STUDIES IN LOGIC
AND THE
FOUNDATIONS OF MATHEMATICS

L. E. J. BROUWER / E. W. BETH / A. HEYTING
EDITORS

Mathematical Interpretation of Formal Systems

TH. SKOLEM • G. HASENJAEGER
G. KREISEL • A. ROBINSON • HAO WANG
L. HENKIN • J. ŁOŚ

NORTH-HOLLAND PUBLISHING COMPANY
AMSTERDAM

MATHEMATICAL INTERPRETATION OF FORMAL SYSTEMS

This book contains the lectures, held at the symposion on "Mathematical interpretation of formal systems" which was organized by the "Wiskundig genootschap" (Mathematical society) at Amsterdam on September 9 and 10, 1954, with financial aid from U.N.E.S.C.O. Discussion remarks by G. Hasenjaeger were added.

A. Heyting

PRINTED IN THE NETHERLANDS
DRUKKERIJ HOLLAND N.V., AMSTERDAM

CONTENTS

TH. SKOLEM

PEANO'S AXIOMS AND MODELS OF ARITHMETIC

Introduction

More than 30 years ago I proved by use of a theorem of Löwenheim that a theory based on axioms formulated in the lower predicate calculus could always be satisfied in a denumerable infinite domain of objects. Later one has often expressed this by saying that a denumerable model exists for such a theory. Of particular interest was of course the application of this theorem to axiomatic set theory, showing that also for this an arithmetical model can be found. As I emphasized this leads to a relativisation of set theoretic notions. On the other hand, if one desires to develop arithmetic as a part of set theory, a definition of the natural number series is needed and can be set up as for example done by Zermelo. However, this definition cannot then be conceived as having an absolute meaning, because the notion set and particularly the notion subset in the case of infinite sets can only be asserted to exist in a relative sense. It was then to be expected that if we try to characterize the number series by axioms, for example by Peano's, using the reasoning with sets given axiomatically or what amounts to the same thing given by some formal system, we would not obtain a complete characterisation. By closer study I succeeded in showing that this really is so. This fact can be expressed by saying that besides the usual number series other models exist of the number theory given by Peano's axioms or any similar axiom system. In the sequel I will first give an account as short as possible of my old proof of this, my exposition now being a little different in some respects. After that I intend to show how models of a similar kind can be set up in a perfectly constructive way when we consider some very restricted arithmetical theories.

§ 1. Preliminary Remarks

We may set up a theory of natural numbers by adding to the predicate calculus of first order some constants namely the individual constant 1, the predicate = and some functions namely the successor function, denoted by an apostroph, and addition and multiplication. Further we may assume the non-logical axioms

$$x' \neq 1$$
$$(x'=y') \rightarrow (x=y)$$
$$(y \neq 1) \rightarrow (Ex)(y=x')$$
$$x+1 = x'$$
$$x+y' = (x+y)'$$
$$x \cdot 1 = x$$
$$xy' = xy + x$$
$$x = x$$
$$(x=y) \rightarrow (U(y) \rightarrow U(x))$$
$$U(1) \,\&\, (x)(U(x) \rightarrow U(x')) \rightarrow U(y).$$

Here U denotes an arbitrary propositional function. It is most natural and convenient to let the propositional functions be those which can be constructed from equations by use of the connectives &, $\vee$ and $-$ together with the quantifiers extended over individuals, i.e. numbers. The two last axioms containing U are meant as axiom-schemes so that every individual case is an axiom. This formal system of arithmetic contains Peano's axioms. Other systems could be used as well, for example the system Z_μ in Hilbert–Bernays [1], p. 293.

Every proposition is equivalent to one which is built by use of quantifiers on an elementary expression, namely built by use of &, $\vee$ and $-$ on equations with polynomial terms on both sides when we replace x' by $x+1$. However, we may omit the negation, because $x \neq y$ may be replaced by $(Ez)((x=y+z) \vee (y=x+z))$. Further any proposition constructed by use of & and $\vee$ from equations is equivalent to a single equation because of the equivalences

(1) $$(a=b) \vee (c=d) \leftrightarrow (ad+bc=ac+bd)$$

(2) $$(a=b) \,\&\, (c=d) \leftrightarrow (a^2+b^2+c^2+d^2=2ab+2cd)$$

Thus every proposition is equivalent to an expression beginning with a sequence of quantifiers followed by an equation between two polynomial terms.

