Elliott Mendelson

Introduction to Mathematical Logic

Second Edition

D. Van Nostrand Co. New York 1979

To Arlene

D. Van Nostrand Company Regional Offices:
New York Cincinnati

D. Van Nostrand Company International Offices:
London Toronto Melbourne

Library of Congress Catalog Card Number: 78-65959
ISBN: 0-442-25307-9

Published by D. Van Nostrand Company
135 West 50th Street, New York, N.Y. 10020

10 9 8 7 6 5 4 3 2 1

PREFACE TO THE SECOND EDITION

This new edition contains considerable improvements over the first edition. Much new material has been added. For example, in Chapter 2 there are two new sections on model theory devoted to elementary equivalence and elementary extensions and to ultrapowers and nonstandard analysis. The greatest change has been the addition of a large number of exercises. There are 389 exercises, many of them consisting of several parts. Completely new is a section at the end of the book, Answers to Selected Exercises, which should improve the usefulness of the book as a textbook as well as for independent study. With all these changes, I have attempted to preserve the spirit of the original book, which was intended to be a simple, clear introduction to mathematical logic unencumbered by excessive notation and terminology.

I should like to thank the many people who have given me suggestions for corrections and improvement. I am particularly indebted to Professor Frank Cannonito for much helpful advice.

ELLIOTT MENDELSON

PREFACE TO THE FIRST EDITION

In this book we have attempted to present a compact introduction to some of the principal topics of mathematical logic. In order to give a full and precise treatment of the more important basic subjects, certain subsidiary topics, such as modal, combinatory, and intuitionistic logics, and some interesting advanced topics, such as degrees of recursive unsolvability, have had to be omitted.

In the belief that beginners should be exposed to the most natural and easiest proofs, free-swinging set-theoretic methods have been used. The significance of a demand for constructive proofs can be evaluated only after a certain amount of experience with mathematical logic has been obtained. After all, if we are to be expelled from "Cantor's paradise" (as non-constructive set theory was called by Hilbert), at least we should know what we are missing.

The five chapters of the book can be covered in two semesters, but, for a one-semester course, Chapters 1 through 3 will be quite adequate (omitting, if hurried, Sections 5 and 6 of Chapter 1 and Sections 10, 11, and 12 of Chapter 2). The convention has been adopted of prefixing a superscript " D to any section or exercise which will probably be difficult for a beginner, and a superscript " A to any section or exercise which presupposes familiarity with a topic that has not been carefully explained in the text. Bibliographical references are given to the best source of information, which is not always the earliest paper; hence these references give no indication as to priority. For example, Boone [1959] gives the most complete account of his work on the word problem, which was actually done independently of and about the same time as Novikov's work [1955].

The present book is an expansion of lecture notes for a one-semester course in mathematical logic given by the author at Columbia University from 1958 to 1960 and at Queens College in 1961 and 1962. The author hopes that it can be read with ease by anyone with a certain amount of experience in abstract mathematical thought, but there is no specific prerequisite. The author would like to thank J. Barkley Rosser for encouragement and guidance during his graduate studies in logic, and he would like to acknowledge also the obvious debt owed to the books of Hilbert-Bernays, 1934, 1939; Kleene, 1952; Rosser, 1953; and Church, 1956.

CONTENTS

INTRODUCTION

One of the most popular definitions of logic is that it is the analysis of methods of reasoning. In studying these methods, logic is interested in the form rather than the content of the argument. For example, consider the two deductions:

(1) All men are mortal. Socrates is a man. Hence Socrates is mortal.
(2) All rabbits like carrots. Sebastian is a rabbit. Hence, Sebastian likes carrots.

Both have the same form: All A are B. S is an A. Hence S is a B. The truth or falsity of the particular premisses and conclusions is of no concern to the logician. He wants to know only whether the truth of the premisses implies the truth of the conclusion. The systematic formalization and cataloguing of valid methods of reasoning is one of the main tasks of the logician. If his work uses mathematical techniques and if it is primarily devoted to the study of mathematical reasoning, then it may be called mathematical logic. We can narrow the domain of mathematical logic if we define its principal aim to be a precise and adequate definition of the notion of "mathematical proof'.

Impeccable definitions have little value at the beginning of the study of a subject. The best way to find out what mathematical logic is about is to start doing it, and the student is advised to begin reading the book even though (or especially if) he has qualms about the meaning or purposes of the subject.

Although logic is basic to all other studies, its fundamental and apparently self-evident character discouraged any deep logical investigations until the late nineteenth century. Then, under the impetus of the discovery of non-Euclidean geometries and of the desire to provide a rigorous foundation for analysis, interest in logic revived. This new interest, however, was still rather unenthusiastic until, around the turn of the century, the mathematical world was shocked by the discovery of the paradoxes, i.e., arguments leading to contradictions. The most important of these paradoxes are the following.

Logical Paradoxes

(1) (Russell, 1902) By a set, we mean any collection of objects, e.g., the set of all even integers, the set of all saxophone players in Brooklyn, etc. The objects which make up a set are called its members. Sets may themselves be members of sets, e.g., the set of all sets of integers has sets as its members. Most sets are not members of themselves; the set of cats, for example, is not a member of itself, because the set of cats is not a cat. However, there may be sets which do belong to themselves, e.g., the set of all sets. Now, consider the set A of all those sets X such that X is not a member of X. Clearly, by definition, A is a member of A if and only if A is not a member of A. So, if A is a member of A, then A is also not a member of A; and if A is not a member of A, then A is a member of A. In any case, A is a member of A and A is not a member of A.

(2) (Cantor, 1899) This paradox involves a certain amount of the theory of cardinal numbers and may be skipped by those having no previous acquaintance with that theory. The cardinal number $\overline{\overline{Y}}$ of a set Y is defined to be the set of all sets X which are equinumerous with Y (i.e., for which there is a one-one correspondence between Y and X, cf. page 7). We define $\overline{\overline{Y}} \leqslant \overline{\overline{Z}}$ to mean that Y is equinumerous with a subset of Z; by $\overline{\overline{Y}} < \overline{\overline{Z}}$ we mean $\overline{\overline{Y}} \leqslant \overline{\overline{Z}}$ and $\overline{\overline{Y}} \neq \overline{\overline{Z}}$. Cantor proved that, if $\mathcal{P}(Y)$ is the set of all subsets of Y, then $\overline{\overline{Y}} < \overline{\overline{\mathcal{P}(Y)}}$ (cf. page 195). Let C be the universal set, i.e., the set of all sets. Now, $\mathcal{P}(C)$ is a subset of C, so it follows easily that $\overline{\overline{\mathcal{P}(C)}} \leqslant \overline{\overline{C}}$. On the other hand, by Cantor's Theorem, $\overline{\overline{C}} < \overline{\overline{\mathcal{P}(C)}}$. The Schröder-Bernstein Theorem (cf. page 194) asserts that if $\overline{\overline{Y}} \leqslant \overline{\overline{Z}}$ and $\overline{\overline{Z}} \leqslant \overline{\overline{Y}}$, then $\overline{\overline{Y}} = \overline{\overline{Z}}$. Hence, $\overline{\overline{C}} = \overline{\overline{\mathcal{P}(C)}}$, contradicting $\overline{\overline{C}} < \overline{\overline{\mathcal{P}(C)}}$.

(3) (Burali-Forti, 1897) This paradox is the analogue in the theory of ordinal numbers of Cantor's Paradox and will make sense only to those already familiar with ordinal number theory. Given any ordinal number, there is a still larger ordinal number. But the ordinal number determined by the set of all ordinal numbers is the largest ordinal number.

Semantic Paradoxes

(4) The Liar Paradox. A man says, "I am lying." If he is lying, then what he says is true, and so he is not lying. If he is not lying, then what he says is true, and so he is lying. In any case, he is lying and he is not lying.†

†The Cretan "paradox", known in antiquity, is similar to the Liar Paradox. The Cretan philosopher Epimenides said, "All Cretans are liars." If what he said is true, then, since Epimenides is a Cretan, it must be false. Hence, what he said is false. Thus, there must be some Cretan who is not a liar. This is not logically impossible, so we do not have a genuine paradox. However, the fact that the utterance by Epimenides of that false sentence could imply the existence of some Cretan who is not a liar is rather unsettling.

(5) (Richard, 1905) Some phrases of the English language denote real numbers, e.g., "the ratio between the circumference and diameter of a circle" denotes the number π. All phrases of the English language can be enumerated in a standard way: order all phrases having k letters lexicographically (as in a dictionary), and then place all phrases with k letters before all phrases with a larger number of letters. Hence, all phrases of the English language denoting real numbers can be enumerated merely by omitting all other phrases in the given standard enumeration. Call the n^{th} real number in this enumeration the n^{th} Richard number. Consider the phrase: "the real number whose n^{th} decimal place is 1 if the n^{th} decimal place of the n^{th} Richard number is not 1, and whose n^{th} decimal place is 2 if the n^{th} decimal place of the n^{th} Richard number is 1". This phrase defines a Richard number, say the k^{th} Richard number; but, by its definition, it differs from the k^{th} Richard number in the k^{th} decimal place.

(6) (Berry, 1906) There are only a finite number of syllables in the English language. Hence, there are only a finite number of English expressions containing fewer than forty syllables. There are, therefore, only a finite number of positive integers which are denoted by an English expression containing fewer than forty syllables. Let k be *the least positive integer which is not denoted by an expression in the English language containing fewer than forty syllables*. The italicized English phrase contains fewer than forty syllables and denotes the integer k.

(7) (Grelling, 1908) An adjective is called *autological* if the property denoted by the adjective holds for the adjective itself. An adjective is called *heterological* if the property denoted by the adjective does not apply to the adjective itself. For example, "polysyllabic" and "English" are autological, while "monosyllabic", "French", and "blue" are heterological. Consider the adjective "heterological". If "heterological" is heterological, then it is not heterological. If "heterological" is not heterological, then it is heterological. In any case, "heterological" is both heterological and not heterological.

All of these paradoxes are genuine in the sense that they contain no obvious logical flaws. The logical paradoxes involve only notions from the theory of sets, whereas the semantic paradoxes also make use of concepts like "denote", "true", "adjective", which need not occur within our standard mathematical language. For this reason, the logical paradoxes are a much greater threat to a mathematician's peace of mind than the semantic paradoxes.

Analysis of the paradoxes has led to various proposals for avoiding them. All of these proposals are restrictive in one way or another of the "naive" concepts which enter into the derivation of the paradoxes. Russell noted the self-reference present in all the paradoxes and suggested that every object must have a definite non-negative integer as its "type". Then an expression, "x is a member of the set y", is *meaningful* if and only if the type of y is one greater than the type of x.

This approach, known as the theory of types and systematized and developed by Russell-Whitehead [1910–1913], is successful in eliminating the known paradoxes,? but it is clumsy in practice and has certain other drawbacks as well. A different criticism of the logical paradoxes is aimed at their assumption that, for every property $P(x)$, there exists a corresponding set of all objects x which satisfy $P(x)$. If we reject this assumption, then the logical paradoxes are no longer derivable.‡ It is necessary, however, to provide new postulates that will enable us to prove the existence of those sets which are a daily necessity to the practicing mathematician. The first such axiomatic set theory was invented by Zermelo [1908]. In Chapter 4 we shall present an axiomatic theory of sets which is a descendant of Zermelo's system (with some new twists given to it by von Neumann, R. Robinson, Bernays, and Gödel). There are also various hybrid theories combining some aspects of type theory and axiomatic set theory, e.g., Quine's system NF (cf. Rosser [1953]).

A more radical interpretation of the paradoxes has been advocated by Brouwer and his intuitionist school (cf. Heyting [1956]). They refuse to accept the universality of certain basic logical laws, such as the law of excluded middle: P or not-P. Such a law, they claim, is true for finite sets, but it is invalid to extend it on a wholesale basis to all sets. Likewise, they say it is invalid to conclude that "there exists an object x such that not-$P(x)$" follows from "not-(for all x, $P(x)$)"; we are justified in asserting the existence of an object having a certain property only if we know an effective method for constructing (or finding) such an object. The paradoxes are, of course, not derivable (or even meaningful) if we obey the intuitionist strictures, but, alas, so are many beloved theorems of everyday mathematics, and, for this reason, intuitionism has found few converts among mathematicians.

Whatever approach one takes to the paradoxes, it is necessary first to examine the language of logic and mathematics to see what symbols may be used, to determine the ways in which these symbols are put together to form terms, formulas, sentences, and proofs, and to find out what can and cannot be proved if certain axioms and rules of inference are assumed. This is one of the tasks of mathematical logic, and, until it is done, there is no basis for comparing rival foundations of logic and mathematics. The deep and devastating results of Gödel, Tarski, Church, Rosser, Kleene, and many others have been ample reward for the labor invested and have earned for mathematical logic its status as an independent branch of mathematics.

†Russell's Paradox, for example, depends upon the existence of the set A of all sets which are not members of themselves. Because, according to the theory of types, it is meaningless to say that a set belongs to itself, there can be no such set A.

$Russell's Paradox then proves that there is no set A of all sets which do not belong to themselves; the paradoxes of Cantor and Burali-Forti show that there is no universal set and no set containing all ordinal numbers. The semantic paradoxes cannot even be formulated, since they involve notions not expressible within the system.

For the absolute novice a summary will be given here of some of the basic ideas and results used in the text. The reader is urged to skip these explanations now, and, if necessary, to refer to them later on.

A *set* is a collection of objects.? The objects in the collection are called *elements* or *members* of the set, and we shall write "$x \in y$" for the statement that x is a member of y. (Synonymous expressions are "x belongs to y" and "y contains x".) The negation of "$x \in y$" will be written "$x \notin y$".

By "$x \subseteq y$" we mean that every member of x is also a member of y, or, in other words, that x is a subset of y (or, synonymously, that x is included in y). We shall write "t = s" to mean that "t" and "s" denote the same object. As usual, "$t \neq s$" is the negation of "$t = s$". For sets x and y, we assume that x = y if and only if $x \subseteq y$ and $y \subseteq x$; that is, if and only if x and y have the same members. A set x is called aproper subset of a set y, written "$x \subset y$", if $x \subseteq y$ but $x \neq y$.‡

The union $x \cup y$ of sets x and y is defined to be the set of all elements which are members of x or y or both. Hence, $x \cup x = x$, x u y = $y \cup x$, and $(x \cup y) \cup z = x \cup (y$ u $z)$. The intersection $x \cap y$ is the set of elements which x and y have in common. It is easy to verify that x n $x = x$, $x \cap y = y \cap x$, $x \cap (y \cap z) = (x \cap y) \cap z$, $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$, and $x \cup (y \cap z) = (x \cup y) \cap (x$ u $z)$. The relative complement $x - y$ is the set of members of x which are not members of y. We also postulate the existence of the empty set (or null set) 0, i.e., a set which has no members at all. Then, $x \cap 0 = 0$, x U $0 = x$, $x - 0 = x$, $0 - x = 0$, andx $- x = 0$. Two sets x andy arecalled disjoint if $x \cap y = 0$.

Given any objects $b_1, \ldots, b_k$, the set which contains b,, $\ldots, b_k$ as its only members is denoted {b,, $\ldots, b_k\}$. In particular, {x, y) is a set having x and y as its only members and, if $x \neq y$, is called the unorderedpair of x and y. The set {x, $x\}$ is written {x) and is called the unit set of x. Notice that {x, y) = {y, x). On the other hand, by (b,, $\ldots, b_k\rangle$ we mean the ordered k-tuple of b,, $\ldots, b_k$. The basic property of ordered k-tuples is that (b,, $\ldots, b_k\rangle$ = (c,, $\ldots, c_k\rangle$ if and only if $b_1 = c_1, b_2 = c_2, \ldots, b_k = c_k$. Thus, (b,, $b_2\rangle = \langle b_2, b_1\rangle$ if and only if $b_1 = b_2$. Ordered 2-tuples are called ordered pairs. If X is a set and k is a positive integer, we denote by X^k the set of all ordered k-tuples (b,, $\ldots, b_k\rangle$ of elements $b_1, \ldots, b_k$ of X. We also make the convention that X^1 stands for X. X^k is called the Cartesian product of X with itself k times. If Y and Z are sets, then by $Y \times Z$ we denote the set of all ordered pairs (y, $z\rangle$ such that $y \in Y$ and $z \in Z$. $Y \times Z$ is called the Cartesian product of Y and Z.

†Which collections of objects form sets will not be specified here. Cue will be exercised to avoid using any ideas or procedures which may lead to the paradoxes; all the results can be formalized in the axiomatic set theory of Chapter 4. The term "class" is sometimes used as a synonym for "set,,, but it will be avoided here because it has a differentmeaning in Chapter 4. If the property $P(x)$ does determine a set, this set is often denoted $\{x|P(x)\}$.

‡The notation $x \subsetneq y$ is often used instead of $x \subset y$.

An n-place relation (or a relation with *n* arguments) on a set X is a subset of X^n, **i.e.,** a set of ordered n-tuples of elements of X. For example, the 3-place relation of betweenness for points on a line is the set of all 3-tuples (x, y, z) such that the point x lies between the points y and z. A 2-place relation is called a binary relation, **e.g.,** the binary relation of fatherhood on the set of human beings is the set of all ordered pairs (x, y) such that x and y are human beings and x is the father of y. A 1-place relation on X is a subset of X, and is called a property on X.

Given a binary relation R on a set X, the domain of R is defined to be the set of all y such that (y, z) $\in$ R for some z; the range of R is the set of all *z* such that (y, z) $\in$ R for some y; and **the** ***field*** of R is the union of the domain and range of R. The inverse relation R^{-1} of R is the set of all ordered pairs (y, z) such that (z, y) $\in$ R. For example, the domain of the relation $<$ on the set ω of non-negative **integers**† is ω, its range is $\omega - \{0\}$, and the inverse of $<$ is $>$. Notation: Very often xRy is written instead of (x, y) $\in$ R. Thus, in the example just given, we usually write x $<$ y instead of (x, y) $\in$ $<$.

A binary relation R is said to be ***reflexive*** if xRx for all x in the field of R. R is ***symmetric*** if xRy implies yRx, and R is transitive if xRy and yRz imply xRz. Examples: The relation $\leqslant$ on the set of integers is reflexive and transitive but not symmetric. The relation "having at least one parent in common" on the set of human beings is reflexive and symmetric but not transitive.

A binary relation which is reflexive, symmetric, and transitive is called an equivalence relation. Examples of equivalence relations: (1) the identity relation I_X on a set X consisting of all pairs (y, y), where y $\in$ X; (2) the relation of parallelism between lines in a plane; (3) given a fixed positive integer *n*, the relation x $\equiv$ y (mod n) holds when x and y are integers and x $-$ y is divisible by n; (4) the relation between directed line segments in three-dimensional space which holds when and only when they have the same length and the same direction; (5) the congruence relation on the set of triangles in a plane; (6) the similarity relation on the set of triangles in a plane. Given an equivalence relation R on a set X, and given any y $\in$ X, define [y] as the set of all *z* in X such that yRz. Then [y] is called the R-equivalence ***class*** of y. It is easy to check that [y] = [z] if and only if yRz and that, if [y] $\neq$ [z], then [y] $\cap$ [z] = **0, i.e.,** different R-equivalence classes have no elements in common. Hence, the set X is completely partitioned into the R-equivalence classes. For some of the examples above: (1) the equivalence classes are just the unit sets {y), where y $\in$ X; (2) the equivalence classes can be considered to be the directions in the plane; (3) there are *n* equivalence classes, the k^{th} equivalence class (k = 0, 1, . . . , $n-1$) being the set of all numbers which leave the remainder k upon division by n; (4) the equivalence classes are the three-dimensional vectors.

†ω **will also be referred to as the set of** ***natural numbers.***

A ***function*** f is a binary relation such that (x, y) $\in$ f and (x, z) $\in$ f imply $y = z$. **Thus,** for any element x of the domain of a function f, there is a unique y **such that** $\langle x, y\rangle \in f$; this unique element y is denoted $f(x)$. If x is in the domain **of** f, **then** $f(x)$ is said to be defined. A function f with domain X and range Y is **said to be a** function from X onto Y. If f is a function from X onto Y, and $Y \subseteq Z$, **then** f is called a function from X into Z. For example, if $f(x) = 2x$ for **every integer** x, f is a function from the set of integers onto the set of even **integers, and** f is a function from the set of integers into the set of integers. A **function the** domain of which consists **of** n**-tuples** is said to be a function of *n* ***arguments.*** **A** (total) function of *n* arguments on a set X is a function f whose **domain** is X^n. We usually write $f(x_1, \ldots, x_n)$ instead of $f(\langle x_1, \ldots,$ x,,)). A ***partial*** **function** of *n* arguments on a set X is a function whose domain is a **subset of** X^n; **e.g.** ordinary division is a partial, but not total, function of two arguments on the set of integers (since division by zero is not defined). If f is a function **with domain** X and range Y, then the restriction f_Z of f to a set Z is the function $f \cap (Z \times Y)$. Clearly, $f_Z(u) = v$ if and only if $u \in Z$ and $f(u) = v$. **The** image **of the set** Z under the function f is the range of f,. The inverse image of **a** set W under the function f is the set of all elements u of the domain of f such that $f(u) \in W$. We say that f maps X onto (into) Y if X is a subset of the domain of f and the image of X under f is (a subset of) Y. By an n-place operation (or operation with *n* arguments) on a set X we mean a function from X^n into X. For example, ordinary addition is a binary (**i.e.,** 2-place) operation on the set of natural numbers {**0**, 1, 2, . . . }. But ordinary subtraction is not a binary operation on the set of natural numbers, though it is a binary operation on the set of integers.

Given two functions f and g, the composition f $\circ$ g (also sometimes denoted fg) is the function such that $(f \circ g)(x) = f(g(x))$; $(f \circ g)(x)$ is defined if and only **if** $g(x)$ is defined and $f(g(x))$ is defined. For example, if $g(x) = x^2$ and $f(x) = x + 1$ for every integer x, then $(f \circ g)(x) = x^2 + 1$ and $(g \circ f)(x) = (x + 1)^2$. **Also,** if $h(x) = -x$ for every real number x and $f(x) = \sqrt{x}$ for every **non-negative** real number x, then $(f \circ h)(x)$ is defined only for $x \leqslant 0$, and, for such x, $(f \circ h)(x) = \sqrt{-x}$. A function f such that $f(x) = f(y)$ implies x = y is called a 1–1 (*one–one*) function. Examples: (1) The identity relation I_X on a set X is a **1–1 function, since** $I_X(y) = y$ for any y $\in$ X; (2) the function $g(x) = 2x$, for **every integer** x, is a 1–1 function; (3) the function $h(x) = x^2$, for every integer x, **is not 1–1,** since $h(-1) = h(1)$. Notice that a function f is 1–1 if and only if its **inverse** relation f^{-1} is a function. If the domain and range of a 1–1 function f **are** X **and** Y, respectively, then f is said to be a 1–1 (one–one) correspondence ***between*** X and Y; then f^{-1} is a 1–1 correspondence between Y and X, and $(f^{-1} \circ f) = I_X$ and $(f \circ f^{-1}) = I_,$. If f is a 1–1 correspondence between X and Y, **and** g **is** a 1–1 correspondence between Y and Z, then g $\circ$ f is a 1–1 **correspondence** between X and Z. Sets X and Y are said to be equinumerous (written X ≅ Y) if and only if there is a 1–1 correspondence between X and Y. Clearly, X ≅ X; X ≅ Y implies Y ≅ X; and X ≅ Y and $Y \cong Z$ imply X ≅ Z. One can prove (cf. **Schröder-Bernstein** Theorem, page 194) that if X ≅ Y, ⊆ Y and Y ≅ X, ⊆ X, then X ≅ Y. If X ≅ Y, one sometimes says that X and Y *have* the same cardinal number, and if X is equinumerous with a subset of Y but Y is not equinumerous with a subset of X, one says that the cardinal number d X is smaller than the cardinal number of Y.†

A set X is denumerable if it is equinumerous with the set of positive integers. A denumerable set is said to have cardinal number $\aleph_0$, and any set equinumerous with the set of all subsets of a denumerable set is said to have the cardinal number $2^{\aleph_0}$ (or to have the power d the continuum). A set X is finite if it is empty or if it is equinumerous with the set of all positive integers (1, 2, . . . , n) which are less than or equal to some positive integer n. A set which is not finite is said to be infinite. A set is countable if it is either finite or denumerable. Clearly, any subset of a denumerable set is countable. A denumerable sequence is a function s whose domain is the set of positive integers; one usually writes s_n instead of $s(n)$. A *finite* sequence is a function whose domain is (1, 2, . . . , n), for some positive integer n.

Let $P(x, y,, \dots, y_k)$ be some relation on the set of non-negative integers. In particular, P may involve only the variable x and thus be a property. If $P(0, y,, \dots, y_k)$ holds, and, if, for any n, $P(n, y,, \dots, y_k)$ implies $P(n + 1, y_1, \dots, y_k)$, then $P(x, y,, \dots, y_k)$ is true for all non-negative integers x (Principle d Mathematical Induction). In applying this principle, one usually proves that, for any n, $P(n, y,, \dots, y_k)$ implies $P(n + 1, y,, \dots, y_k)$ by assuming $P(n, y,, \dots, y_k)$ and then deducing $P(n + 1, y_1, \dots, y_k)$; in the course of this deduction, $P(n, y,, \dots, y_k)$ is called the inductive hypothesis. If the relation P actually involves variables $y,, \dots, y_k$ other than x, then the proof of "for all x, $P(x)$" is said to proceed by induction on x. A similar induction principle holds for the set of integers greater than some fixed integer **j**. Example: to prove by mathematical induction that the sum of the first n odd integers $1 + 3 + 5 + \dots + (2n - 1)$ is n^2, first show that $1 = 1^2$ (i.e., $P(1)$), and then, that if $1 + 3 + 5 + \dots + (2n - 1) = n^2$, then $1 + 3 + 5 + \dots + (2n - 1) + (2n + 1) = (n + 1)^2$ (i.e., if $P(n)$ then $P(n + 1)$). From the Principle of Mathematical Induction one can prove the Principle d Complete Induction: if, for every non-negative integer x the assumption that $P(u, y,, \dots, y_k)$ is true for all $u < x$ implies that $P(x, y,, \dots, y_k)$ holds, then, for all non-negative integers x, $P(x, y,, \dots, y_k)$ is true. (Exercise: show, by complete induction, that every integer greater than 1 is divisible by a prime number.)

†One can attempt to define the cardinal number of a set X as the collection $[X]$ of all sets equinumerous with X. However, in certain systems of set theory, $[X]$ does not exist, whereas in others (cf. page 196), $[X]$ exists but is not a set. For cardinal numbers $[X]$ and $[Y]$, one can define $[X] \leqslant [Y]$ to mean that X is equinumerous with a subset of Y.

A *partial* order is a binary relation R such that R is transitive and, for every x in the field of R, xRx is false. If R is a partial order, then the relation R' which is the union of R and the set of all ordered pairs (x, x), where x is in the field of R, we shall call a reflexive partial order; in the literature, "partial order" is used for either partial order or reflexive partial order. Notice that (xRy and yRx) is impossible if R is a partial order, while (xRy and yRx) implies x = y if R is a reflexive partial order. A (reflexive) total order is a (reflexive) partial order R such that, for any x and y in the field of R, either x = y or xRy or yRx. Examples: (1) the relation < on the set of integers is a total order, while ⩽ is a reflexive total order; (2) the relation ⊂ on the set of all subsets of the set of positive integers is a partial order, but not a total order, while the relation ⊆ is a reflexive partial order but not a reflexive total order. If C is the field of a relation R, and if B is a subset of C, then an element y of B is called an R-least *element* of B if yRz for every element z of B different from y. A well-order (or *well-ordering* relation) is a total order R such that every non-empty subset of the field of R has an R-least element. Examples: (1) the relation < on the set of non-negative integers is a well-order; (2) the relation < on the set of non-negative rational numbers is a total order but not a well-order; (3) the relation < on the set of integers is a total order but not a well-order. Associated with every well-order R having field X there is a corresponding Complete Induction Principle: if P is a property such that, for any u in X, whenever all z in X such that zRu have the property P, then u has the property P, then it follows that all members of X have the property P. If the set X is infinite, a proof using this principle is called a proof by transfinite induction. One says that a set X can be well-ordered if there exists a well-order whose field includes X. An assumption which is useful in modem mathematics but about the validity of which there has been considerable controversy is the Well-Ordering Principle: every set can be well-ordered. The Well-Ordering Principle is equivalent (given the usual axioms of set theory) to the Axiom d Choice (*Multiplicative* Axiom): given any set X of non-empty pairwise disjoint sets, there is a set Y (called a choice set) which contains exactly one element in common with each set in X.

Let B be a non-empty set, f a function from B into B, and g a function from B^2 into B. Let us write x' for $f(x)$, and $x \cap y$ for $g(x, y)$. Then (B, f, g) is called a *Boolean* algebra if and only if the following conditions are satisfied:

(i) $x \, n \, y = y \cap x$ for all x, y in B.
(ii) $(x \, n \, y) \, n \, z = x \cap (y \cap z)$ for all x, y, z in B.
(iii) $x \, n \, y' = z \cap z'$ if and only if $x \cap y = x$ for any x, y, z in B.

We let $x \cup y$ stand for $(x' \cap y')'$; and we write $x \leqslant y$ for $x \cap y = x$. It is easily proved that $z \cap z' = w \cap w'$ for any w, z in B; we denote the value of $z \, n \, z'$ by 0. (The symbols ∩, ∪, 0 should not be confused with the corresponding symbols used in set theory.) We let 1 stand for 0'. Then: $z \cup z' = 1$ for all z in

B; $\leqslant$ is a reflexive partial order on B; and (B, f, $\cup$) is a Boolean algebra. ***An ideal*** in (B, f, *g*) is a non-empty subset **J** of B such that: (1) if $x \in J$ and $y \in J$, then $x \cup y \in J$, and (2) if $x \in J$ and $y \in B$, then $x \cap y \in J$. Clearly, {0} and B are ideals. An ideal different from B is called a ***proper ideal.*** A ***maximal ideal*** is a proper ideal which is included in no other proper ideal. It can be shown that a proper ideal **J** is maximal if and only if, for any u in B, $u \in J$ or $u' \in J$. From the Well-Ordering Principle (or the Axiom of Choice) it can be proved that every Boolean algebra contains a maximal ideal, or, equivalently, that every proper ideal is included in some maximal ideal. Example: let B be the set of all subsets of a set X; for Y E B, let $Y' = X - Y$, and for Y, Z in B, let $Y \cap Z$ be the ordinary set-theoretic intersection of Y and Z. Then (B, ′, $\cap$) is a Boolean algebra. The 0 of B is the empty set 0, and 1 is X. Given an element u in X, let J_u be the set of all subsets of X which do not contain u. Then J_u is a maximal ideal. For a detailed study of Boolean algebras, cf. Sikorski [1960], Halmos [1963], Mendelson [1970].

CHAPTER 1

THE PROPOSITIONAL CALCULUS

1. Propositional Connectives. Truth Tables.

Sentences may be combined in various ways to form more complicated sentences. Let us consider only ***truth-functional*** combinations, in which the truth or falsity of the new sentence is determined by the truth or falsity of its component sentences.

Negation is one of the simplest operations on sentences. Although a sentence in a natural language may be negated in many ways, we shall adopt a uniform procedure, that of placing a sign for negation, the symbol $\sim$, in front of the entire sentence. Thus, if A is a sentence, then $\sim A$ denotes the negation of A. The truth-functional character of negation is made apparent in the following ***truth table.***

A	—A
T	F
F	T

When A is true, $\sim$ A is false; when A is false, $\sim A$ is true. We use T and F to denote the ***truth values*** Truth and Falsity.

Another common truth-functional operation is ***conjunction:*** "and". The conjunction of sentences *A* and B will be designated by $A \wedge$ B and has the following truth table.

A	B	$A \wedge B$
T	T	T
F	T	F
T	F	F
F	F	F

$A \wedge B$ is true when and only when both *A* and *B* are true. *A* and B are called the ***conjuncts*** of A $\wedge$ B. Note that there are four rows in the table, corresponding to the number of possible assignments of truth values to A and *B.*

In natural languages, there are two distinct uses of "or", the inclusive and the exclusive. According to the inclusive usage, "A or B" means "A or B or both", whereas according to the exclusive usage, the meaning is "*A* or *B*, but not both". We shall introduce a special sign, $\vee$, for the inclusive connective. Its truth table is as follows:

A	B	$A \vee B$
T	T	T
F	T	T
T	F	T
F	F	F

Thus, A $\vee$ B is false when and only when both A and B are false. "A $\vee$ B" is called a disjunction, with the disjuncts A and B.

EXERCISE

1.1. Write the truth table for the exclusive usage of "or".

Another important truth-functional operation is the conditional: "If A, then *B*." Ordinary usage is unclear here. Surely, "If A, then *B*" is false when the antecedent A is true and the consequent B is false. However, in other cases, there is no well-defined truth value. For example, the following sentences would be considered neither true nor false:

(1) If $1 + 1 = 2$, then Paris is the capital of France.
(2) If $1 + 1 \neq 2$, then Paris is the capital of France.
(3) If $1 + 1 \neq 2$, then Rome is the capital of France.

Their meaning is unclear, since we are accustomed to the assertion of some sort of relationship (usually causal) between the antecedent and the consequent. We shall make the convention that "If A, then B" is false when and only when A is true and B false. Thus, sentences (1)–(3) are assumed to be true. Let us denote "If A, then B" by "A $\supset$ B". An expression "A 3 B" is called a conditional. Then $\supset$ has the following truth table:

A	B	$A \supset B$
T	T	T
F	T	T
T	F	F
F	F	T

This sharpening of the meaning of "If A, then B" involves no conflict with ordinary usage, but rather only an extension of that usage.?

†There seems to be a common non-truth-functional interpretation of "If A, then B", connected with causal laws. The sentence, "If this piece of iron is placed in water at time *t*, then the iron will dissolve", is regarded as false even in the case that the piece of iron is not placed in water at time *t*, i.e., even when the antecedent is false. Another non-truth-functional usage of "If..., then —"

A justification of the truth table for $\supset$ is the fact that we wish "If A and B, then *B*" to be true in all cases. Thus, the case in which A and B are true justifies the first line of our truth table for $\supset$, since (A and B) and B are both true. If A is false and B true, then (A and B) is false while B is true. This corresponds to the second line of the truth table. Finally, if A is false and B is false, (A and B) is false and *B* is false. This gives the fourth line of the truth table. Still more support for our definition comes from the meaning of statements such as, "For every *x*, if *x* is an odd positive integer, then x^2 is an odd positive integer." This asserts that, for every x, the statement "if x is an odd positive integer, then x^2 is an odd positive integer" is true. Now, we certainly do not want to consider cases in which x is not an odd positive integer as counterexamples to our general assertion. This provides us with the second and fourth lines of our truth table. In addition, any case in which x is an odd positive integer and x^2 is an odd, positive integer confirms our general assertion. This corresponds to the first line of the truth table.

Let us denote "A if and only if B" by "A $\equiv$ *B*". Such an expression is called a biconditional. Clearly, A $\equiv$ B is true when and only when *A* and *B* have the same truth value. Its truth table, therefore, is

A	B	$A \equiv B$
T	T	T
F	T	F
T	F	F
F	F	T

The symbols $\sim$, $\wedge$, $\vee$, $\supset$, $\equiv$ will be called propositional connectives.$ Any sentence built up by application of these connectives has a truth value which depends on the truth values of the constituent sentences. In order to make this dependence apparent, let us apply the name statement *form* to an expression built up from the statement letters, A, *B*, *C*, etc., by appropriate applications of the propositional connectives. More precisely,

(1) All statement letters (capital Roman letters) and such letters with numerical subscripts† are statement forms.

occurs in so-called counterfactual conditionals, such as, "If Sir Walter Scott had not written any novels, then there would have been no War Between the States." (This was Mark Twain's contention in *Life on the Mississippi*: "Sir Walter had so large a hand in making Southern character, as it existed before the war, that he is in great measure responsible for the war".) This sentence might be asserted to be false even though the antecedent is admittedly false. Fortunately, causal laws and counterfactual conditionals are not needed in mathematics and logic. For a clear treatment of conditionals and other connectives, cf. Quine [1951]. (The quotation from *Life on the Mississippi* was brought to my attention by Professor J. C. Owings, Jr.)

‡We shall avoid the use of quotation marks to form names, whenever this is not likely to cause confusion. Strictly speaking, the given sentence should have quotation marks around each of the connectives. Cf. Quine [1951], pages 23–27.

†For example, $A_1, A_2, A_{17}, B_{31}, C_2, \ldots$.

(2) If $\mathcal{A}$ and $\mathcal{B}$ are statement forms, then so are $(\sim \mathcal{A})$, $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \supset \mathcal{B})$, and $(\mathcal{A} \equiv \mathcal{B})$.

(3) Only those expressions are statement forms which are determined to be so by means of (1) and (2).‡

Examples of statement forms: B, (∼ C_2), (D_3 ∧ (∼ B)), ((∼ B,) ∨ B_2) ⊃ (A, A C_2)), (((∼ A) ≡ A) ≡ (C ⊃ (B V C))).

For every assignment of truth values T or F to the statement letters occurring in a statement form, there corresponds, by virtue of the truth tables for the propositional connectives, a truth value for the statement form. Thus, each statement form determines a truth function, which can be graphically represented by a truth table for the statement form. For example, the statement form (((∼ A) ∨ B) ⊃ C) has the following truth table:

A	B	C	(∼ A)	((∼ A) ∨ B)	(((∼ A) ∨ B) 3 C)
T	T	T	F	T	T
F	T	T	T	T	T
T	F	T	F	F	T
F	F	T	T	T	T
T	T	F	F	T	F
F	T	F	T	T	F
T	F	F	F	F	T
F	F	F	T	T	F

Each row represents an assignment of truth values to the letters A, B, C, and the corresponding truth values assumed by the statement forms which appear in the construction of (((∼ A) ∨ B) ⊃ C).

The truth table for ((A ≡ B) ⊃ ((∼ A) ∧ B)) is as follows:

A	B	(A ≡ B)	(--A)	((∼ A) ∧ B)	((A ≡ B) ⊃ ((∼ A) ∧ B))
T	T	T	F	F	F
F	T	F	T	T	T
T	F	F	F	F	T
F	F	T	T	F	F

‡This can be rephrased as follows: $\mathcal{C}$ is a statement form if and only if there is a finite sequence $\mathcal{A}_1, \ldots, \mathcal{A}_n$ $(n > 1)$ such that $\mathcal{A}_n = \mathcal{C}$, and if $1 < i < n$, $\mathcal{A}_i$ is either a statement letter or is a negation, conjunction, disjunction, conditional, or biconditional constructed from previous expressions in the sequence. Notice that we use script letters $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ to stand for arbitrary expressions, whereas Roman letters are being used as statement letters.

If there are *n* distinct letters in a statement form, then there are 2" possible assignments of truth values to the statement letters and, hence, 2" rows in the truth table.

EXERCISE

1.2. Construct truth tables for the statement forms ((A ⊃ B) ∨ (∼ A)) and ((A ⊃ (B 3 C)) ⊃ ((A ⊃ B) ⊃ (A ⊃ C))).

A truth table can be abbreviated by writing only the full statement form, putting the truth values of the statement letters underneath all occurrences of these letters, and writing, step by step, the truth value of each component statement form under the principal connective? of the form. As an example, for ((A ≡ B) ⊃ ((∼ A) ∧ B)), we obtain

((A	≡	B)	3	((∼	A)	∧	B))
T	T	T	F	F	T	F	T
F	F	T	T	T	F	T	T
T	F	F	T	F	T	F	F
F	T	F	F	T	F	F	F

EXERCISE

1.3. Write the abbreviated truth tables for ((A ⊃ B) ∧ A) and ((A ∨ (∼ C)) ≡ B).

1.4. Write the following sentences as statement forms, using statement letters to stand for the atomic sentences, i.e., those sentences which are not built up out of other sentences.

(a) If Mr. Jones is happy, Mrs. Jones is unhappy, and if Mr. Jones is unhappy, Mrs. Jones is unhappy.
(b) Either Sam will come to the party and Max will not, or Sam will not come to the party and Max will enjoy himself.
(c) A necessary and sufficient condition for the sheik to be happy is that he has wine, women, and song.
(d) Fiorello goes to the movies only if a comedy is playing.
(e) A sufficient condition for x to be odd is that x is prime.
(f) A necessary condition for a sequence s to converge is that s be bounded.
(g) The bribe will be paid if and only if the goods are delivered.
(h) The Giants will win the pennant unless the Dodgers win today.
(i) If x is positive, x^2 is positive.

†The *principal connective* of a statement form is the one which is applied last in constructing the form.

(2) If $\mathcal{A}$ and $\mathcal{B}$ are statement forms, then so are $(\sim \&)$, $(\mathcal{A} \wedge \mathcal{B})$, $(\mathcal{A} \vee \mathcal{B})$, $(\mathcal{A} \supset \mathcal{B})$, and $(\mathcal{A} \equiv \mathcal{B})$.

(3) Only those expressions are statement forms which are determined to be so by means of (1) and (2).‡

Examples of statement forms: B, $(\sim C_2)$, $(D_3\, A (\sim B))$, $((\sim B,) \vee B_2) \supset (A,\ A\, C_2))$, $(((\sim A) \equiv A) \equiv (C \supset (B\, V\, C)))$.

For every assignment of truth values T or F to the statement letters occurring in a statement form, there corresponds, by virtue of the truth tables for the propositional connectives, a truth value for the statement form. Thus, each statement form determines a truth ***function***, which can be graphically represented by a truth table for the statement form. For example, the statement form $(((\sim A) \vee B) \supset C)$ has the following truth table:

A	B	C	$(\sim A)$	$((\sim A) \vee B)$	$(((\sim A) \vee B) \supset C)$
T	T	T	F	T	T
F	T	T	T	T	T
T	F	T	F	F	T
F	F	T	T	T	T
T	T	F	F	T	F
F	T	F	T	T	F
T	F	F	F	F	T
F	F	F	T	T	F

Each row represents an assignment of truth values to the letters A, B, C, and the corresponding truth values assumed by the statement forms which appear in the construction of $(((--A) \vee B) \supset C)$.

The truth table for $((A \equiv B) \supset ((\sim A) \wedge B))$ is as follows:

A	B	$(A \equiv B)$	$(--A)$	$((\sim A) \wedge B)$	$((A \equiv B) \supset ((\sim A) \wedge B))$
T	T	T	F	F	F
F	T	F	T	T	T
T	F	F	F	F	T
F	F	T	T	F	F

‡This can be rephrased as follows: $\mathcal{C}$ is a statement form if and only if there is a finite sequence $\mathcal{A}_1, \ldots, \mathcal{A}_n$ $(n > 1)$ such that $\mathcal{A}_n = \mathcal{C}$, and if $1 < i < n$, $\mathcal{A}_i$ is either a statement letter or is a negation, conjunction, disjunction, conditional, or biconditional constructed from previous expressions in the sequence. Notice that we use script letters $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ to stand for arbitrary expressions, whereas Roman letters are being used as statement letters.

If there are n distinct letters in a statement form, then there are 2^n possible assignments of truth values to the statement letters and, hence, 2^n rows in the truth table.

EXERCISE

1.2. Construct truth tables for the statement forms $((A \supset B) \vee (\sim A))$ and $((A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C)))$.

A truth table can be abbreviated by writing only the full statement form, putting the truth values of the statement letters underneath all occurrences of these letters, and writing, step by step, the truth value of each component statement form under the principal connective† of the form. As an example, for $((A \equiv B)\ 3\ ((\sim A) \wedge B))$, we obtain

$((A$	$\equiv$	$B)$	$\supset$	$((\sim$	$A)$	A	$B))$
T	T	T	F	F	T	F	T
F	F	T	T	T	F	T	T
T	F	F	T	F	T	F	F
F	T	F	F	T	F	F	F

EXERCISES

1.3. Write the abbreviated truth tables for $((A \supset B) \wedge A)$ and $((A \vee (\sim C)) \equiv B)$.

1.4. Write the following sentences as statement forms, using statement letters to stand for the ***atomic sentences***, i.e., those sentences which are not built up out of other sentences.

(a) If Mr. Jones is happy, Mrs. Jones is unhappy, and if Mr. Jones is unhappy, Mrs. Jones is unhappy.
(b) Either Sam will come to the party and Max will not, or Sam will not come to the party and Max will enjoy himself.
(c) A necessary and sufficient condition for the sheik to be happy is that he has wine, women, and song.
(d) Fiorello goes to the movies only if a comedy is playing.
(e) A sufficient condition for x to be odd is that x is prime.
(f) A necessary condition for a sequence s to converge is that s be bounded.
(g) The bribe will be paid if and only if the goods are delivered.
(h) The Giants will win the pennant unless the Dodgers win today.
(i) If x is positive, x^2 is positive.

†The *principal connective* of a statement form is the one which is applied last in constructing the form.

2. Tautologies.

A ***truth function*** of n arguments is defined to be a function of n arguments, the arguments and values of which are the truth values T or F. As we have seen, any statement form determines a corresponding truth function.†

A statement form which is always true, no matter what the truth values of its statement letters may be, is called a ***tautology***. A statement form is a tautology if and only if its corresponding truth function takes only the value T, or, equivalently, if, in its truth table, the column under the statement form contains only T's. Simple examples of tautologies are $(A \vee (\sim A))$ (Law of the Excluded Middle), $(\sim (A \wedge (\sim A)))$, $(A \equiv (\sim (\sim A)))$, $((A \wedge B)\ 3\ A)$, $(A\ 3\ (A \vee B))$.

If $(\mathcal{A} \supset \mathcal{B})$ is a tautology, $\mathcal{A}$ is said to ***logically imply*** $\mathcal{B}$, or, alternatively, $\mathcal{B}$ is said to be a ***logical consequence*** of $\mathcal{A}$. For example, $(A \wedge B)$ logically implies A, $(\sim (\text{--}\ A))$ logically implies A, and $(A \wedge (A\ 3\ B))$ logically implies B.

If $(\mathcal{A} \equiv \mathcal{B})$ is a tautology, $\mathcal{A}$ and $\mathcal{B}$ are said to be ***logically equivalent.*** For example, B and $(\sim (\text{--}\ B))$ are logically equivalent, as are $(A\ 3\ B)$ and $((\text{--}A) \vee B)$.

By means of truth tables, we have effective procedures for determining whether a statement form is a tautology and for determining whether a statement form logically implies or is logically equivalent to another statement form.

EXERCISES

1.5. Determine whether the following are tautologies.

(a) $(((A \supset B) \supset B) \supset B)$
(b) $((A \equiv B) \equiv (A \equiv (B \equiv A)))$
(c) $(A\ 3\ (B \supset (B \supset A)))$
(d) $((A \wedge B)\ 3\ (A \vee C))$
(e) $((A \vee (\sim (B \wedge C))) \supset ((A \equiv C) \vee B))$
(f) $(((B \supset C)\ 3\ (A \supset B)) \supset (A \supset B))$.

†If we wish to be precise, we should enumerate all statement letters as follows $A, B, \ldots, Z, A_,, B_1, \ldots, Z_1, A_2, \ldots$. If a statement form contains the $i_1^{\text{th}}, \ldots, i_n^{\text{th}}$ statement letters in this enumeration, where $i_1 < \ldots < i_n$, then the corresponding truth function is to have $x_{i_1}, \ldots, x_{i_n}$, in that order, as its arguments, where x_{i_j} corresponds to the i_j^{th} statement letter. For example, $A \supset B$ generates the truth function

x_1	x_2	$f(x_1, x_2)$
T	T	T
F	T	T
T	F	F
F	F	T

while $B \supset A$ generates the truth function

x_1	x_2	$g(x_1, x_2)$
T	T	T
F	T	F
T	F	T
F	F	T

1.6. Verify *or disprove:*

(a) *$(A \equiv B)$ logically implies $(A \supset B)$.*
(b) *$((\sim A) \vee B)$ is logically equivalent to $((\sim B) \vee A)$.*

1.7. Show *that $\mathcal{A}$ and 93 are logically equivalent if and only if,* in *their* truth *tables, the columns under $\mathcal{A}$ and 93 are the same.*

1.8. *Which of the following statement forms are logically implied by $(A \wedge B)$?*

(a) A
(b) B
(c) $(A \vee B)$
(d) $((\sim A) \vee B)$
(e) $((\sim B) \supset A)$
(f) $(A \equiv B)$
(g) $(A\ 3\ B)$
(h) $((\sim B) \supset (\sim A))$
(i) $(A \wedge (\sim B))$

19. Same as Exercise 1.8, with $(A \wedge B)$ replaced by $(A \supset B)$.

1.10. Same as Exercise 1.8, with $(A \wedge B)$ replaced by $(A \vee B)$.

1.11. Same as Exercise 1.8, with $(A \wedge B)$ replaced by $(A \equiv B)$.

A statement form which is false for all possible truth values of its statement letters is called a ***contradiction.*** Its truth table has only F's in the column under the statement form.

Example. $(A \equiv (\sim A))$

A	--A	$(A \equiv (\sim A))$
T	F	F
F	T	F

Another example of a contradiction is $(A \wedge (\sim A))$.

Notice that a statement form $\mathcal{A}$ is a tautology if and only if $(\sim \mathcal{A})$ is a contradiction, and vice versa.

A sentence (in some natural language like English, or in a formal theory†) which arises from a tautology by substitution of sentences for all the statement letters, occurrences of the same letter being replaced by the same sentence, is said to be ***logically true*** (according to the propositional calculus). Such a sentence may be said to be true by virtue of its truth-functional structure alone. An example is the English sentence, "If it is raining or snowing, and it is not snowing, then it is raining", which arises by substitution from the tautology $(((A \vee B) \wedge (\sim B)) \supset A)$. A sentence which comes from a contradiction by means of substitution is said to be ***logically false*** (according to the propositional calculus).

†By a formal theory, we mean an artificial language in which the notions of "meaningful expression", axioms, and rules of inference are precisely described; cf. pp. 29–30.

Now let us prove a few general facts about tautologies.

PROPOSITION 1.1. ***If $\mathscr{A}$ and $(\mathscr{A} \supset \mathscr{B})$ are tautologies, then so is $\mathscr{B}$***

PROOF. Assume that $\mathscr{A}$ and $(\mathscr{A} \ni \mathscr{B})$ are tautologies. If $\mathscr{B}$ took the value F for some assignment of truth values to the statement letters of $\mathscr{A}$ and $\mathscr{B}$, then, since $\mathscr{A}$ is a tautology, $\mathscr{A}$ would take the value T, and, therefore, $(\mathscr{A} \supset \mathscr{B})$ would have the value F for that assignment. This contradicts the assumption that $(\mathscr{A} \supset 9\ )$ is a tautology. Hence $\mathscr{B}$ never takes the value F.

PROPOSITION 1.2. ***If $\mathscr{A}$ is a tautology containing as statement letters*** A,, A„ . . . , A„ ***and $\mathscr{B}$ arises from $\mathscr{A}$ by substituting statement forms $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ for $A_1, A_2, \ldots,$*** A„ ***respectively, then $\mathscr{B}$ is a tautology, i.e., substitution in a tautology yields a tautology.***

Example. Let $\mathscr{A}$ be ((A, $\wedge$ A_2) $\supset$ A,), let $\mathscr{A}_1$ be (B $\vee$ C), and let $\mathscr{A}$**,** be (C $\wedge$ D). Then $\mathscr{B}$ is (((B V C) $\wedge$ $(C \wedge D)) \supset (B$ V $C))$.

PROOF. Assume that $\mathscr{A}$ is a tautology. For any assignment of truth values to the statement letters in 9 , the forms $\mathscr{A}_1, \ldots, \mathscr{A}_n$ have truth values **x,, . . . ,** x_n (where each x_i is T or F). If we assign the values $x_1, \ldots, x_n$ to A,, . . . , A„ respectively, then the resulting truth value of $\mathscr{A}$ is the truth value of $\mathscr{B}$ for the given assignment of truth values. Since $\mathscr{A}$ is a tautology, this truth value must be T. Thus, $\mathscr{B}$ always takes the value T.

PROPOSITION 1.3. ***If $\mathscr{B}_1$ arises from $\mathscr{A}_1$ by substitution of $\mathscr{B}$ for one or more occurrences of $\mathscr{A}$, then $((\mathscr{A} \equiv 9\ ) \supset (\mathscr{A}_1 \equiv \mathscr{B}_1))$ is*** a ***tautology. Hence,*** if ***$\mathscr{A}$ and $\mathscr{B}$ are logically equivalent, then so are $\mathscr{A}_1$ and $\mathscr{B}_1$.***

PROOF. Consider any assignment of truth values to the statement letters. If $\mathscr{A}$ and $\mathscr{B}$ have opposite truth values under this assignment, then $(\mathscr{A} \equiv \mathscr{B})$ takes the value F, and so $((\mathscr{A} \equiv \mathscr{B}) \ni (\mathscr{A}_1 \equiv \mathscr{B}_1))$ is T. If $\mathscr{A}$ and 9 take the same truth values, then so do $\mathscr{A}_1$ and $\mathscr{B}_1$, since $\mathscr{B}_1$ differs from $\mathscr{A}_1$ only in containing $\mathscr{B}$ in some places where $\mathscr{A}_1$ contains $\mathscr{A}$. Hence, in this case, $(\mathscr{A} \quad \mathscr{B})$ is T, $(\mathscr{A}_1 \equiv \mathscr{B}_1)$ is T, and, therefore, $((\mathscr{A} \equiv \mathscr{B}) \supset (\mathscr{A}_1 \equiv \mathscr{B}_1))$ is T.

It would be profitable, at this point, to agree on some conventions to avoid the use of so many parentheses in writing formulas. This will make the reading of complicated expressions easier. First, we may omit the outer pair of parentheses of a statement form. (In the case of a statement letter, there is no outer pair of parentheses.) Second, when a form contains only one binary connective (namely, $\ni$, $\equiv$, $\wedge$, or $\vee$), parentheses are omitted by association to the left.

Examples. A $\supset$ B $\supset$ A $\supset$ C stands for ((A $\ni$ B) $\supset$ A) $\supset$ C, and B $\vee$ B V A $\vee$ C V A stands for ((((B $\vee$ B) $\vee$ A) $\vee$ C) $\vee$ A).

Third, the connectives are ordered as follows: , $\supset$, $\vee$, $\wedge$, $\sim$, and parentheses are eliminated according to the rule that, first, $\sim$ applies to the smallest statement form following it, then $\wedge$ is to connect the smallest statement it, then $\vee$ connects the smallest forms surrounding it, and similarly for $\ni$ and $\equiv$. In applying this rule to occurrences of the same connective, we proceed from left to right.

Examples. Parentheses are restored to A $\vee \sim$ B $\supset$ $C \equiv A$ in the following steps.

$$A \vee (\sim B) \supset C \equiv A$$
$$(A \vee (\sim B)) \supset C \equiv A$$
$$((A \vee (\sim B)) \supset C) \equiv A$$
$$(((A \vee (\sim B)) \supset C) \equiv A)$$

As an exercise, show that D $\equiv C \equiv A \wedge D \wedge$ B $\vee \sim$ D $\supset$ B stands for ((D $\equiv C) \equiv ((((A \wedge D) \wedge B)$ V $(\sim D)) \supset B))$.

Not every form can be represented without use of parentheses. For example, parentheses cannot be further eliminated from A $\supset$ (B $\supset$ C), nor from $\sim$ (A $\vee$ B), nor from A $\wedge$ (B $\ni$ C).

EXERCISES

1.12. Eliminate as many parentheses as possible from the following forms.

(a) $((B \equiv ((\sim C)$ V $(D$ A $A))) \equiv (B\ 3\ B))$
(b) $(((A$ A $(\sim B))$ A $C)$ V $D)$
(c) $((A \supset (B$ V $C))$ V $(\sim (C\ 3\ D)))$
(d) $((\sim (\sim (\sim (B$ V $C)))) \equiv (B \equiv C))$
(e) $(((A \supset B) \supset (C \supset D)) \wedge (\sim A)) \vee C)$
(f) $((A \equiv B) \equiv (\sim (C$ V $D)))$
(g) $(A$ **V** $(B$ **V** $C))$

1.13. Restore the parentheses to the forms $C\ 3 \sim (A \vee C) \wedge A \equiv B$ and **C $\supset$ A $\supset$ A $\equiv \sim$ A $\vee$ B.**

1.14. Determine whether the following expressions are abbreviations of statement forms, and, if so, restore all parentheses.

6 (b) $\sim (\sim A \equiv A) \equiv B \vee C$

(c) $A \equiv (\sim A \vee B) \supset (A \wedge (B \vee C)))$
(d) $\sim A \vee B \vee C \wedge D \equiv A \wedge \sim A$
(e) $\sim (A \supset B) \vee C \vee D \supset B$

1.15. If we write $\sim \mathscr{A}$ instead of $(\sim \mathscr{A})$; $\ni \mathscr{A}\mathscr{B}$ instead of $(\mathscr{A} \supset \mathscr{B})$; $\wedge\mathscr{A}\mathscr{B}$ **instead of** $(\mathscr{A} \wedge \mathscr{B})$; $\vee\mathscr{A}\mathscr{B}$ instead of $(\mathscr{A} \vee$ (8); and $\equiv \mathscr{A}\mathscr{B}$ instead of $(\mathscr{A} \equiv \mathscr{B})$, **then there is no** need of parentheses. For example, $((\sim A)\ 3\ (B \vee (\sim D)))$ becomes $>$ $A \vee B$ ‾ D. This way of writing forms is called ***Polish notation.***

(a) **Write** $(C$ **V** $((B \wedge (\sim D)) \supset C))$ *in* this notation.
(b) **If we count** $\supset$, $\wedge$, $\vee$, $\equiv$ each as +1, each statement letter as -1, **and** $\sim$ **as** 0, prove that an expression $\mathscr{A}$ in this parenthesis-free

notation is a statement **form** if and only if (i) **the sum** of the symbols of $\mathcal{A}$ is -1, and (ii) the sum of the symbols in any proper initial segment of $\mathcal{A}$ is non-negative.

(c) Write the statement forms of Exercise 1.12 in Polish notation.

(d) Determine whether the following expressions are statement forms in Polish notation. If so, write the statement forms in the standard way.

(i) $\sim\supset ABC \vee AB \sim C$

(ii) $\supset\supset$ AB $\supset\supset$ BC $\supset\sim AC$

(iii) $\vee\wedge\vee\sim A \sim BC \wedge \vee AC \vee \sim C \sim A$

1.16. **Determine** whether each of the following is a tautology, a contradiction, or neither.

(a) B $\equiv$ (B $\vee$ B)

(a) $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$

(c) $((A \supset B)$ A $B) \supset A$

(d) $(\sim A) \supset (A$ A $B)$

(e) A A $(\sim (A \vee B))$

(f) $(A \supset B) \equiv ((\sim A) \vee B)$

(g) $(A \supset B) \equiv \sim (A \wedge (\sim B))$

1.17. If A and B are true and C is false, what are the truth values of the following statement forms?

(a) $A \vee C$

(b) $A \wedge C$

(c) $\sim A \wedge \sim C$

(d) $A \equiv \sim B \vee C$

(e) $B \vee \sim C \supset A$

(f) $(B \vee A) \supset (B \supset \sim C)$

(g) (B $\equiv \sim$ A) $\equiv$ (A $\equiv$ C)

(h) $(B \supset A) \supset ((A \supset \sim C) \supset (\sim C \supset B))$

1.18. If A $\supset$ B is T, what can be deduced about the truth values of:

(a) $A \vee C \supset B \vee C$,

(b) $A \wedge C \supset B \wedge C$,

(c) $\sim A \wedge B \equiv A \vee B$.

1.19. What further truth values can be deduced from those already given?

(a) $\sim A \vee \left(A \underset{F}{\supset} B\right)$

(a) $\sim\left(A \underset{T}{\wedge} B\right) \equiv \sim A \vee \sim B$

(c) $(\sim A \vee B) \underset{F}{\supset} (A \supset \sim C)$

1.20. If A $\equiv$ B is F, what can be deduced about the truth values of:

(a) A A B

(a) $A \vee B$

(c) A $\supset$ B

(d) $A \wedge C \equiv B \wedge C$

1.21. Same as Exercise 1.20, except that A $\equiv$ B is assumed to be T.

1.22. What further truth values can be deduced from those given?

(a) $(A \wedge B) \underset{F}{\equiv} \left(\underset{F}{A} \vee B\right)$

(b) $(A \supset \sim B) \underset{F}{\supset} (C \supset B)$

1.23. (a) **Apply Proposition 1.2 when** $\mathcal{A}$ **is** $A_1 \supset A_1 \vee A_2$, $\mathcal{A}_1$ **is** $B \wedge D$, **and** $\mathcal{A}_2$ **is** $\sim$ B.

(b) **Apply** Proposition 1.3 when $\mathcal{A}_1$ is $(B \supset C) \vee D$, $\mathcal{A}$ is $B \supset C$, and $\mathcal{B}$ is $\sim B \vee C$.

Show that the following pairs are logically equivalent:

(a) $\sim(A \vee B)$ and $(\sim A) \wedge (\sim B)$

(b) $\sim(A \wedge B)$ and $(\sim A) \vee (\sim B)$

(c) $A \wedge (B \vee C)$ and $(A \wedge B) \vee (A \wedge C)$

(d) $A \vee (B \wedge C)$ and $(A \vee B) \wedge (A \vee C)$

(e) $A \vee (A \wedge B)$ and A

(f) $A \supset B$ and $\sim$ B >— A ($\sim$ B $\supset \sim A$ is called the contrapositive of A $\supset$ B)

(g) $(A \wedge B) \vee (\sim B)$ and $A \vee (\sim B)$

(h) A A $(A \vee B)$ and A

(i) $A \wedge B$ and $B \wedge A$

(j) $A \vee$ B and B $\vee$ A

(k) $(A \wedge B) \wedge C$ and $A \wedge (B \wedge C)$

(l) $(A \vee B) \vee C$ and $A \vee (B \vee C)$

(m) $A \equiv B$ and $B \equiv A$

(n) (A $\equiv B) \equiv C$ and $A \equiv (B \equiv C)$

(o) (A 3 B) 3 (A $\supset C)$ and (A A $B) \supset C$

1.25. Show the logical equivalence of the following pairs.

(a) (A $\wedge$ B) $\vee \sim$ B and A $\vee$ ‾ B

(b) $(A \vee B) \wedge \sim B$ and $A \wedge \sim B$

(c) $\mathfrak{T} \wedge$ A and A where 5 is a tautology

(d) $\mathfrak{T} \vee$ A and $\mathfrak{T}$ where $\mathfrak{T}$ is a tautology

(e) 4 $\wedge$ A and 5 where 4 is a contradiction

(f) $\mathfrak{F} \vee$ A and A where $\mathfrak{F}$ is a contradiction

1.26. (Duality) (a) If $\mathcal{A}$ is a statement form involving only $\sim$, $\wedge$, and $\vee$, and $\mathcal{A}'$ arises from $\mathcal{A}$ by replacing each $\wedge$ by $\vee$, and each $\vee$ by $\wedge$, show that $\mathcal{A}$ is a tautology if and only if $\sim \mathcal{A}'$ is a tautology. Prove that, if $\mathcal{A} \supset \mathcal{B}$ is a tautology, so **is** $\mathcal{B}' \supset \mathcal{A}'$, and, if $\mathcal{A} \equiv \mathcal{B}$ is a tautology, so is $\mathcal{A}' \equiv \mathcal{B}'$.

