A proof of a proposition is a mathematical construction which can itself be treated mathematically. The intention of such a proof thus yields a new proposition. If we symbolize the proposition 'the proposition p is provable' by '$+p$', then '+' is a logical function, viz., "provability." The assertions '$\vdash p$' and '$\vdash +p$' have exactly the same meaning. For, if p is proved, the provability of p is also proved, and if $+p$ is proved, then the intention of a proof of p has been fulfilled, i.e., p has been proved. Nevertheless, the propositions p and $+p$ are not identical, as can best be made clear by an example. In the computation of Euler's constant C, it can happen that a particular rational value, say A, is contained for an unusually long time within the interval within which we keep more narrowly enclosing C so that we finally suspect that $C=A$; i.e., we expect that, if we continued the computation of C, we would keep on finding A within this interval. But such a suspicion is by no means a proof that it will always happen. The proposition $+(C\neq A)$, therefore, contains more than the proposition $(C=A)$.

If we apply negation to both of these propositions, then we get not only two different propositions, '$\neg p$' and '$\neg +p$', but also the assertions, '$\vdash \neg p$' and '$\vdash \neg +p$', are different. '$\vdash \neg +p$' means that the assumption of such a construction as $+p$ requires is contradictory. The simple expectation p, however, need not lead to a contradiction. Here is how this works in our example just cited. Assume that we have proved the contradictoriness of the assumption that there is a construction which proves that A lies within every interval that contains C ($\vdash \neg +p$). But still the assumption that in the actual computation of C we will always in fact find A within our interval need not lead to a contradiction. It is even conceivable that we might prove that the latter assumption could never be proved to be contradictory, and hence that we could assert at the same time both '$\vdash \neg +p$' and '$\vdash \neg \neg p$'. In such an event, the problem whether $C=A$ would be essentially unsolvable.

The distinction between p and $+p$ vanishes as soon as a construction is intended in p itself, for the possibility of a construction can be proved only by its actual execution. If we limit ourselves to those propositions which require a construction, the logical function of provability generally does not arise. We can impose this restriction by treating only propositions of the form 'p is provable' or, to put it another way, by regarding every intention as having the intention of a construction for its fulfillment added to it. It is in this sense that intuitionist logic, insofar as it has been developed up to now without using the function +, must be understood. The introduction of provability would lead to serious complications. Yet its minimal practical value would hardly make it worthwhile to

deal with those complications in detail.[2] But here this notion has given us an insight into how to conceive of essentially unsolvable problems.

We will have accomplished our purpose if we have shown you that intuitionism contains no arbitrary assumptions. Still less does it contain artificial prohibitions, such as those used to avoid the logical paradoxes. Rather, once its basic attitude has been adopted, intuitionism is the only possible way to construct mathematics.

3. The formalist foundations of mathematics

JOHANN VON NEUMANN

I

Critical studies of the foundations of mathematics during the past few decades, in particular Brouwer's system of "intuitionism," have reopened the question of the origins of the generally supposed absolute validity of classical mathematics. Noteworthy is the fact that this question, in and of itself philosophico-epistemological, is turning into a logico-mathematical one. As a result of three important advances in the field of mathematical logic (namely: Brouwer's sharp formulation of the defects of classical mathematics; Russell's thorough and exact description of its methods – both the good and the bad; and Hilbert's contributions to the mathematical-combinatorial investigation of these methods and their relations), more and more it is unambiguous mathematical questions, not matters of taste, that are being investigated in the foundation of mathematics. As the other papers have dealt extensively both with the domain (delimited by Brouwer) of unconditionally valid (i.e., needing no justification) "intuitionist" or "finitistic" definitions and methods of proof and with Russell's formal characterization (which has been further developed by his school) of the nature of classical mathematics, we need not dwell on these topics any longer. An understanding of them is, of course, a necessary prerequisite for an understanding of the utility, tendency, and *modus procedendi* of Hilbert's theory of proof. We turn instead directly to the theory of proof.

The leading idea of Hilbert's theory of proof is that, even if the statements of classical mathematics should turn out to be false as to content, nevertheless, classical mathematics involves an internally closed procedure which operates according to fixed rules known to all mathematicians

[2]The question dealt with in this paragraph was fully clarified only in a discussion with H. Freudenthal after the conference. The results of this discussion are reproduced in the text.