As to the arithmetical functions many more are definable than the polynomials. Indeed let the proposition

(3) $$(x_1)\ldots(x_m)(Ey)A(x_1,\ldots,x_m,y)$$

be true. Here A is a propositional function which may be arbitrarily complicated. It may for example still contain quantifiers. The word true may mean either provable in the system or that the statement is assumed as a further axiom. Now it is well known that we can prove by use of the induction axioms that if

$$(Ey)A(y)$$

is true, then

$$(Ey)[A(y) \,\&\, (z)(\bar{A}(z) \vee (y \leqslant z))]$$

follows which means that every non void set of numbers contains a least element. Therefore from (3) follows

$$(x_1)\ldots(x_m)(Ey)(A(x_1,\ldots,x_m,y) \,\&\, (z)(\bar{A}(x_1,\ldots,x_m,z) \vee (y \leqslant z))).$$

Then one and only one y here exists corresponding to a given m-tuple $x_1,\ldots,x_m$. This y is therefore a function $f(x_1,\ldots,x_m)$. Using this function we may write (3) as a formula containing no other quantifiers than those which perhaps occur in $A(x_1,\ldots,x_m,y)$ namely as

$$A(a_1,\ldots,a_m,f(a_1,\ldots,a_m)).$$

Repeating this introduction of functions one finds (see my paper "Über die Nichtcharakterisierbarkeit der Zahlenreihe etc." [2], that every correct formula

$$(x_1)\ldots(x_m)(Ey_1)\ldots(Ey_n)(z_1)\ldots(z_p)(Eu_1)\ldots(Eu_q)\ldots$$
$$\ldots A(x_1,\ldots x_m,y_1,\ldots y_n,z_1,\ldots))$$

may be written with free variables only

$$A(a_1,\ldots,a_m, f_1(a_1,\ldots,a_m),\ldots,f_n(a_1,\ldots,a_m), b_1,\ldots,b_p, g_1(a_1,\ldots,a_m,b_1,\ldots,b_p),\ldots).$$

Since for example we have the correct formula

$$(x)(y)((x=y) \vee (Ez)((x=y+z) \vee (y=x+z)))$$

a function exists, usually written $|x-y|$, such that

$$(a=b) \vee (a=b+|a-b|) \vee (b=a+|a-b|)$$

is a correct formula.

Let F be the set of all arithmetical functions in this sense. It is easily seen that F is closed with regard to the operation called nesting or substitution. Let for example $z=f(x,y)$ and $y=g(u)$ be respectively equivalent to $A(x,y,z)$ and $B(y,u)$. Then it is evident that $z=f(x,g(u))$ is equivalent to $C(x,u,z)$, where $C(x,u,z)$ is the propositional function

$$(Ey)(A(x,y,z) \;\&\; B(y,u)).$$

It is clear after these preparations that every statement can be replaced by an equivalent equation between two elements of F containing only free variables.

It is evident that all true formulas may be listed as an enumerated set S. To each of them we may find an equivalent equation whose both sides are functions belonging to F. Therefore in order to prove the existence of a model N' different from N for the set S of statements it will suffice to prove the following theorem.

Let S be a set of equations whose both sides are elements of a denumerable set of functions closed with regard to nesting. Assuming the equations belonging to S all valid for the natural number series N we may define a greater series N^* such that by suitable extension of all notions concerning N to corresponding ones in N^* all equations in S are also valid for N^*. In order to establish this I need an arithmetical lemma which I shall prove first. It ought to be added that this procedure is sufficient for our purpose because it will turn out that the equivalences we used above will remain valid in N^*.