(b) Derive the logical equivalence in **1.24(d)** from that in **1.24(c).**

(c) If $\mathcal{A}$ is a statement form involving only $\sim$, $\wedge$, and $\vee$, and $\mathcal{A}^*$ results **from** $\mathcal{A}$ **by** interchanging $\wedge$ and $\vee$, and replacing every statement letter by its **negation,** show that $\mathcal{A}^*$ is logically equivalent to $\sim \mathcal{A}$. Find a statement form **logically** equivalent to the negation of (A $\vee \sim$ B) $\wedge$ A $\wedge (\sim C \vee (A$ A $C))$.

A statement form containing only the connective $\equiv$ is a tautology if and **only** if each statement letter occurs an even number of times.

(Shannon [1935]) An electric circuit containing only on-off switches **(when a switch** is on, it passes current; otherwise, not) can be represented by a **diagram in which,** next to each switch, we put a letter representing a necessary and **sufficient** condition for the switch to be on; see Fig. 1.1. The condition that a **flows** through this network can be given by a statement form: (A $\wedge$ $B) \vee$ $(C \wedge \sim A)$.

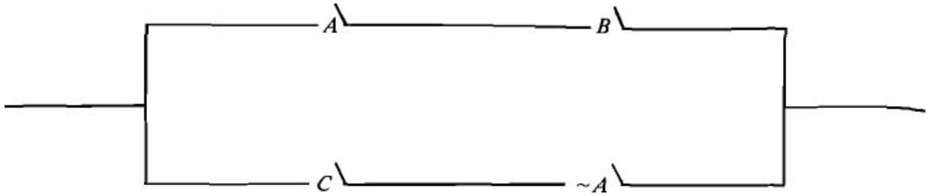


FIG. 1.1

A statement form representing the circuit shown in Fig. 1.2 is $(A \wedge B) \vee ((C \vee A) \wedge \sim B)$. Using Exercise 1.24(d, e, g, j, l), we find that this is logically equivalent to $((A \wedge B) \vee (C \vee A)) \wedge ((A \wedge B) \vee \sim B)$, which, in turn, is logically equivalent to $(((A \wedge B) \vee A) \vee C) \wedge (A \vee \sim B)$, then to $(A \vee C) \wedge (A \vee \sim B)$, and finally to $A \vee (C \wedge \sim B)$. Hence, the given circuit is equivalent to the simpler circuit shown in Fig. 1.3. (Two circuits are said to be equivalent if current flows through one if and only if it flows through the other; and one circuit is simpler if it contains fewer switches.)

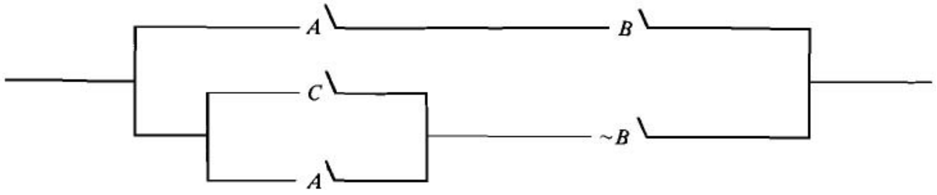


FIG. 1.2

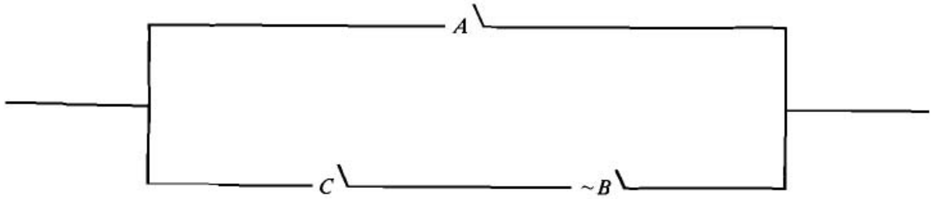


FIG. 1.3

(a) Find simpler equivalent circuits for those shown in Figs. 1.4, 1.5, and 1.6.

(b) Assume that each of the three members of a committee votes Yes on a proposal by pressing a button. Devise as simple a circuit as you can which will allow current to pass when and only when at least two of the members vote in the affirmative.

(c) We wish a light to be controlled by three different switches in a room in such a way that flicking any one of these switches will turn the light on if it is off and will turn it off if it is on. Construct a simple circuit which will do the required job.

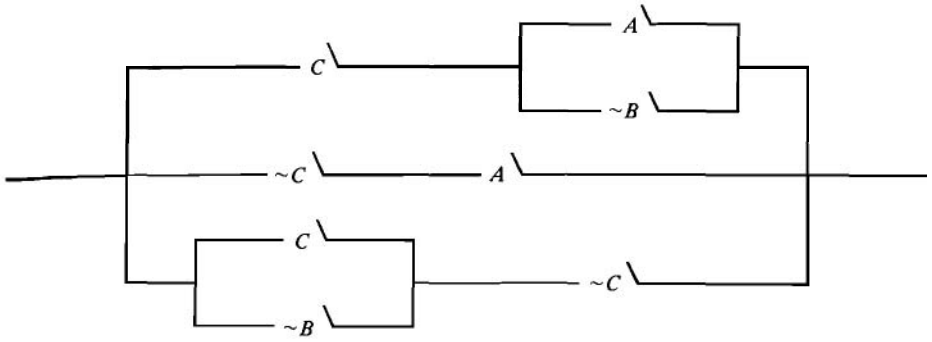


FIG. 1.4

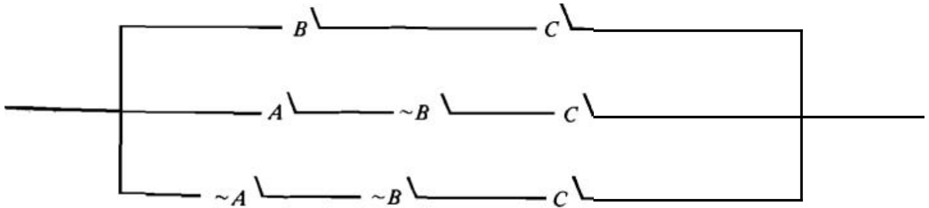


FIG. 1.5

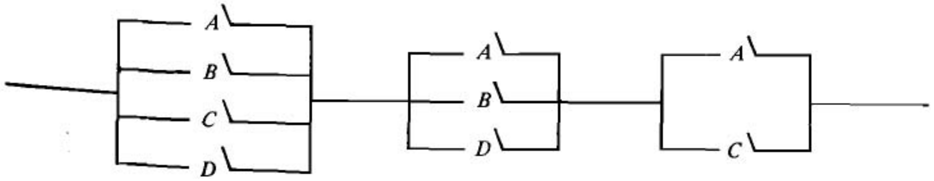


FIG. 1.6

1.29. Determine whether the following arguments are **logically correct** by representing each sentence as a statement form and checking **whether** the conclusion is logically implied by the conjunction of the assumptions.

(a) If Jones is a Communist, Jones is an atheist. Jones is an atheist. Hence, Jones is a Communist.

(b) If fallout shelters are built, other countries will feel endangered and our people will get a false sense of security. If other countries will feel endangered, they may start a preventive war. If our people will get a false sense of security, they will put less effort into preserving peace. If fallout shelters are not built, we run the risk of tremendous losses in the event of war. Hence, either other countries may start a preventive war and our people will put less effort into preserving peace, or we run the risk of tremendous losses in the event of war.

(c) If Jones did not meet Smith last night, then either Smith was the murderer or Jones is lying. If Smith was not the murderer, then Jones did not meet Smith last night and the murder took place after midnight. If the murder took place after midnight, then either Smith was the murderer or Jones is lying. Hence, Smith was the murderer.

(d) If capital investment remains constant, then government spending will increase or unemployment will result. If government spending will not increase, taxes can be reduced. If taxes can be reduced and capital investment remains constant, then unemployment will not result. Hence, government spending will increase.

130. Which of the following sets of statement forms are consistent, in the sense that there is an assignment of truth values to the statement letters which makes all of the forms in the set true?

(a) $A \supset B$
$B \equiv C$
$C \vee D \equiv \sim B$

(b) $\sim(\sim B \vee A)$
$A \vee \sim C$
B 3— C

(c) $D \supset B$
$A \vee \sim B$
$\sim(D \wedge A)$
D

1.31. Check each of the following sets of statements for consistency by representing the sentences as statement forms and then testing their conjunction to see whether it is a contradiction.

(a) Either the witness was not intimidated, or, if Doherty committed suicide, a note was found. If the witness was intimidated, then Doherty did not commit suicide. If a note was found, then Doherty committed suicide.

(b) Either love is blind and happiness is attainable or love is blind and women are smarter than men. If happiness is attainable, then love is not blind. Women are not smarter than men.

(c) If John loves Mary, Jane will marry Tom. If Jane marries Tom, Jane's father will disinherit her or Jane's mother will obtain a divorce. However, Jane's mother will not obtain a divorce.

(d) The contract is satisfied if and only if the building is completed by November 30. The building is completed by November 30 if and only if the electrical subcontractor completes his work by November 10. The bank loses money if and only if the contract is not satisfied. Yet the electrical subcontractor completes his work by November 10 if and only if the bank loses money.

3. Adequate Sets of Connectives

Every statement form containing n statement letters generates a corresponding truth function of n arguments. The arguments and values of the function are T or F. Logically equivalent forms generate the same truth function. The question naturally presents itself as to whether all truth functions are so generated.

PROPOSITION 1.4. *Every truth function is generated by a statement form involving the connectives* $\sim$, $\wedge$, *and* $\vee$.

PROOF. (Refer to Examples (a) and (b) below for clarification.) Let $f(x_1, \ldots, x_n)$ be a truth function. Clearly f can be represented by a truth table of 2^n rows, where each row represents some assignment of truth values to the variables x,, . . . , x„ followed by the corresponding value of $f(x_1, \ldots, x_n)$. If $1 < i < 2^n$, let C_i be the conjunction $U_1^i \wedge U_2^i \wedge \ldots \wedge U_n^i$, where U_j^i is A, if, in the i^{th} row of the truth table, x_j takes the value T, and U_j^i is $\sim A_j$ if x, takes the value F. Let D be the disjunction of all those C_i's such that f has the value T for the i^{th} row of the truth table. (If there are no such rows, then f always takes the value F, and we let D be A, $\wedge$ — A,, which satisfies the theorem.) As its corresponding truth function, D has f. For, let there be given an assignment of truth values to the statement letters A,, . . . , A„ and assume that the corresponding assignment to the variables x,, . . . , x, is row k of the truth table for f. Then C_k has the value T for this assignment, whereas every other C_i has the value F. If f has the value T for row k, then C_k is a disjunct of D. Hence, D would also have the value T for this assignment. If f has the value F for row k, then C_k is not a disjunct of D and all the disjuncts of D take the value F for this assignment. Therefore, D would also have the value F. Thus, D generates the truth function f.

Examples.

(a)

x_1	x_2	$f(x_1, x_2)$
T	T	F
F	T	T
T	F	T
F	F	T

D is $(\sim A_1 \wedge A_2) \vee (A_1 \wedge \sim A_2) \vee (\sim A_1 \wedge \sim A_2)$

(b)

x_1	x_2	x_3	$g(x_1, x_2, x_3)$
T	T	T	T
F	T	T	F
T	F	T	T
F	F	T	T
T	T	F	F
F	T	F	F
T	F	F	F
F	F	F	T

D is

$$(A_1 \wedge A_2 \wedge A_3) \vee (A_1 \wedge \sim A_2 \wedge A_3) \vee (\sim A_1 \wedge \sim A_2 \wedge A_3)$$
$$\vee (\sim A_1 \wedge \sim A_2 \wedge \sim A_3)$$

EXERCISES

132. Find a statement form in the connectives — , $\wedge$, and $\vee$ which has the following truth function (fx_1, x_2, x_3).

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
T	T	T	T
F	T	T	T
T	F	T	F
F	F	T	F
T	T	F	F
F	T	F	F
T	F	F	F
F	F	F	T

133. Find statement forms having the given truth tables.

A	*B*	*C*	$f(x_1, x_2, x_3)$	$g(x_1, x_2, x_3)$	$h(x_1, x_2, x_3)$
T	T	T	T	T	T
F	T	T	T	T	T
T	F	T	T	T	F
F	F	T	F	F	F
T	T	F	F	T	T
F	T	F	F	F	T
T	F	F	F	T	F
F	F	F	T	F	T

COROLLARY 1.5. *Every truth function corresponds to a statement form containing as connectives only $\wedge$ and -- , or only $\vee$ and -- , or only 3 and -- .*

PROOF. Notice that A $\vee$ B is logically equivalent to $\sim$(-- A $\wedge \sim B$). Hence, by Proposition 1.3 (second part), any statement form in $\wedge$, $\vee$, and $\sim$ is

logically equivalent to a statement form in only $\wedge$ and $\sim$ (obtained by replacing all expressions $\mathcal{A} \vee \mathcal{B}$ by $\sim(\sim \mathcal{A} \wedge \sim \mathcal{B})$). The other parts of the corollary are similar consequences of the following tautologies:

$$A \wedge B \equiv \sim (\sim A \vee \sim B)$$
$$A \vee B \equiv (\sim A) \supset B$$
$$A \wedge B \equiv \sim (A \supset \sim B)$$

We have just seen that there are certain pairs of connectives, e.g., $\sim$ and $\wedge$, in terms of which all other truth functions are definable (in the sense of Corollary 1.5). It turns out that there is a single connective, ↓ (joint denial), which will do the same job. Its truth table is

A	B	$A \downarrow B$
T	T	F
F	T	F
T	F	F
F	F	T

$A \downarrow B$ is true when and only when neither A nor B is true. Clearly, $\sim$ A $\equiv$ (AJA) and $(A \wedge$ B) $\equiv ((A \downarrow A) \downarrow (B \downarrow B))$ are tautologies. Hence, the adequacy of ↓ for the construction of all truth functions follows from Corollary 1.5.

Another connective, | (alternative denial), is also adequate for this purpose. Its truth table is

A	B	$A \mid B$
T	T	F
F	T	T
T	F	T
F	F	T

$A \mid B$ is true when and only when not both A and B are true. The adequacy of | follows from the tautologies $\sim$ A $\equiv$ (A|A) and (A $\vee$ B) $\equiv ((A|A)|(B|B))$.

PROPOSITION 1.6. ***The only binary connectives which alone are adequate for the construction of all truth functions are ↓ and |.***

PROOF. Assume that h(A, B) is an adequate connective. Now, if h(T, T) were T, then any statement form built up using only h would take the value T when all its statement letters take the value T. Hence, $\sim A$ would not be definable in terms of h. So, h(T, T) = F. Likewise, h(F, F) = T. Thus, we have the truth table

A	*B*	h(*A*, *B*)
T	T	F
F	T	
T	F	
F	F	T

If the second and third entries in the last column are F, F or T, T, then h is ↓ or |. If they are F, T, then h(*A*, B) ≡ ∼ B would be a tautology; and if they are T, F, then h(*A*, B) ≡ ∼ A is a tautology. In both cases, h would be definable in terms of ∼. But ∼ is not adequate by itself, because the only truth functions of one variable definable from it are the identity function and negation itself, whereas the truth function that is always T would not be definable.

EXERCISES

1.34. Prove that each of the pairs ɜ , ∨, and ∼ , ≡ , is not alone adequate to express all truth functions.

135. (a) Prove that A ∨ B can be expressed in terms of ⊃ alone.

(b) Prove that A ∧ B cannot be expressed in terms of ɜ alone.

(c) Prove that A ≡ B cannot be expressed in terms of ɜ alone.

1.36. (a) A statement form is said to be in ***disjunctive normal form*** if it is a disjunction consisting of one or more disjuncts, each of which is a conjunction of one or more statement letters and negations of statement letters, **e.g.**, (A ∧ ***B***) ∨ **(∼ *A* ∧ *C*), (*A* ∧ *B* ∧ ∼ *A*) ∨ (*C* ∧ ∼ *B*) ∨ (*A* ∧ ∼ *C*), *A*, *A* ∧ *B*, *A* ∨ (*B* ∧** C). A form is in ***conjunctiw normal form*** if it is a conjunction of one or more conjuncts, each of which is a disjunction of one or more statement letters and negations of statement letters. For example, the following are in conjunctive normal form: **(*B* ∨ ∼ *C*) ∧ (*A* ∨ *D*), *A* ∧ (*B* ∨ *A*) ∧ (∼ *B* ∨ *A*),** A, A A B, A V ∼ B. Note that we consider statement letters and their negations as (degenerate) conjunctions or disjunctions. The proof of Proposition **1.4** shows that every statement form $\mathcal{A}$ is logically equivalent to one in disjunctive normal form. By applying this result to ∼ $\mathcal{A}$, prove that $\mathcal{A}$ is also logically equivalent to a form in conjunctive normal form.

(b) Find logically equivalent disjunctive and conjunctive normal forms for ∼ (A ɜ B) ∨ (∼ A ∧ C) and A ≡ ((B ∧ ∼ A) ∨ C). (Suggestion: Instead of relying on Proposition 1.4, it is usually easier to use Exercise **1.24(c,** d).)

(c) Let us call a statement letter ***A*** and its negation —A ***literals*** with the letter A. A disjunctive (conjunctive) normal form is called ***full*** if no disjunct (conjunct) contains two occurrences of literals with the same letter and if a letter occumng in one disjunct (conjunct) also occurs in all the others. For example, **(*A*** A — A A ***B*)** ∨ **(*A*** A ***B*), (*B* ∧ *B* ∧ *C*) ∨ (*B* ∧ *C*), and (*B* ∧ *C*) ∨ *B* are not** full, whereas (A ∧ ∼ B) ∨ (B ∧ A) and (A ∧ B ∧ ∼ C) ∨ (A ∧ B ∧ C) ∨ (A ∧ ∼ B ∧ ∼ C) are full disjunctive normal forms. (i) Find full disjunctive and conjunctive normal forms for —(A ɜ B) ∨ (—A A C) and A ≡ ((B A ∼ A) ∨ C). (ii) Prove that every non-contradictory (non-tautologous) statement form $\mathcal{A}$ is logically equivalent to a full disjunctive (conjunctive) normal form 8, and, if $\mathcal{B}$ contains exactly ***n*** letters, then $\mathcal{A}$ is a tautology (contradiction) if and only if 4 has 2^n disjuncts (conjuncts).

(d) For each of the following, find a logically equivalent statement form in disjunctive (conjunctive) normal form, and then find logically equivalent **full** disjunctive (conjunctive) normal forms. (i) (A ∨ B) ∧ (∼ ***B*** ∨ C) (ii) ∼ A V **(*B*** ɜ — C) **(iii) (*A* ∧ ∼ *B*)** ∨ **(*A*** A C) **(iv) (*A*** ∨ B) ≡ ∼ C.

(e) Construct statement forms in ∼ and A (respectively, in ∼ and ∨, or **in → and** ⊃) logically equivalent to the statement forms in Part (d).

1.37. (a) A certain country is inhabited only by people who either always tell the **truth or al**ways tell lies, and who **will** respond to questions only with a yes or no. A **tourist comes** to a fork in the road, where one branch leads to the capital **and the other does** not. There is no sign indicating which branch to take, but there is **an inhabitant** standing at the fork. What yes-or-no question should the tourist ask **him to determine** which branch to take? (Hint: Let A stand for "You always tell **the truth", and** let B stand for "The left-hand branch leads to the capital". Construct, **by means** of a suitable truth table, a statement form involving A and B such that **the** native's answer to the question as to whether this statement form is true will be **"yes"** when and only when B is true.)

(b) In a certain country, there are three kinds of people: workers (who **always** tell the truth), capitalists **(who** never tell the truth), and students (who sometimes tell the truth and sometimes lie). At a fork in the road, one branch leads to the capital. A worker, a capitalist, and a student are standing at the side of the road, but are not identifiable by their speech or clothing. By asking two yes-or-no questions, find out which fork leads to the capital. (Each question may be addressed to any one of the three.)

4. An Axiom System for the Propositional Calculus

Truth tables enable us to answer most of the significant questions concerning the truth-functional connectives, such as whether a given statement form is a tautology, contradiction, or neither, and whether it logically implies or is logically equivalent to some other given statement form. The more complex parts of logic which we shall treat later cannot be handled by truth tables, or by any other similar effective procedure. Consequently, another approach, by **means** of formal theories, will have to be tried. Although, as we have seen, the **propositional** calculus surrenders completely to the truth table method, it will be **instructive** to illustrate the axiomatic method in this simple branch of logic.

A formal theory S is defined when the following conditions are satisfied.

(1) A countable set of **symbols**† is given as the symbols of $\mathcal{S}$. A finite **sequence of** symbols of S is called an ***expression*** of S.

(2) **There** is a subset of the expressions of S called the set of ***well-formed formulas*** (abbreviated **"wfs"**) of $\mathcal{S}$. (There is usually an effective procedure to **determine** whether a given expression is a **wf.)**

(3) A set of wfs is set aside and called the set of ***axioms*** of $\mathcal{S}$**.** (Most often, one **can effectively** decide whether a given wf is an axiom, and, in such a case, $\mathcal{S}$ is **called an** *axiomatic* theory.)

† **If desired, these** "**symbols" can be taken to be arbitrary objects rather than just linguistic objects.**

(4) There is a finite set $R_1, \ldots, R_n$ of relations among wfs, called rules *of* inference. For each R,, there is a unique positive integer **j** such that, for every set of **j** wfs and each wf $\mathcal{A}$, one can effectively decide whether the given *j* wfs are in the relation R, to $\mathcal{A}$, and, if so, $\mathcal{A}$ is called a direct consequence of the given wfs by virtue of R,.

Aproof in $\mathcal{S}$ is a sequence $\mathcal{A}_1, \ldots, \mathcal{A}_n$ of wfs such that, for each i, either $\mathcal{A}_i$ is an axiom of $\mathcal{S}$ or $\mathcal{A}_i$ is a direct consequence of some of the preceding wfs by virtue of one of the rules of inference.

A theorem of $\mathcal{S}$ is a wf $\mathcal{A}$ of $\mathcal{S}$ such that there is a proof the last wf of which is $\mathcal{A}$. Such a proof is called aproof of $\mathcal{A}$.

Even if $\mathcal{S}$ is axiomatic, **i.e.**, if there is an effective procedure for checking any given wf to see whether it is an axiom, the notion of "theorem" is not necessarily effective, since, in general, there is no mechanical method (effective procedure) for determining, given any wf $\mathcal{A}$, whether there is a proof of $\mathcal{A}$. A theory for which there is such a mechanical method is said to be decidable; otherwise, it is called undecidable. A decidable theory is, roughly speaking, one for which a machine can be devised to test wfs for theoremhood, whereas, in an undecidable theory, ingenuity is required to determine whether wfs are theorems.

A wf $\mathcal{A}$ is said to be a consequence in $\mathcal{S}$ of a set Γ of wfs if and only if there is a sequence $\mathcal{A}_1, \ldots, \mathcal{A}$, of wfs such that $\mathcal{A} = \mathcal{A}_n$ and, for each i, either $\mathcal{A}_i$ is an axiom or $\mathcal{A}_i$ is in Γ, or $\mathcal{A}_i$ is a direct consequence by some rule of inference of some of the preceding wfs in the sequence. Such a sequence is called a proof (or deduction) of $\mathcal{A}$ from Γ. The members of Γ are called the hypotheses or premisses of the proof. We use $\Gamma \vdash \mathcal{A}$ as an abbreviation for "$\mathcal{A}$ is a consequence of Γ". In order to avoid confusion when dealing with more than one theory, we write $\Gamma \vdash_{\mathcal{S}} \mathcal{A}$, adding the subscript $\mathcal{S}$ to indicate the theory in question. If Γ is a finite set $\{\mathcal{B}_1, \ldots, \mathcal{B}_n\}$, we write $\mathcal{B}_1, \ldots, \mathcal{B}_n \vdash \mathcal{A}$ instead of $\{\mathcal{B}_1, \ldots, \mathcal{B}_n\} \vdash \mathcal{A}$. If Γ is the empty set 0, then $0 \vdash \mathcal{A}$ if and only if $\mathcal{A}$ is a theorem. It is customary to omit the sign "0" and simply write $\vdash \mathcal{A}$. Thus, $\vdash \mathcal{A}$ is another way of asserting that $\mathcal{A}$ is a theorem.

The following are simple properties of the notion of consequence.

(1) If $\Gamma \subseteq$ A and $\Gamma \vdash \mathcal{A}$, then A t $\mathcal{A}$.
(2) $\Gamma \vdash \mathcal{A}$ if and only if there is a finite subset A of Γ such that $\Delta \vdash \mathcal{A}$.
(3) If A $\vdash \mathcal{A}$, and, for each $\mathcal{B}$ in A, $\Gamma \vdash \mathcal{B}$, then $\Gamma \vdash \mathcal{A}$.

Assertion (1) represents the fact that if $\mathcal{A}$ is provable from a set Γ of premisses, then, if we add still more premisses, $\mathcal{A}$ is still provable. Half of (2) follows from (1). The other half is obvious when we notice that any proof of $\mathcal{A}$ from Γ uses only a finite number of premisses from Γ. Proposition (3) is also quite simple: if $\mathcal{A}$ is provable from premisses in A, and each premiss in Δ is provable from the premisses in Γ, then $\mathcal{A}$ is provable from premisses in Γ.

now introduce a formal axiomatic theory L for the propositional calculus.

(1) The symbols of L are $\sim$, $\supset$, (,), and the letters A, with positive integers i as subscripts: A,, A_2, A_3, ... The symbols $\sim$ and $\supset$ are called *primitive* connectives, and the letters A, are called statement letters.

(2) (a) All statement letters are wfs. (b) If $\mathcal{A}$ and $\mathcal{B}$ are wfs, so are $(\sim \mathcal{A})$ and $(\mathcal{A} \supset \mathcal{B})$.† Thus, a wf of L is just a statement form built up from the statement letters A_i by means of the connectives $\sim$ and $\supset$.

(3) If $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are any **wfs** of L, then the following are axioms of L.

(Al). $(\mathcal{A} \supset (\mathcal{B} \supset \mathcal{A}))$
(A2). $((\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})) \supset ((\mathcal{A} \supset \mathcal{B}) \supset (\mathcal{A} \supset \mathcal{C})))$
(A3). $((\sim \mathcal{B} \supset \sim \mathcal{A}) \supset ((\sim \mathcal{B} \supset \mathcal{A}) \supset \mathcal{B}))$.

(4) The only rule of inference of L is *modus* ponens: $\mathcal{B}$ is a direct consequence of @ and @ $\supset$ %. We shall abbreviate application of this rule by MP.

We shall use our conventions for eliminating parentheses.

Notice that the infinite set of axioms of L is given by means of three axiom schemas **(A1)–(A3)**, each schema standing for an infinite number of axioms. One can easily check for any given wf whether or not it is an axiom; therefore, L is axiomatic. It is our intention, in setting up the system L, to obtain as theorems precisely the class of all tautologies.

We introduce other connectives by definition.

(Dl), $(\mathcal{A} \wedge \mathcal{B})$ for $\sim(\mathcal{A} \supset \sim \mathcal{B})$
(D2). $(\mathcal{A} \vee \mathcal{B})$ for $(\sim \mathcal{A}) \supset \mathcal{B}$
(D3). $(\mathcal{A} \equiv \mathcal{B})$ for(@$\supset \mathcal{B}) \wedge (\mathcal{B} \supset \mathcal{A})$.

The meaning of **D1**, for example, is that, for any wfs $\mathcal{A}$ and $\mathcal{B}$, "($\mathcal{A}$ A $\mathcal{B}$)" is an abbreviation for "$\sim(\mathcal{A} \supset \sim \mathcal{B})$".‡

† To be precise, we should add the so-called extremal clause: (c) An expression is a wf only if it can be shown to be a wf on the basis of clauses (a) and (b). This definition can be made rigorous using as a model the definition in the footnote on page 14.

‡ When we say that "$(\mathcal{A} \wedge \mathcal{B})$" is an abbreviation for "$\sim(\mathcal{A} \supset \sim \mathcal{B})$" we mean that "($\mathcal{A}$ A $\mathcal{B}$)" is to be taken as another name in the English language (or in whatever language $\mathcal{L}$ we happen to be using to talk about the theory L) for the expression "$\sim(\mathcal{A} \supset \sim \mathcal{B})$". Notice that as a name of an built up by juxtaposing various other expressions we use the expression in English (or in $\mathcal{L}$) made by juxtaposing the names of these other expressions; in addition, we use parentheses and as their own names except, of course, when this may cause confusion. For example, name of the expression (A_1 3 A_2) and "$\mathcal{B}$" is the name of the expression $(\sim A_1)$, then we use "$(\mathcal{A} \supset \mathcal{B})$" as the name of the expression ((A, 3 A_2) $\supset (\sim A_1)$). These conventions are quite and would not be noticed by most people if we had not explicitly pointed them out. For further elucidation, consult Quine's discussion of quasi-quotation (Quine [1951]); Carnap's treatment of autonymous symbols (Carnap [1934], $4, and $42); Rosser [1953], Chapter III; Suppes [1957], Chapter 6; Church [1956], Introduction and pages 74–77.

LEMMA 1.7. *For any* wf $\mathscr{A}$, $\vdash_L \mathscr{A} \supset \mathscr{A}$.

PROOF.† We shall construct a proof in L of $\mathscr{A} \supset \mathscr{A}$.

(1)	$(\mathscr{A} \supset ((\mathscr{A} \supset \mathscr{A}) \supset \mathscr{A})) \supset ((\mathscr{A} \supset (\mathscr{A} \supset \mathscr{A})) \supset (\mathscr{A} \supset @))$	(Instance of Axiom Schema A2)
(2)	$\mathscr{A} \supset ((\mathscr{A} \supset \mathscr{A}) \supset \mathscr{A})$	Axiom Schema A1
(3)	$(\mathscr{A} \supset (\mathscr{A} \supset \mathscr{A})) \supset (\mathscr{A} \supset \mathscr{A})$	From 1,2 by MP
(4)	$\mathscr{A} \supset (\mathscr{A} \supset \mathscr{A})$	Axiom Schema A1
(5)	$\mathscr{A} \supset \mathscr{A}$	From 3, 4 by MP

EXERCISE

1.38. Prove:

(a) $\vdash_L (\sim \mathscr{A}$ 3 $\mathscr{A})$ 3 $\mathscr{A}$.
(b) $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash_L \mathscr{A} \supset \mathscr{C}$.
(c) a $\supset (\mathscr{B} \supset \mathscr{C}) \vdash_L \mathscr{B} \supset$ (a $\supset \mathscr{C}$).
(d) $\vdash_L (\sim \mathscr{B} \supset \sim \mathscr{A})$ 3 $(\mathscr{A}$ 3 $\mathscr{B})$.

In mathematical arguments, one often proves a statement $\mathscr{B}$ on the assumption of some other statement $\mathscr{A}$ and then concludes that "If $\mathscr{A}$ then $\mathscr{B}$" is true. This procedure is justified for the system L by the following theorem.

PROPOSITION 1.8 (DEDUCTION THEOREM).‡ *If* Γ *is a set of* wfs, *and* $\mathscr{A}$ *and* $\mathscr{B}$ *are* wfs, *and* Γ, $\mathscr{A} \vdash \mathscr{B}$, *then* $\Gamma \vdash \mathscr{A} \supset \mathscr{B}$. *In particular, if* $\mathscr{A} \vdash \mathscr{B}$, *then* $\vdash \mathscr{A} \supset \mathscr{B}$. (Herbrand [19301.)

PROOF. Let $\mathscr{B}_1, \ldots,$ '43 be a proof of $\mathscr{B}$ from Γ u $\{\mathscr{A}\}$, where $\mathscr{B}_n = \mathscr{B}$. Let us prove, by induction on i, that $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$ for $1 \leqslant i \leqslant n$. First of all, $\mathscr{B}_1$ must be in Γ or an axiom of L or $\mathscr{A}$. By Axiom (Al), $\mathscr{B}_1 \supset (\mathscr{A} \supset \mathscr{B}_1)$ is an axiom. Hence, in the first two cases, by MP, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_1$. For the third case, when $\mathscr{B}_1$ is $\mathscr{A}$, we have $\vdash \mathscr{A} \supset \mathscr{B}_1$, by Lemma 1.7, and, therefore, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_1$.

† The word "proof" is used in two distinct senses. First, it has a precise meaning defined above as a certain kind of finite sequence of **wfs** of L. However, in another sense, it also designates certain sequences of sentences of the English language (supplemented by various technical terms) which are supposed to serve as an argument justifying some assertion about the language L (or other formal theories). In general, the language we are studying (in this case L) is called the object language, while the language in which we formulate and prove results about the object language is called the metalanguage. The metalanguage might also be formalized and made the subject of study, which we would carry out in a metametalanguage, etc. However, we shall use the English language as our (unformalized) metalanguage, although, for a substantial part of this book, we employ only a mathematically weak portion of the English language. The contrast between object language and metalanguage is also present in the study of a foreign language; for example, in a German class, German is the object language, while the metalanguage, the language we use, is English. distinction between "proof" and "metaproof" (**i.e.,** a proof in the metalanguage) leads to a distinction between theorems of the object language and ***metatheorems*** of the metalanguage. To avoid confusion, we generally use "proposition" instead of "metatheorem". The word "metamathematics" refers to the study of logical and mathematical object languages; sometimes the word is restricted to those investigations which use what appear to the metamathematician to be constructive (or so-called ***finitary***) methods.

‡ We use $\Gamma, \mathscr{A}$ t $\mathscr{B}$ to stand for $\Gamma \cup \{\mathscr{A}\}$ t $\mathscr{B}$. In general, we let $\Gamma, \mathscr{A}_1, \ldots, \mathscr{A}_n$ t 9 stand for Γ u $\{\mathscr{A}_1, \ldots, \mathscr{A}_n\}$ t 9.

This takes care of the case i = 1. Assume now that $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_k$ for all k < i. Either $\mathscr{B}_i$ is an axiom or $\mathscr{B}_i$ is in Γ, or $\mathscr{B}_i$ is $\mathscr{A}$, or $\mathscr{B}_i$ follows by **modus** ponens from some $\mathscr{B}_j$ and $\mathscr{B}_m$, where $j < i$, $m < i$, and $\mathscr{B}_m$ has the form $\mathscr{B}_j \supset \mathscr{B}_i$. In the first three cases, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$, as in the case i = 1 above. In the last case, we have, by inductive hypothesis, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_j$ and $\Gamma \vdash \mathscr{A} \supset (\mathscr{B}_j \supset \mathscr{B}_i)$. But, by Axiom (A2), $\vdash(\mathscr{A}$ 3 $(\mathscr{B}_j$ 3 $\mathscr{B}_i))$ 3 $((\mathscr{A}$ 3 $\mathscr{B}_j)$ 3 $(\mathscr{A} \supset \mathscr{B}_i))$. Hence, by **MP**,$\Gamma \vdash (\mathscr{A} \supset \mathscr{B}_j) \supset (\mathscr{A}$ 3 $\mathscr{B}_i)$, and again by MP, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$. Thus, the inductive proof is complete. The case i = n is the desired result. (**Notice** that, given a deduction of $\mathscr{B}$ from Γ and $\mathscr{A}$, the proof just given enables us to construct a deduction of $\mathscr{A} \supset \mathscr{B}$ from Γ. Also note that only Axiom Schemas **(A1)–(A2)** are used in proving the Deduction Theorem.)

COROLLARY 1.9.
(i) $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash \mathscr{A} \supset \mathscr{C}$.
(ii) $\mathscr{A} \supset (\mathscr{B}$ 3 $\mathscr{C}), \mathscr{B} \vdash \mathscr{A} \supset \mathscr{C}$.

PROOF. (i)

(a)	$\mathscr{A} \supset \mathscr{B}$	Hyp (abbreviation for "Hypothesis")
(b)	$\mathscr{B} \supset \mathscr{C}$	Hyp
(c)		Hyp
(d)	$\mathscr{B}$	(a), (c), MP
(e)	$\mathscr{C}$	(b), (d), MP

Thus, $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C}, \mathscr{A} \vdash \mathscr{C}$. So, by the Deduction Theorem, $\mathscr{A} \supset \mathscr{B}, \mathscr{B} \supset \mathscr{C} \vdash \mathscr{A} \supset \mathscr{C}$.

(ii) Exercise (Use the Deduction Theorem).

LEMMA 1.10. *For any* wfs $\mathscr{A}$, 93, *the following are theorems of L.*

(a)	$\sim\sim \mathscr{B}$ 3 $\mathscr{B}$	(e)	$(\mathscr{A}$ 3 $\mathscr{B}) \supset (\sim \mathscr{B} \supset \sim \mathscr{A})$
(b)	$\mathscr{B} \supset \sim\sim \mathscr{B}$	(f)	$\mathscr{A} \supset (\sim \mathscr{B} \supset \sim (\mathscr{A}$ 3 '43))
(c)	$\sim \mathscr{A} \supset (\mathscr{A}$ 3 3)	(g)	$(\mathscr{A} \supset \mathscr{B}) \supset ((\sim \mathscr{A} \supset \mathscr{B}) \supset \mathscr{B})$
(d)	$(\sim \mathscr{B} \supset \sim \mathscr{A}) \supset (\mathscr{A} \supset \mathscr{B})$		

PROOF.

(a) $\vdash \sim\sim \mathscr{B} \supset \mathscr{B}$

1.	$(\sim \mathscr{B} \supset \sim\sim \mathscr{B})$ 3 $((\sim \mathscr{B} \supset \sim \mathscr{B}) \supset \mathscr{B})$	Axiom (A3)
2.	$\sim \mathscr{B} \supset \sim \mathscr{B}$	Lemma 1.77
3.	$(\sim \mathscr{B} \supset \sim\sim \mathscr{B}) \supset \mathscr{B}$	1, 2, Corollary 1.9(ii)
4.	$\sim\sim \mathscr{B} \supset (\sim \mathscr{B} \supset \sim\sim \mathscr{B})$	Axiom (A1)
5.	$\sim\sim \mathscr{B} \supset \mathscr{B}$	3, 4, Corollary 1.9(i)

† Instead of writing down here the complete pmof of $\sim \mathscr{C} \supset \sim \mathscr{B}$, we simply cite Lemma 1.7. In this way we indicate how the proof of $\sim\sim \mathscr{B} \supset \mathscr{B}$ could be written down, if we wished to take the time and space to do so. This, of course, is nothing more than the ordinary application of previously obtained theorems.

(b) $\vdash \mathscr{B} \supset \sim\sim \mathscr{B}$

1.	$(\sim\sim\sim \mathscr{B} \supset \sim \mathscr{B}) \supset ((\sim\sim\sim \mathscr{B}\ 3\ \mathscr{B}) \supset \sim\sim \mathscr{B})$	Axiom (A3)
2.	$\sim\sim\sim \mathscr{B} \supset \sim \mathscr{B}$	Part (a) above
3.	$(\sim\sim\sim \mathscr{B}\ 3\ \mathscr{B}) \supset \sim\sim \mathscr{B}$	1, 2, MP
4.	$\mathscr{B} \supset (\sim\sim\sim \mathscr{B} \supset \mathscr{B})$	Axiom (Al)
5.	$\mathscr{B} \supset \sim\sim \mathscr{B}$	3, 4, Corollary 1.9(i)

(c) $\vdash \sim \mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$

1.	$\sim \mathscr{A}$	Hyp
2.	$\mathscr{A}$	Hyp
3.	$\mathscr{A} \supset (\sim \mathscr{B} \supset \mathscr{A})$	Axiom (Al)
4.	$\sim \mathscr{A} \supset (\sim \mathscr{B} \supset \sim \mathscr{A})$	Axiom (Al)
5.	$\sim \mathscr{B} \supset \mathscr{A}$	2, 3, MP
6.	$\sim \mathscr{B} \supset \sim \mathscr{A}$	1, 4, MP
7.	$(\sim \mathscr{B} \supset \sim \mathscr{A}) \supset ((\sim \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B})$	Axiom (A3)
8.	$(\sim \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B}$	6, 7, MP
9.	$\mathscr{B}$	5, 8, MP

Thus, by 1–9, $\sim \mathscr{A}, \mathscr{A} \vdash \mathscr{B}$. Therefore, by the Deduction Theorem, $\sim \mathscr{A} \vdash \mathscr{A} \supset \mathscr{B}$, and, again by the Deduction Theorem, $\vdash \sim \mathscr{A} \supset (\mathscr{A} \supset \mathscr{B})$.

(d) $\vdash (\sim \mathscr{B} \supset \sim \mathscr{A}) \supset (\mathscr{A}\ 3\ \%\ )$

1.	$\sim \mathscr{B} \supset \sim \mathscr{A}$	Hyp
2.	$\mathscr{A}$	Hyp
3.	$(\sim \mathscr{B} \supset \sim \mathscr{A}) \supset ((\sim \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B})$	Axiom (A3)
4.	$\mathscr{A}\ 3\ (\sim \mathscr{B} \supset \mathscr{A})$	Axiom (A1)
5	$(\sim \mathscr{B} \supset \mathscr{A}) \supset \mathscr{B}$	1, 3, MP
6.	$\mathscr{A} \supset \mathscr{B}$	4, 5, Corollary 1.9(i)
7.	$\mathscr{B}$	2, 6, MP

Thus, by 1–7, $\sim \mathscr{B} \supset \sim \mathscr{A}, \mathscr{A} \vdash \mathscr{B}$, and two applications of the Deduction Theorem yield the desired result.

(e) $\vdash (\mathscr{A} \supset \mathscr{B}) \supset (\sim \mathscr{B} \supset \sim \mathscr{A})$

1.	$\mathscr{A} \supset \mathscr{B}$	Hyp
2.	$\sim\sim \mathscr{A} \supset \mathscr{A}$	Part (a)
3.	$\sim\sim \mathscr{A} \supset \mathscr{B}$	1, 2, Corollary 1.9(i)
4.	$\mathscr{B} \supset \sim\sim \mathscr{B}$	Part (b)
5.	$\sim\sim \mathscr{A} \supset \sim\sim \mathscr{B}$	3, 4, Corollary 1.9(i)
6.	$(\sim\sim \mathscr{A} \supset \sim\sim \mathscr{B}) \supset (\sim \mathscr{B} \supset \sim \mathscr{A})$	Part (d)
7.	$(\sim \mathscr{B} \supset \sim \mathscr{A})$	5, 6, MP

by 1–7, $\mathscr{A} \supset \mathscr{B} \vdash \sim \mathscr{B} \supset \sim \mathscr{A}$, and, by the Deduction Theorem, (e) lows.

$\vdash \mathscr{A} \supset (\sim \mathscr{B} \supset \sim (\mathscr{A} \supset \mathscr{B}))$

Clearly, $\mathscr{A}, \mathscr{A} \supset a \vdash \mathscr{B}$ by MP. Hence, $\vdash \mathscr{A} \supset ((\mathscr{A} \supset a\ ) \supset a\ )$ by two uses of the Deduction Theorem. By Part (e), $\vdash ((\mathscr{A} \supset \mathscr{B}) \supset \mathscr{B}) \supset (\sim \mathscr{B} \supset \sim (\mathscr{A} \supset \mathscr{B}))$. Hence, using Corollary 1.9(i),

$$\vdash \mathscr{A} \supset (\sim \mathscr{B} \supset \sim (\mathscr{A} \supset \mathscr{B}))$$

(g) $\vdash (\mathscr{A} \supset \mathscr{B}) \supset ((\sim \mathscr{A} \supset \mathscr{B}) \supset \mathscr{B})$

1.	$\mathscr{A} \supset \mathscr{B}$	Hyp
2.	$\sim \mathscr{A} \supset \mathscr{B}$	Hyp
3.	$(\mathscr{A} \supset \mathscr{B}) \supset (\sim \mathscr{B} \supset \sim \mathscr{A})$	Part (e)
4.	$\sim \mathscr{B} \supset \sim \mathscr{A}$	1, 3, MP
5.	$(\sim \mathscr{A} \supset \mathscr{B}) \supset (\sim \mathscr{B} \supset \sim\sim \mathscr{A})$	Part (e)
6.	$\sim \mathscr{B} \supset \sim\sim \mathscr{A}$	2, 5, MP
7.	$(\sim \mathscr{B} \supset \sim\sim \mathscr{A}) \supset ((\sim \mathscr{B} \supset \sim \mathscr{A}) \supset \mathscr{B})$	Axiom (A3)
8.	$(\sim \mathscr{B} \supset \sim \mathscr{A}) \supset \mathscr{B}$	6, 7, MP
9.	$\mathscr{B}$	4, 8, MP

Thus, $\mathscr{A} \supset \mathscr{B}, \sim \mathscr{A} \supset \mathscr{B} \vdash \mathscr{B}$. Two applications of the Deduction Theorem yield (g).

EXERCISES

1.39. Show that the following are theorems of L.

(a) $\mathscr{A} \supset (\mathscr{A} \vee \mathscr{B})$
(b) $\mathscr{A} \supset (\mathscr{B} \vee \mathscr{A})$
(c) $\mathscr{B} \vee \mathscr{A} \supset \mathscr{A} \vee \mathscr{B}$
(d) $\mathscr{A} \wedge \mathscr{B} \supset \mathscr{A}$
(e) $\mathscr{A} \wedge \mathscr{B} \supset \mathscr{B}$
(f) $(\mathscr{A} \supset \mathscr{C}) \supset [(\mathscr{B} \supset \mathscr{C}) \supset (\mathscr{A}\ \mathrm{V}\ \mathscr{B} \supset \mathscr{C})]$
(g) $((\mathscr{A} \supset \mathscr{B}) \supset \mathscr{A}) \supset \mathscr{A}$
(h) $\mathscr{A} \supset (\mathscr{B} \supset (\mathscr{A} \wedge \mathscr{B}))$

1.40. Exhibit a complete proof in L of Lemma 1.10(c). (Hint: apply the procedure used in the proof of the Deduction Theorem to the demonstration given above of Lemma 1.10(c).) Greater fondness for the Deduction Theorem will result if the reader tries to prove Lemma 1.10 without using the Deduction Theorem.

It is our purpose to show that a wf of L is a theorem of L if and only if it is a tautology. Half of this is very easy.

Proposition 1.11. *Every theorem of* L *is a tautology.*

Proof. As an exercise, verify that all the axioms of L are tautologies. By Proposition 1.1, modus ponens leads from tautologies to other tautologies. Hence, every theorem of L is a tautology.

The following lemma is to be used in the proof that every tautology is a theorem of L.

LEMMA 1.12. *Let* $\mathscr{A}$ *be a* wf, *and let* $B_1, \ldots, B_k$ *be the statement letters occurring in* $\mathscr{A}$. *For a given assignment of truth values to* $B_1, \ldots, B_k$, *let* B_i' *be* B_i if B_i *takes the value* T; *and let* B_i' *be* $\sim B_i$ *if* B_i *takes the value* F. *Let* $\mathscr{A}'$ *be* $\mathscr{A}$, if $\mathscr{A}$ *takes the value* T *under the assignment; and let* $\mathscr{A}'$ *be* $\sim \mathscr{A}$ if $\mathscr{A}$ *takes the value* F. *Then* $B_1', \ldots, B_k' \vdash \mathscr{A}'$.

For example, let $\mathscr{A}$ be $\sim(\sim$ A, $\supset$ A,). Then, for each row of the truth table

A_2	A_5	$\sim(\sim A_2 \supset A_5)$
T	T	F
F	T	F
T	F	F
F	F	T

Lemma 1.12 asserts a corresponding deducibility relation. For instance, corresponding to the third row there is A„ $\sim A_5 \vdash \sim\sim(\sim A_2 \supset A_5)$, and, to the fourth row, $\sim A_2$, $\sim$ A, $\vdash\sim$ (-- $A_2 \supset A_5$).

PROOF. By induction on the number n of occurrences of primitive connectives in $\mathscr{A}$. (We assume $\mathscr{A}$ written without abbreviations.) If $n = 0$, then $\mathscr{A}$ is just a statement letter B,, and then the Lemma reduces to B, $\vdash$ B, and $\sim$ B, $\vdash\sim$ B,. Assume now that the Lemma holds for all $j < n$.

Case 1. $\mathscr{A}$ is $\sim \mathscr{B}$. Then $\mathscr{B}$ has fewer than n occurrences of primitive connectives.

Subcase la. Let $\mathscr{B}$ take the value T under the given truth value assignment. Then $\mathscr{A}$ takes the value F. So, $\mathscr{B}'$ is $\mathscr{B}$, and $\mathscr{A}'$ is $\sim \mathscr{A}$. By the inductive hypothesis applied to 9 , $B_1', \ldots, B_k' \vdash$ 3. Then, by Lemma 1.10(b) and MP, $B_1', \ldots, B_k' \vdash\sim\sim \mathscr{B}$. But $\sim\sim \mathscr{B}$ is $\mathscr{A}'$.

Subcase lb. Let $\mathscr{B}$ take the value F. Then $\mathscr{B}'$ is $\sim \mathscr{B}$, and $\mathscr{A}'$ is $\mathscr{A}$. By inductive hypothesis, $B_1', \ldots, B_k' \vdash\sim$ 9 . But $\sim \mathscr{B}$ is $\mathscr{A}'$.

Case 2. $\mathscr{A}$ is ($\mathscr{B} \supset \mathscr{C}$). Then $\mathscr{B}$ and $\mathscr{C}$ have fewer occurrences of primitive connectives than $\mathscr{A}$. So, by inductive hypothesis, $B_1', \ldots, B_k' \vdash \mathscr{B}'$ and $B_1', \ldots, B_k' \vdash \mathscr{C}'$.

Case 2a. $\mathscr{B}$ takes the value F. Hence, $\mathscr{A}$ takes the value T. Then $\mathscr{B}'$ is $\sim \mathscr{B}$, and $\mathscr{A}'$ is $\mathscr{A}$. So, $B_1', \ldots, B_k' \vdash\sim \mathscr{B}$. By Lemma 1.10(c), $B_1', \ldots, B_k' \vdash \mathscr{B} \supset \mathscr{C}$. But $\mathscr{B} \supset \mathscr{C}$ is $\mathscr{A}'$.

Case 2b. $\mathscr{C}$ takes the value T. Hence $\mathscr{A}$ takes the value T. Then $\mathscr{C}'$ is $\mathscr{C}$ and $\mathscr{A}'$ is $\mathscr{A}$. Now, $B_1', \ldots, B_k' \vdash \mathscr{C}$. Then, by Axiom (Al), $B_1', \ldots, B_k' \vdash \mathscr{B} \supset \mathscr{C}$. But $\mathscr{B} \supset \mathscr{C}$ is $\mathscr{A}'$.

Case 2c. $\mathscr{B}$ takes the value T and $\mathscr{C}$ the value F. Then $\mathscr{A}$ has the value F, $\mathscr{B}'$ is $\mathscr{B}$, $\mathscr{C}'$ is $\sim \mathscr{C}$, and $\mathscr{A}'$ is $\sim \mathscr{A}$. Now, $B_1', \ldots, B_k' \vdash \mathscr{B}$ and $B_1', \ldots, B_k' \vdash \sim \mathscr{C}$. So, by Lemma 1.10(f), $B_1', \ldots, B_k' \vdash\sim$ (9 $\supset \mathscr{C}$). But $\sim$(9 $\supset \mathscr{C}$) is a'.

OPOSITION 1.13 (COMPLETENESS THEOREM). *If a* wf $\mathscr{A}$ *of L is a tautology,* *it is a theorem of L.*

OOF. (Kalmár) Assume $\mathscr{A}$ a tautology, and let B,, . . . , B_k be the statement letters in @.For any truth value assignment to B,, . . . , B_k, we have, by mma 1.12, $B_1', \ldots, B_k' \vdash \mathscr{A}$. ($\mathscr{A}'$ is $\mathscr{A}$, because $\mathscr{A}$ always takes the value T.) nce, if B_k is given the value T, $B_1', \ldots, B_{k-1}', B_k \vdash \mathscr{A}$, and, if B_k is given the lue F, $B_1', \ldots, B_{k-1}', \sim B_k \vdash \mathscr{A}$. So, by the Deduction Theorem, $B_1', \ldots, B_{k-1}'$ $B_k \supset \mathscr{A}$ and $B_1', \ldots, B_{k-1}' \vdash\sim B_k \supset \mathscr{A}$. Then, by Lemma 1.10(g), I,, . . . , $B_{k-1}' \vdash \mathscr{A}$. Similarly, B_{k-1} may be chosen to be T or F, and, again applying the Deduction Theorem and Lemma 1.10(g), we can eliminate B_{k-1}' just as we eliminated B_k'. After k such steps, we finally obtain $\vdash \mathscr{A}$.

EXERCISE 1.41. $B_1 \wedge B_2 \supset B_1$ *is a tautology. By the method of the proof of Proposition* 1.13, *show that* $\vdash$ B, $\wedge B_2 \supset B_1$.

COROLLARY 1.14. *If* $\mathscr{B}$ *is an expression involving the signs* $\sim$, $\supset$, $\wedge$, $\vee$, $\equiv$ *which is an abbreviation for a* wf $\mathscr{A}$ *of* L, *then* $\mathscr{B}$ *is a tautology* if *and only* if $\mathscr{A}$ *is a theorem of L.*

PROOF. In Definitions D1–D3, the abbreviating formulas replace wfs to which they are logically equivalent. Hence, by Proposition 1.3, $\mathscr{A}$ and $\mathscr{B}$ are logically equivalent, and $\mathscr{B}$ is a tautology if and only if $\mathscr{A}$ is. The corollary now follows from Propositions 1.11 and 1.13.

COROLLARY 1.15. *The system L is consistent, i.e., there is no* wf $\mathscr{A}$ *such that both* $\mathscr{A}$ *and* $\sim \mathscr{A}$ *are theorems of L.*

PROOF. By Proposition 1.11, every theorem of L is a tautology. The negation of a tautology cannot be a tautology, and, therefore, it is impossible for both $\mathscr{A}$ and $\sim \mathscr{A}$ to be theorems of L.

Notice that L is consistent if and only if not all wfs of L are theorems. For, clearly, if L is consistent, then there are wfs which are not theorems (e.g., the negations of theorems). On the other hand, by Lemma 1.10(c), $\vdash_L \sim \mathscr{A} \supset$ ($\mathscr{A} \supset \mathscr{B}$), and so, if L were inconsistent, i.e., if some wf $\mathscr{A}$ and its negation $\sim \mathscr{A}$ were Provable, then, by MP, any wf $\mathscr{B}$ would be provable. (This equivalence holds for any theory having modus ponens as a rule of inference and in which Lemma 1.10(c) is provable.) A theory in which not all wfs are theorems is often to be *absolutely consistent,* and this definition is applicable even to theories not containing a negation sign.

EXERCISE 1.42. *Let* $\mathscr{A}$ *be a statement form which is not a tautology. Let* L^+ *be the formal theory obtained from* L *by adding as new axioms all formulas obtainable from* $\mathscr{A}$ *by substituting arbitrary statement forms for the statement letters in* $\mathscr{A}$, *the same forms being substituted for all occurrences of a statement letter. Show that* L *is inconsistent.*

5. Independence. Many-Valued Logics.

Given an axiomatic theory, a subset X of the axioms is said to be ***independent*** if some wf in X cannot be proved by means of the rules of inference from the set of those axioms not in X.

PROPOSITION 1.16. ***Each of Axiom Schemas*** (A1)–(A3) ***is independent.***

PROOF.

(a) Independence of (Al). Consider the following tables.

A	$\sim A$
0	1
1	1
2	0

A	B	$A \supset B$
0	0	0
1	0	2
2	0	0
0	1	2
1	1	2
2	1	0
0	2	2
1	2	0
2	2	0

Given any assignment of the values 0, 1, 2 to the statement letters of a wf $\mathscr{A}$, these tables determine a corresponding value of $\mathscr{A}$. If it always takes the value 0, $\mathscr{A}$ is called ***select.*** Now, modus ponens preserves selectness. Check that, if $\mathscr{A} \supset \mathscr{B}$ and $\mathscr{A}$ are select, so is $\mathscr{B}$. Verify also that all instances of Axioms (A2)–(A3) are select. Hence, any wf derivable from (A2)–(A3) by modus ponens is select. However, A, ⊃ (A, ⊃ A,), which is an instance of (Al), is not select, since it takes the value 2 when A, is 1 and A, is 2.

(b) Independence of (A2). Consider the following tables.

A	$\sim A$
0	1
1	0
2	1

A	B	$A \supset B$
0	0	0
1	0	0
2	0	0
0	1	2
1	1	2
2	1	0
0	2	1
1	2	0
2	2	0

Let us call a wf which always takes the value 0 according to these tables ***grotesque.*** Modus ponens preserves grotesqueness, and all instances of Axioms

(A1) and (A3) are grotesque. (Exercise.) However, the instance A, ⊃ (A, ∃ A_3) ⊃ ((A_1 ⊃ A_2) ⊃ (A, ⊃ A,)) of (A2) takes the value 2 when A, is 0, A, is 0, and A_3 is 1, and, therefore, is not grotesque.

(c) Independence of (A3). If $\mathscr{A}$ is any wf, let h($\mathscr{A}$) be the wf obtained by erasing all negation signs in $\mathscr{A}$. For each instance $\mathscr{A}$ of Axioms (A1)—(A2), h($\mathscr{A}$) is a tautology. Also, modus ponens preserves the property of a wf $\mathscr{A}$ that h($\mathscr{A}$) is a tautology; for, if h(& ⊃ $\mathscr{B}$) and h($\mathscr{A}$) are tautologies, then h($\mathscr{B}$) is a tautology. (Just note that h($\mathscr{A}$ ⊃ 48) is h($\mathscr{A}$) ⊃ h($\mathscr{B}$).) Hence, every wf $\mathscr{A}$ derivable from (A1)–(A2) by modus ponens has the property that h($\mathscr{A}$) is a tautology. But h((∼ A_1 ⊃ ∼ A_1) ⊃ ((∼ A_1 ⊃ A,) ⊃ A,)) is (A, ⊃ A,) ⊃ ((A_1 ∃ A_1) ⊃ A_1), which is not a tautology. Hence, (∼ A, ⊃ ∼ A_1) ⊃ ((∼ A_1 ⊃ A,) ⊃ A,), an instance of (A3), is not derivable from (A1)–(A2) by modus ponens.

EXERCISE 1.43. ***Prove the independence of Axiom Schema*** (A3) ***by constructing*** tables ***for the connectives ∼ and ⊃ .***

The idea used in the proof of independence of Axiom Schemas (A1)–(A2) may be generalized to the notion of a many-valued logic. Call the numbers 0, 1, 2, . . . , n "truth values", and let $0 \leqslant m < n$. The numbers 0, 1, . . . , m are ***called designated values.*** Take a finite number of "truth tables" representing functions from sets of the form (0, 1, . . . , $n\}^k$ into {0, 1, . . . , n). For each truth table, introduce a sign, called the corresponding ***connective.*** Using these connectives and statement letters, we may construct "statement forms", and every such statement form containing j distinct letters defines a "truth function" from {0, 1, . . . , $n\}^j$ into {0, 1, . . . , n). A statement form whose corresponding truth function takes only designated values is said to be ***exceptional.*** The numbers m, n and the basic truth tables are said to define a (finite) ***many-valued logic*** M. An axiomatic theory involving statement letters and the connectives of M is said to be ***suitable*** for M if and only if the theorems of the theory coincide with the exceptional statement forms o f M. All these notions obviously can be generalized to the case of an infinite number of truth values. If $n = 1$ and m = 0, and the truth tables are those given for ∼ and ∃ in §1, the corresponding 2-valued logic is that studied in this chapter. The exceptional wfs in this case were called tautologies. The system **L** is suitable for this logic, as proved in Propositions 1.11 and 1.13. In the proofs of the independence of Axiom Schemas (A1)–(A2), two three-valued logics were used.

EXERCISES

1.44. (McKinsey-Tarski) Consider the axiom system P in which there is exactly one binary connective *, the only rule of inference is modus ponens (i.e., $\mathscr{B}$ follows from $\mathscr{A}$ and $\mathscr{A} * \mathscr{B}$), and the axioms are all wfs of the form $\mathscr{A} * \mathscr{A}$. Show that P is not suitable for any (finite) many-valued logic.

1.45. For any (finite) many-valued logic M, prove that there is an axiomatic theory suitable for M.

Further information about many-valued logics can be gained from the monograph [1952] of Rosser and Turquette and from Rescher [1969].

6. Other Axiomatizations

Although the axiom system L is quite simple, there are many other systems which would do as well. We can use, instead of $\sim$ and 3 , any collection of primitive connectives, so long as these are adequate for the definition of all other truth-functional connectives.

Examples.

L_1: $\vee$ and $\sim$ are the primitive connectives. We use $\mathcal{A}$ 3 $\mathcal{B}$ as an abbreviation for $\sim \mathcal{A} \vee \mathcal{B}$. We have four axiom schemas: (1) $\mathcal{A} \vee \mathcal{A}$ 3 $\mathcal{A}$; (2) $\mathcal{A} \supset \mathcal{A} \vee \mathcal{B}$; (3) $\mathcal{A} \vee \mathcal{B}$ 3 % $\vee \mathcal{A}$; (4) $(\mathcal{B} \supset \mathcal{C}) \supset (\mathcal{A} \vee \mathcal{B} \supset \mathcal{A} \vee \mathcal{C})$. The only rule of inference is modus ponens. This system is developed in Hilbert-Ackermann [1950].

