic, and then the rest of mathematics, be reduced to logic. It is somewhat odd that logic followed the old geometric tradition, for by this time geometric axioms were no longer viewed as geometric truths but rather as postulates that may hold in one situation and fail in another.

Frege was the first to detail the principles of reasoning with *generality*, with the idea that if we can prove a property $A(x)$ for an *arbitrary* x, then we are allowed to conclude the universal claim $\forall x\, A(x)$. Arbitrariness means simply that the *eigenvariable* x of the step of inference does not occur free anywhere in any assumptions on which the premiss of inference to generality $A(x)$ may depend.

Frege took the crucial step into today's logic. His notation was impossible, but Bertrand Russell adapted Peano's notation to Frege's logic, in the great synthetic work *Principia Mathematica* that he wrote together with Alfred Whitehead. The *Principia* contained a correct account of universality, with the instantiation axiom $\forall x\, A(x) \supset A(a)$ for any chosen object a, and the converse rule of generalization.

Existence is a kind of dual to universality. Thus, it can be taken as an axiom that an instance implies existence; that is, $A(a) \supset \exists x\, A(x)$. There is a rule dual to generalization that tells how to deal with an existential assumption $\exists x\, A(x)$: Take an arbitrary instance $A(y)$, and if some claim C follows from $A(y)$, independently of the choice of y, it follows from $\exists x\, A(x)$. This rule, with y an eigenvariable, is used informally all through the history of logic and mathematics, but it did not get its first explicit formulation until the late 1920s.

Frege's rule and axiom give a clear sense to generality: To infer generality, prove an arbitrary instance. In the other direction, if a generality is at hand, either assumed or proved, instances can be taken. But is inference enough? How should that which can be inferred relate to truth?

Philosophical realism dictates an absolute notion of truth. Somewhere in a big imaginary book is a list of all truths. To be a truth just means to be in the list. As the list is infinite, we human beings don't have direct access to it but have to proceed on the basis of evidence for truth. In the best of cases, such evidence amounts to a proof, or inference in the sense of logic and mathematics. The list is not affected by what we happen to have proved; it's at most worth a marginal remark: This truth was even proved by human beings.

By the 1920s, especially under the influence of Ludwig Wittgenstein, the view of logical truths as *tautologies* emerged. A tautology is a logical sentence that is true under all possible circumstances, or true

by virtue of its form. Such truths can be found out by analyzing this form:

1. $A \& B$ is true when both A and B are true, otherwise it is false.
2. $A \vee B$ is true when at least one of A and B is true, otherwise it is false.
3. $A \supset B$ is true if B is true as soon as A is true, otherwise it is false.
4. $\neg A$ is true when A is false, otherwise it is false.

Clause 3 can be put also as: $A \supset B$ is true when A is false or B is true, otherwise it is false.

Given a formula such as $(P \supset Q) \vee (Q \supset R)$, built out of three atomic formulas P, Q, and R that do not have any logical structure, there are altogether $2 \times 2 \times 2 = 8$ combinations of truth values to P, Q, and R. If Q is true, $P \supset Q$ is true by clause 3 and the disjunction $(P \supset Q) \vee (Q \supset R)$ as well by clause 2. If Q is false, $Q \supset R$ is true and so is $(P \supset Q) \vee (Q \supset R)$. Whichever way P, Q, and R are, $(P \supset Q) \vee (Q \supset R)$ turns out true, with no consideration of P and R. Such a tautology does not exclude any possible state of affairs, and therefore it is empty: It does not state anything. Combined with the logicist thesis, even mathematical truths are mere empty tautologies. Moreover, any relation they might bear to each other is just apparent, as in the preceding example. Say, with any two mathematical claims A and B, we get from that example, with A in place of P and R and B in place of Q, that either $A \supset B$ or $B \supset A$, a rather startling result by which any mathematical claim implies any other, or the other way around!

Wittgenstein listed in his little book *Tractatus Logico-Philosophicus*, originally just the German "Logisch-Philosophische Abhandlung," a number of logical maxims, from 1 (the world is all that is the case) to 7 (what one cannot speak about, on that one must be silent). One maxim is that tautologies stand on their own feet, so to say; there is no need for a concept of inference from other tautologies or assumptions (maxim 6.1265):

> One can always conceive logic in such a way that every theorem is its own proof.

Axiomatic propositional logic has a few axioms and just the rule of inference: If $A \supset B$ and A have been proved, B can be inferred.

The notion of a tautology can be used in place of the axioms and inferences from them; inference is indeed completely absent from the *Tractatus*.

One would normally think that if a philosophy leads to consequences such as that mathematical theorems have no content but just form, and that there is never any relation between one theorem and another as each theorem is its own proof, there is something wrong with it, but this was not the view taken in the 1920s or 1930s. Georg Kreisel, who was even a student of Wittgenstein's, told me in a discussion about this matter in the summer of 2010: "A position was taken to its extreme to show its absurdity."

