HILBERT-BERNAYS ON PROOF-THEORY

Grundlagen der Mathematik, Volume I. By D. Hilbert and P. Bernays. (Grundlehren der Mathematischen Wissenschaften, Volume XL.) Berlin, Springer, 1934. xii+471 pp.

This is undoubtedly the most important book on the foundations of mathematics since Whitehead and Russell's *Principia Mathematica*, for it offers an authoritative formulation of the famous Hilbert *Proof-theory*. All the recent work in the foundations has been dominated by the discovery of contradictions in the body of mathematics, especially in Cantor's *Mengenlehre*. There have been many attempts to avoid this difficulty by using axiom systems so limited that the known contradictions could not arise. Hilbert, however, planned a direct attack on the difficulty: an attempt to prove that, in a suitably limited system, no *new* contradiction could ever arise. Bernays here discusses the cases in which Hilbert's plan has succeeded. In brief, the Hilbert school has developed a powerful and fascinating method for investigating mathematical proofs and has shown by these methods that a large part of elementary number theory is *consistent* (free from contradiction). However, the extension to more complicated branches of mathematics has met with serious obstacles.

How is it possible to show that a mathematical system is consistent? Only by means of a thoroughgoing formalization of the axioms and proofs of that system. In other words, the logical methods usually used uncritically in carrying out a mathematical proof must themselves be subjected to mathematical formulation. This is possible by means of the calculus of propositions, which was developed by Peano and by Russell and Whitehead. In this calculus, all the axioms of logic and mathematics can be precisely and symbolically expressed. Furthermore, the operations of logic are all reduced to a few simple, mechanical rules of procedure. A proof must thus start with one or more known axioms, and must proceed step by step, each step following some one of the mechanical rules. Any formal proof is thus finite and combinatorial in character, and hence the possibility that some proof might lead to a contradiction can be investigated by combinatorial methods. This is Hilbert's plan of attack.

But this finite analysis of formal proofs must itself be mathematical and so must itself involve proofs. These latter proofs belong to metamathematics—they are not the mathematics to be investigated; they are rather the tools of the investigation. For example, any general study of proofs will need some sort of complete induction on the number of steps in a proof. This process of induction, together with the other tools needed in the investigation, is essentially *finite* in character. Bernays has explained excellently exactly wherein this finiteness consists. Roughly speaking, finite arguments about numbers are those which can be grasped perceptually (that is, which are *anschaulich überblickbar*). In particular, the existence of a number with some property has a finite meaning only when there is a definite method whereby some such number can be constructed. In this respect, finite theorems are subject to the intuitionistic logic of Brouwer. This means that the tools of proof-theory are to be finite methods which are themselves clearly consistent.

Symbolic logic, the next prerequisite for proof-theory, is developed in §§3–5 in a masterly fashion. In the calculus of propositions the usual operators —"and," "or," "implies," "not," and "equivalent"—are introduced, both by means of axioms and by the superior method of truth-value tables. (For example, "not" is the operator which produces a false proposition from a true one.) For the calculus of propositional functions the author uses a symmetric system of axioms and rules concerning the two operators "for all x" and "there exists an x". The rules of procedure in this system include the usual rule of inference, which allows us to assert the conclusion of a true theorem "A implies B" once the hypothesis A has been established, and the rule of substitution, according to which variables may be replaced by constants or combinations of variables. An additional rule allows us to *rename* the *apparent* variable x in "for all x" or "there exists an x." A final section discusses a method of adjoining to this calculus the relation of equality.

The sixth section of the book introduces the first typical application of proof-theory to an infinite system: the demonstration that a certain axiom system for whole numbers is consistent. This system consists of the calculus of propositional functions, including equality, and the Peano axioms for whole numbers, excluding the principle of mathematical induction. The Peano axioms are slightly modified, in that the function $a'=a+1$ is used instead of the relation "b is the successor of a". If this system of axioms were inconsistent, then there would be a proof starting from these axioms and leading to a contradiction of the form $0\neq 0$. In the simplest case, this proof would involve no apparent variables. In such a proof, all free variables can be eliminated, for any application of the rule of substitution can be moved back in the proof until the substitution in question takes place right in the original axioms. All the formulas of the proof are then simple *numerical* formulas—equalities and inequalities between concrete numbers, together with combinations of such by the operations of the propositional calculus. Any such numerical formula is either "true" or "false" in a finite, constructive sense. Furthermore, the particular axioms from which the proof starts are all "true" in this sense, while all the rules of procedure give true results when applied to true premises. In particular, if two formulas "S" and "S implies T" are true, then the conclusion "T" of the inference is likewise true. Hence all the formulas derived in the course of the proof are true, so that a contradiction $0\neq 0$ at the end of the proof cannot occur.

This result must next be extended to proofs which do involve apparent variables. This is possible with the methods of Herbrand and Presburger. The formulas of such a proof are not all numerical formulas, but it is possible to associate with any one of the formulas several corresponding *reduced* numerical formulas. For example, (Ex) $(a<x \,\&\, x<b)$ would have the reduced form $0<b \,\&\, (a+1)<b$. Here, as in the other cases, the reduced formula is effectively equivalent to the original. Hence any formula is called *verifiable* if one of its reduced forms is true. As before, all the formulas of a proof are verifiable, so that no contradiction can arise.

Much of the rest of the book is concerned with extensions of this method of establishing consistency by means of "verifiable" formulas and methods of "reduction." In particular, these ideas are still applicable if the axiom of mathematical induction is added to the other Peano axioms. In other words, the combination of the Peano axioms for whole numbers, the axioms for equality, and the calculus of propositional functions gives a consistent system.