L_2: $\wedge$ and $\sim$ are the primitive connectives. $\mathcal{A} \supset \mathcal{B}$ is an abbreviation for $\sim(\mathcal{A}$ A $\sim \mathcal{B})$. There are three axiom schemas: (1) $\mathcal{A} \supset (\mathcal{A} \wedge \mathcal{A})$; (2) $\mathcal{A} \wedge \mathcal{B} \supset \mathcal{A}$; (3) $(\mathcal{A} \supset \mathcal{B}) \supset$ (-- $(\mathcal{B} \wedge \mathcal{C}) \supset \sim (\mathcal{C} \wedge \mathcal{A}))$. Modus ponens is the only rule. Consult Rosser [1953] for a detailed study.

L_3: This is just like our original system L except that, instead of the axiom schemas (A1)–(A3), we have three specific axioms: (1) A, ⊃ (A, ⊃ A,); (2) $(A_1$ 3 $(A_2$ 3 $A_3))$ 3 $((A_1$ 3 $A_2)$ 3 $(A_1$ 3 $A_3))$; (3) $(\sim A_2 \supset \sim A_1)$ 3 $((\sim A_2 \supset A_1) \supset$ A). In addition to modus ponens, we have a substitution rule: we may substitute any wf for all occurrences of a statement letter in a given wf.

L,: The primitive connectives are $\supset$, $\wedge$, $\vee$, and $\sim$. Modus ponens is the only rule, and we have ten axiom schemas:

(1) $\mathcal{A} \supset (\mathcal{B} \supset \mathcal{A})$
(2) $(\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})) \supset ((\mathcal{A} \supset \mathcal{B}) \supset (\mathcal{A} \supset \mathcal{C}))$
(3) $\mathcal{A} \wedge \mathcal{B} \supset \mathcal{A}$
(4) $\mathcal{A} \wedge \mathcal{B}$ 3 %
(5) $\mathcal{A} \supset (\mathcal{B} \supset (\mathcal{A} \wedge \mathcal{B}))$
(6) $\mathcal{A} \supset (\mathcal{A} \vee \mathcal{B})$
(7) $\mathcal{B} \supset (\mathcal{A} \vee \mathcal{B})$
(8) $(\mathcal{A} \supset \mathcal{C}) \supset ((\mathcal{B} \supset \mathcal{C}) \supset (\mathcal{A} \vee \mathcal{B} \supset \mathcal{C}))$
(9) $(\mathcal{A}$ 3 $\mathcal{B})$ 3 $((@ \supset \sim \mathcal{B}) \supset \sim \mathcal{A})$
(10) $\sim\sim \mathcal{A} \supset \mathcal{A}$

We define, as usual, $\mathcal{A} \equiv \mathcal{B}$ to be $(\mathcal{A} \supset \mathcal{B}) \wedge (\mathcal{B} \supset \mathcal{A})$. This system may be found in Kleene [1952].

ERCISES

1.46. (Hilbert-Ackermann [1950]). Prove the following results about the theory L_1.

(a) $\mathcal{A} \supset \mathcal{B} \vdash_{L_1} \mathcal{C}$ V $\mathcal{A} \supset \mathcal{C} \vee \mathcal{B}$
(b) $\vdash_{L_1} (\mathcal{A} \supset \mathcal{B}) \supset ((\mathcal{C} \supset \mathcal{A}) \supset (\mathcal{C} \supset \mathcal{B}))$
(c) $\mathcal{C} \supset \mathcal{A}, \mathcal{A} \supset \mathcal{B} \vdash_{L_1} \mathcal{C} \supset \mathcal{B}$
(d) $\vdash_{L_1} \mathcal{A} \supset \mathcal{A}$ (i.e., $\vdash_{L_1} \sim \mathcal{A}$ V $\mathcal{A})$
(e) $\vdash_{L_1} \mathcal{A}$ V $\sim \mathcal{A}$
(f) $\vdash_{L_1} \mathcal{A} \supset \sim\sim \mathcal{A}$
(g) $\vdash_{L_1} \sim \mathcal{B} \supset (\mathcal{B} \supset \mathcal{C})$
(h) $\vdash_{L_1} \mathcal{A} \vee (\mathcal{B}$ V $\mathcal{C}) \supset ((\mathcal{B}$ V $(\mathcal{A}$ V $\mathcal{C})) \vee \mathcal{A})$
(i) $\vdash_{L_1} (\mathcal{B} \vee (\mathcal{A} \vee \mathcal{C})) \vee \mathcal{A} \supset \mathcal{B} \vee (\mathcal{A} \vee \mathcal{C})$
(j) $\vdash_{L_1} \mathcal{A} \vee (\mathcal{B}$ V $\mathcal{C}) \supset \mathcal{B}$ V $(\mathcal{A}$ V $\mathcal{C})$
(k) $\vdash_{L_1} (\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})) \supset (\mathcal{B} \supset (\mathcal{A} \supset \mathcal{C}))$
(l) $\vdash_{L_1} (\mathcal{C} \supset \mathcal{A}) \supset ((\mathcal{A} \supset \mathcal{B}) \supset (\mathcal{C} \supset \mathcal{B}))$
(m) $\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C}), \mathcal{A} \supset \mathcal{B} \vdash_{L_1} \mathcal{A} \supset (\mathcal{A} \supset \mathcal{C})$
(n) $\mathcal{A}$ 3 (53 $\supset \mathcal{C}), \mathcal{A} \supset \mathcal{B} \vdash_{L_1} \mathcal{A} \supset \mathcal{C}$
(o) If $\Gamma, \mathcal{A} \vdash_{L_1} \mathcal{B}$, then $\Gamma \vdash_{L_1} \mathcal{A} \supset \mathcal{B}$ (Deduction Theorem)
(p) 53 $\supset \mathcal{A}, \sim \mathcal{B} \supset \mathcal{A} \vdash_{L_1} \mathcal{A}$
(q) $\vdash_{L_1} \mathcal{A}$ if and only if $\mathcal{A}$ is a tautology. (Hint: prove the analogues of Lemma 1.12 and Proposition 1.13.)

1.47. (Rosser [1953]). Prove the following assertions about the theory L_2.

(a) $\mathcal{A} \supset \mathcal{B}, \mathcal{B} \supset \mathcal{C} \vdash_{L_2} \sim(\sim \mathcal{C} \wedge \mathcal{A})$
(b) $\vdash_{L_2} \sim(\sim \mathcal{A}$ A $\mathcal{A})$
(c) $\vdash_{L_2} \sim\sim \mathcal{A} \supset \mathcal{A}$
(d) $\vdash_{L_2} \sim(\mathcal{A}$ A $\mathcal{B}) \supset (\mathcal{B} \supset \sim \mathcal{A})$
(e) $\vdash_{L_2} \mathcal{A} \supset \sim\sim \mathcal{A}$
(f) $\vdash_{L_2} (\mathcal{A}$ 3 $\mathcal{B})$ 3 (— 3$\supset \sim \mathcal{A})$
(g) $\sim \mathcal{A}$ 3—53 $\vdash_{L_2} \mathcal{B} \supset \mathcal{A}$
(h) $\mathcal{A} \supset \mathcal{B} \vdash_{L_2} \mathcal{C} \wedge \mathcal{A} \supset \mathcal{B} \wedge \mathcal{C}$
(i) $\mathcal{A} \supset \mathcal{B}, \mathcal{B} \supset \mathcal{C}, \mathcal{C} \supset \mathcal{D} \vdash_{L_2} \mathcal{A} \supset \mathcal{D}$
(j) $\vdash_{L_2} \mathcal{A}$ 3 $\mathcal{A}$
(k) $\vdash_{L_2} \mathcal{A}$ A $\mathcal{B} \supset \mathcal{B}$ A
(l) $\mathcal{A} \supset \mathcal{B}, \mathcal{B} \supset \mathcal{C} \vdash_{L_2} \mathcal{A} \supset \mathcal{C}$
(m) $\mathcal{A} \supset \mathcal{B}, \mathcal{C} \supset \mathcal{D} \vdash_{L_2} \mathcal{A} \wedge \mathcal{C} \supset \mathcal{B} \wedge \mathcal{D}$
(n) $\mathcal{B} \supset \mathcal{C} \vdash_{L_2} \mathcal{A} \wedge \mathcal{B}$
(o) $\vdash_{L_2} (\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})) \supset ((\mathcal{A}$ A $\mathcal{B}) \supset \mathcal{C})$
(p) $\vdash_{L_2} ((\mathcal{A}$ A $\mathcal{B}) \supset \mathcal{C}) \supset (\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C}))$
(q) $\mathcal{A} \supset \mathcal{B}, \mathcal{A} \supset (\mathcal{B} \supset \mathcal{C}) \vdash_{L_2} \mathcal{A} \supset \mathcal{C}$
(r) $\vdash_{L_2} \mathcal{A} \supset (\mathcal{B} \supset \mathcal{A} \wedge \mathcal{B})$
(s) $\vdash_{L_2} \mathcal{A} \supset$ (53 $\supset \mathcal{A})$
(t) If $\Gamma, \mathcal{A} \vdash_{L_2} \mathcal{B}$, then $\Gamma \vdash_{L_2} \mathcal{A} \supset \mathcal{B}$ (Deduction Theorem)
$\vdash_{L_2} (\sim \mathcal{A} \supset \mathcal{A}) \supset \mathcal{A}$
(v) $\mathcal{A} \supset \mathcal{B}, \sim \mathcal{A} \supset \mathcal{B} \vdash_{L_2} \mathcal{B}$
(w) $\vdash_{L_2} \mathcal{A}$ if and only if $\mathcal{A}$ is a tautology. (Hint: prove analogues of Lemma 1.12 and Proposition 1.13.)

1.48. Show that the theory $\mathbf{L}_3$ has the same theorems as the theory L.

1.49. (Kleene [1952]). Derive the following statements about the theory $\mathbf{L}_4$.

(a) $\vdash_{\mathrm{L}_4} \mathcal{A} \supset \mathcal{A}$

(b) If $\Gamma, \mathcal{A} \vdash_{\mathrm{L}_4} \mathcal{B}$, then $\Gamma \vdash_{\mathrm{L}_4} \mathcal{A} \supset \mathcal{B}$ (Deduction Theorem)

(c) $\mathcal{A} \supset \mathcal{B}, \mathcal{B} \supset \mathcal{C} \vdash_{\mathrm{L}_4} \mathcal{A} \supset \mathcal{C}$

(d) $\vdash_{\mathrm{L}_4} (\mathcal{A} \supset \mathcal{B}) \supset (\sim \mathcal{B} \supset \sim \mathcal{A})$

(e) $\mathcal{B}, \sim \mathcal{B} \vdash_{\mathrm{L}_4} \mathcal{C}$

(f) $\vdash_{\mathrm{L}_4} \mathcal{B} \supset \sim\sim \mathcal{B}$

(g) $\vdash_{\mathrm{L}_4} \sim \mathcal{B} \supset (\mathcal{B} \supset \mathcal{C})$

(h) $\vdash_{\mathrm{L}_4} \mathcal{B} \supset (\sim \mathcal{C} \supset \sim (\mathcal{B} \supset \mathcal{C}))$

(i) $\vdash_{\mathrm{L}_4} \sim \mathcal{B} \supset (\sim \mathcal{C} \supset \sim (\mathcal{B} \vee \mathcal{C}))$

(j) $\vdash_{\mathrm{L}_4} (\sim \mathcal{B} \supset \mathcal{A}) \supset ((\mathcal{B} \supset \mathcal{A}) \supset \mathcal{A})$

(k) $\vdash_{\mathrm{L}_4} \mathcal{A}$ if and only if $\mathcal{A}$ is a tautology. (Prove analogues of Lemma 1.12 and Proposition 1.13.)

1.50.[D] Consider the following axiomatization of the propositional **calculus** $\mathfrak{L}$ (due to Lukasiewicz). $\mathfrak{L}$ has the same wfs as our system L. Its only rule of inference is **modus ponens** (MP). Its axiom schemas are: (I) $(\sim \mathcal{A} \supset \mathcal{A}) \supset \mathcal{A}$, **(II)** $\mathcal{A} \supset (\sim \mathcal{A} \supset \mathcal{B})$, **(III)** $(\mathcal{A} \supset \mathcal{B}) \supset ((\mathcal{B} \supset \mathcal{C}) \supset (\mathcal{A} \supset \mathcal{C}))$. Prove that a wf $\mathcal{A}$ of C is provable in $\mathfrak{L}$ if and only if $\mathcal{A}$ is a tautology. (Hint: Show that C and L have the same theorems, and then use the result that the theorems of L are precisely the tautologies. However, remember that none of the results proved about L (such as Propositions 1.7–1.12) automatically carries over to C. In particular, the Deduction Theorem is not available until it is proved for $\mathfrak{L}$.)

Axiomatizations can be found for the propositional calculus which contain only one axiom schema. For example, if $\sim$ and 3 are the primitive connectives and **modus** ponens the only rule of inference, the axiom schema

$$[(((\mathcal{A} \supset \mathcal{B}) \supset (\sim \mathcal{C} \supset \sim \mathcal{D})) \supset \mathcal{C}) \supset \mathcal{E}] \supset [(\mathcal{E} \supset \mathcal{A}) \supset (\mathcal{D} \supset \mathcal{A})]$$

is sufficient (C. A. Meredith [1953]). Another single-axiom formulation, due to J. Nicod [1917], uses only alternative denial |. Its rule of inference is: $\mathcal{C}$ **follows** from $\mathcal{A}|(\mathcal{B}|\mathcal{C})$ and $\mathcal{A}$, and its axiom schema is

$$(\mathcal{A}|(\mathcal{B}|\mathcal{C}))|\{[\mathcal{D}|(\mathcal{D}|\mathcal{D})]|[(\mathcal{E}|\mathcal{B})|((\mathcal{A}|\mathcal{E})|(\mathcal{A}|\mathcal{E}))]\}.$$

Further information, including historical background, may be found in Church [1956] and in a paper by Lukasiewicz and **Tarski** [1956, IV].

EXERCISES

1.51. Show that Axiom Schema (A3) of the system L can be replaced by the schema $(\sim \mathcal{A} \supset \sim \mathcal{B}) \supset (\mathcal{B} \supset \mathcal{A})$ without altering the class of theorems.

1.52. If, in $\mathbf{L}_4$, Axiom Schema (10) is replaced by the schema **(10)′**—$\sim \mathcal{A} \supset (\mathcal{A} \supset \%)$—then the new system $\mathbf{L}_1$ is called the ***intuitionistic*** propositional **calculus.**

(a) Consider an n + 1-valued logic with these connectives: $\sim \mathcal{A}$ is **0** when $\mathcal{A}$ is n, and otherwise it is n; $\mathcal{A} \wedge \mathcal{B}$ has the maximum of the values of $\mathcal{A}$ and $\mathcal{B}$, while $\mathcal{A} \vee \mathcal{B}$ has the minimum of these values; $\mathcal{A} \supset \mathcal{B}$ is 0 if $\mathcal{A}$ has a value not less than that of $\mathcal{B}$, and, otherwise, it has the same value as $\mathcal{B}$. If we take **0** as the only designated value, show that all theorems of L_I are exceptional.

(b) $A_1 \vee \sim A_1$ and $\sim\sim$ A, $\supset A_1$ are not theorems of L,.

(c) For any m, the wf

$$(A_1 \equiv A_2) \vee \dots \vee (A_1 \equiv A_m) \vee (A_2 \equiv A_3) \vee \dots$$
$$\vee (A_2 \equiv A_m) \vee \dots \vee (A_{m-1} \equiv A_m)$$

is not a theorem of $\mathbf{L}_I$.

(d) (Gödel [1933]) $\mathbf{L}_I$ is not suitable for any finite many-valued logic.

(e) (i) If $\Gamma, \mathcal{A} \vdash_{\mathrm{L}_I} \mathcal{B}$, then $\Gamma \vdash_{\mathrm{L}_I} \mathcal{A} \supset \mathcal{B}$ (Deduction Theorem)

(ii) $\mathcal{A} \supset \mathcal{B}, \mathcal{B} \supset \mathcal{C} \vdash_{\mathrm{L}_I} \mathcal{A} \supset \mathcal{C}$

(iii) $\vdash_{\mathrm{L}_I} \mathcal{A} \supset \sim\sim \mathcal{A}$

(iv) $\vdash_{\mathrm{L}_I} (\mathcal{A} \supset \mathcal{B}) \supset (\sim \mathcal{B} \supset - \mathcal{A})$

(v) $\vdash_{\mathrm{L}_I} \mathcal{A} \supset (\sim \mathcal{A} \supset \mathcal{B})$

(vi) $\vdash_{\mathrm{L}_I} \sim\sim (\sim\sim \mathcal{A} \supset \mathcal{A})$

(vii) $\sim\sim (\mathcal{A} \supset \mathcal{B}), \sim\sim \mathcal{A} \vdash_{\mathrm{L}_I} \sim\sim \mathcal{B}$

(viii) $\vdash_{\mathrm{L}_I} \sim\sim\sim \mathcal{A} \supset \sim \mathcal{A}$

[D](f) $\vdash_{\mathrm{L}_I} \sim\sim \mathcal{A}$ if and only if $\mathcal{A}$ is a tautology.

(g) $\vdash_{\mathrm{L}_I} \sim \mathcal{A}$ if and only if $\sim \mathcal{A}$ is a tautology.

[D](h) If $\mathcal{A}$ has $\wedge$ and $\sim$ as its only connectives, $\vdash_{\mathrm{L}_I} \mathcal{A}$ if and **only** if $\mathcal{A}$ is a tautology.

For further information on intuitionist logic, cf. Heyting [1956], Kleene [1945], Jaskowski [1936]. The latter paper shows that $\mathbf{L}_I$ is suitable for a many-valued logic with denumerably many values.

1.53.[A] Let $\mathcal{A}$ and $\mathcal{B}$ be in the relation R if and only if $\vdash_{\mathrm{L}} \mathcal{A} \equiv \mathcal{B}$. Show that R is an equivalence relation. Given equivalence classes $[\mathcal{A}]$ and $[\mathcal{B}]$, let $[\mathcal{A}] \cup [\%] = [\mathcal{A}$ V $\mathcal{B}$ I, $[\mathcal{A}] \cap [\%] = [\mathcal{A} \wedge \mathcal{B}]$ and $\overline{[\mathcal{A}]} = [\sim \mathcal{A}]$. Show that the equivalence classes under R form a Boolean algebra with respect to $\cup$, $\cap$, and , called the **Lindenbaum** algebra **L★ determined** by L. The element **0** of L* is the equivalence class consisting of all contradictions (i.e., negations of tautologies). The element 1 of **L★** is the equivalence class consisting of all tautologies. Notice that $\vdash_{\mathrm{L}} \mathcal{A} \supset \mathcal{B}$ if **and only** if $[\mathcal{A}] \leqslant [\mathcal{B}]$ in L*, and that $\vdash_{\mathrm{L}} \mathcal{A} \equiv \mathcal{B}$ if and only if $[\mathcal{A}] = [\mathcal{B}]$. **Show that** a Boolean function f (built up from variables, **0** and 1, using U, $\cap$, $\overline{}$) is **equal to** the constant function 1 in all Boolean algebras if and only if $\vdash_{\mathrm{L}}$ **f#**, where **f# is** obtained from f by changing $\cup$, $\cap$, , 0, 1 into $\vee$, $\wedge$, $\sim$, A_1 A $\sim A_1$, A_1 V $\sim A_1$, respectively.

HAPTER 2

QUANTIFICATION THEORY

1. Quantifiers

There are various kinds of logical inference which obviously cannot be justified on the basis of the propositional calculus; for example:

(1) Any friend of Martin is a friend of John.
Peter is not John's friend.
Hence Peter is not Martin's friend.
(2) All men are immortal.
Socrates is a man.
Hence Socrates is immortal.
(3) All men are animals.
Hence the head of a man is the head of an animal.

The correctness of these inferences rests not only upon the truth-functional relations among the sentences involved, but also upon the internal structure of these sentences as well as upon the meaning of such expressions as "all", "any", etc.

In order to make the structure of complex sentences more transparent, it is convenient to introduce special notation to represent frequently occurring expressions. If $P(x)$ asserts that x has the property P, then $(x)P(x)$ is to mean that, for every x, property P holds, or, in other words, that everything has the property P. On the other hand, $(Ex)P(x)$ shall mean that there is an x having the property P, i.e., that there is at least one object having the property P. In $(x)P(x)$, the first "(x)" is called a *universal* quantifier; in $(Ex)P(x)$, "(Ex)" is called an existential quantifier. The study of quantifiers and related concepts is the principal subject of this chapter; hence the title "Quantification Theory".

Examples. Let m, j, p, s, $F(x, y)$, $M(x)$, $I(x)$, $A(x)$, $h(x)$ stand, respectively, for Martin, John, Peter, Socrates, x is a friend of y, x is a man, x is immortal, is an animal, and the head of x.

Then (1)–(3) above become:

(1′)
$$(x)(F(x,m) \supset F(x,j))$$
$$\frac{\sim F(p,j)}{\sim F(p,m)}$$

(2′)
$$(x)(M(x) \supset I(x))$$
$$\frac{M(s)}{I(s)}$$

(3′)
$$\frac{(x)(M(x) \supset A(x))}{(x)((Ey)(x = h(y) \text{ A } M(y)) \supset (Ey)(x = h(y) \text{ A } A(y)))}$$

Notice that the validity of these inferences does not depend upon the particular meanings of m, j, p, s, F, M, I, A, and h.

Just as statement forms were used to indicate logical structure dependent upon the propositional connectives, so also the form of inferences involving quantifiers, such as (1)–(3), can be represented abstractly, as in (1')–(3'). For this purpose, we shall use commas, parentheses, the symbols $\sim$ and $\supset$ of the propositional calculus, individual variables $x_1, x_2, \ldots, x_n, \ldots$; *individual constants* a,, $a_2, \ldots$, a,, ... ; predicate letters $A_1^1, A_1^2, \ldots, A_k^j, \ldots$; and junction letters $f_1^1, f_1^2, \ldots, f_k^j, \ldots$. The positive integer which is a superscript of a predicate or function letter indicates the number of arguments, whereas the subscript is just an indexing number to distinguish different predicate or function letters with the same number of arguments. In the examples above, m, j, p, s are individual constants, F and $=$ are binary predicate letters (i.e., letters with two arguments), M, I, A are monadic predicate letters (i.e., letters with one argument), and h is a function letter with one argument.

The function letters applied to the variables and individual constants generate the terms, that is,

(a) Variables and individual constants are terms.
(b) Iff: is a function letter, and t,, ... , t_n are terms, then $f_i^n(t_1, \ldots, t_n)$ is a term.
(c) An expression is a term only if it can be shown to be a term on the basis of clauses (a) and (b).

The predicate letters applied to terms yield the atomic jormulas, i.e., if A," is a predicate letter and t,, ... , t_n are terms, then $A_i^n(t_1, \ldots, t_n)$ is an atomic formula.

The well-formed formulas (wfs) of quantification theory are defined as follows:

(a) Every atomic formula is a wf.

(b) If $\mathcal{A}$ and $\mathcal{B}$ are wfs, and y is a variable, then $(\sim \mathcal{A})$, $(\mathcal{A} \supset \mathcal{B})$, and $((y)\mathcal{A})$ are wfs.
(c) An expression is a wf only if it can be shown to be a wf on the basis of clauses (a) and (b).

In $((y)\mathcal{A})$, "$\mathcal{A}$" is called the scope of the quantifier "(y)". Note that $\mathcal{A}$ need not contain the variable y. In that case, we ordinarily understand $((y)\mathcal{A})$ to mean the same thing as $\mathcal{A}$. The expressions $\mathcal{A}$ A $\mathcal{B}$, $\mathcal{A} \vee \mathcal{B}$, $\mathcal{A} \equiv \mathcal{B}$ are defined as in the system L of the propositional calculus (cf. page 31). It was unnecessary for us to use the symbol E as a primitive symbol, because we can define existential quantification as follows:

((Ex)@)stands for $(\sim ((x)(\sim \mathcal{A})))$

This definition is obviously faithful to the meaning of the quantifiers: $\mathcal{A}(x)$ is true for some x if and only if it is not the case that $\mathcal{A}(x)$ is false for all x.

The same conventions made in Chapter 1 as to omission of parentheses are here, with the additional convention that quantifiers (y) and (Ey) rank in strength between $\equiv$, 3 , and $\vee$, A , $\sim$.

Examples.

$$(x_1)A_1^1(x_1) \supset A_1^2(x_1, x_2) \text{ stands for } (((x_1)A_1^1(x_1)) \supset A_1^2(x_1, x_2))$$
$$(x_1)A_1^1(x_1) \text{ V } A_1^2(x_1, x_2) \text{ stands for } ((x_1)(A_1^1(x_1) \text{ V } A_1^2(x_1, x_2)))$$

EXERCISE 2.1. Restore parentheses to $(x_2) \sim A_1^1(x_1)$ 3 $A_2^3(x_1, x_1, x_2)$ V $(x_1)A_2^1(x_1)$, and to $\sim (x_1)A_1^1(x_1) \supset (Ex_2)A_2^1(x_2)$ 3 $A_1^2(x_1, x_2)$ V $A_1^1(x_2)$.

As an additional convention, we also omit parentheses around quantified formulas when they are preceded by other quantifiers.

Example.

$$(x_1)(Ex_2)(x_4)A_1^3(x_1, x_2, x_4) \text{ stands for } ((x_1)((Ex_2)((x_4)A_1^3(x_1, x_2, x_4))))$$

EXERCISES

2.2. Restore parentheses to the following.
(a) $(x_1)(x_3)(x_4)A_1^1(x_1) \supset A_2^1(x_3)$ A ‾ $A_1^1(x_1)$
(b) $(Ex_1)(x_2)(Ex_3)A_1^1(x_1)$ V $(Ex_2) \sim (x_3)A_1^2(x_3, x_2)$
(c) $(x_1)A_1^1(x_1)$ V $A_1^1(x_2)$
(d) $(x_1)A_1^1(x_1) \supset A_1^1(x_2)$
(e) $(x_1)(x_2)A_1^2(x_1, x_2) \wedge (x_1) \sim A_1^2(x_1, x_1)$
Eliminate parentheses from the following wfs, as far as is possible.
(a) $(((x_1)(A_1^1(x_1) \supset A_2^1(x_1)))$ V $((Ex_1)A_1^1(x_1)))$
(b) $((\sim ((Ex_2)(A_1^1(x_2) \vee A_1^1(a_1)))) \equiv A_1^1(x_2))$
(c) $(((x_1)(\sim (\sim A_1^1(a_3))))$ 3 $(A_1^1(x_1) \supset A_2^1(x_2)))$.

The notions of ***free*** and ***bound*** occurrences of variables in a wf are defined as follows: an occurrence of a variable x is ***bound*** in a wf if and only if either it is the variable of a quantifier "(x)" in the wf, or it is within the scope of a quantifier "(x)" in the wf. Otherwise, the ocurrence is said to be ***free*** in the wf.

Examples.

(i) $A_1^2(x_1, x_2)$
(ii) $A_1^2(x_1, x_2) \supset (x_1)A_1^1(x_1)$
(iii) $(x_1)(A_1^2(x_1, x_2) \supset (x_1)A_1^1(x_1))$

In (i), the single occurrence of x_1 is free. In (ii), the first occurrence of x_1 is free, but the second and third occurrences are bound. In (iii), all occurrences of x_1 are bound. In all three wfs, every occurrence of x_2 is free. Notice that, as in (ii), a variable may have both free and bound occurrences in a given wf. Also notice that an occurrence of a variable may be bound in some wf $\mathcal{A}$, but free in a subformula of $\mathcal{A}$. For example, the first occurrence of x, is free in (ii), but is bound in the larger wf (iii).

EXERCISES

2.4. Pick out the free and bound occurrences of variables in the following:
(a) $(x_3)(((x_1)A_1^2(x_1, x_2)) \supset A_1^2(x_3, a_1))$
(b) $(x_2)A_1^2(x_3, x_2) \supset (x_3)A_1^2(x_3, x_2)$
(c) $((x_2)(Ex_1)A_1^3(x_1, x_2, f_1^2(x_1, x_2)))$ V $\sim (x_1)A_1^2(x_2, f_1^1(x_1))$

2.5. Indicate the free and bound occurrences of all variables in the wfs of Exercises **2.2–2.3.**

A variable is said to be free (bound) in a wf if and only if it has a free (bound) occurrence in the wf. Thus, a variable may be both bound and free in the same wf, e.g., x, is bound and free in example (ii).

EXERCISES

2.6. Indicate the free variables and the bound variables in the wfs of Exercises **2.2–2.4.**

2.7. Write a wf in which x is both free and bound.

We shall often indicate that a wf & has some of the free variables $x_{i_1}, \ldots, x_{i_k}$ by writing it as $\mathcal{A}(x_{i_1}, \ldots, x_{i_k})$. This does not mean that $\mathcal{A}$ contains these variables as free variables nor does it mean that $\mathcal{A}$ does not contain other free variables. This notation is convenient because we then can agree to write as $\mathcal{A}(t_1, \ldots, t_k)$ the result of substituting in $\mathcal{A}$ the terms t,, . . . , t_k for all free occurrences (if any) of $x_{i_1}, \ldots, x_{i_k}$, respectively.

If $\mathcal{A}$ is a wf and ***t*** is a term, then t is said to be ***free for x_i in $\mathcal{A}$*** if and only if no free occurrences of x_i in $\mathcal{A}$ lie within the scope of any quantifier (x,), where x_j is a variable in t.

ples.

The term x_j is free for x_i in $A_1^1(x_i)$, but x_j is not free for x_i in $(x_j)A_1^1(x_i)$.

The term $f_1^2(x_1, x_3)$ is free for x_1 in $(x_2)A_1^2(x_1, x_2)$ 3 $A_1^1(x_1)$, but is not free for x_1 in $(Ex_3)(x_2)A_1^2(x_1, x_2) \supset A_1^1(x_1)$.

Any term containing no variables is free for any variable in any wf.

A term t is free for any variable in $\mathcal{A}$ if none of the variables of t is bound in $\mathcal{A}$.

(d) x_i is free for x_i in any wf.

(e) Any term is free for x_i in $\mathcal{A}$ if $\mathcal{A}$ contains no free occurrences of x_i.

RCISES

2.8. Is the term $f_1^2(x_1, x_2)$ free for x_1 in:
(a) $\mathrm{A}_1^2(x_1, x_2) \supset (x_2)A_1^1(x_2)$
(b) $((x_2)A_1^2(x_2, a_1))$ V $(Ex_2)A_1^2(x_1, x_2)$
(c) $(x_1)A_1^2(x_1, x_2)$
(d) $(x_2)A_1^2(x_1, x_2)$
(e) $(x_2)A_1^1(x_2) \supset A_1^2(x_1, x_2)$.

2.9. Prove the assertions made in Examples (b)–(e) above.

2.10. Translate the following sentences into wfs.
(a) All fish except sharks are kind to children.
(b) Either every wine-drinker is very communicative or some pawnbroker is honest and doesn't drink wine.
(c) Not all birds can fly.
(d) Everyone loves somebody and no one loves everybody, or somebody loves everybody and someone loves nobody.
(e) You can fool some of the people all the time, and you can fool all the people some of the time, but you can't fool all the people all the time.
(f) Some people are witty only if they are drunk.
(g) No politician is honest.
(h) If anyone can do it, Jones can.
(i) Anyone who is persistent can learn logic.
(j) If all clever philosophers are cynics and only women are clever philosophers, then, if there are any clever philosophers, some women are cynics.

2.11. Translate the following into every-day English. (Note that every-day English does not use variables.)
(a) $(x)(P(x) \supset (Ey)(C(y)$ A $(Ez)(T(z)$ A $S(x, y, z))))$, where $P(x)$ means x is a student, $C(x)$ means *x is a* course, $T(x)$ means x is a bad teacher, and $S(x, y, z)$ means x studies y with z.
(b) $(x)(y)(z)(w)([A_1^1(x) \wedge A_1^2(y, x)$ A $A_1^2(z, x)$ A $A_1^2(w, x)$ A $A_2^2(y, z)$ A $A_2^2(y, w)$ A $A_2^2(z, w)] \supset A_3^2(f_1^2(f_1^1(y), f_1^1(z)), f_1^1(w)))$, where $A_1^1(x)$ means x is a *triangle*, $A_1^2(x, y)$ means x is a side *of y*, $A_2^2(x, y)$ means $x \neq y$, $A_3^2(x, y)$ means x is greater than y, $f_1^2(x, y)$ means x + y, and $f_1^1(x)$ means the length o j x.

(c) $(v)[(Ey)A_1^2(y, v) \supset (Ex)(A_1^2(x. v) \wedge (z)(A_1^2(z, v) \supset A_2^2(x, z)))]$, where $A_1^2(x, y)$ means $x \in y$, and $A_2^2(x, y)$ means $x \leqslant y$.

(d) In the following, $A_1^1(x)$ means x is a person and $A_1^2(x, y)$ means *x loves* y.

(i) $(Ex)(A_1^1(x) \wedge (y)(A_1^1(y) \supset A_1^2(x, y)))$
(ii) $(x)(A_1^1(x) \supset (y)(A_1^1(y) \supset A_1^2(x, y)))$
(iii) $(Ey)(A_1^1(y) \wedge (Ex)(A_1^1(x) \wedge A_1^2(y, x)))$.

2. Interpretations. Satisfiability and Truth. Models.

Wfs have meaning only when an interpretation is given for the symbols. An interpretation M consists of a non-empty set D, called the domain of the interpretation, and an assignment to each predicate letter A," of an n-place relation $(A_j^n)^M$ in D, to each function letter f_j^n of an n-place operation $(f_j^n)^M$ in D (i.e., a function from D^n into D), and to each individual constant a_i of some fixed element $(a_i)^M$ of D. Given such an interpretation, variables are thought of as ranging over the set D, and $\sim$, $\supset$, and quantifiers are given their usual meaning. (Remember that an n-place relation in D can be thought of as a subset of D^n, the set of all n-tuples of elements of D. For example, if D is the set of human beings, then the relation "father of" can be identified with the set of all ordered pairs (x, y) such that x is the father of y.)

For a given interpretation, a wf without free variables (called a closed wf or a sentence) represents a proposition which is true or false, whereas a wf with free variables stands for a relation on the domain of the interpretation which may be satisfied (true) for some values in the domain of the free variables and not satisfied (false) for the others.

Examples.

(i) $A_1^2(x_1, x_2)$
(ii) $(x_2)A_1^2(x_1, x_2)$
(iii) $(Ex_2)(x_1)A_1^2(x_2, x_1)$

If we take as domain the set of positive integers and interpret $A_1^2(y, z)$ as $y \leqslant z$, then (i) represents the relation $y \leqslant z$ which is satisfied by all the ordered pairs (a, b) of positive integers such that $a \leqslant b$; (ii) represents the property (i.e., relation with one argument) "For all positive integers y, $z \leqslant y$", which is satisfied only by the integer 1; and (iii) is a true sentence asserting that there is a smallest positive integer. If we were to take as domain the set of all integers, then (iii) would be false.

EXERCISES

2.12. For the following wfs 1–3 and for the following interpretations, indicate for what values the wfs are satisfied (if they contain free variables) or whether they are true or false (if they contain no free variables).

$A_1^2(f_1^2(x_1, x_2), a_1)$
$A_1^2(x_1, x_2) \supset A_1^2(x_2, x_1)$
$(x_1)(x_2)(x_3)(A_1^2(x_1, x_2) \supset (A_1^2(x_2, x_3) \supset A_1^2(x_1, x_3)))$

) The domain is the set of positive integers, $A_1^2(y, z)$ is $y \geqslant z$, $f_1^2(y, z)$ is $y \cdot z$, a_1 is 1.

b) The domain is the set of human beings, $A_1^2(y, z)$ is "y loves z", $f_1^2(y, z)$ is z, a_1 is Hitler.

(c) The domain is the set of all sets of integers, $A_1^2(y, z)$ is $y \supseteq z$, $f_1^2(y, z)$ is $y \cup z$, and a_1 is the empty set 0.

2.13. Describe in every-day English the assertions determined by the following wfs and interpretations.

(a) $(x)(y)(A_1^2(x, y) \supset (Ez)(A_1^1(z)$ A $A_1^2(x, z)$ A $A_1^2(z, y)))$, where the domain D is the set of real numbers, $A_1^2(x, y)$ means $x < y$, and $A_1^1(z)$ means z is a rational number.

(b) $(x)(A_1^1(x) \supset (Ey)(A_2^1(y)$ A $A_1^2(y, x)))$, where D is the set of all days and people, $A_1^1(x)$ means x is a day, $A_2^1(y)$ means y is a sucker, and $A_1^2(y, x)$ means y is born on day x.

(c) In the following wfs, D is the set of integers, and $A_1^2(u, u)$ means $u < u$.

(i) $(x)(Ey)A_1^2(x, y)$
(ii) $(Ey)(x)A_1^2(x, y)$
(iii) $(x)(Ey)(A_1^2(x, y)$ A $\sim(Ez)(A_1^2(x, z)$ A $A_1^2(z, y)))$.

(d) In the following wfs, D is the set of all people, and $A_1^2(u, v)$ means u *loves* u.

(i) $(Ex)(y)A_1^2(x, y)$
(ii) $(y)(Ex)A_1^2(x, y)$
(iii) $(Ex)((y)((z)A_1^2(y, z) \supset A_1^2(x, y)))$
(iv) $(Ex)(y) \sim A_1^2(x, y)$.

The notions of satisfiability and truth are intuitively clear, but, for the skeptical, they can be made precise in the following way. (Tarski [1936]) Let there be given an interpretation M with domain D. Let Σ be the set of denumerable sequences of elements of D. We shall define what it means for a sequence $s = (b_1, b_2, \ldots)$ in Σ to satisfy a wf $\mathscr{A}$ in M. As a preliminary step we define a function s* of one argument, with terms as arguments and values in D.

(1) If t is x_i, let $s^*(t)$ be b_i.

(2) If t is an individual constant, then $s^*(t)$ is the interpretation in D of this constant.

If f_j^n is a function letter and $(f_j^n)^M$ is the corresponding operation in D, and t,, . . .', t_n are terms, then $s^*(f_j^n(t_1, \ldots, t_n)) = (f_j^n)^M(s^*(t_1), s^*(t_2), \ldots, s^*(t_n))$.

Thus, s* is a function, determined by the sequence s, from the set of terms into **D.** Intuitively, for a sequence s = (b,, b_2, . . .) and a term t, $s^\star(t)$ is the element of **D** obtained by substituting, for each i, b_i for all occurrences of x_i in t, and then performing the operations of the interpretation corresponding to the function letters of t. For instance, if t is $f_2^2(x_3, f_1^2(x_1, a,))$, and the interpretation has the set of integers as its domain, f_2^2 and f_1^2 are interpreted as ordinary multiplication and addition, and a, is interpreted as 2, then, for any sequence s = (b_1, b_2, . . .) of integers, $s^\star(t)$ is the integer $b_3 \times (b_1 + 2)$.

Now we proceed to the definition proper, which is an inductive definition.

(i) If $\mathcal{A}$ is an atomic wf $A_j^n(t_1, \ldots, t_n)$ and $(A_j^n)^M$ is the corresponding relation of the interpretation, then the sequence s satisfies $\mathcal{A}$ if and only if $(A_j^n)^M(s^\star(t_1), \ldots, s^\star(t_n))$, i.e., if the n-tuple $(s^\star(t_1), \ldots, s^\star(t_n))$ is in the relation $(A_j^n)^M$.†

(ii) s satisfies $\sim \mathcal{A}$ if and only if s does not satisfy $\mathcal{A}$.

(iii) s satisfies $\mathcal{A} \supset \mathcal{B}$ if and only if either s does not satisfy $\mathcal{A}$ or s satisfies '3.

(iv) s satisfies $(x_i)\mathcal{A}$ if and only if every sequence of Σ which differs from s in at most the i^{th} component satisfies $\mathcal{A}$.

Intuitively, a sequence s = (b,, b_2, . . .) satisfies a wf $\mathcal{A}$ if and only if, when we substitute, for each i, a symbol representing b_i for all free occurrences of x_i in $\mathcal{A}$, the resulting proposition is true under the given interpretation.

Definitions. A wf $\mathcal{A}$ is true for the interpretation M (written $\models_M \mathcal{A}$) if and only if every sequence in Σ satisfies $\mathcal{A}$.

$\mathcal{A}$ is false for M if and only if no sequence in Σ satisfies $\mathcal{A}$.

An interpretation M is said to be a *model* for a set Γ of wfs if and only if every wf in Γ is true for M.

Verification of the following consequences of the definitions above is left to the reader. Most of the results are also obvious if one wishes to use only the ordinary intuitive understanding of the notions of truth and satisfaction.

(I) $\mathcal{A}$ is false for a given interpretation M if and only if $\models_M \sim \mathcal{A}$; and $\models_M \mathcal{A}$ if and only if $\sim \mathcal{A}$ is false for M.

† For example, if the domain of the interpretation is the set of real numbers, the interpretation of A_1^2 is the relation $<$ and the interpretation of $f_1^1(x)$ is e^x, then a sequence s = (b_1, b_2, . . .) of real numbers satisfies $A_1^2(f_1^1(x_2), x_5)$ if and only if $e^{b_2} <$ b,. If the domain is the set of points in a plane, the interpretation of $A_1^3(x, y, z)$ is "x and y are equidistant from z", and the interpretation of $f_1^2(x, y)$ is "the midpoint of the line segment connecting x and y", then a sequence s = (b_1, b_2, . . .) of points in the plane satisfies $A_1^3(f_1^2(x_1, x_2), f_1^2(x_3, x_1), x_4)$ if and only if the midpoint of the line segment between b_1 and b_2 is at the same distance from b_4 as the midpoint of the line segment between b, and b_1. If the domain is the set of integers, the interpretation of $A_1^4(x, y, u, v)$ is "x . v = u . y", and the interpretation of a, is 2, then a sequence s = (b,, b_2, . . .) of integers satisfies $A_1^4(x_3, a,, x,, x_3)$ if and only if $(b_3)^2 = 2b_1$.

(II) It is not the case that both $\models_M \mathcal{A}$ and $\models_M \sim \mathcal{A}$, that is, no wf can be both true and false for M.

(III) If $\models_M \mathcal{A}$ and $\models_M \mathcal{A}$ 3 '3, then $\models_M \mathcal{B}$.

(IV) $\mathcal{A} \supset \mathcal{B}$ is false for M if and only if $\models_M \mathcal{A}$ and $\models_M \sim \mathcal{B}$.

(M) (i) A sequence s satisfies $\mathcal{A} \wedge \mathcal{B}$ if and only if s satisfies $\mathcal{A}$ and s satisfies 9. A sequence s satisfies $\mathcal{A} \vee \mathcal{B}$ if and only if s satisfies $\mathcal{A}$ or s satisfies $\mathcal{B}$. A sequence s satisfies $\mathcal{A} \equiv \mathcal{B}$ if and only if s satisfies both $\mathcal{A}$ and $\mathcal{B}$ or s satisfies neither $\mathcal{A}$ nor $\mathcal{B}$†.

(ii) A sequence s satisfies $(Ex_i)\mathcal{A}$ if and only if there is a sequence s' which differs from s in at most the i^{th} place such that s′ satisfies $\mathcal{A}$.†

(VI) $\models_M \mathcal{A}$ if and only if $\models_M (x_i)\mathcal{A}$. We can extend this result in the following way. By the closure of $\mathcal{A}$ we mean the closed wf obtained from $\mathcal{A}$ by prefixing as universal quantifiers those variables, in order of decreasing subscripts, which are free in $\mathcal{A}$. If $\mathcal{A}$ has no free variables, the closure of $\mathcal{A}$ is defined to be $\mathcal{A}$ itself. For example, if $\mathcal{A}$ is $A_1^2(x_2, x,) \supset \sim (Ex_2)A_1^3(x_1, x_2, x,)$, its closure is $(x_5)(x_3)(x_2)(x_1)\mathcal{A}$. It follows from (VI) that a wf & is true if and only if its closure is true.

(VII) Every instance of a tautology is true for any interpretation. (An instance of a statement form is a wf obtained from the statement form by substituting wfs for all statement letters, all occurrences of the same statement letter being replaced by the same wf. For example, an instance of A, ⊃ ‾ A, ∨ A, is $A_1^2(x_1, x_2) \supset (\sim (x_1)A_1^1(x_1)) \vee A_1^2(x_1, x_2)$.) To prove (VII), show that all instances of the axioms of L are true, and then use (III) and Proposition 1.13.

(VIII) If the free variables (if any) of a wf $\mathcal{A}$ occur in the list $x_{i_1}, \ldots,$: t_h, and if the sequences s and s· have the same components in the $i_1^{th}, \ldots,$ I, places, then s satisfies $\mathcal{A}$ if and only if s′ satisfies $\mathcal{A}$. (Hint: induction on the number of connectives and quantifiers in $\mathcal{A}$. First prove: Lemma. If the variables in a term t occur in the list $x_{i_1}, \ldots, x_{i_k}$, and if s and s· have the same components in the $i_1^{th}, \ldots, i_k^{th}$ places, then $s^\star(t) = (s')^\star(t)$. In particular, if t contains no variables at all, $s_1^\star(t) = s_2^\star(t)$ for any sequences s_1 and s_2.)

Although, by (VIII), a particular wf $\mathcal{A}$ with k free variables is essentially satisfied or not only by k-tuples, rather than by denumerable sequences, it is more convenient for a general treatment of satisfiability to deal with infinite rather than finite sequences. If we were to define satisfiability using finite sequences, clauses (iii) and (iv) of the definition of satisfiability would become much more complicated.

The set of k-tuples $(b_{i_1}, \ldots, b_{i_k})$ of the domain **D** such that any sequence with $b_{i_1}, \ldots, b_{i_k}$ in its $i_1^{th}, \ldots, i_k^{th}$ places, respectively, satisfies a wf $\mathcal{A}$ having $x_{i_1}, \ldots, x_{i_k}$ as its only free variables, is called the relation (or property) of the

† Remember that $\mathcal{A} \wedge$ 9, $\mathcal{A} \vee$ 9, $\mathcal{A} \equiv$ 9, $(Ex_i)\mathcal{A}$ are abbreviations for $\sim (\mathcal{A} \supset$ ‾ $\mathcal{B})$, $\sim \mathcal{A} \supset$ 9, $(\mathcal{A} \supset$ 9 $) \wedge (\mathcal{B} \supset B)$, $\sim (x_i) \sim \mathcal{A}$, respectively.

interpretation associated with $\mathscr{A}$. Extending our terminology, we shall say that every k-tuple $(b_{i_1}, \ldots, b_{i_k})$ in this relation satisfies $\mathscr{A}(x_{i_1}, \ldots, x_{i_k})$ in the interpretation M; this will be written as $\models_M \mathscr{A}[b_{i_1}, \ldots, b_{i_k}]$.

Examples.

(1) If the domain D of M is the set of human beings, $A_1^2(x, y)$ is interpreted as "x is a brother of y", and $A_2^2(x, y)$ is interpreted as "x is a parent of y", then the binary relation on D corresponding to the wf $\mathscr{A}(x_1, x_2)$: $(Ex_3)(A_1^2(x_1, x_3) \wedge A_2^2(x_3, x_2))$ is the relation of unclehood. $\models_M \mathscr{A}[b, c]$ when and only when b is an uncle of c.

(2) If the domain is the set of positive integers, A_1^2 is interpreted as $=$, f_1^2 is interpreted as multiplication, and a, is interpreted as 1, then the wf $\mathscr{B}$(x,):

$$\sim A_1^2(x_1, a_1) \wedge (x_2)((Ex_3)A_1^2(x_1, f_1^2(x_2, x_3)) \supset A_1^2(x_2, x_1) \vee A_1^2(x_2, a_1))$$

determines the property of being a prime number. Thus, $\models_M \mathscr{B}[k]$ if and only if k is a prime number.

(IX) If $\mathscr{A}$ is a closed wf, then, for any interpretation M, either $\models_M \mathscr{A}$ or $\models_M \sim \mathscr{A}$, that is, either $\mathscr{A}$ is true for M or $\mathscr{A}$ is false for M. (Hint: Use (VIII).) Of course, $\mathscr{A}$ may be true for some interpretations and false for others. (As an example, consider $A_1^1(a_1)$.)

If $\mathscr{A}$ is not closed, i.e., if $\mathscr{A}$ contains free variables, $\mathscr{A}$ may be neither true nor false for some interpretations. For example, if $\mathscr{A}$ is $A_1^2(x_1, x_2)$ and we consider an interpretation in which the domain is the set of integers and $A_1^2(y, z)$ is interpreted as $y < z$, then $\mathscr{A}$ is satisfied only by those sequences s = (b,, b_2, . . .) of integers in which b, $< b_2$. Hence, $\mathscr{A}$ is neither true nor false for this interpretation. On the other hand, there are wfs which are not closed, but which, nevertheless, are true or false for every interpretation. An example of such a wf is $A_1^1(x_1) \vee \sim A_1^1(x_1)$, which is true for every interpretation.

(X) LEMMA. *If t and u are terms and s is a sequence in Σ, and t' results from* t by substituting u for all occurrences of x_i, and s' results from s by substituting $s^\star(u)$ *for* the i^{th} component of s, then $s^\star(t') = (s')^\star(t)$. (Hint: Induction on the length of t.†)

COROLLARY. Let $\mathscr{A}(x_i)$ be a wf, t a term free for x_i in $\mathscr{A}(x_i)$, and $\mathscr{A}(t)$ the wf obtained from $\mathscr{A}(x_i)$ by substituting t *for* all free occurrences of x_i in $\mathscr{A}(x_i)$.

(i) A sequence s = (b,, b_2, . . .) satisfies $\mathscr{A}(t)$ if and only if the sequence s', obtained from s by substituting $s^\star(t)$ for b_i in the i^{th} place, satisfies $\mathscr{A}(x_i)$. (Hint: Induction on the number of connectives and *quantifiers* in $\mathscr{A}(x_i)$, using the lemma.)

(ii) If $(x_i)\mathscr{A}(x_i)$ is satisfied by the sequence s, then $\mathscr{A}(t)$ also is satisfied by s.

† The length of an expression is the number of occurrences of symbols in the expression.

(iii) $(x_i)\mathscr{A}(x_i) \supset \mathscr{A}(t)$ is true for all interpretations.

(XI) If $\mathscr{A}$ does not contain x_i free, then $(x_i)(\mathscr{A} \supset \mathscr{B})$ 3 $(\mathscr{A} \supset (x_i)\mathscr{B})$ is true for all interpretations.

PROOF. Assume (XI) is not correct. Then $(x_i)(\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset (x_i)\mathscr{B})$ is not true for some interpretation. By clause (iii) of the definition of satisfiability, there is a sequence such that s satisfies $(x_i)(\mathscr{A} \supset \mathscr{B})$ and s does not satisfy $\mathscr{A} \supset (x_i)\mathscr{B}$. From the latter and clause (iii), s satisfies $\mathscr{A}$ and s does not satisfy $(x_i)\mathscr{B}$. Hence, by clause (iv), there is a sequence s' differing from s in at most the i^{th} place such that s' does not satisfy $\mathscr{B}$. Since x_i is free in neither $(x_i)(\mathscr{A} \supset \mathscr{B})$ nor $\mathscr{A}$, and since s satisfies both of these wfs, it follows by (VIII) that s' also satisfies both $(x_i)(\mathscr{A} \supset \mathscr{B})$ and $\mathscr{A}$. Since s' satisfies $(x_i)(\mathscr{A} \supset \mathscr{B})$, it follows by clause (iv) that s' satisfies $\mathscr{A} \supset \mathscr{B}$. Since s' satisfies $\mathscr{A} \supset \mathscr{B}$ and $\mathscr{A}$, clause (iii) implies that s' satisfies $\mathscr{B}$, which contradicts the fact that s' does not satisfy $\mathscr{B}$. Hence, (XI) is proved.

EXERCISES

2.14. Verify (I)–(X).

2.15. Prove that a closed wf $\mathscr{A}$ is true for M if and only if $\mathscr{A}$ is satisfied by some sequence s in Σ. (Remember that Σ is the set of denumerable sequences of elements of the domain of M.)

2.16. Find the properties or relations determined by the following wfs and interpretations.

(a) $[(Eu)A_1^2(f_1^2(x, u), y)] \wedge [(Ev)A_1^2(f_1^2(x, v), z)]$, where the domain D is the set of all integers, $A_1^2(u, v)$ means u = v, and $f_1^2(u, v)$ means uv.

(b) Here, D is the set of non-negative integers, $A_1^2(x, y)$ means x = y, a, denotes 0, a_2 denotes I, $f_1^2(x, y)$ stands for x + y, and $f_2^2(x, y)$ stands for xy.

(i) $(Ez)(\sim A_1^2(z, a_1)$ A $A_1^2(f_2^2(x, z), y))$

(ii) $(Ey)(A_1^2(x, f_2^2(y, y)))$

(c) $(Ex_3)A_1^2(f_1^2(x_1, x_3), x_2)$, where D is the set of all positive integers, $A_1^2(x, y)$ means x = y, and $f_1^2(x, y)$ means xy.

(d) $A_1^1(x_1) \wedge (x_2) \sim A_1^2(x_1, x_2)$, where D is the set of all living people, $A_1^1(x_1)$ means x is a man, and $A_1^2(x, y)$ means x is married to y.

(e) $(Ex_1)(Ex_2)(A_1^2(x_1, x_3)$ A $A_1^2(x_2, x_4)$ A $A_2^2(x_1, x_2))$, where D is the domain of all people, $A_1^2(x, y)$ means x is a parent of y, and $A_2^2(x, y)$ means x and y are siblings.

(f) $(x_3)((Ex_4)A_1^2(f_1^2(x_4, x_3), x_1)$ A $(Ex_4)(A_1^2(f_1^2(x_4, x_3), x_2)) \supset A_1^2(x_3, a_1))$, where D is the set of all positive integers, a, denotes 1, $A_1^2(x, y)$ means x = y, and $f_1^2(x, y)$ means xy.

2.17. For each of the following wfs and interpretations, write a translation into ordinary English and determine its truth or falsity.

(a) Here, D is the set of non-negative integers, $A_1^2(x, y)$ means $x = y$, a_1 denotes 0, a_2 denotes 1, $f_1^2(x, y)$ means x + y, and $f_2^2(x, y)$ means xy.

(i) $(x)(Ey)(A_1^2(x, f_1^2(y, y)) V A_1^2(x, f_1^2(f_1^2(y, y), a_2)))$
(ii) $(x)(y)(A_1^2(f_2^2(x, y), a_1) \supset A_1^2(x, a_1) V A_1^2(y, a_1))$
(iii) $(Ey)A_1^2(f_1^2(y, y), a_2)$.

(b) *Here, D is the set of all integers, $A_1^2(x, y)$ means $x = y$, and $f_1^2(x, y)$ means $x + y$.*

(i) $(x_1)(x_2)A_1^2(f_1^2(x_1, x_2), f_1^2(x_2, x_1))$
(ii) $(x_1)(x_2)(x_3)A_1^2(f_1^2(x_1, f_1^2(x_2, x_3)), f_1^2(f_1^2(x_1, x_2), x_3))$
(iii) $(x_1)(x_2)(Ex_3)A_1^2(f_1^2(x_1, x_3), x_2)$.

(c) The same wfs as in Part (b), but the domain is the set of all positive integers, $A_1^2(x, y)$ means $x = y$, and $f_1^2(x, y)$ is x^y.

(d) The domain is the set of all rational numbers, $A_1^2(x, y)$ means $x = y$, $A_2^2(x, y)$ means $x < y$, $f_1^2(x, y)$ is xy, $f_1^1(x)$ is $x + 1$, and a, is 0.

(i) $(Ex)(A_1^2(f_1^2(x, x), f_1^1(f_1^1(a_1))))$
(ii) $(x)(y)(A_2^2(x, y) \supset (Ez)(A_2^2(x, z) A A_2^2(z, y)))$
(iii) $(x)(\sim A_1^2(x, a_1) \supset (Ey)A_1^2(f_1^2(x, y), f_1^1(a_1)))$.

(e) The domain is the set of non-negative integers, $A_1^2(u, v)$ means $u \leqslant v$, and $A_1^3(u, u, w)$ means $u + u = w$.

(i) $(x)(y)(z)(A_1^3(x, y, z) \supset A_1^3(y, x, z))$
(ii) $(x)(y)(A_1^3(x, x, y) \supset A_1^2(x, y))$
(iii) $(x)(y)(A_1^2(x, y) \supset A_1^3(x, x, y))$
(iv) $(Ex)(y)A_1^3(x, y, y)$
(v) $(Ey)(x)A_1^2(x, y)$
(vi) $(x)(y)(A_1^2(x, y) \equiv (Ez)A_1^3(x, z, y))$.

A wf $\mathcal{A}$ is said to be *logically valid* if and only if $\mathcal{A}$ is true for every interpretation.

$\mathcal{A}$ is said to be *satisfiable* if and only if there is an interpretation for which $\mathcal{A}$ is satisfied by at least one sequence in Σ.

It is obvious that $\mathcal{A}$ is logically valid if and only if $\sim \mathcal{A}$ is not satisfiable; and $\mathcal{A}$ is satisfiable if and only if $\sim \mathcal{A}$ is not logically valid. *If* $\mathcal{A}$ is a closed wf, then we know that $\mathcal{A}$ is either true or false for any given interpretation, i.e., $\mathcal{A}$ is satisfied by all sequences or by none; therefore, if $\mathcal{A}$ is closed, then $\mathcal{A}$ is satisfiable if and only if $\mathcal{A}$ is true for some interpretation.

We say that $\mathcal{A}$ is *contradictory* if and only if $\sim \mathcal{A}$ is logically valid, or, equivalently, if and only if $\mathcal{A}$ is false for every interpretation.

$\mathcal{A}$ is said to *logically imply* $\mathcal{B}$ *if* and only if, in every interpretation, any sequence satisfying $\mathcal{A}$ also satisfies $\mathcal{B}$. More generally, $\mathcal{B}$ is a *logical consequence* of a set Γ of wfs if and only if, in every interpretation, every sequence which satisfies every wf in Γ also satisfies 93. & and $\mathcal{B}$ are *logically equivalent* if and only if they logically imply each other.

The following assertions are easy consequences of these definitions.

(a) $\mathcal{A}$ logically implies $\mathcal{B}$ if and only if $\mathcal{A}$ 3 $\mathcal{B}$ is logically valid.
(b) $\mathcal{A}$ and $\mathcal{B}$ are logically equivalent if and only if $\mathcal{A} \equiv \mathcal{B}$ is logically valid.
(c) If $\mathcal{A}$ logically implies $\mathcal{B}$, and $\mathcal{A}$ is true in a given interpretation, so is $\mathcal{B}$.
(d) If $\mathcal{B}$ is a logical consequence of a set Γ of wfs, and all wfs in Γ are true in a given interpretation, so is $\mathcal{B}$.

Any sentence of a formal or natural language which is an instance of a logically valid wf is called *logically true*, and *an* instance of a contradictory wf is said to be *logically false.*

Examples.

1. Every instance of a tautology is logically valid. *(VII)*
2. If $\mathcal{A}$ does not contain x free, then $(x)(\mathcal{A}$ 3 $\mathcal{B}) \supset (\mathcal{A} \supset (x)\mathcal{B})$ is logically valid. *(XI)*
3. *If* t is free for x in $\mathcal{A}$, then $(x)\mathcal{A}(x)$ 3 $\mathcal{A}(t)$ is logically valid. (X)
4. The wf $(x_2)(Ex_1)A_1^2(x_1, x_2) \supset (Ex_1)(x_2)A_1^2(x_1, x_2)$ is not logically valid. As a counterexample, let the domain D be the set of integers, and let $A_1^2(y, z)$ be $y < z$. Then $(x_2)(Ex_1)A_1^2(x_1, x_2)$ is true, but $(Ex_1)(x_2)A_1^2(x_1, x_2)$ is false.
5. $\mathcal{A}$ is logically valid if and only if $(y_1) \ldots (y_n)\mathcal{A}$ is logically valid. **(VI)**

EXERCISES

2.18. *Show that the following wfs are not logically valid.*
(a) $[(x_1)A_1^1(x_1) \supset (x_1)A_2^1(x_1)] \supset [(x_1)(A_1^1(x_1) \supset A_2^1(x_1))]$
(b) $[(x_1)(A_1^1(x_1) V A_2^1(x_1))] \supset [((x_1)A_1^1(x_1)) V ((x_1)A_2^1(x_1))]$

2.19. **Show** *that the following wfs are logically valid.*
(a) $\mathcal{A}(t)$ 3 $(Ex_i)\mathcal{A}(x_i)$ *if t is free for* x_i *in* $\mathcal{A}(x_i)$
(b) $(x_i)\mathcal{A} \supset (Ex_i)\mathcal{A}$
(c) $(x_i)(x_j)\mathcal{A} \equiv (x_j)(x_i)\mathcal{A}$
(d) $(x_i)\mathcal{A} \equiv \sim (Ex,) \sim \mathcal{A}$
(e) $(x_i)(\mathcal{A} \supset 8) \supset ((x_i)\mathcal{A} \supset (x_i)\mathcal{B})$
(f) $((x_i)\mathcal{A}\ A\ (x_i)\mathcal{B}) \equiv (x_i)(\mathcal{A} \wedge 8)$
(g) $((x_i)\mathcal{A}) \vee (x_i)\mathcal{B} \supset (x_i)(\mathcal{A} \vee 8)$
(h) $(Ex_i)(Ex_j)\mathcal{A} \equiv (Ex_j)(Ex_i)\mathcal{A}$
(i) $(Ex_i)(x_j)\mathcal{A} \supset (x_j)(Ex_i)\mathcal{A}$

2.20. If $\mathcal{A}$ is a *closed* **wf,** *show that $\mathcal{A}$ logically implies $\mathcal{B}$ if and only if 8 is true* every interpretation *in which $\mathcal{A}$ is true.* (This *is not always the case when $\mathcal{A}$ has* ee variables. For *example, let $\mathcal{A}$ be $A_1^1(x_1)$ and $\mathcal{B}$ be $(x_1)A_1^1(x_1)$; 8 is true* henever $\mathcal{A}$ is *(by* VI); *produce an interpretation showing that $\mathcal{A}$ does not logically* ply $\mathcal{B}$.)