§ 2. An Arithmetical Lemma

We consider an enumerated sequence of arithmetical functions

$$(4) \qquad f_1(t),\ f_2(t),\ \ldots .$$

Let $N^{(1)}$, $N^{(2)}$, $N^{(3)}$ be resp. the subsets of N for which

$$f_1(t) < f_2(t),\ f_1(t) = f_2(t),\ f_1(t) > f_2(t).$$

One at least of $N^{(1)}$, $N^{(2)}$, $N^{(3)}$ is infinite. Let N_1 be that with the least upper index which is infinite. Then there are for each $t \in N_1$ at most 5 possible cases for $f_3(t)$ in relation to $f_1(t)$ and $f_2(t)$, namely if for example N_1 is $N^{(1)}$

$$f_3(t) < f_1(t),\ f_3(t) = f_1(t),\ f_1(t) < f_3(t) < f_2(t),$$
$$f_3(t) = f_2(t),\ f_3(t) > f_2(t).$$

If N_1 is $N^{(2)}$ so that $f_1(t) = f_2(t)$ for all $t \in N_1$ we have only 3 possible cases namely

$$f_3(t) < f_1(t),\ f_3(t) = f_1(t),\ f_3(t) > f_1(t).$$

Let $N_1^{(1)}$, $N_1^{(2)}$, $N_1^{(3)}$ and eventually $N_1^{(4)}$, $N_1^{(5)}$ denote the subsets of N_1 for which the mentioned relations take place. Then again one at least of $N_1^{(1)}$, $N_1^{(2)}$, .. is infinite. We let N_2 be the $N_1^{(r)}$ with least r which is infinite. This procedure is continued so that we get an infinite sequence of infinite subsets of N

$$N = N_0 \supset N_1 \supset N_2 \supset \ldots\ldots$$

For all $t \in N_{n-1}$ the same relations $<$ and $=$ will take place between $f_1(t), \ldots f_n(t)$.

Now let $g(n)$ be the least number in N_{n-1}. Then it is evident that if

$$f_a(g(n)) \lesseqgtr f_b(g(n)),$$

where $n = \max(a, b)$, then we have accordingly

$$f_a(g(t)) \lesseqgtr f_b(g(t))$$

for all $t \geqslant n$. Thus the following lemma is proved:

If (4) is an infinite sequence of arithmetical functions, an arithmetical function $g(t)$ exists such that for any pair i, j the same relation $<$, $=$ or $>$ takes place between $f_i(g(t))$ and $f_j(g((t))$ for all $t > \max(i, j)$. The function $g(t)$ is steadily non-decreasing. In our applications of this lemma we will assume that all polynomials, in particular all constants, occur in (4). Then one sees that the values of $g(t)$ cannot possess an upper bound, because the intersection of all N_r is the null set.

§ 3. The Proof of the Existence of N^*

Let F be an enumerated set of arithmetical functions of one or more variables containing besides the successor, addition and multiplication all functions occurring in the left and right terms of a set S of equations with only free variables supposed true for N, F further being supposed closed with regard to nesting. Let F_1 be the denumerable subset of F consisting of the functions $f_r(t)$ of one variable. Then relations $<$ and $=$ can be defined between the elements of F_1 in the following way. According to the lemma a function $g(t)$ exists such that for any two i and j one of the three relations

$$f_i(g(t)) < f_j(g(t)),\ f_i(g(t)) = f_j(g(t)),\ f_i(g(t)) > f_j(g(t))$$

holds for all $t > \max(i, j)$. I put respectively

$$f_i < f_j,\ f_i = f_j,\ f_i > f_j$$

in these three cases. It is easy to see that the relation $=$ thus defined is an equivalence relation and that the relation $<$ is asymmetric and transitive. The different equivalence classes of the elements of F_1 defined by $=$ shall then constitute the diverse elements of N^*.

In a very simple and natural way every function $f(x_1, \ldots, x_n)$ in F can be extended to mean a function in the domain N^*. Indeed, if every $X_r(t)$ for $r = 1, \ldots, n$ is $\in F_1$, then

$$Y = f(X_1(t), \ldots, X_n(t))$$

is $\in F_1$, because F_1 is closed with regard to nesting. Further one easily sees that if $X_{r,1}(t)$ and $X_{r,2}(t)$ for $r=1,..,n$ are the same elements of N^*, then

$$Y_1=f(X_{1,1}(t),\dots,X_{n,1}(t))$$

and

$$Y_2=f(X_{1,2}(t),\dots,X_{n,2}(t))$$

denote the same element of N^*. Thus f also defines a function in the domain N^*. Clearly all elements of N also belong to N^*. Indeed they are furnished by the f in F_1 which are constants.

