R E M A R K S

O N

F O R M A L I Z E D A R I T H M E T I C

A N D

S U B S Y S T E M S T H E R E O F

by

C. BRINK

An extended essay presented in partial fulfilment
of the requirements for the degree of

MASTER OF SCIENCE

at

Rhodes University

1974

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Prof. H.J. Schutte, for his unfailing interest and valuable comments on the preliminary drafts of this essay.

Also I wish to express my gratitude to Rhodes University and the Council for Scientific and Industrial Research for their financial assistance.

Finally, I am grateful to Sue Hoffmann for her care and patience in typing the manuscript.

§

CONTENTS

§

CHAPTER I

INTRODUCTION

In a famous paper of 1931, Gödel proved that any formalization of elementary Arithmetic is incomplete, in the sense that it contains statements which are neither provable nor disprovable. Some two years before this, Presburger proved that a mutilated system of Arithmetic, employing only addition but not multiplication, is complete. This essay is partly an exposition of a system such as Presburger's, and partly an attempt to gain insight into the source of the incompleteness of Arithmetic, by linking Presburger's result with Gödel's. Gödel himself states that:

"The true source of the incompleteness attaching to all formal systems of Mathematics is to be found ------- in the fact that the formation of ever higher types can be continued into the transfinite, whereas in every formal system at most denumerably many types occur."

([5], p.62)

Gödel intended to substantiate this statement in a sequel to his paper, but this never appeared. The "types" referred to in the above quotation is a reference to Russell's "Theory of Types".

This is not the approach adopted in this essay. Gödel's proof is taken as known, and the emphasis is on the completeness of certain subsystems of Arithmetic. No definite answer is reached to the question of what engenders the incompleteness of Arithmetic. However, a possible answer, resting on two conjectures, is proposed in the conclusion.

The essay proceeds as follows. All formal systems considered in this essay are presented as first-order theories, and

Chapter 2 offers an exposition of this notion. Most of the material of this chapter was taken from [10], and proofs of all statements left unproved in Chapter 2 can be found there. Since heavy emphasis is placed on semantic methods, it was considered necessary to devote a chapter to the notion of truth. Chapter 3 deals with this matter; the approach adopted is based on Tarski's "Theory of Truth". Chapter 4 is a detailed exposition of a subsystem of Arithmetic employing only addition, such as the system for which Presburger's results were obtained. The reduction procedure used to prove completeness is due to Presburger, but the exposition given of this procedure is a paraphrase of that given in [6], pp. 359 - 366, here suitably altered to fit the slightly different axiom system. In Chapter 5 the axiom system of Chapter 4 is enlarged to an axiom system such as the one for which Gödel's results were obtained. A hypothesis is advanced which is refuted in Chapter 6. In Chapter 7 another complete subsystem of Arithmetic is described, and it is in turn related to the system of Chapter 4. Chapter 8 concludes with a suggestion as to what the reason for the incompleteness of Arithmetic may be.

§

CHAPTER II

FIRST-ORDER THEORIES : EXPOSITION AND GENERAL RESULTS

§ 1. Formal Systems:

The subsystems of Arithmetic with which this essay is concerned will all be presented as a certain kind of formal system (specifically: as "First-order Theories"). Since, in the literature, it is not always clear what is meant by "formal system", "formalization" and the like, the following brief exposition is offered.

A "Formal System" (sometimes called a "calculus") is a system built up as follows. Certain symbols (marks, signs, objects) are indicated as being the only symbols belonging to the system. Certain "Rules of Formation" are stated, which build up strings of these signs in a specified way. These strings are called "well-formed-formulae" — "wff" for short. Of these well-formed-formulae some are selected as "axioms" ("initial formulae"), and certain "Rules of Inference" ("Transformation Rules") are stated which produce new wff's from the axioms. The symbols used to present the system do not mean anything or stand for anything or denote anything. Consequently the wff's do not offer any objective information.

A formal system may be given an interpretation, however, roughly as follows. Some of the symbols are interpreted as denoting certain (abstract or concrete) objects, some others as denoting operations on these objects, and some others as denoting logical operations on wff's. Thus a semantics is attached to the formal system, each wff now having a truth-value. Some wff's are selected as axioms (either by convention, or because they seem evidently true) and new wff's

produced by the rules of inference then yield results concerning the interpretation.

A formal system with an interpretation may loosely be called a "Deductive System", since the rules of inference in the formal system are usually made to correspond to some sort of fairly natural deduction rules. It is important to note that a formal system (without an interpretation) is purely syntactical — the semantics comes in with the interpretation. Thus while a formal system has only syntax, a deductive system has both syntax and semantics. The process of obtaining a deductive system from a formal system, as described above, may also be viewed in reverse. That is, given some kind of natural deductive system (e.g. elementary "naive" arithmetic) a formal system may be obtained from it by abstraction of the purely structural properties of the system. Thus the semantics is abandoned, but the syntax is retained. In this case the formal system may be called a "formalization" of the deductive system.

The development of the subsystems of Arithmetic in this essay does not strictly follow any one of the two approaches sketched above. Rather, it proceeds on two parallel lines: the structure of the formal system is (formally) stated, and its intended interpretation is indicated. Results within the system and results concerning the system may occur indisciminately, but the status of a result will always be clearly indicated.

The notion of "truth" will be treated in Chapter 3, but some preliminary remarks are necessary here. Wff's in a formal system do not have "meaning", since their symbols are interpreted, and consequently they have no truth-values. How the truth-value of a wff is determined when an interpretation is attached to the formal system, will be explained in Chapter 3. Given the interpretation, each wff now has a truth-value. If one or more wff's are transformed by some truth-functional operation(s) within the system into a new wff which has the

value "true" no matter what the truth-values of its constituent wff's may be this new wff is called a tautology.

§ 2. First-Order Theories:

The type of formal system used in this paper is normally called a "First-order theory". It is developed within the normal framework of the Predicate Calculus and the Propositional Calculus — some knowledge of both of these is assumed.

Any First-Order Theory K has the following symbols:

(i) Logical Symbols : Negation : $\sim$
Implication : $\Rightarrow$
Universal Quantifier : $\forall$

(ii) Auxilary Symbols : Brackets : [( )]
Comma : ,

(iii) Individual Constants : a_i ; $i \geq 1$.
A finite or denumerable, possibly empty set.

(iv) Individual Variables : x_i ; $i \geq 1$.
A denumerable set.

(v) Predicate Letters : A_j^n ; $n \geq 1$, $j \geq 1$.
("A_j^n" is the j'th predicate letter of "n" arguments.) A finite or denumerable non-empty set.

(vi) Function Letters : f_j^n ; $n \geq 1$, $j \geq 1$.
("f_j^n" is the j'th function letter of "n" arguments.) A finite or denumerable, possibly empty set.

Different theories may differ in which of the above symbols they possess. Normally meta-variables such as "x", "y" etc. are employed in meta-results — these are thought of as ranging over the individual variables. From the given logical symbols others ($\wedge$, $\vee$, $\exists$, etc.) may be defined by the usual definitions.

The function letters applied to individual variables and individual constants generate what are called terms : variables and constants are terms, and if $t_1 \cdots t_n$ are terms, then $f_i^n(t_1,\cdots,t_n)$ is a term. Nothing is a term if it cannot be generated in this way.

The predicate letters applied to the terms yield what are called atomic formulae : for any terms $t_1 \cdots t_n$, and any predicate letter A_i^n, $A_i^n(t_1 \cdots t_n)$ is an atomic formula. Nothing else is an atomic formula.

The well-formed formulae are defined as follows:

(i) Every atomic formula is a wff.

(ii) If A and B are wff's, and x is some individual variable, then $\sim A$, $A \Rightarrow B$ and $(\forall x)A$ are wff's.

(iii) An expression is a wff only if it can be shown to be a wff on the basis of (i) and (ii).

As has been done in (iii) above, any string of symbols may be referred to as an "expression" when it is convenient to do so.

The axioms of a first-order theory K divided into two groups: the logical axioms and the proper axioms.

Logical Axioms

LA1 $A \Rightarrow (B \Rightarrow A)$.

LA2 $[A \Rightarrow (B \Rightarrow C)] \Rightarrow [(A \Rightarrow B) \Rightarrow (A \Rightarrow C)]$.

LA3 $(\sim B \Rightarrow \sim A) \Rightarrow (A \Rightarrow B)$.

LA4 $(\forall x_i)A(x_i) \Rightarrow A(t)$, if $A(x_i)$ is a wff and t is a term free for x_i in $A(x_i)$.

LA5 $(\forall x_i)[A \Rightarrow B] \Rightarrow [A \Rightarrow (\forall x_i)B]$, if A is a wff containing no free occurrence of x_i .

Note: In $(\forall x)A$, "A" is called the scope of the quantifier. An occurrence of a variable x is said to be bound in a wff if and only if it is either the variable in the quantifier, or is the same variable as the one in the quantifier, and occurs within the scope of the quantifier. A variable which is not bound in a wff is free. If A is a wff, and t is a term, then t is said to be free for x_i in A iff no free occurrence of x_i in A lie within the scope of any quantifier containing some variable x_j occurring in t . A wff containing no free variables is called a closed wff.

Proper Axioms:

These vary from theory to theory, and can only be specified for a particular theory.

The rules of inference of any first-order-theory K are the following:

Modus Ponens: (M.P)

From the two wffs : A

$A \Rightarrow B$

the wff B may be inferred.

Generalization: (Gen.)

From the wff A , the wff $(\forall x)A$ may be inferred.

Some formal systems include as a third rule of inference a "Rule of Substitution", allowing any wff to be substituted for (e.g.) "A" and "B" in LA1. The view taken here, however, is that A and B are meta-variables ranging over wff's of a first-order theory, and that such a substitution rule is unnecessary.

Any wff of a first-order theory K which follows directly or indirectly from the axioms of K by means of the rules of inference, is called a theorem of K. The notation

$$\vdash_K A$$

is used to indicate that A is a theorem of K. Furthermore, the notation

$$\Gamma \vdash_K A$$

is used to indicate that the wff A follows from the axioms of K plus the assumptions Γ, where Γ is a set of wff's. (Obviously, if Γ is empty, the first notation is applicable).

A first-order theory K may or may not have some of the following properties:

Completeness: K is complete if and only if, given any closed wff A of K, either A or ~A is a theorem of K.

Consistency: K is consistent if and only if, given any wff A of K, not both A and ~A are theorems of K.

Decidability: K is decidable if and only if there is an effective procedure* for determining whether any given wff of K is a theorem of K or not.

Axiomatic: K is axiomatic if and only if there is an effective procedure for determining whether any given wff of K is an axiom of K or not.

Some general results concerning first-order theories are now stated — proofs of these results can be found in [10]. All these results hold for an arbitrary first-order theory K, hence they are meta-results. Such results will be referred to as propositions.

2.1 Proposition:

Every wff A of K which is an instance of a tautology is a theorem of K, and may be proved using only

---

* Also : "mechanical method" or "algorithm". An "effective" procedure is precisely statable as a finite set of instructions; reliable in the sense of always yielding an answer, and completable in a finite number of steps. Further information can be found in [15], pp. 223 - 232.

LA1 - LA3, and M.P.

([10], p. 59)

2.2 Proposition: (Deduction Theorem)

Assume that

$$\Gamma, A \vdash_K B ,$$

where, in the deduction, no application of Gen. to a wff which depends upon A has as its quantified variable a free variable of A. Then :

$$\Gamma \vdash A \Rightarrow B .$$

([10], p. 61)

Corollary:

If A is a closed wff, and $A \vdash_K B$, then $\vdash_K A \Rightarrow B$.

([10], p. 61)

2.3 Proposition:

If the term t is free for x in $A(x)$, then:

$$(\forall x)A(x) \vdash_K A(t) .$$

([10], p. 70)

2.4 Proposition:

If the term t is free for x in $A(x)$, then:

$$A(t) \vdash (\exists x)A(x) .$$

([10], p. 71)

2.5 Proposition: (Rule C)

In any proof in K, the following procedure may be followed:
If a wff of the form $(\exists x)A(x)$ has already been proved, $A(b)$ may be asserted in any proof after an occurrence of $(\exists x)A(x)$, provided that "b" is a constant which has not previously occurred in the proof, and also does not occur in the final line of the proof. ("C" for "choice").

([10], pp. 73 - 74)

An expression of the form $A \vee B$ is said to be a disjunction, having A and B as disjuncts. An expression of the form $A \wedge B$ is said to be a conjunction, having A and B as conjuncts. A wff containing no quantifiers is said to be in Disjunctive Normal Form (DNF) iff it is an unnegated disjunction consisting of one or more disjuncts, each of which is an unnegated conjunction of atomic wff's, negated or unnegated. Thus a wff in DNF contains only the three logical symbols "~", "$\vee$" and "$\wedge$".

2.6 Proposition:

There is an effective procedure for transforming any wff A of K containing no quantifiers into a wff B of K which is in DNF such that:

$$\vdash_K A \Leftrightarrow B .$$

([10], pp. 27 - 28)*

A wff A of K is said to be in Prenex Normal Form iff it is of the form:

$$(Q_1 x_1)(Q_2 x_2)\cdots(Q_n x_n)A ,$$

where each Q_i is a quantifier ("$\forall$"(universal) or "$\exists$"(existential)), $x_i \neq x_j$ for $i \neq j$, and A contains no quantifiers.

2.7 Proposition:

There is an effective procedure for transforming any wff A of K into a wff B of K which is in Prenex Normal Form, such that:

$$\vdash_K A \Leftrightarrow B .$$

([10], p. 87)

Now let K be any first-order theory which has A_1^2 as one of its predicate letters, where $A_1^2(t,s)$ is abbreviated

---

* See also [8], pp. 73 - 76.

as "$t = s$", and $\sim A_1^2(t,s)$ is abbreviated as "$t \neq s$". Then K is called a <u>first-order theory with equality</u> iff the following are theorems of K:

LA6* $(\forall x_1)[x_1 = x_1]$ (reflexivity of equality).

LA7 $x = y \Rightarrow [A(x,x) \Rightarrow A(x,y)]$ (substitutivity of equality), where x and y are individual variables, $A(x,x)$ is any wff containing x as a variable, and $A(x,y)$ arises from $A(x,x)$ by replacing some, but not necessarily all, free occurrences of x by y, with the proviso that y is free for those occurrences of x which it replaces.

2.8 <u>Proposition</u>:

Let K be a first-order theory in which LA6 holds, and LA7 holds for <u>atomic</u> wff's. Then K is a first-order theory with equality.

([10], p. 76)

§

---

* The numbering here is a continuation of the numbering of the logical axioms on page 6.

CHAPTER III

THE CONCEPT OF "TRUTH" IN FORMALIZED ELEMENTARY ARITHMETIC

§ 1. "Truth" in a First-Order Theory:*

As has been pointed out, wff's have meaning only when an interpretation is given for the symbols. An interpretation of a first-order theory K consists of a non-empty set D (the domain of the interpretation) and an assignment:

to each individual constant a_i of some fixed element of D — say d_i,

to each predicate letter A_j^n of an n-place relation in D — say B_j^n, and

to each function letter f_j^n of a function from D^n into D — i.e. an n-place operation on D — say g_j^n.

Individual variables are thought of as ranging over the elements of D.

Now let Σ be the set of all denumerable sequences $s = (\delta_1, \delta_2, \delta_3 \ldots)$ of elements of D. A function S determined by the sequence s, having the set of terms of K as domain and D as range is now defined:

(i) $S(a_i) = d_i$.

(ii) $S(x_i) = \delta_i$.

(iii) $S[f_i^n(t_1, \ldots, t_n)] = g_j^n[S(t_1), \ldots, S(t_n)]$.

Intuitively, for a sequence $s = (\delta_1, \delta_2 \ldots)$ and a term t of K, S(t) is that element of D obtained by substituting,

---

* The material of § 1. was taken from [2], pp. 55 - 56, and [10], pp. 50 - 53.

for each i, δ_i for all occurrences of x_i in t, and then performing the operations of the interpretation corresponding to the function letters of t. It is now recursively defined what it means for a sequence s to satisfy a wff A of K, written:

$$K \models_s A$$

3.1 Definition:

(i) $K \models_s A_j^n(t_1,\dots,t_n)$ if and only if $B_j^n(S(t_1),\dots,S(t_n))$ – i.e. s satisfies an atomic wff A_j^n iff the n-tuple $(S(t_1),\dots,S(t_n))$ is in the corresponding relation B_j^n.

(ii) $K \models_s \sim A$ iff not– $K \models_s A$.

(iii) $K \models_s (A \Rightarrow B)$ iff: either not– $K \models_s A$, or $K \models_s B$.

(iv) $K \models_s (\forall x_i)A$ iff for every sequence s' differing from s in at most the i'th component, $K \models_{s'} A$.

Note: "Not– $K \models_s A$" is to be read as: "s does not satisfy A in K".

This definition leads to a definition of truth and falsehood.

3.2 Definition:

A wff A is true for a given interpretation if and only if every sequence s in Σ satisfies A.

3.3 Definition:

A wff A is false for a given interpretation if and only if no sequence of Σ satisfies A.

From these definitions the following facts can easily be ascertained:

(a) Since the definition of the satisfaction relation has the same recursive base as the definition of a wff, truth and falsehood are defined for every wff of K.

(b) The truth or falsehood of a wff of K is relative to the interpretation assigned to K — i.e. the same wff may be true in one interpretation and false in another.

(c) Truth and falsehood are mutually exclusive properties — i.e. for a given interpretation, no wff can be both true and false.

(d) A closed wff is either true or false. A wff containing free variables, however, may be satisfied by some sequences in the domain of the interpretation and not satisfied by others. Such a wff is called a contingent wff.

(e) A wff A is true iff its closure is true — the closure of a wff A being the closed wff obtained by prefixing as universal quantifiers those variables which are free in A. If A has no free variables, the closure of A is A itself.

§ 2. A Problem in verifying Arithmetical Statements.

The method of defining truth given in § 1. is due to Tarski, and is a precise application of the imprecise:

Schema T: x is a true sentence if and only if p.
(p is any sentence, and x is a name of this sentence.)
([14], p. 155)

As a natural-language example, the following will suffice:

A: "Snow is white" is a true sentence if and only if snow is white.
([14], p. 156)

(The quotation marks, in this example, serve as a name-forming functor). In some sense then, Tarski's theory of truth may be

regarded as a "correspondence" theory of truth* — a statement is true iff it corresponds with the facts. Furthermore, in examples such as A, "the facts" may be empirically verified — snow is white because it can be seen that it is white.

Consider now a first-order theory K which is a formalization of elementary Arithmetic. That is, the Natural Numbers is the domain of the interpretation, operations such as addition and multiplication are assigned to function letters in K, and relations such as equality are assigned to predicate letters in K. Those constants in K corresponding to the natural numbers in the interpretation will from now on be called numerals, the numeral corresponding to the natural number "n" being written as "$\bar{n}$".

Now suppose that A_1^2 is the predicate letter corresponding to the equality relation "=". Then, by (i) of the definition of the satisfaction relation, an atomic wff of the form

$$A_1^2(t_1 t_2)$$

is satisfied by a sequence s if and only if

$$S(t_1) = S(t_2)$$

where S is the function mapping the terms onto their corresponding interpretation. Consequently, a wff of the form

$$\bar{3} + \bar{2} = \bar{5}$$

in K is satisfied by a sequence s if and only if

$$S(\bar{3} + \bar{2}) = S(\bar{5}).$$

Since the numerals correspond to the natural numbers, S maps each numeral onto its corresponding natural number — i.e.:

$$S(\bar{5}) \text{ is } \text{"5"}$$

---

* This is a generally accepted point of view. See, for example, the Encyclopedia of Philosophy, Vol 2, "Correspondence Theory of Truth." — especially pp. 230 - 231.

and from (iii) of the definition of S it follows that

$$S(\bar{3} + \bar{2}) \text{ is } "3 + 2" .$$

Hence s satisfies the wff

$$\bar{3} + \bar{2} = \bar{5}$$

in K if and only if

$$3 + 2 = 5 .$$

Since the function S determined by <u>any</u> sequence s maps the constant "a_i" in K onto its corresponding interpretation, it is clear that <u>any</u> sequence s will satisfy the wff "$\bar{3} + \bar{2} = \bar{5}$" iff $3 + 2 = 5$.
Consequently:

<u>B</u>: "$\bar{3} + \bar{2} = \bar{5}$" is true if and only if $3 + 2 = 5$.

It is clear that B is analogous to A. However, whereas in A it could be empirically verified that snow is indeed white, the situation is not altogether as clear in B. The Natural Numbers are not normally regarded as entities that lend themselves to empirical verification.

There is a problem in verifying arithmetical (and in general, mathematical) statements. Note that this problem does not find a solution in formally <u>proving</u> that 3 plus 2 equals 5, since provability is a syntactical concept belonging to a formal system, such as K. The problem is precisely to show that the provable statement "$\bar{3} + \bar{2} = \bar{5}$" describes an existing state of affairs. If this can be done, then, by definition the statement will be true.

There seems to be at least two possible courses of action. Firstly, it may be said that it is "intuitively" recognizable that it is indeed the case that the sum of three and two is five. Thus the verification is not empirical, but intuitive. This, however, seems to subject Mathematics to the realm of Psychology.

Another possibility is the following:
Frege and (independently) Russell defined the cardinal number of a set X to be the class of all those sets equivalent (in a precise way) to X. Loosely translated, this means that a natural number "n" can be regarded as an abstraction of all those sets with "n" elements. Or, taking the reverse view, any set with "n" elements can be regarded as an instance of the natural number "n". This leads to a method on the lines of Hilbert's formalism*. It is taken as axiomatic that whatever is the case concerning any natural number is also the case concerning an instance of it. As far as numerical properties go, the reverse is also true.
Now regard:

|	as	an	instance	of	the	Natural	Number						1
||	"	"	"	"	"	"	"	"	"	"	"	"	"	2
|||	"	"	"	"	"	"	"	"	"	"	"	"	"	3
|||		"	"	"	"	"	"	"	"	"	"	"	"	4

etc.

Also regard addition of natural numbers as concatenation of strings of marks.
Then

\|\|\| concatenated with \|\| is \|\|\|\|\|

is an empirical representation of the statement that

3 plus 2 equals 5

and this representation can indeed be empirically verified. This is taken as empirical verification of the statement "3 + 2 = 5", which, going back to B, yields the result that "$\bar{3} + \bar{2} = \bar{5}$" is true in K.

This method, however, is not without its drawbacks. Hilbert and Bernays state:

---

* Hilbert, however, in [6], used this method to define truth, not to verify (in the sense explained above) arithmetical statements.

"We shall always use the word "finitary" to indicate that the discussion, assertion or definition in question is kept within the bounds of thorough-going producibility of objects and thorough-going practicability of processes, and may accordingly be carried out within the domain of concrete inspection."

([6], p. 32)

It is clear, then, that the above method is essentially finitary. Thus it fails as a method for verifying statements concerning (e.g.) all natural numbers.

The above (second) course of action is adopted in this essay. Note that it also allows verification of statements such as

$$4 < 5$$

and

$$7 \equiv 2 \pmod 5 ,$$

as leading to the conclusion that

$$\bar{4} < \bar{5}$$

and

$$\bar{7} \equiv \bar{2} \pmod{\bar{5}}$$

are true wff's of a first-order theory K. This fact will be used in the sequel.

Note that Tarski's Theory of Truth does yield necessary and sufficient conditions for an (arithmetical) statement to be true — what it does not yield is a method of verification.

§ 3. Explicit and Recursive Definitions.*

(This paragraph fits more naturally into Chapter 2, but the notions of "numeral" and "natural number" were prerequisites. Hence its inclusion here.)

Given a first-order theory K, once the existence of a unique object "u" having the property $A(y_1,\cdots,y_n,u)$ has been

---

* The material of § 3. was taken from [10], pp. 82, 118 and 120.

proved, it is often convenient to introduce a new function $f(y_1 \cdots y_n)$ such that $A[y_1,\cdots,y_n, f(y_1,\cdots,y_n)]$ holds for all $y_1,\cdots,y_n$. Since the first-order theories treated in this essay all find their interpretations in the set of natural numbers, function letters in these theories will correspond to operations (functions) on natural numbers. A function having natural numbers as arguments and values will be called a number-theoretic function. Such functions, being defined on the natural numbers, are not attached to any particular first-order theory.

3.1 Definition

A number-theoretic function $f(x_1 \cdots x_n)$ is said to be representable in a first-order theory K with equality if and only if there is a wff $A(x_1,\cdots,x_{n+1})$ of K, having $n+1$ as free variables, such that for any natural numbers $k_1 \cdots k_{n+1}$:

(i) If $f(k_1 \cdots k_n) = k_{n+1}$, then $\vdash_K A(\bar{k}_1,\cdots,\bar{k}_n,\bar{k}_{n+1})$.

(ii) $\vdash_K (\exists!\, x_{n+1})\, A(\bar{k}_1,\cdots,\bar{k}_n, x_{n+1})$.

If in this definition, (ii) is changed to:

(ii') $\vdash_K (\exists!\, x_{n+1})\, A(x_1,\cdots,x_n, x_{n+1})$

then f is said to be strongly representable in K.