2.21. Show *that the following wfs are not logically valid.*
(a)^D $(Ex)(y)(A_1^2(x, y)\ A \sim A_1^2(y, x) \supset [A_1^2(x, x) \equiv A_1^2(y, y)])$
(b) $(x)(y)(z)(A_1^2(x, y)\ A\ A_1^2(y, z) \supset A_1^2(x, z))\ A\ (x) - A_1^2(x, x) \supset (Ex)(y) \sim A_1^2(x, y)$

(c)^D $(x)(y)(z)(A_1^2(x, x) \mathrm{A} (A_1^2(x, z) \supset A_1^2(x, y) \mathrm{V} A_1^2(y, z)))$
$\supset (Ey)(z)A_1^2(y, z)$

(d) $[(Ex)A_1^1(x) \equiv (Ex)A_2^1(x)] \supset (x)(A_1^1(x) \equiv A_2^1(x))$

(e) $(Ex)(A_1^1(x) \supset A_2^1(x)) \supset ((Ex)A_1^1(x) \supset (Ex)A_2^1(x))$

(f) $(Ex)(y)(Ez)((A_1^2(y, z) \supset A_1^2(x, z)) \supset (A_1^2(x, x) \supset A_1^2(y, x)))$

(g) $(x)(Ey)A_1^2(x, y) \supset (Ey)A_1^2(y, y)$

(h) $(Ex)(Ey)A_1^2(x, y) \supset (Ez)A_1^2(z, z)$

(i) $[(x)(y)(A_1^2(x, y) \supset A_1^2(y, x)) \mathrm{A} (x)(y)(z)(A_1^2(x, y) \mathrm{A} A_1^2(y, z) \supset$
$A_1^2(x, z))] \supset (x)A_1^2(x, x)$

2.22. Prove: If the free variables of $\mathcal{A}$ are $y_1, \ldots, y_n$, then $\mathcal{A}$ is satisfiable if and only if (Ey,) . . . $(Ey_n)\mathcal{A}$ is satisfiable.

2.23. Introducing appropriate abbreviations, write the sentences of the following arguments as wfs, and determine whether the conclusion is logically implied by the conjunction of the premisses.

(a) Everyone who is sane can understand mathematics. None of **Hegel's** sons can understand mathematics. No madmen are fit to vote. Hence none of **Hegel's** sons is fit to vote.

(b) For every set x, there is a set y such that the cardinality of y is greater than the cardinality of x. If x is included in y, the cardinality of **x** is not greater than the cardinality of y. Every set is included in V. Hence, V is not a set.

(c) If every ancestor of an ancestor of an individual is also an ancestor of the same individual, and no individual is his own ancestor, then there must be a person who has no ancestor.

(d) Any barber in Jonesville shaves exactly those men who do not shave themselves. Hence there is no barber in Jonesville.

(e) Kilroy was here. Therefore, someone was here.

(f) Some geniuses are celibate. Some students are not celibate. Therefore, some students are not geniuses.

2.24. Determine whether the following sets of **wfs** or sentences are consistent, **i.e.,** whether their conjunction is satisfiable.

(a) $(Ex)(y)A_1^2(x, y)$
$(x)(y)(Ez)(A_1^2(x, z) \mathrm{A} A_1^2(z, y))$

(b) $(x)(Ey)A_1^2(y, x)$
$(x)(y)(A_1^2(x, y) \supset - A_1^2(y, x))$
$(x)(y)(z)(A_1^2(x, y) \mathrm{A} A_1^2(y, z) \supset A_1^2(x, z))$

(c) All unicorns are animals
No unicorns are animals

2.25. Exhibit a logically valid wf which is not an instance of a tautology. However, show that any logically valid open wf (**i.e.,** a wf without quantifiers) must be an instance of a tautology.

3. First-Order Theories

In the case of the propositional calculus, the method of truth tables provides an effective test as to whether any given statement form is a tautology. However, there does not seem to be any effective process to determine whether a given wf

is logically valid, since, in general, one has to check the truth of a wf for interpretations with arbitrarily large finite or infinite domains. in fact, we shall see later that, according to a plausible definition of "effective", it may actually be proved that there is no effective way to test for logical validity. The axiomatic method, which was a luxury in the study of the propositional calculus, thus appears to be a necessity in the study of wfs involving quantifiers,? and we therefore turn now to the consideration of first-order *theories*‡.

The symbols of a first-order theory K are essentially those introduced earlier in this chapter: the propositional connectives ~ , ⊃ ; the punctuation marks (,), , (the comma is not strictly necessary but is convenient for ease in reading formulas); denumerably many individual variables x,, *x*,, . . . ; a finite or denumerable non-empty set of predicate letters $A_j^n(n, J \geqslant 1)$; a finite or denumerable, possibly empty, set of function letters $f_j^n(n, J \geqslant 1)$; and a finite or denumerable, possibly empty, set of individual constants $a_i(i \geqslant 1)$. Thus, in a theory K, some or all of the function letters and individual constants may be absent, and some (but not all) of the predicate letters may be absent. Different theories may differ in which of these symbols they possess.

The definitions given in Section 1 for term, wf, and for the propositional connectives ⋀, ⋁, ≡ , are adopted for any first-order theory. Of course, for a particular theory K, only those symbols occurring in K are used in the formation of terms and wfs.

The axioms of **K** are divided into two classes: the logical axioms and the proper (or non-logical) axioms.

Logical *Axioms*: If $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ are wfs of **K**, then the following are logical axioms of K.

(1) $\mathcal{A} \supset (\mathcal{B} \supset \mathcal{A})$

(2) $(\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})) \supset ((\mathcal{A} \supset \mathcal{B}) \supset (\mathcal{A} \supset \mathcal{C}))$

(3) $(\sim \mathcal{B} \supset \sim \mathcal{A}) \supset ((\sim \mathcal{B} \supset \mathcal{A}) \supset \mathcal{B})$

(4) $(x_i)\mathcal{A}(x_i) \supset \mathcal{A}(t)$, if $\mathcal{A}(x_i)$ is a wf of K and t is a term of K free for x_i in $\mathcal{A}(x_i)$. Note here that t may be identical with x_i, giving the axioms
I $(x_i)\mathcal{A}(x_i) \supset \mathcal{A}(x_i)$.

? There is still another reason for a formal axiomatic approach. Concepts and propositions which involve the notion of interpretation, and related ideas such as truth, model, etc., are often called *semantical* to distinguish them from *syntactical* concepts, which refer to simple relations among symbols and expressions of precise formal languages. Since semantical notions are set-theoretic in character, and since set theory, because of the paradoxes, is considered a rather shaky foundation for the study of mathematical logic, many logicians consider a syntactical approach, consisting in a study of formal axiomatic theories using only rather weak number-theoretic methods, to be much safer. For further discussions, see the pioneering study on semantics by Tarski [1936], Kleene [1952], Church [1956], and Hilbert-Bernays[1934].

‡ The adjective "first-order" is used to distinguish the theories we shall study from those in which there are predicates having other predicates or functions as arguments or in which predicate quantifiers or function quantifiers are permitted, or both. First-order theories suffice for the expression of known mathematical theories, and, in any case, most higher-order theories can be suitably "translated" into first-order theories. Examples of higher-order theories may be found in Church [1940], Gödel [1931], Tarski [1933], Scholz-Hasenjaeger[1961: §§200–219].

(5) $(x_i)(\mathcal{A} \supset \mathcal{B}) \supset (\mathcal{A} \supset (x_i)\mathcal{B})$ if $\mathcal{A}$ is a wf of **K** containing no free occurrences of x_i.

Proper Axioms: These cannot be specified, since they vary from theory to theory. A first-order theory in which there are no proper axioms is called a first-order predicate calculus.

The rules of inference of any first-order theory are

(i) **Modus** ponens: $\mathcal{B}$ follows from $\mathcal{A}$ and $\mathcal{A} \supset \mathcal{B}$

(ii) Generalization: $(x_i)\mathcal{A}$ follows from &.

We shall use MP and Gen, respectively, to indicate applications of these rules.

By a model of a first-order theory K we mean an interpretation in which all the axioms of K are **true.**† By **(III)** and **(VI), p.** 53, if the rules of **modus** ponens and generalization are applied to wfs true in a given interpretation, then the results of these applications are also true. Hence every theorem of **K** is true in any model of K.

As we shall see, the logical axioms are so designed that the logical consequences (in the semantic sense, cf. p. 56) of the closure of the axioms of K are precisely the theorems of K. In particular, if K is a first-order predicate calculus, it turns out that the theorems of **K** are precisely those wfs of **K** which are logically valid.

Some explanation is needed for the restrictions in Axiom Schema (4) and (5). In the case of **(4),** if t were not free for x, in $\mathcal{A}$, the following unpleasant result would arise. Let $\mathcal{A}(x_1)$ be $\sim (x_2)A_1^2(x_1, x_2)$ and let t be x_2. Notice that t is not free for x_1 in $\mathcal{A}(x_1)$. Consider the instance of Axiom (4):

$$(✠)\quad (x_1)(\sim (x_2)A_1^2(x_1, x_2)) \supset \sim (x_2)A_1^2(x_2, x_2)$$

Now, take as interpretation any domain with at least two members and let A_1^2 stand for the identity relation. Then the antecedent of **(✠)** is true and the consequent false.

In the case of **(5),** relaxation of the restriction that x_i not be free in $\mathcal{A}$ would lead to the following misfortune. Let $\mathcal{A}$ and $\mathcal{B}$ both be $A_1^1(x_1)$. Thus, x, is free in $\mathcal{A}$. Consider the instance of (5):

$$(✠✠)\quad (x_1)(A_1^1(x_1) \supset A_1^1(x_1)) \supset (A_1^1(x_1) \supset (x_1)A_1^1(x_1))$$

The antecedent of **(✠✠)** is logically valid. However, if we take any interpretation in which A_1^1 holds for some but not all elements of the domain, then the consequent will not be true.

[†] **In talking about an interpretation of K, we need only specify the interpretations of the symbols of K. We shall use the notion of interpretation in this extended sense.**

Examples of first-order theories.

(i) Partial order. Let K have a single predicate letter A_1^2 and no function letters and individual constants. We shall write $x_i < x_j$ instead of $A_1^2(x_i,$ x) and $x_i \nless x_j$ for $\sim (x_i <$ x,). We have two proper axioms:

(a) $(x_1)(x_1 \nless x_1)$ (Irreflexivity)

(b) $(x_1)(x_2)(x_3)(x_1 < x_2 \mathrm{A}\ x_2 < x_3 \supset x_1 < x_3)$ (Transitivity)

A model of this theory is called a partially-ordered structure.

(ii) Group theory. Let K have one predicate letter A_1^2, one function letter f_1^2, **and** one individual constant a,. (To conform with ordinary notation, we shall write $t = s$ instead of $A_1^2(t,$ s), $t + s$ instead of $f_1^2(t,$ s) and **0** instead of a,.) As proper axioms we have:

(a) $(x_1)(x_2)(x_3)(x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3)$ (Associativity)

(b) $(x_1)(0 + x_1 = x_1)$ (Identity)

(c) $(x_1)(Ex_2)(x_2 + x_1 = 0)$ (Inverse)

(d) $(x_1)(x_1 = x_1)$ (Reflexivity of =)

(e) $(x_1)(x_2)(x_1 = x_2 \,3\, x_2 = x_1)$ (Symmetry of =)

(f) $(x_1)(x_2)(x_3)(x_1 = x_2 \,3\, (x_2 = x_3 \supset x_1 = x_3))$ (Transitivity of =)

(g) $(x_1)(x_2)(x_3)(x_2 = x_3 \supset (x_1 + x_2 = x_1 + x_3 \wedge x_2 + x_1 = x_3 + x_1))$ (Substitutivity of =)

A model for this theory, in which the interpretation of = is the identity relation, is called a group. If, in addition, the wf $(x_1)(x_2)(x_1 + x_2 = x_2 + x_1)$ is true in a group, the latter is called abelian (or commutative).

The theories of partial order and of groups are both axiomatic. In general, any theory with a finite number of proper axioms is axiomatic, since it is obvious that one can effectively decide whether any given wf is a logical axiom (cf. pp. 59–60).

4. Properties of First-Order Theories

All the results in this section refer to an arbitrary first-order theory K, unless otherwise stated. Notice that any first-order theory is a formal theory **(cf.** pp. 29–36). In addition, since we shall deal in this book only with first-order theories, from now on we shall refer to first-order theories simply as theories.

PROPOSITION 2.1. *Every* **wf** & *of* K which is an instance *of* a tautology is a theorem of K, and it may be proved using only Axioms (1)–(3) and **MP.**

PROOF. $\mathcal{A}$ arises from a tautology W by substitution. By Proposition 1.13, there is a proof of W in L. **In** such a proof, make the same substitutions of wfs **of K** for statement letters as were used in obtaining $\mathcal{A}$ from W, and, for all statement letters in the proof which do not occur in W, substitute an arbitrary **wf of** K. Then the resulting sequence of wfs is a proof of $\mathcal{A}$, and this proof uses only Axiom Schemas (1)–(3) and MP.

Application of Proposition 2.1 in a proof will be indicated by writing "Tautology".

PROPOSITION 2.2. Any first-order predicate calculus K is consistent.

PROOF. For each wf $\mathscr{A}$ of K, let **h**($\mathscr{A}$) be the expression obtained **by** erasing all the quantifiers and terms in $\mathscr{A}$ (together with the associated commas and parentheses). Examples: $h((x_1)(A_1^2(x_1, x_2) \supset A_1^1(x_3))$ is $A_1^2 \supset A_1^1$; and h($\sim$ $(x_7)A_2^3(x_4$, a,, x,) 3 $A_3^1(x_4)))$ is $\sim A_2^3 \supset A_3^1$. Then **h**($\mathscr{A}$) is essentially a statement form, with the symbols A_j^k playing the role of statement letters. **Clearly**, h($\sim \mathscr{A}$) = $\sim$ (h($\mathscr{A}$)) and h(& $\supset$ 9) = h($\mathscr{A}$) $\supset$ h($\mathscr{B}$). Now, for every axiom $\mathscr{A}$ given by Schemas (1)–(5), h($\mathscr{A}$) is a tautology. This is clear for (1)–(3). An instance of (4), $(x_i)\mathscr{A}(x_i) \supset \mathscr{A}(t)$, is transformed by h into a tautology of the form $\mathscr{B}$ 3 $\mathscr{B}$; and an instance of (5), $(x_i)(\mathscr{A} \supset \mathscr{B}) \supset (\mathscr{A} \supset (x_i)\mathscr{B})$ is transformed into a tautology of the form (9 $\supset$ &) 3 ($\mathscr{D}$ 3 &). In addition, if h($\mathscr{A}$) and h(& $\supset \mathscr{B}$) are tautologies, then, by Proposition 1.1, h($\mathscr{B}$) is also a tautology; and, if h($\mathscr{A}$) is a tautology, so is h($(x_i)\mathscr{A}$), which is the same as h($\mathscr{A}$). Hence, h($\mathscr{A}$) is a tautology whenever $\mathscr{A}$ is a theorem of K. If there were a wf $\mathscr{B}$ of K such that $\vdash_K \mathscr{B}$ and $\vdash_K \sim$ 9 , then both h($\mathscr{B}$) and $\sim$ h($\mathscr{B}$) would be tautologies, which is impossible. Thus, K is consistent. (The transformation h amounts to interpreting K in a domain with a single element. All the theorems of K are true in such an interpretation, but no wf and its negation can be true in any interpretation.)

The Deduction Theorem (Proposition 1.8) for the propositional calculus cannot be carried over without modification to arbitrary theories K. For example, for any wf $\mathscr{A}$, $\mathscr{A} \vdash_K (x_1)\mathscr{A}$, but it is not always the case that $\vdash_K \mathscr{A} \supset (x_1)\mathscr{A}$. Consider a domain containing at least two elements c and d. Let K be a predicate calculus, and let $\mathscr{A}$ be $A_1^1(x_1)$. Interpret Af as a property which holds only for c. Then $A_1^1(x_1)$ is satisfied by any sequence s = (b_1, b_2, . . .) where b_1 = c, but $(x_1)A_1^1(x_1)$ is satisfied by no sequence at all. Hence, $A_1^1(x_1) \supset (x_1)A_1^1(x_1)$ is not true in this interpretation, and so it is not logically valid. But it is easy to see (Proposition 2.7) that every theorem of a predicate calculus is logically valid.

However, a modified, but still useful, form of the Deduction Theorem may be derived.

Let $\mathscr{A}$ be a wf in a set Γ of wfs; assume given a deduction $\mathscr{B}_1$, . . . , 9, from Γ, together with justification for each step of the deduction. We shall say that $\mathscr{B}_1$ depends upon $\mathscr{A}$ in this proof if and only if:

(i) $\mathscr{B}_i$ is $\mathscr{A}$ and the justification for $\mathscr{B}_i$ is that it belongs to Γ; or

(ii) $\mathscr{B}_i$ is justified as a direct consequence by MP or Gen of some preceding wfs of the sequence, where at least one of these preceding wfs depends upon $\mathscr{A}$.

Example.

$$\mathscr{A}, (x_1)\mathscr{A} \supset \mathscr{C} \vdash (x_1)\mathscr{C}$$

$(\mathscr{B}_1)$	$\mathscr{A}$	Hyp
$(\mathscr{B}_2)$	$(x_1)\mathscr{A}$	$(\mathscr{B}_1)$, Gen
$(\mathscr{B}_3)$	$(x_1)\mathscr{A} \supset \mathscr{C}$	Hyp
$(\mathscr{B}_4)$	$\mathscr{C}$	$(\mathscr{B}_2)$, $(\mathscr{B}_3)$, MP
$(\mathscr{B}_5)$	$(x_1)\mathscr{C}$	$(\mathscr{B}_4)$, Gen

Here, (9,) depends upon $\mathscr{A}$; $(\mathscr{B}_2)$ depends upon $\mathscr{A}$; $(\mathscr{B}_3)$ depends upon $(x_1)\mathscr{A} \supset \mathscr{C}$; $(\mathscr{B}_4)$ depends upon $\mathscr{A}$ and $(x_1)\mathscr{A}$ 3 $\mathscr{C}$, and (9,) depends upon $\mathscr{A}$ and $(x_1)\mathscr{A} \supset \mathscr{C}$.

PROPOSITION 2.3. If $\mathscr{B}$ *does* not depend upon $\mathscr{A}$ in a deduction $\Gamma, \mathscr{A} \vdash \mathscr{B}$, then $\Gamma \vdash \mathscr{B}$.

PROOF. Let $\mathscr{B}_1$, . . . , 9, = $\mathscr{B}$ be a deduction of $\mathscr{B}$ from Γ and $\mathscr{A}$, in which $\mathscr{B}$ does not depend upon $\mathscr{A}$. As inductive hypothesis, let us assume that the proposition is true for all deductions of length less than n. If $\mathscr{B}$ belongs to Γ or is an axiom, then $\Gamma \vdash$ 9. If $\mathscr{B}$ is a direct consequence of one or two preceding **wfs,** then, since $\mathscr{B}$ does not depend upon $\mathscr{A}$, neither do these preceding wfs. By the inductive hypothesis, these preceding wfs are deducible from Γ alone. Consequently, so is $\mathscr{B}$.

PROPOSITION 2.4 (DEDUCTION THEOREM). Assume that $\Gamma, \mathscr{A} \vdash \mathscr{B}$, where, in the deduction, no application of Gen to a wf which ***depends*** upon $\mathscr{A}$ has as its ***quantified*** variable a free variable of $\mathscr{A}$. Then $\Gamma \vdash \mathscr{A} \supset \mathscr{B}$.

PROOF. Let $\mathscr{B}_1$, . . . , 9, = $\mathscr{B}$ be a deduction of $\mathscr{B}$ from Γ, $\mathscr{A}$ satisfying the assumption of our proposition. Let us show by induction that $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$ for each **i** $\leqslant$ n. If $\mathscr{B}_i$ is an axiom or belongs to Γ, then $\Gamma \vdash \mathscr{A}$ 3 $\mathscr{B}_i$, since $\mathscr{B}_i \supset (\mathscr{A} \supset \mathscr{B}_i)$ **is** an axiom. If $\mathscr{B}_i$ is $\mathscr{A}$, then $\Gamma \vdash \mathscr{A}$ 3 $\mathscr{B}_i$, since, by Proposition 2.1, $\vdash \mathscr{A} \supset \mathscr{A}$. If there exist j, k less than i such that $\mathscr{B}_k$ is $\mathscr{B}_j \supset \mathscr{B}_i$, then, by inductive hypothesis, $\Gamma \vdash \mathscr{A}$ 3 $\mathscr{B}_j$ and $\Gamma \vdash \mathscr{A}$ 3 ($\mathscr{B}_j$ 3 $\mathscr{B}_i$). Hence, $\Gamma \vdash \mathscr{A}$ 3 $\mathscr{B}_i$, **by Áxiom** (2) and MP. Finally suppose there is some **j < i** such that $\mathscr{B}_i$ is $(x_k)\mathscr{B}_j$. By hypothesis, $\Gamma \vdash \mathscr{A}$ 3 $\mathscr{B}_j$ and either $\mathscr{B}_j$ does not depend upon $\mathscr{A}$ or x_k **is** not a free variable of $\mathscr{A}$. If $\mathscr{B}_j$ does not depend upon $\mathscr{A}$, then, by Proposition 2.3, $\Gamma \vdash \mathscr{B}_j$, and, consequently, by Gen, $\Gamma \vdash (x_k)\mathscr{B}_j$. Thus, $\Gamma \vdash \mathscr{B}_i$. Now, by Axiom (1), $\vdash \mathscr{B}_i$ 3 $(\mathscr{A} \supset \mathscr{B}_i)$. So, $\Gamma \vdash \mathscr{A}$ 3 $\mathscr{B}_i$, by MP. If x_k is not a free variable **of** $\mathscr{A}$, then, by Axiom (5), $\vdash (x_k)(\mathscr{A}$ 3 $\mathscr{B}_j)$ 3 ($\mathscr{A}$ 3 $(x_k)\mathscr{B}_j$). Since $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_j$, **we** have, by Gen, $\Gamma \vdash (x_k)(\mathscr{A} \supset \mathscr{B}_j)$, and so, by MP, $\Gamma \vdash \mathscr{A} \supset (x_k)\mathscr{B}_j$, **i.e.**, $\Gamma \vdash \mathscr{A} \supset \mathscr{B}_i$. This completes the induction, and our proposition is just the special case **i = n.**

The hypothesis of Proposition 2.4 is rather cumbersome, and the following weaker corollaries often prove to be more useful.

COROLLARY 2.5. *If a deduction* $\Gamma, \mathcal{A}$ t $\mathcal{B}$ *involves no application of* Gen *of which the quantified variable is free in* $\mathcal{A}$, *then* $\Gamma \vdash \mathcal{A} \supset \mathcal{B}$.

COROLLARY 2.6. *If* $\mathcal{A}$ *is a closed* wf, *and* $\Gamma, \mathcal{A} \vdash \mathcal{B}$, *then* $\Gamma \vdash \mathcal{A} \supset \mathcal{B}$

In Propositions 2.3–2.6, the following additional conclusion can be drawn from the proof. The new proof of $\Gamma \vdash \mathcal{A} \supset \mathcal{B}$ (in the case of 2.3, of $\Gamma \vdash \mathcal{B}$) involves an application of Gen to a wf depending upon a wf $\mathcal{C}$ of Γ only if there is an application of Gen in the given proof of $\Gamma, \mathcal{A} \vdash \mathcal{B}$ which involves the same quantified variable and is applied to a wf which depends upon $\mathcal{C}$. (In the proof of Proposition 2.4, one should observe that $\mathcal{B}_j$ depends upon a premiss $\mathcal{C}$ of Γ in the original proof if and only if $\mathcal{A} \supset \mathcal{B}_j$ depends upon $\mathcal{C}$ in the new proof.)

This supplementary conclusion is useful when we wish to apply the Deduction Theorem several times in a row to a given deduction, e.g., to obtain $\Gamma \vdash \mathcal{D} \supset (\mathcal{A} \supset \mathcal{B})$ from $\Gamma, \mathcal{D}, \mathcal{A} \vdash \mathcal{B}$; from now on, it is to be considered as part of the statements of Propositions 2.3–2.6.

Example. $\vdash (x_1)(x_2)\mathcal{A}$ 3 $(x_2)(x_1)\mathcal{A}$

PROOF.

1.	$(x_1)(x_2)\mathcal{A}$	Hyp
2.	$(x_1)(x_2)\mathcal{A}$ 3 $(x_2)\mathcal{A}$	Axiom (4)
3.	$(x_2)\mathcal{A}$	1, 2, MP
4.	$(x_2)\mathcal{A}$ 3 $\mathcal{A}$	Axiom (4)
5.	$\mathcal{A}$	3, 4, MP
6.	$(x_1)\mathcal{A}$	5, Gen
7.	$(x_2)(x_1)\mathcal{A}$	6, Gen

Thus, by 1–7, we have $(x_1)(x_2)\mathcal{A}$ t $(x_2)(x_1)\mathcal{A}$, where, in the deduction, no application of Gen has as a quantified variable a free variable of $(x_1)(x_2)\mathcal{A}$. Hence, by Corollary 2.5, $\vdash (x_1)(x_2)\mathcal{A} \supset (x_2)(x_1)\mathcal{A}$.

EXERCISES

2.26. Show that
(a) $\vdash (x_1)(\mathcal{A} \supset \mathcal{B}) \supset ((x_1)\mathcal{A} \supset (x_1)\mathcal{B})$.
(b) $\vdash (x)(\mathcal{A} \supset$ 4 $) \supset ((Ex)\mathcal{A} \supset (Ex)\mathcal{B})$.
(c) $\vdash (x)(\mathcal{A}$ A $\mathcal{B}) \equiv (x)\mathcal{A}$ A $(x)\mathcal{B}$.
(d) $\vdash (y_1) \ldots (y_n)\mathcal{A} \supset \mathcal{A}$.
(e) $\vdash \sim (x)\mathcal{B} \supset (Ex) \sim \mathcal{B}$.

2.27^D. Let K be a first-order theory, and let K# be an axiomatic theory having the following axioms: (1) (y,) . . . $(y_n)\mathcal{A}$ where $\mathcal{A}$ is any axiom of K and $y_1, \ldots,$ y, $(n \geqslant 0)$ are any variables; (2) $(y_1) \ldots (y_n)(\mathcal{A} \supset \mathcal{B}) \supset$ [(y,) . . . $(y_n)\mathcal{A} \supset$ $(y_1) \ldots (y_n)\mathcal{B}]$ where $\mathcal{A}$ and 4 are any wfs and $y_1, \ldots, y_n$ are any variables. Moreover, K# has the rule of modus ponens as its only rule of inference. Show that K# has the same theorems as K.

5. Completeness Theorems

PROPOSITION 2.7. *Every theorem of a first-order predicate calculus is logically valid.*

PROOF. By property (VII) of the notion of truth (cf. page 53), Axioms (1)–(3) are logically valid. By properties (X) (Corollary) and (XI), Axioms (4)–(5) are logically valid. By (III) and (VI), the rules of inference MP and Gen preserve logical validity. Hence, every theorem of a predicate calculus is logically valid.

EXERCISES

2.28. For any first-order theory K, if $\Gamma \vdash_K \mathcal{A}$ and each wf in Γ is true in a given model M of K, then $\mathcal{A}$ is also true in M.

2.29. If a wf $\mathcal{A}$ without quantifiers is provable in a predicate calculus, then it is an instance of a tautology, and, hence, by Proposition 2.1, has a proof without quantifiers using only Axioms (1)–(3) and MP. (Hint: if $\mathcal{A}$ were not a tautology, one could construct an interpretation having the set of terms occumng in $\mathcal{A}$ as its domain, in which $\mathcal{A}$ is not true, contradicting Proposition 2.7.) Note that this implies the consistency of the predicate calculus and also provides a decision procedure for provability of wfs without quantifiers.

Proposition 2.7 establishes only half of the completeness result that we are seeking. The other half will follow from a much more general proposition established below. First, we must prove a few preliminary lemmas.

If x_i and x_j are distinct, then $\mathcal{A}(x_i)$ and $\mathcal{A}(x_j)$ are said to be ***similar*** if and only if X, is free for x_i in $\mathcal{A}(x_i)$ and $\mathcal{A}(x_i)$ has no free occurrences of x_j. It is assumed here that $\mathcal{A}(x_j)$ arises from $\mathcal{A}(x_i)$ by substituting x_j for all free occurrences of x_i. If $\mathcal{A}(x_i)$ and $\mathcal{A}(x_j)$ are similar, then x_i is free for x_j in $\mathcal{A}(x_j)$ and $\mathcal{A}(x_j)$ has no free occurrences of x_i. Thus, similarity is a symmetric relation. Intuitively, $\mathcal{A}(x_i)$ and $\mathcal{A}(x_j)$ are similar if and only if $\mathcal{A}(x_j)$ has free occurrences of x, in exactly those places where $\mathcal{A}(x_i)$ has free occurrences of x_i.

LEMMA 2.8. *If* $\mathcal{A}(x_i)$ *and* $\mathcal{A}(x_j)$ *are similar, then* $\vdash (x_i)\mathcal{A}(x_i) \equiv (x_j)\mathcal{A}(x_j)$.

PROOF. $\vdash (x_i)\mathcal{A}(x_i) \supset \mathcal{A}(x_j)$ by Axiom (4). By Gen,

$$\vdash (x_j)((x_i)\mathcal{A}(x_i) \supset \mathcal{A}(x_j))$$

and, by Axiom (5), $\vdash (x_i)\mathcal{A}(x_i)$ 3 $(x_j)\mathcal{A}(x_j)$. In the same way, $\vdash (x_j)\mathcal{A}(x_j) \supset (x_i)\mathcal{A}(x_i)$. Hence, by the tautology A, ⊃ (A, ⊃ $(A_1 \wedge$ A,)), and Proposition 2.1, $\vdash (x_i)\mathcal{A}(x_i) \equiv (x_j)\mathcal{A}(x_j)$.

EXERCISE 2.30. *If* $\mathcal{A}(x_i)$ *and* $\mathcal{A}(x_j)$ *are similar, prove*: $\vdash (Ex_i)\mathcal{A}(x_i) \equiv$ (Ex,)&(+).

LEMMA 2.9. *If a* closed wf $\sim \mathcal{A}$ *of* K is not provable in *K*, then the theory K', obtained *from* K by adding $\mathcal{A}$ as an axiom, is consistent.

PROOF. Assume K' inconsistent. Then, for some wf $\mathcal{B}$, $\vdash_{K'}\mathcal{B}$ and $\vdash_{K'} \sim \mathcal{B}$. Now, $\vdash_{K'}\mathcal{B} \supset (\sim \$3\ 3 \sim \mathcal{A})$, by Proposition 2.1. So, $\vdash_{K'} \sim \mathcal{A}$. Hence, $\mathcal{A} \vdash_{K} \sim \mathcal{A}$. Since $\mathcal{A}$ is closed, we have $\vdash_{K}\mathcal{A}\ 3 \sim \mathcal{A}$, by Corollary 2.6 of the Deduction Theorem. However, by Proposition 2.1, $\vdash_{K}(\mathcal{A}\ 3 \sim \mathcal{A})\ 3 \sim \mathcal{A}$. Hence, $\vdash_{K} \sim \mathcal{A}$, contradicting our hypothesis. (Similarly, if $\mathcal{A}$ is not provable in K, then the new theory obtained by adding $\sim \mathcal{A}$ as an axiom to K is consistent.)

LEMMA 2.10. The set *of* expressions *of* a theory K is denumerable. (Hence the same is true *of* the set *of terms*, wfs, closed wfs, etc.)

PROOF. First assign a distinct odd number $g(u)$ to each symbol u as follows: $g(()=3$, $g())=5$, $g(,)=7$, $g(\sim)=9$, $g(\supset)=11$; $g(x_k)=5+8k$; $g(a_k)=7+8k$; $g(f_k^n)=9+8(2^n3^k)$; $g(A_k^n)=11+8(2^n3^k)$. Then, to an expression $u_1u_2\ldots u_r$, associate the number $2^{g(u_1)}3^{g(u_2)}\ldots p_r^{g(u_r)}$, where p_i is the i^{th} prime number. We can enumerate all expressions in the order of their associated numbers.

Moreover, if we can effectively tell whether any given symbol is a symbol of K, then this enumeration can be effectively carried out, and, in addition, we can effectively decide whether any given number is the number of an expression of K. The same holds true for terms, wfs, closed wfs, etc. If K is also axiomatic, i.e., if we can effectively decide whether any given wf is an axiom of K, then we can effectively enumerate the theorems of K as follows: Starting with a list consisting of the first axiom of K in the given enumeration (according to the associated numbers) of the axioms, add all the direct consequences of this axiom by MP and by Gen used only with x_1 as quantified variable. Add the second axiom to this new list (if it is not already there), and write down all new direct consequences of the wfs in this augmented list, this time with Gen used only with x_1, x_2. If at the k^{th} step, we add the k^{th} axiom and restrict Gen to the variables $x_1, \ldots, x_k$, we eventually obtain, in this manner, all theorems of K. However, in contradistinction to the case of expressions, wfs, terms, etc., it turns out that there are theories K for which we cannot tell in advance whether any given wf of K will eventually appear in the list of theorems.

We say that a theory K is complete if and only if, for any closed wf $\mathcal{A}$ of K, either $\vdash_{K}\mathcal{A}$ or $\vdash_{K} \sim \mathcal{A}$.

A theory K' having the same symbols as a theory K is said to be an extension of K if every theorem of K is a theorem of K'. (Obviously, it suffices to prove that every proper axiom of K is a theorem of K'.)

LEMMA 2.11 (LINDENBAUM'S LEMMA). If *K is* a consistent theory, then there is a consistent, complete extension *of* K.

PROOF. Let $\mathcal{B}_1, \mathcal{B}_2, \ldots,$ be an enumeration of all closed wfs of K, by Lemma 2.10. Define a sequence J_0, J,, $J_2, \ldots$ of theories in the following way. J_0 is K. Assume J, defined, with $n > 0$. If it is not the case that $\vdash_{J_n} \sim \mathcal{B}_{n+1}$ then let J_{n+1} be obtained from J_n by adding $\mathcal{B}_{n+1}$ as an additional axiom. On the other hand, if $\vdash_{J_n} \sim \mathcal{B}_{n+1}$, let $J_{n+1} = J_n$. Let J be the theory obtained by taking as axioms all the axioms of all the J_i's. Clearly, J_{n+1} is an extension of J_n, and J is an extension of all the J_i's, including $J_0 = K$. To show that J is consistent, it suffices to prove that all the J_i's are consistent, because a proof of a contradiction in J, involving as it does only a finite number of axioms, is also a proof of a contradiction in some J_n. We prove the consistency of the J_i's by induction. By hypothesis, $J_0 = K$ is consistent. Assume that J_i is consistent. If $J_{i+1} = J_i$, then J_{i+1} is consistent. If $J_i \neq J_{i+1}$ and, therefore, by the definition of J_{i+1}, $\sim \mathcal{B}_{i+}$, is not provable in J_i, then, by Lemma 2.9, J_{i+1} is also consistent. Hence, J_{i+1} is consistent if J_i is, and, therefore, J is consistent. To prove the completeness of J, let $\mathcal{A}$ be any closed wf of K. Then $\mathcal{A} = \mathcal{B}_{j+1}$ for some $j > 0$. Now, either $\vdash_{J_j} \sim \mathcal{B}_{j+1}$ or $\vdash_{J_{j+1}}\mathcal{B}_{j+1}$, since, if not $\vdash_{J_j} \sim \mathcal{B}_{j+1}$, then $\mathcal{B}_{j+1}$ is added as an axiom in J_{j+1}. Therefore, either $\vdash_{J} \sim \mathcal{B}_{j+1}$ or $\vdash_{J}\mathcal{B}_{j+1}$. Thus, J is a complete consistent extension of K.

Note that even if one can effectively determine whether any wf is an axiom of K, it may not be possible to do the same with (or even to effectively enumerate) the axioms of J, i.e., J may not be axiomatic even if K is. This is due to the possibility of not being able to determine, at each step, whether or not $\sim \mathcal{B}_{n+1}$ is provable in J_n.

EXERCISES

2.31. Show that a theory K is complete if and only if, for any closed wfs $\mathcal{A}$ and $\mathcal{B}$ of K, if $\vdash_{K}\mathcal{A} \vee \mathcal{B}$, then $\vdash_{K}\mathcal{A}$ or $\vdash_{K}\mathcal{B}$.

2.32.^{D} Prove that every consistent, decidable theory has a consistent, decidable, complete extension.

PROPOSITION 2.12.† Every consistent theory K has a denumerable model (*i.e.*, a model in which the domain is denumerable).

PROOF. Add to the symbols of K a denumerable set $\{b,, b_2, \ldots\}$ of new individual constants. Call this new theory K_0. Its axioms are those of K plus those logical axioms which involve the new constants. K_0 is consistent. For, if not, $\vdash_{K_0}\mathcal{A} \wedge \sim \mathcal{A}$ for some wf 6?. Replace each b_i appearing in this proof by a variable which does not appear in the proof. This transforms axioms into axioms

† The proof given here is due to Henkin [1949], as simplified by Hasenjaeger [1953]. The result was originally proved by Gödel [1930]. Other proofs have been published by Rasiowa-Sikorski [1951–52] and Beth [1951], using (Boolean) algebraic and topological methods, respectively. Still other proofs may be found in Hintikka [1955a, b] and in Beth [1959].

and preserves the correctness of the applications of the rules of inference. The final wf in the proof is still a contradiction, but now the proof does not involve any of the b_i's and therefore is a proof in K. This contradicts the consistency of K. Therefore, K_0 is consistent.

By Lemma 2.10, let $F_1(x_{i_1}), F_2(x_{i_2}), \ldots, F_k(x_{i_k}), \ldots$ be an enumeration of all wfs of K_0 having at most one free variable. (Let x_{i_k} be the free variable of F_k if the latter has a free variable; otherwise, let x_{i_k} be x,.) Choose a sequence $b_{j_1}, b_{j_2}, \ldots$ of some of the new individual constants such that b_{j_k} is not contained in $F_1(x_{i_1}), F_2(x_{i_2}), \ldots, F_k(x_{i_k})$, and such that b_{j_k} is different from each of $b_{j_1}, b_{j_2}, \ldots, b_{j_{k-1}}$. Consider the wf:

$$(S_k) \qquad \sim (x_{i_k})F_k(x_{i_k}) \supset \sim F_k(b_{j_k})$$

Let K_n be the theory obtained by adding (S,), . . . , (S_n) to the axioms of K_0, and let K, be the theory obtained by adding all the (S_i)'s as axioms to K_0. Any proof in K, contains only a finite number of the (S_i)'s, and will also be a proof in some K_n. Hence, if all the K_i's are consistent, so is K,. To demonstrate that all the K_i's are consistent, proceed by induction. We know that K_0 is consistent. Assume that K_{n-1} is consistent but that K_n is inconsistent (n $\geqslant$ 1). Then, as we know, any wf is provable in K_n (by the tautology A, 3 (--A, 3 A_2) and Proposition 2.1). In particular, $\vdash_{K_n} \sim (S_n)$. Hence, $(S_n) \vdash_{K_{n-1}} \sim (S_n)$. Since (S_n) is closed, we have, by Corollary 2.6, $\vdash_{K_{n-1}} (S_n) \, 3 \sim (S_n)$. But, by the tautology (A, $\supset$ ‾ A_1) $\supset \sim$ A, and Proposition 2.1, we then have $\vdash_{K_{n-1}}$ ‾ (S_n), i.e.,

$$\vdash_{K_{n-1}} \sim (\sim (x_{i_n})F_n(x_{i_n}) \supset \sim F_n(b_{j_n}))$$

Now, by the tautologies $\sim (A_1 \, 3$ A,) $\supset (A_1$ A $\sim$ A,); (A, A $A_2) \supset A_1$; $(A_1$ A $A_2)$ 3 A,; $\sim\sim A_1$ 3 A,, we obtain $\vdash_{K_{n-1}} \sim (x_{i_n})F_n(x_{i_n})$ and $\vdash_{K_{n-1}} F_n(b_{j_n})$. From the latter and from the fact that b_{j_n} does not occur in (S,), . . . , (S_{n-1}), we conclude $\vdash_{K_{n-1}} F_n(x_p)$, where x_p is a variable not occurring in the proof of $F_n(b_{j_n})$ in K_{n-1}. (Simply replace in the proof all occurrences of b_{j_n} by x_p.) By Gen, $\vdash_{K_{n-1}} (x_p)F_n(x_p)$, and, then by Lemma 2.8, $\vdash_{K_{n-1}} (x_{i_n})F_n(x_{i_n})$. (We use the fact that $F_n(x_{i_n})$ and $F_n(x_p)$ are similar.) But $\vdash_{K_{n-1}} \sim (x_{i_n})F_n(x_{i_n})$. This contradicts the assumed consistency of K_{n-1}. Hence, K_n must also be consistent. In this way, all the K_i's are consistent, and so also is K,. Note that K, is a consistent extension of K_0. Now, by Lemma 2.11, let J be a consistent, complete extension of K,.

By a closed term, we mean a term which contains no variables. The denumerable interpretation M of K_0 shall have as its domain the set of closed terms of K_0. (By Lemma 2.10, this is a denumerable set.) If c is an individual constant of K_0, its interpretation shall be c itself. If f_j^n is a function letter of K, then the associated operation $f_j^{n\star}$ in M shall have, for arguments t,, . . . , t_n (which are closed terms of K_0), the value $f_j^n(t_1, \ldots, t_n)$, which is a closed term of K_0. If A_j^n is a predicate letter of K, then the associated relation $(A_j^n)^\star$ in M shall hold, for arguments t,, . . . , t_n, if and only if $\vdash_J A_j^n(t_1, \ldots, t_n)$. To show that M is a model for K_0, it suffices to prove that a closed wf $\mathcal{A}$ of K_0 is true for M if and only if $\vdash_J \mathcal{A}$, because all theorems of K_0 are theorems of J. We prove this, by induction on the number of connectives and quantifiers in $\mathcal{A}$. First, let $\mathcal{A}$ be a closed atomic wf. Then, by definition, $\mathcal{A}$ is true for M if and only if $\vdash_J \mathcal{A}$. Now, assume that, for the induction step, if $\mathcal{B}$ is any closed wf with fewer connectives and quantifiers than $\mathcal{A}$, $\mathcal{B}$ is true for M if and only if $\vdash_J \mathcal{B}$.

Case 1. $\mathcal{A}$ is $\sim$ 3. If $\mathcal{A}$ is true for M, then $\mathcal{B}$ is false for M, and so, by inductive hypothesis, not-$\vdash_J \mathcal{B}$. Since J is complete and $\mathcal{B}$ is closed, $\vdash_J \sim \mathcal{B}$, i.e., $\vdash_J \mathcal{A}$. On the other hand, if $\mathcal{A}$ is not true for M, then $\mathcal{B}$ is true for M. Hence, $\vdash_J \mathcal{B}$. Since J is consistent, not-$\vdash_J \sim \mathcal{B}$, i.e., not-I,&.

Case 2. $\mathcal{A}$ is ($\mathcal{B} \supset$ C). Since $\mathcal{A}$ is closed, so are $\mathcal{B}$ and $\mathcal{C}$. If $\mathcal{A}$ is false for M, then $\mathcal{B}$ is true and $\mathcal{C}$ is false. Hence, by inductive hypothesis, $\vdash_J \mathcal{B}$ and not-$\vdash_J \mathcal{C}$. By the completeness of J, $\vdash_J \sim \mathcal{C}$. Therefore, by the tautology A, $\supset$ ($\sim A_2 \, 3 \sim$ (A, 3 A_2)), $\vdash_J \sim (\mathcal{B} \; 3 \; \mathcal{C})$, i.e., $\vdash_J \sim \mathcal{A}$, and so, by the consistency of J, not-I,&. On the other hand, if not-I,&, then, by the completeness of J, $\vdash_J \sim \mathcal{A}$. By the tautologies $\sim (A_1 \supset A_2)$ 3 A, and $\sim (A_1 \, 3 \, A_2) \supset \sim A_2$, we obtain $\vdash_J \mathcal{B}$ and $\vdash_J \sim \mathcal{C}$. Hence, $\mathcal{B}$ is true for M. By the consistency of J, not-$\vdash_J \mathcal{C}$, and, therefore, $\mathcal{C}$ is false for M. Thus, $\mathcal{A}$ is false for M.

Case 3. $\mathcal{A}$ is $(x_n)\mathcal{B}$. Let $\mathcal{B}$ be $F_k(x_{i_k})$. We may assume that x_n is x_{i_k}. (Otherwise, $\mathcal{B}$ is closed and does not contain x_n free. But, in this case, $\mathcal{A}$ is true if and only if $\mathcal{B}$ is true (by (VI) of page 53); moreover, $I_J\mathcal{A}$ if and only if $I^{J\mathcal{B}}$. Therefore, the result for $\mathcal{A}$ follows from that for $\mathcal{B}$.) Assume that $\mathcal{A}$ is true for M, but not $\vdash_J \mathcal{A}$. By the completeness of J, $\vdash_J \sim \mathcal{A}$, i.e., $\vdash_J \sim (x_{i_k})F_k(x_{i_k})$. But, $\vdash_J (S_k)$. Hence, I, $\sim F_k(b_{j_k})$. Since $\mathcal{A} = (x_{i_k})F_k(x_{i_k})$ is true for M, it follows (by (X), Corollary, page 54) that $F_k(b_{j_k})$ is true in M. So, by inductive hypothesis, $\vdash_J F_k(b_{j_k})$, contradicting the consistency of J. On the other hand, assume $\mathcal{A}$ false for M, but $\vdash_J \mathcal{A}$. Since $(x_{i_k})F_k(x_{i_k})$ is false for M, some sequence does not satisfy $(x_{i_k})F_k(x_{i_k})$. Hence, some sequence s does not satisfy $F_k(x_{i_k})$. Let t_{i_k} be the i_k^{th} component of s. Notice that $s^\star(t) =$ t for all closed terms t. Therefore, s does not satisfy $F_k(t)$, by (X), Corollary (i) (p. 54). Hence, $F_k(t)$ is false for M. But $\vdash_J (x_{i_k})F_k(x_{i_k})$. Hence, by Axiom (4), $\vdash_J F_k(t)$. By inductive hypothesis, $F_k(t)$ is, therefore, true for M, contradicting the falsity of $F_k(t)$ for M.

Thus, M is a denumerable model for J, and hence also for K_0. Since all theorems of **K** are theorems of K_0, M is also a denumerable model for K. (Notice that M is not necessarily effectively constructible. The interpretaton of predicate letters depends upon the concept of provability in J, and this, as was noted at the end of Lemma 2.11, may not be effectively decidable.)

COROLLARY 2.13. Any logically *valid* wf $\mathcal{A}$ of a theory K is a theorem of K.

PROOF. We need only consider closed wfs $\mathcal{A}$, since a wf $\mathcal{B}$ is logically valid if and only if its closure is logically valid, and $\mathcal{B}$ is provable in K if and only if its closure is provable in K. So, let $\mathscr{A}$ be a logically valid closed wf of K. Now, assume that $\mathscr{A}$ is not a theorem of K. Then, if we add $\sim \mathscr{A}$ as an axiom to K, the new theory K' is consistent (by Lemma 2.9). Hence, by Proposition 2.12, K' has a model **M.** Since $\sim \mathscr{A}$ is an axiom of K', $\sim \mathscr{A}$ is true in **M;** and, since $\mathscr{A}$ is logically valid, $\mathscr{A}$ is true in **M.** Hence, $\mathscr{A}$ is both true and false in **M,** which is impossible ((11), page 53). Thus, $\mathscr{A}$ must be a theorem of K.

COROLLARY 2.14 (GÖDEL'S COMPLETENESS THEOREM [1930]). *In any predicate calculus, the theorems are precisely the logically valid* wfs.

PROOF. By Proposition 2.7 and Corollary 2.13. (Gödel's original proof runs along quite different lines. For a constructive proof of a related result, cf. Herbrand [1930], [1970], and, for still other proofs, cf. Dreben [1952], Hintikka [1955a, b], Beth [1951], and Rasiowa-Sikorski [1950, 1951].)

COROLLARY 2.15.

(a) *$\mathscr{A}$ is true in every denumerable model of* K *if and only if* $\vdash_K \mathscr{A}$. *Hence, $\mathscr{A}$ is true in every model of K if and only if* $\vdash_K \mathscr{A}$.

(b) *If, in every model of* K, *every sequence, satisfying all* wfs *in a set* Γ *of* wfs, *also satisfies* $\mathscr{B}$, *then* $\Gamma \vdash_K \mathscr{B}$.

(c) *If a* wf $\mathscr{B}$ *of* K *is a logical consequence (cf. page* 56) *of a set* Γ *of* wfs *of* K, *then* $\Gamma \vdash_K \mathscr{B}$.

(d) *If the* wf $\mathscr{B}$ *of* K *is a logical consequence of a* wf $\mathscr{A}$ *of* K, *then* $\mathscr{A} \vdash_K \mathscr{B}$.

PROOF.

(a) We may assume $\mathscr{A}$ closed. If not-$\vdash_K \mathscr{A}$, then the theory K' = K + $\{\sim \mathscr{A}\}$ is consistent.† Hence, K' has a denumerable model **M.** However, $\sim \mathscr{A}$, being an axiom of K', is true in **M;** and since **M** is also a model for K, $\mathscr{A}$ is true in **M.** Therefore, $\mathscr{A}$ is true and false in **M,** which is a contradiction.

(b) Consider the theory K + Γ. The wf $\mathscr{B}$ is true in every model of this theory. Hence, by (a), $\vdash_{K+\Gamma} \mathscr{B}$. So, $\Gamma \vdash_K \mathscr{B}$.

(c) is a consequence of (b), and (d) is a special case of (c).

EXERCISE 2.33. *Show that* $\vdash_K \mathscr{A}$ *if and only if there is a wf* $\mathscr{C}$ *which is the closure of the conjunction of some axioms of K such that* $\mathscr{C} \supset \mathscr{A}$ *is logically valid.*

Corollaries 2.13–2.15 show that the syntactical approach to quantification theory by means of first-order theories is equivalent to the semantical approach through the notions of interpretations, models, logical validity, etc. For the propositional calculus, Corollary 1.14 demonstrated the analogous equivalence between the semantical notions (tautology, etc.) and the syntactical notions (theorem of L, etc.). Notice also that, in the propositional calculus, completeness of the system L (cf. Proposition 1.13) led to a solution of the decision problem. However, for first-order theories, we cannot obtain a decision procedure for logical validity, or, equivalently, for provability in a first-order predicate calculus. We shall prove this and related results later on (Chapter 5).

† If K is theory and A is a set of wfs of K, then K + A denotes the theory obtained from K by adding the wfs of A as additional axioms.

There is another important classical result which falls out of Proposition 2.12.

COROLLARY 2.16 (SKOLEM-LÖWENHEIM THEOREM [1919, 1915]). *Any theory K which has a model has a denumerable model.*

PROOF. If K has a model, then K is consistent (by (11), page 53). Hence, by Proposition 2.12, K has a denumerable model.

We have another stronger consequence of Proposition 2.12.

^{A}COROLLARY 2.17. *For any cardinal number* a $\geqslant \aleph_0$, *any consistent theory K has a model of cardinality* a.

PROOF. We know, by Proposition 2.12, that K has a denumerable model. Therefore, for our result, it suffices to prove the following lemma.

LEMMA. *If* a *and* β *are two cardinal numbers such that* a $\leqslant \beta$ *and if K has a model of cardinality* a, *then K has a model of cardinality* β.

PROOF. Let **M** be a model of K with domain D of cardinality a. Let D' be a set of cardinality β containing D. Extend the model **M** to an intepretation **M'** having D' as domain in the following way. Let c be a fixed element of D. We stipulate that the elements of D' – D behave like c. For example, if B_j^n is the interpretation in **M** of the predicate letter A_j^n, and $(B_j^n)'$ is the new interpretation in M', then, for any d,, . . . , d_n in D', $(B_j^n)'$ holds for (d,, . . . , d_n) if and only if B_j^n holds for (u,, . . . , u_n) where $u_i = d_i$ if 4 $\in$ D and u_i = c if $d_i \in$ D' – D. The interpretation of the function letters is extended in an analogous way, and the same interpretations as in **M** are taken for the individual constants. It is an easy exerçise to show, by induction on the number of connectives and quantifiers in a wf, that any wf $\mathscr{A}$ is true in **M'** if and only if it is true in **M.** Hence, **M'** is a model of K of cardinality β.

EXERCISES

2.34. (Compactness) If all finite subsets of the set of axioms of a theory K have models, prove that K has a model.

2.35.^{A} If, for some cardinal a $\geqslant \aleph_0$, **a wf & is true for every interpretation of cardinality** a, **prove that $\mathscr{A}$ is logically valid.**

2.36.^{A} If a wf $\mathscr{A}$ is true for all interpretations of cardinality a, **prove that $\mathscr{A}$ is true for all interpretations of cardinality** $\leqslant$ a.

237. (a) For any wf $\mathscr{A}$, prove that there are only a finite number of interpretations of $\mathscr{A}$ on a given domain of finite cardinality k.

(b) For any wf $\mathcal{A}$, prove that there is an effective way of determining whether $\mathcal{A}$ is true for all interpretations with domain of some fixed finite cardinality k.

(c) Let a wf $\mathcal{A}$ be called k-valid if it is true for all interpretations having k elements. Call $\mathcal{A}$ precisely k-valid if it is k-valid but not (k + 1)-valid. Show that (k + 1)-validity implies k-validity, and give an example of a wf which is precisely k-valid. (Cf. Hilbert-Bernays I [1934, 34-51; Wajsberg [1933])

2.38. Show that the following wf is true for all finite domains, but is false in some infinite domain.

$$\{(x)(y)(z)[A_1^2(x, x) \wedge (A_1^2(x, y) \wedge A_1^2(y, z) \supset A_1^2(x, z)) \wedge$$
$$(A_1^2(x, y) \vee A_1^2(y, x))]\} \supset (Ey)(x)A_1^2(y, x)$$

239. Prove that there is no theory K whose models are exactly the interpretations with finite domains.

2.40. Let $\mathcal{A}$ be any wf containing no quantifiers, function letters or individual constants.

(a) Show that a closed prenex wf (x,) . . . $(x_n)(Ey_1) \ldots (Ey_m)\mathcal{A}$ (with $m \geqslant 0$, $n \geqslant 1$) is logically valid if and only if it is true for every interpretation with a domain of n objects.

(b) Prove that a closed prenex wf (Ey$_1$) . . . $(Ey_m)\mathcal{A}$ is logically valid if and only if it is true for all interpretations with a domain of one element.

(c) Show that there is an effective procedure to determine the logical validity of all wfs of the forms given in Parts (a) and (b).

2.41. Let $\mathbf{K}_1$ and $\mathbf{K}_2$ be theories having the same set of symbols. Assume that any interpretation of $\mathbf{K}_1$ is a model of $\mathbf{K}_1$ if and only if it is not a model of $\mathbf{K}_2$. Prove that K, and $\mathbf{K}_2$ are finitely **axiomatizable**, that is, there are finite sets of sentences Γ and A such that, for any sentence $\mathcal{A}$, $\vdash_{\mathbf{K}_1}\mathcal{A}$ if and only if $\Gamma \vdash \mathcal{A}$, and $\vdash_{\mathbf{K}_2}\mathcal{A}$ if and only if A t $\mathcal{A}$.†

2.42.^{D} A set Γ of sentences is called an independent axiomatization of a theory K if (i) all sentences in Γ are theorems of K; (ii) $\Gamma \vdash \mathcal{A}$ for every theorem $\mathcal{A}$ of **K**;† (iii) for every sentence $\mathcal{B}$ of Γ, it is not the case that $\Gamma - \{\mathcal{B}\} \vdash \mathcal{B}$. Prove that every theory K has an independent axiomatization.

6. Some Additional Metatheorems

For the sake of smoothness in working with particular theories later, it is convenient to prove a few additional facts about theories. We assume in this section that we are dealing with some arbitrary theory K.

In many cases, one has proved $(x)\mathcal{A}(x)$ and one wants $\mathcal{A}(t)$, where t is a term free for x in $\mathcal{A}(x)$. This is justified by the

† Here, an expression $\Gamma \vdash$ &, without any subscript attached to $\vdash$, means that $\mathcal{A}$ is derivable from Γ using only logical axioms (that is, within the predicate calculus).

PARTICULARIZATION RULE *A4*. *If t is jree jor x in $\mathcal{A}(x)$, then $(x)\mathcal{A}(x) \vdash \mathcal{A}(t)$.*

PROOF. From $(x)\mathcal{A}(x)$ and the instance $(x)\mathcal{A}(x) \supset \mathcal{A}(t)$ of **Axiom (4)**, we obtain $\mathcal{A}(t)$ by **modus** ponens.

PROPOSITION 2.18. *If $\mathcal{A}$ and $\mathcal{B}$ are* wfs *and x is not free in $\mathcal{A}$, the following are theorems of K.*

(a) $\mathcal{A} \supset (x)\mathcal{A}$ (hence, by **Axiom (4)**, $\vdash \mathcal{A} \equiv (x)\mathcal{A}$)
(b) *(Ex)@*$\supset \mathcal{A}$ (hence, by rule **E4** below, $\vdash$ *(Ex)@*$\equiv \mathcal{A}$)
(c) $(x)(\mathcal{A} \supset \mathcal{B}) \equiv (\mathcal{A} \supset (x)\mathcal{B})$
(d) $(x)(\mathcal{B}$ *3* $\mathcal{A}) \equiv$ *((Ex)%* *3* $\mathcal{A})$

PROOF. Exercise.

A useful derived rule which is just the contrapositive of Rule *A4* is obtained in the following way.

Let t be a term which is free for x in a wf $\mathcal{A}(x, t)$, and let $\mathcal{A}(t, t)$ arise from $\mathcal{A}(x, t)$ by replacing all free occurrences of x by t.†

EXISTENTIAL RULE E4. $\mathcal{A}(t, t) \vdash (Ex)\mathcal{A}(x, t)$. *As special cases of Rule E4, we haue*

(i) $\mathcal{B}(t) \vdash$ *(Ex)%(x)*, whenever t is free for x in $\mathcal{B}(x)$.
(ii) $\mathcal{B}(x) \vdash (Ex)\mathcal{B}(x)$. This follows from (i) by taking t to be x.

To justify Rule E4 it suffices to show that $\vdash \mathcal{A}(t, t) \supset (Ex)\mathcal{A}(x, t)$. But, by **Axiom (4)**, $\vdash (x) \sim \mathcal{A}(x, t) \supset \sim \mathcal{A}(t, t)$. Hence, by the tautology $(A \supset \sim B) \supset (B \supset \sim A)$ and MP, $\vdash \mathcal{A}(t, t)$ *3* $\sim (x) \sim \mathcal{A}(x, t)$, which, in abbreviated form is: $\vdash \mathcal{A}(t, t) \supset (Ex)\mathcal{A}(x, t)$.

Example. $\vdash (x)\mathcal{A} \supset$ *(Ex)@*.

1.	$(x)\mathcal{A}$	Hyp
2.	$\mathcal{A}$	1, Rule *A4*
3.	*(Ex)@*	2, Rule E4
4.	$(x)\mathcal{A} \vdash$ *(Ex)@*	1–3
5.	$\vdash (x)\mathcal{A} \supset$ *(Ex)@*	*1–4*, Corollary 2.5

EXERCISES

2.43. Justify the following derived rules.

(a) Negation: Elimination $\sim\sim \mathcal{A} \vdash \mathcal{A}$
Introduction $\mathcal{A} \vdash \sim\sim \mathcal{A}$
(b) Conjunction: Elimination $\mathcal{A} \wedge \mathcal{B} \vdash \mathcal{A}$
$\mathcal{A} \wedge \mathcal{B} \vdash \mathcal{B}$
Introduction $\mathcal{A}, \mathcal{B} \vdash \mathcal{A}$ A $\mathcal{B}$

† $\mathcal{A}(x$, t) may or may not contain occurrences of t.

(c) Disjunction: Elimination $\mathcal{A} \supset \mathcal{C}, \mathcal{B} \supset \mathcal{C}, \mathcal{A} \vee \mathcal{B} \vdash \mathcal{C}$
Introduction $\mathcal{A} \vdash \mathcal{A} \vee \mathcal{B}$
$\mathcal{B} \vdash \mathcal{A} \vee \mathcal{B}$
(d) Biconditional: Elimination $\mathcal{A} \equiv \mathcal{B}, \mathcal{A} \vdash \mathcal{B}$ $\mathcal{A} \equiv \mathcal{B}, \sim \mathcal{A} \vdash \sim \mathcal{B}$
$\mathcal{A} \equiv \mathcal{B}, \mathcal{B} \vdash \mathcal{A}$ $\mathcal{A} \equiv \mathcal{B}, \sim \mathcal{B} \vdash \sim \mathcal{A}$
Introduction $\mathcal{A} \supset \mathcal{B}, \mathcal{B} \supset \mathcal{A} \vdash \mathcal{A} \equiv \mathcal{B}$

(e) Proof by Contradiction: If a proof of $\Gamma, \sim \mathcal{A} \vdash \mathcal{C} \wedge \sim \mathcal{C}$ involves no application of Gen using a variable free in $\mathcal{A}$, then $\Gamma \vdash \mathcal{A}$. (Similarly, from $\Gamma, \mathcal{A} \vdash \mathcal{C} \wedge \sim \mathcal{C}$, one obtains $\Gamma \vdash \sim \mathcal{A}$.)

2.44. Prove:
(a) $\vdash (x)(y)A_1^2(x, y) \supset (x)A_1^2(x, x)$
(b) $\vdash [(x)A_1^1(x)] \vee [(x)A_2^1(x)] \supset (x)(A_1^1(x) \vee A_2^1(x))$
(c) $\vdash (Ey)(A_1^1(y) \supset (y)A_1^1(y))$
(d) t— $(Ex)\mathcal{A} \equiv (x) \sim \mathcal{A}$
(e) $\vdash (x)\mathcal{A} \supset (x)(\mathcal{A} \vee \mathcal{B})$
(f) $\vdash (x)(y)(A_1^2(x, y) \supset \sim A_1^2(y, x)) \supset (x) \sim A_1^2(x, x)$
(g) $\vdash [(Ex)\mathcal{A} \supset (x)\mathcal{B}[\supset (x)(\mathcal{A} \supset \mathcal{B})$
(h) $\vdash (x)(\mathcal{A} \vee \mathcal{B}) \supset ([(x)\mathcal{A}] \vee (Ex)\mathcal{B})$

PROPOSITION 2.19. ***For any*** wfs $\mathcal{A}, \mathcal{B} : \vdash (x)(\mathcal{A} \equiv \mathcal{B}) \supset ((x)\mathcal{A} \equiv (x)\mathcal{B})$.