Further, since the relation $=$ has been defined in N^*, all the equations constituting S have a meaning in N^*. It remains to see that they are all valid in N^*. Let us consider an equation in S. It has left- and right-hand terms with some free variables, say $a_1, a_2, \dots$ Replacing these by arbitrary elements

$$\alpha_1(t),\ \alpha_2(t),\ \dots$$

of N^* we get an equation in N^*. Since this is valid for every value of t in N, it is valid for every t' when t has been replaced by $g(t')$. A fortiori the equation takes place for all $t' >$ the maximum of the indices which the left- and right-hand sides of the equation possess in the sequence $f_1(t), f_2(t), \dots$. Thus, remembering the definition of $=$ in N^*, we see that the equation holds good for arbitrary elements in N^*.

Now I will prove that the equivalence (1) remains valid in N^*. The correctness of the implication

$$(\alpha=\beta) \vee (\gamma=\delta) \rightarrow (\alpha\delta+\beta\gamma=\alpha\gamma+\beta\delta)$$

for arbitrary elements $\alpha, \beta, \gamma, \delta$ of N^* is seen so easily that I may confine myself to the treatment of the inverse implication. Let $\alpha\delta+\beta\gamma=\alpha\gamma+\beta\delta$. This means that for all $t'>h$ say and $t=g(t')$

$$(5)\qquad \alpha(t)\delta(t)+\beta(t)\gamma(t)=\alpha(t)\gamma(t)+\beta(t)\delta(t).$$

The number h may be chosen as the maximum of the indices of the left- and right-hand sides of (5) in the sequence (4). According to (1) this implies that for every $t'>h$ and $t=g(t')$

$$(\alpha(t)=\beta(t) \vee (\gamma(t)=\delta(t)).$$

Now let h_1 be the maximum of the indices in (4) of the functions $\alpha(t)$, $\beta(t)$, $\gamma(t)$, $\delta(t)$. Then if t' is $> \max(h, h_1)$ either $\alpha(g(t')) = \beta(g(t'))$ and then we have $\alpha = \beta$ or $\gamma(g(t')) = \delta(g(t'))$ so that $\gamma = \delta$. Hence (1) remains valid in N^*. Similarly we can show that (2) remains valid.

Let us now assume that $|a-b| \in F$. Then if α, β are $\in N^*$, we have for all t $(\alpha(t) = \beta(t)) \vee (\alpha(t) = \beta(t) + |\alpha(t) - \beta(t)|) \vee (\beta(t) = \alpha(t) + |\alpha(t) - \beta(t)|)$. Putting $t = g(t')$, the last formula is valid for all t'. Let h be the maximum of the indices of the two sides of the three equations. For a value of $t' > h$ one of the equations is fulfilled. Then just this equation holds for all greater values of t'. Therefore we have either $\alpha = \beta$ or $\alpha = \beta + |\alpha - \beta|$ or $\beta = \alpha + |\alpha - \beta|$. A consequence of this is that the equivalence between $\alpha \neq \beta$ and $(Ex)((\alpha = \beta + x) \vee (\beta = \alpha + x))$ holds good in the theory of N^*.

Let $A(a, f(a), b, g(a, b))$ be a free variable formula equivalent to the true formula

$$(x)(Ey)(z)(Eu)A(x, y, z, u)$$

in the previously explained sense. Then as I have just shown

$$A(\alpha, f(\alpha), \beta, g(\alpha, \beta))$$

is true in N^* and hence also

$$(x')(Ey')(z')(Eu')A(x', y', z', u'),$$

where x', y', z', u' are variables extended over N^*. This means that also every formula containing quantifiers and true concerning N is also true for N^*. In particular we may remark that the induction scheme remains valid for N. Now let us start with the general formula

$$(x')(Ey')(z')(Eu')A(x', y', z', u')$$

and as previously explained find an equivalent free variable formula

$$A(\alpha, \bar{f}(\alpha), \beta, \bar{g}(\alpha, \beta)).$$

Then according to the determination of $\bar{f}(\alpha)$ we have $\bar{f}(\alpha) \leqslant f(\alpha)$. On the other hand the definition of f in N yields for every t that $f(\alpha(t)) \leqslant \bar{f}(\alpha(t))$, whence $f(\alpha) \leqslant \bar{f}(\alpha)$. Hence the formula