Proponents of the tautology view, such as Wittgenstein and the logical empiricists who followed him, did not recognize that there is no account of quantificational logic without rules of inference. We shall see later how desperately Wittgenstein struggled with the quantifiers, but no amount of inward-bound philosophical reflection could replace the command over quantificational inferences reached in other quarters in the latter part of the 1920s, Göttingen in the first place. With his characteristic blindness to what others had accomplished, Wittgenstein's teaching had a devastating effect on some of his students, who never understood quantificational logic under his guidance. The first victim of this attitude was Frank Ramsey whose 1926 essay on mathematical logic makes for very sad reading. As to the logical empiricists, Rudolf Carnap, perhaps their main proponent, published in 1929 a short "outline" of Russell's *Principia*, the *Abriss der Logistik*. One searches in vain for the rule of universal generalization in this booklet: Carnap's logic is propositional, augmented with an axiom of universal instantiation.

Ignorant of the crucial role of a rule of generalization, the proponents of the tautology view extended, or rather pretended to extend, the truth conditions of classical propositional logic to quantificational formulas by two additional clauses:

5. $\forall x\, A(x)$ is true in a given domain $\mathcal{D}$ of objects whenever $A(a)$ is true for all a in $\mathcal{D}$, otherwise it is false.
6. $\exists x\, A(x)$ is true in a given domain $\mathcal{D}$ of objects whenever $A(a)$ is true for at least one a in $\mathcal{D}$, otherwise it is false.

What happens in the case where the domain $\mathcal{D}$ is infinite? With $a_1, a_2, a_3 \ldots$ the objects, from 5 and 6 we then have the following:

$\forall x\, A(x) A$ is true in $\mathcal{D}$ if $A(a_1)$ is true in $\mathcal{D}$ and $A(a_2)$ is true in $\mathcal{D}$ and $A(a_3)$ is true in $\mathcal{D}\ldots$

$\exists x\, A(x) A$ is true in $\mathcal{D}$ if $A(a_1)$ is true in $\mathcal{D}$ or $A(a_2)$ is true in $\mathcal{D}$ or $A(a_3)$ is true in $\mathcal{D}\ldots$

How should we put this? Perhaps it would do to say that *there is no well-founded explanation of truth* under the tautology notion extended to infinite domains. It would not be sufficient to find, next to a claim, an oracular marginal remark to the effect that the claim is true.

In Hilbert's Göttingen, it was realized by 1920 that the logical steps in mathematical proofs could be represented formally as steps in propositional and quantificational logic. Hilbert's earlier work, such as that on foundations of geometry in 1899, had left the logical part on an intuitive basis. Some twenty-odd years later, as a first step under the leadership of Hilbert's assistant Paul Bernays, pure predicate logic got a clear and concise formulation. The next step was to apply it to mathematical axiom systems. They would appear as premisses in formal logical derivations, and thus not as given truths but as hypotheses that could hold in one situation, fail in another, such as the Euclidean axiom of parallels. A crucial component here was to show that a logical derivation of a theorem P from given hypotheses H could be turned into a derivation of the implication $H \supset P$ in pure logic. Step by step, the view of logic and mathematics as a collection of tautologies gave way to the idea of logic as the deductive machinery of mathematics.

(B) UNDECIDABILITY. The tautology view of logic and mathematics, and the *verificationist* philosophy of truth more generally, derives from the *decidability* of classical propositional logic: There is an algorithm for deciding if a proposition is a logical truth. Quantificational logic instead is not decidable, but that result was not confirmed until 1936. Now the choice becomes one between the tautology view and quantificational logic.

There is another notion of decidability, quite different from the preceding one about logical truth, namely the decidability of the atomic formulas of a given mathematical theory. The arithmetic of natural numbers is the best example here. It can be formulated so that the

equality of two numbers, $n = m$, is its only basic notion. Then, for any two numerical terms n and m, $n = m$ is either a true or a false numerical equation, something that can be decided by computing the values on both sides, as in $7 + 5 = 3 \times 4$. As suggested in Section 1.3, the way to express this matter inside a logical calculus is to change the underlying pure logic so that the law of excluded middle is not applied as a general logical principle but just for those basic relations that are meant to be decidable. Thus, in arithmetic we pose $n = m \vee \neg n = m$ for any numerical terms n, m. It follows that all quantifier-free formulas A are decidable; that is, that $A \vee \neg A$ is provable for any such formula. Here we have a way of expressing decidability that is lost in classical logic. The law of excluded middle is an example of a tautology, for if A is true, so is $A \vee \neg A$, and if A is false, $\neg A$ is true and thereby also $A \vee \neg A$. It does not follow, in general, that either A or $\neg A$ would be a tautology. If instead arithmetic is formulated constructively, one of A and $\neg A$ is provable whenever $A \vee \neg A$ is.