PROOF.

1.	$(x)(\mathcal{A} \equiv \mathcal{B})$	Hyp
2.	$(x)\mathcal{A}$	Hyp
3.	$\mathcal{A} \equiv \mathcal{B}$	1, Rule *A4*
4.	$\mathcal{A}$	2, Rule *A4*
5.	$\mathcal{B}$	3, *4*, Tautology $(\mathcal{A} \equiv \mathcal{B}) \supset (\mathcal{A} \supset \mathcal{B})$, MP
6.	$(x)\mathcal{B}$	5, Gen
7.	$(x)(\mathcal{A} \equiv \mathcal{B}), (x)\mathcal{A} \vdash (x)\mathcal{B}$	1–6
8.	$(x)(\mathcal{A} \equiv \mathcal{B}) \vdash (x)\mathcal{A} \supset (x)\mathcal{B}$	1–7, Prop. 2.4
9.	$(x)(\mathcal{A} \equiv \mathcal{B}) \vdash (x)\mathcal{B} \supset (x)\mathcal{A}$	Proved in a way similar to that for 8
10.	$(x)(\mathcal{A} \equiv \mathcal{B}) \vdash (x)\mathcal{A} \equiv (x)\mathcal{B}$	8, 9, Conjunction Rule
11.	$\vdash (x)(\mathcal{A} \equiv \mathcal{B}) \supset ((x)\mathcal{A} \equiv (x)\mathcal{B})$	1–10, Prop 2.4

PROPOSITION 2.20 ***(EQUIVALENCE THEOREM).*** ***If 93 is a subformula of $\mathcal{A}$, and $\mathcal{A}'$ is the result of replacing zero or more occurrences of $\mathcal{B}$ in $\mathcal{A}$ by a*** wf ***$\mathcal{C}$, and every free variable of $\mathcal{B}$ or $\mathcal{C}$ which is also a bound variable of $\mathcal{A}$ occurs in the list $y_1, \ldots, y_k$, then***

$$\vdash [(y_1) \ldots (y_k)(\mathcal{C} \equiv \mathcal{B})] \supset (\mathcal{A} \equiv \mathcal{A}')$$

Example. $(x)(A_2^1(x) \equiv A_1^1(x)) \supset [(Ex)A_1^1(x) \equiv (Ex)A_2^1(x)]$.

PROOF. Induction on the number n of connectives and quantifiers of $\mathcal{A}$. Note that if zero occurrences are replaced, then $\mathcal{A}'$ is $\mathcal{A}$, and the wf to be proved is an instance of the tautology $B\ 3\ (A \equiv A)$. If $\mathcal{B}$ is identical with $\mathcal{A}$, and this occurrence of $\mathcal{B}$ is replaced by $\mathcal{C}$ the wf to be proved, $(y,) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C}) \supset (\mathcal{B} \equiv \mathcal{C})$, is derivable (cf. page *64,* Exercise 2.26(d)) from Axiom *(4).* Thus, we may assume that $\mathcal{B}$ is a proper part of $\mathcal{A}$ and that at least one occurrence of $\mathcal{B}$ is replaced. Also let us assume the theorem for all wfs with fewer connectives and quantifiers than $\mathcal{A}$.

Case 1. $\mathcal{A}$ is an atomic wf. Then $\mathcal{B}$ cannot be a proper part of $\mathcal{A}$.

Case 2. $\mathcal{A}$ is $\sim \mathcal{D}$. Let $\mathcal{A}'$ be $\sim 9'$. By inductive hypothesis, $\vdash (y,) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C}) \supset (9 \equiv 9')$. Hence, by the tautology $(A \equiv B) \supset (\sim A \equiv \sim B)$, $\vdash (y_1) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C}) \supset (\mathcal{A} \equiv \mathcal{A}')$.

Case 3. $\mathcal{A}$ is $\mathcal{D}\ 3\ \mathcal{E}$. Let $\mathcal{A}'$ be $\mathcal{D}' \supset \mathcal{E}'$. By inductive hypothesis, $\vdash (y_1) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C}) \supset (9 \equiv 9')$ and $\vdash (y,) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C})\ 3\ (\mathcal{E} \equiv \mathcal{E}')$. Using the tautology $((A \equiv B) \wedge (C \equiv D))\ 3\ ((A\ 3\ C) \equiv (B \supset D))$, we obtain $\vdash (y_1) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C}) \supset (\mathcal{A} \equiv \mathcal{A}')$.

Case *4.* $\mathcal{A}$ is $(x)\mathcal{D}$. Let $\mathcal{A}'$ be $(x)\mathcal{D}'$. By inductive hypothesis, $\vdash (y_1) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C})\ 3\ (\mathcal{D} \equiv \mathcal{D}')$. Now, x does not occur free in $(y_1) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C})$, for, if it did, then it would be free in $\mathcal{B}$ or $\mathcal{C}$, and, since it is bound in $\mathcal{A}$, it would be one of $y,, \ldots, y_k$, and x would not be free in $(y,) \ldots (y_k)(\mathcal{B} \equiv C?)$. Hence, using Axiom (5), we obtain $\vdash (y_1) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C})\ 3\ (x)(\mathcal{D} \equiv \mathcal{D}')$. However, by Proposition 2.19, $\vdash (x)(\mathcal{D} \equiv \mathcal{D}')\ 3\ ((x)\mathcal{D} \equiv (x)\mathcal{D}')$. Thus,

$$\vdash (y_1) \ldots (y_k)(\mathcal{B} \equiv \mathcal{C}) \supset (\mathcal{A} \equiv \mathcal{A}').$$

COROLLARY 2.21 ***(REPLACEMENT THEOREM).*** ***Let $\mathcal{A}, \mathcal{B}, \mathcal{A}', \mathcal{C}$ be as in Proposition*** 2.20. ***If*** ⊢ % $\mathcal{C}$, ***then*** ⊢ @ @'. ***Also, if*** ⊢ % = (? ***and*** ⊢ @, ***then t*** $\mathcal{A}'$.

COROLLARY 2.22 ***(CHANGE OF BOUND VARIABLES).*** ***If $(x)\mathcal{B}(x)$ is a subformula of $\mathcal{A}$, and $\mathcal{B}(y)$ is similar to $\mathcal{B}(x)$, and $\mathcal{A}'$ is the result of replacing one or more occurrences of $(x)\mathcal{B}(x)$ in $\mathcal{A}$ by $(y)\mathcal{B}(y)$, then $\vdash \mathcal{A} \equiv \mathcal{A}'$.***

PROOF. Apply Lemma 2.8 and Corollary 2.21.

EXERCISES

2.45. Prove $\vdash$ (Ex) $\sim \mathcal{A} \equiv \sim (x)\mathcal{A}$ and $\vdash (x)\mathcal{A} \equiv \sim$ (Ex) $\sim \mathcal{A}$.

2.46. Let $\mathcal{A}$ be a wf involving only quantifiers and $\wedge, \vee, \sim$, but not $\supset, \equiv$. Exchange universal and existential quantifiers, and exchange $\wedge$ and $\vee$. The result $\mathcal{A}^\star$ is called the dual of $\mathcal{A}$.

(i) In any predicate calculus, prove: (a) $\vdash \mathscr{A}$ if and only if $\vdash \sim \mathscr{A}^{\star}$; (b) $\vdash \mathscr{A} \supset \mathscr{B}$ if and only if $\vdash \mathscr{B}^{\star} \supset \mathscr{A}^{\star}$; (c) $\vdash \mathscr{A} \equiv \mathscr{B}$ if and only if $\vdash \mathscr{A}^{\star} \equiv \mathscr{B}^{\star}$; (d) Using $\vdash (x)(\mathscr{A} \wedge \mathscr{B}) \equiv ((x)\mathscr{A}) \wedge (x)\mathscr{B}$ (cf. p. 64, Exercise 2.26(c)), prove $\vdash$ (Ex)(@$\vee$ $\mathscr{B}$) $\equiv$ (Ex)@$\vee$ $(Ex)\mathscr{B}$.

(ii) Show that the duality results of Part (i), (a)–(c), do not hold for arbitrary theories.

2.47. If 8 is obtained from $\mathscr{A}$ by erasing all quantifiers (x) or (Ex) whose scope does not contain x free, prove that $\vdash \mathscr{A} \equiv \mathscr{B}$.

2.48. Write formulas logically equivalent to the negations of the formulas below; in the new formulas, all negations are to apply to atomic formulas.

(a) $(x)(y)(Ez)A_1^3(x, y, z)$

(b) $(\varepsilon)(\varepsilon > 0 \supset (E\delta)(\delta > 0$ A $(x)(|x - c| < \delta \supset |f(x) - f(c)| < \varepsilon)))$

(c) $(\varepsilon)(\varepsilon > 0 \supset (En)(m)(m > n \supset |a_m - b| < \varepsilon))$

2.49. Prove: (a) $\vdash$ (Ex)(@$\supset\sim$(8 $\vee$ $\mathscr{C}$)) $\equiv (Ex)(\mathscr{A} \supset (\sim \mathscr{B}$ A $\sim \mathscr{C}))$ (b) $\vdash (Ey)(\mathscr{A}(y)$ V $(y)\mathscr{B}(y)) \equiv (Ey)(\mathscr{A}(y)$ V $(z)\mathscr{B}(z))$.

2.50. Show by a counterexample that we cannot omit the quantifiers $(y_1) \ldots (y_k)$ in Proposition 2.20.

7. Rule *C*

It is very common in mathematics to reason in the following way. Assume that we have proved a wf of the form $(Ex)\mathscr{A}(x)$. Then, we say, let b be an object such that $\mathscr{A}(b)$. We continue the proof, finally arriving at a formula which does not involve the arbitrarily chosen element b.

For example, let us say that we wish to show that $(Ex)(\mathscr{B}(x) \supset \mathscr{C}(x)), (x)\mathscr{B}(x) \vdash (Ex)\mathscr{C}(x)$.

1.	$(Ex)(\mathscr{B}(x) \supset \mathscr{C}(x))$	Hyp
2.	$(x)\mathscr{B}(x)$	Hyp
3.	$\mathscr{B}(b) \supset \mathscr{C}(b)$ for some b	1
4.	$\mathscr{B}$(b)	2, Rule A4
5.	$\mathscr{C}(b)$	3, 4, MP
6.	$(Ex)\mathscr{C}(x)$	5, Rule FA
7.	$(Ex)(\mathscr{B}(x) \supset \mathscr{C}(x)), (x)\mathscr{B}(x) \vdash (Ex)\mathscr{C}(x)$	1–6

Such a proof seems to be perfectly legitimate, on an intuitive basis. In fact, we can achieve the same result without making an arbitrary choice of an element b as in step 3. This can be done as follows:

1.	$(x)\mathscr{B}(x)$	Hyp
2.	$(x) \sim \mathscr{C}(x)$	Hyp
3.	$\mathscr{B}(x)$	1, Rule A4
4.	$\sim \mathscr{C}(x)$	2, Rule A4
5.	$\sim (\mathscr{B}(x) \supset \mathscr{C}(x))$	3, 4, Tautology (A A $\sim B) \supset \sim$ (A $\supset$ B)
6.	$(x) \sim (\mathscr{B}(x) \supset \mathscr{C}(x))$	5, Gen
7.	$(x)\mathscr{B}(x), (x) \sim \mathscr{C}(x) \vdash (x) \sim (\mathscr{B}(x)$ з $\mathscr{C}(x))$	1–6
8.	$(x)\mathscr{B}(x) \vdash [(x) \sim \mathscr{C}(x)] \supset [(x) \sim (\mathscr{B}(x) \supset \mathscr{C}(x))]$	7; Prop. 2.4
9.	$(x)\mathscr{B}(x) \vdash [\sim (x) \sim (\mathscr{B}(x) \supset \mathscr{C}(x))] \supset [\sim (x) \sim \mathscr{C}(x)]$	8, Tautology (A $\supset$ B) $\supset$ ($\sim$ B $\supset \sim$ A)
10.	$(x)\mathscr{B}$(x) $\vdash$ (Ex)(%(x) $\supset \mathscr{C}(x)) \supset (Ex)\mathscr{C}(x)$	Abbreviation of 9
11.	(Ex)(%(x) $\supset \mathscr{C}(x)), (x)\mathscr{B}$(x) $\vdash (Ex)\mathscr{C}(x)$	10, MP

In general, any wf which can be proved using arbitrary acts of choice, can also be proved without such acts of choice. We shall call the rule which permits us to go from $(Ex)\mathscr{A}(x)$ to $\mathscr{A}(b)$, *Rule* C (“C” for "choice"). More precisely, the definition of a Rule C deduction in a first-order theory K is as follows:

$\Gamma \vdash_C \mathscr{A}$ if and only if there is a sequence of wfs $\mathscr{B}_1, \ldots, \mathscr{B}_n = \mathscr{A}$ such that the following four statements hold.

(I) For each i, either

(i) $\mathscr{B}_i$ is an axiom of K, or

(ii) $\mathscr{B}_i$ is in Γ, or

(iii) $\mathscr{B}_i$ follows by MP or Gen from preceding wfs in the sequence, or

(iv) There is a preceding wf $(Ex)\mathscr{C}(x)$ and $\mathscr{B}_i$ is $\mathscr{C}(d)$, where d is a new individual constant. (Rule C)

(II) As axioms in **(I)(i)**, we can also use all logical axioms involving the new individual constants already introduced by applications of **(I)(iv)**, Rule C.

(III) No application of Gen is made using a variable which is free in some $(Ex)\mathscr{C}(x)$ to which Rule C has been previously applied.

(IV) $\mathscr{A}$ contains none of the new individual constants introduced in any application of Rule C.

A word should be said about the reason for including clause **(III)**. Without this clause, we could proceed as follows:

1.	$(x)(Ey)A_1^2(x, y)$	Hyp
2.	$(Ey)A_1^2(x, y)$	1, Rule A4
3.	$A_1^2(x, b)$	2, Rule C with b
4.	$(x)A_1^2(x, b)$	3, Gen
5.	$(Ey)(x)A_1^2(x, y)$	4, Rule E4
6.	$(x)(Ey)A_1^2(x, y) \vdash_C (Ey)(x)A_1^2(x, y)$	1–5

However, (cf. page 57, **(4))**, there is an interpretation for which $(x)(Ey)A_1^2(x, y)$ is true but $(Ey)(x)A_1^2(x,$ y) is false.

PROPOSITION 2.23. If $\Gamma \vdash_C \mathscr{A}$, then $\Gamma \vdash \mathscr{A}$. Moreover, from the proof below it is easy to verify that if there is an application of Gen in the new proof of $\mathscr{A}$ from Γ using a certain variable and applied to a wf depending upon a certain wf of Γ, then there was such an application of Gen in the original proof.?

PROOF. Let $(Ey_1)\mathscr{C}_1(y_1), \ldots, (Ey_k)\mathscr{C}_k(y_k)$ be the wfs, in order of occurrence, to which Rule C is applied in the proof of $\Gamma \vdash_C \mathscr{A}$, and let $c_1, \ldots, c_k$ be the corresponding new individual constants. Then $\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_k(c_k) \vdash \mathscr{A}$; but then, by clause (III) of the definition above, and the Deduction Theorem 2.4, $\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \mathscr{C}_k(c_k) \supset \mathscr{A}$. Replace c_k everywhere by a variable z not occurring in the proof. Then

$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \mathscr{C}_k(z)$ 3 $\mathscr{A}$,	and, by Gen,
$\Gamma, \mathscr{C}_1(c_1), \quad , \mathscr{C}_{k-1}(c_{k-1}) \quad (z)(\mathscr{C}_k(z) \supset \mathscr{A})$.	Hence, by Proposition 2.18(d),
$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash (Ey_k)\mathscr{C}_k(y_k) \supset \mathscr{A}$.	But,
$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash (Ey_k)\mathscr{C}_k(y_k)$.	Hence

$$\Gamma, \mathscr{C}_1(c_1), \ldots, \mathscr{C}_{k-1}(c_{k-1}) \vdash \mathscr{A}.$$

Repeating this argument, we can eliminate $\mathscr{C}_{k-1}(c_{k-1}), \ldots, \mathscr{C}_1(c_1)$ one after the other, obtaining $\Gamma \vdash$ 62.

Example. $\vdash (x)(\mathscr{A}(x) \supset \mathscr{B}(x)) \supset ((Ex)\mathscr{A}(x) \supset (Ex)\mathscr{B}(x))$

1.	$(x)(\mathscr{A}(x)$ 3 $\mathscr{B}(x))$	Hyp
2.	$(Ex)\mathscr{A}(x)$	Hyp
3.	$\mathscr{A}(b)$	2, Rule C with b
4.	$\mathscr{A}(b) \supset \mathscr{B}(b)$	1, Rule A4
5.	$\mathscr{B}(b)$	3, 4, MP
6.	(Ex)%(x)	5, Rule E4
7.	$(x)(\mathscr{A}(x) \supset \mathscr{B}(x)), (Ex)\mathscr{A}(x) \vdash_C (Ex)\mathscr{B}(x)$	1–6
8.	$(x)(\mathscr{A}(x) \supset \mathscr{B}(x)), (Ex)\mathscr{A}(x) \vdash (Ex)\mathscr{B}(x)$	7, Prop. 2.23
9.	$(x)(\mathscr{A}(x) \supset \mathscr{B}(x)) \vdash (Ex)\mathscr{A}(x) \supset (Ex)\mathscr{B}(x)$	8, Prop. 2.4
10.	$\vdash (x)(\mathscr{A}(x) \supset \mathscr{B}(x)) \supset ((Ex)\mathscr{A}(x) \supset (Ex)\mathscr{B}(x))$	9, Prop. 2.4

EXERCISES

Use Rule C and Proposition 2.23 to prove Exercises 2.51–2.58 below.

2.51. $\vdash (Ex)(\mathscr{A}(x)$ 3 $\mathscr{B}(x))$ 3 $((x)\mathscr{A}(x) \supset (Ex)\mathscr{B}(x))$

2.52. $\vdash \sim (Ey)(x)(A_1^2(x,y) \equiv \sim A_1^2(x,x))$

[†] The first formulation of a version of Rule C similar to that given here seems to be due to Rosser [1953].

2.53. $\vdash [(x)(A_1^1(x) \supset A_2^1(x) \vee A_3^1(x)) \wedge \sim (x)(A_1^1(x) \supset A_2^1(x))] \supset (Ex)(A_1^1(x) \wedge A_3^1(x))$

2.54. $\vdash [(Ex)\mathscr{A}(x)]$ A $[(x)\mathscr{B}(x)]$ 3 $(Ex)(\mathscr{A}(x)$ A $\mathscr{B}(x))$

2.55. $\vdash (Ex)\mathscr{B}(x) \supset (Ex)(\mathscr{A}(x) \vee \mathscr{B}(x))$

2.56. $\vdash (Ex)(Ey)\mathscr{A}(x,y) \equiv (Ey)(Ex)\mathscr{A}(x,y)$

2.57. $\vdash (Ex)(y)\mathscr{A}(x,y)$ 3 $(y)(Ex)\mathscr{A}(x,y)$

2.58. $\vdash (Ex)(\mathscr{A}(x)$ A $\mathscr{B}(x)) \supset [(Ex)\mathscr{A}(x)]$ A $[(Ex)\mathscr{B}(x)]$

2.59. What is wrong with the following alleged derivations?

(a)	1.	$(Ex)\mathscr{A}(x)$	Hyp
	2.	$\mathscr{A}(b)$	1, Rule C
	3.	$(Ex)\mathscr{B}(x)$	Hyp
	4.	$\mathscr{B}(b)$	3, Rule C
	5.	$\mathscr{A}(b)$ A $\mathscr{B}(b)$	2, 4, Conjunction Rule
	6.	$(Ex)(\mathscr{A}(x) \wedge \mathscr{B}(x))$	5, Rule E4
	7.	$(Ex)\mathscr{A}(x), (Ex)\mathscr{B}(x) \vdash (Ex)(\mathscr{A}(x)$ A $\mathscr{B}(x))$	1–6, Proposition 2.23.
(b)	1.	$(Ex)(\mathscr{A}(x) \supset \mathscr{B}(x))$	Hyp
	2.	$(Ex)\mathscr{A}(x)$	Hyp
	3.	$\mathscr{A}(b)$ 3 $\mathscr{B}(b)$	1, Rule C
	4.	$\mathscr{A}(b)$	2, Rule C
	5.	$\mathscr{B}(b)$	3, 4, MP
	6.	$(Ex)\mathscr{B}(x)$	5, Rule E4
	7.	$(Ex)(\mathscr{A}(x)$ 3 $\mathscr{B}(x)), (Ex)\mathscr{A}(x) \vdash (Ex)\mathscr{B}(x)$	1–6, Proposition 2.23.

8. First-Order Theories with Equality

Let K be a theory which has as one of its predicate letters A_1^2. Let us write $t = s$ as an abbreviation for $A_1^2(t, s)$, and $t \neq s$ as an abbreviation for $\sim A_1^2(t, s)$. Then K is called a first-order theory with equality (or simply a theory with equality) if the following are theorems of K.

(6)† $(x_1)(x_1 = x_1)$ (Reflexivity of Equality)

(7) $x = y \supset (\mathscr{A}(x, x) \supset \mathscr{A}(x, y))$ (Substitutivity of Equality)

where x and y are any variables, $\mathscr{A}(x, x)$ is any wf, and $\mathscr{A}(x, y)$ arises from $\mathscr{A}(x, x)$ by replacing some, but not necessarily all, free occurrences of x by y, with the proviso that y is free for the occurrences of x which it replaces. Thus, $\mathscr{A}(x, y)$ may or may not contain free occurrences of x.

PROPOSITION 2.24. In any theory with equality,

(a) for any term t, $\vdash t = t$

(b) $\vdash x = y \supset y = x$

(c) $\vdash x = y \supset (y = z \supset x = z)$.

[†] The numbering here is a continuation of the numbering of the Logical Axioms on pp. ***59–60.***

PROOF. (a) From (6), $\vdash (x_1)(x_1 = x,)$; hence, by Rule *A4*, $\vdash t = t$. (b) Let $\mathscr{A}(x, x)$ be $x = x$ and $\mathscr{A}(x, y)$ be $y = x$. Then, by (7), $\vdash x = y \supset (x = x \supset y = x)$. But, by (a), $\vdash x = x$. So, by the tautology $B \supset ((A \supset (B \supset C)) \supset (A \supset C))$, we have $\vdash x = y \supset y = x$. (c) Let $\mathscr{A}(y, y)$ be $y = z$ and $\mathscr{A}(y, x)$ be $x = z$. Then, by (7), with x and y interchanged, $\vdash y = x \supset (y = z \supset x = z)$. But, by (b), $\vdash x = y \supset y = x$. Hence, using the tautology $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$, we have: $\vdash x = y \supset (y = z \supset x = z)$.

EXERCISES

2.60. Show that *(6)* **and (7) are true for any model M in which** $(A_1^2)^M$ **is the identity relation on the domain of the model.**

2.61. Prove the following in any theory with equality.

(a) $\vdash (x)(\mathscr{B}(x) \equiv (Ey)(x = y \wedge \mathscr{B}(y)))$ if y **does not occur in** $\mathscr{B}(x)$.
(b) $\vdash (x)(\mathscr{B}(x) \equiv (y)(x = y \supset \mathscr{B}(y)))$ **if** y **does not occur in** $\mathscr{B}(x)$.
(c) $\vdash (x)(Ey)(x = y)$.

We can reduce condition *(7)* for equality to a few simpler cases.

PROPOSITION 2.25. *Let K be a theory for which (6) holds and (7) holds for atomic* wfs $\mathscr{A}(x, x)$. *Then K is a theory with equality,* i.e., *(7) holds for all* wfs $\mathscr{A}(x, x)$.

PROOF. We must prove *(7)* for all wfs $\mathscr{A}(x, x)$. It holds for atomic wfs by assumption. Note that we have Proposition 2.24, since its proof used *(7)* only with atomic wfs. Proceeding by induction on the number n of connectives and quantifiers in $\mathscr{A}$, we assume that *(7)* holds for all k < n.

Case 1. $\mathscr{A}(x, x)$ is $\sim 93(x, x)$. By inductive hypothesis, we have $\vdash y = x \supset (\mathscr{B}(x,y) \supset \mathscr{B}(x,x))$, since $\mathscr{B}(x,x)$ arises from $\mathscr{B}(x,y)$ by replacing some occurrences of y by x. Hence, by Proposition 2.24(b), and the tautologies $(A \supset B) \supset (\sim B \supset \sim A)$ and $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$, we obtain $\vdash x = y \supset (\mathscr{A}(x, x) \supset \mathscr{A}(x, y))$.

Case 2. $\mathscr{A}(x, x)$ is $\mathscr{B}(x,x) \supset \mathscr{C}(x, x)$. By inductive hypothesis, and Proposition 2.24(b), $\vdash x = y \supset (93(x,y) \supset \mathscr{B}(x,x))$ and $\vdash x = y \supset (\mathscr{C}(x, x) \supset \mathscr{C}(x, y))$. Hence, by the tautology $(A \supset (B, \supset B)) \supset [(A \supset (C \supset C_1)) \supset (A \supset ((B \supset C) \supset (B, \supset C_1)))$, we have $\vdash x = y \supset (\mathscr{A}(x, x) \supset \mathscr{A}(x, y))$.

Case 3. $\mathscr{A}(x, x)$ is $(z)\mathscr{B}(x, x, z)$. By inductive hypothesis, $\vdash x = y \supset (\mathscr{B}(x, x, z) \supset \mathscr{B}(x, y, z))$. Now, by Gen and Axiom (5), $\vdash x = y \supset (z)(\mathscr{B}(x, x, z) \supset \mathscr{B}(x, y, z))$. By Exercise 2.26(a) on page 64, $\vdash (z)(\mathscr{B}(x, x, z) \supset \mathscr{B}(x, y, z)) \supset [(z)(\mathscr{B}(x, x, z)) \supset (z)(\mathscr{B}(x, y, z))]$, and so, by the tautology $(A \supset B) \supset ((B \supset C) \supset (A \supset C))$, $\vdash x = y \supset (\mathscr{A}(x, x) \supset \mathscr{A}(x, y))$.

The instances of *(7)* can be still further reduced.

PROPOSITION 2.26. *Let K be a theory in which (6) holds and (7) holds for all atomic* wfs $\mathscr{A}(x, x)$ *such that no function letters occur in* $\mathscr{A}(x, x)$ *and* $\mathscr{A}(x, y)$ *comes from* $\mathscr{A}(x, x)$ *by replacing exactly one occurrence of* x *by* y. *In addition, we assume the following:(*) for any function letter* f_j^n, *if* $z_1, \ldots, z_n$ *are variables and* $f_j^n(w_1, \ldots, w_n)$ *arises from* $f_j^n(z_1, \ldots, z_n)$ *by replacing one occurrence of* x *by* y, *then* $\vdash x = y \supset (f_j^n(z_1, \ldots, z_n) = f_j^n(w_1, \ldots, w_n))$. *Then K is a theory with equality.*

PROOF. Note, by repeated application, our assumptions can be extended to replacements of more than one occurrence of x by y. Also, Proposition 2.24 is still derivable. By Proposition 2.25, it suffices to prove *(7)* only for atomic wfs. But, one can easily prove $\vdash (y_1 = z_1 \wedge \ldots \wedge y_n = z_n) \supset (\mathscr{A}(y_1, \ldots, y_n) \supset \mathscr{A}(z_1, \ldots, z_n))$ for all variables $y_,, \ldots, y_n, z_,, \ldots, z_n$ and any atomic wf $\mathscr{A}$ without function letters. Hence, using Rule *A4*, we reduce the problem to showing that if $t(x, x)$ is a term and $t(x, y)$ comes from $t(x, x)$ by replacing some occurrences of x by y, then $\vdash x = y \supset (t(x, x) = t(x, y))$. But, this can be proved, using (*), by induction on the number of function letters in t, and we leave this as an exercise.

EXERCISES

2.62. Let K_1 **be a theory having only** $=$ **as a predicate letter, and no function letters or individual constants; and let its proper axioms be** $(x_1)(x_1 = x,)$, $(x_1)(x_2)(x_1 = x_2 \supset x_2 = x_1)$, **and** $(x_1)(x_2)(x_3)(x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3))$. **Show that** K_1 **is a theory with equality. Hint: by Proposition** 2.26, **it suffices to prove the following wfs:**

$$x = y \supset (x = x \supset y = x)$$
$$x = y \supset (x = x \supset x = y)$$
$$x = y \supset (x = y \supset y = y)$$
$$x = y \supset (y = x \supset y = y)$$
$$x = y \supset (x = z \supset y = z)$$
$$x = y \supset (z = x \supset z = y)$$

K_1 **is called the first-order theory of equality.**

2.63. Let K_2 **be a theory having only** $=$ **and** $<$ **as predicate letters, and no function letters or individual constants. Let** K_2 **have the proper axioms:**

(a) $(x_1)(x_1 = x_1)$
(b) $(x_1)(x_2)((x_1 = x_2) \supset (x_2 = x_1))$
(c) $(x_1)(x_2)(x_3)(x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3))$
(d) $(x_1)(Ex_2)(Ex_3)(x_1 < x_2 \wedge x_3 < x_1)$
(e) $(x_1)(x_2)(x_3)(x_1 < x_2 \wedge x_2 < x_3 \supset x_1 < x_3)$
(f) $(x_1)(x_2)(x_1 = x_2 \supset \sim x_1 < x_2)$
(g) $(x_1)(x_2)(x_1 < x_2 \vee x_1 = x_2 \vee x_2 < x_1)$
(h) $(x_1)(x_2)(x_1 < x_2 \supset (Ex_3)(x_1 < x_3 \wedge x_3 < x_2))$

Using Proposition 2.26, show that K_2 is a theory with equality. (K_2 is the theory of densely-ordered sets with neither first nor last element.)

2.64. Let K **be any theory with equality. (a) Prove that** $\vdash_K x_1 = y_1 \wedge \ldots \wedge x_n = y_n \supset t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)$, **where** $t(y_1, \ldots, y_n)$ **arises from a term**

$t(x_1, \dots, x_n)$ by substitution of $y_1, \dots, y_n$ for $x_1, \dots, x_n$, respectively. (b) *Prove that $\vdash_K x_1 = y_1 \wedge \dots \wedge x_n = y_n \supset (\mathscr{A}(x_1, \dots, x_n) \equiv \mathscr{A}(y_1, \dots, y_n))$ where $\mathscr{A}(y_1, \dots, y_n)$ is obtained by substituting $y_1, \dots, y_n$ for one or more free occurrences of $x,, \dots, x_n$, respectively, in the wf $\mathscr{A}(x_1, \dots, x_n)$, and $y_1, \dots, y_n$ are free for $x,, \dots, x,,$ respectively, in the wf $\mathscr{A}(x_1, \dots, x,)$.*

Examples. (In the literature, "elementary" is sometimes used instead of "first-order".)

1. Elementary Theory G of Groups: predicate letter =, function letter f_1^2, and individual constant a,. We abbreviate $f_1^2(t, s)$ by t + s, and a, by 0. The proper axioms are:

(a) $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$
(b) $x_1 + 0 = x_1$
(c) $(x_1)(Ex_2)(x_1 + x_2 = 0)$
(d) $x_1 = x_1$
(e) $x_1 = x_2 \supset x_2 = x_1$
(f) $x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)$
(g) $x, = x_2 \supset (x, + x_3 = x_2 + x_3 \wedge x_3 + x_1 = x_3 + x_2)$

From Proposition 2.26, one easily proves that G is a theory with equality. If one adds to the axioms the following wf

(h) $x_1 + x_2 = x, + x_1$

the new theory G_C is called the elementary theory of abelian groups.

2. Elementary Theory F of Fields: predicate letter =, function letters f_1^2 and f_2^2, and individual constants a, and a,. Abbreviate $f_1^2(t, s)$ by t + s and $f_2^2(t, s)$ by t . s and a, and a, by 0 and 1. As proper axioms, take (a)–(h) of (1) above, plus

(i) $x_1 = x_2 \mathrel{3} (x_1 \cdot x_3 = x_2 \cdot x_3 \wedge x_3 \cdot x_1 = x_3 \cdot x_2)$
(j) $(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)$
(k) $x_1 \cdot (x_2 + x_3) = (x_1 . x_2) + (x_1 . x_3)$
(1) $x_1 \cdot x_2 = x_2 \cdot x_1$
(m) $x_1 \cdot 1 = x,$
(n) $x, \neq 0 \supset (Ex_2)(x_1 \cdot x_2 = 1)$
(0) $0 \neq 1$

F is a theory with equality. Axioms (a)–(m) define the elementary theory R_C of commutative rings with unit. If we add to F the predicate letter A_2^2, denoting $A_2^2(t, s)$ by $t < s$, and add the axioms (e), (f), (g) of Exercise 2.63 above, as well as $x_1 < x_2 \mathrel{3} x_1 + x_3 < x_2 + x_3$ and $x, < x_2 \wedge 0 < x_3 \mathrel{3} x_1 \cdot x_3 < x_2 \cdot x_3$, then the new theory $F_<$ is called the elementary theory of ordered fields.

EXERCISE 2.65. Show that the axioms *(d)–(f)* of equality (*reflexivity, symmetry*, transitiuity), mentioned in Examples 1 and 2 *above*, can be replaced by (d) *and (f')*: $x = y \mathrel{3} (z = y \mathrel{3} x = z)$.

One often encounters first-order theories K in which = may be defined, i.e., there is a wf $\mathscr{E}(x, y)$ with two free variables x, y such that, if we abbreviate $\mathscr{E}(t, s)$ by t = s, then (6) and (7) are provable in K. We make the convention that, if t and s are terms that are not free for x and y, respectively, in $\mathscr{E}(x, y)$ then we take t = s to be the abbreviation not of $\mathscr{E}(t, s)$ but rather of a wf $\mathscr{E}^\star(t, s)$ obtained from $\mathscr{E}(t, s)$ by suitable changes of bound variables (cf. Corollary 2.22) so that t and s are free for x and y, respectively, in $\mathscr{E}^\star(x, y)$. Analogues of Propositions 2.25 and 2.26 hold for such theories if, in the propositions, we assume (7) also for suitable wfs of the form $\mathscr{E}^\star(t, s)$. (Exercise) There is no harm in extending the name "theory with equality" to cover such theories.

In first-order theories with equality, it is possible to define phrases using the expression "There exists one and only one x such that . . . " in the following way.

DEFINITION. $(E_1x)\mathscr{A}(x)$ for $(Ex)\mathscr{A}(x) \wedge (x)(y)(\mathscr{A}(x) \wedge \mathscr{A}(y) \mathrel{3} x = y)$.†

EXERCISES

Prove:

2.66. $\vdash (x)(E_1 y)(x = y)$
2.67. $\vdash (E_1x)\mathscr{A}(x) \equiv (Ex)(y)(x = y \equiv \mathscr{A}(y))$
2.68. $\vdash (x)(\mathscr{A}(x) \equiv \mathscr{B}(x)) \supset [(E_1x)\mathscr{A}(x) \equiv (E_1x)\mathscr{B}(x)]$
2.69. $\vdash (E_1x)(\mathscr{A} \vee \mathscr{B}) \supset ((E_1x)\mathscr{A}) \vee (E_1x)\mathscr{B}$.

In any model for a theory K with equality, the relation E in the model corresponding to the predicate letter = is an equivalence relation (by Proposition 2.24). If this relation E is the identity relation in the domain of the model, then the model is called normal.

Any model M for K can be contracted to a normal model M' for K by taking the domain D' of M' to be the set of equivalence classes determined by the relation E in the domain D of M. For a predicate letter A_j^n with interpretation $(A_j^n)^\star$ in M, we define the new interpretation $(A_j^n)'$ in M' as follows: for any equivalence classes [b,], . . . , $[b_n]$ in D' determined by the elements b,, . . . , b_n in D, $(A_j^n)'$ holds for ([b,, . . . , $[b_n]$) if and only if $(A_j^n)^\star$ holds for $b_1, \dots, b_n$. Notice that it makes no difference which representatives b,, . . . , b_n we select in the given equivalence classes, for, by (7), $\vdash x, = y, \wedge \dots \wedge x_n = y_n \supset (A_j^n(x_1, \dots, x_n) \equiv A_j^n(y_1, \dots, y_n))$. Likewise, if $(f_j^n)^\star$ is the interpretation in M of f_j^n, then we define the new interpretation $(f_j^n)'$ in M' as follows: for any equivalence classes $[b_1]$, . . . , $[b_n]$ in D' determined by the elements b,, . . . , b_n in D, $(f_j^n)'([b_1], \dots, [b_n]) = [(f_j^n)^\star(b_1, \dots, b_n)]$. Again note that this is independent of the choice b,, . . . , b_n of representatives, since, by (7), $\vdash x, = y,$

† The new variable y is assumed to be the first variable not occurring in $\mathscr{A}(x)$. A similar assumption is to be made in all other definitions where new variables are introduced.

$\wedge \dots \wedge x_n = y_n \supset f_j^n(x_1, \dots, x_n) = f_j^n(y_1, \dots, y_n)$. If c is the interpretation in M of an individual constant a,, then we take the equivalence class [c] to be the interpretation in M' of a,. The relation E' corresponding to = in the model M' is the identity relation in D': E′([b$_1$], [b$_2$]) if and only if E(b$_1$, b$_2$), i.e., if and only if [b,] = [b$_2$]. Now, one can easily prove by induction the following lemma: if s = (b,, b$_2$, . . .) is a denumerable sequence of elements of D, [b$_i$] is the equivalence class of b$_i$, and s' = ([b,], [b$_2$], . . .), then $\mathcal{A}$ is satisfied by s in M if and only if $\mathcal{A}$ is satisfied by s' in M'. It follows that, for any wf $\mathcal{A}$, $\mathcal{A}$ is true in M if and only if $\mathcal{A}$ is true in M'. Hence, because M is a model of K, M' is a normal model for K.

PROPOSITION 2.27 (EXTENSION OF PROPOSITION 2.12; GÖDEL [1930]). Any consistent theory K with equality has a finite or denumerable normal model.

PROOF. By Proposition 2.12, K has a denumerable model M. Hence the contraction of M to a normal model yields a finite or denumerable normal model M', for the set of equivalence classes in a set D has cardinality less than or equal to the cardinality of D.

COROLLARY 2.28 (EXTENSION OF THE SKOLEM-LÖWENHEIM THEOREM). Any theory K with equality which has an infinite normal model M has a denumerable normal model.

PROOF. Add to K the denumerably many new individual constants b, $b_2, \dots$ together with the axioms $b_i \neq b_j$ for i ≠ j. Then the new theory K' is consistent. For, if K' were inconsistent, there would be a proof in K' of a contradiction $\mathcal{C} \wedge \sim \mathcal{C}$ where we may assume that $\mathcal{C}$ is a wf of K. But this proof uses only a finite number of the new axioms: $b_{i_1} \neq$ b,,, . . . , $b_{i_n} \neq b_{j_n}$. Now M can be extended to a model of K with the axioms $b_{i_1} \neq b_{j_1}, \dots, b_{i_n} \neq b_{j_n}$, for, since M is an infinite normal model, we can choose interpretations of $b_{i_1}, b_{j_1}, \dots, b_{i_n}, b_{j_n}$ so that the wfs $b_{i_1} \neq$ b,,, . . . , $b_{i_n} \neq b_{j_n}$ are true in M. But, since $\mathcal{C} \wedge \sim \mathcal{C}$ is derivable from these wfs and the axioms of K, it would follow that $\mathcal{C} \wedge \sim \mathcal{C}$ is true in M, which is impossible ((11), p. 53). Hence, K' must be consistent. Now, by Proposition 2.27, K' has a finite or denumerable normal model N. But, since the wfs $b_i \neq b_j$, for i ≠ j, are axioms of K', they are true in N. Hence the elements in N which are the interpretations of b,, $b_2, \dots$ must be distinct, which implies that the domain of N is infinite, and, therefore, denumerable.

EXERCISES

2.70. We define $(E_n x)\mathcal{A}(x)$ by induction on n ⩾ 1. The case n = 1 has already been taken care of. Let $(E_{n+1}x)\mathcal{A}(x)$ stand for $(Ey)(\mathcal{A}(y) \wedge (E_n x)(x \neq y \wedge \mathcal{A}(x)))$. (a) Show that $(E_n x)\mathcal{A}(x)$ asserts that there are exactly n objects for which $\mathcal{A}$ holds, in the sense that in any normal model for $(E_n x)\mathcal{A}(x)$ there are exactly n objects for which the property corresponding to $\mathcal{A}(x)$ holds. (b) (i) For each positive integer n, write a wf $\mathcal{B}_n$ such that $\mathcal{B}_n$ holds in a normal model when and only when that model contains at least n elements. (ii) Prove that the theory K, whose axioms are those of the theory of equality K, (cf. Exercise 2.62) plus the axioms $\mathcal{B}_1, \mathcal{B}_2, \dots$, is not finitely axiomatizable, i.e., there is no theory K' with a finite number of axioms such that K and K' have the same theorems.

2.71. (a) Prove that, if a theory K with equality has arbitrarily large finite normal models, then it has a denumerable normal model.

(b) Prove that there is no theory with equality whose normal models are precisely all finite normal interpretations.

2.72. Prove that any predicate calculus with equality is consistent. (A predicate calculus with equality is assumed to have (6) and (7) as axioms.)

2.73. Prove the independence of Axioms (1)–(7) in any predicate calculus with equality. (Hints: for the independence of (1)–(3), replace all $t = s$ by the statement form $A \supset A$; then erase all quantifiers, terms, and associated commas and parentheses; Axioms (4)–(6) go over into statement forms of the form P ⊃ P, and (7) into (P ⊃ P) ⊃ (Q ⊃ Q). Now, for (2)–(3), use the same proofs as for Axioms (A2)–(A3) for the propositional calculus (cf. pp. 38–39).† For (1), the three-valued truth table used on p. 38 does not give the value 0 for P ⊃ P; instead, use the following four-valued truth tables:

A	$-A$
0	1
1	0
2	3
3	2

A	B	$A \supset B$
0	0	0
1	0	0
2	0	0
3	0	0
0	1	1
1	1	0
2	1	1
3	1	1

A	B	$A \supset B$
0	2	1
1	2	0
2	2	0
3	2	0
0	3	1
1	3	0
2	3	1
3	3	0

For (4), replace all universal quantifiers (x) by existential quantifiers (Ex). For (5), change all terms t to x, and replace all universal quantifiers by (x,). For (6), replace all wfs $t = s$ by the negation of some fixed theorem. For (7), consider an interpretation in which the interpretation of = is a reflexive non-symmetric relation.)

2.74. If $\mathcal{A}$ is a wf not containing the = symbol and $\mathcal{A}$ is provable in a predicate calculus with equality K, show that $\mathcal{A}$ is provable in K without using Axioms (6) and (7).

9. Definitions of New Function Letters and Individual Constants

In mathematics, once we have proved, for any y,, . . . , y,, the existence of a unique object u having the property $\mathcal{A}(u$, y,, . . . , y,), we often introduce a new function $f(y_1, \dots,$ y,) such that $\mathcal{A}(f(y_1, \dots,$ y,), y,, . . . , $y_n)$ holds for all $y_1, \dots,$ y,. In cases where we have proved the existence of a unique object u satisfying $\mathcal{A}(u)$, and $\mathcal{A}(u)$ contains u as its only free variable, then we introduce

† For (A2), however, we must use new truth tables for which $P \supset P$ is exceptional.

a new individual constant b. It is generally acknowledged that such definitions, though convenient, add nothing really new to the theory. This can be made precise in the following way.

PROPOSITION 2.29. Let K be a theory with equality. Assume that $\vdash_K (E_1 u)\mathscr{Q}(u, y_1, \ldots, y_n)$. Let K' be the theory with equality obtained by adding to **K** a new function letter f of n arguments, and the proper axiom $\mathscr{Q}(f(y_1, \ldots, y_n), y_1, \ldots, y_n)$,† as well as all instances of (1)–(7) involving f. Then there is an effective transformation mapping each wf $\mathscr{B}$ of K' into a wf $\mathscr{B}'$ of *K* such that

(1) iff does not occur in $\mathscr{B}$, then $\mathscr{B}$' is $\mathscr{B}$
(2) (-- $\mathscr{B}$)$'$ is $\sim(\mathscr{B}')$
(3) $(\mathscr{B} \supset \mathscr{C})'$ is $\mathscr{B}' \supset \mathscr{C}'$
(4) $((x)\mathscr{B})'$ *is* $(x)(\mathscr{B}')$
(5) $\vdash_{K'} \mathscr{B} \equiv \mathscr{B}'$
(6) if $\vdash_{K'} \mathscr{B}$, then $\vdash_K \mathscr{B}$'

Hence, if $\mathscr{B}$ does not contain f and $\vdash_{K'} \mathscr{B}$, then $\vdash_K \mathscr{B}$.

PROOF. A simple f-term is an expression $f(t_1, \ldots,$ t,) where t,, $\ldots, t_n$ are terms not containing f. Given an atomic wf $\mathscr{B}$ of K', let $\mathscr{B}\star$ be the result of replacing the left-most occurrence of a simple f-term $f(t_1, \ldots, t_n)$ in $\mathscr{B}$ by the first variable u not in $\mathscr{B}$. Call the wf $(Eu)(\mathscr{Q}(u,$ t,, $\ldots,$ t,) $\wedge\, \mathscr{B}\star)$ the f-transform of 93. If $\mathscr{B}$ does not contain f, let $\mathscr{B}$ be its own f-transform. Clearly $\vdash_{K'} (Eu)(\mathscr{Q}(u, t_1, \ldots, t_n) \wedge \mathscr{B}^\star) \equiv \mathscr{B}$. (Here we use $\vdash_K (E_1 u)\mathscr{Q}(u,$ y,, $\ldots,$ y,) and the axiom $\mathscr{Q}(f(y_1, \ldots, y_n),$ y,, $\ldots,$ y,) of K'.) Since the f-transform $\mathscr{B}^\#$ of $\mathscr{B}$ contains one less f than 93, and $\vdash_{K'} \mathscr{B}^\# \equiv$ 93, if we take successive f-transforms, eventually we obtain a wf $\mathscr{B}'$ which does not contain f, and such that $\vdash_{K'} \mathscr{B}' \equiv \mathscr{B}$. Call $\mathscr{B}'$ the f-less transform of 93. Extend the definition to all wfs of K' by letting (-- $\mathscr{B}$)' be $\sim(\mathscr{B}')$, $(\mathscr{B} \supset \mathscr{C})'$ be $\mathscr{B}' \supset \mathscr{C}'$, and $((x)\mathscr{B})'$ be $(x)(\mathscr{B}')$. Properties (1) through (5) of the theorem are then obvious. To prove (6), it suffices, by (5), to show that, if $\mathscr{B}$ does not contain f and $\vdash_{K'} \mathscr{B}$, then $\vdash_K \mathscr{B}$. We may assume that $\mathscr{B}$ is a closed wf, since a wf and its closure are deducible from each other.

Assume that M is a model of K. Let $\mathbf{M}_1$ be the corresponding normal model of K (cf. p. 83). We know that a wf is true in M if and only if it is true in $\mathbf{M}_1$. Since $\vdash_K (E_1 u)\mathscr{Q}(u, y_1, \ldots,$ y,), then, for any b,, $\ldots$, $\mathrm{b_n}$ in the domain of $\mathbf{M}_1$, there is a unique c in the domain of $\mathbf{M}_1$ such that $\vdash_{\mathbf{M}_1} \mathscr{Q}[\mathrm{c}, \mathrm{b}_1, \ldots, \mathrm{b_n}]$. If we define $\mathrm{f}'(\mathrm{b}_1, \ldots,$ b,) to be c, then, taking f' to be the interpretation of the function letter *f*, we obtain from $\mathbf{M}_1$ a model M' of K'. For, the logical axioms of $\mathbf{K}'$ (including the equality axioms of K') are true in any interpretation, and the axiom $\mathscr{Q}(f(y_1, \ldots,$ y,), $y_1, \ldots,$ y,) also holds in M' by virtue of the definition of f'. Since the proper axioms of K do not contain *f*, and since they are true in $\mathbf{M}_1$, they are also true in M'. But $\vdash_{K'} \mathscr{B}$. Hence, $\mathscr{B}$ is true in M', but since $\mathscr{B}$ does not contain f, $\mathscr{B}$ is true in $\mathbf{M}_1$, and hence also in M. Thus, $\mathscr{B}$ is true in every model of K. Therefore, by Corollary 2.15(a) of the Completeness Theorem, $\vdash_K \mathscr{B}$. (In the case where $\vdash_K (E_1 u)\mathscr{Q}(u)$ and $\mathscr{Q}(u)$ contains only u as a free variable, we form K' by adding a new individual constant b and the axiom $\mathscr{Q}(b)$. Then the analogue of Proposition 2.29 follows from practically the same proof as the one just given.)

EXERCISE 2.75. Find the f-less transforms of

$$(x)(Ey)\big(A_1^3(x, y, f(x, y, \ldots, y)) \supset f(y, x, x, \ldots, x) = x\big)$$

and of

$$A_1^1(f(y_1, \ldots, y_{n-1}, f(y_1, \ldots, y_n))) \wedge (Ex)A_1^2(x, f(y_1, \ldots, y_n)).$$

Note that Proposition 2.29 also applies when we have introduced several new symbols $f_1, \ldots, f_n$, for we can assume that we have added each f_i to the theory already obtained by the addition of $f_1, \ldots, f_{i-1}$; then n successive applications of Proposition 2.29 are necessary. In addition, the wf $\mathscr{B}'$ of K in Proposition 2.29 can be considered an f-free translation of $\mathscr{B}$ into the language of K.

Examples.

1. In the elementary theory of groups G (cf. page 82), one can prove $(E_1 x_2)(x_1 + x_2 = 0)$. Then introduce a new function letter f of one argument, abbreviate $f(t)$ by $(-$ t), and add the new axiom $x_1 + (-$ x,$) = 0$. By Proposition 2.29, we now cannot prove any wf of G which we could not prove before. Thus, the definition of $(-$ t) adds no really new power to the original theory.

2. In the elementary theory of fields F (cf. page 82), one can prove $(E_1 x_2)((x_1 \neq 0 \wedge x_1 \cdot x_2 = 1) \vee (x_1 = 0 \wedge x_2 = 0))$. We then introduce a new function letter g of one argument, abbreviate $g(t)$ by t^{-1}, and introduce the axiom (x, $\neq 0 \wedge x_1 \cdot x_1^{-1} = 1) \vee ($x, $= 0 \wedge x_1^{-1} = 0)$, from which one can prove x, $\neq 0 \supset x_1 \cdot x_1^{-1} = 1$.

Ffom Proposition 2.29, we can see that, in theories with equality, only predicate letters are needed; function letters and individual constants are dispensable. Iff; is a function letter, we can replace it by a new predicate letter A_k^{n+1} if we add the axiom $(E_1 u)A_k^{n+1}(y_1, \ldots$ y,, u). An individual constant is to be replaced by a new predicate letter A_k^1 if we add the axiom $(E_1 u)A_k^1(u)$.

Example. In the elementary theory G of groups, we can replace + and 0 by predicates A_1^3 and A_1^1 if we add the axioms $(x_1)(x_2)(E_1 x_3)A_1^3(x_1, x_2, x_3)$ and $(E_1 x_1)A_1^1(x_1)$, and if we replace Axioms (a), (b), (c), (g) by

(a') $A_1^3(x_2, x_3, y_1)$ A $A_1^3(x_1, y_1, y_2)$ A $A_1^3(x_1, x_2, y_3) \wedge A_1^3(y_3, x_3, y_4)$
$\qquad \supset y_2 =$ Y4

(b′) $A_1^1(y_1)$ A $A_1^3(x_1, y_1, y_2) \supset y_2 = x_1$

† It is better to take this axiom in the form $(u)(u = f(y_1, \ldots, y_n) \supset \mathscr{Q}(u, y_1, \ldots, y_n))$, since $f(y_1, \ldots,$ *y,)* might not be free for *u* in $\mathscr{Q}(u, y_1, \ldots,$ *y,)*.

(c′) $(Ex_2)(y_1)(y_2)(A_1^1(y_1) \wedge A_1^3(x_1, x_2, y_2) \supset y_2 = y_1)$

(g′) $[x_1 = x_2 \wedge A_1^3(x_1, x_3, y_1) \wedge A_1^3(x_2, x_3, y_2) \wedge A_1^3(x_3, x_1, y_3)$
$\wedge A_1^3(x_3, x_2, y_4)] \supset y_1 = y_2 \wedge y_3 = y_4$

Notice that the proof of Proposition 2.29 is highly non-constructive, since it uses semantical notions (model, truth) and is based upon Corollary 2.15(a), which was proved in a non-constructive way. Constructive, syntactical proofs have been given for Proposition 2.29 (cf. Kleene [1952], § 74), but, in general, they are quite complex.

Descriptive phrases of the kind "the u such that $\mathcal{A}(u, y_1, \ldots, y_n)$" are very common in ordinary language and in mathematics. Such phrases are called definite descriptions. We let $\iota u(\mathcal{A}(u, y_1, \ldots,$ y,)) denote the unique object u such that $\mathcal{A}(u,$ y,, $\ldots, y_n)$ if there is such a unique object. If there is no such unique object, we may either let $\iota u(\mathcal{A}(u,$ y,, $\ldots, y_n))$ stand for some fixed object, say 0, or we may consider it meaningless. (For example, we may say that the phrases "the present king of France" or "the smallest integer" are meaningless, or we may arbitrarily make the convention that they denote 0.) There are various ways of incorporating these ι-terms in formalized theories, but since in most cases the same results are obtained by using new function letters as above, and since they all lead to theorems similar to Proposition 2.29, we shall not discuss them any further here. For details, cf. Hilbert-Bernays [1934] and Rosser [1939a], [1953].

10. Prenex Normal Forms

A wf $(Q_1$ y,$) \ldots (Q_n y_n)\mathcal{A}$, where each $(Q_i y_i)$ is a universal or existential quantifier, $y_i \neq y_j$ for i ≠ j, and $\mathcal{A}$ contains no quantifiers, is said to be inprenex normal *form*. (We include the case n = 0 when there are no quantifiers at all.) We shall prove that for every wf we can construct an equivalent wf in prenex normal form.

LEMMA 2.30. In any theory, *if* y is not *free* in $\mathcal{D}$, and $\mathcal{C}(x)$ and $\mathcal{C}(y)$ are similar,

(I) $\vdash ((x)\mathcal{C}(x) \supset \mathcal{D}) \equiv (Ey)(\mathcal{C}(y) \supset \mathcal{D})$
(II $\vdash ((Ex)\mathcal{C}(x) \supset \mathcal{D}) \equiv (y)(\mathcal{C}(y) \supset \mathcal{D})$
(III) $\vdash \mathcal{D} \supset (x)\mathcal{C}(x) \equiv (y)(\mathcal{D} \supset \mathcal{C}(y))$
(IV) $\vdash \mathcal{D} \supset (Ex)\mathcal{C}(x) \equiv (Ey)(\mathcal{D} \supset \mathcal{C}(y))$
(V) $\vdash \sim (x)\mathcal{C} \equiv (Ex) \sim \mathcal{C}$
(VI) $\vdash \sim (Ex)\mathcal{C} \equiv (x) \sim \mathcal{C}$

PROOF. I(A)

1.	$(x)\mathcal{C}(x) \supset \mathcal{D}$	Hyp
2.	$\sim (Ey)(\mathcal{C}(y) \supset \mathcal{D})$	Hyp
3.	$\sim\sim (y) \sim (\mathcal{C}(y) \supset \mathcal{D})$	2, Abbreviation 3, Tautologies
4.	$(y)(\mathcal{C}(y) \wedge \sim \mathcal{D})$	----A ɜ A, —(A ɜ B) ≡ $(A$ A $\sim B)$, Corollary 2.21
5.	$\mathcal{C}(y) \wedge \sim \mathcal{D}$	4, Rule A4
6.	$\mathcal{C}(y)$	5, Tautology $(A \wedge B) \supset A$
7.	$(y)\mathcal{C}(y)$	6, Gen
8.	$(x)\mathcal{C}(x)$	7, Lemma 2.8
9.	$\mathcal{D}$	1, 8, MP
10.	$\sim \mathcal{D}$	5, Tautology†
11.	$\mathcal{D} \wedge \sim \mathcal{D}$	9, 10, Tautology
12.	$(x)\mathcal{C}(x) \supset \mathcal{D}, \sim (Ey)(\mathcal{C}(y) \supset \mathcal{D}) \vdash \mathcal{D} \wedge \sim \mathcal{D}$	1–11
13.	$(x)\mathcal{C}(x) \supset \mathcal{D} \vdash\sim (Ey)(\mathcal{C}(y) \supset \mathcal{D})$ ɜ $\mathcal{D}$ A $\sim \mathcal{D}$	12, Prop. 2.4
14.	$(x)\mathcal{C}(x) \supset \mathcal{D} \vdash (Ey)(\mathcal{C}(y) \supset \mathcal{D})$	13, Tautology
15.	$\vdash ((x)\mathcal{C}(x) \supset \mathcal{D}) \supset (Ey)(\mathcal{C}(y) \supset \mathcal{D})$	14, Proposition 2.4

PROOF. I(B)

1.	$(Ey)(\mathcal{C}(y) \supset \mathcal{D})$	Hyp
2.	$(x)\mathcal{C}(x)$	Hyp
3.	$\mathcal{C}(b) \supset \mathcal{D}$	1, Rule C
4.	$\mathcal{C}(b)$	2, Rule A4
5.	$\mathcal{D}$	3, 4, MP
6.	$(Ey)(\mathcal{C}(y) \supset \mathcal{D}), (x)\mathcal{C}(x) \vdash_C \mathcal{D}$	1–5
7.	$(Ey)(\mathcal{C}(y) \supset \mathcal{D}), (x)\mathcal{C}(x) \vdash \mathcal{D}$	6, Prop. 2.23
8.	$\vdash (Ey)(\mathcal{C}(y) \supset \mathcal{D}) \supset ((x)\mathcal{C}(x) \supset \mathcal{D})$	7, Prop. 2.4 twice

PROOF. I(C)

$\vdash ((x)\mathcal{C}(x) \supset \mathcal{D}) \equiv (Ey)(\mathcal{C}(y) \supset \mathcal{D})$	(A), (B), Tautology

Parts (II) through (VI) are proved easily and left as an exercise. ((VI) is trivial, and (V) appeared in Exercise 2.45, p. 75; (III) and (IV) follow easily from (II) and (I), respectively.)

Lemma 2.30 allows us to move interior quantifiers to the front of a wf. This is the essential process in the proof of the following theorem.

PROPOSITION 2.31. There *is* an *effective* procedure *for transforming* any wf $\mathcal{A}$ into a wf $\mathcal{B}$ in prenex normal *form* such that $\vdash \mathcal{A} \equiv \mathcal{B}$.

PROOF. We describe the procedure by induction on the number k of connectives and quantifiers in $\mathcal{A}$. (By Proposition 2.18 (a)–(b), we can assume that the

† From now on, application of obvious tautologies will merely be indicated by the word "Tautology".

quantified variables in the prefix that we shall obtain are distinct.) If k = 0, $\mathscr{B}$ is $\mathscr{A}$ itself. Assume that we can find a corresponding $\mathscr{B}$ for all wfs with k < n. Assume $\mathscr{A}$ has n connectives and quantifiers.

Case 1. If $\mathscr{A}$ is $\sim \mathscr{C}$, then, by inductive hypothesis, we can construct a wf $\mathscr{D}$ in prenex normal form such that $\vdash \mathscr{C} \equiv 9$. Hence, $\vdash \sim \mathscr{C} \equiv \sim \mathscr{D}$, i.e., $\vdash \mathscr{A} \equiv \sim \mathscr{D}$; but, applying (V) and (VI) of Lemma 2.30 and Corollary 2.21, we can find a wf $\mathscr{B}$ in prenex normal form such that $\vdash \sim \mathscr{D} \equiv \mathscr{B}$. Hence, $\vdash \mathscr{A} \equiv \mathscr{B}$.

Case 2. If $\mathscr{A}$ is $\mathscr{C} \supset \mathscr{E}$, then by inductive hypothesis, we can find wfs $\mathscr{C}_1$ and $\mathscr{E}_1$ in prenex normal form such that $\vdash \mathscr{C} \equiv \mathscr{C}_1$ and $\vdash \mathscr{E} \equiv \mathscr{E}_1$. Hence, by a tautology, $\vdash (\mathscr{C} \supset \mathscr{E}) \equiv (\mathscr{C}_1 \supset \mathscr{E}_1)$, i.e., $\vdash \mathscr{A} \equiv (\mathscr{C}_1 \supset \mathscr{E}_1)$. Now, applying (I)–(IV) of Lemma 2.30 and Corollary 2.21, we can move the quantifiers in the prefixes of $\mathscr{C}_1$ and $\mathscr{E}_1$ to the front obtaining a wf $\mathscr{B}$ in prenex normal form with $\vdash \mathscr{A} \equiv \mathscr{B}$.

Case 3. $\mathscr{A}$ is $(x)\mathscr{C}$. By inductive hypothesis, there is a wf $\mathscr{C}_1$ in prenex normal form such that $\vdash \mathscr{C} \equiv \mathscr{C}_1$. Hence $\vdash (x)\mathscr{C} \equiv (x)\mathscr{C}_1$, i.e., $\vdash \mathscr{A} \equiv (x)\mathscr{C}_1$. But $(x)\mathscr{C}_1$ is in prenex normal form.

Examples.

1. Let $\mathscr{A}$ be $(x)(A_1^1(x) \supset (y)(A_2^2(x, y) \supset \sim (z)A_3^2(y, z)))$.
By (V) of Lemma 2.30: $(x)(A_1^1(x) \supset (y)(A_2^2(x, y) \supset (Ez) \sim A_3^2(y, z)))$.
By (IV): $(x)(A_1^1(x) \supset (y)(Eu)(A_2^2(x, y) \supset \sim A_3^2(y, u)))$.
By (III): $(x)(v)(A_1^1(x) \supset (Eu)(A_2^2(x, v) \supset \sim A_3^2(v, u)))$.
By (IV): $(x)(v)(Ew)(A_1^1(x) \supset (A_2^2(x, v) \supset \sim A_3^2(v, w)))$.
Changing bound variables (Corollary 2.22): $(x)(y)(Ez)(A_1^1(x) \supset (A_2^2(x, y) \supset \sim A_3^2(y, z)))$.