$$A(\alpha, f(\alpha), \beta, \bar{g}(\alpha, \beta));$$

but according to the determination of $\bar{g}$ the relation $\bar{g}(\alpha,\beta) \leqslant g(\alpha,\beta)$ takes place for arbitrary α and β in N^*. On the other hand we have for all t according to the determination of $g(a, b)$ in N that $g(\alpha(t), \beta(t)) \leqslant \bar{g}(\alpha(t), \beta(t))$ with the consequence $g(\alpha, \beta) \leqslant \bar{g}(\alpha, \beta)$. Thus the functions f and g retain after the transition from N to N^* their roles as least elements with the considered properties.

The transition from N to N^* may of course be repeated so that we get a model N^{**} and so on.

§ 4. Some more Special Results

I would like to add some remarks on the setting up of models of certain fragments of number theory, in particular fragments of recursive arithmetic. In these simple cases the definition of non-standard models can often be established in a perfectly constructive way.

Let us for example consider the following theory T. The statements of T shall be built by &, $\vee$ and $-$ from the propositional functions $x<y$ and $x=y$ assuming the classical propositional calculus and the axioms concerning $=$. The recursive definitions of addition and multiplication shall belong to T, the successor being here simply denoted by addition of 1. Further we shall have the recursive definition of $<$ namely

$$a<0 \text{ is always false}$$

$$(a<b+1) \leftrightarrow (a<b) \vee (a=b). \tag{6}$$

Also the substitution rule shall be valid, i.e. from a correct formula we always obtain a correct formula by substitution of a variable (variables) by a numerical term (numerical terms).

Finally we assume the induction scheme

$$\frac{\begin{array}{c} U(0, b, c..) \\ U(a, b, c,..) \rightarrow U(a+1, b, c,..) \end{array}}{U(a, b, c,..)}$$

It is well known that we can derive in T the ordinary laws of addition and multiplication, namely the associative, commutative and distributive laws, and the ordinary laws concerning the relation $<$, namely asymmetry, transitivity and the theorems

$$(7) \qquad (a<b) \vee (a=b) \vee (a>b)$$

$$(8) \qquad (a<b) \rightarrow (a+c<b+c)$$

$$(9) \qquad (c>0) \ \& \ (a<b) \rightarrow (ac<bc).$$

On the other hand many formulas expressible in T and valid for the natural numbers are probably not provable in T. Thus for example nobody has ever succeeded in proving on this basis the statement

$$(10) \qquad (a=0) \vee (b=0) \vee (a^2<2b^2) \vee (a^2>2b^2)$$

which means that $\sqrt{2}$ is irrational.

Now let N' denote the set of polynomials

$$f(t)=a_n t^n+\ldots+a_0, \text{ all } a_r \text{ integers,}$$

with all $a_r \geqslant 0$ and $a_n>0$ resp. $a_0 \geqslant 0$ when $n=0$. If $g(t)=b_m t^m+ +\ldots+b_0$, I write $f=g$ when and only when $n=m$ and, for all r, $a_r=b_r$. Further I write $f<g$, if $n<m$ or $n=m$ and $a_r<b_r$ for the greatest r for which a_r differs from b_r. This definition can also be expressed thus: We put $f<g$, $f=g$, $f>g$ according as $f(t)<g(t)$, $f(t)=g(t)$, $f(t)>g(t)$ for $t=f(1)+g(1)$. Then the same relation takes place also for all greater t. However, I will not enter upon the proof of this. We may also with the same effect say that $f<g$ or $f=g$ according as always $f(t)<g(t)$ for sufficiently great t or always $f(t)=g(t)$. It is clear that if addition and multiplication are defined for the polynomials in the usual way, $f(t)+1$ will be the successor of $f(t)$, i.e. (6) is satisfied for N'. Further the formulas of recursive definition of addition and multiplication remain valid in N'. Also (7), (8) and (9) are easily seen to remain valid. Finally I will prove that the induction scheme will remain valid in N'. Indeed, let the two formulas

$$U(0, \beta, \gamma, \ldots)$$

$$\overline{U}(\alpha, \beta, \gamma, \ldots) \vee U(\alpha+1, \beta, \gamma, \ldots)$$