The possibility of undecidable basic relations took a long time to become understood. One clear expression of such awareness is found in Hilbert's 1894 lectures on geometry, with the idea that the intersection point of two lines escapes to infinity as the lines approach parallelism (Hilbert 2004, p. 75):

> It escapes our experience whether one can always *find a point of intersection* for 2 lines. *We leave the matter undecided for the time being and state only*:
>
> 2 lines on a plane have either one or no points in common.

In Emile Borel's version of constructivism from the first decade of the twentieth century, there is a rather clear recognition that the equality of real numbers cannot be a decidable relation. For example, there is a way of computing what is known as Riemann's constant C, and the computation has so far given $0.4999\ldots$. If all successive decimals are 9's, we have $C = 0.5$, otherwise $\neg C = 0.5$ holds, but the answer is unknown.

The same insight as in Borel's work got a more forceful expression in L. Brouwer's ideas about real numbers in the 1920s. He replaced equality of real numbers as a basic notion with the *apartness* of two reals that we can write as $a \neq b$ (Brouwer 1924a). That a and b are in

this way distinct requires that there be a positive lower bound for their difference. Thus, a finite determination of values will verify apartness, though not falsify it, the precise contrary to the case of equality. The latter notion can now be defined as the negation of apartness, and its transitivity comes from the contraposition of Brouwer's *apartness axiom* $a \neq b \supset a \neq c \vee b \neq c$ that is justified as follows. Let a and b be apart, and let it be infinitely difficult to decide if $a \neq c$. Then c must make a positive distance to b so that $b \neq c$.

The point is how to reason with infinitely fine, ideal objects and concepts such as real numbers and their properties and relations. If we follow the lead of the logical positivists, there should be no undecidable basic relations. The doctrine of verificationism requires a method for deciding truth, otherwise a notion is not meaningful. All of traditional synthetic plane geometry, for example, would be declared meaningless metaphysical speculation about infinitely fine points on infinitely thin lines that remain forever unobservable. At the other extreme, there is the unlimited acceptance of classical logic, with its law of excluded middle. Say, begin a proof by $C = 0.5 \vee \neg C = 0.5$ with C Riemann's constant. There are two cases, with two different consequences. As long as the value of C remains undecided, nothing concrete follows from the cases. If instead the classical law is not allowed to enter, computability is maintained. Constructive logical reasoning will never lead from assumptions with a finitary meaning into something infinitistic. That is the main point in the use of a constructive or intuitionistic logic.

The standard view in the 1930s was that finitism and constructivism contain the requirement that all basic relations be decidable and all functions be computable. The requirement on relations is an erroneous view to which one, however, could easily be led if one considered only intuitionistic arithmetic that has a decidable equality as the only primitive relation, instead of also considering the intuitionistic theory of real numbers that cannot be based on a decidable equality, or the first intuitionistic axiomatization ever, Arend Heyting's 1925 system of intuitionistic projective geometry in which decidability of the basic apartness relations cannot be assumed. One of the first outside the intuitionist camp to realize the difference was Kurt Gödel, whose lectures on intuitionism in Princeton in 1941 have been preserved in manuscript form. The extant text begins with two pages of improve-

ments for the lectures, written in his Gabelsberger shorthand. One of the improvements is: "The belief is put aside that a system of axioms has an intuitionistic sense only if the basic concepts are decidable."

From the actual formal work of the intuitionists, Brouwer and his student Heyting in the first place, it can be seen that they required all functions to be computable but not all basic relations to be decidable. So, why was there such a belief or requirement? One reason lies in the possibility to emulate operations through added basic relations. For example, one could substitute the operation of sum in arithmetic by a three-place relation written, say, $\Sigma(a,b,c)$, with the intended meaning that c is the sum of a and b. One result of this move from functions to relations can be seen in Gerhard Gentzen's thesis of 1933, where a theory, elementary arithmetic in this case, gets formulated in pure predicate logic so that general results for the latter can be applied, whereas this would not necessarily be so in a formulation with functions.

(C) TRUTH VS. PROVABILITY. With the insight that axioms can be taken as assumptions in a given situation, logic and mathematics returned to an old Aristotelian form of *hypothetical reasoning*, exemplified by syllogistic inferences that have some assumptions or previously proved statements as premisses. The task of logic is just to guarantee that the steps from assumptions to a conclusion are correct. The latter, in turn, means that whenever the assumptions hold, even the conclusion has to hold. An example from mathematics will be instructive. Let a theorem have the form *For all x and y such that $A(x)$ and $B(x,y)$, there is a z such that $C(z)$.* Let x, y, and z be real numbers so that the conditions $A(x)$ and $B(x,y)$ express some properties and relations between real numbers and $C(z)$ likewise some property of real numbers. A sufficiently detailed proof of such a theorem will do the following: Given any two real numbers a and b in place of x and y, given numerical verifications of the properties and relations $A(a)$ and $B(a,b)$, the proof will produce a real number c and a numerical verification of the property $C(c)$.