2. Let $\mathscr{A}$ be $A_1^2(x, y) \supset (Ey)[A_1^1(y) \supset (((Ex)A_1^1(x)) \supset A_2^1(y))]$.
By (II): $A_1^2(x, y) \supset (Ey)[A_1^1(y) \supset (u)(A_1^1(u) \supset A_2^1(y))]$.
By (III): $A_1^2(x, y) \supset (Ey)(v)(A_1^1(y) \supset (A_1^1(v) \supset A_2^1(y)))$.
By (IV): $(Ew)(A_1^2(x, y) \supset (v)(A_1^1(w) \supset (A_1^1(v) \supset A_2^1(w))))$.
By (III): $(Ew)(z)(A_1^2(x, y) \supset (A_1^1(w) \supset (A_1^1(z) \supset A_2^1(w))))$.

EXERCISES

Find a prenex normal form equivalent to the following wfs:

2.76. $[(x)(A_1^1(x) \supset A_1^2(x, y))]$ 3 $([(Ey)A_1^1(y)] \supset [(Ez)A_1^2(y, z)])$

2.77. $(Ex)A_1^2(x, y) \supset (A_1^1(x) \supset \sim (Eu)A_1^2(x, u))$

A predicate calculus in which there are no function letters or individual constants and in which, for any positive integer n, there are infinitely many predicate letters with n arguments is called a pure predicate calculus. For pure predicate calculi, we can find a very simple prenex normal form theorem. A wf in prenex normal form such that all existential quantifiers precede all universal quantifiers is said to be in *Skolem* normal form.

PROPOSITION 2.32. In a pure predicate calculus, there is an *effective* process assigning to each wf $\mathscr{A}$ another wf $\mathscr{B}$ in *Skolem* normal form such that $\vdash \mathscr{A}$ if and only if $\vdash \mathscr{B}$ (or, equivalently, by *Gödel's* Completeness Theorem 2.14, such that $\mathscr{A}$ is logically valid if and only if $\mathscr{B}$ is logically valid).

PROOF. First we may assume that $\mathscr{A}$ is a closed wf, since a wf is provable if and only if its closure is provable. By Proposition 2.31, we may also assume that $\mathscr{A}$ is in prenex normal form. Let the rank r of $\mathscr{A}$ be the number of universal quantifiers in $\mathscr{A}$ which precede existential quantifiers. By induction on the rank, we shall describe the process for finding Skolem normal forms. Clearly, when the rank r = 0, we already have the Skolem normal form. Let us assume that we can construct Skolem normal forms when the rank is less than r, and let r be the rank of $\mathscr{A}$. $\mathscr{A}$ can be written as follows: (Ey,) . . . $(Ey_n)(u)\mathscr{B}(y_1, \ldots, y_n,$ u), where $\mathscr{B}$(y,, . . . , y_n, u) has only y,, . . . , y_n, u as its free variables. Let A_j^{n+1} be the first predicate letter of n + 1 arguments not occurring in $\mathscr{A}$. Construct the wf

$$(\mathscr{A}_1) \quad (Ey_1) \ldots (Ey_n)\big(\big[(u)\big(\mathscr{B}(y_1, \ldots, y_n, u) \supset A_j^{n+1}(y_1, \ldots, y_n, u)\big)\big] \supset (u)A_j^{n+1}(y_1, \ldots, y_n, u)\big)$$

Let us show that $\vdash \mathscr{A}$ if and only if $\vdash \mathscr{A}_1$. Assume $\vdash \mathscr{A}_1$. In the proof of $\mathscr{A}_1$ replace all occurrences of $A_j^{n+1}(z_1, \ldots, z_n,$ w) by $\mathscr{B}^\star(z_1, \ldots, z_n,$ w), where $\mathscr{B}^*$ is obtained from $\mathscr{B}$ by replacing all bound variables having free occurrences in the proof by new variables not occurring in the proof. The result is a proof of the wf:

$$(Ey_1) \ldots (Ey_n)(((u)(\mathscr{B}(y_1, \ldots, y_n, u) \supset \mathscr{B}^\star(y_1, \ldots, y_n, u))) \supset (u)\mathscr{B}^\star(y_1, \ldots, y_n, u))$$

($\mathscr{B}$ was replaced by $\mathscr{B}^*$ so that applications of Axiom (4) would remain applications of the same axiom.) Now, by changing the bound variables back .again by Corollary 2.22, we see that

$$\vdash (Ey_1) \ldots (Ey_n)\big[(u)(\mathscr{B}(y_1, \ldots, y_n, u) \supset \mathscr{B}(y_1, \ldots, y_n, u)) \supset (u)\mathscr{B}(y_1, \ldots, y_n, u)\big]$$

Since $\vdash (u)(\mathscr{B}(y_1, \ldots, y_n, u) \supset \mathscr{B}$(y,, . . . , y_n, u)), we obtain by Corollary 2.21, $\vdash (Ey_1) \ldots (Ey_n)(u)\mathscr{B}(y_1, \ldots, y_n,$ u), i.e., $\vdash \mathscr{A}$. Conversely, assume $\vdash \mathscr{A}$. By Rule C, we obtain $(u)\mathscr{B}$(b,, . . . , b_n, u). But $\vdash (u)D \supset ((u)(\mathscr{D} \supset \mathscr{F}) \supset (u)\mathscr{F})$ (cf. Exercise 2.26(a), p. 64), for any wfs 9 , 9 . Hence, $(u)(\mathscr{B}(b_1, \ldots, b_n, u) \supset A_j^{n+1}(b_1, \ldots, b_n,$ u)) $\supset (u)A_j^{n+1}(b_1, \ldots, b_n,$ u). So, by Rule E4, $(Ey_1) \ldots (Ey_n)([(u)(\mathscr{B}(y_1, \ldots, y_n,$ u) $\supset A_j^{n+1}(y_1, \ldots, y_n, u))] \supset (u)A_j^{n+1}(y_1, \ldots, y_n,$ u)), i.e., $\vdash_C \mathscr{A}_1$. Now, by Proposition 2.23, $\vdash \mathscr{A}_1$. **A** prenex normal form of $\mathscr{A}_1$ has the form $\mathscr{A}_2$: (Ey₁) . . . $(Ey_n)(Eu)(Q_1z_1) \ldots (Q_sz_s)(v)\mathscr{G}$, where $\mathscr{G}$ has no quantifiers and $(Q_1z_1) \ldots (Q_sz_s)$ is the prefix of $\mathscr{B}$. (For, in deriving the prenex normal form, first, by Lemma 2.30(I), we pull out the first (u), which changes to (Eu); then we pull out of the first conditional the quantifiers in the prefix of $\mathcal{B}$. By Proposition 2.30(II), this changes existential and universal quantifiers, but then we again pull these out of the second conditional of $\mathcal{A}_1$, which brings the prefix back to its original form. Finally, by Proposition 2.30(III), we bring the second (u) out to the prefix, changing it to a new variable (u).) Clearly, $\mathcal{A}_2$ has rank one less than the rank of $\mathcal{A}$, and, by Proposition 2.31, $\vdash \mathcal{A}_1 \equiv \mathcal{A}_2$; but $\vdash \mathcal{A}$ if and only if $\vdash \mathcal{A}_1$. Hence, $\vdash \mathcal{A}$ if and only if $\vdash \mathcal{A}_2$. By inductive hypothesis, we can find a Skolem normal form for $\mathcal{A}_2$, which is also a Skolem normal form for $\mathcal{A}$.

Example. $\mathcal{A}$: $(x)(y)(Ez)\mathcal{C}(x, y, z)$, where $\mathcal{C}$ contains no quantifiers. $\mathcal{A}_1$: $(x)((y)(Ez)\mathcal{C}(x, y, z) \supset A_j^1(x)) \supset (x)A_j^1(x)$, where A; is not in $\mathcal{C}$. We obtain the prenex normal form of $\mathcal{A}_1$:

$$(Ex)([(y)(Ez)\mathcal{C}(x, y, z) \supset A_j^1(x)] \supset (x)A_j^1(x)) \qquad (2.30\text{I})$$
$$(Ex)((Ey)[(Ez)\mathcal{C}(x, y, z) \supset A_j^1(x)] \supset (x)A_j^1(x)) \qquad (2.30\text{I})$$
$$(Ex)((Ey)(z)(\mathcal{C}(x, y, z) \supset A_j^1(x)) \supset (x)A_j^1(x)) \qquad (2.30\text{II})$$
$$(Ex)(y)((z)(\mathcal{C}(x, y, z) \supset A_j^1(x)) \supset (x)A_j^1(x)) \qquad (2.30\text{II})$$
$$(Ex)(y)(Ez)(\mathcal{C}(x, y, z) \supset A_j^1(x)) \supset (x)A_j^1(x)) \qquad (2.30\text{I})$$
$$(Ex)(y)(Ez)(v)((\mathcal{C}(x, y, z) \supset A_j^1(x)) \supset A_j^1(v)) \qquad (2.30\text{III})$$

We repeat this process again: Let $\mathcal{D}(x, y, z, v)$ be $(\mathcal{C}(x, y, z) \ni A_j^1(x)) \ni A_j^1(v)$. Let A_k^2 not occur in $\mathcal{D}$. Form:

$$(Ex)[[(y)[(Ez)(v)(\mathcal{D}(x, y, z, v)) \supset A_k^2(x, y)]] \supset (y)A_k^2(x, y)]$$
$$(Ex)(Ey)[(Ez)(v)(\mathcal{D}(x, y, z, v)) \supset A_k^2(x, y) \supset (y)A_k^2(x, y)] \ (2.30(\text{I}))$$
$$(Ex)(Ey)(Ez)(v)([\mathcal{D}(x, y, z, v) \supset A_k^2(x, y)] \supset (y)A_k^2(x, y)) \ (2.30(\text{I}), (\text{II}))$$
$$(Ex)(Ey)(Ez)(v)(w)([\mathcal{D}(x, y, z, v) \supset A_k^2(x, y)] \supset A_k^2(x, w)) \ (2.30(\text{III}))$$

Thus, a Skolem normal form of $\mathcal{A}$ is

$$(Ex)(Ey)(Ez)(v)(w)\Big(\Big[\Big(\big(\mathcal{C}(x, y, z) \supset A_j^1(x)\big) \supset A_j^1(v)\Big) \supset A_k^2(x, y)\Big] \supset A_k^2(x, w)\Big)$$

EXERCISES

2.78. Find Skolem normal forms for the wfs:

(a) $\sim (Ex)A_1^1(x) \supset (u)(Ey)(x)A_1^3(u, x, y)$

(b) $(x)(Ey)(u)(Ev)A_1^4(x, y, u, v)$

2.79. Show that there is an effective process which gives, for each wf $\mathcal{A}$ of a pure predicate calculus, another wf $\mathcal{B}$ of this calculus of the form $(y_1) \ldots (y_n)(Ez_1) \ldots (Ez_m)\mathcal{C}$, such that $\mathcal{C}$ is quantifier-free, n, m $\geqslant$ 0, and $\mathcal{A}$ is satisfiable if and only if $\mathcal{B}$ is satisfiable. (Hint: apply Proposition 2.32 to $\sim \mathcal{A}$.)

2.80. Find a Skolem normal form $\mathcal{B}$ for $(x)(Ey)A_1^2(x, y)$, and show that not-$\vdash \mathcal{B} \equiv (x)(Ey)A_1^2(x, y)$. Hence a Skolem normal form for $\mathcal{A}$ is not necessarily logically equivalent to $\mathcal{A}$, in contradistinction to the prenex normal form given by Proposition 2.31.

11. Isomorphism of Interpretations. Categoricity of Theories

We shall say that an interpretation M of the wfs of some first-order theory K is isomorphic with another interpretation M' of K if and only if there is a 1–1 correspondence g (called an isomorphism) of the domain D of M with the domain D' of M' such that:

(i) For any predicate letter A_j^n of K, and for any b,, . . . , b_n in D, $\models_{\mathrm{M}} A_j^n[b_1, \ldots, b_n]$ if and only if $\models_{\mathrm{M'}} A_j^n[g(b_1), \ldots, g(b_n)]$;

(ii) For any function letter f_j^n of K and for any b,, . . . , b_n in D, $g((f_j^n)^M(b_1, \ldots, b_n)) = (f_j^n)^{M'}(g(b_1), \ldots, g(b_n))$;

(iii) For any individual constant a_j of K, $g((a_j)^M) = (a_j)^{M'}$.

The notation M, $\approx \mathbf{M}_2$ will be used to indicate that $\mathbf{M}_1$ is isomorphic with $\mathbf{M}_2$. Notice that, if $\mathbf{M}_1 \approx \mathbf{M}_2$, the domains of $\mathbf{M}_1$ and $\mathbf{M}_2$ must be of the same cardinality.

PROPOSITION 2.33. If g is an *isomorphism* of M with M' then (1) for any wf $\mathcal{A}$ of K, any sequence $s = (\text{b},, b_2, \ldots)$ of elements of D, and the corresponding sequence $g(s) = (g(b_1), g(b_2), \ldots)$, s satisfies $\mathcal{A}$ *if* and only *if* $g(s)$ satisfies $\mathcal{A}$; (2) hence, $\models_{\mathrm{M}} \mathcal{A}$ *if* and only *if* $\models_{\mathrm{M'}} \mathcal{A}$.

PROOF. (2) follows directly from (1). The proof of (1) is a simple induction on the number of connectives and quantifiers in $\mathcal{A}$, and is left as an exercise.

We see from Proposition 2.33 that isomorphic interpretations have the same "structure" and, thus, differ in no essential way.

EXERCISES

Prove:

2.81. If M is an interpretation with domain D, and D' is a set having the same cardinality as D, then one can define an interpretation M' with domain D' such that M is isomorphic with M'.

2.82. M is isomorphic with M. If M is isomorphic with M', then M' is isomorphic with M. If M is isomorphic with M' and M' is isomorphic with M'', then M is isomorphic with M''.

A theory K with equality is said to be m-categorical, where m is a cardinal number, if and only if (1) any two normal models of K of cardinality $\mathfrak{m}$ are isomorphic; (2) K has at least one normal model of cardinality $\mathfrak{m}$ (cf. Loś [1954c]).

Examples.

1. Let $\mathbf{K}^2$ be the theory of equality K, (cf. p. 81) to which we have added the axiom (E2):

$$(Ex_1)(Ex_2)(x_1 \neq x_2 \text{ A } (x_3)(x_3 = x_1 \text{ V } x_3 = x_2))$$

Then K^2 is 2-categorical. Moreover, every normal model of $\mathbf{K}^2$ has exactly two elements. More generally, define (En) to be

$$(Ex_1)(Ex_2) \ldots (Ex_n)\Big(\bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j \wedge$$
$$(x_{n+1})(x_{n+1} = x_1 \vee x_{n+1} = x_2 \vee \ldots \vee x_{n+1} = x_n)\Big)$$

where $\bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j$ is the conjunction of all wfs $x_i \neq x_j$ with 1 *6* i $<j \leqslant$ n. Then, if $\mathbf{K}^n$ is obtained from K, by adding (En) as an axiom, $\mathbf{K}^n$ is n-categorical, and every normal model of $\mathbf{K}^n$ has exactly n elements.

2. The theory $\mathbf{K}_2$ (cf. p. 81) of densely-ordered sets with neither first nor last element is ti_0-categorical (cf. Kamke [1950], page 71: every denumerable normal model of $\mathbf{K}_2$ is isomorphic with the model consisting of the set of rational numbers under .their natural ordering). But one can prove that $\mathbf{K}_2$ is not rn-categorical for any m different from $\aleph_0$.

EXERCISES

2.83.^{A} Find a first-order theory with equality which is not $\aleph_0$-categorical, but is m-categorical for all m $> \aleph_0$. (Hint: consider the theory $\mathbf{G}_c$ of commutative groups (cf. p. 82). For each integer n, let *nx* stand for the term $\underbrace{(x + x) + \ldots + x}_{\text{n-times}}$. Add to $\mathbf{G}_c$ the new axioms ($\mathfrak{B}_n$): $(x)(E_1 y)(ny = x)$ for all n $\geqslant$ 2. The new theory is the theory of uniquely divisible commutative groups. Its normal models are essentially vector spaces over the field of rational numbers. However, any two vector spaces over the rationals of the same non-denumerable cardinality are isomorphic, and there are denumerable vector spaces over the rationals which are not isomorphic (cf. Bourbaki [1947]).)

2.84.^{A} Find a theory with equality which is m-categorical for all infinite cardinals m. (Hint: add to the theory $\mathbf{G}_c$ of commutative groups the axiom $(x_1)(2x_1 = 0)$. The normal models of the new theory are just the vector spaces over the field of integers modulo 2. Any two such vector spaces of the same cardinality are isomorphic (cf. Bourbaki [1947]).)

2.85. Show that the theorems of the theory $\mathbf{K}^n$ in Example 1 above are precisely the set of all **wfs** of K^n which are true in all normal models of cardinality n.

2.86.^{A} Find two non-isomorphic densely-ordered sets of cardinality $2^{\aleph_0}$ with neither first nor last element. (This shows that the theory K_2 of Example 2 is not 2'0-categorical.)

Is there a theory with equality which is rn-categorical for some non-countable cardinal m but not n-categorical for some other non-countable cardinal n? In Example 2 we found a theory which is only ti_0-categorical; in Exercise 2.83 we found a theory which is rn-categorical for all infinite m $> \aleph_0$, but not $\aleph_0$-categorical; and in Exercise 2.84, a theory which is rn-categorical for all infinite m. The elementary theory G of groups is not rn-categorical for any infinite m. The problem is whether these four cases exhaust all the possibilities. That this is so has been proved by M. D. Morley [1965].

12. Generalized First-Order Theories. Completeness and Decidability†

If, in the definition of the notion of first-order theory, we allow a noncountable number of predicate letters, function letters, and individual constants, and possibly a noncountable number of axioms, we arrive at the notion of a generalized first-order theory. First-order theories are special cases of generalized first-order theories. The reader may easily check that all the results for first-order theories, through Lemma 2.9, hold also for generalized first-order theories, without any changes in the proofs. Lemma 2.10 becomes Lemma 2.10': if the set of symbols of a generalized theory K has cardinality ti„ then the set of expressions of K also can be well-ordered and has cardinality ti,. (First, order the expressions by their length, which is some positive integer, and then stipulate that if e_1 and e_2 are two distinct expressions of the same length k, and j is the first place in which they differ, then e, "precedes" e_2 if the j$^{\text{th}}$ symbol of e_1 precedes the j$^{\text{th}}$ symbol of e_2 according to the given well-ordering of the symbols of K.) Now, under the same assumption as for Lemma 2.10′, Lindenbaum's Lemma 2.11' can be proved for generalized theories much as before, except that all the enumerations (of the wfs $\mathfrak{B}_i$ and of the theories J_i) are transfinite, and the proof that J is consistent and complete uses transfinite induction. The analogue of Henkin's Theorem 2.12 runs as follows:

PROPOSITION 2.34. If the set of symbols of a consistent generalized theory K has cardinality ti„ then K has a model of cardinality ti,.

PROOF. The original proof for Proposition 2.12 is modified in the following way. Add ti, new individual constants b,, $b_2, \ldots,$ b„ . . . . As before, the new theory K_0 is consistent. Let $F_1(x_{i_1}), \ldots, F_\lambda(x_{i_\lambda}), \ldots$ (A $< \omega_\alpha$) be a sequence consisting of all wfs of K_0 with at most one free variable. Let (S_λ) be the wf $\sim (x_{i_\lambda})F_\lambda(x_{i_\lambda}) \supset \sim F_\lambda(b_{j_\lambda})$, where the sequence $b_{j_1}, b_{j_2}, \ldots, b_{j_\lambda}, \ldots$ of distinct constants is chosen so that b_{j_λ} does not occur in $F_\beta(x_{i_\beta})$ for $\beta \leqslant$ A. The new theory K, obtained by adding all the wfs (S_λ) as axioms is consistent, by a transfinite induction analogous to that of Proposition 2.12. Now, by the extension 2.11' of Lindenbaum's Lemma, there is a complete, consistent extension J of K,. The model is defined now as in Proposition 2.12, and its domain, the set of closed terms of K_0, has cardinality ti,.

† Presupposed in parts of this Section is a slender acquaintance with ordinal and cardinal numbers (cf. Chapter 4, or Kamke [1950], or Sierpinski [1958]).

COROLLARY 2.35. (1) If the set of symbols of a consistent generalized theory K with equality has cardinality $\aleph_\alpha$, then K has a normal model of cardinality $\leqslant \aleph_\alpha$. (2) If, in addition, K has an infinite normal model (or *if K* has arbitrarily *large* finite normal models), then K has a normal model of any cardinality $\aleph_\beta \geqslant \aleph_\alpha$. (3) In particular, if K is an ordinary theory with equality (i.e., $\aleph_\alpha = \aleph_0$), and K has an infinite normal model (or if K has arbitrarily large finite normal *models*), then K has a normal model of any cardinality $\aleph_\beta (\beta > 0)$.

PROOF. (1) The model guaranteed by Proposition 2.34 can be contracted to a normal model (cf. p. 83) consisting of equivalence classes in a set of cardinality $\aleph_\alpha$. Such a set of equivalence classes has cardinality $\leqslant \aleph_\alpha$. (2) Assume $\aleph_\beta \geqslant \aleph_\alpha$. Let b,, $b_2, \ldots$ be a set of new individual constants of cardinality $\aleph_\beta$, and add the axioms $b_\lambda \neq b_\mu$ for $\lambda \neq \mu$. As in the proof of Corollary 2.28, this new theory is consistent, and so, by (1), has a normal model of cardinality $\leqslant \aleph_\beta$ (since the new theory has $\aleph_\beta$ symbols). But, because of the axioms b, $\neq b_\mu$, the normal model has exactly $\aleph_\beta$ elements. (3) is a special case of (2).

EXERCISE 2.87. If the set of symbols of a predicate calculus *K* with equality has cardinality $\aleph_\alpha$, prove that there is an extension *K'* of K (with the same symbols as K) such that K' has a normal model of cardinality $\aleph_\alpha$, but K' has no normal model of cardinality $< \aleph_\alpha$.

From Lemma 2.9' and Corollary 2.35(1, 2), it follows easily that, if a generalized first-order theory K with equality has $\aleph_\alpha$ symbols, is $\aleph_\beta$-categorical for some $\beta \geqslant a$, and has no finite models, then K is complete, in the sense that, for any closed wf $\mathscr{A}$, either $\vdash_K \mathscr{A}$ or $\vdash_K \sim \mathscr{A}$ (Vaught [1954]). For, if not-$\vdash_K \mathscr{A}$ and not-$\vdash_K \sim$ W, then the theories K' = K + $\{- \mathscr{A}\}$ and K" = K + $\{\mathscr{A}\}$ are consistent by Lemma 2.9', and so, by Corollary 2.35(1), there are normal models M, and M_2 of K' and K", respectively, of cardinality $\leqslant \aleph_\alpha$. Since K has no finite models, M_1 and M_2 are infinite. Hence, by Corollary 2.35(2), there are normal models N, and N_2 of K' and K", respectively, of cardinality $\aleph_\beta$. By the $\aleph_\beta$-categoricity of K, N, and N_2 must be isomorphic. But, since $\sim \mathscr{A}$ is true in N_1 and $\mathscr{A}$ is true in N_2, this is impossible. Therefore, either $\vdash_K \mathscr{A}$ or $\vdash_K \sim$ W.

In particular, if K is an ordinary first-order theory with equality which has no finite models and is $\aleph_\beta$-categorical for some $\beta \geqslant 0$, then K is complete. As an example, consider the theory K_2 of densely-ordered sets with neither first nor last element (cf. p. 81, Example 2). K_2 has no finite models and is $\aleph_0$-categorical.

If an ordinary first-order theory K is axiomatic (i.e., one can effectively decide whether any wf is an axiom) and complete, then K is decidable, that is, there is an effective procedure to determine whether any given wf is a theorem. To see this, remember (cf. p. 66) that if a theory is axiomatic, one can effectively enumerate the theorems. Any wf $\mathscr{A}$ is provable if and only if its closure is provable. Hence, we may confine our attention to closed wfs W. Since K is complete, either $\mathscr{A}$ is a theorem or $\sim \mathscr{A}$ is a theorem, and, therefore, one or the other will eventually turn up in our enumeration of the theorems. This provides an effective test for theoremhood. Notice that if K is inconsistent, then every wf is a theorem, and there is an obvious decision procedure; if K is consistent, then not both $\mathscr{A}$ and $\sim \mathscr{A}$ can show up as theorems, and we need only wait till one or the other appears.

If an ordinary axiomatic theory K with equality has no finite models and is $\aleph_\beta$-categorical for some $\beta \geqslant 0$, then, by what we have proved above, K is decidable. In particular, the theory K_2 mentioned above is decidable.

In certain cases, there is a more direct method of proving completeness or decidability. Let us take as an example the theory K_2 of densely-ordered sets with neither first nor last element. Langford [1927] has given the following procedure for K_2. Consider any closed wf W. By Proposition 2.31, we can assume that $\mathscr{A}$ is in prenex normal form (Qy,)... $(Qy_n)\mathscr{B}$, where $\mathscr{B}$ contains no quantifiers. If (Qy_n) is (y,), replace $(y_n)\mathscr{B}$ by $\sim$(Ey,) $\sim \mathscr{B}$. In all cases, then, we have, at the right side of the wf, $(Ey_n)\mathscr{C}$, where $\mathscr{C}$ has no quantifiers. Any negation x $\neq$y can be replaced by x $<$y $\vee$ y $<$ x, and x $\not<$y can be replaced by x = y $\vee$ y $<$ x. Hence, all negation signs may be eliminated from $\mathscr{C}$. We can now put $\mathscr{C}$ into disjunctive normal form, i.e., a disjunction of conjunctions of atomic wfs (cf. p. 28, Exercise 1.36). Now $(Ey_n)(\mathscr{C}_1 \vee \mathscr{C}_2 \vee \ldots \vee \mathscr{C}_k)$ is equivalent to $(Ey_n)\mathscr{C}_1 \vee (Ey_n)\mathscr{C}_2 \vee \ldots \vee (Ey_n)\mathscr{C}_k$. Consider each $(Ey_n)\mathscr{C}_i$ separately. $\mathscr{C}_i$ is a conjunction of atomic wfs of the form t $<$ *s* and t = s. If $\mathscr{C}_i$ does not contain y,, just erase (Ey,). Note that, if a wf $\mathscr{D}$ does not contain y,,, then $(Ey_n)(\mathscr{D} \wedge \mathscr{E})$ may be replaced by $\mathscr{D} \wedge {}^{(Ey_n)\mathscr{E}}$. Hence, we are reduced to the consideration of $(Ey_n)\mathscr{F}$, where 4 is a conjunction of atomic wfs, each of which contains y_n. Now, if one of the conjuncts is y, = z for some z different from y_n, replace in 4 all occurrences of y, by z and erase (Ey,). If we have $y_n =$ y, alone, then just erase (Ey,). If we have y, = y, as one conjunct among others, erase y_n = y,. If 4 has a conjunct y, $<$y,, replace all of $(Ey_n)\mathscr{F}$ by $y_n <$y,. If $\mathscr{F}$ consists of $y_n <$ z, $\wedge \ldots \wedge$ y, $< z_j$, or if $\mathscr{F}$ consists of $u_1 <$y, $\wedge \ldots \wedge u_m < y_n$, where $z_1, \ldots, z_j, u_1, \ldots, u_m$ are different from y,, replace $(Ey_n)\mathscr{F}$ by $y_n = y_n$. If 4 consists of $y_n <$ z, $\wedge \ldots \wedge y_n < z_j \wedge u_1 < y_n \wedge \ldots$ A $u_m < y_n$, replace $(Ey_n)\mathscr{F}$ by the conjunction of all the wfs $u_i < z_i$ for 1 $\leqslant$ i $\leqslant$ m and 1 $\leqslant$ 1 $\leqslant$ j. This exhausts all possibilities, and, in every case, we have replaced $(Ey_n)\mathscr{C}$ by a wf $\mathscr{R}$ containing no quantifiers, i.e., we have eliminated the quantifier (Ey,). We are left with $(Qy_1) \ldots (Qy_{n-1})\mathscr{S}$ where $\mathscr{S}$ contains no quantifiers. Now we apply the same procedure successively to $(Qy_{n-1}), \ldots, (Qy_1)$. Finally, we are left with a wf without quantifiers built up out of wfs of the form x = x and x $<$ x. Now, if we replace x = x by x = x $\supset$ x = x and x $<$ x by $\sim$(x = x $\supset$ x = x), then the result is either an instance of a tautology or the negation of such an instance (Exercise). Hence, by Proposition 2.1, either the result or its negation is provable. Now, one can easily check that all the replacements we have made in this whole reduction process applied to $\mathscr{A}$ have been replacements of wfs $\mathscr{T}$ by other wfs $\mathscr{U}$ such that $\vdash_K \mathscr{T} \equiv \mathscr{U}$. Hence, by Corollary 2.21, if our final result is provable, then so is the original wf $\mathcal{A}$, and, if the negation of our result is provable, so is $\sim \mathcal{A}$. Thus, K_2 is complete and decidable.

The method employed in this proof, the successive elimination of existential quantifiers, has been applied to other theories. It yields a decision procedure (cf. Hilbert-Bernays [1934]I, § 5) for the elementary theory K, of equality (cf. p. 81). It has been applied by Tarski [1951] to prove the completeness and decidability of elementary algebra (i.e., of the elementary theory of real-closed fields; cf. van der Waerden [1949]) and by Szmielew [1955] to prove the decidability of the elementary theory of abelian groups. For more details and examples cf. Chang-Keisler [1973], Section 1.5.

EXERCISES

2.88. (Henkin [1955]) If an ordinary theory K with equality is finitely axiomatizable and $\aleph_\alpha$-categorical for some a, prove that K is decidable.

2.89. (a) Prove the decidability of the theory K_1 of equality (cf. p. 81).

(b) Give an example of a theory with equality which is $\aleph_\alpha$-categorical for some a, but is incomplete.

Mathematical Applications

(1) Let F be the elementary theory of fields (cf. p. 82). We let n stand for the term $\underbrace{1 + 1 + \ldots + 1}_{\text{n-times}}$. Then the assertion that a field-has characteristic p can be expressed by the wf $\mathcal{C}_p$: p = 0. A field has characteristic zero if and only if it does not have characteristic p for any prime p. Then for any closed wf $\mathcal{A}$ of F which holds for all fields of characteristic zero, there is a prime number q such that $\mathcal{A}$ holds for all fields of characteristic $\geqslant$ q. For, if F' is obtained from F by adding as axioms $\sim \mathcal{C}_2, \sim \mathcal{C}_3, \ldots, \sim \mathcal{C}_p, \ldots$ (for all primes p), the normal models of F' are the fields of characteristic zero. Hence, by Corollary 2.15(a), noting that if $\mathcal{A}$ holds in all normal models of F' it holds in all models of F', $\vdash_{F'} \mathcal{A}$; but then, for some finite number of the new axioms $\sim \mathcal{C}_{q_1}$, $\sim \mathcal{C}_{q_2}, \ldots, \sim \mathcal{C}_{q_n}$, we have $- \mathcal{C}_{q_1}, \ldots, - \mathcal{C}_{q_n} \vdash_F \mathcal{A}$. Let q be a prime greater than all q,, . . . , q_n. In every field of characteristic $\geqslant$ q, the wfs $\sim \mathcal{C}_{q_1}$, $\sim \mathcal{C}_{q_2}, \ldots, \sim \mathcal{C}_{q_n}$ are true; hence, $\mathcal{A}$ is also true. (Other applications in algebra may be found in A. Robinson [1951], Cherlin [1976].)

(2) A graph may be considered as a set partially ordered by a symmetric binary relation R (i.e., the relation which holds between any two vertices if and only if they are connected by an edge). Call a graph k-colorable if and only if the graph can be divided into k disjoint (possibly empty) sets such that no two elements in the same set are in the relation R. (Intuitively, these k sets correspond to k colors, each color being painted on the points in the corresponding set, with the proviso that two points connected by an edge are painted different colors.) Notice that any subgraph of a k-colorable graph is also k-colorable. Now, we can show that if every finite subgraph of a graph $\mathcal{G}$ is k-colorable, and if $\mathcal{G}$ can be well-ordered, then the whole graph $\mathcal{G}$ is k-colorable. To prove this, construct the following generalized theory K with equality (Beth [1953]). There are two binary predicate letters $A_1^2(=)$ and A_2^2 (corresponding to the relation R on $\mathcal{G}$); there are k monadic predicate letters $A_1^1, \ldots, A_k^1$ (corresponding to the k subsets into which we hope to divide the graph), and there are individual constants a_c, one for each element c of the graph $\mathcal{G}$. We have as proper axioms, in addition to the usual assumptions (6)–(7) for equality, the following wfs:

(I) $\sim A_2^2(x, x)$ (irreflexivity of R)

(II) $A_2^2(x, y) \supset A_2^2(y, x)$ (symmetry of R)

(III) $(x)(A_1^1(x) \vee A_2^1(x) \vee \ldots \vee A_k^1(x))$ (division into k classes)

(IV) (x) $\sim (A_i^1(x) \wedge A_j^1(x))$ for $1 \leqslant i < j \leqslant k$ (disjointness of the k classes)

(V) For $1 \leqslant i \leqslant k$, $(x)(y)(A_i^1(x)$ A $A_i^1(y) \supset \sim A_2^2(x, y))$
(Two elements in the same class are not in the relation R.)

(VI) For any two distinct elements b, c of $\mathcal{G}$, a, $\neq$ a,.

(VII) If R(b, c) holds in $\mathcal{G}$, $A_2^2(a_b$, a,).

Now, any finite set of these axioms involves only a finite number of the individual constants $a_{c_1}, \ldots, a_{c_n}$, and since the corresponding subgraph {c,, . . . , c_n} is, by assumption, k-colorable, the given finite set of axioms has a model, and is, therefore, consistent. Since any finite set of axioms is consistent, K is consistent. By Corollary 2.35(1), K has a normal model of cardinality $\leqslant$ the cardinality of the graph $\mathcal{G}$. This model is a k-colorable graph, and by (VI)–(VII), has $\mathcal{G}$ as a subgraph. Hence, $\mathcal{G}$ is also k-colorable. (Compare this proof with a standard mathematical proof of the same result by Bruijn and Erdos [1951]. Generally, use of the method above replaces complicated applications of Tychonoff's Theorem or Konig's Unendlichkeit's Lemma.)

EXERCISES

2.90.^{A} (Loś [1954b]). A group **B** is said to be orderable if there exists a binary relation R on B which totally orders B such that, if x R y, then (x + z) R (y + z) and (z + x) R (z + y). Show, by a method similar to that used in Example (2) above, that a group B is orderable if and only if every finitely-generated subgroup is orderable (if we assume that the set B can be well-ordered).

2.91.^{A} Set up a theory for algebraically-closed fields of characteristic p ($\geqslant$ 0) by adding to the theory F of fields the new axioms P_n, where P_n states that every non-constant polynomial of degree $\leqslant$ n has a root, as well as axioms to determine the characteristic. Show that every wf of F which holds for one algebraically closed field of characteristic zero holds for all of them. (Hint: this theory is $\aleph_\beta$-categorical for $\beta > 0$, axiomatizable, and has no finite models.) (Cf. A. Robinson [1952].)

2.92. By ordinary mathematical reasoning, solve the finite marriage problem: given a finite set M of m men and a set N of women such that each man knows only a finite number of women and, for $1 \leqslant k \leqslant m$, any subset of M having k elements is acquainted with at least k women of N (i.e., there are at least k women in N acquainted with at least one of the k given men). Then it is possible to marry (monogamously) all the men of M to women in N so that every man is mamed to a woman with whom he is acquainted. (Hint—Halmos-Vaughn [1950]: m = 1 is trivial. For m > 1, use induction, considering the cases: (I) for all k with $1 \leqslant k < m$, every set of k men knows at least k + 1 women, and (II) for some k with $1 \leqslant k < m$, there is a set of k men knowing exactly k women.) Extend this result to the infinite case, i.e., when M is infinite and well-orderable and the assumptions above hold for all finite k. (Hint: construct an appropriate generalized first-order theory, analogous to that of Application (2) above and use Corollary 2.35(1).)

2.93. Prove that there is no generalized theory K with equality, having one predicate letter < in addition to = , such that the normal models of K are exactly those interpretations in which the interpretation of < is a well-ordering of the domain of the interpretation.

Let $\mathscr{A}$ be a wf in prenex normal form, and form its closure, say, $(Ey_1)(y_2)(y_3)(Ey_4)(Ey_5)(y_6)\mathscr{B}(y_1, y_2, y_3, y_4, y_5, y_6)$, where $\mathscr{B}$ contains no quantifiers. Erase (Ey,) and replace y, in $\mathscr{B}$ by a new individual constant b,: $(y_2)(y_3)(Ey_4)(Ey_5)(y_6)\mathscr{B}(b_1, y_2, y_3, y_4, y_5, y_6)$. Erase (y_2) and (y_3), obtaining $(Ey_4)(Ey_5)(y_6)\mathscr{B}(b_1, y_2, y_3, y_4, y_5, y_6)$. Now erase (Ey_4) and replace y_4 in $\mathscr{B}$ by a new function letter $g(y_2, y_3)$: $(Ey_5)(y_6)\mathscr{B}(b_1, y_2, y_3, g(y_2, y_3), y_5, y_6)$. Erase (Ey_5) and replace y_5 in $\mathscr{B}$ by a new function letter $h(y_2, y_3)$: $(y_6)\mathscr{B}(b_1, y_2, y_3, g(y_2, y_3), h(y_2, y_3), y_6)$. Finally, erase (y_6). The terminal wf $\mathscr{B}(b_1, y_2, y_3, g(y_2, y_3), h(y_2, y_3), y_6)$ contains no quantifiers, and is denoted by $\mathscr{A}^\star$. Thus, by introducing new function letters, we can eliminate the quantifiers from a wf.

Examples.

1. If $\mathscr{A}$ is $(y_1)(Ey_2)(y_3)(y_4)(Ey_5)\mathscr{B}(y_1, y_2, y_3, y_4, y_5)$ where $\mathscr{B}$ contains no quantifiers, then $\mathscr{A}^\star$ may be taken to be

$$\mathscr{B}(y_1, g(y_1), y_3, y_4, h(y_1, y_3, y_4))$$

2. If $\mathscr{A}$ is $(Ey_1)(Ey_2)(y_3)(y_4)(Ey_5)\mathscr{B}(y_1, y_2, y_3, y_4, y_5)$ where $\mathscr{B}$ contains no quantifiers, then $\mathscr{A}^\star$ is of the form $\mathscr{B}$(b, c, $y_3, y_4, g(y_3, y_4)$).

Notice that $\mathscr{A}^\star \vdash \mathscr{A}$, since we can put the quantifiers back on by several applications of Gen and Rule E4. (To be more precise, in the process of obtaining $\mathscr{A}^\star$, we drop all universal quantifiers and all existential quantifiers, and, for each existentially quantified variable y,, we substitute a function letter $g(z_1, \ldots, z_k)$, where z,, . . . , z_k are the variables which were universally quantified in the prefix preceding (Ey_i). If there are no such variables $z_1, \ldots, z_k$, we replace y_i by a new individual constant.)

PROPOSITION 2.36 (Second ε-Theorem. Rasiowa [1956], Hilbert-Bernays [1939]). Let K be a generalized theory. Replace each axiom $\mathscr{A}$ *of* K *by* $\mathscr{A}^\star$. (The new *function* letters and individual constants *introduced for* one wf are to be different *from* those introduced for another wf.) Let K* be the generalized theory with the proper axioms $\mathscr{A}^\star$. Then, (a) *If* $\mathscr{C}$ is a wf *of* K and $\vdash_{K^\star}\mathscr{C}$, then $\vdash_K\mathscr{C}$; (b) K is consistent if and only if K* is consistent.

PROOF.

(a) Let $\mathscr{C}$ be a wf of K such that $\vdash_{K^\star}\mathscr{C}$. Consider the ordinary theory K, whose axioms $\mathscr{A}_1, \ldots, \mathscr{A}_n$ are such that $\mathscr{A}_1^\star, \ldots, \mathscr{A}_n^\star$ are the axioms used in the proof of $\mathscr{C}$. Let $K_1^\star$ be the theory whose axioms are $\mathscr{A}_1^\star, \ldots, \mathscr{A}_n^\star$. Assume that M is a denumerable model of K,. We may assume that the domain of M is the set P of positive integers (cf. p. 93, Exercise 2.81). Let $\mathscr{A}$ be any axiom of K_1; say, $\mathscr{A}$ is $(Ey_1)(y_2)(y_3)(Ey_4)\mathscr{B}(y_1, y_2, y_3, y_4)$, where $\mathscr{B}$ contains no quantifiers. $\mathscr{A}^\star$ has the form $\mathscr{B}$(b, $y_2, y_3, g(y_2, y_3)$). Extend the model M step by step as follows (note that the domain always remains the set P): since $\mathscr{A}$ is true in M, $(Ey_1)(y_2)(y_3)(Ey_4)\mathscr{B}(y_1, y_2, y_3, y_4)$ is true in M. Let the interpretation b* of *b* be the least positive integer y_1 such that $(y_2)(y_3)(Ey_4)\mathscr{B}(y_1, y_2, y_3, y_4)$ is true in the model. Hence $(Ey_4)\mathscr{B}$(b, y_2, y_3, y_4) is true in this extended model. For any positive integers y_2, y_3 let the interpretation of $g(y_2, y_3)$ be the least positive integer y_4 such that $\mathscr{B}(b, y_2, y_3, y_4)$ is true in the extended model. Hence, $\mathscr{B}(b, y_2, y_3, g(y_2,$ y,)) is true in the extended model. If we do this for all the axioms & of K_1, we obtain a model M* of $K_1^\star$. Since $\vdash_{K_1^\star}\mathscr{C}$, $\mathscr{C}$ is true in M*. Since M* differs from M only in having interpretations of the new individual constants and function letters, and since $\mathscr{C}$ does not contain any of these constants or function letters, $\mathscr{C}$ is true in M. Thus, $\mathscr{C}$ is true in every denumerable model of K_1. Hence, $\vdash_{K_1}\mathscr{C}$ by Corollary 2.15(a). Since the axioms of K, are axioms of K, we have $\vdash_K\mathscr{C}$. (For a constructive proof of an equivalent result, compare Hilbert-Bernays [1939].)

(b) Clearly, K* is an extension of K, since $\mathscr{A}^\star \vdash \mathscr{A}$. Hence, if K* is consistent, so is K. Conversely, assume K consistent. Let $\mathscr{C}$ by any wf of K. If K* is inconsistent, $\vdash_{K^\star}\mathscr{C} \wedge \sim \mathscr{C}$. By Part (a), $\vdash_K\mathscr{C} \wedge \sim \mathscr{C}$, contradicting the consistency of K.

Let us use the term Generalized Completeness Theorem for the proposition that every consistent generalized theory has a model. Clearly, if we assume that every set can be well-ordered (or, equivalently, the axiom of choice), then the Generalized Completeness Theorem is a consequence of Proposition 2.34.

By the Maximal Ideal Theorem (M.I.) we mean the proposition that every Boolean algebra has a maximal ideal. This is equivalent to the Boolean Representation Theorem, which states that every Boolean algebra is isomorphic to a Boolean algebra of sets. (Compare Stone [1936]. For the theory of Boolean algebras, see Sikorski [1960].) The only known proof of the M.I. Theorem uses the axiom of choice, but it is a remarkable fact that the M.I. Theorem is equivalent to the Generalized Completeness Theorem, and this equivalence can be proved without use of the axiom of choice.

PROPOSITION 2.37 (Łoś [1954a], Rasiowa-Sikorski [1951–21). The Generalized Completeness *Theorem* is equivalent to the Maximal Ideal Theorem.

PROOF.

(1) Assume the Generalized Completeness Theorem. Let B be a Boolean algebra. Construct a generalized theory K with equality having the binary function letters u and $\cap$, the singulary function letter f_1^1 (we denote $f_1^1(t)$ by i), predicate letters = and A_1^1, and, for each element b in B, an individual constant a_b. As axioms, we take the usual axioms for a Boolean algebra (cf. Sikorski [1960]), the axioms (6)–(7) for equality, a complete description of B (i.e., if b, c, d, e, b_1 are in B, the axioms a, $\neq a_c$ if b $\neq$ c; a, u a, = a, if b u c = d in B; a, $\cap$ a, = a, if b $\cap$ c = e in B; $\bar{a}_b$ = a,,, if $\bar{b}$ = b, in B, where $\bar{b}$ denotes the complement of b), and axioms asserting that A_1^1 determines a maximal ideal (i.e., $A_1^1(x \cap \bar{x})$, $A_1^1(x) \wedge A_1^1(y) \supset A_1^1(x \text{ u } y)$; $A_1^1(x) \supset A_1^1(x \cap y)$; $A_1^1(x) \vee A_1^1(\bar{x})$; $\sim A_1^1(x \cup \bar{x})$). Now K is consistent, for, if there is a proof in K of a contradiction, this proof contains only a finite number of the symbols a,, a,, . . . , say $a_{b_1}, \ldots, a_{b_n}$. The elements b,, . . . , b_n generate a finite subalgebra B' of B. Every finite Boolean algebra clearly has a maximal ideal. Hence, B' is a model for the wfs occurring in the proof of the contradiction, and therefore the contradiction is true in B', which is impossible. Thus, K is consistent, and, by the Generalized Completeness Theorem, K has a model, which is a Boolean algebra A with a maximal ideal I. But B is a subalgebra of A and $I \cap$ B is a maximal ideal in B.

(2) Assume the Maximal Ideal Theorem. Let K be a consistent generalized theory. For each axiom $\mathscr{A}$ of K, form the wf $\mathscr{A}^\star$ obtained by constructing a prenex normal form for $\mathscr{A}$ and then eliminating the quantifiers through the addition of new individual constants and function letters. Let K' be a new theory having the wfs $\mathscr{A}^\star$, plus all instances of tautologies, as its axioms, such that its wfs contain no quantifiers and its rules of inference are modus ponens and a rule of substitution for variables (viz., substitution of terms for variables). Now K' is consistent, since the theorems of K' are also theorems of the consistent theory K* of Proposition 2.36. Let B be the Lindenbaum algebra determined by K' (i.e., for any wfs $\mathscr{A}$ and $\mathscr{B}$, let $\mathscr{A}$ Eq $\mathscr{B}$ mean that $\vdash_{K'} \mathscr{A} \equiv \mathscr{B}$; Eq is an equivalence relation; let $[\mathscr{A}]$ be the equivalence class of $\mathscr{A}$; define $[\mathscr{A}] \cup [\mathscr{B}] = [\mathscr{A} \vee \mathscr{B}]$, $[\mathscr{A}] \cap [\mathscr{B}] = [\mathscr{A} \wedge \mathscr{B}]$, $[\bar{\mathscr{A}}] = [\sim \mathscr{A}]$; under these operations, the set of equivalence classes is a Boolean algebra, called the **Lindenbaum algebra of K'**). By the Maximal Ideal Theorem, let I be a maximal ideal in B. Define a model M of K' having the set of terms of K' as its domain; the individual constants and function letters are their own interpretations, and, for any predicate letter A_j^n, we say that $A_j^n(t_1, \ldots, t_n)$ is true in M if and only if $[A_j^n(t_1, \ldots, t_n)]$ is not in I. One can show easily that a wf $\mathscr{A}$ of K' is true in M if and only if $[\mathscr{A}]$ is not in I. But, for any theorem $\mathscr{B}$ of $\mathbf{K}'$, $[\mathscr{B}] = 1$, which is not in I. Hence, M is a model for $\mathbf{K}'$. For any axiom $\mathscr{A}$ of K, every substitution instance of $\mathscr{A}^\star(y_1, \ldots, y_n)$ is a theorem in K'; therefore, $\mathscr{A}^\star(y_1, \ldots,$ y,) is true for all y,, . . . , y_n in the model. It follows easily, by reversing the process through which $\mathscr{A}^\star$ arose from $\mathscr{A}$, that $\mathscr{A}$ is true in the model. Hence, M is a model for K.

The Maximal Ideal Theorem (and, therefore, also the Generalized Completeness Theorem) turns out to be strictly weaker than the Axiom of Choice (cf. Halpern [1964]).

EXERCISES

2.94. Show that the Generalized Completeness Theorem implies that every set can be totally ordered (and, therefore, that the axiom of choice holds for any set of non-empty disjoint finite sets).

2.95. In the proof of Proposition 2.37(2), show that if K is an ordinary first-order theory, then the Lindenbaum algebra B is countable and the Maximal Ideal Theorem need not be assumed in the proof.

The natural algebraic structures corresponding to the propositional calculus are Boolean algebras (cf. p. 43, Exercise 1.53, and Rosenbloom [1950], Chapters 1–2). For first-order theories, the presence of quantifiers introduces more algebraic structure. For example, if K is a first-order theory, then, in the corresponding Lindenbaum algebra B, $[(Ex)\mathscr{A}(x)] = \sum_I [\mathscr{A}(t)]$ where $\sum_I$ indicates the least upper bound in B, and t ranges over all terms of K which are free for x in $\mathscr{A}(x)$. Two types of algebraic structures have been proposed to serve as algebraic counterparts of quantification theory. The first, cylindrical algebras, have been studied extensively by Tarski, Thompson, Henkin, Monk, and others (cf. Henkin-Monk-Tarski [1971]). The other approach is the theory of polyadic algebras, invented and developed by Halmos [1962].

13. Elementary Equivalence. Elementary Extensions.

Two interpretations M, and M_2 of a generalized first-order predicate calculus K are said to be elementarily equivalent (written $M_1 \equiv M_2$[†]) if the sentences of K true for M, are the same as the sentences true for M_2. Intuitively, M, $\equiv M_2$ if and only if M, and M_2 cannot be distinguished by means of the language of K.[‡] Of course, K is a generalized predicate calculus and may have non-denumerably many symbols.

Clearly, (i) M $\equiv$ M; (ii) if M, $\equiv M_2$, then $M_2 \equiv M_1$; (iii) if $M_1 \equiv M_2$ and $M_2 \equiv M_3$, then M, $\equiv$ M,.

Two models of a complete theory K must be elementarily equivalent, since the sentences true in these models are precisely the sentences provable in K. This applies, for example, to any two densely ordered sets without first or last elements (cf. p. 81).

[†] This use of $\equiv$ has nothing to do with the connective symbol $\equiv$ used for the biconditional "if and only if'.

[‡] Notice that for M to be a model of a predicate calculus K nothing more is required than that the interpretations provided by M consist only of interpretations of the symbols of K. M is then automatically a model of K, since the only axioms of K are logical axioms.

We already know, by Proposition **2.33(2),** that isomorphic models are elementarily equivalent. The converse, however, is not true. Consider, for example, any complete theory K which has an infinite normal model. By Corollary **2.35(2), K** has normal models of any infinite cardinal $\aleph_\alpha$. If we take two normal models of K of different cardinality, they are elementarily equivalent but not isomorphic. A concrete example is the complete theory $\mathbf{K}_2$ of densely ordered sets **having** neither first nor last element. The rational numbers and the real numbers, **under** their natural **orderings,** are elementarily equivalent models of $\mathbf{K}_2$, but are **not** isomorphic.

EXERCISES

2.96. Let K„ the theory of infinite sets, consist of the pwe theory $\mathbf{K}_1$ of equality, plus the axioms $\mathfrak{B}_n$, where $\mathfrak{B}_n$ asserts that there are at least n elements. Show that any two models of K, are elementarily equivalent (cf. Exercises 2.62 and 2.89(a)).

2.97.^{D} If $\mathbf{M}_1$ and $\mathbf{M}_2$ are elementarily equivalent normal models, and $\mathbf{M}_1$ is finite, prove that M, and $\mathbf{M}_2$ are isomorphic.

2.98. Let K be a theory with equality having $\aleph_\alpha$ symbols.

(a) Prove that there are at most $2^{\aleph_\alpha}$ models of K, no two of which are elementarily equivalent.

(b) Prove that there are at most $2^{\aleph_\gamma}$ mutually non-isomorphic models of K of cardinality $\aleph_\beta$, where γ is the maximum of a and β.

2.99. Let M be any **infinite** normal model of a theory with **equality** K having $\aleph_\alpha$ symbols. Prove that, for any cardinal $\aleph_\gamma \geqslant \aleph_\alpha$, there is a normal model M' of K of cardinality $\aleph_\alpha$ such that M $\equiv$ M'.

A model $\mathbf{M}_2$ of a predicate calculus K is said to be an extension of a model $\mathbf{M}_1$ of K (written $\mathbf{M}_1 \subseteq$ M$_2$‡) if the following conditions hold.

(a) The domain $\mathbf{D}_1$ of $\mathbf{M}_1$ is a subset of the domain $\mathbf{D}_2$ of $\mathbf{M}_2$.

(b) For any individual constant c of K, $c^{\mathbf{M}_2} = c^{\mathbf{M}_1}$, where $c^{\mathbf{M}_2}$ and $c^{\mathbf{M}_1}$ are the interpretations of c in $\mathbf{M}_2$ and M,, respectively.

(c) For any function letter f_j^n of K and any a,, . . . , a„ in $\mathbf{D}_1$, $(f_j^n)^{\mathbf{M}_2}(a_1, \ldots, a_n) = (f_j^n)^{\mathbf{M}_1}(a_1, \ldots, a_n)$.

(d) For any predicate letter A," of K and any a,, . . . , a„ in $\mathbf{D}_1$, $\models_{\mathbf{M}_1} A_j^n[a_1, \ldots,$ a,] if and only if $\models_{\mathbf{M}_2} A_j^n[a_1, \ldots,$ a,].

When M, $\subseteq \mathbf{M}_2$, one also says that $\mathbf{M}_1$ is a substructure (or *submodel*) of $\mathbf{M}_2$.

Examples.

(i) If K contains only the predicate letters = and <, then the set of rational numbers under its natural ordering is an extension of the set of integers under its natural ordering.

(ii) If K is the predicate calculus in the language of field theory (with the predicate letter = , function letters + and ×, and individual constants 0 and 1),

‡The **reader will have no occasion to confuse this use of $\subseteq$ with that for the inclusion relation.**

then the field of real **numbers is an** extension of the field of rational numbers, the field **of** rational numbers **is an** extension of the ring of integers, and the ring of integers is an extension of **the** "semiring" of non-negative integers. For any fields $\mathbf{F}_1$ and $\mathbf{F}_2$, F, $\subseteq \mathbf{F}_2$ if and only if F, is a **subfield** of $\mathbf{F}_2$ in the usual **algebraic** sense.

EXERCISES

2.100. Prove: (a) M $\subseteq$ M. (b) If $\mathbf{M}_1 \subseteq \mathbf{M}_2$ and $\mathbf{M}_2 \subseteq \mathbf{M}_3$, then $\mathbf{M}_1 \subseteq \mathbf{M}_3$. (c) If $\mathbf{M}_1 \subseteq \mathbf{M}_2$ and $\mathbf{M}_2 \subseteq \mathbf{M}_1$, then $\mathbf{M}_1 = \mathbf{M}_2$.

2.101. Assume $\mathbf{M}_1 \subseteq \mathbf{M}_2$.

(a) Let 93(x,, . . . , x_n) be a wf of the form $(y_1) \ldots$ (y,) $\mathcal{C}(x_1, \ldots, x_n, y_1, \ldots,$ y,), where $\mathcal{C}$ contains no **quantifiers.** Show that, for any a,, . . . , a_n in the domain of $\mathbf{M}_1$, if $\models_{\mathbf{M}_2} \mathfrak{B}[a_1, \ldots,$ a,], then $\models_{\mathbf{M}_1} \mathfrak{B}[a_1, \ldots,$ a,]. In particular, any sentence (y,) . . . (y,) $\mathcal{C}(y_1, \ldots, y_m)$, where $\mathcal{C}$ contains no quantifiers, is true in $\mathbf{M}_1$ if it is true in $\mathbf{M}_2$.

(b) Let $\mathfrak{B}(x_1, \ldots, x_n)$ be a wf of the form $(Ey_1) \ldots$ (Ey,) $\mathcal{C}(x_1, \ldots, x_n,$ y$_1, \ldots,$ y,), where $\mathcal{C}$ has no quantifiers. Show that, for any $a_1, \ldots, a_n$ in the domain of $\mathbf{M}_1$, if $\models_{\mathbf{M}_1} \mathfrak{B}$[a,, . . . , a,], then $\models_{\mathbf{M}_2} \mathfrak{B}[a_1, \ldots,$ a,]. In particular, any sentence (Ey,) . . . (Ey_m) $\mathcal{C}(y_1, \ldots, y_m)$, where $\mathcal{C}$ contains no quantifiers, is true in $\mathbf{M}_2$ if it is true in $\mathbf{M}_1$.

2.102. (a) Let K be the predicate calculus of the language of **field** theory. Find a model M of K and a non-empty subset X of the domain D of M such that there is no substructure of M having domain X.

(b) If K is a predicate calculus with no individual constants or function letters, show that, if M is a model of K and X is a subset of the domain D of M, then there is one and only one substructure of M having domain X.

(c) Let K be any predicate calculus. Let M be any model of K and let X be any subset of the domain D of M. Let Y be the intersection of the domains of all submodels M' of M such that X $\subseteq$ D, the domain of M'. Show that there is one and only one **submodel** of M having domain Y. (This **submodel** is called the ***submodel*** generated by X.)

A somewhat stronger relation between interpretations than "extension" is useful in model theory. Let M, and $\mathbf{M}_2$ be models of some predicate calculus K. We say that $\mathbf{M}_2$ is an elementaty ***extension*** of M, (written M, $\leqslant_e \mathbf{M}_2$) if:

(a) $\mathbf{M}_1 \subseteq \mathbf{M}_2$**, and**

(b) For any wf $\mathcal{C}(y_1, \ldots,$ y,) of K and for any a,, . . . , a, **in the domain $\mathbf{D}_1$ of $\mathbf{M}_1$,**

$$\models_{\mathbf{M}_1} \mathcal{C}[a_1, \ldots, a,] \text{ if and only if } \models_{\mathbf{M}_2} \mathcal{C}[a_1, \ldots, \text{a,}].$$

(In particular, for any sentence $\mathcal{C}$ of K, $\mathcal{C}$ is true for M, if and only if $\mathcal{C}$ is true for $\mathbf{M}_2$.) When M, $\leqslant_e \mathbf{M}_2$, we shall also say that M, is an ***elementary*** substructure (or elementaty submodel) of $\mathbf{M}_2$.

It is obvious that, if $M_1 \leqslant_e M_2$, then $M_1 \subseteq M_2$ and $M_1 \equiv M_2$. The converse is not true, as the following example shows. Let K be the first-order theory of groups (cf. p. 82). K has the predicate letter $=$, function letter $+$, and individual constant 0. Let I be the group of integers, and 21 the group of even integers. Then $21 \subseteq$ I and I $\simeq$ 21. (The function g such that $g(x) = 2x$ for all x in I is an isomorphism of I with 21.) Since I $\simeq$ 21, I $\equiv$ 21. Consider the wf $\mathscr{A}(y)$: $(Ex)(x + x = y)$. Then $\models_I \mathscr{A}[2]$, but not-$\models_{21}\mathscr{A}[2]$. Thus, I is not an elementary extension of 21. (This example shows the stronger result that even assuming $M_1 \subseteq M_2$ and $M_1 \simeq M_2$ does not imply M, $\leqslant_e M_2$.)

The following theorem provides an easy method for showing that $M_1 \leqslant_e M_2$.

PROPOSITION 2.38 (TARSKI-VAUGHT [1957]). Let $M_1 \subseteq M_2$. *Assume the* following condition:

($) For *every* wf $\mathscr{B}$(x,, . . . , x,) *of* the form $(Ey)\mathscr{A}(x_1, \ldots,$ x,, y) and *for* all a,, . . . , a, in the domain D_1 *of* M_1, *if* $\models_{M_2}\mathscr{B}$[a,, . . . , a,], then there is some b in D, such that $\models_{M_2}\mathscr{A}[a_1, \ldots,$ a,, b].

Then $M_1 \leqslant_e M_2$.

PROOF. Let us prove: (*) $\models_{M_1}\mathscr{C}[a_1, \ldots, a_k]$ if and only if $\models_{M_2}\mathscr{C}[a_1, \ldots, a_k]$ for any wf $\mathscr{C}(x_1, \ldots, x_k)$ and any a,, . . . , a, in D_1. The proof is by induction on the number m of connectives and quantifiers in $\mathscr{C}$. If m $= 0$, then (*) follows from clause (d) of the definition of M, $\subseteq M_2$. Now assume that (*) holds true for all wfs having fewer than m connectives and quantifiers.

Case 1. $\mathscr{C}$ is $\sim \mathscr{D}$. By inductive hypothesis, $\models_{M_1}\mathscr{D}[a_1, \ldots,$ a,] if and only if $\models_{M_2}\mathscr{D}$[a,, . . . , a_k]. Using the fact that not-$\models_{M_1}\mathscr{D}$[a,, . . . , a,] if and only if $\models_{M_1} \sim \mathscr{D}[a_1, \ldots,$ a,], and similarly for M_2, we obtain (*).

Case 2. $\mathscr{C}$ is $\mathscr{D} \supset 6$. By inductive hypothesis, $\models_{M_1}\mathscr{D}[a_1, \ldots, a_k]$ if and only if $\models_{M_2}\mathscr{D}[a_1, \ldots,$ a,], and similarly for 6. (*) then follows easily.

Case 3. $\mathscr{C}$ is $(Ey)\mathscr{A}(x_1, \ldots, x_k, y)$. By inductive hypothesis, (**) $\models_{M_1}\mathscr{A}[a_1, \ldots,$ a,, b] if and only if $\models_{M_2}\mathscr{A}[a_1, \ldots,$ a,, b] for any a,, . . . , a,, b in D,.

(3a): Assume $\models_{M_1}(Ey)\mathscr{A}(x_1, \ldots, x_k, y)[a_1, \ldots,$ a,] for some a,, . . . , a, in D_1. Then, $\models_{M_1}\mathscr{A}[a_1, \ldots, a_k,$ b] for some b in D,. So, by (**), $\models_{M_2}\mathscr{A}[a_1, \ldots, a_k,$ b]. Hence,

$$\models_{M_2}(Ey)\mathscr{A}(x_1, \ldots, x_k, y)[a_1, \ldots, a_k].$$

(3b): Assume $\models_{M_2}(Ey)\mathscr{A}(x_1, \ldots, x_k, y)[a_1, \ldots, a_k]$ for some a,, . . . , a, in D_1. By assumption ($), there exist b in D_1 such that $\models_{M_2}\mathscr{A}[a_1, \ldots,$ a,, b]. Hence, by (**), $\models_{M_1}\mathscr{A}[a_1, \ldots,$ a,, b], and, therefore, $\models_{M_1}(Ey)\mathscr{A}(x_1, \ldots, x_k, y)[a_1, \ldots, a_k]$.