If f is strongly representable in K, then f can be introduced as a new function letter into K by explicit definition:

$$f(x \cdots x_n) \overset{\text{def}}{=} x_{n+1} ,$$

where x_{n+1} is the unique object whose existence is shown by (ii'). Given a definition similar to 3.1 in the case of relations, new predicate letters may also be introduced by explicit definition. It is generally acknowledged that such

definitions, although convenient, add nothing really new to a first-order theory.

Another method of obtaining new functions from old ones, is <u>definition by recursion</u>, or <u>inductive definition</u>.
Given two functions

$$g(y_1 \cdots y_n)$$

and $$h(y_1 \cdots y_n, y_{n+1}, y_{n+2})$$

a new function $f(y_1 \cdots y_{n+1})$ may be introduced as follows:

$$f(y_1, \cdots, y_n, 0) = g(y_1 \cdots y_n)$$

$$f(y_1 \cdots y_n, x+1) = h(y_1 \cdots y_n, x, f(y_1 \cdots y_n, x)) .$$

Here "n" may equal 0, in which case the definition is:

$$f(0) = k \quad \text{(for } k \text{ a fixed natural number)}$$
$$f(x+1) = h(x, f(x)).$$

The question arises as to what the relation is between these two types of definition. In [3], p. 129, a method is described for reducing recursive to explicit definitions. This method relies on two mappings: one between the natural numbers and ordered pairs of natural numbers, and the other between the natural numbers and ordered triples of natural numbers. For these mappings, two functions are essential: addition and multiplication. This fact will be useful in the sequel.

§

CHAPTER IV

A SUBSYSTEM OF ARITHMETIC EMPLOYING ONLY ADDITION

§ 1. The First-Order Theory S_1 *

The symbols of S_1 are the following:

(i) Logical Symbols : $\sim$ $\Rightarrow$ $\forall$.

(ii) Auxilary Symbols : Brackets : [( )]
Comma : , .

(iii) Individual Variables : x_1 x_2 x_3 .... .

(iv) Predicate Letter : A_1^2
$A_1^2(x_1,x_2)$ will be abbreviated as $x_1 = x_2$.

(v) Function Letters : f_1^1 , f_1^2
$f_1^1(x)$ will be abbreviated as x
$f_1^2(x,y)$ will be abbreviated as $x + y$.

(vi) Individual constant : 0 .

Terms

(i) Individual variables are terms. 0 is a term.

(ii) If t and s are terms, then: t' is a term
$t + s$ is a term.

(iii) An expression is a term only if it can be shown to be a term on the basis of (i) and (ii).

---

* S_1 is a subsystem of a first-order theory appearing in [10], Chapter 3. Proofs of theorems of S_1 occurring in [10] will not be repeated here.

Atomic Formulae

If t and s are terms, $t = s$ is an atomic formula. Nothing else is an atomic formula.

Wff's

(i) Every atomic formula is a wff.

(ii) If A and B are wff's, then $\sim A$, $A \Rightarrow B$ and $(\forall x)A$ are wff's.

(iii) An expression is a wff only if it can be shown to be a wff on the basis of (i) and (ii).

The following further propositional connectives are defined:

$$A \vee B \overset{\text{def}}{=} (\sim A) \Rightarrow B \ .$$

$$A \wedge B \overset{\text{def}}{=} \sim(\sim A \vee \sim B) \ .$$

$$A \Leftrightarrow B \overset{\text{def}}{=} (A \Rightarrow B) \wedge (B \Rightarrow A) \ .$$

$$(\exists x)A \overset{\text{def}}{\Leftrightarrow} \sim(\forall x)\sim A \ .$$

Proper Axioms:

S_1^1 $\quad x_1 = x_2 \Rightarrow (x_1 = x_3 \Rightarrow x_2 = x_3)$

S_1^2 $\quad (x_1 = x_2) \Leftrightarrow (x_1' = x_2')$

S_1^3 $\quad 0 \neq x_1'$

S_1^4 $\quad x_1 + 0 = x_1$

S_1^5 $\quad x_1 + x_2' = (x_1 + x_2)'$

S_1^6 $\quad$ For any wff A of S_1 :

$$A(0) \Rightarrow [(\forall x)[A(x) \Rightarrow A(x')] \Rightarrow (\forall x)A(x)] \ .$$

An additional rule of inference follows from S_1^6 by M.P. , viz:

Induction Rule:

$(\forall x)A(x)$ follows from $A(0)$ and $(\forall x)[A(x) \Rightarrow A(x')]$.

The intended interpretation of S_1 is the Natural Numbers (with 0), hence S_1 is a formalization of a mutilated system of Arithmetic, employing only addition. To make this clear, the terms

$$0 \quad 0' \quad 0'' \quad 0''' \quad \ldots\ldots \text{ etc.}$$

will henceforward be denoted by the symbols

$$0 \quad \overline{1} \quad \overline{2} \quad \overline{3} \quad \ldots\ldots \text{ etc.}$$

These symbols are called numerals, and they constitute a shorthand method of writing the application of the stroke — operation f_1^1 a certain number of times to the individual constant 0. Similarly a shorthand way of writing the application of f_1^2 a certain number of times to some term (say t) is introduced.

Thus:

$t + t$	will be written as	$t \cdot \overline{2}$
$(t + t) + t$	" " " " " " "	$t \cdot \overline{3}$
$((t + t) + t) + t$	" " " " " " "	$t \cdot \overline{4}$
		.
		.
		.
		etc.

Convention 1

Any term t may be written as $t \cdot \overline{1}$ whenever required.

The notation employed above does not, strictly speaking, form a part of S_1 — it is, however, of considerable use in discussing results that do occur in S_1. Consequently, abbreviating (e.g.) $t + t$ as $t \cdot \overline{2}$ does not constitute the introduction of multiplication into S_1.

For example, although

$$0 \cdot \bar{n} = \underbrace{(\ldots(0 + 0) + \ldots + 0)}_{n \text{ times}} = 0$$

is permissable under the above method,

$$\bar{n} \cdot 0 = \underbrace{(\ldots(\bar{n} + \bar{n}) + \ldots + \bar{n})}_{0 \text{ times}}$$

is not. Neither is it permissable to write

$$t \cdot s$$

since t and s may be any terms — i.e. s is not necessarily a numeral. It will be established in § 2. of this chapter that the multiplication function is in fact not representable in S_1 at all.

As a rule, theorems within S_1 will be derived with terms and not individual variables as arguments. This is not strictly correct, since theorems within S_1 should not contain such extra-systematical terminology. However, by Gen. any theorem of S_1 can be transformed into a closed wff, and by Proposition 3.3 $A(t)$ is a direct consequence of $(\forall x)A(x)$, where t is an arbitrary term. On the other hand, any theorem with only terms as arguments can be transformed by Proposition 3.4 into a closed wff with only individual variables as arguments.

By Gen. and Proposition 2.3, the following theorems follow trivially from the axioms:

4.1 $\vdash_{S_1} (t = r) \Rightarrow (t = s \Rightarrow r = s)$.

4.2 $\vdash_{S_1} (t = r) \Leftrightarrow (t' = r')$.

4.3 $\vdash_{S_1} 0 \neq t'$.

4.4 $\vdash_{S_1} t + 0 = t$.

4.5 $\vdash_{S_1} (t + r') = (t + r)'$.

Since this chapter deals only with the first-order theory S_1, the symbol "S_1" will henceforward be omitted from "$\vdash_{S_1}$". Also, the proofs of those theorems of S_1 which are easily established will, as a rule, just be outlined in what follows. Meta-results, however, will always be proved in full detail.

The following theorems are easy consequences of the axioms:*

4.6 $\vdash t = t$.

4.7 $\vdash t = r \Rightarrow r = t$.

4.8 $\vdash t = r \Rightarrow (r = s \Rightarrow t = s)$.

4.9 $\vdash r = t \Rightarrow (s = t \Rightarrow r = s)$.

4.10 $\vdash t = r \Rightarrow t + s = r + s$.

4.11 $\vdash t = 0 + t$.

4.12 $\vdash (t' + r) = (t + r)'$.

4.13 $\vdash t + r = r + t$.

4.14 $\vdash t = r \Rightarrow s + t = s + r$.

4.15 $\vdash (t + r) + s = t + (r + s)$.

Amongst other things, these theorems establish that the two-place predicate A_1^2 (i.e. the equality-symbol) is reflexive, symmetric and transitive, and that addition is commutative and associative.

5.16 Proposition

S_1 is a first-order theory with equality.

---

* Proofs can be found in [10], pp. 104 - 107.

Proof:

S_1 is a first-order theory by construction. Now apply Proposition 2.8.

(a) From 4.6 by Gen : $\vdash (\forall x_1)[x_1 = x_1]$.

(b) Since the only atomic wff's in S_1 are of the form $t = s$, condition LA7 of equality reads:

(i) $\vdash x = y \Rightarrow [x = x \Rightarrow y = x]$

or (ii) $\vdash x = y \Rightarrow [x = x \Rightarrow x = y]$

or (iii) $\vdash x = y \Rightarrow [x = x \Rightarrow y = y]$.

(i) follows from 4.1 .
(ii) follows from 4.1 and 4.7 .
(iii) follows from (i), (ii) and 4.8 .

——→

The next proposition establishes some properties of numerals, which will frequently be needed in proofs of theorems to come.

4.17 Proposition *

For any natural numbers m and n, and any terms t and r of S_1 :

(a) If $m \neq n$, then $\vdash \bar{m} \neq \bar{n}$.

(b) $\vdash \overline{m + n} = \bar{m} + \bar{n}$.

(c) $\vdash t \cdot \bar{m} + t \cdot \bar{n} = t \cdot (\bar{m} + \bar{n})$, where $\bar{m}, \bar{n} \neq 0$.

(d) $\vdash t \cdot \bar{n} + r \cdot \bar{n} = (t + r) \cdot \bar{n}$, where $n \neq 0$.

(e) $\vdash t = r \Leftrightarrow t \cdot \bar{n} = r \cdot \bar{n}$.

Proof:

(a) Assume $m \neq n$ — say $m < n$.

---

* The proofs of (a) and (b) do occur in [10] — see p. 110.

Now suppose $\bar{m} = \bar{n}$ — i.e. $0^{\overbrace{''\ldots'}^{m \text{ times}}} = 0^{\overbrace{''\ldots'}^{n \text{ times}}}$.

4.2 , in the form $t' = r' \Rightarrow t = r$, applied m times in a row then yields:

$$0 = 0^{\overbrace{''\ldots'}^{(n-m) \text{ times}}} \quad . \qquad (1)$$

Since $n > m$, $n - m > 0$

$\therefore\ n - m - 1 \geq 0$.

Now let t be $0^{\overbrace{''\ldots'}^{(n-m-1) \text{ times}}}$ — i.e. t is the numeral $\overline{n - m - 1}$.

Then, from (1) : $0 = t'$, contradicting 4.3 .

The tautology : $[A \Rightarrow (B \wedge \sim B)] \Rightarrow \sim A$ then yields the result : $\bar{m} \neq \bar{n}$.

Since any instance of a tautology is a theorem, it follows that

$$\vdash \bar{m} \neq \bar{n} \ .$$

(b) Proof by induction on "n" in the metalanguage.

$\overline{m + 0} = \bar{m} = \bar{m} + 0$, by 4.4 .

Hence $\vdash \overline{m + 0} = \bar{m} + 0$.

Now assume : $\vdash \overline{m + n} = \bar{m} + \bar{n}$.

$$\therefore \vdash 0^{\overbrace{''\ldots'}^{(m+n) \text{ times}}} = 0^{\overbrace{''\ldots'}^{m \text{ times}}} + 0^{\overbrace{''\ldots'}^{n \text{ times}}}$$

$$\therefore \vdash \left(0^{\overbrace{''\ldots'}^{(m+n) \text{ times}}}\right)' = \left(0^{\overbrace{''\ldots'}^{m \text{ times}}} + 0^{\overbrace{''\ldots'}^{n \text{ times}}}\right)' \text{ by 4.2}$$

$$\therefore \vdash 0^{\overbrace{''\ldots'}^{((m+n)+1) \text{ times}}} = 0^{\overbrace{''\ldots'}^{m \text{ times}}} + \left(0^{\overbrace{''\ldots'}^{n \text{ times}}}\right)' \text{ by 4.5}$$

$$\therefore \vdash \overbrace{0''\ldots'}^{(m+(n+1))\text{ times}} = \overbrace{0''\ldots'}^{m\text{ times}} + \overbrace{0''\ldots'}^{(n+1)\text{ times}}$$

$$\therefore \vdash \overline{m + (n+1)} = \bar{m} + \overline{n+1} \quad .$$

So, by induction, the result holds for all n.

(c) By induction in the metalanguage on "n".

$$\begin{aligned} t\cdot\bar{m} + t\cdot\bar{1} &= t\cdot\bar{m} + t && \text{by Convention 1} \\ &= (\underbrace{\ldots(t+t) + \ldots + t}_{m\text{ times}}) + t \\ &= (\underbrace{\ldots(t+t) + \ldots + t}_{(m+1)\text{ times}}) \\ &= t\cdot\overline{(m+1)} \\ &= t\cdot(\bar{m} + \bar{1}) && \text{by part (b)} . \end{aligned}$$

Hence $\vdash t\cdot\bar{m} + t\cdot\bar{1} = t\cdot(\bar{m}+\bar{1})$. (1)

Now suppose $\vdash t\cdot\bar{m} + t\cdot\bar{n} = t\cdot(\bar{m}+\bar{n})$

$\therefore \vdash t\cdot\bar{m} + t\cdot\bar{n} + t\cdot\bar{1} = t\cdot(\bar{m}+\bar{n}) + t\cdot\bar{1}$ by 4.10

$\therefore \vdash t\cdot\bar{m} + t\cdot(\bar{n} + \bar{1}) = t\cdot[(\bar{m}+\bar{n}) + \bar{1}]$ by (1)

$\therefore \vdash t\cdot\bar{m} + t\cdot\overline{(n + 1)} = t\cdot[\bar{m} + (\bar{n}+\bar{1})]$ by 4.15

$\therefore \vdash t\cdot\bar{m} + t\cdot\overline{(n + 1)} = t\cdot(\bar{m} + \overline{n+1})$ by part (b).

Hence, by induction, the result holds for all n.

(d) $$t\cdot\bar{n} + r\cdot\bar{n} = \underbrace{t + t + \ldots + t}_{n\text{ times}} + \underbrace{r + r + \ldots + r}_{n\text{ times}}$$

An induction proof is easily established by using 4.13, 4.15 and part (c).

(e) Suppose $t = r$. We now prove by induction in the metalanguage on "n" that $t \cdot \bar{n} = r \cdot \bar{n}$.

By convention 1 : $t \cdot \bar{1} = r \cdot \bar{1}$.

Now assume $t \cdot \bar{n} = r \cdot \bar{n}$

$\therefore$ $t \cdot \bar{n} + t = r \cdot \bar{n} + t$ by 4.10

But since $t = r$: $r \cdot \bar{n} + t = r \cdot \bar{n} + r$, by 4.14

$\therefore$ $t \cdot \bar{n} + t = r \cdot \bar{n} + r$ by 4.8

$\therefore$ $t \cdot \bar{n} + t \cdot \bar{1} = r \cdot \bar{n} + r \cdot \bar{1}$ by convention 1

$\therefore$ $t \cdot \overline{n+1} = r \cdot \overline{n+1}$ by (c) and (b).

So, by induction, we have proved:

$$t = r \vdash t \cdot \bar{n} = r \cdot \bar{n} .$$

Then, by 2.2: $\vdash t = r \Rightarrow t \cdot \bar{n} = r \cdot \bar{n}$. (1)

Now let : $t \cdot \bar{n} = r \cdot \bar{n}$, and suppose that $t \neq r$.

Then, by 4.30, $t < r \vee r < t$ — say $t < r$.

By 4.19 : for some $w \neq 0$, $t + w = r$.

Hence : $t \cdot \bar{n} = (t+w) \cdot \bar{n}$

$= t \cdot \bar{n} + w \cdot \bar{n}$ by (c),

so that : $0 + t \cdot \bar{n} = w \cdot \bar{n} + t \cdot \bar{n}$.

But then : $0 = w \cdot \bar{n}$ by 4.21, contradicting the fact that $w \neq 0$.

Then, from the tautology $[A \Rightarrow (B \wedge \sim B)] \Rightarrow \sim A$ it follows that $t = r$.

Hence $t \cdot \bar{n} = r \cdot \bar{n} \vdash t = r$.

Then, by 2.2 : $\vdash t \cdot \bar{n} = r \cdot n \Rightarrow t = r$. (2)

Note : Theorems 4.21 and 4.30 do not depend on 4.17 (e).

The result follows from (1) and (2) by definition of "$\Leftrightarrow$".

——→

4.18 Definition Congruence Relation.

$$t \equiv s \pmod{\bar{k}} \overset{\text{def}}{\Leftrightarrow} (\exists w)[t = s + w \cdot \bar{k} \vee s = t + w \cdot \bar{k}] .$$

4.19 Definition Order Relation.

$$t < s \overset{\text{def}}{\Leftrightarrow} (\exists w)[w \neq 0 \wedge t + w = s] .$$

Definition 4.18 stands in need of clarification. Strictly speaking, it does not form part of the system S_1 as a normal explicit definition (such as 4.19), because of the shorthand notation appearing in it. Considered as a relation between numerals, however, it finds justification in the fact that given any two numerals $\bar{m}$ and $\bar{n}$, it can effectively be decided whether $\bar{m}$ and $\bar{n}$ are in fact congruent mod $\bar{k}$ or not. This fact will prove very useful in establishing the completeness of S_1. For the moment, 4.18 is treated as an explicit definition within S_1, with the understanding that a further explanation will be forthcoming (see p. 62). Since the expression "$w \cdot 0$" is meaningless in S_1, 4.18 does not hold as a definition when $\bar{k} = 0$. Thus the following convention is adopted.

Convention 2

The congruence relation

$$t \equiv s \pmod{\bar{k}}$$

is not defined when $\bar{k} = 0$.

4.20 $\vdash t \neq 0 \Rightarrow (\exists x)[t = x'] .$

Proof: By induction on y in A(y) :

$$y \neq 0 \Rightarrow (\exists x)[y = x'] .$$

(i)	1.	$0 \neq 0$	Hyp.
	2.	$0 = 0$	4.6
	3.	$0 \neq 0 \wedge 0 = 0$	1,2. Taut.
	4.	$(0 \neq 0 \wedge 0 = 0) \Rightarrow (\exists x)[0 = x']$	Taut.
	5.	$(\exists x)[0 = x']$	3,4 M.P.
	6.	$0 \neq 0 \Rightarrow (\exists x)[0 = x']$	1-5, 2.2

Hence $\vdash A(0)$. ⟶

(ii)	1.	$y \neq 0 \Rightarrow (\exists x)[y = x']$	Hyp.
	2.	$y = 0 \vee y \neq 0$	Taut.
	3.	$y = 0$	Hyp.
	4.	$y' = 0'$	3, [illegible]
	5.	$(\exists x)[y' = x']$	4, 2.[illegible]
	6.	$y = 0 \Rightarrow (\exists x)[y' = x']$	3-5, 2.2
	7.	$y \neq 0$	Hyp.
	8.	$(\exists x)[y = x']$	1,7 M.P.
	9.	$y = \bar{k}'$	8, Rule C.
	10.	$y' = \bar{k}''$	9, 4.2
	11.	$(\exists x)[y' = x']$	10, 2.4
	12.	$y \neq 0 \Rightarrow (\exists x)[y' = x']$	7-11 2.2
	13.	$(y = 0 \vee y \neq 0) \Rightarrow (\exists x)[y' =$	6,12, Taut.
	14.	$(\exists x)[y' = x']$	2,13 M.P.
	15.	$y' = 0 \vee (\exists x)[y' = x']$	14 [illegible]
	16.	$y' \neq 0 \Rightarrow (\exists x)[y' = x']$	15
	17.	$[y \neq 0 \Rightarrow (\exists x)[y = x']] \Rightarrow [y' \neq 0 \Rightarrow (\exists x)[y = x'$	1-16 [illegible]

Hence $\vdash A(y) \Rightarrow A(y')$,
then by Gen. : $\vdash (\forall y)[A(y) \Rightarrow A(y')]$

So, by (i), (ii) and the Induction Rule :

$$\vdash (\forall y)[y \neq 0 \Rightarrow (\exists x)[y = x']]$$

and so, by 2.3 :

$$\vdash t \neq 0 \Rightarrow (\exists x)[t = x'] .$$

⟶

4.21 $\vdash (t + s = r + s) \Rightarrow t = r$.

Proof: By induction on z in

$A(z) : (x + z = y + z) \Rightarrow x = y$.

4.22 $\vdash t + \bar{1} = t'$.

Proof: From 4.4 and 4.5 , by using 4.2 and 4.8 .

4.23 $\vdash t \not< t$.

Proof:

1.	$t + x = t$	Hyp.
2.	$x + t = t + x$	4.7
3.	$x + t = t$	2,1, 4.8
4	$t = 0 + t$	4.11
5.	$x + t = 0 + t$	3,4, 4.8
6.	$(x + t = 0 + t) \Rightarrow x = 0$	4.21
7.	$x = 0$	5,6 M.P.
8.	$t + x = t \Rightarrow x = 0$	1-7 C.P.
9.	$t + x \neq t \vee x = 0$	8 Def.
10.	$x = 0 \vee t + x \neq t$	9 T. C.
11.	$\sim[x \neq 0 \wedge t + x = t]$	10 Taut.
12.	$(\forall x) \sim [x \neq 0 \wedge t + x = t]$	11, en
13.	$\sim(\exists x)[x \neq 0 \wedge t + x = t]$	12. Def.
14.	$t \not< t$	13 = 4.9

4.24 $\vdash t < t'$.

Proof: From 4.22 and 4.3 by 2.4 .

4.25 $\vdash t < s \Rightarrow (s < r \Rightarrow t < r)$.

Proof: Conditional Proof, using 4.10, 4.8 and 4.15 with 2.4 .

Note:

A proof is called conditional if it proceeds from certain hypotheses to a certain conclusion, and then employs 2.2. For example, part (ii) in 4.20 is a conditional proof.

4.26 $\vdash t \equiv t \pmod{\bar{k}}$.

Proof: Indirect proof, using the fact that
$t = t + 0 = t + 0 \cdot \bar{k}$. ⟶

Note:

An indirect proof is a conditional proof in which the negation of the conclusion is assumed, a contradiction derived, and the conclusion then reached by means of the tautology

$$(A \wedge \sim A) \Rightarrow B \quad .$$

4.27 $\vdash t \equiv s \pmod{\bar{k}} \Leftrightarrow s \equiv t \pmod{\bar{k}}$.

Proof: By means of the tautology
$A \vee B \Rightarrow B \vee A$. ⟶

$\vdash t \equiv s \pmod{\bar{k}} \Leftrightarrow t + r \equiv s + r \pmod{\bar{k}}$.

Proof: Two conditional proofs, using 4.10 and 4.11 in the first implication, and 4.13 and 4.21 in the second. ⟶

4.29 $\vdash t < s \Rightarrow s \not< t$.

Proof: Indirect proof, using 4.23 and 4.25.

4.30 $\vdash (t < s) \vee (t = s) \vee (s < t)$.

Proof: By induction on y in
$A(y) : (x < y) \vee (x = y) \vee (y < x)$

(i)	1.	$x \neq 0$	Hyp.
	2.	$x = 0 + x$	4.11
	3.	$0 + x = x$	2, 4.7
	4.	$(\exists w)[w \neq 0 \wedge 0 + w = x]$	1,3, 2.4
	5.	$0 < x$	4, 4.19
	6.	$(x < 0) \vee (0 < x)$	5 Taut.
	7.	$x \neq 0 \Rightarrow [(x < 0) \vee (0 < x)]$	1 C., 2.2

	8.	$(x = 0) \vee (x < 0) \vee (0 < x)$	7, Def.
	9.	$(x < 0) \vee (x = 0) \vee (0 < x)$	8 Taut.

Hence $\vdash A(0)$.

(ii)	1.	$(x < y) \vee (x = y) \vee (y < x)$	Hyp.
	2.	$x = y$	Hyp.
	3.	$x + \bar{1} = y + \bar{1}$	4.10
	4.	$y + \bar{1} = y'$	4.22
	5.	$x + \bar{1} = y'$	3,4, 4.8
	6.	$\bar{1} \neq 0$	4.3
	7.	$(\exists w)[w \neq 0 \wedge x + w = y']$	5,6, 2.4
	8.	$x < y'$	7, 4.19
	9.	$(x < y') \vee (x = y') \vee (y' < x)$	8 Taut.
	10.	$x = y \Rightarrow [(x < y') \vee (x = y') \vee (y' < x)]$	2-9, 2.2
	11.	$x < y$	Hyp.
	12.	$y < y'$	4.24
	13.	$x < y'$	11,12, 4.25
	14.	$(x < y') \vee (x = y') \vee (y' < x)$	13 Taut.
	15.	$x < y \Rightarrow [(x < y') \vee (x = y') \vee (y' < x)]$	11-14 2.2
	16.	$y < x$	Hyp.
	17.	$(\exists w)[w \neq 0 \wedge y + w = x]$	16, [illegible]
	18.	$\bar{k} \neq 0 \wedge y + \bar{k} = x$	17
	19.	$\bar{k} \neq 0$	18
	20.	$(\exists z)[\bar{k} = z']$	19, 4
	21.	$\bar{k} = \bar{n}'$	20, [illegible] C
	22.	$\bar{n}' = \bar{n} + \bar{1}$	4.
	23.	$\bar{k} = \bar{n} + \bar{1}$	21,22, [illegible] 8
	24.	$\bar{n} + \bar{1} = \bar{1} + \bar{n}$	4.13
	25.	$\bar{k} = \bar{1} + \bar{n}$	23,24, 4.8
	26.	$y + \bar{k} = x$	18, Taut.
	27.	$y + (\bar{1} + \bar{n}) = y + \bar{k}$	25, 4.14
	28.	$y + (\bar{1} + \bar{n}) = x$	27,26, 4.8
	29.	$(y + \bar{1}) + \bar{n} = x$	28, 4.15
	30.	$y' + \bar{n} = x$	29, 4.22
	31.	$\bar{n} = 0 \vee \bar{n} \neq 0$	Taut.