Benacerraf, Paul and Hilary, Putnam (eds.)
Philosophy of Mathematics: Selected Readings
Cambridge U.P. 1983

and which consists basically in constructing successively certain combinations of primitive symbols which are considered "correct" or "proved." This construction-procedure, moreover, is "finitary" and directly constructive. To see clearly the essential difference between the occasionally non-constructive handling of the "content" of mathematics (real numbers and the like) and the always constructive linking of the steps in a proof, consider this example: Assume that there exists a classical proof of the existence of a real number x with a certain very complicated and deep-seated property $E(x)$. Then it may well happen that, from this proof, we can in no way derive a procedure for constructing an x such that $E(x)$. (We shall give an example of such a proof in a moment.) On the other hand, if the proof somehow violated the conventions of mathematical inference, i.e., if it contained an error, we could, of course, find this error by a finitary process of checking. In other words, although the content of a classical mathematical sentence cannot always (i.e., generally) be finitely verified, the formal way in which we arrive at the sentence can be. Consequently, if we wish to prove the validity of classical mathematics, which is possible in principle only by reducing it to the *a priori* valid finitistic system (i.e., Brouwer's system), then we should investigate, not statements, but methods of proof. We must regard classical mathematics as a combinatorial game played with the primitive symbols, and we must determine in a finitary combinatorial way to which combinations of primitive symbols the construction methods or "proofs" lead.

As we promised, we now produce an example of a non-constructive existence proof. Let $f(x)$ be a function which is linear from 0 to 1/3, from 1/3 to 2/3, from 2/3 to 1, and so on. Let

$$f(0)=-1;\quad f\left(\frac{1}{3}\right)=-\sum_{n=1}^{n=\infty}\frac{\epsilon_{2n}}{2^n};\quad f\left(\frac{2}{3}\right)=\sum_{n=1}^{n=\infty}\frac{\epsilon_{2n}}{2^n};\quad \text{and}\quad f(1)=1$$

ϵ_n is defined as follows: if $2k$ is the sum of two prime numbers, then $\epsilon_k=0$; otherwise $\epsilon_k=1$. Obviously $f(x)$ is continuous and calculable with arbitrary accuracy at any point x. Since $f(0)<0$ and $f(1)>0$, there exists an x, where $0\leqslant x\leqslant 1$, such that $f(x)=0$. (In fact we readily see that $1/3\leqslant x\leqslant 2/3$.) However the task of finding a root with an accuracy greater than $\pm 1/6$ encounters formidable difficulties. Given the present state of mathematics, these difficulties are insuperable, for if we could find such a root, then we could predict with certitude the existence of a root $<2/3$ or $>1/3$, according as its approximate value were $\leqslant 1/2$ or $\geqslant 1/2$, respectively. The former case (where the approximate value of the root is $\leqslant 1/2$) excludes both that $f(1/3)<0$ and that $f(2/3)=0$; the latter case (where the approximate value of the root $\geqslant 1/2$) excludes

both that $f(1/3)=0$ and that $f(2/3)>0$. In other words, in the former case the value of ϵ_n must be 0 for all even n but not for all odd n; in the latter case the value of ϵ_n must be 0 for all odd n but not for all even n. Hence we would have proved that Goldbach's famous conjecture (that $2n$ is always the sum of two prime numbers), instead of holding universally, must already fail to hold for odd n in the former case and for even n in the latter. But no mathematician today can supply a proof for either case, since no one can find the solution of $f(x)=0$ more accurately than with an error of 1/6. (With an error of 1/6, 1/2 would be an approximate value of the root, for the root lies between 1/3 and 2/3, i.e., between $1/2-1/6$ and $1/2+1/6$.)

II

Accordingly, the tasks which Hilbert's theory of proof must accomplish are these:

1. To enumerate all the symbols used in mathematics and logic. These symbols, called "primitive symbols," include the symbols '$\sim$' and '$\rightarrow$' (which stand for "negation" and "implication" respectively).
2. To characterize unambiguously all the combinations of these symbols which represent statements classified as "meaningful" in classical mathematics. These combinations are called "formulas." (Note that we said only "meaningful," not necessarily "true." '$1+1=2$' is meaningful but so is '$1+1=1$', independently of the fact that one is true and the other false. On the other hand, combinations like '$1+\rightarrow=1$' and '$++1=\rightarrow$' are meaningless.)
3. To supply a construction procedure which enables us to construct successively all the formulas which correspond to the "provable" statements of classical mathematics. This procedure, accordingly, is called "proving."
4. To show (in a finitary combinatorial way) that those formulas which correspond to statements of classical mathematics which can be checked by finitary arithmetical methods can be proved (i.e., constructed) by the process described in (3) if and only if the check of the corresponding statement shows it to be true.