This completes the induction proof since any wf is logically equivalent to a wf that can be built up from atomic wfs by forming negations, conditionals, and existential quantifications.

EXERCISES

2.103. Prove: (a) M $\leqslant_e$M; (b) If $M_1 \leqslant_e M_2$ and $M_2 \leqslant_e M_3$, then $M_1 \leqslant_e M_3$.

2.104. If $M_1 \leqslant_e M$, $M_2 \leqslant_e M$, and $M_1 \subseteq M_2$, prove that $M_1 \leqslant_e M_2$.

2.105. Let K be the theory of totally ordered sets with equality (Axioms (a)–(c), (e)–(g) of Exercise 2.63, p. 81). Let M_1 and M_2 be the models for K with domains the set of non-negative integers and the set of positive integers, respectively (under the natural orderings $<$ in both cases). Prove that $M_1 \subsetneq M_2$, $M_1 \simeq M_2$, but $M_1 \nleqslant_e M_2$.

Let M be a model of a theory K. Extend K to a theory K' by adding a new individual constant a_d for every member d of the domain of M. We can extend M to a model of K' by taking d as the interpretation of a_d. By the diagram of M we mean the set of all true sentences of M of the forms $A_j^n(a_{d_1}, \ldots, a_{d_n})$, $\sim A_j^n(a_{d_1}, \ldots, a_{d_n})$, and $f_j^n(a_{d_1}, \ldots, a_{d_n}) = a_{d_m}$. In particular, $a_{d_1} \neq a_{d_2}$ belongs to the diagram if $d_1 \neq d_2$. By the complete diagram of M we mean the set of all sentences of K' that are true for M.

Clearly, any model M' of the complete diagram of M determines an elementary extension M" of M,† and vice versa.

EXERCISES

2.106. (a) Let M be a denumerable normal model of an ordinary theory K with equality such that every element of the domain of M is the interpretation of some closed term of K.

(i) Show that, if M $\subseteq$ M' and M M', then M $\leqslant_e$M'.

(ii) Prove that there is a denumerable normal elementary extension M' of M such that M and M' are not isomorphic.

(b) Let K be a predicate calculus with equality having two function letters $+$ and $\times$, and two individual constants 0 and 1. Let M be the standard model of arithmetic, with domain the set of natural numbers, and $+$, $\times$, 0, 1 having their ordinary meaning. Prove that M has a proper denumerable extension which is not isomorphic to M, that is, there is a denumerable non-standard model of arithmetic.

PROPOSITION 2.39 (Upward Lowenheim-Skolem-Tarski Theorem). Let K be a theory with equality having $\aleph_\alpha$ symbols, and let M be a normal model of K with domain *of* cardinality $\aleph_\beta$. Let y be the maximum *of* α and β. Then, for any $\delta \geqslant$ y, there is a model M' *of* cardinality $\aleph_\delta$ such that M $\neq$ M' and M $\leqslant_e$M'.

PROOF. Add to the complete diagram of M a set of cardinality $\aleph_\delta$ of new individual constants b,, together with axioms b, $\neq b_\rho$ for distinct τ and ρ and axioms b, $\neq a_d$ for all individual constants a_d corresponding to members d of the domain of M. This new theory K' is consistent, since M can be used as a model for any finite number of axioms of K'. (If $b_{\tau_1}, \ldots, b_{\tau_k}, a_{d_1}, \ldots, a_{d_m}$ are the new individual constants in these axioms, interpret $b_{\tau_1}, \ldots, b_{\tau_k}$ as distinct elements of the domain of M different from $d_1, \ldots, d_m$.) Hence, by Corollary 2.35(i), K' has a normal model M of cardinality $\aleph_\delta$ such that M $\subsetneqq$ M' and M $\leqslant_e$M'.

†The elementary extension M" of M is obtained from M' by forgetting about the interpretations of the a_d's.

PROPOSITION 2.40 (DOWNWARD LÖWENHEIM-SKOLEM-TARSKI THEOREM). *Let* K be a theoty with $\aleph_\alpha$ symbols, and let M be a model cf K cf *cardinality* $\aleph_\gamma \geqslant \aleph_\alpha$. Assume A *is* a subset cf the *domain* D cf M *having* cardinality n, *and* assume $\aleph_\beta$ is *such* that $\aleph_\gamma \geqslant \aleph_\beta \geqslant max(\aleph_\alpha$, n). Then there is an *elementary submodel* M' cf M cf cardinality $\aleph_\beta$ and with domain $D' \supseteq$ A.

PROOF. Since n $\leqslant \aleph_\beta \leqslant \aleph_\gamma$, we can add $\aleph_\beta$ elements of D to A to obtain a larger set B of cardinality $\aleph_\beta$. Consider any subset C of D having cardinality $\aleph_\beta$. For every wf $\mathcal{Q}(y_1, \dots,$ y„, z) of K and any a,, $\dots, a_n$ in C such that $\vDash_M (Ez)\mathcal{Q}(y_1, \dots, y_n, z)[a_1, \dots,$ a„], add to C the first element b of D (with respect to some fixed well-ordering of D) such that $\vDash_M \mathcal{Q}[a_1, \dots,$ a„, b]. Denote the so-enlarged set by C$^{\#}$. Since K has $\aleph_\alpha$ symbols, there are $\aleph_\alpha$ wfs. Since $\aleph_\alpha \leqslant \aleph_\beta$, there are at most $\aleph_\beta$ new elements in C^{X}, and, therefore, the cardinality of $C^{\#}$ is $\aleph_\beta$. Form by induction a sequence of sets C_0, C,, ... by setting $C_0 =$ B and $C_{n+1} = C_n{}^{\#}$. Let $D' = \bigcup_{n \in \omega}$ C„. Then the cardinality of D' is X. *In* addition, D' is closed under all the functions $(f_j^n)^M$. (Assume a,, $\dots$, a$_n$ in D'. We may assume a,, $\dots$, a„ in C_k for some k. Now $\vDash_M (Ez)(f_j^n(x_1, \dots, x_n) = z)[a_1, \dots,$ a„]. Hence, $(f_j^n)^M(a_1, \dots,$ a„), being the first and only member b of D such that $\vDash_M (f_j^n(x_1, \dots, x_n) = z)[a_1, \dots,$ a„, b], must belong to C$_k{}^{X} = C_{k+1} \subseteq D'$.) Similarly, all interpretations $(a_j)^M$ of individual constants are in D'. Hence, D' determines a substructure M' of M. To show that $M' \leqslant_e$M, consider any wf $\mathcal{Q}(y_1, \dots, y_n, z)$ and any a,, $\dots$, a„ in D' such that $\vDash_M (Ez)\mathcal{Q}(y_1, \dots, y_n, z)[a_1, \dots,$ a„]. There exists C_k such that a,, $\dots, a_n$ are in C_k. Let b be the first element of D such that $\vDash_M \mathcal{Q}[a_1, \dots,$ a„, b]. Then b $\in C_k{}^{\#} = C_{k+1} \subseteq D'$. So, by the Tarski-Vaught Theorem (Proposition 2.38), M' $\leqslant_e$M.

14. Ultrapowers. Non-Standard Analysis.

By a filter on a non-empty set A we mean a set 5 of subsets of A such that

(i) A $\in$ 5;
(ii) $B \in \mathfrak{F} \wedge C \in \mathfrak{F} \supset B \cap C \in \mathfrak{F}$;
(iii) $B \in \mathfrak{F} \wedge B \subseteq C \supset C \in \mathfrak{F}$.†

Examples.

1. $\mathfrak{F} =$ (A) is a filter on A.

2. 5 $= \mathcal{P}(A)$ is a filter on A.† It is said to be improper and every other filter on A is said to be prover.

3. Let B $\subseteq A$. The set $\mathfrak{F}_B = \{C | B \subseteq$ C $\subseteq$ A) is a filter on A. $\mathfrak{F}_B$ consists of all subsets of A that include B. Any filter of the form $\mathfrak{F}_B$ is called a principal filter. In particular, $\mathfrak{F}_A =$ (A) and $\mathcal{P}(A) = \mathfrak{F}_0$ are principal filters. (Remember that 0 denotes the empty set.)

EXERCISES

2.107. Show that a filter $\mathfrak{F}$ on A is proper if and only if 0 4 $\mathfrak{F}$.

2.108. Show that a filter 9 on A is a principal filter if and only if the intersection of all sets in $\mathfrak{F}$ is a member of 5.

2.109. Prove that every finite filter is a principal filter. In particular, any filter on a finite set A is a principal filter.

2.110. Let A be infinite and let $\mathfrak{F}$ be the set of all subsets of A that are complements of finite sets: $\mathfrak{F} = \{C | (EW)(C = A - W \wedge \text{Fin}(W)))$. Show that $\mathfrak{F}$ is a non-principal filter on A.

2.111. Assume A has cardinality $\aleph_\beta$. Let $\aleph_\alpha \leqslant \aleph_\beta$. Let $\mathfrak{F}$ be the set of all subsets of A whose complements have cardinality $< \aleph_\alpha$. Show that 5 is a non-principal filter on A.

2.112. A collection $\mathcal{G}$ of sets is said to have the *finite* intersection property if $B_1 \cap B_2 \cap \dots \cap B_k \neq 0$ for any sets $B_1, \dots, B_k$ in $\mathcal{G}$. If $\mathcal{G}$ is a collection of subsets of A having the finite intersection property, and $\mathfrak{F} = \{C | (EB)(B \in \mathcal{G} \wedge B \subseteq C \subseteq A))$, show that $\mathfrak{F}$ is aproper filter on A.

DEFINITION. A filter $\mathfrak{F}$ on a set A is called an *ultrafilter* on A if $\mathfrak{F}$ is a maximal proper filter on A, that is, 5 is a proper filter on A and there is no proper filter $\mathcal{G}$ on A such that $\mathfrak{F} \subset \mathcal{G}$.

Example. Let a $\in$ A. The principal filter $\mathfrak{F}_a = \{B | a \in$ B $\wedge$ B $\subseteq$ A) is an ultrafilter on A. For, assume that $\mathcal{G}$ is a filter on A such that $\mathfrak{F}_a$ C $\mathcal{G}$. Let $C \in \mathcal{G} - \mathfrak{F}_a$. Then C $\subseteq$ A and a $\notin$ C. Hence, a $\in$ A $-$ C. Thus, A $-$ C $\in \mathfrak{F}_a \subset \mathcal{G}$. Since $\mathcal{G}$ is a filter and C and A $-$ C are both in $\mathcal{G}$, then 0 = C $\cap$ (A $-$ C) $\in \mathcal{G}$. Hence, $\mathcal{G}$ is not a proper filter.

EXERCISES

2.113. Let $\mathfrak{F}$ be a proper filter on A, and assume that B $\subseteq A$ and $A - B$ 4 $\mathfrak{F}$. Prove that there is a proper filter $\mathfrak{F}' \supseteq \mathfrak{F}$ such that B $\in \mathfrak{F}'$.

2.114. Let $\mathfrak{F}$ be a proper filter on A. Prove that $\mathfrak{F}$ is an ultrafilter on A if and only if, for every $B \subseteq A$, either $B \in \mathfrak{F}$ or $A -$ B $\in \mathfrak{F}$.

2.115. Let 45 be a proper filter on A. Show that 5 is an ultrafilter on A if and only if, for all B and C in $\mathcal{P}(A)$, if $B \notin \mathfrak{F}$ and $C \notin \mathfrak{F}$, then $B \cup C$ 4 $\mathfrak{F}$.

2.116. (a) Show that every principal ultrafilter on A is of the form $\mathfrak{F}_a = \{B | a \in B \wedge B \subseteq A)$, where $a \in A$.

(b) Show that a non-principal ultrafilter on A contains no finite sets.

2.117. Let $\mathfrak{F}$ be a filter on a set A and let $\mathcal{J}$ be the corresponding ideal: $B \in \mathcal{J}$ if and only if $A - B \in$ 5. Prove that $\mathfrak{F}$ is an ultrafilter on A if and only if $\mathcal{J}$ is a maximal ideal.

2.118. Let X be a chain of proper filters on a set A, that is, for any B and C in X, either $B \subseteq C$ or $C \subseteq B$. Prove that the union $\cup(X) = \{a | (EB)(B \in X \wedge a \in B\}$ is a proper filter on A and $B \subseteq \cup(X)$ for all B in X.

[†] The notion of a filter is related to that of an ideal. A collection $\mathfrak{F} \subseteq \mathcal{P}(A)$ is *a* filter on A if and only if the set $\mathcal{G} = \{$A $- B | B \in \mathfrak{F}\}$ of complements of sets in $\mathfrak{F}$ is an ideal in the Boolean algebra $\mathcal{P}(A)$. Remember that $\mathcal{P}(A)$ denotes the set of all subsets of A.

PROPOSITION 2.41 (ULTRAFILTER THEOREM). Every filter $\mathfrak{F}$ on a set A can be extended to an *ultrafilter* on A.[†]

PROOF. Let $\mathfrak{F}$ be a filter on A. Let $\mathfrak{J}$ be the corresponding ideal: $B \in \mathfrak{J}$ if and only if $A - B \in \mathfrak{F}$. By Proposition 2.37, every ideal can be extended to a maximal ideal. In particular, $\mathfrak{J}$ can be extended to a maximal ideal $\mathfrak{J}$. If we let $\mathfrak{G} = \{B|A - B \in \mathfrak{J}\}$, then $\mathfrak{G}$ is easily seen to be an ultrafilter, and $\mathfrak{F} \subseteq 9$.

The existence of an ultrafilter including $\mathfrak{F}$ can be proved easily on the basis of Zorn's Lemma (p. 210). (In fact, consider the set X of all proper filters $\mathfrak{F}'$ such that $\mathfrak{F} \subseteq \mathfrak{F}'$. X is partially ordered by C and any C-chain in X has an upper bound in X, namely, by Exercise 2.118, the union of all filters in the chain. Hence, by Zorn's Lemma, there is a maximal element $\mathfrak{F}^\star$ in X, which is the required ultrafilter.) However, Zorn's Lemma is equivalent to the Axiom of Choice, which is a stronger assumption than the Generalized Completeness Theorem.

COROLLARY 2.42. *If* A is an infinite set, there exists a nun-principal *ultrafilter* on A.

PROOF. Let $\mathfrak{F}$ be the filter on A consisting of all complements $A - B$ of finite subsets B of A (cf. Exercise 2.110). By Proposition 2.41, there is an ultrafilter $\mathfrak{G} \supseteq \mathfrak{F}$. Assume $\mathfrak{G}$ is a principal ultrafilter. By Exercise 2.116(a), $\mathfrak{G} = \mathfrak{F}_a$ for some $a \in A$. Then $A - \{a\} \in \mathfrak{F} \subseteq \mathfrak{G}$. Also, $\{a\} \in \mathfrak{G}$. Hence, $0 = \{a\} \cap (A - \{a\}) \in \mathfrak{G}$, contradicting the fact that an ultrafilter is proper.

Reduced Direct Products. We shall now study an important way of constructing models. Let K be any predicate calculus with equality. Let J be a non-empty set, and, for each j in J, let M_j be some normal model of K. In other words, consider a function F assigning to each j in J some normal model. We denote $F(j)$ by M_j.

Let $\mathfrak{F}$ be an ultrafilter on J. For each j in J, let D_j denote the domain of the model M_j. By the Cartesian product $\prod_{j \in J} D_j$ we mean the set of all functions f with domain J such that $f(j) \in D_j$ for all j in J. If $f \in \prod_{j \in J} D_j$, we shall refer to $f(j)$ as the j^th^ *component* of f. Let us define a binary relation $=_{\mathfrak{F}}$ in $\prod_{j \in J} D_j$ as follows:

$$f =_{\mathfrak{F}} g \text{ if and only if } \{j|f(j) = g(j)\} \in \mathfrak{F}.$$

If we think of the sets in $\mathfrak{F}$ as being "large" sets, then, borrowing a phrase from measure theory, we read $f =_{\mathfrak{F}} g$ as "$f(j) = g(j)$ almost everywhere".

It is easy to see that $=_{\mathfrak{F}}$ is an equivalence relation: (i) $f =_{\mathfrak{F}} f$; (ii) if $f =_{\mathfrak{F}} g$, then $g =_{\mathfrak{F}} f$; (iii) if $f =_{\mathfrak{F}} g$ and $g =_{\mathfrak{F}} h$, then $f =_{\mathfrak{F}} h$. For the proof of (iii), observe that $\{j|f(j) = g(j)\} \cap \{j|g(j) = h(j)\} \subseteq \{j|f(j) = h(j)\}$. If $\{j|f(j) = g(j)\}$

[†] We assume the Generalized Completeness Theorem (p. 101).

and $\{j|g(j) = h(j)\}$ are in $\mathfrak{F}$, then so is their intersection, and, therefore, also $\{j|f(j) = h(j)\}$.

On the basis of the equivalence relation $=_{\mathfrak{F}}$, we can divide $\prod_{j \in J} D_j$ into equivalence classes: For any f in $\prod_{j \in J} D_j$, we define its equivalence class $f_{\mathfrak{F}}$ as $\{g|f =_{\mathfrak{F}} g\}$. Clearly, (i) $f \in f_{\mathfrak{F}}$; (ii) $f_{\mathfrak{F}} = h_{\mathfrak{F}}$ if and only if $f =^{\mathfrak{F}} h$; (iii) if $f_{\mathfrak{F}} \neq h_{\mathfrak{F}}$, then $f_{\mathfrak{F}} \cap h_{\mathfrak{F}} = 0$. We denote the set of all equivalence classes $f_{\mathfrak{F}}$ by $\prod_{j \in J} D_j/\mathfrak{F}$. Intuitively, $\prod_{j \in J} D_j/\mathfrak{F}$ is obtained from $\prod_{j \in J} D_j$ by identifying (or merging) elements of $\prod_{j \in J} D_j$ that are equal almost everywhere.

Now we shall define a model M of K with domain $\prod_{j \in J} D_j/\mathfrak{F}$.

(I) Let c be any individual constant of K, and let c_j be the interpretation of c in M_j. Then the interpretation of c in M will be $f_{\mathfrak{F}}$, where f is the function such that $f(j) = c_j$ for all j in J. We denote f by $\{c_j\}_{j \in J}$.

(II) Let f_k^n be any function letter of K and let A_k^n be any predicate letter of K. Their interpretations $(f_k^n)^M$ and $(A_k^n)^M$ are defined in the following manner. Let $(g_1)_{\mathfrak{F}}, \ldots, (g_n)_{\mathfrak{F}}$ be any members of $\prod_{j \in J} D_j/\mathfrak{F}$.

(a) $(f_k^n)^M((g_1)_{\mathfrak{F}}, \ldots, (g_n)_{\mathfrak{F}}) = h_{\mathfrak{F}}$, where $h(j) = (f_k^n)^M(g_1(j), \ldots, g_n(j))$ for all j in J.

(b) $(A_k^n)^M((g_1)_{\mathfrak{F}}, \ldots, (g_n)_{\mathfrak{F}})$ holds if and only if $\{j|\models_{M_j} A_k^n[g_1(j), \ldots, g_n(j)]\} \in \mathfrak{F}$.

Intuitively, $(f_k^n)^M$ is calculated component-wise, and $(A_k^n)^M$ holds if and only if it holds in almost all components. Definitions (a)–(b) have to be shown to be independent of the choice of the representatives $g_1, \ldots, g_n$ in the equivalence classes $(g_1)_{\mathfrak{F}}, \ldots, (g_n)_{\mathfrak{F}}$:

If $g_1 =_{\mathfrak{F}} g_1^*, \ldots, g_n =_{\mathfrak{F}} g_n^*$ and $h^*(j) = (f_k^n)^{M_j}(g_1^*(j), \ldots, g_n^*(j))$, then (i) $h_{\mathfrak{F}} = h^*_{\mathfrak{F}}$; and (ii) $\{j|\models_{M_j} A_k^n[g_1(j), \ldots, g_n(j)]\} \in \mathfrak{F}$ if and only if $\{j|\models_{M_j} A_k^n[g_1^*(j), \ldots, g_n^*(j)]\} \in \mathfrak{F}$.

(i) follows from the inclusion

$$\{j|g_1(j) = g_1^*(j)\} \cap \ldots \cap \{j|g_n(j) = g_n^*(j)\}$$
$$\subseteq \{j|(f_k^n)^{M_j}(g_1(j), \ldots, g_n(j)) = (f_k^n)^{M_j}(g_1^*(j), \ldots, g_n^*(j))\}.$$

(ii) follows from the inclusions

$$\{j|g_1(j) = g_1^*(j)\} \cap \ldots \cap \{j|g_n(j) = g_n^*(j)\}$$
$$\subseteq \{j|\models_{M_j} A_k^n[g_1(j), \ldots, g_n(j)] \text{ if and only if } \models_{M_j} A_k^n[g_1^*(j), \ldots, g_n^*(j)]\}$$

and

$$\{j \mid \models_{\mathrm{M}_j} A^n_k[g_1(j), \dots, g_n(j)]\} \cap \{j \mid \models_{\mathrm{M}_j} A^n_k[g_1(j), \dots, g_n(j) \mid \text{if and}$$

$$\text{only if} \models_{\mathrm{M}_j} {}^n_k[g_1{}^*(j), \dots, g_n{}^*(j)]\} \subseteq \{j \mid \models_{\mathrm{M}_j} A^n_k[g_1{}^*(j), \dots g_n(j)]\}$$

In the case of the equality relation $=$, which is an abbreviation for A^2_1,

$$\begin{aligned}(A^2_1)^{\mathrm{M}}(g_{\mathcal{F}}, h_{\mathcal{F}}) \quad &\text{if and only if} \quad \{j \mid \models_{\mathrm{M}} A^2_1[g(j), h(j)]\} \in \mathcal{F}\\ &\text{if and only if} \quad \{j \mid g(j) = h(j)\} \in \mathcal{F}\\ &\text{if and only if} \quad g =_{\mathcal{F}} h,\end{aligned}$$

that is, if and only if $g_{\mathcal{F}} = h_{\mathcal{F}}$. Hence, the interpretation $(A^2_1)^{\mathrm{M}}$ is the identity relation, and the model M is normal.

The model M defined above will be denoted $\prod_{j \in J} \mathrm{M}_j/\mathcal{F}$, and will be called a *reduced direct product*. When $\mathcal{F}$ is an ultrafilter, $\prod_{j \in J} \mathrm{M}_j/\mathcal{F}$ is called an *ultraproduct*. When $\mathcal{F}$ is an ultrafilter and all the M_j's are the same model N, then $\prod_{j \in J} \mathrm{M}_j/\mathcal{F}$ is denoted $\mathrm{N}^J/\mathcal{F}$ and is called an *ultrapower*.

Examples.

1. Choose a fixed element r of the index set J, and let $\mathcal{F}$ be the principal ultrafilter $\mathcal{F}_r = \{B \mid r \in B \wedge B \subseteq J\}$. Then for any f, g in $\prod_{j \in J} \mathrm{D}_j$, $f =_{\mathcal{F}} g$ if and only if $\{j \mid f(j) = g(j)\} \in \mathcal{F}$, that is, if and only if $f(r) = g(r)$. Hence, a member of $\prod_{j \in J} \mathrm{D}_j/\mathcal{F}$ consists of all f in $\prod_{j \in J} \mathrm{D}_j$ having the same r^{th} component. For any predicate letter A^n_k of K, and any $g_1, \dots, g_n$ in $\prod_{j \in J} \mathrm{D}_j$, $\models_{\mathrm{M}} A^n_k[(g_1)_{\mathcal{F}}, \dots, (g_n)_{\mathcal{F}}]$ if and only if $\{j \mid \models_{\mathrm{M}_j} A^n_k[g_1(j), \dots, g_n(j)]\} \in \mathcal{F}$, that is, if and only if $\models_{\mathrm{M}_r} A^n_k[g_1(r), \dots, g_n(r)]$. Hence, it is easy to verify that the function φ: $\prod_{j \in J} \mathrm{D}_j/\mathcal{F} \rightarrow \mathrm{D}_r$, defined by $\varphi(g_{\mathcal{F}}) = g(r)$, is an isomorphism of $\prod_{j \in J} \mathrm{M}_j/\mathcal{F}$ with M_r. Thus, when $\mathcal{F}$ is a principal ultrafilter, the ultraproduct $\prod_{j \in J} \mathrm{M}_j/\mathcal{F}$ is essentially the same as one of its components and yields nothing new.

2. Let $\mathcal{F}$ be the filter $\{J\}$. Then, for any f, g in $\prod_{j \in J} \mathrm{D}_j$, $f =_{\mathcal{F}} g$ if and only if $\{j \mid f(j) = g(j)\} \in \mathcal{F}$, that is, if and only if $f(j) = g(j)$ for all j in J, i.e., if and only if $f = g$. Thus, every member of $\prod_{j \in J} \mathrm{D}_j/\mathcal{F}$ is a singleton $\{g\}$ for some g in $\prod_{j \in J} \mathrm{D}_j$. Moreover,

$$(f^n_k)^{\mathrm{M}}((g_1)_{\mathcal{F}}, \dots, (g_n)_{\mathcal{F}}) = \{(f^n_k)^{\mathrm{M}_j}(g_1(j), \dots, g_n(j))\}\, j \in J;$$

$\models_{\mathrm{M}} A^n_k[(g_1)_{\mathcal{F}}, \dots, (g_n)_{\mathcal{F}}]$ if and only if $\models_{\mathrm{M}_j} A^n_k[g_1(j), \dots, g_n(j)]$ for all j. Hence, $\prod_{j \in J} \mathrm{M}_j/\mathcal{F}$ is, in this case, essentially the same as the ordinary "direct product" $\prod_{j \in J} \mathrm{M}_j$, in which the operations and relations are defined component-wise.

3. Let $\mathcal{F}$ be the improper filter $\mathcal{P}(J)$. Then, for any f, g in $\prod_{j \in J} \mathrm{D}_j$, $f =_{\mathcal{F}} g$ if and only if $\{j \mid f(j) = g(j)\} \in \mathcal{F}$, that is, if and only if $\{j \mid f(j) = g(j)\} \in \mathcal{P}(J)$. Thus, $f =_{\mathcal{F}} g$ for all f and g, and $\prod_{j \in J} \mathrm{D}_j/\mathcal{F}$ consists of only one element. For any predicate letter A^n_k, $\models_{\mathrm{M}} A^n_k[f_{\mathcal{F}}, \dots, f_{\mathcal{F}}]$ if and only if $\{j \mid \models_{\mathrm{M}_j} A^n_k[f(j), \dots, f(j)]\} \in \mathcal{P}(J)$, i.e., every atomic wf is true.

The basic theorem on ultraproducts is due to Łoś [1955].

PROPOSITION 2.43 (ŁOŚ'S THEOREM). *Let $\mathcal{F}$ be an ultrafilter on a set J, and let $\mathrm{M} = \prod_{j \in J} \mathrm{M}_j/\mathcal{F}$ be an ultraproduct.*

(a) Let $\mathrm{s} = ((g_1)_{\mathcal{F}}, (g_2)_{\mathcal{F}}, \dots)$ be a denumerable sequence of elements of $\prod_{j \in J} \mathrm{D}_j/\mathcal{F}$. For each j in J, let s_j be the denumerable sequence $(g_1(j), g_2(j), \dots)$ in D_j. Then, for any wf $\mathcal{A}$ of K, s satisfies $\mathcal{A}$ in M if and only if $\{j \mid \mathrm{s}_j$ satisfies $\mathcal{A}$ in $\mathrm{M}_j\} \in \mathcal{F}$.

(b) For any sentence $\mathcal{A}$ of K, $\mathcal{A}$ is true in $\prod_{j \in J} \mathrm{M}_j/\mathcal{F}$ if and only if $\{j \mid \models_{\mathrm{M}_j} \mathcal{A}\} \in \mathcal{F}$. (Thus, (b) asserts that a sentence $\mathcal{A}$ is true in an ultraproduct if and only if it is true in almost all components.)

PROOF. (a) We shall use induction on the number m of connectives and quantifiers in $\mathcal{A}$. We can reduce the case $m = 0$ to the following subcases:† (i) $A^n_k(x_{i_1}, \dots, x_{i_n})$; (ii) $x_l = f^n_k(x_{i_1}, \dots, x_{i_n})$; (iii) $x_l = a_k$. For (i), s satisfies $A^n_k(x_{i_1}, \dots, x_{i_n})$ if and only if $\models_{\mathrm{M}} A^n_k[(g_{i_1})_{\mathcal{F}}, \dots, (g_{i_n})_{\mathcal{F}}]$, which is equivalent to $\{j \mid \models_{\mathrm{M}_j} A^n_k[g_{i_1}(j), \dots, g_{i_n}(j)]\} \in \mathcal{F}$, that is, $\{j \mid \mathrm{s}_j$ satisfies $A^n_k(x_{i_1}, \dots, x_{i_n})$ in $\mathrm{M}_j\} \in \mathcal{F}$.

(ii) and (iii) are handled in similar fashion.

Now let us assume the result holds for all wfs having fewer than m connectives and quantifiers.

Case 1. $\mathcal{A}$ is $\sim \mathcal{B}$. By inductive hypothesis, s satisfies $\mathcal{B}$ in M if and only if $\{j \mid \mathrm{s}_j$ satisfies $\mathcal{B}$ in $\mathrm{M}_j\} \in \mathcal{F}$. Then, s satisfies $\sim \mathcal{B}$ in M if and only if

†A wf $A^n_k(t_1, \dots, t_n)$ can be replaced by $(u_1) \dots (u_n)(u_1 = t_1 \wedge \dots \wedge u_n = t_n \supset A^n_k(u_1, \dots, u_n))$, and a wf $x = f^n_k(t_1, \dots, t_n)$ can be replaced by $(z_1) \dots (z_n)(z_1 = t_1 \wedge \dots \wedge z_n = t_n \supset x = f^n_k(z_1, \dots, z_n))$. In this way, every wf is equivalent to a wf built up from wfs of the forms (i)–(iii) by applying connectives and quantifiers.

$\{j|s_j$ satisfies $\mathscr{B}$ in $M_j\} \notin \mathscr{F}$. But, since $\mathscr{F}$ is an ultrafilter, the last condition is equivalent, by Exercise 2.114, to: $\{j|s_j$ satisfies $\sim\mathscr{B}$ in $M_j\} \in \mathscr{F}$.

Case II. $\mathscr{A}$ is $\mathscr{B} \wedge \mathscr{C}$. By inductive hypothesis, s satisfies $\mathscr{B}$ in M if and only if $\{j|s_j$ satisfies $\mathscr{B}$ in $M_j) \in 9$; s satisfies $\mathscr{C}$ in M if and only if $\{j|s_j$ satisfies $\mathscr{C}$ in $M_j\} \in \mathscr{F}$. Therefore, s satisfies $\mathscr{B} \wedge \mathscr{C}$ if and only if both of the indicated sets belong to $\mathscr{F}$. But this is equivalent to their intersection belonging to $\mathscr{F}$, which, in turn, is equivalent to $\{j|s_j$ satisfies $\mathscr{B} \wedge \mathscr{C}$ in $M_j\} \in \mathscr{F}$.

Case III. $\mathscr{A}$ is $(Ex_i)\mathscr{B}$. Assume s satisfies $(Ex_i)\mathscr{B}$. Then there exists h in $\prod_{j\in J} D_j$ such that s′ satisfies $\mathscr{B}$ in M, where s′ is the same as s except that $h_{\mathscr{F}}$ is the i^{th} component of s′. By inductive hypothesis, s· satisfies $\mathscr{B}$ in M if and only if $\{j|s_j'$ satisfies $\mathscr{B}$ in $M_j\} \in \mathscr{F}$. Hence, $\{j|s_j$ satisfies $(Ex_i)\mathscr{B}$ in $M_j\} \in \mathscr{F}$, since, if s′ satisfies $\mathscr{B}$ in M, then s, satisfies $(Ex_i)\mathscr{B}$ in M_j.

Conversely, assume $W = \{j|s_j$ satisfies $(Ex_i)\mathscr{B}$ in $M_j\} \in \mathscr{F}$. For each j in W, choose some s_j' such that s_j' is the same as s, except in at most the i^{th} component and s_j' satisfies $\mathscr{B}$. Now define h in $\prod_{j\in J} D_j$ as follows: For j in W, let $h(j)$ be the i^{th} component of s_j', and, for $j \notin W$, choose $h(j)$ to be an arbitrary element of D_j. Let s″ be the same as s except that its i^{th} component is $h_{\mathscr{F}}$. Then $W \subseteq \{j|s_j''$ satisfies $\mathscr{B}$ in $M_j\} \in \mathscr{F}$. Hence, by the inductive hypothesis, s″ satisfies $\mathscr{B}$ in M. Therefore, s satisfies $(Ex_i)\mathscr{B}$ in M.

(b) This follows from Part (a) by noting that a sentence $\mathscr{A}$ is true in a model if and only if some sequence satisfies $\mathscr{A}$.

COROLLARY 2.44. *If* M is a model, and $\mathscr{F}$ is an ultrafilter on J, and *if* M* is the ultrapower $M^J/\mathscr{F}$, then M* $\equiv$ M.

PROOF. Let $\mathscr{A}$ be any sentence. Then, by Proposition 2.43(b), $\mathscr{A}$ is true in M★ if and only if $\{j|\mathscr{A}$ is true in M) E $\mathscr{F}$. If $\mathscr{A}$ is true in M, $\{j|\mathscr{A}$ is true in M$\} = J \in \mathscr{F}$. If $\mathscr{A}$ is false in M, $\{j|\mathscr{A}$ is true in M$\} = 0 \notin \mathscr{F}$.

Corollary 2.44 can be strengthened considerably. For each c in the domain D of M, let $c^{\#}$ stand for the constant function such that $c^{\#}(j) = c$ for all j in J. Define the function ψ such that, for each c in D, $\psi(c) = (c^{\#})_{\mathscr{F}} \in D^J/\mathscr{F}$, and denote the range of ψ by $M^{\#}$. $M^{\#}$ obviously contains the interpretations in M★ of the individual constants. Moreover, M′ is closed under the operations $(f_k^n)^{M^*}$; for, $(f_k^n)^{M^*}((c_1{}^{\#})_{\mathscr{F}}, \ldots, (c_n{}^{\#})_{\mathscr{F}})$ is $h_{\mathscr{F}}$, where $h(j) = (f_k^n)^M(c_1, \ldots, c_n)$ for all j in J, and $(f_k^n)^M(c_1, \ldots, c_n)$ is a fixed element b of D. So $h_{\mathscr{F}} = (b^{\#})_{\mathscr{F}} \in M^{\#}$. Thus, $M^{\#}$ is a substructure of M★.

COROLLARY 2.45. ψ is an *isomorphism* of M with M′, and M′ $\leqslant_e$M★

PROOF. (i) By definition of M′, the range of ψ is M′. (ii) ψ is one-one. (For any c, d in D, $(c^{\#})_{\mathscr{F}} = (d^{\#})_{\mathscr{F}}$ if and only if c′ $=_{\mathscr{F}} d^{\#}$, which is equivalent to $\{j|c^{\#}(j) = d^{\#}(j)\} \in \mathscr{F}$, i.e., $\{j|c = d) \in \mathscr{F}$. If $c \neq d$, $\{j|c = d) = 0 \notin \mathscr{F}$, and, therefore, $\psi(c) \neq \psi(d)$. (iii) For any c,, . . . , c_n in D,

$(f_k^n)^{M^*}(\psi(c_1), \ldots, \psi(c_n)) = (f_k^n)^{M^*}((c_1{}^{\#})_{\mathscr{F}}, \ldots, (c_n{}^{\#})_{\mathscr{F}}) = h_{\mathscr{F}}$, where $h(j) = (f_k^n)^M(c_1{}^{\#}(j), \ldots, c_n{}^{\#}(j)) = (f_k^n)^M(c_1, \ldots, c_n)$. Thus $h_{\mathscr{F}} = ((f_k^n)^M(c_1, \ldots, c_n))^{\#}/\mathscr{F} = \psi((f_k^n)^M(c_1, \ldots, c_n))$. (iv) $\models_{M^*} A_k^n[\psi(c_1), \ldots, \psi(c_n)]$ if and only if $\{j| \models_M A_k^n(\psi(c_1)(j), \ldots, \psi(c_n)(j))\} \in \mathscr{F}$, which is equivalent to $\{j| \models_M A_k^n(c_1, \ldots, c_n)\} \in \mathscr{F}$, i.e., $\models_M A_k^n[c_1, \ldots, c_n]$. Thus, ψ is an isomorphism of M with $M^{\#}$.

To see that $M^{\#} \leqslant_e M^\star$, let $\mathscr{A}$ be any wf, and $(c_1{}^{\#})_{\mathscr{F}}, \ldots, (c_n{}^{\#})_{\mathscr{F}} \in M^{\#}$. Then, by Proposition 2.43(a), $\models_{M^*}\mathscr{A}[(c_1{}^{\#})_{\mathscr{F}}, \ldots, (c_n{}^{\#})_{\mathscr{F}}]$ if and only if $\{j| \models_M \mathscr{A}[c_1{}^{\#}(j), \ldots, c_n{}^{\#}(j)]\} \in \mathscr{F}$, which is equivalent to $\{j| \models_M \mathscr{A}[c_1, \ldots, c_n]\} \in \mathscr{F}$, which, in turn, is equivalent to $\models_M \mathscr{A}[c_1, \ldots, c_n]$, that is, to $\models_{M^{\#}} \mathscr{A}[(c_1{}^{\#})_{\mathscr{F}}, \ldots, (c_n{}^{\#})_{\mathscr{F}}]$, since ψ is an isomorphism of M with $M^{\#}$.

EXERCISES

2.119. (The Compactness Theorem again; cf. Exercise 2.34.) If all finite subsets of a set of sentences Γ have a model, prove that Γ has a model.

2.120. (a) A class $\mathscr{W}$ of models of a predicate calculus K is called *elementary* if there is a set Γ of sentences of K such that $\mathscr{W}$ is the class of all models of Γ. Prove that $\mathscr{W}$ is elementary if and only if $\mathscr{W}$ is closed under elementary equivalence and the formation of ultraproducts.

(b) A class $\mathscr{W}$ of models of a predicate calculus K will be called *sentential* if there is a sentence $\mathscr{A}$ of K such that $\mathscr{W}$ is the class of all models of $\mathscr{A}$. Prove that a class $\mathscr{W}$ is sentential if and only if both $\mathscr{W}$ and its complement $\overline{\mathscr{W}}$(all models of K not in $\mathscr{W}$) are closed with respect to elementary equivalence and ultraproducts.

(c) Prove that the theory K of fields of characteristic zero (cf. p. 98) is axiomatizable, but not finitely axiomatizable.

Non-Standard Analysis. From the invention of the calculus until relatively recent times the idea of *infinitesimals* has been used as an intuitively meaningful tool for finding new results in analysis. The fact that there was no rigorous foundation for infinitesimals was a source of embarrassment and led mathematicians to discard them in favor of the rigorous limit ideas of Cauchv and Weierstrass. However, about twenty years ago, Abraham Robinson discovered that it was possible to resurrect infinitesimals in an entirely legitimate and precise way. This can be done by constructing models which are elementarily equivalent to, but not isomorphic to, the ordered field of real numbers. Such models can be produced either by using Proposition 2.34 (p. 95) or as ultrapowers. We shall sketch here the method based on ultrapowers.

Let R be the set of real numbers. Let K be a generalized predicate calculus with equality having the following symbols.

(1) For each real number r, there is an individual constant a,;
(2) For every n-ary operation φ on R, there is a function letter f_φ;
(3) For every n-ary relation Φ on R, there is a predicate letter A,

We can think of R as forming the domain of a model $\mathfrak{R}$ for K; we simply let $(a_r)^{\mathfrak{R}} = r$, $(f_\varphi)^{\mathfrak{R}} = \varphi$, and $(A_\Phi)^{\mathfrak{R}} = \Phi$.

Let $\mathfrak{F}$ be a non-principal ultrafilter on the set ω of natural numbers. We can then form the ultrapower $\mathfrak{R}^\star = \mathfrak{R}^\omega/\mathfrak{F}$. We denote the domain $\mathbf{R}^\omega/\mathfrak{F}$ of C* by R*. By Corollary 2.44, $\mathfrak{R}^\star \equiv \mathfrak{R}$, and, therefore, $\mathfrak{R}^\star$ has all the properties formalizable in K that $\mathfrak{R}$ possesses. Moreover, by Corollary 2.45, C* has an elementary submodel $\mathfrak{R}^\#$, which is an isomorphic image of $\mathfrak{R}$. The domain $\mathbf{R}^\#$ of $\mathfrak{R}^\#$ consists of all elements $(c^\#)_{\mathfrak{F}}$ corresponding to the constant function $c^P(i) = c$ for all i in w. We shall sometimes refer to the members of $\mathbf{R}^\#$ also as real numbers; the elements of R* $- \mathbf{R}^\#$ will be called non-standard reals.

That there exist non-standard reals can be shown by explicitly exhibiting one. Let $\iota(j) = \mathbf{j}$ for all j in ω. Then $\iota_{\mathfrak{F}} \in$ R*. However, (c'), $< \iota_{\mathfrak{F}}$ for all c in R, by virtue of Loś' Theorem and the fact that $\{j|c^\#(j) < \iota(j)\} = \{j|c <j\}$, being the set of all natural numbers greater than a fixed real number, is the complement of a finite set, and is, therefore, in the non-principal ultrafilter $\mathfrak{F}$. $\iota_{\mathfrak{F}}$ is an "infinitely large" non-standard real. (The relation $<$ used in the assertion $(c^\#)_{\mathfrak{F}} < \iota_{\mathfrak{F}}$ is the relation on the ultrapower C* corresponding to the predicate letter $<$ of K. We use the symbol $<$ instead of $(<)^{\mathfrak{R}^\star}$ in order to avoid excessive notation, and we shall often do the same with other relations and functions, such as $u + v$, $u \times v$, and $|u|$.)

Since $\mathfrak{R}^\star$ possesses all the properties of $\mathfrak{R}$ formalizable in K, $\mathfrak{R}^\star$ is an ordered field having the real number field $\mathfrak{R}^\#$ as a proper subfield. ($\mathfrak{R}^\star$ is non-Archimedean: the element $\iota_{\mathfrak{F}}$ defined above is greater than all the natural numbers $(n^\#)_{\mathfrak{F}}$ of $\mathfrak{R}^\star$.) Let $\mathbf{R}_1$, the set of "finite" elements of R*, contain those elements z such that $|z| < u$ for some real number u in R'. ($\mathbf{R}_1$ is easily seen to form a subring of R*.) Let $\mathbf{R}_0$, the set of "infinitesimals" of R*, contain those elements z such that $|z| < u$ for all positive real numbers u in R'. The reciprocal $1/\iota_{\mathfrak{F}}$ is an infinitesimal. (It is not difficult to verify that $\mathbf{R}_0$ is an ideal in the ring $\mathbf{R}_1$. In fact, since x $\in \mathbf{R}_1 - \mathbf{R}_0$ implies that l/x $\in$ R, $- \mathbf{R}_0$, it can be easily proved that $\mathbf{R}_0$ is a maximal ideal in R,.)

EXERCISES

2.121. Prove that the cardinality of R* is $2^{\aleph_0}$.

2.122. Prove that the set $\mathbf{R}_0$ of infinitesimals is closed under the operations of $+$, $-$, and $\times$.

2.123. Prove that, if x $\in \mathbf{R}_1$ and y $\in$ R$_0$, then xy $\in \mathbf{R}_0$.

2.124. Prove that, if x $\in \mathbf{R}_1 - \mathbf{R}_0$, then $1/x \in \mathbf{R}_1 - \mathbf{R}_0$.

Let x $\in \mathbf{R}_1$. Let A $= \{u|u \in \mathbf{R}^\# \wedge u < x\}$ and B $= \{u|u \in \mathbf{R}^\# \wedge u \geqslant$ x$\}$. Then (A, B) is a "cut", and, therefore, determines a unique real number r such that (i) $(x)(x \in A$ 3 x $\leqslant$ r) and (ii) $(x)(x \in B$ 3 x $> r)$.† The difference x $-$ r is an infinitesimal. (Proof: Assume x $-$ r is not an infinitesimal. Then $|x - r| > r_1$ for some positive real number r,. Case 1: x $>$ r. Then x $-$ r $>$ r,. So,

$x > r +$ r, $>$ r. But then $r + r_1 \in A$, contradicting (i). Case 2: x $<$ r. Then , $- x >$ r,, and so, r $>$ r $- r_1 > x$. Thus, r $- r_1 \in B$, contradicting (ii).) The real number r such that x $- r$ is an infinitesimal is called the standardpart of x and is denoted st(x). Note that, if x is itself a real number, then st$(x) =$ x. We shall use the notation x a y to mean that st(x) = st(y). Clearly, x a y if and only if x $-$ y is an infinitesimal. If x a y, we say that x and y are infinitely close.

EXERCISES

2.125. If x $\in$ R$_1$, show that there is a unique real number r such that $x -$ r is an infinitesimal.(It is necessary to check this to ensure that st(x) is well-defined.)

2.126. If x and y are in $\mathbf{R}_1$, prove:

(a) st($x +$ y) = st(x) + st(y);
(b) st(xy) = st(x)st(y);
(c) st$(-x)$ = $-$ st$(x) \wedge$ st($y -$ x) = st(y) $-$ st(x);
(d) x $\geqslant$ 0 $\supset$ st$(x) \geqslant$ 0;
(e) x $\leqslant$ y $\supset$ st$(x) \leqslant$ st(y).

The set ω of natural numbers is a subset of the real numbers. Therefore, in the theory K there is a predicate letter N corresponding to the property x $\in$ w. Hence, in R*, there is a set $\omega^\star$ of elements satisfying the wf N(x). **An** element $f_{\mathfrak{F}}$ of R* satisfies N(x) if and only if $\{j|f(j) \in \omega\} \in 4$. In particular, the elements $n^\#{}_{\mathfrak{F}}$, for n $\in$ w, are the "standard" members of w*, while $\iota_{\mathfrak{F}}$, for example, is a "non-standard" natural number in R*.

Many of the properties of the real number system can be studied from the viewpoint of non-standard analysis. For example, if s is an ordinary sequence of real numbers, and c is a real number, one ordinarily says that lim $s_n =$ c if

$$(\&) \quad (\varepsilon)(\varepsilon > 0 \supset (En)(n \in \omega \wedge (k)(k \in \omega \wedge \text{k} \geqslant \text{n } 3\ |s_n - c| < \varepsilon))).$$

Since s $\in \mathbf{R}^\omega$, s is a relation and, therefore, the theory K contains a predicate letter S(n, x) corresponding to the relation $s_n =$ x. Hence, R* will have a relation of all pairs (n, x) satisfying S(n, x). Since $\mathfrak{R}^\star$ 4 , this relation will be a function which is an extension of the given sequence to the larger domain $\omega^\star$. Then we have the following result.

PROPOSITION 2.46. Let s be a sequence of real numbers and c a real number. Let s* denote the function from w* into R* corresponding to s in $\mathfrak{R}^\star$. Then lim $s_n =$ c *if* and only *if* $s^\star(n) \approx$ c for *all* n in $\omega^\star - \omega$. (The latter condition can be paraphrased by saying *that* $s^\star(n)$ is infinitely close to c when n is infinitely large.)

PROOF. Assume lim $s_n =$ c. Consider any positive real ε. By (&), there is a natural number n_0 such that $(k)(k \in \omega \wedge$ k $\geqslant n_0$ 3 $|s_n - c| < \varepsilon)$ holds in $\mathfrak{R}$. Hence, the corresponding sentence $(k)(k \in$ w* $\wedge$ k $> n_0$ 3 $|s^\star(n) - c| < \varepsilon)$ holds in $\mathfrak{R}^\star$. For any n $\in$ w* $- \omega$, n $> n_0$, and, therefore, $|s^\star(n) - c| < \varepsilon$. Since this holds for all positive reals ε, $s^\star(n) -$ c is an infinitesimal.

† Cf. Mendelson [1973], Chapter 5.

Conversely, assume $s^\star(n) \approx c$ for all $n \in \omega^\star - \omega$. Take any positive real ε. Fix some n_1 in $\omega^\star - \omega$. Then $(k)(k \geqslant n_1 \supset |s^\star(k) - c| < \varepsilon)$. So, the sentence $(En)(n \in \omega \wedge (k)(k \in \omega \wedge k \geqslant n \supset |s_k - c| < \varepsilon)$ is true for $\mathfrak{R}^\star$, and, therefore, also for $\mathfrak{R}$. So, there must be a natural number n_0 such that $(k)(k \in \omega \wedge k \geqslant n_0 \supset |s_k - c| < \varepsilon)$. Since ε was an arbitrary positive real, we have proved lirn $s_n = c$.

EXERCISE

2.127. Using Proposition 2.46, prove the following limit theorems for the real number system.

Let s and u be sequences of real numbers, and c, and c_2 real numbers such that lim $s_n = c_1$ and lim $u_n = c_2$. Then:

(a) lim (s, + u,) $= c_1 + c_2$;

(b) lim $(s_n u_n) = c_1 c_2$;

(c) If $c_2 \neq 0$ and all u, $\neq 0$, lirn $(s_n/u_n) = c,/c_2$.

Let us now consider another important notion of analysis, continuity. Let B be a set of real numbers, let $c \in$ B, and let f be a function defined on B and taking real values. One says that f is continuous at c if

$$(\&\&) \quad (\varepsilon)(\varepsilon > 0 \supset (E\delta)(\delta > 0 \wedge (x)(x \in B \wedge |x - c| < \delta \supset |f(x) - f(c)| < \varepsilon))).$$

PROPOSITION 2.47. *Let f be a real-valued function defined on a set B of real numbers. Let $c \in B$. Let B^* be the subset of R^* corresponding to B, and let f^* be the function corresponding to f.*[†] *Then f is continuous at c if and only if $(x)(x \in B^* \wedge x \approx c \supset f^\star(x) \approx f(c))$.*

EXERCISES

2.128. Prove Proposition 2.47.

2.129. Assume f and g are real-valued functions defined on a set B of real numbers, and assume that f and g are continuous at a point c in B. Using Proposition 2.47, prove:

(a) f + g is continuous at c;

(b) $f \cdot g$ is continuous at c.

2.130. Let f be a real-valued function defined on a set B of real numbers and continuous at a point c in B, and let g be a real-valued function defined on a set A of real numbers containing the image of B under f. Assume that g is continuous at the point $f(c)$. Prove, by Proposition 2.47, that the composition $g \circ f$ is continuous at c.

[†] To be more precise, f is represented in the theory K by a predicate letter A_f, where $A_f(x,y)$ corresponds to the relation $f(x) = y$. Then the corresponding relation $A_f^\star$ in R* determines a function $f^\star$ with domain B*.

2.131. (a) Let $C \subseteq$ R. C is said to be ***closed*** if $(x)((\varepsilon)[\varepsilon > 0 \supset (Ey)(y \in C \wedge |x - y| < \varepsilon)] \supset x \in C)$. Show that C is closed if and only if every real number which is infinitely close to a member of $C^\star$ is in C.

(b) Let $C \subseteq$ R. C is said to be ***open*** if $(x)(x \in C \supset (E\delta)(\delta > 0 \wedge (y)(|y - x| < \delta \supset y \in C)))$. Show that C is open if and only if every non-standard real which is infinitely close to a member of C is a member of $C^\star$.

Many standard theorems of analysis turn out to have much simpler proofs within non-standard analysis. Even stronger results can be obtained by starting with a theory K which has symbols, not only for the elements, operations, and relations on R, but also for sets of subsets of R, sets of sets of subsets of R, etc. In this way, the methods of non-standard analysis can be applied to all areas of modern analysis, sometimes with original and striking results. For further development and applications, cf. A. Robinson [1966], Luxemburg [1969], Bernstein [1973], Stroyan-Luxemburg [1976], and Davis [1977]. A calculus textbook based on non-standard analysis has been written by H. J. Keisler [1976] and has been used in some experimental undergraduate courses.

EXERCISES

2.132. A real-valued function f defined on a closed interval [a, b] = $\{x | a \leqslant x \leqslant b\}$ is said to be ***uniformly continuous*** if

$$(\varepsilon)(\varepsilon > 0 \supset (E\delta)(\delta > 0 \wedge (x)(y)(a \leqslant x \leqslant b \wedge a \leqslant y \leqslant b \wedge |x - y| < \delta \supset |f(x) - f(y)| < \varepsilon))).$$

Prove that f is uniformly continuous if and only if, for all x and y in $[a,b]^\star$, $x \approx y \supset f^\star(x) \approx f^\star(y)$.

2.133. Prove, via non-standard methods, that any function continuous on [a, b] is uniformly continuous on [a, b].

2.134. (Bolzano-Weierstrass Theorem) A real number c is said to be a ***limit point*** of a set A of reals if $(\varepsilon)(\varepsilon > 0 \supset (Eu)(u \in A \wedge |c - u| < \varepsilon))$. Let s be a bounded sequence of reals, that is, there is a number b such that $|s_n| <$ b for all n in ω. Prove that the set of terms of s (i.e., the range of the function s $\in$ R^w) has a limit point.

CHAPTER 3

FORMAL NUMBER THEORY

1. An Axiom System

Together with geometry, the theory of numbers is the most immediately intuitive of all branches of mathematics. It is not surprising then that attempts to formalize mathematics and to establish a rigorous foundation for mathematics should begin with number theory. The first semi-axiomatic presentation of this subject was given by Dedekind in 1879 and has come to be known as **Peano's Postulates.**† It can be formulated as follows:

(P1) 0 is a natural number.

(P2) If x is a natural number, there is another natural number denoted by x' (and called the successor of x).

(P3) $0 \neq x'$ for any natural number **x.**

(P4) If $x' = y'$, then $x = y$.

(P5) If Q is a property which may or may not hold of natural numbers, and if (I) 0 has the property Q, and **(II)** whenever a natural number **x** has the property Q, then x' has the property Q, then all natural numbers have the property Q (Principle of Induction).

These axioms, together with a certain amount of set theory, can be used to develop not only number theory but also the theory of rational, real, and complex numbers (cf. Mendelson [1973]). However, the axioms involve certain intuitive notions, such as "property", which prevent this system from being a rigorous formalization. We therefore shall build a first-order theory S that is based upon Peano's Postulates and seems to be adequate for the proofs of all the basic results of elementary number theory.

The first-order theory S has a single predicate letter A_1^2 (as usual, we write $t = s$ for $A_1^2(t,$ s)); it has one individual constant a, (written, as usual, 0); it has three function letters f_1^1, f_1^2, f_2^2. We shall write t' instead of $f_1^1(t)$; $t + s$ instead of $f_1^2(t,$ s); and $t \,.\, s$ instead of $f_2^2(t,$ s). The proper axioms of S are:

(S1) $x_1 = x_2 \supset (x_1 = x_3 \supset x_2 = x_3)$

(S2) x, = $x_2 \supset$ x; = x;

†For historical information, see Wang [1957].

(S3) $0 \neq (x_1)'$

(S4) $(x,)' = (x_2)' \supset x_1 = x_2$

(S5) $x, + 0 = x,$

(S6) $x, + x_2' = (x, + x_2)'$

(S7) $x_1 \cdot 0 = 0$

(S8) $x_1 \cdot (x_2') = (x_1 \cdot x_2) + x_1$

(S9) For any wf $\mathscr{A}(x)$ of S, $\mathscr{A}(0) \supset ((x)(\mathscr{A}(x)\ 3\ \mathscr{A}(x'))\ 3\ (x)\mathscr{A}(x))$

Notice that Axioms (S1)–(S8) are particular wfs while (S9) is an axiom schema providing an infinite number of axioms. However, (S9), which we shall call the Principle of Mathematical Induction, cannot fully correspond to Peano's Postulate (P5), since the latter refers intuitively to the $2^{\aleph_0}$ properties of natural numbers, while (S9) can only take care of the denumerable number of properties defined by wfs of S.

Axioms (S3) and (S4) correspond to the Peano Postulates (P3) and (P4), respectively. Peano's axioms (P1) and (P2) are taken care of by the presence of 0 as an individual constant and f_1^1 as a function letter. Our axioms (S1)–(S2) furnish some needed properties of equality; they would have been assumed as intuitively obvious by Dedekind and Peano. Axioms (S5)–(S8) are the recursion equations for addition and multiplication. Dedekind and Peano didn't have to assume them because they allowed the use of intuitive set theory, from which the existence of operations + and · satisfying (S5)–(S8) is deducible (cf. Mendelson [1973], Theorems 3.1 and 5.1).

From (S9), by MP, we can obtain the Induction Rule: from $\mathscr{A}(0)$ and $(x)(\mathscr{A}(x) \supset \mathscr{A}(x'))$, we can derive $(x)\mathscr{A}(x)$.

It will be our immediate aim to establish the usual rules of equality, i.e., we shall show that the properties (6) and (7) of equality (cf. p. 79) are derivable in S, and hence that S is a first-order theory with equality.

First, for convenience and brevity in carrying out proofs, we cite some immediate, trivial consequences of the axioms.

LEMMA 3.1. For any terms t, s, r of S, the following wfs are theorems.

(SI') $t = r \supset (t = s \supset r = s)$

(S2′) $t = r \supset t' = r'$

(S3′) $0 \neq t'$

(S4′) $t' = r' \supset t = r$

(S5′) $t + 0 = t$

(S6′) $t + r' = (t + r)'$

(S7′) $t \cdot 0 = 0$

(S8′) $t . r' = (t . r) + t$

PROOF. (S1′)–(S8′) follow from (S1)–(S8) respectively by first forming the closure by means of Gen, and then applying rule A4 with the appropriate terms t, r, s.

PROPOSITION 3.2. For *any* terms t, r, s the following wfs are theorems of S.

(a) $t = t$

(b) $t = r \supset r = t$

(c) $t = r \supset (r = s \supset t = s)$

(d) $r = t \supset (s = t \supset r = s)$

(e) $t = r \supset t + s = r + s$

(f) $t = 0 + t$

(g) $t' + r = (t + r)'$

(h) $t + r = r + t$

(i) $t = r \supset s + t = s + r$

(j) $(t + r) + s = t + (r + s)$

(k) $t = r \supset t \cdot s = r \cdot s$

(l) $0 \cdot t = 0$

(m) $t' \cdot r = t \cdot r + r$

(n) $t \cdot r = r \cdot t$

(o) $t = r \supset s \cdot t = s \cdot r$

PROOF.

(a)	1.	$t + 0 = t$	(S5′)
	2.	$(t + 0 = t) \supset (t + 0 = t \supset t = t)$	(S1′)
	3.	$t + 0 = t \supset t = t$	1, 2, MP
	4.	$t = t$	1, 3, MP
(b)	1.	$t = r \supset (t = t \supset r = t)$	(S1′)
	2.	$t = t \supset (t = r \supset r = t)$	1, Tautology
	3.	$t = r \supset r = t$	2, Part (a), MP
(c)	1.	$r = t \supset (r = s \supset t = s)$	(S1′)
	2.	$t = r \supset r = t$	Part (b)
	3.	$t = r \supset (r = s \supset t = s)$	1, 2, Tautology
(d)	1.	$r = t \supset (t = s \supset r = s)$	Part (c)
	2.	$t = s \supset (r = t \supset r = s)$	1, Tautology
	3.	$s = t \supset t = s$	Part (b)
	4.	$s = t \supset (r = t \supset r = s)$	2, 3, Tautology
	5.	$r = t \supset (s = t \supset r = s)$	4, Tautology

(e) Apply the Induction Rule to $\mathscr{A}(z)$: $x = y \supset (x + z = y + z)$.

(i)	1.	$x + 0 = x$	(S5′)
	2.	$y + 0 = y$	(S5′)
	3.	$x = y$	Hyp
	4.	$x + 0 = y$	1, 3, Part (c)
	5.	$x + 0 = y + 0$	2, 4, Part (d)
	6.	$x = y \supset x + 0 = y + 0$	1–5, Deduction Theorem

i.e., $\vdash \mathscr{A}(0)$.

(ii)	1.	$x = y \supset x + z = y + z$	Hyp
	2.	$x = y$	Hyp
	3.	$x + z' = (x + z)'$	(S6′)
	4.	$y + z' = (y + z)'$	(S6′)
	5.	$x + z = y + z$	1, 2, MP
	6.	$(x + z)' = (y + z)'$	5, (S2′)
	7.	$x + z' = (y + z)'$	3, 6, Part (c)
	8.	$x + z' = y + z'$	4, 7, Part (d)
	9.	$(x = y \supset (x + z = y + z)) \supset (x = y \supset (x + z' = y + z'))$	1–8, Deduction Theorem

i.e., $\vdash \mathscr{A}(z) \supset \mathscr{A}(z')$.

Hence, $\vdash (z)\mathscr{A}(z)$ by the Induction Rule, from (i) and (ii). Therefore, by Gen and Rule A4, $\vdash t = r \supset t + s = r + s$.

(f) Let $\mathscr{A}(x)$ be $x = 0 + x$.

(i) $0 = 0 + 0$, by (S53 and Part (b); i.e., $\vdash \mathscr{A}(0)$.

(ii)	1.	$x = 0 + x$	Hyp
	2.	$(0 + x') = (0 + x)'$	(S6′)
	3.	$x' = (0 + x)'$	1, (S2′)
	4.	$x' = 0 + x'$	2, 3, Part (d)
	5.	$x = 0 + x \supset x' = 0 + x'$	1–4, Deduction Theorem

i.e., $\vdash \mathscr{A}(x) \supset \mathscr{A}(x')$.

By (i)–(ii) and the Induction Rule, $\vdash (x)(x = 0 + x)$. So, by Rule A4, $\vdash t = 0 + t$.

(g) Let $\mathscr{A}(y)$ be $x' + y = (x + y)'$.

(i)	1.	$x' + 0 = x'$	(S5′)
	2.	$x + 0 = x$	(S5′)
	3.	$(x + 0)' = x'$	2, (S2′)
	4.	$x' + 0 = (x + 0)'$	1, 3, Part (d)

i.e., t $\mathscr{A}(0)$.