32.	$\bar{n} = 0$	Hyp.
33.	$y' + 0 = y' + \bar{n}$	32, 4.14
34.	$y' + 0 = x$	33,30, 4.8
35.	$y' = y' + 0$	4.4, 4.7
36.	$y' = x$	35,34, 4.8
37.	$\bar{n} = 0 \Rightarrow y' = x$	32-36, 2.2
38.	$\bar{n} \neq 0$	Hyp.
39.	$(\exists w)[w \neq 0 \wedge y' + w = x]$	38,30, 2.4
40.	$y' < x$	39, 4.19
41.	$\bar{n} \neq 0 \Rightarrow y' < x$	38-40, 2.2
42.	$(\bar{n} = 0 \Rightarrow y' = x) \wedge (\bar{n} \neq 0 \Rightarrow y' < x)$	37, 41 Taut.
43.	$(\bar{n} = 0 \vee \bar{n} \neq 0) \Rightarrow (y' = x \vee y' < x)$	42 Taut.
44.	$(y' = x) \vee (y' < x)$	43,31, M.P.
45.	$(x < y') \vee (x = y') \vee (y' < x)$	44 Taut.
46.	$y < x \Rightarrow [(x < y') \vee (x = y') \vee (y' < x)]$	16, 45, 2.2
47.	$x < y \Rightarrow [(x < y') \vee (x = y') \vee (y' < x)]$ $\wedge\ x = y \Rightarrow [(x < y') \vee (x = y') \vee (y < x)]$ $\wedge\ y < x \Rightarrow [(x < y') \vee (x = y') \vee (y' < x)]$	10,15,46 Taut.
48.	$[(x < y) \vee (x = y) \vee (y < x)] \Rightarrow [(x < y') \vee (x = y') \vee (y' < x)]$	47 Taut.
49.	$[(x < y') \vee (x = y') \vee (y' < x)]$	1,48 M.P.
50.	$[(x < y) \vee (x = y) \vee (y < x)] \Rightarrow [(x < y') \vee (x = y') \vee (y' < x)]$	1-49, 2.2

Hence $\vdash A(y) \Rightarrow A(y')$.

So, by Gen. and the Induction Rule:

$$\vdash (\forall y)Ay .$$

Then, by Gen. and 2.3:

$$\vdash (t < s) \vee (t = s) \vee (s < t) .$$

→

4.31 $\vdash t \equiv s \pmod{\bar{n}} \Leftrightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$

Proof:

1.	$t \equiv s \pmod{\bar{n}}$	Hyp.
2.	$(\exists w)[t = s + w\cdot\bar{n} \vee s = t + w\cdot\bar{n}]$	1, 4.18
3.	$t = s + \bar{k}\cdot\bar{n} \vee s = t + \bar{k}\cdot\bar{n}$	2, Rule C
4.	$t = s + \bar{k}\cdot\bar{n}$	Hyp.
5.	$t + r\cdot\bar{n} = s + \bar{k}\cdot\bar{n} + r\cdot\bar{n}$	4, 4.10
6.	$t + r\cdot\bar{n} = s + (\bar{k} + r)\cdot\bar{n}$	5, 4.17(d)
7.	$t + r\cdot\bar{n} = s + (\bar{k} + r)\cdot\bar{n} \vee s = t + r\cdot\bar{n} + (\bar{k}+r)\cdot\bar{n}$	6 Taut.
8.	$(\exists w)[t + r\cdot\bar{n} = s + w\cdot\bar{n} \vee s = t + r\cdot\bar{n} + w\cdot\bar{n}]$	7, 2.4
9.	$t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$	8, 4.18
10.	$t = s + \bar{k}\cdot\bar{n} \Rightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$	4-9, 2.2
11.	$s = t + \bar{k}\cdot\bar{n}$	Hyp.
12.	$r = \bar{k}$	Hyp.
13.	$r\cdot\bar{n} = \bar{k}\cdot\bar{n}$	12, 4.17(c)
14.	$t + \bar{k}\cdot\bar{n} = t + r\cdot\bar{n}$	13, 4.14
15.	$s = t + r\cdot\bar{n}$	11, 14, 4.8
16.	$t + r\cdot\bar{n} = t + r\cdot\bar{n} + 0\cdot\bar{n}$	4.4, 4.7
17.	$s = t + r\cdot\bar{n} + 0\cdot\bar{n}$	15,16, 4.8
18.	$t + r\cdot\bar{n} = s + 0\cdot\bar{n} \vee s = t + r\cdot\bar{n} + 0\cdot\bar{n}$	17 Taut.
19.	$(\exists w)[t + r\cdot\bar{n} = s + w\cdot\bar{n} \vee s = t + r\cdot\bar{n} +$	18, 2.4
20.	$t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$	19, 4.18
21.	$r = \bar{k} \Rightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$	12-20, 2.1
22.	$r < \bar{k}$	Hyp.
23.	$(\exists w)[w \neq 0 \wedge r + w = \bar{k}]$	22, 4.16
24.	$\bar{m} \neq 0 \wedge r + \bar{m} = \bar{k}$	23, 4.18, 2.4
25.	$r + \bar{m} = \bar{k}$	24 Taut.
26.	$\bar{k} = r + \bar{m}$	25, 4.7
27.	$\bar{k}\cdot\bar{n} = (r + \bar{m})\cdot\bar{n}$	26, 4.17(e)
28.	$t + \bar{k}\cdot\bar{n} = t + (r + \bar{m})\cdot\bar{n}$	27, 4.14
29.	$s = t + (r + \bar{m})\cdot\bar{n}$	11,28, 4.8
30.	$s = t + r\cdot\bar{n} + \bar{m}\cdot\bar{n}$	29, 4.17(d)

31. $t + r\cdot\bar{n} = s + \bar{m}\cdot\bar{n} \vee s = t + r\cdot\bar{n} + \bar{m}\cdot\bar{n}$ 30 Taut.

32. $(\exists w)[t + r\cdot\bar{n} = s + w\cdot\bar{n} \vee s = t + r\cdot\bar{n} + w\cdot\bar{n}]$ 31, 2.4

33. $t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ 32, 4.18

34. $r < \bar{k} \Rightarrow [t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$ 22-33, 2.2

35. $\bar{k} < r$ Hyp.

36. $(\exists w)[w \neq 0 \wedge \bar{k} + w = r]$ 35, 4.19

37. $\bar{p} \neq 0 \wedge \bar{k} + \bar{p} = r$ 36, Rule C

38. $\bar{k} + \bar{p} = r$ 37 Taut.

39. $t + \bar{k}\cdot\bar{n} = s$ 11, 4.7

40. $t + \bar{k}\cdot\bar{n} + \bar{p}\cdot\bar{n} = s + \bar{p}\cdot\bar{n}$ 39, 4.10

41. $t + (\bar{k} + \bar{p})\cdot\bar{n} = t + \bar{k}\cdot\bar{n} + \bar{p}\cdot\bar{n}$ 4.1, d), 4.14

42. $t + (\bar{k} + \bar{p})\cdot\bar{n} = s + \bar{p}\cdot\bar{n}$ 41,40, 4.8

43. $(\bar{k} + \bar{p})\cdot\bar{n} = r\cdot\bar{n}$ 38, 4.17(e)

44. $t + r\cdot\bar{n} = t + (\bar{k} + \bar{p})\cdot\bar{n}$ 43, 4.7, 4.14

45. $t + r\cdot\bar{n} = s + \bar{p}\cdot\bar{n}$ 44,42, 4.8

46. $t + r\cdot\bar{n} = s + \bar{p}\cdot\bar{n} \vee s = t + r\cdot\bar{n} + \bar{p}\cdot\bar{n}$ 45 Taut.

47. $(\exists w)[t + r\cdot\bar{n} = s + w\cdot\bar{n} \vee s = t + r\cdot\bar{n} + w\cdot\bar{n}]$ 46, 2.4

48. $t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ 47, 4.18

49. $\bar{k} < r \Rightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ 35-48, 2.2

50. $r < \bar{k} \Rightarrow [t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$
$\wedge\ r = \bar{k} \Rightarrow [t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$
$\wedge\ \bar{k} < r \Rightarrow [t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$ 34,21,50 Taut.

51. $[(r < \bar{k}) \vee (r = \bar{k}) \vee (\bar{k} < r)] \Rightarrow [t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$ 50 Taut.

52. $t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ 4.30, 51, M.P.

53. $s = t + \bar{k}\cdot\bar{n} \Rightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ 11-53, 2.2

54. $[t = s + \bar{k}\cdot\bar{n} \Rightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$
$\wedge\ [s = t + \bar{k}\cdot\bar{n} \Rightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$ 10,53 Taut.

55. $[t = s + \bar{k}\cdot\bar{n} \vee s = t + \bar{k}\cdot\bar{n}] \Rightarrow [t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}]$ 54 Taut.

56. $t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ 3,55, M.P.

57. $t \equiv s \pmod{\bar{n}} \Rightarrow t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ 1-56, 2.2

58. $t + r\cdot\bar{n} \equiv s \pmod{\bar{n}}$ Hyp.

59. $(\exists w)[t + r\cdot\bar{n} = s + w\cdot\bar{n} \vee s = t + r\cdot\bar{n} + w\cdot\bar{n}]$ 58, 4.18

60. $t + r\cdot\bar{n} = s + \bar{q}\cdot\bar{n} \vee s = t + r\cdot\bar{n} + \bar{q}\cdot\bar{n}$ 59, Rule C

61. $s = t + r\cdot\bar{n} + \bar{q}\cdot\bar{n}$ Hyp.

62. $t + r\cdot\bar{n} + q\cdot\bar{n} = t + (r + \bar{q})\cdot\bar{n}$ 4.17(d), 4.14

63. $s = t + (r + \bar{q})\cdot\bar{n}$ 61,62, 4.8

64. $t = s + (r + \bar{q})\cdot\bar{n} \vee s = t + (r + \bar{q})\cdot\bar{n}$ 63 Taut.

65. $(\exists w)[t = s + w\cdot\bar{n} \vee s = t + w\cdot\bar{n}]$ 64, 2.4

66. $t \equiv s \pmod{\bar{n}}$ 65, 4.18

67. $s = t + r\cdot\bar{n} + \bar{q}\cdot\bar{n} \Rightarrow t \equiv s \pmod{\bar{n}}$ 61-66, 2.2

68. $t + r\cdot\bar{n} = s + \bar{q}\cdot\bar{n}$ Hyp.

69. $r = \bar{q}$ Hyp.

70. $\bar{q}\cdot\bar{n} = r\cdot\bar{n}$ 69,4.7,4.17(e)

71. $s + \bar{q}\cdot\bar{n} = s + r\cdot\bar{n}$ 70, 4.14

72. $t + r\cdot\bar{n} = s + r\cdot\bar{n}$ 68,71, 4.8

73. $t = s$ 72, 4.21

74. $s = s + 0\cdot\bar{n}$ 4.4, 4.7

75. $t = s + 0\cdot\bar{n}$ 73,74, 4.8

76. $t = s + 0\cdot\bar{n} \vee s = t + 0\cdot\bar{n}$ 75 Taut.

77. $(\exists w)[t = s + w\cdot\bar{n} \vee s = t + w\cdot\bar{n}]$ 76, 2.4

78. $t \equiv s \pmod{\bar{n}}$ 77, 4.18

79. $r = \bar{q} \Rightarrow t \equiv s \pmod{\bar{n}}$ 69-78, 2.2

80. $r < \bar{q}$ Hyp.

81. $(\exists w)[w \neq 0 \wedge r + w = \bar{q}]$ 80, 4.19

82. $\bar{\ell} \neq 0 \wedge r + \bar{\ell} = \bar{q}$ 81, Rule C

83. $r + \bar{\ell} = \bar{q}$ 82 Taut.

84. $t + r\cdot\bar{n} + \bar{\ell}\cdot\bar{n} = s + \bar{q}\cdot\bar{n} + \bar{\ell}\cdot\bar{n}$ 68, 4.10

85. $t + (\bar{r} + \bar{\ell})\cdot\bar{n} = t + r\cdot\bar{n} + \bar{\ell}\cdot\bar{n}$ 4.17(d), 4.14

86. $t + (\bar{r} + \bar{\ell})\cdot\bar{n} = s + \bar{q}\cdot\bar{n} + \bar{\ell}\cdot\bar{n}$ 85,84, 4.8

87. $t + \bar{q}\cdot\bar{n} = t + (r + \bar{\ell})\cdot\bar{n}$ 83, 4.17(e), 4.14

88. $t + \bar{q}\cdot\bar{n} = s + \bar{q}\cdot\bar{n} + \bar{\ell}\cdot\bar{n}$ 87,86, 4.8

89. $s + \bar{q}\cdot\bar{n} + \bar{\ell}\cdot\bar{n} = s + \bar{\ell}\cdot\bar{n} + \bar{q}\cdot\bar{n}$ 73, 4.14

90. $t + \bar{q}\cdot\bar{n} = s + \bar{\ell}\cdot\bar{n} + \bar{q}\cdot\bar{n}$ 88,89, 4.8

91.	$t = s + \ell \cdot \bar{n}$	90, 4.21
92.	$t = s + \ell \cdot \bar{n} \vee s = t + \ell \cdot \bar{n}$	91 Taut.
93.	$(\exists w)[t = s + w \cdot \bar{n} \vee s = t + w \cdot \bar{n}]$	92, 2.4
94.	$t \equiv s \pmod{\bar{n}}$	93, 4.18
95.	$r < \bar{q} \Rightarrow t \equiv s \pmod{\bar{n}}$	80-94, 2.2
96.	$\bar{q} < r$	Hyp.
97.	$(\exists w)[w \neq 0 \wedge \bar{q} + w = r]$	96, 4.19
98.	$\bar{i} \neq 0 \wedge \bar{q} + \bar{i} = r$	97, Rule C
99.	$\bar{q} + \bar{i} = \bar{r}$	98 Taut
100.	$t + r \cdot \bar{n} + \bar{i} \cdot \bar{n} = s + \bar{q} \cdot \bar{n} + \bar{i} \cdot \bar{n}$	68, 4.10
101.	$s + \bar{q} \cdot \bar{n} + \bar{i} \cdot \bar{n} = s + (\bar{q} + \bar{i}) \cdot \bar{n}$	4.17(d), 4.14
102.	$t + r \cdot \bar{n} + \bar{i} \cdot \bar{n} = s + (\bar{q} + \bar{i}) \cdot \bar{n}$	100,101, 4.8
103.	$t + \bar{i} \cdot \bar{n} + r \cdot \bar{n} = t + r \cdot \bar{n} + \bar{i} \cdot \bar{n}$	4.13, 4.14
104.	$t + \bar{i} \cdot \bar{n} + r \cdot \bar{n} = s + (\bar{q} + \bar{i}) \cdot \bar{n}$	103,102, 4.8
105.	$s + (\bar{q} + \bar{i}) \cdot \bar{n} = s + r \cdot \bar{n}$	99,4.17(e), 4.14
106.	$t + \bar{i} \cdot \bar{n} + r \cdot \bar{n} = s + r \cdot \bar{n}$	104,105, 4.8
	$t + \bar{i} \cdot \bar{n} = s$	106, 4.21
108.	$s = t + \bar{i} \cdot \bar{n}$	107, 4.7
109.	$t = s + \bar{i} \cdot \bar{n} \vee s = t + \bar{i} \cdot \bar{n}$	108 Taut.
110.	$(\exists w)[t = s + w \cdot \bar{n} \vee s = t + w \cdot \bar{n}]$	109, 2.4
111.	$t \equiv s \pmod{\bar{n}}$	110, 4.18
112.	$\bar{q} < r \Rightarrow t \equiv s \pmod{\bar{n}}$	96-111, 2.2
113.	$[r < \bar{q} \Rightarrow t \equiv s \pmod{\bar{n}}$ $\wedge [r = \bar{q} \Rightarrow t \equiv s \pmod{\bar{n}}]$ $\wedge [\bar{q} < r \Rightarrow t \equiv s \pmod{\bar{n}}]$	95, 79,112 Taut.
114.	$[(r < \bar{q}) \vee (r = \bar{q}) \vee (\bar{q} < r)]$ $\Rightarrow t \equiv s \pmod{\bar{n}}$	113 Taut.
115.	$t \equiv s \pmod{\bar{n}}$	4.30, 114, M.P.
116.	$t + r \cdot \bar{n} = s + \bar{q} \cdot \bar{n} \Rightarrow t \equiv s \pmod{\bar{n}}$	68-115, 2.2
117.	$[s = t + r \cdot \bar{n} + \bar{q} \cdot \bar{n} \Rightarrow t \equiv s \pmod{\bar{n}}]$ $\wedge [t + r \cdot \bar{n} = s + \bar{q} \cdot \bar{n} \Rightarrow t \equiv s \pmod{\bar{n}}]$	67,116 Taut.
118.	$[s = t + r \cdot \bar{n} + \bar{q} \cdot \bar{n} \vee t + r \cdot \bar{n} = s + \bar{q} \cdot \bar{n}]$ $\Rightarrow t \equiv s \pmod{\bar{n}}$	117 Taut.
119.	$t \equiv s \pmod{\bar{n}}$	60,118 M.P.
120.	$t + r \cdot \bar{n} \equiv s \pmod{\bar{n}} \Rightarrow t \equiv s \pmod{\bar{n}}$	58-120, 2.2
121.	$t \equiv s \pmod{\bar{n}} \Leftrightarrow t + r \cdot \bar{n} \equiv s \pmod{\bar{n}}$	57,120 Taut.

→

4.32 $\vdash(\bar{p}' = \bar{n}) \Rightarrow [t + s \equiv r \pmod{\bar{n}} \Leftrightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}]$.

Proof:

1.	$\bar{p}' = \bar{n}$	Hyp.
2.	$t + s \equiv r \pmod{\bar{n}}$	Hyp.
3.	$(\exists w)[t + s = r + w\cdot\bar{n} \vee r = t + s + w\cdot\bar{n}]$	2, 4.18
4.	$t + s = r + \bar{m}\cdot\bar{n} \vee r = t + s + \bar{m}\cdot\bar{n}$	3, Rule C
5.	$t + s = r + \bar{m}\cdot\bar{n}$	Hyp.
6.	$t + s + s\cdot\bar{p} = r + \bar{m}\cdot\bar{n} + s\cdot\bar{p}$	5, 4.10
7.	$r + \bar{m}\cdot\bar{n} + s\cdot\bar{p} = r + s\cdot\bar{p} + \bar{m}\cdot\bar{n}$	4.13, 4.14
8.	$t + s + s\cdot\bar{p} = r + s\cdot\bar{p} + \bar{m}\cdot\bar{n}$	6,7, 4.8
9.	$t + s(\bar{1} + \bar{p}) = t + s + s\cdot\bar{p}$	4.17(c),Conv.1,4.14
10.	$t + s(\bar{1} + \bar{p}) = r + s\cdot\bar{p} + \bar{m}\cdot\bar{n}$	9,8, 4.8
11.	$\bar{n} = \bar{1} + \bar{p}$	1, 4.13, 4.22
12.	$t + s\cdot\bar{n} = t + s\cdot(\bar{1} + \bar{p})$	11,4.17(e),4.14
13.	$t + s\cdot\bar{n} = r + s\cdot\bar{p} + \bar{m}\cdot\bar{n}$	12,10, 4.8
14.	$t + s\cdot\bar{n} = r + s\cdot\bar{p} + \bar{m}\cdot\bar{n} \vee r + s\cdot\bar{p} = t + s\cdot\bar{n} + \bar{m}\cdot\bar{n}$	13 Taut.
15.	$(\exists w)[t + s\cdot\bar{n} = r + s\cdot\bar{p} + w\cdot\bar{n} \vee \ldots \cdot s\cdot\bar{p} = t + s\cdot\bar{n} + w\cdot\bar{n}]$	14, 2.4
16.	$t + s\cdot\bar{n} \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$	15, 4.18
17.	$t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$	16, 4.31
18.	$t + s = r + \bar{m}\cdot\bar{n} \Rightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$	5-17, 2
19.	$r = t + s + \bar{m}\cdot\bar{n}$	Hyp.
20.	$r + s\cdot\bar{p} = t + s + \bar{m}\cdot\bar{n} + s\cdot\bar{p}$	19, 4.10
21.	$t + s + \bar{m}\cdot\bar{n} + s\cdot\bar{p} = t + s(\bar{1} + \bar{p}) + \bar{m}\cdot\bar{n}$	4.13, 4.17(c)
22.	$r + s\cdot\bar{p} = t + s(\bar{1} + \bar{p}) + \bar{m}\cdot\bar{n}$	20,21, 4.8
23.	$\bar{1} + \bar{p} = \bar{n}$	1, 4.22, 4.13
24.	$t + s\cdot(\bar{1} + \bar{p}) + \bar{m}\cdot\bar{n} = t + s\cdot\bar{n} + \bar{m}\cdot\bar{n}$	23,4.17(e).4.10,4.14
25.	$r + s\cdot\bar{p} = t + s\cdot\bar{n} + \bar{m}\cdot\bar{n}$	22,24, 4.8

26. $t + s\cdot\bar{n} = r + s\cdot\bar{p} + \bar{m}\cdot\bar{n} \vee r + s\cdot\bar{p} = t + s\cdot\bar{n} + \bar{m}\cdot\bar{n}$ 25 Taut.

27. $(\exists w)[t + s\cdot\bar{n} = r + s\cdot\bar{p} + w\cdot\bar{n} \vee r + s\cdot\bar{p} = t + s\cdot\bar{n} + w\cdot\bar{n}]$ 26, 2.4

28. $t + s\cdot\bar{n} \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ 27, 4.18

29. $t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ 28, 4.31

30. $r = t + s + \bar{m}\cdot\bar{n} \Rightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ 19-30, 2.2

31. $[t + s = r + \bar{m}\cdot\bar{n} \Rightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}] \wedge [r = t + s + \bar{m}\cdot\bar{n} \Rightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}]$ 18,30 Taut.

32. $[t + s = r + \bar{m}\cdot\bar{n} \vee r = t + s + \bar{m}\cdot\bar{n}] \Rightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ 31 Taut.

33. $t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ 4,32, M.P.

34. $t + s \equiv r \pmod{\bar{n}} \Rightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ 2-33, 2.2

35. $t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ Hyp.

36. $(\exists w)[t = r + s\cdot\bar{p} + w\cdot\bar{n} \vee r + s\cdot\bar{p} = t + w\cdot\bar{n}]$ 35, 4.18

37. $t = r + s\cdot\bar{p} + \bar{k}\cdot\bar{n} \vee r + s\cdot\bar{p} = t + \bar{k}\cdot\bar{n}$ 36, Rule C

38. $t = r + s\cdot\bar{p} + \bar{k}\cdot\bar{n}$ Hyp.

39. $t + s = r + s\cdot\bar{p} + \bar{k}\cdot\bar{n} + s$ 38, 4.1[illegible]

40. $r + s\cdot\bar{p} + \bar{k}\cdot\bar{n} + s = r + s\,(\bar{p} + \bar{1}) + \bar{k}\cdot\bar{n}$ 4.13, 4.17(c)

41. $t + s = r + s\,(\bar{p} + \bar{1}) + \bar{k}\cdot\bar{n}$ 39,40, [illegible].8

42. $\bar{p} + \bar{1} = \bar{n}$ 1,4.22, 4.13

43. $r + s\cdot(\bar{p} + \bar{1}) + \bar{k}\cdot\bar{n} = r + s\cdot\bar{n} + \bar{k}\cdot\bar{n}$ 42,4.17(e),4.10,4.[illegible]

44. $t + s = r + s\cdot\bar{n} + \bar{k}\cdot\bar{n}$ 41,43, 4.8

45. $t + s = r + s\cdot\bar{n} + \bar{k}\cdot\bar{n} \vee r + s\cdot\bar{n} = t + s + \bar{k}\cdot\bar{n}$ 44 Taut.