To accomplish tasks 1–4 would be to establish the validity of classical mathematics as a short-cut method for validating arithmetical statements whose elementary validation would be much too tedious. But since this is in fact the way we use mathematics, we would at the same time sufficiently establish the empirical validity of classical mathematics.

We should remark that Russell and his school have almost completely accomplished tasks 1–3. In fact, the formalization of logic and mathematics suggested by tasks 1–3 can be carried out in many different ways. The real problem, then, is (4).

In connection with (4) we should note the following: If the "effective check" of a numerical formula shows it to be false, then from that formula we can derive a relation $p=q$ where p and q are two different, effectively given numbers. Hence (according to task 3) this would give us a formal proof of $p=q$ from which we could obviously get a proof of $1=2$. Therefore, the sole thing we must show to establish (4) is the formal unprovability of $1=2$; i.e., we need to investigate only this one particular false numerical relation. The unprovability of the formula $1=2$ by the methods described in (3) is called "consistency." The real problem, then, is that of finding a finitary combinatorial proof of consistency.

III

To be able to indicate the direction which a proof of consistency takes, we must consider formal proof procedure – as in (3) – a little more closely. It is defined as follows:

3_1. Certain formulas, characterized in an unambiguous and finitary way, are called "axioms." Every axiom is considered proved.

3_2. If a and b are two meaningful formulas, and if a and $a \rightarrow b$ have both been proved, then b also has been proved.

Note that, although (3_1) and (3_2) do indeed enable us to write down successively all provable formulas, still this process can never be finished. Further, (3_1) and (3_2) contain no procedure for deciding whether a given formula e is provable. As we cannot tell in advance which formulas must be proved successively in order ultimately to prove e, some of them might turn out to be far more complicated and structurally quite different from e itself. (Anyone who is acquainted, for example, with analytic number theory knows just how likely this possibility is, especially in the most interesting parts of mathematics.) But the problem of deciding the provability of an arbitrarily given formula by means of a (naturally finitary) general procedure, i.e., the so-called decision problem for mathematics, is much more difficult and complex than the problem discussed here.

As it would take us too far afield to give the axioms which are used in classical mathematics, the following remarks must suffice to characterize them. Although infinitely many formulas are regarded as axioms (for example, by our definition each of the formulas $1=1$, $2=2$, $3=3$,... is

an axiom), they are nevertheless constructed from finitely many schemata by substitution in this manner: 'If a, b, and c are formulas, then $(a \rightarrow b) \rightarrow ((b \rightarrow c) \rightarrow (a \rightarrow c))$ is an axiom', and the like.

Now if we could succeed in producing a class R of formulas such that

(α) Every axiom belongs to R,

(β) If a and $a \rightarrow b$ belong to R, then b also belongs to R,

(γ) '$1=2$' does not belong to R,

then we would have proved consistency, for according to (α) and (β) every proved formula obviously must belong to R, and according to (γ), $1=2$ must therefore be unprovable. The actual production of such a class at this time is unthinkable, however, for it poses difficulties comparable to those raised by the decision problem. But the following remark leads from this problem to a much simpler one: If our system were inconsistent, then there would exist a proof of $1=2$ in which only a finite number of axioms are used. Let the set of these axioms be called M. Then the axiom system M is already inconsistent. Hence the axiom system of classical mathematics is certainly consistent if every finite subsystem thereof is consistent. And this is surely the case if, for every finite set of axioms M, we can give a class of formulas R_M which has the following properties:

(α) Every axiom of M belongs to R_M.

(β) If a and $a \rightarrow b$ belong to R_M, then b also belongs to R_M.

(γ) $1=2$ does not belong to R_M.

This problem is not connected with the (much too difficult) decision problem, for R_M depends only on M and plainly says nothing about provability (with the help of all the axioms). It goes without saying that we must have an effective, finitary procedure for constructing R_M (for every effectively given finite set of axioms M) and that the proofs of (α), (β), and (γ) must also be finitary.

Although the consistency of classical mathematics has not yet been proved, such a proof has been found for a somewhat narrower mathematical system. This system is closely related to a system which Weyl proposed before the conception of the intuitionist system. It is substantially more extensive than the intuitionist system but narrower than classical mathematics (for bibliographical material, see Weyl 1927).

Thus Hilbert's system has passed the first test of strength: the validity of a non-finitary, not purely constructive mathematical system has been established through finitary constructive means. Whether someone will succeed in extending this validation to the more difficult and more important system of classical mathematics, only the future will tell.