be correct, the variables $\alpha, \beta, \gamma, \ldots$ ranging over N'. Then they are correct by restriction of the range of variation to N which is contained in N', the constants being some of the elements of N'. We may write this

$$U(0, b, c, \ldots)$$
$$\overline{U}(a, b, c, \ldots) \vee U(a+1, b, c \ldots),$$

where $a, b, c, \ldots$ have N as domain of variation. Then the induction scheme for N yields

$$U(a, b, c, \ldots).$$

Let us here replace $a, b, c, \ldots$ by variables $\alpha, \beta, \gamma, \ldots$ ranging over N'. Since $U(\alpha(t), \beta(t), \ldots)$ is obviously true for all t, it is true for values of t so great that the atomic relations $<$ or $=$ building up the expression U remain settled, and that means that

$$U(\alpha, \beta, \gamma, \ldots)$$

is true. Thus the induction scheme remains valid for N'. As a consequence of this every provable formula in T must also be provable in the theory T' with the variables ranging over N' instead of N and obtained by taking into account the definitions above connecting T' with T.

I will insert the following remark. If instead of only the polynomials with integral coefficients we take all those having integral values for integral values of the variable we get a domain N'_{Σ}, where not only addition and multiplication can be carried out with retention of the usual algebraic rules, but also the general summation Σ can always be performed. When $F(T)$ is a function in N'_{Σ}, then $\sum_{T=0}^{A} F(T)$ is a function $G(A)$ in N'_{Σ}. Or in other words a uniquely determined $G(T)$ exists such that $G(0) = F(0)$ and

$$G(T+1) = G(T) + F(T+1).$$

If for example $F(T) = 1$, then $G(T) = T$, and if $F(T) = T$, then $G(T) = 1/2 \cdot T(T+1)$. It is clear that when $T \in N'_{\Sigma}$ also $1/2T(T+1) \in N'_{\Sigma}$. Further, if $F(T) = 1/2T(T+1)$, $G(T) = 1/6T(T+1)(T+2)$ etc. I confine myself to this hint.

One must expect that N' will cease to be a model for a more extended arithmetical theory than T. Let us consider the theory T_1 which arises when a function δ defined by the equations

$$\delta 0 = 0, \quad \delta(a+1) = a$$

is added to T. Simultaneously of course the U in the induction scheme then shall be understood to denote any propositional function that can be built when the function δ is also taken into account. It is easy to see that N' is not a model for T_1. Indeed one proves in T_1 the theorem

$$(a=0) \vee (\delta(a)+1=a).$$

This means that every element except 0 has a predecessor, but this is obviously not true for N'. However, we get a model N'' of T_1 by omitting for $0 \leqq r < n$ the requirement $a_r \geqslant 0$ for the polynomials $f(t)$, retaining $a_n > 0$ and if $n=0$ also $a_0 \geqslant 0$.

Let T_2 be the theory obtained by adding to T_1 the recursive definition of the function $a \dot{-} b$, namely

$$a \dot{-} 0 = a, \quad a \dot{-} (b+1) = \delta(a \dot{-} b).$$

Then it is seen that N'' is still a model for T_2. Just as the function $a \dot{-} b$ in the case of N means $a-b$ when $a>b$ and 0 when $a \leqslant b$, this is also true in T_2' concerning N'' when the true propositions of T_2' are those that can be derived from the provable propositions of T_2 by use of the definitions connecting T_2' with T_2.

However, N'' again ceases to be a model if such a function as $[a/2]$ is added to T_2. I assert that a model N''' for the theory T_3 arising from T_2 by adding the function $[a/b]$, defined for $b>0$, can be chosen as the set of all polynomials where all a_r are rational (eventually fractional) numbers, a_n (the highest coefficient) > 0 and a_0 non-negative integer when $n=0$. Instead of setting up the recursive definition of $[\alpha/\beta]$ for N''' one can show that for arbitrary $f(t)$ and $g(t)$ there are uniquely determined polynomials $g(t)$ and $r(t)$ such that identically in t

$$f(t) = g(t)q(t) + r(t) \text{ and } 0 \leqslant r(t) < g(t).$$

Hence after the definition of $<$ and $=$ between the elements of