46. $(\exists w)[t + s = r + s\cdot\bar{n} + \bar{k}\cdot\bar{n} \vee r + s\cdot\bar{n} = t + s + \bar{k}.\bar{n}]$ 45, 2.4

47. $t + s \equiv r + s\cdot\bar{n} \pmod{\bar{n}}$ 4[illegible] 4.18

48. $t + s \equiv r \pmod{\bar{n}}$ 47, 4.27, 4.31

49. $t = r + s\cdot\bar{p} + \bar{k}\cdot\bar{n} \Rightarrow t + s \equiv r \pmod{\bar{n}}$ 38-48, M.P.

50. $r + s\cdot\bar{p} = t + \bar{k}\cdot\bar{n}$ Hyp.

51. $r + s\cdot\bar{p} + s = t + \bar{k}\cdot\bar{n} + s$ 50, 4.10

52. $\bar{n} = \bar{p} + \bar{1}$ 1,4.7,4.22

53. $r + s\cdot\bar{n} = r + s\cdot(\bar{p} + \bar{1})$ 52,4.17(e), 4.14

54. $r + s\cdot(\bar{p} + \bar{1}) = r + s\cdot\bar{p} + s$ 4.17(c), 4.14

55. $r + s\cdot\bar{n} = r + s\cdot\bar{p} + s$ 53,54, 4.8

56. $r + s\cdot\bar{n} = t + \bar{k}\cdot\bar{n} + s$ 55,51, 4.8

57. $t + \bar{k}\cdot\bar{n} + s = t + s + \bar{k}\cdot\bar{n}$ 4.13, 4.14

58. $r + s\cdot\bar{n} = t + s + \bar{k}\cdot\bar{n}$ 56,57, 4.8

59. $t + s = r + s\cdot\bar{n} + \bar{k}\cdot\bar{n} \vee r + s\cdot\bar{n} = t + s + \bar{k}\,\bar{n}$ 58 Taut

60. $(\exists w)[t + s = r + s\cdot\bar{n} + w\cdot\bar{n} \vee r + s\cdot\bar{n} = t + w\cdot\bar{n}]$ 59, 2.4

61. $t + s \equiv r + s\cdot\bar{n} \pmod{\bar{n}}$ 60, 4.18

62. $t + s \equiv r \pmod{\bar{n}}$ 61,4.27,4.31

63. $r + s\cdot\bar{p} = t + \bar{k}.\bar{n} \Rightarrow t + s \equiv r \pmod{\bar{n}}$ 50-62, 2.2

64. $[t = r + s\cdot\bar{p} + \bar{k}\cdot\bar{n} \Rightarrow t + s \equiv r \pmod{\bar{n}}]$
$\wedge\ [r + s\cdot\bar{p} = t + \bar{k}\cdot\bar{n} \Rightarrow t + s \equiv r \pmod{\bar{n}}]$ 49,63, Taut.

65. $[t = r + s\cdot\bar{p} + \bar{k}\cdot\bar{n} \vee r + s\cdot\bar{p} = t + \bar{k}\cdot\bar{n}]$
$\Rightarrow t + s \equiv r \pmod{\bar{n}}$ 64 Taut.

66. $t + s \equiv r \pmod{\bar{n}}$ 37,65, M.P.

67. $t \equiv r + s\cdot\bar{p} \pmod{\bar{n}} \Rightarrow t + s \equiv r \pmod{\bar{n}}$ 35-66, 2.2

68. $t + s \equiv r \pmod{\bar{n}} \Leftrightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}$ 34,67 Taut.

69. $(\bar{p}' = \bar{n}) \Rightarrow [t + s \equiv r \pmod{\bar{n}} \Leftrightarrow t \equiv r + s\cdot\bar{p} \pmod{\bar{n}}]$ 1-68, 2.2

→

4.33 $\vdash t + s = 0 \Leftrightarrow t = 0 \wedge s = 0$.

Proof: To the right : By induction on y in:
$A(y) : x + y = 0 \Rightarrow x = 0 \wedge y = 0$.
To the left : From 4.4, $0 + 0 = 0$.

→

4.34 $\vdash r = s \Leftrightarrow r < s' \wedge s < r'$

Proof: To the right : Conditional proof, using 4.24.
To the left : Conditional proof, using 4.8, 4.10, 4.13, 4.21, 4.22, 4.23 and 4.33. $\longrightarrow$

4.35 $\vdash r \neq s \Leftrightarrow (r < s \vee s < r)$

Proof: To the right : From 4.30.
To the left : Conditional proof, using 4.23. $\longrightarrow$

4.36 $\vdash r \not< s \Leftrightarrow s < r'$

Proof: Conditional proofs, using 4.30, 4.23 and 4.25. $\longrightarrow$

4.37 $\vdash t + r < s + r \Leftrightarrow t < s$.

Proof: Conditional proofs, using 4.10, 4.13 and 4.21. $\longrightarrow$

4 $\vdash [t \equiv s \pmod{\bar{n}} \wedge s \equiv r \pmod{\bar{n}}] \Rightarrow t \equiv r \pmod{\bar{n}}$.

Proof: Conditional proof, follows easily from definitions and 4.31. $\longrightarrow$

4.39 Proposition:

For any terms r and s, and any numerical $\bar{n}$:

$\vdash_{S_1} + [r \equiv s \pmod{\bar{n}} \vee r \equiv s + \bar{1} \pmod{\bar{n}} \vee \ldots$
$\ldots \vee r \equiv s + \bar{p} \pmod{\bar{n}}]$

where $\bar{p}' = \bar{n}$ — i.e. $p = n - 1$.

Proof: Consider any r, s and $\bar{n}$.

If $r = s$, then $r = s + 0 \cdot \bar{n}$, so that $r \equiv s \pmod{\bar{n}}$.

So, suppose $r \neq s$. Then, by 4.30 :
either $r < s$ or $s < r$.

Suppose $s < r$. Then by 4.19 $(\exists w)[w \neq 0 \wedge s + w = r]$
— say $\bar{k} \neq 0 \wedge s + \bar{k} = r$ (1)
using 2.4.

(i) If $\bar{k} < \bar{n}$, then:

$$r = s + \bar{k} + 0 \cdot \bar{n}$$

hence

$$r \equiv s + \bar{k} \pmod{\bar{n}} .$$

(ii) If $\bar{k} = \bar{n}$, then, from (1):

$$r = s + \bar{n} = s + \bar{1} \cdot \bar{n} ,$$

and hence

$$r \equiv s \pmod{\bar{n}} .$$

(iii) If $\bar{n} < \bar{k}$, then $(\exists w)[w \neq 0 \wedge \bar{n} + w = \bar{k}]$
— say $\bar{p} \neq 0 \wedge \bar{n} + \bar{p} = \bar{k}$, (2)
applying 2.4.

Then, from (1) and (2):

$$\begin{aligned} r &= s + \bar{n} + \bar{p} \\ &= s + \bar{p} + \bar{n} \\ &= s + \bar{p} + \bar{1} \cdot \bar{n} \end{aligned}$$

and hence

$$r \equiv s + \bar{p} \pmod{\bar{n}} .$$

Now if $\bar{p} < \bar{n}$, there is nothing more to prove.
If $\bar{p} = \bar{n}$, then

$$r \equiv s + \bar{n} \pmod{\bar{n}}$$

and hence

$$r \equiv s \pmod{\bar{n}}$$ by 4.31 so that in this case as well the theorem is proved.

If $\bar{n} < \bar{p}$, then simply by repeating the process described in (iii) some $\bar{q} < \bar{n}$ must eventually be reached such that

$$r \equiv s + \bar{q} \pmod{\bar{n}}$$

and hence the theorem is proved.

The case where $r < s$ is proved analogously. ⟶

If the term s is taken to be 0 in 4.39, it is obvious that

$$\vdash [r \equiv 0 \pmod{\bar{n}} \vee r \equiv \bar{1} \pmod{\bar{n}} \vee \ldots . \ldots \vee r \equiv s + \overline{n-1} \pmod{\bar{n}}] .$$

Furthermore, by 4.31 it follows that

$$r \equiv 0 \pmod{\bar{n}} \Leftrightarrow r \equiv \bar{n} \pmod{\bar{n}}$$

so that

$$\vdash [r \equiv \bar{1} \pmod{\bar{n}} \vee r \equiv \bar{2} \pmod{\bar{n}} \vee \ldots\ldots \vee r \equiv \bar{n} \pmod{\bar{n}}] .$$

Also, by simple manipulation of the logical connectives in 4.39, it follows that:

$$\vdash r \not\equiv s \pmod{\bar{n}} \Leftrightarrow [r \equiv s + \bar{1} \pmod{\bar{n}} \vee \ldots \vee r \equiv s + \overline{n-1} \pmod{\bar{n}}] .$$

All three of these formulations are to be regarded as alternative formulations of 4.39. When, in future, reference is made to 4.39, it will in general not be indicated to which of the four alternative formulations is being referred — this should, in any case, be clear from the context.

4.40 $$\vdash x \equiv \bar{k} \pmod{\bar{n}} \Leftrightarrow x \cdot \bar{p} \equiv \bar{k} \cdot \bar{p} \pmod{\bar{n} \cdot \bar{p}} .$$

Proof: Follows easily from definition 4.18 by applying proposition 4.17. →

4.41 Proposition:

$$\vdash (\exists x)[(x \equiv \bar{k} \pmod{\bar{n}}) \wedge (t < x \cdot \bar{p} + r) \wedge (x \cdot \bar{p} + r < s)] \Leftrightarrow (\exists x)[(x \equiv \bar{k} \cdot \bar{p} \pmod{\bar{n} \cdot \bar{p}}) \wedge (t < x + r) \wedge (x + r < s)] .$$

Proof:

(i) Suppose $x \equiv \bar{k} \pmod{\bar{p}} \wedge t < x \cdot \bar{p} + r \wedge x \cdot \bar{p} + r < s$.

Then, by 4.40:

$$x \cdot \bar{p} \equiv \bar{k} \cdot \bar{p} \pmod{\bar{n} \cdot \bar{p}} \wedge t < x \cdot \bar{p} + r \wedge x \cdot \bar{p} + r < s .$$

Now quantify over $x \cdot \bar{p}$.

(ii) Now suppose that

$$x \equiv \bar{k} \cdot \bar{p} \pmod{\bar{n} \cdot \bar{p}} \wedge t < x + r \wedge x + r < s .$$

By 4.39, x can be assumed to be between 1 and $\bar{n} \cdot \bar{p}$.

Now if $\bar{k} \leq \bar{n}$, then it follows that

$$x = \bar{k} \cdot \bar{p} .$$

If $\bar{n} < \bar{k}$, then, for some $\bar{m}$ between $\bar{1}$ and $\bar{n}$ (by 4.39):

$$\bar{k} \equiv \bar{m} \pmod{\bar{n}} ,$$

in which case it follows that

$$x = \bar{m} \cdot \bar{p} .$$

Thus, in any case, it follows that x can be expressed as a product $\bar{q} \cdot \bar{p}$, where $\bar{q} < \bar{n}$.

So:

$$\bar{q} \cdot \bar{p} \equiv \bar{k} \cdot \bar{p} \pmod{\bar{n} \cdot \bar{p}} \wedge t < \bar{q} \cdot \bar{p} + r \wedge \bar{q} \cdot \bar{p} + r < s .$$

Hence, by 4.40:

$$\bar{q} \equiv \bar{k} \pmod{\bar{n}} \wedge t < \bar{q} \cdot \bar{p} + r \wedge \bar{q} \cdot \bar{p} + r < s .$$

Now quantify over $\bar{q}$. $\longrightarrow$

4.42 Proposition:

The wff :

$(\exists x)[x \equiv \bar{m} \pmod{\bar{n}}) \wedge (t < x + r) \wedge (x + r < s)]$

is provable in S_1 iff. the D.N.F. :

$$[(t < r) \vee (r + \bar{m} < s)] \vee D_1 \vee \cdots \vee D_n$$

is true, where D_q is shorthand for :

$$(r < t') \wedge (t + \bar{q} < s) \wedge (t + \bar{q} \equiv r + \bar{m} \pmod{\bar{n}}).$$

Proof:

(i) Suppose the wff is provable. Then, by Rule C, there is some numeral $\bar{k}$ fulfilling the three conditions:

$$\bar{k} \equiv \bar{m} \pmod{\bar{n}} \qquad (1)$$
$$t < \bar{k} + r \qquad (2)$$
$$\bar{k} + r < s \qquad (3) .$$

By 4.39, $\bar{m}$ may be assumed to be between 0 and $\overline{n-1}$, both inclusive.

From (1) it follows by 4.18 that, for some numeral $\bar{p}$:

$$\bar{k} = \bar{m} + \bar{p} \cdot \bar{n} \qquad (4) .$$

From (2) and (3) it follows by 4.25 that

$$t < s ,$$

so that, by 4.19, there is some numeral $\bar{\ell}$ such that:

$$\bar{\ell} \neq 0 \wedge t + \bar{\ell} = s \qquad (5) .$$

By 4.30 : $t < r \vee t = r \vee r < t$.

(a) If $t < r$, then, since:

$$\begin{aligned} r + \bar{m} &\leq r + \bar{m} + \bar{p} \cdot \bar{n} \\ &= r + \bar{k} && \text{by (4)} \\ &< s && \text{by (3)} \end{aligned}$$

it follows that : $(t < r) \wedge (r + \bar{m} < s)$,
so that the D.N.F. is true.

(b) If $t = r$, then $r < t'$ by 4.24, and furthermore:

$$\begin{aligned} t + \bar{m} &= r + \bar{m} \\ &\leq r + \bar{m} + \bar{p} \cdot \bar{n} \\ &= r + \bar{k} && \text{by (4)} \\ &< s && \text{by (3).} \end{aligned}$$

Also, since $t = r$, $t \equiv r \pmod{\bar{n}}$.

$\therefore$ $t + \bar{m} \equiv r + \bar{m} \pmod{\bar{n}}$.

Hence there is a $\bar{q}$, namely $\bar{m}$, such that

$$(r < t') \wedge (t + \bar{q} < s) \wedge (t + \bar{q} \equiv r + \bar{m} \pmod{\bar{n}})$$

and hence the D.N.F. is true.

(c) If $r < t$, then by 4.19 there is some numeral $\bar{i}$ such that

$$\bar{i} \neq 0 \wedge r + \bar{i} = t \qquad (6) .$$

From (2) and (6) it follows that : $\bar{i} < \bar{k}$, and hence, using 4.19 again, there is some $\bar{j}$ such that

$$\bar{j} \neq 0 \wedge \bar{i} + \bar{j} = \bar{k} \qquad (7) .$$

Now

$$\begin{aligned} t + \bar{j} &= r + \bar{i} + \bar{j} && \text{by (6)} \\ &= r + \bar{k} && \text{by (7)} \\ &< s && \text{by (3) .} \end{aligned}$$

Also: $t + \bar{j} = r + \bar{k}$

$= r + \bar{m} + \bar{p} \cdot \bar{n}$ by (4) ,

and hence: $t + \bar{j} \equiv r + \bar{m} \pmod{\bar{n}}$.

Hence: $r < t'$

$t + \bar{j} < s$

$t + \bar{j} \equiv r + \bar{m} \pmod{\bar{n}}$,

and hence D_j is true — if $j \leq n$.

If $n < j$, then for some h and z :

$j = h \cdot n + z$, $z < n$

and then $t + \bar{z} < s$

and $t + \bar{z} \equiv r + \bar{m} \pmod{\bar{n}}$.

Thus, for some q less than n, D_q is true, and hence the D.N.F. is true.

→

(i.) Now suppose the D.N.F. is true for some $\bar{m}$ between 0 and $\overline{n-1}$ and q between 1 and n .

Then at least one of the disjuncts is true.

(a) Suppose $(t < r) \wedge (r + \bar{m} < s)$ is true.

Then $t < \bar{m} + r$

$r + \bar{m} < s$

and $\bar{m} = \bar{m} \pmod{\bar{n}}$

so that the wff is provable.

(b) Now suppose D_q holds. Then

$r < t'$

$t + \bar{q} < s$

$t + \bar{q} \equiv r + \bar{m} \pmod{\bar{n}}$.

Since $r < t'$, it follows that:

$r = t \vee r < t$.

If $r = t$, then : $\bar{q} \equiv \bar{m} \pmod{\bar{n}}$

$\bar{q} + r < s$

and $t < \bar{q} + r$ (since $\bar{q} \neq 0$)

and hence the wff is provable.

If $r < t$, then there is some $\bar{k}$ such that

$\bar{k} \neq 0 \wedge r + \bar{k} = t$.

Hence $r + \bar{k} + \bar{q} \equiv r + \bar{m} \pmod{\bar{n}}$

$\therefore \quad \bar{k} + \bar{q} \equiv \bar{m} \pmod{\bar{n}}$ (1) .

Also: $t < t + \bar{q}$ (since $\bar{q} \neq 0$)

$= (r + \bar{k}) + \bar{q}$

$= (\bar{k} + \bar{q}) + r$ (2) .

And: $t + \bar{q} < s$

$\therefore \quad (r + \bar{k}) + \bar{q} < s$

$\therefore \quad (\bar{k} + \bar{q}) + r < s$ (3) .

So, by (1), (2) and (3), the wff is provable. $\longrightarrow$

4.43 Proposition:

(a) For any $\bar{m}$, there is no $\bar{n}$ such that:

$\bar{m} \cdot \bar{m} < \bar{n} \cdot \bar{n} < \bar{m}' \cdot \bar{m}'$.

(b) Let $\bar{q} = \bar{k} + \bar{q}_o \cdot \bar{n} = p \cdot p$, with $\bar{k} < \bar{n}$

$\bar{n} < \bar{q}_o$

$\bar{n} \neq 0$.

Then (i) $\bar{n} < \bar{p}$

(ii) $\bar{p} \cdot \bar{p} < \bar{q}_o' \cdot \bar{n} + \bar{k} < \bar{p}' \cdot \bar{p}'$.

Proof:

(a) Consider any $\bar{m}$ and $\bar{n}$ such that:

$\bar{m} \cdot \bar{m} < \bar{n} \cdot \bar{n}$ (1) .

By 4.30, $\bar{n} < \bar{m} \vee \bar{n} = \bar{m} \vee \bar{m} < \bar{n}$.

If $\bar{n} = \bar{m}$, then $\bar{m} \cdot \bar{m} = \bar{n} \cdot \bar{n}$ — contradicting (1).

If $\bar{n} < \bar{m}$, say $\bar{n} + \bar{k} = \bar{m}$, then

$$\begin{aligned}\bar{n}\cdot\bar{n} &< \bar{n}\cdot\bar{n} + \bar{2}\cdot\bar{n}\cdot\bar{k} + \bar{k}\cdot\bar{k} \\ &= (\bar{n} + \bar{k})(\bar{n} + \bar{k}) \\ &= \bar{m} \cdot \bar{m} \quad - \text{ contradicting (1) .}\end{aligned}$$

Hence $\bar{m} < \bar{n}$ — say $\bar{m} + \bar{k} = \bar{n}$, $\bar{k} \neq 0$.

Now if $\bar{k} = \bar{1}$, then

$$\bar{n}\cdot\bar{n} = (\bar{m} + \bar{1})(\bar{m} + \bar{1}) = \bar{m}'\cdot\bar{m}' ,$$

so that $\bar{n}\cdot\bar{n} \not< \bar{m}'\cdot\bar{m}'$.

If $\bar{k} > \bar{1}$, say $\bar{1} + \bar{q} = \bar{k}$, then

$$\begin{aligned}\bar{n}\cdot\bar{n} &= (\bar{m} + \bar{k})(\bar{m} + \bar{k}) \\ &= (\bar{m} + \bar{1} + \bar{q})(\bar{m} + \bar{1} + \bar{q}) \\ &= [(\bar{m} + \bar{1}) + \bar{q}]\cdot[(\bar{m} + \bar{1}) + \bar{q}] \\ &= (\bar{m}' + \bar{q})(\bar{m}' + \bar{q}) \\ &= \bar{m}'\cdot\bar{m}' + A \text{ , for constant } A \\ &\geq \bar{m}'\cdot\bar{m}' .\end{aligned}$$

Hence $\bar{n}\cdot\bar{n} \not< \bar{m}'\cdot\bar{m}'$.

Thus in no case does there exist an $\bar{n}$ such that:

$$\bar{m}\cdot\bar{m} < \bar{n}\cdot\bar{n} < \bar{m}'\cdot\bar{m}' .$$

(b)(i) Suppose $\bar{k} = 0$. Then $\bar{p}\cdot\bar{p} = \bar{q}_o\cdot\bar{n}$.

Since $\bar{n} < \bar{q}_o$, for some $\bar{m} \neq 0$,

$$\bar{n} + \bar{m} = \bar{q}_o .$$

Hence $\bar{p}\cdot\bar{p} = (\bar{n} + \bar{m})\cdot\bar{n}$

$$= \bar{n}\cdot\bar{n} + \bar{m}\cdot\bar{n} \quad \text{by 4.17(d) .}$$

Thus, since $\bar{n}, \bar{m} \neq 0$, $\bar{n}\cdot\bar{n} < \bar{p}\cdot\bar{p}$.

Now suppose $\bar{k} \neq 0$. Then, by 4.19:

$$\bar{q}_o\cdot\bar{n} < \bar{p}\cdot\bar{p} .$$

Since $\bar{n} < \bar{q}_o$, $\bar{n}\cdot\bar{n} < \bar{q}_o\cdot\bar{n}$.

Hence, by 4.25 : $\bar{n}\cdot\bar{n} < \bar{p}\cdot\bar{p}$.

Thus in both cases $\bar{n}\cdot\bar{n} < \bar{p}\cdot\bar{p}$, and hence

$$\bar{n} < \bar{p} .$$

→

(ii) $\bar{p}\cdot\bar{p} = \bar{k} + \bar{q}_o\cdot\bar{n}$

$\bar{q}_o'\cdot\bar{n} = (\bar{q}_o + \bar{1})\cdot\bar{n}$

$= \bar{q}_o\cdot\bar{n} + \bar{n}$ by 4.17(d)

$\therefore \quad \bar{q}_o\cdot\bar{n} < \bar{q}_o'\cdot\bar{n}$

$\therefore \quad \bar{k} + \bar{q}_o\cdot\bar{n} < \bar{k} + \bar{q}_o'\cdot\bar{n}$

$\therefore \quad \bar{p}\cdot\bar{p} < \bar{k} + \bar{q}_o'\cdot\bar{n}$ (1) .

Also: $\bar{p}'\cdot\bar{p}' = (\bar{p} + \bar{1})(\bar{p} + \bar{1})$

$= \bar{p}\cdot\bar{p} + \bar{p}\cdot\bar{2} + \bar{1}$.

Since $\bar{n} < \bar{p}$, $\bar{n} < \bar{p}\cdot\bar{2} + \bar{1}$.

Hence $\bar{k} + \bar{q}_o'\cdot\bar{n} = \bar{k} + \bar{q}_o\cdot\bar{n} + \bar{n}$

$= \bar{p}\cdot\bar{p} + \bar{n}$

$< \bar{p}\cdot\bar{p} + \bar{p}\cdot\bar{2} + \bar{1}$

$= \bar{p}'\cdot\bar{p}'$ (2) .

So, by (1) and (2):

$\bar{p}\cdot\bar{p} < \bar{k} + \bar{q}_o'\cdot\bar{n} < \bar{p}'\cdot\bar{p}'$.

The eventual aim in this chapter is to prove the completeness of S_1 . To do so, it is necessary to establish one further property of the congruence relation. This is that, given any conjunction of congruences of the form

$$x\cdot\bar{k} \equiv \bar{m} \pmod{\bar{n}}$$

this conjunction can be "solved for x" , if it is not inconsistent.

A rigid proof of this property will involve establishing certain number-theoretical results which, apart from being used in the proof, make no essential contribution to the main trend of this essay. Consequently, the abovementioned property will be stated as a proposition, and the "proof" is to be regarded as an outline of a proof.

4.44 Proposition:

Any conjunction of congruences, each of the form

$$x \cdot \bar{k} \equiv \bar{m} \pmod{\bar{n}}$$

is either false (in which case this fact can be ascertained) or it can be written as a single congruence of the form

$$x \equiv \bar{p} \pmod{\bar{q}} .$$

Outline Proof:

Consider any congruence of the form

$$x \cdot \bar{k} \equiv \bar{m} \pmod{\bar{n}}.$$

By 4.39 , $\bar{m}$ may be assumed to be between 0 and $\overline{n-1}$.
Again by 4.39

$$x \equiv 0 \pmod{\bar{n}} \vee \cdots \vee x \equiv \overline{n-1} \pmod{\bar{n}} .$$

– say $x = \bar{i} + w \cdot \bar{n}$, for i between 0 and n - 1 .

From 4.31 it can be seen that for ease of expression it may be assumed that $w = 0$ – i.e. $x = \bar{i}$.

Now check which of the alternatives

$$\bar{i} \cdot \bar{k} \equiv \bar{m} \pmod{\bar{n}} \qquad i = 0 \cdots n-1$$

is true.

If none of these alternatives is true, then

$$x \cdot \bar{k} \equiv \bar{m} \pmod{\bar{n}}$$

is false. Hence the whole conjunction is false.

If, for some i between 0 and n - 1 ,

$$\bar{i} \cdot \bar{k} \equiv \bar{m} \pmod{\bar{n}}$$

is true, then $x \equiv \bar{i} \pmod{\bar{n}}$.