This, however, does not prove that all ordinary number theory is consistent, for the usual development of whole numbers uses not only these axioms, but also certain *recursive definitions* for functions such as $a+b$. Such recursive definitions, unlike the ordinary explicit definitions, can at times lead to contradictions in systems which would otherwise be consistent. Hence the next task is an investigation of the consistency of recursive definitions. The author here considers any system of verifiable axioms for number theory, together with mathematical induction, the axioms for equality, and the calculus of propositions for *free* variables only. The addition of recursive definitions to such a system will not give rise to any contradiction, as is shown by a modification of the previous methods. The exclusion of apparent variables is essential to this result, but even with this limitation much can be developed. This the author shows by developing the usual theorems for prime decomposition by means of such recursions.

The last major topic is the analysis of descriptive functions, of the type "the so-and-so" or "the smallest number with such and such a property". This study was begun by Whitehead and Russell. A considerable extension of their method enables Hilbert and Bernays to show that such descriptive functions can always be eliminated: a theorem which does not involve descriptive functions, but which has been proved by the use of descriptive functions, can also be proved without descriptive functions. This result has many applications, in particular to a study of recursive definitions.

This book also contains a wealth of other significant results: a system of positive logic (§3); the deduction theorem (§4); the contributions of Skolem, Löwenheim, Behmann, and others to the *Entscheidungsproblem* (§§4–5); the proofs of several additional rules of procedure (§4); the Ackermann-Péter "folded" recursions which cannot be reduced to primitive recursions (§7); a discussion of normal forms in the propositional calculus with equality (§5); a critique of axioms for equality (§7); and several interesting axiom-systems for parts of number-theory. Indeed, if this book has a fault, it is only in that Professor Bernays' encyclopedic knowledge has led him to include so much that the main theme becomes at times obscured. Nevertheless, the book is very carefully and clearly written. Many of the arguments are of necessity formal in character, but if at such points the reader will bear in mind the non-formal interpretation of the discussion, he will have little trouble. The author has succeeded unusually well in explaining an abstract subject without assuming any previous special knowledge on the part of the reader.

The chief open question is that of extending the results. This volume has established the consistency of a system of recursive number theory; but for more extensive systems, the chief result is the preliminary step of eliminating the descriptive functions. To include all of number theory in a consistency proof, fundamental changes in the method are necessary, as the authors recognize. In spite of the optimism which Hilbert expresses in his preface, the well known results of Gödel point to almost insurmountable difficulties in the program of proof-theory. The second volume of this work, with its discussion of these questions, will be awaited with great interest. It may be that still other points of view will be necessary to complete the foundations of mathematics so well begun by the Hilbert proof-theory.

SAUNDERS MACLANE

SZEGÖ ON JACOBI POLYNOMIALS

Asymptotische Entwicklungen der Jacobischen Polynome. By Gabriel Szegö. Schriften der Königsberger Gelehrten Gesellschaft. Jahr 10, Naturwissenschaftliche Klasse, Heft 3, 1933, pp. 35–111 (1–77).

One of the interesting features in the development of analysis in the twentieth century is the remarkable growth, in various directions, of the theory of orthogonal functions. Two brilliant achievements on the threshold of this century—Fejér's paper on Fourier series and Fredholm's papers on integral equations—have been acting as a powerful inspiring source of attraction, inviting analysts to delve deeper into the theory of orthogonal functions and their applications. First come, due to their simplicity, the trigonometric functions $\{\sin mx, \cos mx\}$ which serve as a yardstick for orthogonal functions in general. Next we may consider orthogonal polynomials, of which Jacobi polynomials are a special case.

Let us recall the general definition of orthogonal polynomials. A weight-function $p(x)$, non-negative in a given interval (a, b), finite or infinite, and such that all "moments" $\int_a^b p(x)x^r dx = \alpha_r$ exist, $(r=0, 1, 2, \cdots)$, with $\alpha_0 > 0$, gives rise to a unique system of orthogonal and normal polynomials $\phi_n(x) = a_n x^n + \cdots$, $(n=0, 1, \cdots; a_n > 0)$, so that

$$(1)\qquad \int_a^b p(x)\phi_m(x)\phi_n(x)dx = 0,\ (m \neq n),\quad = 1,\ (m = n),\quad (m, n = 0, 1, \cdots).$$

On the basis of (1), we obtain the following expansion of an "arbitrary" function:

$$(2)\qquad f(x) \sim \sum_{n=0}^{\infty} f_n\phi_n(x), \quad \text{with} \quad f_n = \int_a^b p(x)f(x)\phi_n(x)dx,$$

and this constitutes the most interesting and important application of the polynomials $\phi_n(x)$ in analysis, as well as in mathematical physics, mathematical statistics, etc.

The oldest and best known are Legendre polynomials, derived from (1) with (a, b) finite, say $(-1, 1)$, and $p(x) \equiv 1$. Their direct generalization are Jacobi polynomials $P_n^{(\alpha,\beta)}(x)$: $(a, b) = (-1, 1)$, $p(x) = (1-x)^\alpha(1+x)^\beta$, $\alpha, \beta > -1$. In case of an infinite interval, the most important are the polynomials of Laguerre: $(a, b) = (0, \infty)$, $p(x) = x^\alpha e^{-x}$, $\alpha > -1$, and those of Hermite: $(a, b) = (-\infty, \infty)$, $p(x) = e^{-x^2}$. These four kinds of orthogonal polynomials constitute what may be considered as one single family of "classical" polynomials, where Jacobi polynomials, from many points of view, represent the most typical member. In fact, by assigning to α, β certain finite or limiting values, we get Legendre polynomials $(\alpha = \beta = 0)$, trigonometric polynomials $(\alpha = \beta = -1/2)$,