Thus, if the conjunction is true, each congruence

$$x \cdot \bar{k} \equiv \bar{m} \pmod{\bar{n}} \qquad (1)$$

can be reduced to a congruence

$$x \equiv \bar{i} \pmod{\bar{n}} \qquad (2)$$

so that the original conjunction of congruences of the form (1) has been reduced to a conjunction of congruences of the form (2).

Now consider any two congruences of the form (2) — say:

$$x \equiv \bar{p}_1 \pmod{\bar{n}_1}$$

and $$x \equiv \bar{p}_2 \pmod{\bar{n}_2} .$$

Then, for some w_1 and w_2 :

$$\bar{p}_1 + w_1 \cdot \bar{n}_1 = x = \bar{p}_2 + w_2 \cdot \bar{n}_2 .$$

If this equation is not satisfied for $x \leq \bar{n}_1 \cdot \bar{n}_2$, then the conjunction of the inequalities is false.

If it is satisfied, then for some $\bar{m}$,

$$x \equiv \bar{m} \pmod{\bar{n}_1 \cdot \bar{n}_2}$$

and this congruence then replaces the conjunction of the previous two. Hence the number of congruences has now been reduced by one, and by repeated application of this process it is either ascertained that the original conjunction of congruences was false, or only one congruence of the form

$$x \equiv \bar{p} \pmod{\bar{q}}$$

is left.

→

§ 2. A Reduction Procedure for S_1 †

A Reduction Procedure will now be described which transforms any closed wff $\mathfrak{B}$ of S_1 into another wff $\mathfrak{B}^*$ — called the reduction of $\mathfrak{B}$ — such that $\mathfrak{B}^*$ contains no bound variables,

---

† The procedure is due to M. Presburger, in [13]. The exposition in §2. follows that given in [6], pp. 361-366, for an axiom system given on p. 357.

and:

Condition R: $\vdash_{S_1} B \Leftrightarrow B^*$ is fulfilled.

What the reduction procedure achieves is not only to eliminate quantifiers and bound variables from a wff, but to do so without any change in the truth-value of that wff. The method of reduction is called the method P — after Presburger.

Consider any wff B of S_1. Since $(\forall x)B$ follows from B by Gen., and since B is true iff $(\forall x)B$ is true, B may be assumed to be a closed wff. Furthermore, by 2.5 B may be assumed to be in Prenex Normal form, say:

$$(Q_1 x_1)(Q_2 x_2)\cdots\cdots(Q_n x_n)A$$

where each Q_i, is either a universal or an existential quantifier, and A contains no quantifiers. A can now be transformed into disjunctive normal form. If $(Q_n x_n)$ is an existential quantifier $(\exists x_n)$, then the method P is applied to the wff $(\exists x_n)A$. If $(Q_n x_n)$ is a universal quantifier $(\forall x_n)$ then by definition $(\forall x_n)A$ can be replaced by $\sim(\exists x_n)\sim A$. The wff $\sim A$ is then restored to D.N.F., and the method P is applied to this wff. So, after one application of the method P, the quantifier $(Q_n x_n)$ as well as the bound variable x_n has been eliminated from B, and by repeated application of the method P eventually all quantifiers and bound variables are eliminated from P.

Thus it is sufficient to describe the method P for a wff of the form $(\exists x)A$.

The Method P.

Consider any wff B of S_1 which is of the form:

$$(\exists x)A(x)$$

and put A into D.N.F.

A: In the D.N.F., each disjunct is an unnegated conjunction of (negated or unnegated) equalities, inequalities and congruences.

Now replace:

An equality : $r = s$

by : $r < s' \wedge s < r'$,

using 4.34 ;

The negation of an equality : $r \neq s$

by : $r < s \vee s < r$

using 4.35 ;

The negation of an inequality : $r \not< s$

by : $s < r'$

using 4.36 ;

The negation of a congruence : $r \not\equiv s \pmod{\bar{k}}$

by a $(k-1)$- termed disjunction :

$r \equiv s + \bar{1} \pmod{\bar{k}} \vee \cdots\cdots \vee r \equiv s + (\overline{k-1}) \pmod{\bar{k}}$,

using 4.39 .

If the wff A is now no longer in D.N.F. it is restored to D.N.F. All equality signs and all negation signs have now been eliminated.

B: (i) Each expression containing the variable x which occurs on one side of an inequality or congruence is now reduced to one of the forms:

$$x \cdot \bar{k} + r$$

or $x \cdot \bar{k}$.

First the stroke-operation is eliminated, by expressing each term of the form:

$$\overbrace{s'\cdots'}^{m \text{ times}} \quad \text{as} \quad s + \bar{m} .$$

The sum of "k" x's is then expressed as $x \cdot \bar{k}$ and the sum of the remaining terms (if any) as a new term r.

(ii) Now replace:

An inequality of the form : $x \cdot \bar{k} + r < x \cdot \bar{k} + s$

by : $r < s$,

using 4.37 ;

And an inequality of the form : $x \cdot \bar{k} + r < x \cdot \bar{\ell} + s$

or : $x \cdot \bar{\ell} + r < x \cdot \bar{k} + s$

where $\bar{k} < \bar{\ell}$, and hence $\bar{\ell}$ is of the form $\bar{k} + \bar{n}$, for $\bar{n} \neq 0$,

by : $r < x \cdot \bar{n} + s$

or $x \cdot \bar{n} + r < s$,

using 4.37 again.

The same method can be employed for congruences, using 4.28. Each inequality and congruence now contains the variable x on most one side.

(iii) Now remove the term r from congruences of the form

$$x \cdot \bar{k} + r \equiv s \pmod{\bar{n}}$$

by replacing it by :

$$x \cdot \bar{k} \equiv s + r \cdot \bar{p} \pmod{\bar{n}}$$

using 4.32 $(\bar{p}' = \bar{n})$.

Since, by Convention 2, congruence is not defined if $\bar{n} = 0$, this is a legitimate replacement.

Only congruences of the form

$$x \cdot \bar{k} \equiv s \pmod{\bar{n}}$$

now occur in A .

Now replace each such congruence by the n-termed disjunction.

$$[s \equiv 0 \pmod{\bar{n}} \wedge x \cdot \bar{k} \equiv 0 \pmod{\bar{n}}]$$
$$\vee \quad .$$
$$\quad .$$
$$\quad .$$
$$\vee [s \equiv \overline{n-1} \pmod{\bar{n}} \wedge x \cdot \bar{k} \equiv \overline{n-1} \pmod{\bar{n}}] ,$$

using 4.27, 4.38 and 4.39.

The expression occurring on the right of each congruence is now a numeral.

(iv) Restore A to D.N.F. if necessary. Each disjunct is now a conjunction of expressions which either do not contain x, or has one of the following forms:

$$x \cdot \bar{p} + r < s$$

or $$r < x \cdot \bar{p} + s$$

or $$x \cdot \bar{p} \equiv \bar{k} \pmod{\bar{n}} .$$

C: (i) Consider a conjunction of congruences of the form:

$$x \cdot p \equiv \bar{k} \pmod{\bar{n}} .$$

By Proposition 4.44 there are two alternatives: either the conjunction is false, or it can be written as a single congruence.

If the conjunction is false, replace it by

$$0 < 0 .$$

If not, replace the conjunction by the congruence

$$x \equiv \bar{p} \pmod{\bar{q}} ,$$

the existence of which is shown by 4.44 .

(ii) Now consider a conjunction of inequalities of the form:

$$x \cdot \bar{n} + r < s .$$

Given any two such inequalities : $x \cdot \bar{n}_1 + r_1 < s_1$

$$x \cdot \bar{n}_2 + r_2 < s_2$$

they can be expressed in the forms:

$$x \cdot \bar{n}_1 \cdot \bar{n}_2 + (r_1 \cdot \bar{n}_2 + r_2 \cdot \bar{n}_1) < s_1 \cdot \bar{n}_2 + s_2 \cdot \bar{n}_1$$

$$x \cdot \bar{n}_1 \cdot \bar{n}_2 + (r_1 \cdot \bar{n}_2 + r_2 \cdot \bar{n}_1) < s_2 \cdot \bar{n}_1 + s_1 \cdot \bar{n}_2$$

by using 4.19, 4.17, 4.14 and 4.13 .

Thus the number of inequalities of the form $x \cdot \bar{n} + r < s$ which have different terms $\bar{n}$ and r has been reduced by one, and by repeated application of this process eventually all these inequalities will have the same terms $\bar{n}$ and r .

What is left is a conjunction of inequalities:

$$x\cdot\bar{n} + r < s_1 \wedge x\cdot\bar{n} + r < s_2 \wedge \cdots \wedge x\cdot\bar{n} + r < s_\upsilon$$

Such a conjunction can now be replaced by a υ-termed disjunction ; in which the i-th disjunct is :

$$(s_i < s_1 + \bar{1}) \wedge (s_i < s_2 + \bar{1}) \wedge \cdots\cdots$$
$$\cdots\cdots \wedge (s_i < s_\upsilon + \bar{1}) \wedge (x\cdot\bar{n} + r < s_\upsilon) .$$

The replacement is valid, since the disjunct in which the smallest s_i occurs will be valid. The reason for this replacement will soon become apparent.

A process similar to the one above is applicable to a conjunction of inequalities of the form

$$s < x\cdot\bar{n} + r .$$

(iii) Restore A to D.N.F. (if necessary). In each disjunct variable x now appears in at most three conjuncts — it was to ensure this state of affairs that the conjunction of inequalities was replaced by a disjunction.

So, in each disjunct, the variable x appears in at most one congruence, which is of the form

$$x \equiv \bar{p} \pmod{\bar{q}} ,$$

in at most one inequality of the form

$$x\cdot\bar{n} + r < s$$

and in at most one inequality of the form

$$t < x\cdot\bar{n} + r .$$

Note that if the two inequalities have different terms $\bar{n}$ and $\bar{r}$, these can be made to be the same by means of the process described above.

D: (i) By applying the rule

$$(\exists x)[B(x) \vee C(x)] \Leftrightarrow (\exists x)B(x) \vee (\exists x)C(x)$$

the quantifier $(\exists x)$ is now distributed over the D.N.F. of the wff A as transformed by A , B and C .

Since, in each disjunct, the variable x occurs in at most three conjuncts (which may be assumed to occur next to each other) the rule

$$(\exists x)[Q \wedge B(x)] \Leftrightarrow Q \wedge (\exists x)B(x)$$

allows the quantifier to be written in front of the conjunction of the three expressions in which x occurs.

Hence it is only necessary to describe a method for eliminating the variable x from expressions of the form

$$C : (\exists x)[(x \equiv \bar{k} \pmod{\bar{n}}) \wedge (t < x\cdot\bar{p} + r) \wedge (x\cdot\bar{p} + r < s)]$$

where one or more of the conjuncts may be lacking.

(ii) If the inequality : $x\cdot\bar{p} + r < s$
is lacking, then the other inequality is replaced by the conjunction:

$$(0 < x\cdot\bar{p} + r') \wedge (x\cdot\bar{p} + r' < s')$$

ng 4.3, 4.2 and 4.5.

If the inequality : $x\cdot\bar{p} + r < s$
is lacking, the entire expression C is replaces by :

$$0 < \bar{1} .$$

This is a valid replacement, since the absence of an upper bound on $x\cdot\bar{p} + r$ ensures that an x satisfying the other two conditions can always be found.

If the congruence is lacking, there are two possibilities :

$$\bar{p} = \bar{1} \quad \text{or} \quad \bar{p} > \bar{1} .$$

If $\bar{p} = \bar{1}$, then replace :

$$(\exists x)[t < x + r) \wedge (x + r < s)]$$

by : $(t' < s) \wedge (r < s)$.

If $\bar{p} > \bar{1}$, then replace :

$$(\exists x)[(t < x\cdot\bar{p} + r) \wedge (x\cdot\bar{p} + r < s)]$$

by : $(\exists x)[(x \equiv 0 \pmod{\bar{p}}) \wedge (t < x + r) \wedge (x + r < s)]$

so that a congruence is now no longer lacking — then proceed to (iii) .

(iii) If none of the conjuncts are lacking in C, proceed as follows.

First make $\bar{p}$ equal to $\bar{l}$ (if necessary), by replacing C with:

$$(\exists x)[x \equiv \bar{k}\cdot\bar{p} \pmod{\bar{n}\cdot\bar{p}}) \wedge (t < x + r) \wedge (x + r < s)]$$

using Proposition 4.41.

Hence C has now been transformed into the form:

$$(\exists x)[(x \equiv \bar{m} \pmod{\bar{n}}) \wedge (t < x + r) \wedge (x + r < s)] .$$

Now replace this wff by the D.N.F. :

$$[(t < r) \wedge (r + \bar{m} < s)] \vee D_1 \quad \ldots\ldots \vee D_n ,$$

where D_k is shorthand for :

$$(r < t') \wedge (t + \bar{k} < s) \wedge (t + \bar{k} \equiv r + \bar{m} \pmod{\bar{n}})$$

using Proposition 4.42.

(iv) Restore A to D.N.F. . The quantifier $(\exists x)$ and the bound variable x has now been eliminated from B, and the new wff which has been obtained is B^*, the reduction of B.

Now note that Condition R for the reduction procedure is fulfilled — i.e.

$$\vdash_{S_1} B \Leftrightarrow B^* .$$

This follows from the fact that in the given exposition of the method P, each replacement of a wff by another wff has been justified by the appropriate theorem or proposition.

Furthermore, since the method P is applied to closed wffs, and eliminates all the bound variables, it follows that the reduction of a wff is built up only with numerals as terms, and does not (or at least need not) contain any free variables. The process can be completed by eliminating all remaining instances of the two functions of S_1 — i.e. all terms:

$(\bar{k})^{\overbrace{'''\ldots'}^{\text{m times}}}$ is written as $\bar{k} + \bar{m}$ and all sums $\bar{k} + \bar{m}$ is then written as the single appropriate numeral.

Eventually only instances of the two relations defined by 4.18 and 4.19 are left — i.e. only expressions of the forms

$$\bar{k} < \bar{\ell}$$

and / or $\bar{m} \equiv \bar{n} \pmod{\bar{p}}$.

The truth or falsehood of such expressions can be determined, and thus it follows that the truth or falsehood of the reduction A^* of any wff A of S_1 can be determined. Hence, finally, since a wff and its reduction are equivalent in truth-value, it follows that the truth or falsehood of any wff of S_1 can effectively be determined.

§ 3. Properties of the First Order Theory S_1

4.45 Proposition:

S_1 is complete.

Proof:*

Consider any wff A of S_1, and find its reduction A^*. A^* is a D.N.F., and for each conjunct "p" it can be determined whether p is true or false.

If "p" is true, replace it by : $p \Rightarrow p$ and
if "p" is false, replace it by : $\sim(p \Rightarrow p)$.

The result of this is either an instance of a tautology, or an instance of a contradiction.

Hence if A^* is true, it can be written as an instance of a tautology, and if A^* is false, then $\sim A^*$ can be written as an instance of a tautology.

So, by 2.1, either A^* or $\sim A^*$ is provable:

$$\vdash_{S_1} A^* \quad \text{or} \quad \vdash_{S_1} \sim A^* .$$

---

* A similar proof can be found in [10], p. 95, for an axiom system given on p. 78.

Then, by Condition R it follows that either A or $\sim A$ is provable:

$$\vdash_{S_1} A \quad \text{or} \quad \vdash_{S_1} \sim A \ .$$

Hence S_1 is complete.

It still remains to redeem the promise made on p.30 to justify definition 4.18. As has been pointed out, 4.18 does not, strictly speaking, form part of S_1 although it has been treated as though it does. The reason for this is the following.

Firstly, it is evident that, for any specific numeral $\bar{n}$, the congruence relation can in fact be defined within S_1, as for example:

$$t \equiv s \ (\mathrm{mod}\ \bar{5}) \overset{\text{def}}{\Leftrightarrow} (\exists w)[t = s + w + w + w + w + w \vee s = t + w + w + w + w + w] \ .$$

For each such definition, all those theorems relating to the congruence relation can be proved. Thus 4.18 is in fact a definition-schema, (just as S_1^6 is an axiom-schema), and similarly each theorem proved from 4.18 is a schema generating analogous theorems for different values of $\bar{n}$.
Secondly, the argument leading up to the independence proof for S_1 is essentially a meta-argument. In this argument the congruence relation was extensively used to simplify matters by dealing with equivalence classes rather than individual numerals (as the equality relation would have done).
Thus it can be seen that treating 4.18 as a proper definition of S_1 was not only harmless (in that a definition schema rather than a definition proper was used) but it had the distinct advantage of simplifying the argument leading up to the independence proof for S_1.

The next result to be established is that S_1 is also a consistent first-order theory – i.e. for any wff A, not both A and $\sim A$ are provable. If S_1 is inconsistent, (say

both A and ~A are provable) then by the tautology

$$(A \wedge \sim A) \Rightarrow B$$

any wff of S_1 will be provable — i.e. all wff's of S_1 will be theorems. Thus to establish that S_1 is consistent it is sufficient to exhibit a wff of S_1 which is not provable. If, furthermore, it can be proved that every theorem of S_1 is <u>true</u> in the standard interpretation (i.e. numbers for numerals, etc.), then it will only be necessary to exhibit a wff of S_1 which is false under the standard interpretation, for this wff will then not be provable.

The set of all denumerable sequences of elements of the standard interpretation — i.e. the set of all denumerable sequences of natural numbers — will for the rest of this chapter simply be referred to as Σ.

4.46 <u>Proposition</u>:

The axioms of S_1 are true under the standard interpretation.

<u>Proof</u>:

To prove that an axiom is true, it must be shown that any sequence s in Σ satisfies that axiom.

So, let s be an arbitrary sequence in Σ — say:

$$s = (k_1, k_2, k_3, \ldots\ldots) .$$

$$S_1^1 : x_1 = x_2 \Rightarrow (x_1 = x_3 \Rightarrow x_2 = x_3) .$$

For this axiom, S, the mapping determined by the sequence s, is as follows:

$$S(x_1) = k_1 \quad S(x_2) = k_2 \quad S(x_3) = k_3 .$$

By definition 3.1, s satisfies S_1^1 iff:

(a) either s does not satisfy $x_1 = x_2$, or

(b) s satisfies $x_1 = x_3 \Rightarrow x_2 = x_3$.

(a): s does not satisfy $x_1 = x_2$ iff $S(x_1) \neq S(x_2)$ – i.e. $k_1 \neq k_2$.

(b): s satisfies $x_1 = x_3 \Rightarrow x_2 = x_3$ iff either

(i) s does not satisfy $x_1 = x_3$, in which case $k_1 \neq k_3$, or

(ii) s satisfies $x_2 = x_3$, in which case $k_2 = k_3$.

Now for the natural numbers it can be determined by the method sketched in Chapter 3, § 2. , that:

either (1) $k_1 = k_2 = k_3$

or (2) $k_1 \neq k_2$, $k_2 \neq k_3$ and $k_3 \neq k_1$

(3) $k_1 = k_2 \neq k_3$

or (4) $k_1 = k_3 \neq k_2$

or (5) $k_2 = k_3 \neq k_1$.

If (1) holds, then by (b)(ii), s satisfies $x_2 = x_3$, so that s satisfies $x_1 = x_3 \Rightarrow x_2 = x_3$, and hence s satisfies S_1^1 .

If (2) holds, then by (a) s does not satisfy $x_1 = x_2$, and hence s satisfies S_1^1 .

If (3) holds, then by (b)(i) s does not satisfy $x_1 = x_3$, hence s satisfies $x_1 = x_3 \Rightarrow x_2 = x_3$, hence s satisfies S_1^1 .

If (4) holds, then, as in (2), s satisfies S_1^1 .

If (5) holds, then, as in (3), s satisfies S_1^1 .

Hence in all cases s satisfies S_1^1 , and thus, since s was arbitrary, S_1^1 is true. $\longrightarrow$

The truth of axioms S_1^2 - S_1^5 can be established in the same way. $\longrightarrow$

The situation is somewhat different, however, with the axiom schema.

S_1^6 : $A(0) \Rightarrow [(\forall x_i)[A(x_i) \Rightarrow A(x_i')] \Rightarrow (\forall x_i)A(x_i)]$.

Again let s be an arbitrary sequence — say

$$s = (k_1, k_2 \cdots k_i \cdots\cdots) .$$

Then $S(x_i) = k_i$.

We note the following:
The expression $A(x_i)$ above is used to indicate that the variable x_i occurs free in the wff A . (It may be assumed that all other variables occurring in A are bound.) Thus, as has been explained in § 1. of Chapter 3, $A(x_i)$ may be neither true, nor false, but <u>contingent</u>. That is, $A(x_i)$ may be satisfied by some sequences, but not by others. Whether a sequence satisfies $A(x_i)$ or not, depends on the value of the i-th component of the sequence. Suppose every sequence with "n" as its i-th component satisfies $A(x_i)$. Then $A(n)$, the wff obtained by replacing each occurrence of "x_i" in A by "n" is true. Conversely, if $A(n)$ is true, then every sequence with "n" as its i-th component will satisfy $A(x_i)$.

The proof that S_1^6 is true is as follows:

The sequence s satisfies S_1^6 iff:

either s does not satisfy $A(0)$, or s satisfies

$$(\forall x_i)[A(x_i) \Rightarrow A(x_i')] \Rightarrow (\forall x_i)A(x_i).$$

$A(0)$, not containing any free variables, is either true or false. If $A(0)$ is false, then no sequence satisfies it, consequently s does not satisfy it, and hence s satisfies S_1^6. So in this case there is nothing more to prove.

So suppose $A(0)$ is true.

Then it must be proved that s also satisfies

$$(\forall x_i)[A(x_i) \Rightarrow A(x_i')] \Rightarrow (\forall x_i)A(x_i).$$

Now s satisfies $(\forall x_i)[A(x_i) \Rightarrow A(x_i')] \Rightarrow (\forall x_i)A(x_i)$ iff:

either s does not satisfy $(\forall x_i)[A(x_i) \Rightarrow A(x_i')]$ or s satisfies $(\forall x_i)A(x_i)$.

If s does not satisfy $(\forall x_i)[A(x_i) \Rightarrow A(x_i')]$ then there is nothing more to prove. So suppose that it does. Then it remains to be proved that s also satisfies $(\forall x_i)A(x_i)$.

Since s satisfies $(\forall x_i)[A(x_i) \Rightarrow A(x_i')]$, every sequence differing from s in at most the i-th component satisfies:

$$A(x_i) \Rightarrow A(x_i').$$

But $A(x_i) \Rightarrow A(x_i')$ is satisfied iff:

either $A(x_i)$ is not satisfied, or $A(x_i')$ is satisfied (by the same sequence).

Now consider that sequence differing from s only in its i-th component, which is 0. Since $A(0)$ is true, by the

remarks above this sequence satisfies $A(x_i)$.

But then, in order to satisfy

$$A(x_i) \Rightarrow A(x_i')$$

(as it must), this sequence must also satisfy $A(x_i')$.

But $S(x_i') = S(x_i) + 1 = 0 + 1 = 1$.

Consequently that sequence with 1 as its i-th component satisfies $A(x_i)$. In general, then, if a sequence with "n" as its i-th component satisfies $A(x_i)$ then, in order to satisfy

$$A(x_i) \Rightarrow A(x_i')$$

(as it must) it must also satisfy $A(x_i')$, so that the same sequence, but now with $n+1$ as its i-th component, then also satisfies $A(x_i)$.

Hence each sequence differing from s in at most its i-th component satisfies $A(x_i)$ and thus s satisfies $(\forall x_i)A(x_i)$.

This was all that remained to be proven, consequently S_1^6 is true.

This establishes the truth of the proper axioms of S_1. It is easily verified that the logical axioms of S_1 are also true under the standard interpretation. Thus all axioms of S_1 are true.

4.47 Proposition:

The property of Truth is preserved by the rules of inference of S_1.

Proof:

(a) Consider any wff's A and B such that A and $A \Rightarrow B$ are true.

Then, given any arbitrary sequence s in Σ, s satisfies A, and s satisfies $A \Rightarrow B$.

Now s satisfies $A \Rightarrow B$ iff:
either s does not satisfy A, or s satisfies B.

Since, by hypotheses, s does satisfy A, s must also satisfy B.

Hence, since s was arbitrary, B is true.

(b) Consider any wff A which is true.

Since A is true, every sequence in Σ satisfies A.

Let s be an arbitrary sequence in Σ.

Then every sequence differing from s in at most the i-th component satisfies A.

Thus s satisfies $(\forall x_i)A$, and hence, since s was was arbitrary, $(\forall x_i)A$ is true.

→

4.48 Proposition:

The set of theorems of S_1 coincides with the set of wff's of S_1 which are true under the standard interpretation.

Proof:

Since the theorems of S_1 follow from the axioms by means of the rules of inference, it follows from 4.46 and 4.47 that each theorem of S_1 is true under the standard interpretation.

Now consider any wff A of S_1 which is true under the standard interpretation.

Since A is true, $\sim A$ is false. Hence $\sim A$ is not provable in S_1.

But, by 4.45, S_1 is complete. Hence A is provable — i.e. A is a theorem of S_1. $\longrightarrow$

4.49 Proposition:

S_1 is consistent

Proof:

By the remarks on p. 62 and 63; S_1 is consistent iff there is some wff of S_1 which is not provable.

Now: $0 \neq 0$ is a wff of S_1.

But $0 \neq 0$ is false.

Hence, by 4.48, $0 \neq 0$ is not provable.

S_1 is consistent. $\longrightarrow$

4.50 Proposition:

S_1 is decidable.

Proof:

The reduction procedure described in § 2. provides an effective method for deciding whether a given wff A is true or not. By 4.48, this is also an effective method for deciding whether A is a theorem of S_1 or not. Hence S_1 is decidable. $\longrightarrow$

4.51 Proposition:*

The multiplication function is not representable in S_1.

---

* An outline of the proof can be found in [6], pp. 369 - 370.

Proof:

First note the following:
The multiplication function can recursively be defined in S_1 as follows:

$$t \cdot 0 = 0$$
$$t \cdot (r+1) = t \cdot r + r \ .$$

However, it follows from the remarks on p. 20, Chapter 3, § 2., that this recursive definition cannot be reduced to an explicit definition, since the multiplication function (which is to be removed) is essential in the method of reducing recursive to explicit definitions.

It remains to prove that the multiplication function cannot satisfy the definition (3.1, p.19) of representability.

So, suppose multiplication is representable in S_1 by the wff:

$$A(x_1, x_2, x_3) \ .$$

This wff can be chosen in such a way that only x_1, x_2 and x_3 occur in it as free variables, and a certain variable x_4 does not occur in it.

Since multiplication is representable (by assumption), for any natural number k_1 it is the case that:

If $k_1 \cdot k_1 = k_2$, then $\vdash_{S_1} A(\bar{k}_1, \bar{k}_1, \bar{k}_2)$.

By 4.48, this implication can be strengthened to an equivalence:

(1) $k_1 \cdot k_1 = k_2$ iff $\vdash_{S_1} A(\bar{k}_1, \bar{k}_1, \bar{k}_2)$.

Consequently, since S_1 is complete:

(2) $k_1 \cdot k_1 \neq k_2$ iff $\vdash_{S_1} \sim A(\bar{k}_1, \bar{k}_1, \bar{k}_2)$.

Now consider the wff:

B: $(\exists x_4) A(x_4, x_4, x_1)$ containing x_1 as its only free variable.

By the method P, this wff can be reduced to a D.N.F. in which each disjunct is a conjunction of expressions having one of the forms:

$$x_1 \equiv \bar{k} \pmod{\bar{n}}$$

or : $\bar{m} < x_1$

or : $x_1 < \bar{p}$.

Two alternatives are distinguished:

(a) An expression of the form $x_1 < \bar{p}$ occurs in each disjunct of the D.N.F.

This D.N.F. is then false whenever x_1 is replaced by a numeral bigger than $\bar{p}$.

Now replace x_1 by the numeral $\overline{p \cdot p}$.

The D.N.F. is then false, and so, by condition R (p.54), the wff B is also false for this replacement. Hence its negation is true.

So, by 4.48:

$$\vdash_{S_1} \sim(\exists x_4)A(x_4, x_4, \overline{p \cdot p})$$

– i.e. $$\vdash_{S_1} (\forall x_4)\sim A(x_4, x_4, \overline{p \cdot p})$$

and so, by 2.3 :

$$\vdash_{S_1} \sim A(\bar{p}, \bar{p}, \overline{p \cdot p}) .$$

But then, by condition (2) above:

$$p \cdot p \neq p \cdot p$$

which is a contradiction.

(b) At least one disjunct of the D.N.F. contains only expressions of the form:

$$x_1 \equiv \bar{k} \pmod{\bar{n}}$$

and : $\bar{m} < x_1$.

The D.N.F. is then true whenever x_1 is replaced by a numeral bigger than $\bar{m}$ and congruent mod $\bar{n}$ to $\bar{k}$.

By 4.39 it may be assumed that:

$$\bar{k} < \bar{n} \qquad (1) .$$

Now let $\bar{q}_o$ be a numeral such that:

$$\bar{m} < \bar{q}_o \qquad (2)$$

$$\bar{n} < \bar{q}_o \qquad (3) ,$$

and put

$$\bar{q} = \bar{k} + \bar{q}_o \cdot \bar{n} \qquad (4) .$$

Now suppose that there is some numeral $\bar{p}$ such that:

$$\bar{p} \cdot \bar{p} = \bar{q}$$

— i.e., from (4): $\bar{p} \cdot \bar{p} = \bar{k} + \bar{q}_o \cdot \bar{n}$.

Then, by (1), (3), Convention 2 and proposition 4.43(b), it follows that:

$$\bar{n} < \bar{p}$$

and: $$\bar{p} \cdot \bar{p} < \bar{k} + \bar{q}_o' \cdot \bar{n} < \bar{p}' \cdot \bar{p}' .$$

But, by 4.43(a), $\bar{k} + \bar{q}_o' \cdot \bar{n}$ cannot be expressed as a product of the form $\bar{n} \cdot \bar{n}$. i.e. for any natural number n:

$$n \cdot n \neq k + q_o' \cdot n .$$

So, by (2): $\vdash_{S_1} \sim A(\bar{n}, \bar{n}, \bar{k} + \bar{q}_o' \cdot \bar{n})$

Hence, by Gen.: $\vdash_{S_1} (\forall x_4) \sim A(x_4, x_4, \bar{k} + \bar{q}_o' \cdot \bar{n})$

and thus: $\vdash_{S_1} \sim (\exists x_4) A(x_4, x_4, \bar{k} + \bar{q}_o' \cdot \bar{n}) \qquad (5) .$

But now, from (4) it can be seen that $\bar{q} \equiv \bar{k} \pmod{\bar{n}}$.

Consequently $\bar{k} + \bar{q}_o' \cdot \bar{n}$ is also congruent to $\bar{k}$ mod $\bar{n}$.

Furthermore, since $\bar{m} < \bar{q}_o$ by (2),

$$\bar{m} < \bar{k} + \bar{q}_o' \cdot \bar{n} .$$

So by the remark above, the D.N.F. will be true if x_1 is replaced by $\bar{k} + \bar{q}_o' \cdot \bar{n}$. Thus, by condition R, so is the wff B, and hence, by 4.48:

$$\vdash_{S_1} (\exists x_4) A(x_4, x_4, \bar{k} + \bar{q}_o' \cdot \bar{n}) \qquad (6).$$

(5) and (6) now consitute a contradiction. $\longrightarrow$

From (a) and (b) it now follows that, from the assumption that multiplication is representable in S_1, a contradiction can always be derived. Hence the multiplication-function is not representable in S_1. $\longrightarrow$

§

CHAPTER V

A FULL* FORMALIZATION OF ARITHMETIC

§ 1. The First-Order Theory S

In Chapter 4 it has been proved that that subsystem of Arithmetic which only employs the operation of addition is, as a first-order theory, consistent, complete, and decidable. It is, however, not a full formalization of arithmetic, since multiplication is not representable in it. Nevertheless, a full formalization can be obtained from S_1.

Let S be the first-order theory which, besides having all symbols and axioms of S_1, also has:

the function letter f_2^2, where $f_2^2(x,y)$ is abbreviated as $x \cdot y$,

and the proper axioms:

S^7 $\quad x_1 \cdot 0 = 0$

S^8 $\quad x_1 \cdot (x_2') = (x_1 \cdot x_2) + x_1$.

The definition of terms is accordingly adjusted by adding:

If t and s are terms, then $t \cdot s$ is a term,

and the further development of S then proceeds analogously to that of S_1.**

---

* A formalization will be said to be "full" if it can take the whole set of natural numbers as the domain of its interpretation; addition, multiplication and exponentiation are representable within it, and the class of functions recursively definable in it coincides with the class of functions representable in it.

** See [10], Chapter 3. S is the first-order theory referred to in the footnote on p. 21.

For present purposes the following remarks will suffice.

Firstly, it can be shown that:

The zero function : $z(x) = 0$;
The successor function : $N(x) = x + 1$;
The projection function : $U_i^n(x_1,\cdots,x_i,\cdots,x_n) = x_i$;

are all representable within S . Then, using these as initial functions, other functions can be recursively defined in S — for example, the exponentiation function :

$$x^0 = 1$$
$$x^{y+1} = x^y \cdot x \ .$$

Furthermore, it can be shown that the class of functions recursively definable in S is identical with the class of functions which are representable in S . It follows that S is indeed a full formalization of Arithmetic.

Gödel, in [5], proved that any full formalization of Arithmetic is incomplete, hence S is incomplete.* Thus the complete first-order theory S_1 is transformed into an incomplete first-order theory S by the introduction of the two axioms S^7 and S^8 , which govern the use of multiplication. In retrospect, it is therefore not surprising that the multiplication function was not representable in S_1 .

§ 2. A Conjecture concerning Multiplication

An informal "multiplication" proceeding on the schema:

$\underline{\alpha}$ $$k \times n = \underbrace{k + k + \cdots + k}_{n \text{ times}}$$

was used in S_1 , and this schema was formalized in S .

---

* The construction of an undecidable sentence in S is carried out in [10], pp. 135 - 144.

The schema

β $\qquad k \times n = \underbrace{n + n + \cdots + n}_{k \text{ times}}$

could obviously have been used with equal effect in S_1. In S β is derivable from α, since S allows a proof that multiplication is commutative.*

In S_1, the "product" $\bar{n} \cdot 0$ was excluded by the use of α. Hence, combining α and β into informal "multiplication" excludes the product $0 \cdot 0$. In S, however, $0 \cdot 0$ is a term, and hence part of the system. Furthermore, whereas for non-zero n (in α) and k (in β) both $n \times k$ and $k \times n$ denote operations "carried out within the domain of concrete inspection",** $0 \cdot 0$ does not — it is not finitary. Also, α in S_1 allowed a reduction procedure for S_1, as would β, [illegible] been used instead.

These remarks lead to the following conjecture : ***

> For a first-order theory combining the schemas α and β, but excluding the produc[illegible] $\cdot 0$, a reduction procedure similar to that used in S_1 can be found.

§

---

* [10], p. 104.

** See the definition of "finitary", p. 18.

*** For a refutation of this conjecture, see Ch. 6 § 2.

CHAPTER VI

MULTIPLICATION WITHOUT THE PRODUCT 0·0

§ 1. The First-Order Theory SS

The symbols of SS are the same as those of S_1, except for two additional function letters:

$f_2^2(x,y)$: abbreviated as $x \times_L y$

$f_3^2(x,y)$: abbreviated as $x \times_R y$.

The definition of terms is accordingly modified, and atomic formulae, wff's and the further logical symbols are defined as usual.

The proper axioms of SS are:

SS^1 $\quad x_1 = x_2 \Rightarrow (x_1 = x_3 \Rightarrow x_2 = x_3)$

SS^2 $\quad (x_1 = x_2) \Leftrightarrow (x_1' = x_2')$

SS^3 $\quad 0 \neq x_1'$

SS^4 $\quad x_1 + 0 = x_1$

SS^5 $\quad x_1 + x_2' = (x_1 + x_2)'$

SS^6 $\quad 0' \times_L x_2 = x_2$

SS^7 $\quad x_1'' \times_L x_2 = (x_1' \times_L x_2) + x_2$

SS^8 $\quad x_1 \times_R 0' = x_1$

SS^9 $\quad x_1 \times_R x_2'' = (x_1 \times_R x_2') + x_1$

SS^{10} For any wff A of SS :

$A(0) \Rightarrow [(\forall x)[A(x) \Rightarrow A(x')] \Rightarrow (\forall x)A(x)]$.

The intended interpretation of SS is the Natural Numbers with addition and multiplication, excluding the product $0 \cdot 0$. As in S_1, the function letter f_1^1 generate the numerals

$$\bar{1},\ \bar{2},\ \bar{3},\ \bar{4}\ \ldots\ldots\ldots\ldots \text{etc.}$$

from 0. The function letter f_2^2 is a formalization of multiplication, where the multiplier is on the left and the multiplicand on the right of the multiplication sign:

$\bar{k} \times_L \bar{n}$ is the formal counterpart of the schema:

$$\underbrace{n + n + \ldots\ldots + n}_{k \text{ times}} .$$

From Axioms SS^6 and SS^7 it follows that $\bar{k} \neq 0$. Thus $0 \times_L t$ is not defined in SS. However, if $t \neq 0$, then $t \times_L 0$ is defined in SS. — i.e. $t' \times_L 0$ is defined for any term t.

Similarly, $\bar{k} \times_R \bar{n}$ is the formal counterpart of the schema:

$$\underbrace{k + k + \ldots\ldots + k}_{n \text{ times}} .$$

$t \times_R 0$ is not defined in SS, but $0 \times_R t'$ is defined for any term t.

Since all axioms of S_1 are also axioms of SS, it is obvious that every theorem of S_1 is also a theorem of SS. These theorems will not be derived again in SS, but, wherever they are required in a proof of a theorem of SS, they will be referred to by the numbers indicating their positions in S_1 — i.e. 4.12, 4.21, etc.

Some theorems of SS will now be derived, the aim being to show how the multiplication formalized in SS^6 — SS^9 corresponds to "ordinary" multiplication, as (e.g.) defined by the

axioms S^7 and S^8 of the first-order theory S .

For obvious reasons the two kinds of multiplication are referred to as "multiplication from the left" (SS^6, SS^7) and "multiplication from the right" (SS^8, SS^9) resepectively.

Firstly, note that since

$$\bar{k} \times_L \bar{n} = \underbrace{\bar{n} + \bar{n} + \ldots + \bar{n}}_{k \text{ times}}$$

and $$\bar{n} \times_R \bar{k} = \underbrace{\bar{n} + \bar{n} + \ldots + \bar{n}}_{k \text{ times}}$$

it should be provable in SS that

$$\bar{k} \times_L \bar{n} = \bar{n} \times_R \bar{k} ,$$

wherever both these expressions are defined

6.1 $\quad \vdash t' \times_R r' = r' \times_L t' .$

Proof: By induction on y in:

$$A(y) : x' \times_R y' = y' \times_L x' .$$

(i)	1.	$x' \times_R 0' = x'$	SS^8
	2.	$0' \times_L x' = x'$	SS^6
	3.	$x' \times_R 0' = 0' \times_L x'$	1,2, 4.9

Hence $\vdash A(0)$.

(ii)	1.	$x' \times_R y' = y' \times_L x'$	Hyp.
	2.	$x' \times_R y'' = (x' \times_R y') + x'$	SS^9
	3.	$(x' \times_R y') + x' = (y' \times_L x') + x'$	1, 4.10
	4.	$x' \times_R y'' = (y' \times_L x') + x'$	2,3, 4.8
	5.	$(y' \times_L x') + x' = y'' \times_L x'$	SS^7

6. $x' \times_R y'' = y'' \times_L x'$ 4,5, 4.8

7. $(x' \times_R y' = y' \times_L x') \Rightarrow (x' \times_R y'' = y'' \times_L x')$ 1-6, 2.2

Hence $\vdash A(y) \Rightarrow A(y')$

and by Gen. : $\vdash (\forall y)[A(y) \Rightarrow A(y')]$.

So, by (i), (ii) and the Induction Rule :

$$\vdash (\forall y)A(y) \ ,$$

and then, by Gen. and 2.3 :

$$\vdash t' \times_R r' = r' \times_L t' \ .$$

Furthermore, multiplication (both kinds) by 0 (wherever permitted) is always 0 , and multiplication by $\bar{1}$ leaves the multiplicand unaltered.

6.2 $$\vdash 0 \times_R t' = 0 \ .$$

Proof: By induction on $A(x) : 0 \times_R x' = 0$, using SS^9, 4.10, 4.8 and 4.11 .

6.3 $$\vdash t' \times_L 0 = 0 \ .$$

Proof: Similar to 6.2 .

6.4 $$\vdash \bar{1} \times_R t' = t' \ .$$

Proof: By induction on $A(x) : \bar{1} \times_R x' = x'$, using 4.10, 4.8 and 4.22 .

6.5 $$\vdash t' \times_L \bar{1} = t' \ .$$

Proof: Similar to 6.4 .

Already a pattern is beginning to emerge from these theorems. Whatever is proved for multiplication from the left is also,

in appropriate form, proved for multiplication from the right.

By SS^9, $(\bar{k} + \bar{l}) \times_R (\bar{n} + \bar{l})$ is defined as

$$(\bar{k} + \bar{l}) \times_R \bar{n} + (\bar{k} + \bar{l}) .$$

It turns out, however, that this is in fact equivalent to:

$$\bar{k} \times_R (\bar{n} + \bar{l}) + (\bar{n} + \bar{l}) .$$

6.6 $$\vdash t' \times_R r' = (t \times_R r') + r' .$$

Proof: By induction on

$$A(y) : x' \times_R y' = (x \times_R y') + y' .$$

(i)	1.	$x' \times_R 0' = x'$	SS^8
	2.	$x \times_R 0' = x$	SS^8
	3.	$(x \times_R 0') + 0' = x + 0'$	2, 4.10
	4.	$x + 0' = x'$	4.22
	5.	$(x \times_R 0') + 0' = x'$	3,4, 4.8
	6.	$x' \times_R 0' = (x \times_R 0') + 0'$	1,5, 4.9

Hence $\vdash A(0)$.

(ii)	1.	$x' \times_R y' = (x \times_R y') + y'$	Hyp.
	2.	$x' \times_R y'' = (x' \times_R y') + x'$	SS^9
	3.	$(x' \times_R y') + x' = (x \times_R y') + y' + x'$	1, 4.10
	4.	$x' \times_R y'' = (x \times_R y') + y' + x'$	2,3, 4.8
	5.	$(x \times_R y') + y' + x' = (x \times_R y') + y' + (x + 0')$	4.22
	6.	$x' \times_R y'' = (x \times_R y') + y' + (x + 0')$	4,5, 4.8

7. $(x \times_R y') + y' + (x + 0') = (x \times_R y') + (y' + 0') + x$ 4.13, 4.15

8. $(x' \times_R y'') = (x \times_R y') + (y' + 0') + x$ 6,7, 4.8

9. $(x \times_R y') + (y' + 0') + x = (x \times_R y') + y'' + x$ 4.22

10. $x' \times_R y'' = (x \times_R y') + y'' + x$ 8,9, 4.8

11. $(x \times_R y') + y'' + x = (x \times_R y') + x + y''$ 4.13

12. $x' \times_R y'' = (x \times_R y') + x + y''$ 10,11, 4.8

13. $(x \times_R y') + x + y'' = (x \times_R y'') + y''$ SS^9, 4.12

14. $x' \times_R y'' = (x \times_R y'') + y''$ 12,13, 4.8

15. $[x' \times_R y' = (x \times_R y') + y']$
$[x' \times_R y'' = (x \times_R y'') + y'']$ 1-14, 2.2

Hence $\vdash A(y) \Rightarrow A(y')$.

Then, by Gen. : $\vdash (\forall y)[A(y) \Rightarrow A(y')]$.

And so, by (i), (ii) and the Induction Rule

$$\vdash (\forall y) A(y) .$$

Hence, by Gen. and 2.3

$$\vdash t' \times_R r' = (t \times_R r') + r' .$$ →

6.7 $$\vdash t' \times_L r' = (t' \times_L r) + t' .$$

Proof: Similar to 6.6 . →

Theorems 6.4 and 6.6 now allow a proof that, whenever multiplication from the left and multiplication from the right are

simultaneously defined, they are in fact equivalent. (Alternatively, the function letters f_2^2 and f_3^2 are interchangeable whenever both are applicable.)

6.8 $\quad \vdash t' \times_R r' = t' \times_L r' .$

Proof: By induction on $A(x) : x' \times_R y' = x' \times_L y' .$

(i)	1.	$0' \times_R y' = y'$	6.4
	2.	$0' \times_L y' = y'$	SS^6
	3.	$0' \times_R y' = 0' \times_L y'$	1,2, 4.9

Hence $\vdash A(0) .$

(ii)	1.	$x' \times_R y' = x' \times_L y'$	Hyp.
	2.	$x'' \times_R y' = (x' \times_R y') + y'$	6.6
	3.	$(x' \times_R y') + y' = (x' \times_L y') + y'$	1, 4.10
	4.	$x'' \times_R y' = (x' \times_L y') + y'$	2,3, 4.8
	5.	$(x' \times_L y') + y' = x'' \times_L y'$	SS^7
	6.	$x'' \times_R y' = x'' \times_L y'$	4,5, 4.8
	7.	$(x' \times_R y' = x' \times_L y') \Rightarrow (x'' \times_R y' = x'' \times_L y')$	1-6, 2.2

Hence $\vdash A(y) \Rightarrow A(y')$

So, first by Gen. , then by (i), (ii) and the Induction Rule,

$$\vdash (\forall y) A(y) .$$

The conclusion then follows by Gen. and 2.3 . $\longrightarrow$

Furthermore, it is now also possible to prove that both multiplication from the right and from the left are in fact commutative.

6.9 $\vdash t' \times_R r' = r' \times_R t'$.

Proof:

1.	$t' \times_R r' = r' \times_L t'$	6.1
2.	$r' \times_L t' = r' \times_R t'$	6.8
3.	$t' \times_R r' = r' \times_R t'$	1,2, 4.8

6.10 $\vdash t' \times_L r' = r' \times_L t'$.

Proof:

1.	$t' \times_L r' = r' \times_R t'$	6.1
2.	$r' \times_R t' = r' \times_L t'$	6.8
3.	$t' \times_L r' = r' \times_L t'$	1,2, 4.8

It can also be proved that both multiplication from the right and multiplication from the left are associative and distributive. Thus it can be seen that each of the two forms of multiplication correspond very closely to "ordinary" multiplication — the only difference being that a firm distinction is made between multiplier and multiplicand, and that the multiplier is never allowed to be zero. This prompts a definition of a new function letter f_4^2 representing a combination of f_2^2 and f_3^2. $f_4^2(t,r)$ will be abbreviated as $t \cdot r$.

6.11 Definition:

$$0 \cdot t' \overset{\text{def}}{=} 0 \times_R t' \quad (= 0)$$

$$t' \cdot 0 \overset{\text{def}}{=} t' \times_L 0 \quad (= 0)$$

$$t' \cdot r' \overset{\text{def}}{=} t' \times_R r' \quad (= t' \times_L r') \ .$$

It can be seen from this definition that the product $0 \cdot 0$ is not defined, and that this is the only case where a product

between two terms is not defined. Consequently SS is a close approximation of the system S of Chapter 5, § 1.

6.12 Definition: Order Relation :

$$t < s \overset{\text{def}}{\Leftrightarrow} (\exists w)[w \neq 0 \wedge t + w = s] .$$

6.13 Definition: Congruence Relation :

$$t \simeq s \pmod{r} \overset{\text{def}}{\Leftrightarrow} (\exists w)[t = s + w \cdot r \vee s = t + w \cdot r] .$$

The following theorems are easily proved:

6.14 $t = r \Leftrightarrow t \cdot s = r \cdot s$.

6.15 $t \cdot (r \cdot s) = (t \cdot r) \cdot s$.

6.16 $t \cdot (r + s) = t \cdot r + t \cdot s$.

6.17 $s \neq 0 \Rightarrow [t < t \cdot s \vee t = t \cdot s]$.

For the next theorem a new logical symbol is necessary:

$$(\exists! x)A(x) \overset{\text{def}}{\Leftrightarrow} (\exists x)A(x) \wedge (\forall x)(\forall y)[(A(x) \wedge A(y)) \Rightarrow x = y] .$$

Thus $(\exists! x)A(x)$ means that there is one and only one x such that $A(x)$.

6.14 $\vdash s \neq 0 \Rightarrow (\exists! y)(\exists! z)[t = s \cdot y + z \wedge z < s]$.

Proof:

(a) Existence Proof by induction on u in

$A(u) : x \neq 0 \Rightarrow (\exists y)(\exists z)[u = x \cdot y + z \wedge z < x]$.

(i)	1.	$x \neq 0$	Hyp.
	2.	$0 = x \cdot 0 + 0$	6.11, SS^4
	3.	$0 < x$	1, SS^4, 6.12
	4.	$0 = x \cdot 0 + 0 \wedge 0 < x$	2,3 Taut.
	5.	$(\exists z)[0 = x \cdot 0 + z \wedge z < x]$	4, 2.4

	6.	$(\exists y)(\exists z)[0 = x \cdot y + z \ \wedge \ z < x]$	5, 2.4
	7.	$x \neq 0 \Rightarrow (\exists y)(\exists z)[0 = x \cdot y + z \ \wedge \ z < x]$	1-6, 2.2

Hence $\vdash A(0)$.

(ii)	1.	$x \neq 0 \Rightarrow (\exists y)(\exists z)[u = x \cdot y + z \ \wedge \ z < x]$	Hyp.
	2.	$x \neq 0$	Hyp.
	3.	$(\exists y)(\exists z)[u = x \cdot y + z \ \wedge \ z < x]$	1,2, M.P.
	4.	$(\exists z)[u = x \cdot \bar{n} + z \ \wedge \ z < x]$	3, Rule C
	5.	$u = x \cdot \bar{n} + \bar{k} \ \wedge \ \bar{k} < x$	4, Rule C
	6.	$u = x \cdot \bar{n} + \bar{k}$	5 Taut.
	7.	$\bar{k} < x$	5 Taut.
	8.	$(\exists w)[w \neq 0 \ \wedge \ \bar{k} + w = x]$	7, 6.12
	9.	$\bar{m} \neq 0 \ \wedge \ \bar{k} + \bar{m} = x$	8, Rule C
	10.	$\bar{m} \neq 0$	9 Taut.
	11.	$\bar{m} = \bar{1} \ \vee \ \bar{1} < \bar{m}$	10, 4.30
	12.	$\bar{1} < \bar{m}$	Hyp.
	13.	$(\exists w)[w \neq 0 \ \wedge \ \bar{1} + w = \bar{m}]$	12, 6.12
	14.	$\bar{p} \neq 0 \ \wedge \ \bar{1} + \bar{p} = \bar{m}$	13, Rule C
	15.	$\bar{1} + \bar{p} = \bar{m}$	14 Taut.
	16.	$\bar{k} + \bar{1} + \bar{p} = \bar{k} + \bar{m}$	15, 4.15
	17.	$\bar{k} + \bar{m} = x$	9 Taut.
	18.	$\bar{k} + \bar{1} + \bar{p} = x$	16,17, 4.8
	19.	$\bar{p} \neq 0$	14 Taut.
	20.	$\bar{p} \neq 0 \ \wedge \ \bar{k} + \bar{1} + \bar{p} = x$	18,19 Taut.
	21.	$(\exists w)[w \neq 0 \ \wedge \ \bar{k} + \bar{1} + w = x]$	20, 2.4
	22.	$\bar{k} + \bar{1} < x$	21, 6.12
	23.	$u + \bar{1} = x \cdot \bar{n} + \bar{k} + \bar{1}$	6, 4.10
	24.	$u' = u + \bar{1}$	4.22
	25.	$u' = x \cdot \bar{n} + \bar{k} + \bar{1}$	24,23, 4.8
	26.	$u' = x \cdot \bar{n} + \bar{k} + \bar{1} \ \wedge \ \bar{k} + \bar{1} < x$	22,25 Taut.
	27.	$(\exists z)[u' = x \cdot \bar{n} + z \ \wedge \ z < x]$	26, 2.4
	28.	$(\exists y)(\exists z)[u' = x \cdot y + z \ \wedge \ z < x]$	27, 2.4
	29.	$\bar{1} < \bar{m} \Rightarrow (\exists y)(\exists z)[u' = x \cdot y + z \ \wedge \ z < x]$	12-28, 2.2

30.	$\bar{m} = \bar{l}$	Hyp.
31.	$\bar{k} + \bar{m} = \bar{k} + \bar{l}$	30, 4.10
32.	$\bar{k} + \bar{m} = x$	9 Taut.
33.	$\bar{k} + \bar{l} = x$	31,32, SS^1
34.	$u + \bar{l} = x \cdot \bar{n} + \bar{k} + \bar{l}$	6, 4.10
35.	$x \cdot \bar{n} + \bar{k} + \bar{l} = x \cdot \bar{n} + x$	33, 4.10
36.	$u' = x \cdot \bar{n} + x$	34,35, 4.8
37.	$x \cdot \bar{n} + x = x \cdot (\bar{n} + \bar{l})$	6.16
38.	$u' = x \cdot (\bar{n} + \bar{l}) + 0$	36,37, SS^4
39.	$0 < x$	SS^4, 6.12
40.	$(\exists z)[u' = x \cdot (\bar{n} + \bar{l}) + z \wedge z < x]$	38,39, 2.4
41.	$(\exists y)(\exists z)[u' = x \cdot y + z \wedge z < x]$	40, 2.4
42.	$\bar{m} = \bar{l} \Rightarrow (\exists y)(\exists z)[u' = x \cdot y + z \wedge z < x]$	30-41, 2.2
43.	$(\bar{m} = \bar{l} \vee \bar{l} < \bar{m}) \Rightarrow (\exists y)(\exists z)[u' = x \cdot y + z \wedge z < x]$	29,42 Taut.
44.	$(\exists y)(\exists z)[u' = x \cdot y + z \wedge z < x]$	11,43, M.P.
45.	$x \neq 0 \Rightarrow (\exists y)(\exists z)[u' = x \cdot y + z \wedge z < x]$	2-44, 2.2
46.	$[x \neq 0 \Rightarrow (\exists y)(\exists z)[u = x \cdot y + z \wedge z < x]] \Rightarrow [x \neq 0 \Rightarrow (\exists y)(\exists z)[u' = x \cdot y + z \wedge z < x]]$	1-45, 2.2

Hence $\vdash A(u) \Rightarrow A(u')$.

So, by Gen. : $\vdash (\forall u)[A(u) \Rightarrow A(u')]$, then, by (i), (ii) and the Induction Rule

$$\vdash (\forall u) A(u) .$$

Hence, by Gen. and 2.3, the conclusion follows. $\longrightarrow$

(b) Uniqueness

1.	$x \neq 0$	Hyp.
2.	$[u = x \cdot y_1 + z_1 \wedge z_1 < x] \wedge [u = x \cdot y_2 + z_2 \wedge z_2 < x]$	Hyp.
3.	$u = x \cdot y_1 + z_1 \wedge z_1 < x$	2 Taut.

4.	$u = x \cdot y_1 + z_1$	3 Taut.
5.	$u = x \cdot y_2 + z_2 \wedge z_2 < x$	2 Taut.
6.	$u = x \cdot y_2 + z_2$	5 Taut.
7.	$z_1 < x$	3 Taut.
8.	$z_2 < x$	5 Taut.
9.	$x \cdot y_1 + z_1 = x \cdot y_2 + z_2$	4,6, 4.1
10.	$y_1 < y_2$	Hyp.
11.	$(\exists w)[w \neq 0 \wedge y_1 + w = y_2]$	10, 6.12
12.	$\bar{k} \neq 0 \wedge y_1 + \bar{k} = y_2$	11, Rule C
13.	$\bar{k} \neq 0$	12 Taut.
14.	$y_1 + \bar{k} = y_2$	12 Taut.
15.	$x \cdot (y_1 + \bar{k}) = x \cdot y_2$	14, 6.14
16.	$x \cdot y_1 + x \cdot \bar{k} = x \cdot y_2$	15, 6.16
17.	$x \cdot y_1 + x \cdot \bar{k} + z_2 = x \cdot y_2 + z_2$	16, 4.10
18.	$x \cdot y_1 + z_1 = x \cdot y_1 + x \cdot \bar{k} + z_2$	9,17, 4.9
19.	$z_1 = x \cdot \bar{k} + z_2$	18, 4.21
20.	$\bar{k} \neq 0 \Rightarrow (x < x \cdot \bar{k} \vee x = x \cdot \bar{k})$	6.17
21.	$x < x \cdot \bar{k} \vee x = x \cdot \bar{k}$	13,20, M.P.
22.	$x = x \cdot \bar{k}$	Hyp.
23.	$x \cdot \bar{k} + z_2 = x + z_2$	22, 4.10
24.	$z_1 = x + z_2$	19,23, 4.8
25.	$z_2 = 0 \vee 0 < z_2$	Taut.
26.	$z_1 = x \vee x < z_1$	24,25
27.	$(z_1 = x \vee x < z_1) \Rightarrow z_1 \not< x$	4.30 Taut.
28.	$z_1 \not< x$	26,27, M.P.
29.	$z_1 \not< x \vee y_1 \not< y_2$	28 Taut.
30.	$y_1 \not< y_2$	7,29 Taut.

31. $y_1 < y_2 \Rightarrow y_1 \not< y_2$ — 10-30, 2.2

32. $y_1 \not< y_2 \vee y_1 \not< y_2$ — 31 Taut.

33. $y_1 \not< y_2$ — 32 Taut.

34. $y_2 \not< y_1$ — Remark below

35. $y_1 \not< y_2 \wedge y_2 \not< y_1$ — 33,34 Taut.

36. $\sim(y_1 < y_2 \vee y_2 < y_1)$ — 35 Taut.

37. $y_1 = y_2$ — 36, 4.30

38. $x \cdot y_1 = x \cdot y_2$ — 37, 6.14

39. $z_1 = z_2$ — 9,38, 4.21

40. $y_1 = y_2 \wedge z_1 = z_2$ — 37,39 Taut.

41. $[u = x \cdot y_1 + z_1 \wedge z_1 < x] \wedge [u = x \cdot y_2 + z_2 \wedge z_2 < x] \Rightarrow [y_1 = y_2 \wedge z_1 = z_2]$ — 2-40, 2.2

42. $(\forall y_1)(\forall y_2)(\forall z_1)(\forall z_2)[[(u = x \cdot y_1 + z_1 \wedge z_1 < x) \wedge (u = x \cdot y_2 + z_2 \wedge z_2 < x)] \Rightarrow [y_1 = y_2 \wedge z_1 = z_2]]$ — 41, Gen.

43. $x \neq 0 \Rightarrow (\forall y_1)(\forall y_2)(\forall z_1)(\forall z_2)[[(u = x \cdot y_1 + z_1 \wedge z_1 < x) \wedge (u = x \cdot y_2 + z_2 \wedge z_2 < x)] \Rightarrow [y_1 = y_2 \wedge z_1 = z_2]]$ — 1-42, 2.2

The conclusion now follows from (a), (b) and the definition of the quantifier $(\exists!x)$.

Remark:

The proof of 35 above is exactly similar to that carried out in 10-34 .

§ 2. An Impossibility Proof concerning a Reduction Procedure for SS

6.15 Definition: A Reduction Procedure for a first-order theory K is an effective procedure whereby any wff A of K may be transformed into a wff A* of K containing no bound variables or quantifiers, such that

Condition R: $\vdash_K A \Leftrightarrow A^*$ is fulfilled. →

What is required of a reduction procedure is that it must allow the systematic removal of bound variables from a wff without changing the truth-value of that wff. In eliminating a particular variable, it must therefore give necessary and sufficient conditions on the other (remaining) terms and variables in the wff, such that these conditions exactly determine the range of values of the variable to be eliminated. Since it is required that the reduction must be an effective procedure, additional bound variables may be introduced only if it can be shown that:

1) The process of introducing new variables must eventually stop.
2) The new variables in turn can be eliminated.

If SS is inconsistent, then every wff of SS is a theorem of SS, regardless of whether it is true or false. In this case, for every two wffs A and A*,

$$\vdash_{SS} A \Leftrightarrow A^* .$$

Thus, if SS is inconsistent, it will have a reduction procedure.

A consistency proof for SS similar to 4.49 (for S_1) is not immediately possible, since it is not known whether SS is complete or not. It is easily shown that all theorems of SS are true under the normal interpretation, hence SS has a

model, and so is consistent.* Nevertheless, this argument was not used for S_1, and will not be used here. The consistency of SS will be taken as an assumption.**

In searching for a reduction procedure applicable to SS, it is natural to keep in mind the method P described for S_1 — since S_1 is, after all, a subsystem of SS. It turns out that the method P, however, is not applicable to SS. In B(ii) on p. 56, for example, it was possible to eliminate the variable x from one side of an inequality

$$x \cdot \bar{k} + r < x \cdot \bar{\ell} + s \ .$$

This was possible because the terms $\bar{k}$ and $\bar{\ell}$ were particular numerals, so that the shorthand forms $x \cdot \bar{k}$ and $x \cdot \bar{\ell}$ could be written out in full. Using 4.10 and 4.21 to provide necessary and sufficient conditions, all the x's on one side could then be "cancelled" — which side depends on whether $\bar{k} < \bar{\ell}$, $\bar{\ell} < \bar{k}$ or $\bar{k} = \bar{\ell}$.

The situation is different, however, in SS, where inequalities such as

$$y + z \cdot x < u + v \cdot x$$

occur — the terms z and v now being variables. The trichotomy

$$z < v \ \vee \ z = v \ \vee \ v < z$$

still holds, but here it cannot be determined which of these possibilities is in fact the case. Furthermore, even if it can be determined that (say) $z < v$, it still needs to be determined which numeral $\bar{k}$ satisfies the equation $z + \bar{k} = v$.

---

* A First-Order theory is consistent iff it has a model. See [2], p.102.

** For S this is common practice. See [10], p. 107 .

Necessary and sufficient conditions for removing the variable x from one side of this inequality can be given, however, by introducing new variables. In fact:

$$
\begin{aligned}
& y + z \cdot x < u + v \cdot x \quad \Longleftrightarrow \\
& \Big[[y = u \wedge z < v] \\
& \vee [(\exists w_1)[w_1 \neq 0 \wedge u + w_1 = y \wedge \\
& \quad \{(w_1 < x \wedge z < v) \vee (w_1 = x \wedge z + \bar{1} < v) \vee \\
& \quad (x < w_1 \wedge (\exists^{!} w_2)(\exists^{!} w_3)[w_1 = w_2 \cdot x + w_3 \wedge \\
& \quad w_3 < x \wedge z + w_2 < v])\}]] \\
& \vee [(\exists w_1)[w_1 \neq 0 \wedge y + w_1 = u \wedge \\
& \quad \{(w_1 < x \wedge z < v + \bar{1}) \vee (w_1 = x \wedge z = v + \bar{1}) \vee \\
& \quad (x < w_1 \wedge (\exists^{!} w_2)(\exists^{!} w_3)[w_1 = w_2 \cdot x + w_3 \wedge \\
& \quad w_3 < x \wedge z < w_2 + v + \bar{1}])\}]] \Big] .
\end{aligned}
$$

(A proof of this is tedious but not difficult. It depends mainly on 4.30 and 6.14.)
However this equivalence cannot form an essential part of a reduction procedure for SS, since it introduces new variables without an upper bound on their range, so that the process of introducing new variables may not stop. — thereby violating condition (2) above.

6.16 Proposition: If SS is consistent, then there is no reduction procedure for SS.

Proof:

First note that if SS does have a reduction procedure, then SS is complete. (This can be shown by a proof similar to 4.45.) Consequently:

$\underline{\alpha}$: If SS is incomplete, it does not have a reduction procedure.

Now suppose that SS is complete. By reasoning analogous to that of 4.48, it then follows that the true wff's in SS coincide with the theorems of SS . Suppose further that there is a reduction procedure — say P — for SS .
Consider the wff:

$$(\exists w)[x_1 + x_2 \cdot w < x_3 + x_4 \cdot w] \ .$$

Since this is a wff of SS , and since by assumption there is a reduction procedure for SS , there must be a wff $A(x_1, x_2, x_3, x_4)$ of SS containing x_1, x_2, x_3 and x_4 as free variables, such that

(1) $\vdash_{SS} (\exists w)[x_1 + x_2 \cdot w < x_3 + x_4 \cdot w] \Leftrightarrow A(x_1, x_2, x_3, x_4)$

The wff A can be chosen in such a way that it does not contain a certain variable x_5 .

Now consider the wff:

(2) $(\exists x_5)A(x_1, x_5, x_5, x_5)$.

This wff contains x_5 as a bound variable and x_1 as its only free variable. By the reduction procedure P the bound variable x_5 can now be eliminated, and the reduction of the wff (2) can then be put into D.N.F., where each disjunct is a conjunction of terms of the form:

$$x_1 \simeq \bar{k} \pmod{\bar{n}}$$

or $\bar{m} < x_1$

or $x_1 < \bar{p}$.

Two alternatives are distinquished:

a) An expression of the form $x_1 < \bar{p}$ occurs in each disjunct of the D.N.F.

In this case the D.N.F. is false when x_1 is replaced by a numeral bigger than $\bar{p}$ — say $\overline{p+1}$. The negation of the D.N.F. is then true for this replacement, and so, by the conditions on a reduction procedure, the negation of the wff (2) is then also true for this replacement. Since SS is complete (by assumption) this wff is then provable, so that

$$\vdash_{SS} \sim(\exists x_s)A[\overline{p+1}, x_s, x_s, x_s] .$$

$$\therefore \quad (\forall x_s) \sim A[\overline{p+1}, x_s, x_s, x_s] .$$

$$\therefore \quad \sim A[\overline{p+1}, \overline{p+2}, \overline{p+2}, \overline{p+2}] \qquad \text{by 2.3}$$

$$\therefore \quad \sim(\exists w)[\overline{p+1} + \overline{p+2}\cdot w < \overline{p+2} + \overline{p+2}\cdot w] \qquad \text{by (1)}$$

$$\therefore \quad (\forall w)[\overline{p+1} + \overline{p+2}\cdot w \not< \overline{p+2} + \overline{p+2}\cdot w]$$

$$\therefore \quad \overline{p+1} + \overline{p+2}\cdot\bar{q} \not< \overline{p+2} + \overline{p+2}\cdot\bar{q} \qquad \text{by 2.3}$$

$$\therefore \quad \overline{p+1} \not< \overline{p+2}$$

$$\therefore \quad \bar{1} \not< \bar{2} .$$

Consequently: $\vdash_{SS} \bar{1} \not< \bar{2}$.

Since, however, 4.24 is a theorem of SS, it follows that

$$\vdash_{SS} \bar{1} < \bar{2} .$$

This contradicts the consistency of SS.

b) At least one disjunct of the D.N.F. contains only expressions of the form:

$$x_1 \simeq \bar{k} \pmod{\bar{n}}$$

$$\bar{m} < x_1 .$$

The D.N.F. is then false whenever x_1 is replaced by a numeral less than or equal to $\bar{m}$ — say $\bar{m}$ itself. Hence the negation

of the D.N.F. is true for this replacement, hence the negation of the wff (2) is true for this replacement, and hence provable.

Therefore:

$$\vdash_{SS} \sim(\exists x_5)A[\bar{m}, x_5, x_5, x_5]$$

$$\therefore \quad (\forall x_5) \sim A[\bar{m}, x_5, x_5, x_5]$$

$$\therefore \quad \sim A[\bar{m}, \overline{m+1}, \overline{m+1}, \overline{m+1}] \qquad \text{by 2.3}$$

$$\therefore \quad \sim(\exists w)[\bar{m} + \overline{m+1}\cdot w < \overline{m+1} + \overline{m+1}\cdot w] \qquad \text{by (1)}$$

$$\therefore \quad (\forall w)[\bar{m} + \overline{m+1}\cdot w \not< \overline{m+1} + \overline{m+1}\cdot w]$$

$$\therefore \quad \bar{m} + \overline{m+1}\cdot\bar{q} \not< \overline{m+1} + \overline{m+1}\cdot\bar{q} \qquad \text{by 2.3}$$

$$\therefore \quad \bar{m} \not< \overline{m+1}$$

$$\therefore \quad 0 \not< \bar{1}$$

which again contradicts the consistency of SS . ⟶

Thus, from the assumption that there is a reduction procedure for SS , a contradiction can always be derived. This conclusion is subject to the prior assumption that SS is complete. Hence:

β: If SS is complete, it does not have a reduction procedure.

From α and β it now follows that there is no reduction procedure for SS . ⟶

Theorem 6.16 achieves a double purpose. Firstly, it refutes a conjecture made in Ch. 5 § 2. Secondly, since SS is a subsystem of S , it shows that there is no reduction procedure for S , under the assumption that S is consistent.
(The latter result is of course not surprising, since if there were a reduction procedure for S , it could have been proved to be complete by a proof similar to 4.45 – contradicting Gödel's result.)

§

CHAPTER VII

ARITHMETIC ON A SUBSET OF THE NATURAL NUMBERS

§ 1. The First-Order Theory S_2

The symbols of S_2 are as follows:

The logical symbols, auxilary symbols, individual variables and predicate letters are as for S_1 .

As in S_1 , S_2 has two function letters, f_1^1 and f_1^2 .

$f_1^1(x)$ is to be written as x^*

$f_1^2(x,y)$ is to be written as $x \cdot y$.

As in S_1 , S_2 has one individual constant: Δ .

Terms:

1) Individual variables are terms
   Δ is a term .
2) If t and s are terms, then:
   t^* is a term
   $t \cdot s$ is a term .
3) An expression is a term only if it can be shown to be a term on the basis of (1) and (2).

Atomic Formulae, wff's and the further logical symbols are defined as usual.

Proper Axioms:

$S_2^1 \quad x_1 = x_2 \Rightarrow (x_1 = x_3 \Rightarrow x_2 = x_3)$

$S_2^2 \quad x_1 = x_2 \Leftrightarrow x_1^* = x_2^*$

S_2^3 $\Delta \neq x_1^*$

S_2^4 $x_1 \cdot \Delta = x_1$

S_2^5 $x_1 \cdot x_2^* = (x_1 \cdot x_2)^*$

S_2^6 For any wff A of S_2:

$$A(\Delta) \Rightarrow [(\forall x)[A(x) \Rightarrow A(x^*)] \Rightarrow (\forall x)A(x)] .$$

The induction rule is obtained as in S_1, and again special symbols are introduced for the terms

$$\Delta \quad \Delta^* \quad \Delta^{**} \quad \Delta^{***} \quad \text{.....etc.}$$

These terms are henceforward denoted by

$$\bar{1} \quad \bar{2} \quad \bar{4} \quad \bar{8} \quad \text{.....etc.},$$

called numerals again.

The axioms of S_2 are precisely the same as those of S_1, except that different symbols are used for the function letters and individual constant. In fact, S_1 and S_2 can be regarded as the same first-order theory. A different interpretation is intended for S_2, however, hence S_2 is presented as a distinct first-order theory.

The intended interpretation of S_2 is a subset of the Natural Numbers, namely those which are of the form 2^n, where "n" is any Natural Number. Thus the domain of the interpretation is the set:

$$\{1, 2, 4, 8, \ldots\} .$$

Unlike S_1, in S_2 there is no general shorthand method for writing the application of f_1^2 a number of times to some term t. This follows from the following facts:

Whereas in S_1 f_1^1 was interpreted as addition of 1, in S_2 f_1^1 is interpreted as multiplication by 2. Thus, in

S_2 only the numerals corresponding to powers of 2 are generated. Since these are available,

$t \cdot t$ can be abbreviated as $t^{\bar{2}}$,

$((t \cdot t) \cdot t) \cdot t$ " " " " " " $t^{\bar{4}}$

etc. ,

but $(t \cdot t) \cdot t$, $(((t \cdot t) \cdot t) \cdot t) \cdot t$, etc. cannot be so abbreviated, since the appropriate numerals do not occur in S_2 .

Convention 1: Any term t may be written as $t^{\bar{1}}$ (t^{Δ}) whenever required.

This differs from S_1 , where $t \cdot 0$ was not defined.

As in S_1 , the following theorems are immediate consequences of the axioms:

7.1 $\quad \vdash t = r \Rightarrow (t = s \Rightarrow r = s)$

7.2 $\quad \vdash t = r \Leftrightarrow (t^* = r^*)$

7.3 $\quad \vdash \Delta \neq t^*$

7.4 $\quad \vdash t \cdot \Delta = t$

7.5 $\quad \vdash (t \cdot r^*) = (t \cdot r)^*$

For the sake of brevity, the result of applying f_1^1 "n" times to a term t :

$$\overbrace{t^{**\ldots*}}^{\text{n times}}$$

may henceforward be written as $t^{(n)}$ <u>in meta-results</u> , whenever convenient. Thus, in meta-results, Δ may be written as $\Delta^{(0)}$.

In the meta-language, not only is the multiplication-operation available, but also addition and subtraction. Thus, in meta-results, expressions such as

$$\overline{n + 1}$$

are legitimate — this expression indicating the numeral corresponding to the successor of the natural number "n".

Similarly

$$\overline{n - 1}$$

indicates the numeral corresponding to the predecessor of the natural number "n" .

Note further that:

$$\bar{2} = \Delta^* = \Delta^{(1)}$$

$$\bar{4} = \Delta^{**} = \Delta^{(2)}$$

$$\bar{8} = \Delta^{***} = \Delta^{(3)}$$

$$\vdots$$

$$\text{etc.},$$

so that, in general:

$$\overline{(2^n)} = \Delta^{\overbrace{*\ldots*}^{n \text{ times}}} = \Delta^{(n)} .$$

The following theorems are easily proved — as in S_1 .

7.6 $\quad \vdash t = t$

7.7 $\quad \vdash t = r \Rightarrow r = t$

7.8 $\quad \vdash t = r \Rightarrow (r = s \Rightarrow t = s)$

7.9 $\quad \vdash r = t \Rightarrow (s = t \Rightarrow r = s)$.

The following theorems also correspond to their counterparts in S_1 — as an example, 7.10 is proved.

7.10 $\quad \vdash t = r \Rightarrow t \cdot s = r \cdot s$.

Proof:

Let $A(z)$ be : $x = y \Rightarrow (x \cdot z = y \cdot z)$.

(i)	1.	$x \cdot \Delta = x$	7.4
	2.	$y \cdot \Delta = y$	7.4
	3.	$x = y$	Hyp.
	4.	$x \cdot \Delta = y$	1,3, 7.8
	5.	$x \cdot \Delta = y \cdot \Delta$	4,2, 7.9
	6.	$x = y \Rightarrow x \cdot \Delta = y \cdot \Delta$	1-5, 2.2

Hence $\quad \vdash A(\Delta)$.

(ii) 1.	$x = y \Rightarrow (x \cdot z = y \cdot z)$		Hyp.
2.	$x = y$		Hyp.
3.	$x \cdot z^* = (x \cdot z)^*$		7.5
4.	$y \cdot z^* = (y \cdot z)^*$		7.5
5.	$x \cdot z = y \cdot z$		1,2, M.P.
6.	$(x \cdot z)^* = (y \cdot z)^*$		5, 7.2
7.	$x \cdot z^* = (y \cdot z)^*$		3,6, 7.8
8.	$x \cdot z^* = y \cdot z^*$		7,4, 7.9
9.	$x = y \Rightarrow (x \cdot z^* = y \cdot z^*)$		2-8, 2.2
10.	$[x = y \Rightarrow (x \cdot z = y \cdot z)] \Rightarrow$		
		$[x = y \Rightarrow (x \cdot z^* = y \cdot z^*)]$	1-9, 2.2

Hence $\vdash A(z) \Rightarrow A(z^*)$

Hence $\vdash (\forall z)A(z)$ by the induction rule, and thus by Gen. and 2.3 :

$$t = r \Rightarrow t \cdot s = r \cdot s \ .$$

Similarly 7.11 – 7.15 are proved (corresponding to 4.11 – 4.15 in S_1) .

As for S_1 , the following result can now be proved:

7.16 Proposition:

S_2 is a first-order theory with equality.

7.17 Proposition:

For any natural numbers m and n of the forms 2^k and 2^p respectively:

a) If $m \neq n$, then $\vdash \bar{m} \neq \bar{n}$

b) $\vdash \overline{m \cdot n} = \bar{m} \cdot \bar{n}$

c) $\vdash t^{\bar{m}} \cdot t^{\bar{n}} = t^{(\bar{m}+\bar{n})}$

d) $\vdash t^{\bar{n}} \cdot r^{\bar{n}} = (t \cdot r)^{\bar{n}}$

e) $\vdash t = r \Rightarrow t^{\bar{n}} = r^{\bar{n}}$.

Proof:

(a) Suppose $m \neq n$

$\therefore \quad 2^k \neq 2^p$

$\therefore \quad k \neq p$ — say $k < p$.

Now suppose $\bar{m} = \bar{n}$ — i.e. $\Delta^{(k)} = \Delta^{(p)}$

7.2, in the form $t^* = r^* \Rightarrow t = r$, applied k times in a row then yields:

$$\Delta = \Delta^{(p-k)} \qquad (1)$$

Since $p > k$, $p - k > 0$

$\therefore \quad p - k - 1 \geq 0$.

Let $t = \Delta^{(p-k-1)}$.

Then, from (1): $\Delta = t^*$, contradicting 7.3 .

Then, by the tautology $[A \Rightarrow (B \wedge \sim B)] \Rightarrow \sim A$ and the fact that any instance of a tautology is a theorem:

$$\vdash \bar{m} \neq \bar{n} \ .$$

(b) Induction on p in the metalanguage

$\overline{m \cdot 2^0} = \overline{m \cdot 1} = \bar{m} = \bar{m} \cdot \Delta$, by 7.4 .

Suppose $\vdash \overline{m \cdot n} = \bar{m} \cdot \bar{n}$

$\therefore \quad \vdash \overline{2^k \cdot 2^p} = \overline{2^k} \cdot \overline{2^p}$

$\therefore \quad \vdash \Delta^{(k+p)} = \left(\Delta^{(k)}\right) \cdot \left(\Delta^{(p)}\right)$

$\therefore \quad \vdash \left(\Delta^{(k+p)}\right)^* = \left(\left(\Delta^{(k)}\right)\left(\Delta^{(p)}\right)\right)^*$ by 7.2

$\therefore \quad \vdash \Delta^{((k+p)+1)} = \left(\Delta^{(k)}\right)\left(\Delta^{(p)}\right)^*$ by 7.5

$\therefore \quad \vdash \Delta^{(k+(p+1))} = \left(\Delta^{(k)}\right)\left(\Delta^{(p+1)}\right)$

$\therefore \quad \vdash \overline{2^k \cdot 2^{p+1}} = \overline{2^k} \cdot \overline{2^{p+1}}$

$$\therefore \quad \vdash \overline{2^k \cdot 2^p \cdot 2} = \overline{2^k} \cdot \overline{2^p \cdot 2}$$

$$\therefore \quad \vdash \overline{m \cdot n \cdot 2} = \bar{m} \cdot \overline{n \cdot 2} \ .$$

So, by induction, the result holds for all p, and hence for any numerals $\bar{m}$ and $\bar{n}$ of S_2.

(c) By induction in the metalanguage on "n" — as in S_1.

(d) As in S_1.

(e) As in S_1. ⟶

7.18 Definition:

$$t \approx s \pmod{\bar{k}} \overset{\text{def}}{\Leftrightarrow} (\exists w)[t = s \cdot w^{\bar{k}} \vee s = t \cdot w^{\bar{k}}]$$

7.19 Definition:

$$t \prec s \overset{\text{def}}{\Leftrightarrow} (\exists w)[w \neq \Delta \wedge t \cdot w = s] \ .$$

There is one further dissimilarity between S_1 and S_2. Whereas for S_1, 4.17(c) reads:

$$t \cdot \bar{m} + t \cdot \bar{n} = t \cdot (\bar{m} + \bar{n})$$

this result does not find its counterpart in 7.17(c), which reads:

$$t^{\bar{m}} \cdot t^{\bar{n}} = t^{\bar{m}+\bar{n}} \ .$$

That this is a dissimilarity rather than a similarity, follows from the fact that "+" in S_1 corresponds to "·" in S_2, and that multiplication by a numeral (the shorthand way of writing repeated addition) in S_1 corresponds to raising to some numeral power (the shorthand way of writing repeated multiplication) in S_2.

$$\therefore \quad \vdash \overline{2^k \cdot 2^p \cdot 2} = \overline{2^k} \cdot \overline{2^p \cdot 2}$$

$$\therefore \quad \vdash \overline{m \cdot n \cdot 2} = \bar{m} \cdot \overline{n \cdot 2} \ .$$

So, by induction, the result holds for all p, and hence for any numerals $\bar{m}$ and $\bar{n}$ of S_2.

(c) By induction in the metalanguage on "n" — as in S_1.

(d) As in S_1.

(e) As in S_1.

→

7.18 Definition:

$$t \approx s \pmod{\bar{k}} \overset{\text{def}}{\Leftrightarrow} (\exists w)[t = s \cdot w^{\bar{k}} \vee s = t \cdot w^{\bar{k}}]$$

7.19 Definition:

$$t \prec s \overset{\text{def}}{\Leftrightarrow} (\exists w)[w \neq \Delta \wedge t \cdot w = s] \ .$$

There is one further dissimilarity between S_1 and S_2. Whereas for S_1, 4.17(c) reads:

$$t \cdot \bar{m} + t \cdot \bar{n} = t \cdot (\bar{m} + \bar{n})$$

this result does not find its counterpart in 7.17(c), which reads:

$$t^{\bar{m}} \cdot t^{\bar{n}} = t^{\bar{m}+\bar{n}} \ .$$

That this is a dissimilarity rather than a similarity, follows from the fact that "+" in S_1 corresponds to "·" in S_2, and that multiplication by a numeral (the shorthand way of writing repeated addition) in S_1 corresponds to raising to some numeral power (the shorthand way of writing repeated multiplication) in S_2.

Thus special attention will have to be given to deriving theorems in S_2 using 7.17(c).

The counterpart of these theorems in S_2 are those theorems in S_1 employing 4.17(c), of which there is only one, namely 4.32 .

First note that 4.20 – 4.31 , with the necessary notational corrections, are results which carry over directly to S_2 , and are correspondingly labelled 7.20 – 7.31.

Theorem 4.32, however, does not find an exact counterpart in S_2 .

4.32 "translated" into S_2 reads:

$\underline{\alpha}$: $(\bar{p}^* = \bar{n}) \Rightarrow [t \cdot s \approx r \pmod{\bar{n}} \Leftrightarrow t \approx r \cdot s^{\bar{p}} \pmod{\bar{n}}]$.

However, by reasoning on a meta-level it can be seen that in S_1 :

$\underline{\beta}$: $t + s \equiv r \pmod{\bar{n}} \Leftrightarrow t + s \equiv r + s \cdot \bar{n} \pmod{\bar{n}}$

$\Leftrightarrow t \equiv r + s(\overline{n-1}) \pmod{\bar{n}}$.

Now it follows from 7.17(c) that similarly, in S_2 :

$\underline{\gamma}$: $t \cdot s \approx r \pmod{\bar{n}} \Leftrightarrow t \cdot s \approx r \cdot s^{\bar{n}} \pmod{\bar{n}}$

$\Leftrightarrow t \approx r \cdot s^{\overline{n-1}} \pmod{\bar{n}}$.

But γ differs from α in that in α the power of s is $\bar{p}$, with $\bar{p} \cdot \bar{2} = \bar{n}$, whereas in γ the power of s is $\overline{n-1}$.

Hence, as a result of 7.17(c), the counterpart of 4.31 in S_2 is <u>not</u> the formal translation α of 4.32, but a statement of the form γ .

The numeral $\overline{n-1}$, however, is not available in S_2 .

That is, for no $\bar{n}$ (except, incidentally, $\bar{2}$) can the

numeral $\overline{n-1}$ be found in the sequence

$\underline{\delta}$: $\bar{1}$, $\bar{2}$, $\bar{4}$, $\bar{8}$, $\overline{16}$ .....

By reasoning on a meta-level it can be seen, however, that for any $\bar{n}$, the numeral $\overline{n-1}$ can be expressed as the sum of the numerals proceeding it in the sequence δ.

This follows, since $2^{n+1} = 1 + \sum_{k=0}^{n} 2^k$.

Addition is not available in S_2, but neither is it needed in in this case since the problem is to express $s^{\overline{n-1}}$ in S_2 (for some term s) and not $\overline{n-1}$.

Accordingly, it can be seen that

$s^{\overline{n-1}}$ is expressible in S_2 as

$s \cdot s^{\bar{2}} \cdot s^{\bar{4}} \cdot \ldots \cdot s^{\bar{p}}$, with $\bar{p}^* = \bar{n}$.

Thus a counterpart of 4.32 has been found in S_2, and it reads:

$$(\bar{p}^* = \bar{n}) \Rightarrow [t \cdot s \approx r \pmod{\bar{n}} \Leftrightarrow t \approx r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \pmod{\bar{n}}] .$$

For any particular $\bar{n}$, this result can be expressed in S_2, and proved analogously to the proof of 4.32 in S_1 .

As a general result, however, it cannot be expressed in S_2, owing to the fact that the expression.

$$s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}}$$

is not expressible in S_2 if $\bar{n}$ is not a particular given numeral.

Thus the counterpart of 4.32 is proved in S_2 as a meta-result.

7.32 Proposition:

For any particular $\bar{n}$,

$$\vdash_{S_2} (\bar{p}^* = \bar{n}) \Rightarrow [t \cdot s \approx r \pmod{\bar{n}} \Leftrightarrow t \approx r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \pmod{\bar{n}}].$$

Proof:

Let $\bar{p}^* = \bar{n}$.

Suppose first that:

$$t \cdot s \approx r \pmod{\bar{n}}.$$

Then, for some w:

$$t \cdot s = r \cdot w^{\bar{n}}.$$

$$\therefore \quad t \cdot s \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} = r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \cdot w^{\bar{n}}$$

$$\therefore \quad t \cdot s^{\overline{\left(1 + \sum_{k=0}^{m} 2^k\right)}} = r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \cdot w^{\bar{n}},$$

where $p = 2^m$, hence $n = 2^{m+1}$.

$$\therefore \quad t \cdot s^{\bar{n}} = r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \cdot w^{\bar{n}}$$

$$\therefore \quad t \cdot s^{\bar{n}} \approx r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \pmod{\bar{n}}$$

$$t \approx r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \pmod{\bar{n}} \qquad \text{by 4.31}.$$

Now suppose that:

$$t \approx r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \pmod{\bar{n}}$$

Then, for some w:

$$t = r \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \cdot w^{\bar{n}}$$

$$\therefore \quad t \cdot s = r \cdot s \cdot s \cdot s^{\bar{2}} \cdot \ldots \cdot s^{\bar{p}} \cdot w^{\bar{n}}$$

$$\therefore \quad t \cdot s = r \cdot s^{\overline{\left(1 + \sum_{k=0}^{m} 2^k\right)}} \cdot w^{\bar{n}},$$

where $p = 2^m$, hence $n = 2^{m+1}$.

$$\therefore \quad t \cdot s = r \cdot s^{\bar{n}} \cdot w^{\bar{n}}$$

$$\therefore \quad t \cdot s \approx r \cdot s^{\bar{n}} \pmod{\bar{n}}$$

$$\therefore \quad t \cdot s \approx r \cdot \pmod{\bar{n}}. \longrightarrow$$

Theorems 4.33 – 4.38 and 4.40 translate readily into S_2, and are correspondingly labelled 7.33 – 7.38 and 7.40 .

Thus only Propositions 7.39 and 7.41 – 7.44 remains to be proved.

Proposition 7.39 in particular deserves further attention.

In S_1 we proved (4.39) that, for any term t ; and any $\bar{n}$:

$$t \equiv \bar{1} \pmod{\bar{n}} \vee t \equiv \bar{2} \pmod{\bar{n}} \vee \ldots\ldots$$

$$\ldots\ldots \vee t \equiv \bar{n} \pmod{\bar{n}} .$$

Thus what may be termed as the "range" of the congruence relation mod $\bar{n}$ is the sequence

$$\bar{1}, \quad \bar{2}, \quad \bar{3} \ldots\ldots \bar{n}$$

which also happens to be the first "n" numerals generated from the individual constant 0 .

In S_2, the first "n" numerals generated from the individual constant Δ are

$$\bar{2}, \quad \bar{4}, \quad \bar{8} \ldots\ldots \overline{2^{\bar{n}}}.$$

If "n" is such that $\bar{n}$ is in S_2, then, since $\bar{n} \prec \overline{2^{\bar{n}}}$, $\bar{n}$ occurs in the sequence above.

Thus, in S_2, the "range" of the congruence relation mod $\bar{n}$ is not merely the sequence

$$\bar{2}, \quad \bar{4}, \quad \bar{8} \ldots\ldots \bar{n} ,$$

which terminates in the numeral $\bar{n}$, but the sequence

$$\bar{2}, \quad \bar{4}, \quad \bar{8} \ldots\ldots 2^{\bar{n}} ,$$

which terminates in the "n"-th numeral generated from Δ .

The difference between S_1 and S_2 in this respect is that in S_1 the numeral $\bar{n}$ is in fact the n-th numeral generated from 0, whereas in S_2 the numeral $\bar{n}$ is less than the n-th numeral generated from Δ.

7.39 Proposition:

For any terms r and s, and any numeral $\bar{n}$ of S_2:

$$\vdash_{S_2} [r \approx s\cdot\bar{2} \pmod{\bar{n}} \vee r \approx s\cdot\bar{4} \pmod{\bar{n}} \vee \ldots\ldots \vee r \approx s\cdot\overline{2^n} \pmod{\bar{n}}] .$$

Proof:

If $r = s$, then $r\cdot\overline{2^n} = s\cdot\overline{2^n}$

$$\therefore r\cdot\bar{2}^{\bar{n}} = s\cdot\overline{2^n}$$

$$\therefore r \approx s\cdot\overline{2^n} \pmod{\bar{n}} .$$

If $r \neq s$, then by 7.30 : $r \prec s \vee s \prec r$.

Suppose $s \prec r$.

Then by 7.19 : $(\exists w)[w \neq \Delta \wedge s\cdot w = r]$

— say $\bar{k} \neq \Delta \wedge s\cdot\bar{k} = r$.

By 7.30: $\bar{k} \prec \overline{2^n} \vee \bar{k} = \overline{2^n} \vee \overline{2^n} \prec \bar{k}$.

a) If $\bar{k} \prec \overline{2^n}$, then:

$$r = s\cdot\bar{k} = s\cdot\bar{k}\cdot\Delta^{\bar{n}}$$

$$\therefore r \approx s\cdot\bar{k} \pmod{\bar{n}} .$$

b) If $\bar{k} = \overline{2^n}$, then:

$$r = s\cdot\bar{k} = s\cdot\overline{2^n} = s\cdot\overline{2^n}\cdot\Delta^{\bar{n}}$$

$$\therefore r \approx s\cdot\overline{2^n} \pmod{\bar{n}} .$$

c) If $\overline{2^n} \prec \bar{k}$, then by 7.19:

$$(\exists w)[w \neq \Delta \wedge \overline{2^n}.w = \bar{k}]$$

— say $\bar{m} \neq \Delta \wedge \overline{2^n}.\bar{m} = \bar{k}$.

Then: $r = s.\bar{k} = s.\bar{m}.\overline{2^n} = s.\bar{m}.\overline{2^{\bar{n}}}$

$\therefore$ $r \approx s.\bar{m} \pmod{\bar{n}}$.

Now if $\bar{m} \prec \overline{2^n}$ or $\bar{m} = \overline{2^n}$, there is nothing left to prove.

If $\overline{2^n} \prec \bar{m}$, then repeat the process described in (c) until eventually the term $\bar{m}$ is less than $\overline{2^n}$.
Thus, eventually, for some $\bar{m} \prec \overline{2^n}$,

$$r \approx s.\bar{m} \pmod{\bar{n}}.$$

So for $s \prec r$ the proof is complete.

The case where $r \prec s$ is treated in an analogous manner.

Since $s \prec r \vee s = r \vee r \prec s$, this completes the proof.

$\longrightarrow$

7.41 Proposition:

$$\vdash_{S_2} (\exists x)[(x \approx \bar{k} \pmod{\bar{n}}) \wedge (t \prec x^{\bar{p}}.r) \wedge (x^{\bar{p}}.r \prec s)]$$

$$\Leftrightarrow (\exists x)[(x \approx \bar{k}^{\bar{p}} \pmod{\bar{n}.\bar{p}}) \wedge (t \prec x.r) \wedge (x.r \prec s)] .$$

Whereas in 4.41 the modulus-numeral is increased from $\bar{n}$ to $\bar{n}.\bar{p}$, in 7.41 the modulus-numeral is <u>not</u> increased from $\bar{n}$ to $\bar{n}^{\bar{p}}$, but merely, as before, to $\bar{n}.\bar{p}$.

This is a consequence of the fact that although

$$(\bar{k}.\bar{m}).\bar{n} = \bar{k}.(\bar{m}.\bar{n}) \quad \text{in } S_1 ,$$

$$(k^{\bar{m}})^{\bar{n}} \neq k^{\bar{m}^{\bar{n}}} \quad \text{in } S_2 ,$$

but $(k^{\bar{m}})^{\bar{n}} = k^{\bar{m}.\bar{n}}$.

The proof of 7.41 is analogous to that of 4.41.

7.42 Proposition:

The wff

$$(\exists x)[x \approx \bar{m} \pmod{\bar{n}}) \wedge (t \prec x \cdot r) \wedge (x \cdot r \prec s)]$$

is provable in S_2 if and only if the D.N.F.

$$[(t \prec r) \wedge (r \cdot \bar{m} \prec s)] \vee D_2 \vee D_4 \vee \cdots \vee D_\mu$$

holds, where $\mu = 2^n$, and D_q is shorthand for:

$$(r \prec t^*) \wedge (t \cdot \bar{q} \prec s) \wedge (t \cdot \bar{q} \approx r \cdot \bar{m} \pmod{\bar{n}}).$$

The proof of this proposition is exactly analogous to the proof given for 4.42.

Propositions 7.43 and 7.44 are the exact counterparts of 4.43 and 4.44, and the proofs are again analogous.

As has been seen, every theorem or proposition concerning S_1 has correlated with it a theorem or proposition concerning S_2.

It follows that the reduction procedure P is also applicable to S_2. Furthermore, the axioms of S_2, are true, and, as before, the rules of inference preserve the property of truth. Consequently, all those results established for S_1 carry over to S_2. Thus S_2 is consistent, complete and decidable, and the operation of exponentiation is not representable in S_2.

§ 2. Different Interpretations of S_2, and their relation to S_1

The given interpretation is not the only possible interpretation of S_2. For example, the function letter f_1^1 may be interpreted as multiplication by any prime number –

the domain of the interpretation would then vary accordingly. If f_1^1 is interpreted as multiplication by five, for example, the domain of the interpretation would be the set of all those natural numbers expressible in the form 5^n .

Except for having different symbols, the proper axioms of S_2 are exactly the same as those of S_1 . If f_1^1 and f_1^2 are interpreted in terms of multiplication, then the individual constant must be interpreted as the number "one". Otherwise the third and fourth axioms would be false. Similarly, if f_1^1 and f_1^2 are interpreted in terms of addition, then the individual constant must be interpreted as zero, in order not to invalidate the fourth axiom.

In S_2 , t^* was interpreted as $t \cdot 2$, for any term t . Since $t \cdot 2 = t + t$, S_2 can equally well be viewed as a first-order theory with a special kind of addition — any term may be added to itself once, and different terms cannot be added together. The recursive definition of the other function letter, f_1^2 , can now also be "translated" back into addition. For example:

$$\begin{aligned}
\bar{8} \cdot \bar{4} &= \bar{8} \cdot \bar{2}^* \\
&= (\bar{8} \cdot \bar{2})^* \\
&= (\bar{8} \cdot \bar{2}) + (\bar{8} \cdot \bar{2}) \\
&= (\bar{8} \cdot \bar{1}^*) + (\bar{8} \cdot \bar{1}^*) \\
&= (\bar{8} \cdot \bar{1})^* + (\bar{8} \cdot \bar{1})^* \\
&= \bar{8}^* + \bar{8}^* \\
&= \bar{8} + \bar{8} + \bar{8} + \bar{8} \ .
\end{aligned}$$

Since S_2 can thus be viewed as a subsystem of Arithmetic employing only a specialized addition on a proper subset of the natural numbers, S_2 under the given interpretation is

in fact a subsystem of S_1. In retrospect it is therefore not surprising that S_2 turned out to be complete. Each of the other interpretations of S_2 mentioned above are subsystems of S_1 in the same way, and each of them will be complete.

§

CHAPTER VIII

CONCLUSION

In a full formalization of Arithmetic denumerably many arithmetical operations can be defined by double recursion as follows*

A function $H(p,n,a)$ is defined by the equations:

$$\begin{aligned} H(0,n,a) &= n + 1 \\ H(1,0,a) &= a \\ H(2,0,a) &= 0 \\ H(p+3,0,a) &= 1 \\ H(p+1,n+1,a) &= H(p,H(p+1,n,a),a) \ , \end{aligned}$$

then $H(1,n,a)$ defines addition, $H(2,n,a)$ multiplication, etc.

If S_i is now any formalization of a (not necessarily proper) part of Arithmetic, call an operation belonging to the recursion schema above the <u>strongest</u> arithmetical operation in S_i if the next operation in the recursion schema is not representable in S_i.

For example, addition is the strongest operation in S_1, and multiplication is the strongest operation in S_2. There is no strongest operation in S.

I <u>Conjecture</u>:

If a formalization S_i of a (not necessarily proper) part of Arithmetic does <u>not</u> have a strongest operation, then there is no reduction procedure for S_i.

---

* [7], pp. 13 - 23.

II Conjecture:

If a formalization S_i of a (not necessarily proper) part of Arithmetic is complete, then there is a reduction procedure for S_i.

The systems S, S_1 and S_2 support both these conjectures. If these conjectures are both correct, they lead to the conclusion that the incompleteness of Arithmetic arises from the fact that it does not have a strongest operation.

§

BIBLIOGRAPHY

[1] ACKERMANN, W. Solvable Cases of the Decision Problem. Studies in Logic and Founds. of Maths. North Holland Publishing Co. 1962.

[2] BELL, J.L. and SLOMSON, A.B. Models and Ultra-products. North Holland. 1971.

[3] BETH, E.W. The Foundations of Mathematics. North Holland. 1959.

[4] COPI, I.M. Symbolic Logic. Macmillan. 1969.

[5] GÖDEL, K. On Formally Undecidable Propositions of Principia Mathematica and Related Systems. Oliver and Boyd, London. 1962.

[6] HILBERT, D. and BERNAYS, P. Grundlagen der Mathematik. Band I. Springer Verlag. 1934.

[7] GOODSTEIN, R.L. Recursive Number Theory. Studs. in Logic and Founds. of Maths. 1964.

[8] HUGHES, E. and LONDEY, D.G. The Elements of Formal Logic. Methuen and Co. 1965.

[9] KNEEBONE, G.T. Mathematical Logic and the Foundations of Mathematics. Van Nostrand. 1963.

[10] MENDELSON, E. Introduction to Mathematical Logic. Van Nostrand. 1964.

[11] MOSTOWSKI, A. Sentences Undecidable in Formalized Arithmetic. Studies in Logic and Founds. of Maths. North Holland. 1957.

[12] NAGEL, E. and NEWMAN, J.R. Gödel's Proof. Routledge and Kegan Paul. 1964.

[13] PRESBURGER, M. Über die vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. Comptes — Rend. du Premier Congr. d. Math. des Pays Slaves. 1929. Warschau. 1930.

[14] TARSKI, A. Logic,Semantics, Metamathematics. Oxford. 1956.

[15] KLEENE, S.C. Mathematical Logic. Wiley and Sons. 1968.

§