(ii)	1.	$x' + y = (x + y)'$	Hyp
	2.	$x' + y' = (x' + y)'$	(S6′)
	3.	$(x' + y)' = (x + y)''$	1, (S2′)
	4.	$x' + y' = (x + y)''$	2, 3, Part (c)
	5.	$(x + y') = (x + y)'$	(S6′)
	6.	$(x + y')' = (x + y)''$	5, (S2′)
	7.	$x' + y' = (x + y')'$	4, 6, Part (d)
	8.	$x' + y = (x + y)' \supset x' + y' = (x + y')'$	1–7, Deduction Theorem

i.e., $\vdash \mathscr{A}(y) \supset \mathscr{A}(y')$.

So, by (i), (ii), and the Induction Rule, $\vdash (y)(x' + y = (x + y)')$, and, then by Gen and Rule A4, $\vdash t' + r = (t + r)'$.

(h) Let $\mathscr{A}(y)$ be $x + y = y + x$.

(i)	1.	$x + 0 = x$	(S5′)
	2.	$x = 0 + x$	Part (f)
	3.	$x + 0 = 0 + x$	1, 2, Part (c)

i.e., $\vdash \mathscr{A}(0)$.

(ii)	1.	$x + y = y + x$	Hyp
	2.	$x + y' = (x + y)'$	(S6′)
	3.	$y' + x = (y + x)'$	Part (g)
	4.	$(x + y)' = (y + x)'$	1, (S2′)
	5.	$x + y' = (y + x)'$	2, 4, Part (c)
	6.	$x + y' = y' + x$	3, 5, Part (d)
	7.	$x + y = y + x \supset x + y' = y' + x$	1–6, Deduction Theorem

i.e., $\vdash \mathscr{A}(y) \supset \mathscr{A}(y')$.

So, by (i), (ii), and the Induction Rule, $\vdash (y)(x + y = y + x)$, and, then by Gen and Rule A4, $\vdash t + r = r + t$.

(i)	1.	$t = r \supset t + s = r + s$	Part (e)
	2.	$t + s = s + t$	Part (h)
	3.	$r + s = s + r$	Part (h)
	4.	$t = r$	Hyp
	5.	$t + s = r + s$	1, 4, MP
	6.	$s + t = r + s$	2, 5, (S1′)
	7.	$s + t = s + r$	3, 6, Part (c)
	8.	$t = r \supset s + t = s + r$	1–7, Deduction Theorem

(j) Let $\mathscr{A}(z)$ be $(x + y) + z = x + (y + z)$.

(i)	1.	$(x + y) + 0 = x + y$	(S5′)
	2.	$y + 0 = y$	(S5′)
	3.	$x + (y + 0) = x + y$	2, Part (i)
	4.	$(x + y) + 0 = x + (y + 0)$	1, 3, Part (d)

i.e., $\vdash \mathscr{A}(0)$.

(ii)	1.	$(x + y) + z = x + (y + z)$	Hyp
	2.	$(x + y) + z' = ((x + y) + z)'$	(S6′)
	3.	$((x + y) + z)' = (x + (y + z))'$	1, (S2′)
	4.	$(x + y) + z' = (x + (y + z))'$	2, 3, Part (c)
	5.	$y + z' = (y + z)'$	(S6′)
	6.	$x + (y + z') = x + (y + z)'$	5, Part (i)
	7.	$x + (y + z)' = (x + (y + z))'$	(S6′)
	8.	$x + (y + z') = (x + (y + z))'$	6, 7, Part (d)
	9.	$(x + y) + z' = x + (y + z')$	4, 8, Part (d)
	10.	$(x + y) + z = x + (y + z) \supset (x + y) + z' = x + (y + z')$	1–9, Deduction Theorem

i.e., $\vdash \mathscr{A}(z) \supset \mathscr{A}(z')$.

By (i), (ii), and the Induction Rule, $\vdash (z)((x + y) + z = x + (y + z))$, and then, by Gen and Rule A4, $\vdash (t + r) + s = t + (r + s)$.

Parts (k)–(o) are left as exercises for the reader.

Corollary 3.3. S is a *theory with equality*, *i.e.*, we have (6): t x, = x,, and (7): $\vdash x = y \supset \mathcal{A}(x, x) \supset \mathcal{A}(x, y)$, where $\mathcal{A}(x, y)$ comes from $\mathcal{A}(x, x)$ by replacing one or more occurrences of x by y, with the proviso that y is free *for* those occurrences of x (cf. p. 79).

PROOF. By Proposition 2.26, this reduces to Proposition 3.2 (a)–(e), (i), (k), (o), and (S2′).

Notice that the interpretation in which

(a) the set of non-negative integers is the domain,
(b) the integer 0 is the interpretation of the symbol 0,
(c) the successor operation (addition of 1) is the interpretation of the ′ function (i.e., of f_1^1),
(d) ordinary addition and multiplication are the interpretations of + and ·,
(e) the interpretation of the predicate letter = is the identity relation,

is a normal model for S. This model is called the standard model for S. Any normal model for S which is not isomorphic to the standard model will be called a non-standard model for S.

If we recognize the standard interpretation to be a model for S, then of course, S is consistent. However, semantic methods, involving as they do a certain amount of set-theoretic reasoning, are regarded by some as too precarious to serve as a basis for consistency proofs; likewise, we have not proved in a rigorous way that the axioms of S are true under the standard interpretation, but have taken it as intuitively obvious. For these and other reasons, when the consistency of S enters into the argument of a proof, it is common practice to take the statement of the consistency of S as an explicit, unproved assumption.

Some important additional properties of addition and multiplication are covered by the following result.

Proposition 3.4. For any term t, r, s the following wfs are theorem of S.

(a)	$t . (r + s) = (t \cdot r) + (t . s)$	(Distributivity)
(b)	$(r + s) \cdot t = (r \cdot t) + (s \cdot t)$	(Distributivity)
(c)	$(t \cdot r) \cdot s = t \cdot (r \cdot s)$	(Associativity of .)
(a)	$t + s = r + s \supset t = r$	(Cancellation Law for +)

PROOF.

(a) Prove $\vdash x . (y + z) = (x \cdot y) + (x . z)$ by induction on z.
(b) From (a) by Proposition 3.2(n).
(c) Prove $\vdash (x . y) . z = x \cdot (y . z)$ by induction on z.
(d) Prove $\vdash x + z = y + z \supset x = y$ by induction on z. This requires, for the first time, use of (S4′).

The terms 0, 0′, 0 , 0‴, . . . we shall call numerals, and denote by 0, I, 2, 3, . . . in the usual way. In general, if n is a non-negative integer, we shall let $\bar{n}$ stand for the corresponding numeral 0 ′ . . . ′, i.e., for 0 followed by strokes. We can define the numerals recursively by stating that 0 is a numeral and, if u is a numeral, then u′ is also a numeral.

Proposition 3.5

(a) $\vdash t + \bar{1} = t'$
(b) $\vdash t \cdot \bar{1} = t$
(c) $\vdash t \cdot \bar{2} = t + t$ (etc., for 3, 4, . . .)
(d) $\vdash t + s = 0 \supset t = 0 \wedge s = 0$
(e) $\vdash t \neq 0 \supset (s \cdot t = 0 \supset s = 0)$
(f) $\vdash t + s = \bar{1} \supset (t = 0 \wedge s = \bar{1}) \vee (t = \bar{1} \wedge s = 0)$
(g) $\vdash t \cdot s = \bar{1} \supset (t = \bar{1} \wedge s = \bar{1})$
(h) $\vdash t \neq 0 \supset (Ey)(t = y')$
(i) $\vdash s \neq 0 \supset (t \cdot s = r \cdot s \supset t = r)$
(j) $\vdash t \neq 0 \supset (t \neq \bar{1} \supset (Ey)(t = y''))$

PROOF.

(a)	1.	$t + 0' = (t + 0)'$	(S6′)
	2.	$t + 0 = t$	(S5′)
	3.	$(t + 0)' = t'$	2, (S2′)
	4.	$t + 0' = t'$	1, 3, Proposition 3.2(c)
	5.	$t + i = t'$	4, Abbreviation
(b)	1.	$t \cdot 0' = t \cdot 0 + t$	(S8′)
	2.	$t \cdot 0 = 0$	(S7′)
	3.	$(t \cdot 0) + t = 0 + t$	2, Proposition 3.2(e)
	4.	$t \cdot 0' = 0 + t$	1, 3, Proposition 3.2(c)
	5.	$0 + t = t$	Proposition 3.2(f), (b)
	6.	$t \cdot 0' = t$	4, 5, Proposition 3.2(c)
	7.	$t \cdot \bar{1} = t$	6, Abbreviation
(c)	1.	$t \cdot \bar{1}' = (t \cdot \bar{1}) + t$	(S8′)
	2.	$t \cdot \bar{1} = t$	Part (b)
	3.	$(t \cdot \bar{1}) + t = t + t$	2, Proposition 3.2(e)
	4.	$t \cdot \bar{1}' = t + t$	1, 3, Proposition 3.2(c)
	5.	$t \cdot \bar{2} = t + t$	4, Abbreviation

(d) Let $\mathcal{A}(y)$ be $x + y = 0 \supset x = 0 \wedge y = 0$. It is easy to prove that $\vdash \mathcal{A}(0)$. Also, since $\vdash (x + y)' \neq 0$ by (S3′), then, by (S6′), it follows that $\vdash x + y' \neq 0$. Hence, $\vdash \mathcal{A}(y')$ by the tautology $\sim A \supset (A \supset B)$. So, $\vdash \mathcal{A}(y) \supset \mathcal{A}(y')$ by the tautology $A \supset (B \supset A)$. Thus, by the Induction Rule, $\vdash (y)\mathcal{A}(y)$, and then, by Gen and Rule A4, we obtain Part (d).
(e) The proof is similar to that for (d) and is left as an exercise.
(f) By induction on y in $x + y = \bar{1} \supset ((x = 0 \wedge y = \bar{1}) \vee (x = \bar{1} \wedge y = 0))$.
(g) By induction on y in $x \cdot y = \bar{1} \supset (x = \bar{1} \wedge y = \bar{1})$.
(h) Perform induction on x in $x \neq 0 \supset (Ew)(x = w')$.

(i) Let $\mathscr{Q}(y)$ be $(x)(z \# 0 \supset (x \cdot z = y \,.\, z \supset x = y))$.

(i) 1.	$z \neq 0$	Hyp
2.	$x \cdot z = 0 \cdot z$	Hyp
3.	$0 \cdot z = 0$	Proposition 3.2(l)
4.	$x \cdot z = 0$	2, 3, Proposition 3.2(c)
5.	$x = 0$	1, 4, Part (e) above
6.	$z \neq 0 \supset (x \cdot z = 0 \cdot z \supset x = 0)$	1–5, Deduction Theorem
7.	$(x)(z \neq 0 \supset (x \,.\, z = 0 \cdot z \; 3 \; x = 0))$ i.e., $\vdash \mathscr{Q}(0)$.	6, Gen

(ii) 1.	$(x)(z \neq 0 \supset (x \cdot z = y \,.\, z \supset x = y))$	Hyp $(\mathscr{Q}(y))$
2.	$z \neq 0$	Hyp
3.	$x \cdot z = y' \cdot z$	Hyp
4.	$y' \neq 0$	(S3′), Proposition 3.2(b)
5.	$y' \cdot z \neq 0$	2, 4, Part (e) and a tautology
6.	$x \cdot z \neq 0$	3, 5, (S1′) and tautologies
7.	$x \neq 0$	6, (S7′), Proposition 3.2(o), (n), (S1′), and tautologies
8.	$(Ew)(x = w')$	7, (h) above
9.	$x = b'$	8, Rule C
10.	$b' \cdot z = y' \cdot z$	3, 9, Equality law (7)
11.	$b \cdot z + z = y \cdot z + z$	10, Proposition 3.2(m), (d)
12.	$b \cdot z = y \cdot z$	11, Proposition 3.4(d)
13.	$z \neq 0 \supset ((b \cdot z = y \cdot z) \supset (b = y))$	1, Rule A4
14.	$b \cdot z = y \cdot z \supset b = y$	2, 13, MP
13.	$b = y$	12, 14, MP
16.	$b' = y'$	15, (S2′)
17.	$x = y'$	9, 16, Proposition 3.2(c)
18.	$\mathscr{Q}(y), z \neq 0, x \cdot z = y' \,.\, z \vdash x = y'$	1–17, Proposition 2.23
19.	$\mathscr{Q}(y) \vdash z \neq 0 \supset (x \cdot z = y' \cdot z \supset x = y')$	19, Deduction Theorem twice
20.	$\mathscr{Q}(y) \vdash (x)(z \neq 0 \supset (x \cdot z = y' \,.\, z \supset x = y'))$	19, Gen
21.	$\vdash \mathscr{Q}(y) \supset \mathscr{Q}(y')$	20, Deduction Theorem

Hence, by (i) and (ii) and the Induction Rule, we obtain $\vdash (y)\mathscr{Q}(y)$, and then, by Gen and Rule A4, we have the desired result.

(j) Exercise for the reader.

PROPOSITION 3.6. (a) Let m, n be any natural numbers. (i) If m # n, then $\vdash$ iii # ii. (ii) $\vdash \overline{m + n} = \overline{m} + a$ and $\vdash \overline{m \cdot n} = \overline{m} \,.\, A$. (b) Any model for S is *infinite*. (c) For any cardinal number $\aleph_\beta$, S has a normal model of *cardinality* $\aleph_\beta$.

PROOF.

(a) Assume $m \neq n$. Now, either $m < n$ or $n < m$; say, $m < n$.

1.	$\overline{m} = \overline{n}$	Hyp
2.	$0\underbrace{{}^{\prime\cdots\prime}}_{m \text{ times}} = 0\underbrace{{}^{\prime\cdots\prime}}_{n \text{ times}}$	1 is an abbreviation of 2

3. Apply (S4′) m times in a row. Then $0 = 0\underbrace{{}^{\prime\cdots\prime}}_{(n-m)\text{ times}}$. Let t be $\overline{(n - m - 1)}$. Since $n > m$, $n - m - 1 \geqslant 0$. Thus, $0 = t'$.

4.	$0 \neq t'$	(S3′)
5.	$0 = t' \wedge 0 \neq t'$	3, 4, Tautology
6.	$\vdash \overline{m} = \overline{n} \supset (0 = t' \wedge 0 \neq t')$	1–5, Deduction Theorem
7.	$\vdash \overline{m} \neq \overline{n}$	6, Tautology

A similar proof holds in the case when $n < m$. (A more rigorous proof can be given by induction in the metalanguage with respect to n.) (ii) We use induction in the metalanguage. First, $\overline{m + 0}$ is iii. Hence, $\vdash \overline{m + 0} =$ iii $+ \overline{0}$ by (S5′). Now assume $\vdash \overline{m + n} = \overline{m} +$ ii. Therefore, $\vdash (\overline{m + n})' = \overline{m} +$ (ii)′ by (S2′) and (S6′). But $\overline{m + (n + 1)}$ is $(\overline{m + n})'$ and $\overline{n + 1}$ is $(\overline{n})'$. Hence, $\vdash \overline{m + (n + 1)} =$ iii $+ \overline{n + 1}$. The proof that $\vdash \overline{m \cdot n} = \overline{m} \cdot \overline{n}$ is left as an exercise.

(b) By Part (a), (i), in a model for S, the objects corresponding to the numerals must be distinct. But there are denumerably many numerals.

(c) This follows from Corollary 2.35(3) and the fact that the standard model is an infinite normal model.

An order relation can be introduced by definition in S.

DEFINITIONS

$t < s$ for $(Ew)(w \neq 0$ A $w + t = s)$
$t \leqslant s$ for $t < s \vee t = s$
$t > s$ for $s < t$
$t \geqslant s$ for $s \leqslant t$
$t \not< s$ for $\sim(t < s)$, etc.

In the first definition, to be precise, we can choose w to be the first variable not in t or s.

PROPOSITION 3.7. For any terms t, r, s the following wfs are theorems.

(a) $t \not< t$
(b) $t < s \supset (s < r \supset t < r)$
(c) $t < s \supset s \not< t$
(d) $t < s \equiv t + r < s + r$
(e) $t \leqslant t$
(f) $t \leqslant s \supset (s \leqslant r \supset t \leqslant r)$
(g) $t \leqslant s \equiv (t + r \leqslant s + r)$
(h) $t \leqslant s \supset (s < r \supset t < r)$
(i) $0 \leqslant t$
(j) $0 < t'$
(k) $t < r \equiv t' \leqslant r$
(l) $t \leqslant r \equiv t < r'$
(m) $t < t'$
(n) $(0 < T), (\overline{1} < \overline{2}), (\overline{2} < \overline{3}), \ldots$
(o) $t \neq r \supset (t < r \vee r < t)$
(o′) $t = r \vee t < r \vee r < t$
(p) $t \leqslant r \vee r \leqslant t$
(q) $t + r \geqslant t$
(r) $r \neq 0 \supset t + r > t$
(s) $r \neq 0 \supset t \cdot r \geqslant t$
(t) $r \neq 0 \equiv r > 0$
(u) $r > 0 \supset (t > 0 \supset r \cdot t > 0)$

(v) $r \neq 0 \supset (t > \bar{1} \supset t \cdot r > r)$

(w) $r \neq 0 \supset (t < s \equiv t \cdot r < s \cdot r)$

(x) $r \neq 0 \supset (t \leqslant s \equiv t \cdot r \leqslant s \cdot r)$

(y) $t \nless 0$

(z) $t \leqslant r \wedge r \leqslant t \supset t = r$

PROOF.

(a) By Proposition 3.4(d).

(b)	1.	$t < s$	Hyp
	2.	$s < r$	Hyp
	3.	$(Ew)(w \neq 0 \wedge w + t = s)$	1, Definition
	4.	$(Ev)(v \neq 0$ A $v + s = r)$	2, Definition
	5.	$b \neq 0 \wedge b + t = s$	3, Rule C
	6.	$c \neq 0 \wedge c + s = r$	4, Rule C
	7.	$b + t = s$	5, Tautology
	8.	$c + s = r$	6, Tautology
	9.	$c + (b + t) = r$	7, 8, Proposition 3.2(i), (c)
	10.	$(c + b) + t = r$	9, Proposition 3.2(j), (c)
	11.	$b \neq 0$	5, Tautology
	12.	$c + b \neq 0$	11, Proposition 3.5(d)
	13.	$c + b \neq 0 \wedge (c + b) + t = r$	10, 12, Tautology
	14.	$(Eu)(u \neq 0 \wedge u + t = r)$	13, Rule E4
	15.	$t < r$	14, Definition
	16.	$\vdash t < s \supset (s < r \supset t < r)$	1–15, Deduction Theorem, Proposition 2.23

Parts (c)–(z) are left as exercises. These theorems are not arranged in any special order, though, generally, they can be proved more or less directly from preceding ones in the list.

PROPOSITION 3.8. (a) For any natural number k,

$$\vdash x = 0 \vee \dots \vee x = \bar{k} \equiv x \leqslant \bar{k}.$$

(a') For any natural number k and any wf $\mathcal{A}$,

$$\vdash \mathcal{A}(0) \wedge \mathcal{A}(\bar{1}) \wedge \dots \wedge \mathcal{A}(\bar{k}) \equiv (x)(x \leqslant \bar{k} \supset \mathcal{A}(x)).$$

(b) For any natural number $k > 0$,

$$\vdash x = 0 \vee \dots \vee x = (\overline{k-1}) \equiv x < \bar{k}.$$

(b') For any natural number $k > 0$, and any wf $\mathcal{A}$,

$$\vdash \mathcal{A}(0) \wedge \mathcal{A}(\bar{1}) \wedge \dots \wedge \mathcal{A}(\overline{k-1}) \equiv (x)(x < \bar{k} \supset \mathcal{A}(x))$$

(c) $\vdash ((x)(x < y \supset \mathcal{A}(x)) \wedge (x)(x \geqslant y \supset \mathcal{B}(x))) \supset (x)(\mathcal{A}(x) \vee \mathcal{B}(x))$.

PROOF. (a) We prove $\vdash x = 0 \vee \dots \vee x = \bar{k} \equiv x \leqslant \bar{k}$ by induction in the metalanguage on k. The case for $k = 0$, $\vdash x = 0 \equiv x \leqslant 0$ is obvious from the definitions and Proposition 3.7. Assume $\vdash x = 0 \vee \dots \vee x = \bar{k} \equiv x \leqslant \bar{k}$. Now, assume $x = 0 \vee \dots \vee x = \bar{k} \vee x = \overline{k+1}$; but, $x = \overline{k+1} \supset x \leqslant \overline{k+1}$; also, $x = 0 \vee \dots \vee x = \bar{k} \supset x \leqslant \bar{k}$, and $x \leqslant \bar{k} \supset x \leqslant \overline{k+1}$. Hence, $x = 0 \vee \dots \vee x = \overline{k+1} \supset x \leqslant \overline{k+1}$. On the other hand, assume $x \leqslant \overline{k+1}$. Then $x = \overline{k+1} \vee x < \overline{k+1}$. If $x = \overline{k+1}$, then $x = 0 \vee \dots \vee x = \overline{k+1}$. If $x < \overline{k+1}$, then, since $\overline{k+1}$ is $(\bar{k})'$, we have $x \leqslant k$, by Proposition 3.7(l). By inductive hypothesis, $x = 0 \vee \dots \vee x = \bar{k}$, and so, $x = 0 \vee \dots \vee x = \overline{k+1}$. (This proof has been given in an informal manner that we shall generally use from now on. In particular, the Deduction Theorem, the elirninability of Rule C, and the Replacement Theorem (Corollary 2.21) will be tacitly applied, and tautologies used will not be explicitly mentioned.)

Parts (a'), (b), (b') follow easily from (a). Part (c) follows almost immediately from Proposition 3.7(o), using obvious tautologies.

There are several stronger forms of the induction principle which we can prove at this point.

PROPOSITION 3.9

(a) (Complete Induction)

$$\vdash (x)((z)(z < x \supset \mathcal{A}(z)) \supset \mathcal{A}(x)) \supset (x)\mathcal{A}(x)$$

(Consider a property P such that, *for* any x, *if* P holds *for* all natural numbers less than x, then P *holds for* x also. Then P holds *for all* natural numbers.)

(b) (Least-number Principle)

$$\vdash \mathcal{A}(x) \supset (Ey)(\mathcal{A}(y) \wedge (z)(z < y \supset \sim \mathcal{A}(z)))$$

(*If* a property P *holds for* some natural number, then there is a least number satisfying P.)

PROOF.

(a) Let $\mathcal{B}(x)$ be $(z)(z \leqslant x \supset \mathcal{A}(z))$.

(i)	1.	$(x)((z)(z < x \supset \mathcal{A}(z)) \supset \mathcal{A}(x))$	Hyp
	2.	$(z)(z < 0 \supset \mathcal{A}(z)) \supset \mathcal{A}(0)$	1, Rule A4
	3.	$z \nless 50$	Proposition 3.7(y)
	4.	$(z)(z < 0 \supset \mathcal{A}(z))$	3, Tautology, Gen
	5.	$\mathcal{A}(0)$	2, 4, Gen
	6.	$(z)(z \leqslant 0\ 3\ \mathcal{A}(z))$ i.e., $\mathcal{B}(0)$	5, Proposition 3.8(a′)
	7.	$(x)((z)(z < x \supset \mathcal{A}(z)) \supset \mathcal{A}(x)) \vdash \mathcal{B}(0)$	1–6
(ii)	1.	$(x)((z)(z < x\ 3\ \mathcal{A}(z))\ 3\ \mathcal{A}(x))$	Hyp
	2.	$\mathcal{B}(x)$, i.e., $(z)(z \leqslant x \supset \mathcal{A}(z))$	Hyp
	3.	$(z)(z < x'\ 3\ \mathcal{A}(z))$	2, Proposition 3.7(l)
	4.	$(z)(z < x'\ 3\ \mathcal{A}(z))\ 3\ \mathcal{A}(x')$	I, Rule A4
	5.	$\mathcal{A}(x')$	3, 4, MP
	6.	$z \leqslant x' \supset z < x' \vee z = x'$	Definition, Tautology
	7.	$z < x' \supset \mathcal{A}(z)$	3, Rule A4

8. $z = x' \supset \mathscr{A}(z)$ — 5, Equality Axiom (7)

9. $(z)(z \leqslant x' \supset \mathscr{A}(z))$ — 6, 7, 8, Tautology, Gen
   i.e., $\mathscr{B}(x')$

10. $(x)((z)(z < x \supset \mathscr{A}(z)) \supset \mathscr{A}(x)) \vdash (x)(\mathscr{B}(x) \supset \mathscr{B}(x'))$
    1–9, Deduction Theorem, Gen

From (i), (ii), and the Induction Rule, we obtain $\mathscr{C} \vdash (x)\mathscr{B}(x)$, i.e., $\mathscr{C} \vdash (x)(z)(z \leqslant x \supset \mathscr{A}(z))$, where $\mathscr{C}$ is $(x)((z)(z < x \supset \mathscr{A}(z)) \supset \mathscr{A}(x))$. Hence, by Rule A4 twice, $\mathscr{C} \vdash x \leqslant x \supset \mathscr{A}(x)$; but, $\vdash x \leqslant x$. So, $\mathscr{C} \vdash \mathscr{A}(x)$, and, by Gen and the Deduction Theorem, $\vdash \mathscr{C} \supset (x)\mathscr{A}(x)$.

(b) 1. $\sim(Ey)(\mathscr{A}(y) \wedge (z)(z < y \supset \sim \mathscr{A}(z)))$ — Hyp

2. Y $\sim(\mathscr{A}(y)$ A $(z)(z <$ Y $\supset \sim \mathscr{A}(z)))$ — 1, Tautology

3. $(y)((z)(z <$ Y $\supset \sim \mathscr{A}(z)) \supset \sim \mathscr{A}(y))$ — 2, Tautology

4. $(y) \rightarrow \mathscr{A}(y)$ — 3, Part (a) with $\sim \mathscr{A}$ instead of $\mathscr{A}$

5. $\sim \mathscr{A}(x)$ — 4, Rule A4

6. $\sim(Ey)(\mathscr{A}(y)$ A $(z)(z < y \supset \sim \mathscr{A}(z))) \supset \sim \mathscr{A}(x)$
   1–5, Deduction Theorem

7. $\mathscr{A}(x) \supset (Ey)(\mathscr{A}(y) \supset (z)(z < y \supset \sim \mathscr{A}(z)))$
   6, Tautology

Exercise 3.1. Show that

$$\vdash (x)(\mathscr{A}(x) \supset (Ey)(y < x \text{ A } \mathscr{A}(y))) \supset (x) - \mathscr{A}(x)$$

(Method of Infinite Descent).

Another important notion in number theory is divisibility, which we now define.

Definition. $t|s$ for $(Ez)(s = t\,.\,\text{ɪ})$, where z is the first variable not in t or s.

Proposition 3.10. The following wfs are *theorems*.

(a) $t|t$

(b) $\bar{1}|t$

(c) $t|0$

(d) $t|s \wedge s|r \supset t|r$

(e) $s \neq 0 \wedge t|s \supset t \leqslant s$

(f) $t|s \wedge s|t \supset s = t$

(g) $t|s \supset t|r \cdot s$

(h) $t|s \wedge t|r \supset t|(s + r)$

Proof. (a) $t = t\,.\,\bar{1}$. Hence $t|t$. (b) $t = \bar{1}\,.\,t$. Hence $\bar{1}|t$. (c) $0 = t \cdot 0$. Hence, $t|0$. (d) If $s = t \cdot z$ and $r = s\,.\,w$, then $r = t\,.\,(z \cdot w)$. (e) If $s \neq 0$ and $t|s$, then $s = t \cdot z$ for some z. If $z = 0$, then $s = 0$. Hence, $z \neq 0$. So, $z = u'$ for some u. $s = t\,.\,(u') = t\,.\,u + t \geqslant t$. (f)–(h) are left as exercises.

EXERCISES

Prove the following:

3.2. $\vdash t|\bar{1} \supset t = \bar{1}$

3.3. $\vdash (t|s \wedge t|s') \supset t = \bar{1}$

It will be useful, for later purposes, to prove the existence of a unique quotient and remainder upon division of one number by another.

Proposition 3.11. $\vdash y \neq 0 \supset (E_1u)(E_1v)(x = y \cdot u + v \wedge v < y)$.

Proof. Let $\mathscr{A}(x)$ bey $\neq 0 \supset (Eu)(Ev)(x = y\,.\,u + v \wedge v < y)$.

(i) 1. $y \neq 0$ — Hyp

2. $0 = y \cdot 0 + 0$ — (S5′), (S7′)

3. $0 < y$ — 1, Proposition 3.7(t)

4. $0 = y \cdot 0 + 0 \wedge 0 < y$ — 2, 3, Tautology

5. $(Eu)(Ev)(0 = y\,.\,u + v \wedge v < y)$ — 4, Rule E4

6. $y \neq 0 \supset (Eu)(Ev)(0 = y \cdot u + v \wedge v < y)$
   1–5, Deduction Theorem

(ii) 1. $\mathscr{A}(x)$, i.e., $y \neq 0 \supset (Eu)(Ev)(x = y\,.\,u + v$ A $v < y)$
   Hyp

2. $y \neq 0$ — Hyp

3. $(Eu)(Ev)(x = y \cdot u + v \wedge v < y)$ — 1, 2, MP

4. $x = y \cdot a + b \wedge b < y$ — 3, Rule C twice

5. $b < y$ — 4, Tautology

6. $b' \leqslant y$ — 5, Proposition 3.7(k)

7. $b' < y \vee b' = y$ — 6, Definition

8. $b' < y \supset (x' = y \cdot a + b' \wedge b' < y)$ — 4, (S6′)

9. $b' < y \supset (Eu)(Ev)(x' = y \cdot u + v \wedge v < y)$
   8, Rule E4, Deduction Theorem

10. $b' = y \supset x' = y \cdot a + y \cdot \bar{1}$ — 4, (S6′), Proposition 3.5(b)

11. $b' = y \supset (x' = y \cdot (a + \bar{1}) + 0 \wedge 0 < y)$
    10, Proposition 3.4, 2, Proposition 3.7(t), (S5′)

12. $b' = y \supset (Eu)(Ev)(x' = y \cdot u + v \wedge v < y)$
    11, Deduction Theorem, Rule E4

13. $(Eu)(Ev)(x' = y\,.\,u + v \wedge$ v $< y)$ — 7, 9, 12, Tautology

14. $\mathscr{A}(x) \supset (y \neq 0 \supset (Eu)(Ev)(x' = y \cdot u + v \wedge v < y))$
    i.e., $\mathscr{A}(x) \supset \mathscr{A}(x')$ — 1–13 Deduction Theorem

By (i), (ii), and the Induction Rule, $\vdash (x)\mathscr{A}(x)$. This establishes the existence of a quotient u and a remainder v. To prove uniqueness, proceed as follows. Assume Y $\neq 0$. Assume $x = y \cdot$ u, $+ v_1 \wedge v_1 < y$ and $x = y\,.\,u_2 + v_2 \wedge v_2 < y$. Now, $u_1 = u_2$ or u, $< u_2$ or $u_2 <$ u,. If u, $= u_2$, then $v_1 = v_2$ by Proposition 3.4(d). If $u_1 < u_2$, then $u_2 =$ u, $+$ w for some w $\neq 0$. Then $y\,.\,u_1 + v_1 = y \cdot$ (u, $+$ w) $+ v_2 = y\,.$ u, $+ y\,.\,w + v_2$. Hence, $v_1 = y\,.\,w + v_2$; but w $\neq 0$. Hence, $y\,.\,w \geqslant y$. So, $v_1 = y \cdot w + v_2 \geqslant y$, contradicting v, $< y$. Hence, u, $\nless u_2$. Similarly, $u_1 \ngtr u_2$. Hence, u, $= u_2$, and so, $v_1 = v_2$.

From this point on, one can generally translate into S and prove the results from any text on elementary number theory. There are certain number-theoretic functions, such as x^y and $x!$, which we have to be able to define in S, and this we shall do later in this chapter. (In most cases, by suitable paraphrasing, one can get along without explicitly defining these functions, but, after a short time, this leads to unwieldy complications.) Some standard results of number theory, such as Dirichlet's Theorem, are proved with the aid of the theory of complex variables, and it is often not known whether elementary proofs (or proofs in S) can be given for such theorems. The statement of some results in number theory involve non-elementary concepts, such as the logarithmic function, and, except in cases where an equivalent elementary formula can be obtained, cannot even be formulated in S. More information about the strength and expressive powers of S will be revealed in the sequel. For example it will be shown later that there are closed wfs which are neither provable nor disprovable in S, if S is consistent; hence there is a wf which is true under the standard interpretation but is not provable in S. We shall also see that this incompleteness of S cannot be attributed to omission of some essential axiom, but has deeper underlying causes which apply to other theories as well.

EXERCISES

3.4. Show that the Induction Principle (S9) is independent of the other axioms of S.

3.5.^{D} (a) Show that there exist non-standard models for S of any cardinality $\aleph_\alpha$.
(b) Ehrenfeucht [1958] has shown the existence of at least $2^{\aleph_0}$ mutually non-isomorphic models of S of cardinality $\aleph_\alpha$. Prove the special case that there are $2^{\aleph_0}$ mutually non-isomorphic denumerable models of S.

3.6.^{D} Give a standard mathematical proof of the categoricity of Peano's Postulates, in the sense that any two "models" are isomorphic. Explain why this proof does not apply to the first-order theory S.

3.7.^{D} (Presburger [1929]) If we eliminate from S the function letter f_2^2 for multiplication and the axioms (S7)–(S8), show that the new system S_+ is complete and decidable.

3.8. (a) Show that every closed atomic wf $t = s$ of S is decidable, i.e., either $\vdash_S t = s$ or $\vdash_S t \neq s$.
(b) Show that every closed wf of S without quantifiers is decidable.

2. Number-Theoretic Functions and Relations

A number-theoretic function is one whose arguments and values are natural numbers, and a number-theoretic relation is a relation whose arguments are natural numbers. For example, multiplication is a number-theoretic function of two arguments, and the expression $x + y < z$ determines a number-theoretic relation of three arguments. Number-theoretic functions and relations are intuitive and are not bound up with any formal system.

A number-theoretic relation $R(x_1, \ldots, x_n)$ is said to be *expressible* in S if and only if there is a wf $\mathscr{A}(x_1, \ldots, x_n)$ of S with n free variables such that: for any natural numbers $k_1, \ldots, k_n$,

(1) if $R(k_1, \ldots, k_n)$ is true, then $\vdash_s \mathscr{A}(\overline{k_1}, \ldots, \overline{k_n})$.
(2) if $R(k_1, \ldots, k_n)$ is false, then $\vdash_s \sim \mathscr{A}(\overline{k_1}, \ldots, \overline{k_n})$.

For example, the number-theoretic relation of equality is expressed in S by the wf $x_1 = x_2$. In fact, if $k_1 = k_2$, then $\overline{k_1}$ is the same term as $\overline{k_2}$, and so, by Proposition 3.2(a), $\vdash_s \overline{k_1} = \overline{k_2}$. Also, if $k_1 \neq k_2$, then, by Proposition 3.6(a), $\vdash_s \overline{k_1} \neq \overline{k_2}$.

Likewise, the relation "less than" is expressed in S by wf $x_1 < x_2$. For, if $k_1 < k_2$, then there is some non-zero number n such that $k_2 = n + k_1$. Now, by Proposition 3.6(a)(ii), $\vdash_S \overline{k_2} = \overline{k_1} + \overline{n}$. Also, by (S3′), since $n \neq 0$, $\vdash \overline{n} \neq 0$. Hence, one can prove in S the wf $(Ew)(w \neq 0 \wedge w + \overline{k_1} = \overline{k_2})$, i.e., $\overline{k_1} < \overline{k_2}$. Now, if $k_1 \nless k_2$, then $k_2 < k_1$ or $k_2 = k_1$. If $k_2 < k_1$, then, as we have just seen, $\vdash \overline{k_2} < \overline{k_1}$. If $k_2 = k_1$, then $\vdash \overline{k_2} = \overline{k_1}$. In either case, $\vdash \overline{k_2} \leqslant \overline{k_1}$, and then by Proposition 3.7(a), (c), $\vdash \overline{k_1} \nless \overline{k_2}$.

EXERCISES

3.9. Show that the negation, conjunction, and disjunction of expressible relations are also expressible (in S).

3.10. Show that the relation $x + y = z$ is expressible in S.

A number-theoretic function $f(x_1, \ldots, x_n)$ is said to be *representable* in S if and only if there is a wf $\mathscr{A}(x_1, \ldots, x_{n+1})$ of S with the free variables $x_1, \ldots, x_{n+1}$ such that, for any numbers $k_1, \ldots, k_{n+1}$:

(1) if $f(k_1, \ldots, k_n) = k_{n+1}$, then $\vdash_s \mathscr{A}(\overline{k_1}, \ldots, \overline{k_n}, \overline{k_{n+1}})$;
(2) $\vdash_s (E_1 x_{n+1}) \mathscr{A}(\overline{k_1}, \ldots, \overline{k_n}, x_{n+1})$.

If, in this definition, we change (2) to (2′), $\vdash_s (E_1 x_{n+1}) \mathscr{A}(x_1, \ldots, x_n, x_{n+1})$, then the function f is said to be *strongly representable* in S. Notice that (2′) implies (2), by Gen and Rule A4. Hence, every strongly representable function is also representable. (For the converse, cf. Exercise 3.35 on p. 151.)

Examples.

(a) The zero function, $Z(x) = 0$, is strongly representable in S by the wf $x_1 = x_1 \wedge x_2 = 0$. For any k_1, if $Z(k_1) = k_2$, then $k_2 = 0$, and $\vdash \overline{k_1} = \overline{k_1} \wedge 0 = 0$, i.e., (1) holds. Also, $\vdash (E_1 x_2)(x_1 = x_1 \wedge x_2 = 0)$. Thus, (2′) holds.

(2) The successor function, $N(x) = x + 1$, is strongly representable in S by the wf $x_2 = (x_1)'$. For any k_1, if $N(k_1) = k_2$, then $k_2 = k_1 + 1$; hence, $\overline{k_2}$ is $(\overline{k_1})'$. Then $\vdash \overline{k_2} = (\overline{k_1})'$. Also, $\vdash (E_1 x_2)(x_2 = (x_1)')$.

(c) The projection function, $U_i^n(x_1, \ldots, x_n) = x_i$, is strongly representable in S by the wf $x_1 = x_1 \wedge x_2 = x_2 \wedge \cdots \wedge x_n = x_n \wedge x_{n+1} = x_i$. If $U_i^n(k_1, \ldots, k_n) = k_{n+1}$, then $k_{n+1} = k_i$, and $\overline{k_{n+1}}$ is $\overline{k_i}$. Hence,

$$\vdash \overline{k_1} = \overline{k_1} \wedge \overline{k_2} = \overline{k_2} \wedge \cdots \wedge \overline{k_n} = \overline{k_n} \wedge \overline{k_{n+1}} = \overline{k_i}.$$

Thus, (1) holds. In addition,

$$\vdash (E_1 x_{n+1})(x_1 = x_1 \wedge x_2 = x_2 \wedge \cdots \wedge x_n = x_n \wedge x_{n+1} = x_i),$$

i.e., (2′) holds.

(d) Assume that the functions $g(x_1, \ldots, x_m)$, $h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)$ are (strongly) representable in S, by the wfs

$$\mathscr{B}(x_1, \ldots, x_m, x_{m+1}),\ \mathscr{A}_1(x_1, \ldots, x_{n+1}), \ldots, \mathscr{A}_m(x_1, \ldots, x_{n+1}),$$

respectively. Define a new function f by the equation $f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$. f is said to be obtained from g, h,, . . . , h_m by substitution. Then f is also (strongly) representable in S, by the wf $\mathscr{A}(x_1, \ldots, x_{n+1})$:

$$(Ey_1) \ldots (Ey_m)(\mathscr{A}_1(x_1, \ldots, x_n, y_1) \text{ A } \ldots$$
$$\wedge \mathscr{A}_m(x_1, \ldots, x_n, y_m) \text{ A } \mathscr{B}(y_1, \ldots, y_m, x_{n+1}))$$

To prove (1), let $f(k_1, \ldots, k_n) = k_{n+1}$. Let $h_i(k_1, \ldots, k_n) = r_i$ for $1 \leqslant i \leqslant m$; then $g(r_1, \ldots, r_m) = k_{n+1}$. By our assumption that P , $\mathscr{A}_1, \ldots, \mathscr{A}_m$ (strongly) represent g, h,, . . . , h_m, respectively, we have I- $\mathscr{A}_i(\overline{k_1}, \ldots, \overline{k_n}, \overline{r_i})$ for $1 \leqslant i \leqslant m$, and I- $\mathscr{B}(\overline{r_1}, \ldots, \overline{r_m}, \overline{k_{n+1}})$. Hence, I- $\mathscr{A}_1(\overline{k_1}, \ldots, \overline{k_n}, \overline{r_1}) \wedge \ldots \wedge$ a_m^*; $\ldots, \overline{k_n}, \overline{r_m}) \wedge \mathscr{B}(\overline{r_1}, \ldots, \overline{r_m}, k_{n+1})$. BY Rule FA, I- a &,. . . , $\overline{k_n}, k_{n+1})$, i.e., (1) holds. We shall prove (2') in the case of strong representability; the proof of (2) in the case of representability is similar. Assume

$$(✠)\quad (Ey_1)(Ey_2) \ldots (Ey_m)(\mathscr{A}_1(x_1, \ldots, x_n, y_1) \wedge \ldots$$
$$\wedge \mathscr{A}_m(x_1, \ldots, x_n, y_m) \text{ A } \mathscr{B}(y_1, \ldots, y_m, u))$$

and

$$(✠✠)\quad (Ey_1)(Ey_2) \ldots (Ey_m)(\mathscr{A}_1(x_1, \ldots, x_n, y_1) \wedge \ldots$$
$$\wedge \mathscr{A}_m(x_1, \ldots, x_n, y_m) \text{ A } \mathscr{B}(y_1, \ldots, y_m, v))$$

By (✠), using Rule C m times,

$$\mathscr{A}_1(x_1, \ldots, x_n, b_1) \text{ A } \ldots \text{ A } \mathscr{A}_m(x_1, \ldots, x_n, b_m) \text{ A } \mathscr{B}(b_1, \ldots, b_m, u)$$

By (✠✠), using Rule C again,

$$\mathscr{A}_1(x_1, \ldots, x_n, c_1) \wedge \ldots \wedge \mathscr{A}_m(x_1, \ldots, x_n, c_m) \wedge \mathscr{B}(c_1, \ldots, c_m, v))$$

Since I- $(E_1x_{n+1})\mathscr{A}_i(x_1, \ldots,$ x,,, $x_{n+1})$, we obtain, from $\mathscr{A}_i(x_1, \ldots,$ x,,, $b_i)$ and $\mathscr{A}_i(x_1, \ldots,$ x,,, $c_i)$, that $b_i = c_i$. From $\mathscr{B}(b_1, \ldots, b_m,$ u) and b, = c,, . . . , $b_m = c_m$, we have $\mathscr{B}(c_1, \ldots, c_m,$ u). Hence, from I- $(E_1x_{n+1})\mathscr{B}$(x,, . . . , x,,+1) and $\mathscr{B}$(c,, . . . , $c_m, v)$, we obtain $u = v$. We have shown I- $\mathscr{A}(x_1, \ldots,$ x,,, u) A $\mathscr{A}(x_1, \ldots,$ x,,, u) $\supset u =$ u. It is also easy to show that I- $(Ex_{n+1})\mathscr{A}(x_1, \ldots, x_{n+1})$ (Exercise). From this, we have I- $(E_1x_{n+1})\mathscr{A}(x_1, \ldots,$ x,, $x_{n+1})$, i.e., (2').

EXERCISES

Show that the following functions are strongly representable in S.

3.11. $Z_n(x_1, \ldots, x_n) = 0$ (Hint: $Z_n(x_1, \ldots, x_n) = Z(U_1^n(x_1, \ldots, x_n))$. Use (a), (c), (d).)

3.12. For any given k, $C_k^n(x_1, \ldots, x_n) = k$ (Hint: by 3.11, we have C_0^n; assume C_k^n is strongly representable. Then $C_{k+1}^n(x_1, \ldots, x_n) = N(C_k^n(x_1, \ldots, x_n))$; use (b), (d).)

3.13. Addition.

3.14. Multiplication.

If $R(x_1, \ldots, x_n)$ is a relation, then the characteristic function $C_R(x_1, \ldots, x_n)$ is defined as follows:

$$C_R(x_1, \ldots, x_n) = \begin{cases} 0 & \text{if } R(x_1, \ldots, x_n) \text{ is true} \\ 1 & \text{if } R(x_1, \ldots, x_n) \text{ is false} \end{cases}$$

PROPOSITION 3.12. $R(x_1, \ldots, x_n)$ is expressible in S *if* and only *if* $C_R(x_1, \ldots, x_n)$ *is* (strongly) representable in S.

PROOF. If $R(x_1, \ldots, x_n)$ is expressible in S by a wf $\mathscr{A}(x_1, \ldots,$ x,), then it is easy to verify that $C_R(x_1, \ldots, x_n)$ is strongly representable in S by the wf $(\mathscr{A}(x_1, \ldots,$ x,,) A $x_{n+1} = 0) \vee (\sim \mathscr{A}(x_1, \ldots,$ x,,) $\wedge x_{n+1} = \overline{1})$. Conversely, if $C_R(x_1, \ldots,$ 3 is representable in S by a wf $\mathscr{B}(x_1, \ldots, x_n, x_{n+1})$, then $R(x_1, \ldots, x_n)$ is expressible in S by the wf $\mathscr{B}$(x,, . . . , x,,, 0).

EXERCISES

3.15. The representing relation (or graph) of a function $f(x_1, \ldots, x_n)$ is the relation $f(x_1, \ldots, x_n) = x_{n+1}$. Show that $f(x_1, \ldots, x_n)$ is representable in S if and only if its representing relation is expressible in S.

3.16. If R_1 and R_2 are relations of n arguments, prove that $C_{\text{not-}R_1} = 1 - C_{R_1}$, $C_{(R_1 \text{ or } R_2)} = C_{R_1} \cdot C_{R_2}$, and $C_{(R_1 \text{ and } R_2)} = C_{R_1} + C_{R_2} - C_{R_1} \cdot C_{R_2}$.

3.17. Show that $f(x_1, \ldots, x_n)$ is representable in S if and only if there is a wf $\mathscr{A}(x_1, \ldots, x_{n+1})$ such that, for any natural numbers $k_1, \ldots, k_n$, m, if $f(k_1, \ldots, k_n) = m$, then $\vdash_S (x_{n+1})(\mathscr{A}(\overline{k_1}, \ldots, k_n, x_{n+1}) \equiv x_{n+1} = \overline{m})$.

3.18. Show that Proposition 3.12 remains valid for any theory with equality K containing all the numerals 0, I, 2, . . . , except that the "if' part requires that $\vdash_K \overline{0} \neq \overline{1}$.

3. Primitive Recursive and Recursive Functions

The study of representability of functions in S leads to a class of number-theoretic functions which turn out to be of great importance in mathematical logic.

DEFINITION

(1) The following functions are called initial junctions.

(I) The zero function: $Z(x) = 0$ for all x.

(II) The successor function: $N(x) = x + 1$ for all x.

(III) The projection functions: $U_i^n(x_1, \ldots, x_n) = x_i$ for all $x_1, \ldots, x_n$.

(2) The following are rules for obtaining new functions from given functions.

(IV) Substitution:

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$$

f is said to be obtained by substitution from the functions $g(y_1, \ldots, y_m)$, $h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)$.

(V) Recursion:

$$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$$

$$f(x_1, \ldots, x_n, y + 1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y))$$

Here, we allow n = 0, in which case we have

$$f(0) = k \qquad \text{(where k is a fixed integer)}$$

$$f(y + 1) = h(y, f(y)).$$

We shall say that f is obtained from g and h (or, in the case $n = 0$, from h alone) by recursion. The ***parameters*** of the recursion are $x_1, \ldots, x_n$. Notice that f is well-defined: the value of $f(x_1, \ldots, x_n, 0)$ is given by the first and if we already know the value $f(x_1, \ldots, x_n, y)$, then we can obtain $f(x_1, \ldots, x_n, y + 1)$ by the second equation.

(VI) μ-Operator: assume that $g(x_1, \ldots, x_n, y)$ is a function such that for any $x_1, \ldots, x_n$ there is at least one y such that $g(x_1, \ldots, x_n, y) = 0$. We $\mu y(g(x_1, \ldots, x_n, y) = 0)$ the least number y such that $\ldots, x_n, y) = 0$. In general, for any relation $R(x_1, \ldots, x_n, y)$, we denote by $\mu y R(x_1, \ldots, x_n, y)$ the least y such that $R(x_1, \ldots, x_n, y)$ is true, if there is any y at all such that $R(x_1, \ldots, ,\ y)$ holds. Let $f(x_1, \ldots, x_n) = \mu y(g(x_1, \ldots, x_n, y) = 0)$. Then f is said to be obtained from g by means of the μ-operator, if the given assumption about g holds: for any $x_1, \ldots, x_n$, there is at least one y such that $g(x_1, \ldots, x_n, y) = 0$.

(3) A function f is said to be ***primitive recursive*** if and only if it can be obtained from the initial functions by any finite number of substitutions (IV) and recursions (V), i.e., if there is a finite sequence of functions $f_0, \ldots, f_n$ such that $f_n = f$, and, for $0 \leqslant i \leqslant n$, either f_i is an initial function or f_i comes from preceding functions in the sequence by an application of Rule (IV) (Substitution) or Rule (V) (Recursion).

(4) A function f is said to be ***recursive*** if and only if it can be obtained from the initial functions by any finite number of applications of Substitution (IV), Recursion (V), and the μ-operator (VI). This differs from the definition above primitive recursive functions only in the addition of possible applications the μ-operator (Rule VI). Hence, every primitive recursive function is recursive. We shall see later that the converse is false.

We shall show that the class of recursive functions is identical with the class of functions representable in S. (In the literature, the phrase "general is sometimes used instead of "recursive".)

First, let us prove that we can add dummy variables to and also permute and dentifv variables in any primitive recursive or recursive function, obtaining a function of the same type.

PROPOSITION 3.13. *Let* $g(y_1, \ldots, y_k)$ *be primitive recursive (or recursive).* $x_1, \ldots, x_n$ *be distinct variables, and, for* $1 \leqslant i \leqslant k$, *let* z_i *be one of* $x_1, \ldots, x_n$. *Then the function* f *such that* $f(x_1, \ldots, x_n) = g(z_1, \ldots, z_k)$ *is primitive recursive (or recursive).*

PROOF. Let $z_i = x_{j_i}$ (where $1 \leqslant j_i \leqslant n$). Then $z_i = U^n_{j_i}(x_1, \ldots, x_n)$. Thus,

$$f(x_1, \ldots, x_n) = g\big(U^n_{j_1}(x_1, \ldots, x_n), U^n_{j_2}(x_1, \ldots, x_n), \ldots, U^n_{j_k}(x_1, \ldots, x_n)\big)$$

and therefore f is primitive recursive (or recursive), since it arises from g, $U^n_{j_1}, \ldots, U^n_{j_k}$ by substitution.

Examples.

1. (Adding dummy variables.) If $g(x_1, x_3)$ is primitive recursive and if $f(x_1, x_2, x_3) = g(x_1, x_3)$, then $f(x_1, x_2, x_3)$ is also primitive recursive. In tion 3.13, let $z_1 = x_1$ and $z_2 = x_3$.

2. (Permuting variables.) If $g(x_1, x_2)$ is primitive recursive and if $f(x_1, x_2) = g(x_2, x_1)$, then $f(x_1, x_2)$ is also primitive recursive. In Proposition 3.13, let $z_1 = x_2$ and $z_2 = x_1$.

3. (Identifying variables.) If $g(x_1, x_2, x_3)$ is primitive recursive and if $f(x_1, x_2) = g(x_1, x_2, x_1)$, then $f(x_1, x_2)$ is primitive recursive. In Proposition 3.13, let $n = 2$ and let $z_1 = x_1$, $z_2 = x_2$, and $z_3 = x_1$.

COROLLARY 3.14. (a) *The zero junction* $Z_n(x_1, \ldots, x_n) = 0$ *is primitive recursive.* (b) *The constant junction* $C^n_k(x_1, \ldots, x_n) = k$, *where* k *is some fixed integer, is primitive recursive.* (c) *The Substitution Rule* (IV) *can be extended to the case where each* h_i *may be a junction of some but not all of the variables* $x_1, \ldots, x_n$; *and* h *may not involve all of the variables* $x_1, \ldots, x_n$, y, *or* $f(x_1, \ldots, x_n, y)$. *Likewise, in the Recursion Rule* (V), *the function* g *may not involve all of the*

PROOF. (a) In Proposition 3.13, let g be the zero function Z; then k = Take z_1 to be x_1. (b) For $k = 0$, this is part (a). Assume true for k. Then $C^n_{k+1}(x_1, \ldots, x_n) = N(C^n_k(x_1, \ldots, x_n))$. (c) By Proposition 3.13, any variables among $x_1, \ldots, x_n$ not present in a function can be added as "dummy variables". For example, if $h(x_1, x_3)$ is given as primitive recursive (or recursive), then $h\#(x_1, x_2, x_3) = h(x_1, x_3) = h(U^3_1(x_1, x_2, x_3), U^3_3(x_1, x_2, x_3))$ is also primitive recursive (or recursive).

PROPOSITION 3.15. *The following functions are primitive recursive.*

(a) $x + y$; (b) $x \cdot y$; (c) x^y; (d) $\delta(x) = \begin{cases} x - 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \end{cases}$,

(e) $x \dot{-} y = \begin{cases} x - y & \text{if } x \geqslant y \\ 0 & \text{if } x < y \end{cases}$; (f) $|x - y| = \begin{cases} x - yy & \text{if } x \geqslant y \\ y - x & \text{if } x < y \end{cases}$;

(g) $sg(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}$; (h) $\overline{sg}(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}$;

(i) $x!$; (j) $\min(x, y)$ = *minimum of* x *and* y; (k) $\min(x_1, \dots, x_n)$;
(l) $\max(x, y)$ = *maximum of* x *and* y; (m) $\max(x,, \dots, x_n)$;
(n) $rm(x, y)$ = *remainder upon division of* y *by* x;
(o) $qt(x, y)$ = *quotient upon division of* y *by* x.

PROOF.

(a) Recursion Rule (V).

$$\begin{aligned} x + 0 &= x & && f(x, 0) &= U_1^1(x) \\ x + (y + 1) &= N(x + y) & \text{i.e.,} && f(x, y + 1) &= N(f(x, y)) \end{aligned}$$

(b)
$$\begin{aligned} x \cdot 0 &= 0 & && g(x, 0) &= Z(x) \\ x \cdot (y + 1) &= (x \cdot y) + x & \text{i.e.,} && g(x, y + 1) &= f(g(x, y), x), \end{aligned}$$

where f is the addition function

(c)
$$x^0 = 1$$
$$x^{y+1} = (x^y) \cdot x$$

(d)
$$\delta(0) = 0$$
$$\delta(y + 1) = y$$

(e)
$$x \dot{-} 0 = x$$
$$x \dot{-} (y + 1) = \delta(x \dot{-} y)$$

(f) $|x - y| = (x \dot{-} y) + (y \dot{-} x)$ (Substitution)

(g)
$$sg(0) = 0$$
$$sg(y + 1) = 1$$

(h) $\overline{sg}(x) = 1 \dot{-} sg(x)$

(i)
$$0! = 1$$
$$(y + 1)! = (y!) \cdot (y + 1)$$

(j) $\min(x, y) = x \dot{-} (x \dot{-} y)$

(k) Assume $\min(x,, \dots, x_n)$ already shown primitive recursive.

$$\min(x_1, \dots, x_n, x_{n+1}) = \min(\min(x_1, \dots, x_n), x_{n+1})$$

(l) $\max(x, y) = y + (x \dot{-} y)$

(m) $\max(x_1, \dots, x_{n+1}) = \max(\max(x_1, \dots, x_n), x_{n+1})$

(n)
$$rm(x, 0) = 0$$
$$rm(x, y + 1) = N(rm(x, y)) \cdot sg(|x - N(rm(x, y))|)$$

(o)
$$qt(x, 0) = 0$$
$$qt(x, y + 1) = qt(x, y) + \overline{sg}(|x - N(rm(x, y))|)$$

DEFINITIONS

$$\sum_{y<z} f(x_1, \dots, x_n, y) = \begin{cases} 0 & \text{if } z = 0 \\ f(x_1, \dots, x_n, 0) + \dots + f(x_1, \dots, x_n, z - 1) & \text{if } z > 0 \end{cases}$$

$$\sum_{y\leqslant z} f(x_1, \dots, x_,, y) = \sum_{y<z+1} f(x_1, \dots, x_n, y)$$

$${}_{y<z} f(x_1, \dots, x_n, y) = \begin{cases} 1 & \text{if } z = 0 \\ f(x_1, \dots, x_n, 0) \cdot \dots \cdot f(x_1, \dots, x_n, z - 1) & \text{if } z > 0 \end{cases}$$

$$\prod_{y\leqslant z} f(x_1, \dots, x_,, y) = \prod_{y<z+1} f(x_1, \dots, x_n, y)$$

These *bounded* sums and products are functions of $x_1, \dots, x_n, z$. We can define doubly bounded sums and products in terms of the ones already given, e.g.,

$$\begin{aligned} {}_{u<y<v} f(x_1, \dots, x_n, y) &= f(x_1, \dots, x_n, u + 1) + \dots + f(x_1, \dots, x_n, v - 1) \\ &= {}_{y<(v \dot{-} u) \dot{-} 1} f(x_1, \dots, x_n, y + u + 1) \end{aligned}$$

PROPOSITION 3.16. *If* $f(x_1, \dots, x_n, y)$ *is primitiue recursive (or recursive), then all the bounded sums and products defined above are also primitive recursive (or recursive).*

PROOF. Let $g(x_1, \dots, x_n, z) = \sum_{y<z} f(x_1, \dots, x_n, y)$. Then, we have the following recursion.

$$g(x_1, \dots, x_n, 0) = 0$$
$$g(x_1, \dots, x_n, z + 1) = g(x_1, \dots, x_n, z) + f(x_1, \dots, x_n, z)$$

If $h(x_1, \dots, x_n, z) = \sum_{y\leqslant z} f(x_1, \dots, x_n, y)$, then

$$h(x_1, \dots, x_n, z) = g(x_1, \dots, x_n, z + 1) \text{ (Substitution).}$$

The proofs for bounded products and doubly bounded sums and products are left as exercises.

Example. Let D(x) be the number of divisors of x, if $x > 0$; let D(0) = I. Then D(x) is primitive recursive, since

$$D(x) = \sum x\ \overline{sg}(rm(y, x)).$$

Given number-theoretic relations, we can apply the connectives of the propositional calculus to them to obtain new relations. We shall use the same symbols ($\sim$, $\wedge$, $\vee$, $\supset$, $\equiv$) for them here, except where confusion may arise between these symbols as they occur in our intuitive metalanguage and as they occur in first-order theories. For example, if $R_1(x_1, \ldots, x_n)$ and $R_2(x_1, \ldots, x_n)$ are relations, then $R_1(x_1, \ldots, x_n) \vee R_2(x_1, \ldots, x_n)$ is a new relation which holds for $x,, \ldots, x_n$ when and only when $R_1(x_1, \ldots, x_n)$ holds or $R_2(x_1, \ldots, x_n)$ holds. We shall use $(y)_{y<z}R(x_1, \ldots, x_n, y)$ to express the relation: for all y, if y is less than z, then $R(x_1, \ldots, x_{,,,} y)$ holds. We shall use $(y)_{y\leqslant z}$, $(Ey)_{y<z}$, $(Ey)_{y\leqslant z}$ in an analogous way, e.g., $(Ey)_{y<z}R(x_1, \ldots, x_n, y)$ means that there is some $y < z$ such that $R(x_1, \ldots, x_n, y)$ holds. We shall call $(y)_{y<z}$, $(y)_{y\leqslant z}$, $(Ey)_{y<z}$, $(Ey)_{y\leqslant z}$ bounded quantifiers. In addition, we define a bounded *μ-operator*:

$$\mu y_{y<z}R(x_1, \quad , x_n, Y = \begin{cases} \text{the least } y < z \text{ for which } R(x_1, \ldots, x_n, y) \\ \quad \text{holds if there is such a } y; \\ z \text{ otherwise} \end{cases}$$

(The value z is chosen in the second case because it is more convenient in later proofs; this choice has no intuitive significance.)

A relation $R(x_1, \ldots, x_n)$ is said to be primitive recursive (or recursive) if and only if its characteristic function $C_R(x_1, \ldots, x_n)$ is primitive recursive (or recursive). In particular, a set A of natural numbers is primitive recursive (or recursive) if and only if its characteristic function $C_A(x)$ is primitive recursive (or recursive).

*Examp*les.

(1) The relation $x, = x_2$ is primitive recursive. Its characteristic function is $sg(|x_1 - x_2|)$, which is primitive recursive, by Proposition 3.15(f), (g).

(2) The relation $x, < x_2$ is primitive recursive, since its characteristic function is $\overline{sg}(x_2 \dot{-} x_1)$, which is primitive recursive, by Proposition 3.15(e), (h).

(3) The relation $x_1|x_2$ is primitive recursive, since its characteristic function is $sg(rm(x_1, x_2))$.

(4) The relation $Pr(x)$, x is a prime, is primitive recursive, since $C_{Pr}(x) = sg((D(x) \dot{-} 2) + \overline{sg}(|x - 1|) + \overline{sg}(|x - 0|))$. Remember that x is a prime if and only if it has exactly two divisors and is not equal to 0 or 1.

PROPOSITION 3.17. *Relations* obtainedfrom primitive recursive (or recursiue) relations by means of the propositional connectives and the bounded *quantifiers* are also primitive recursive (or recursive). Also, application of the bounded *μ-operators* $\mu y_{y<z}$ or $\mu y_{y\leqslant z}$ *leads* from primitive recursive (or recursive) relations to primitive recursive (or recursive)functions.

PROOF. Assume $R_1(x_1, \ldots, x_n)$ and $R_2(x_1, \ldots, x_n)$ primitive recursive (or recursive) relations. Then the characteristic functions C_{R_1} and C_{R_2} are primitive recursive (or recursive). But $C_{\sim R_1}(x_1, \ldots, x_n) = 1 - C_{R_1}(x_1, \ldots, x_n)$; hence $\sim R_1$ is primitive recursive (or recursive). Also, $C_{R_1 \vee R_2}(x_1, \ldots, 3 = C_{R_1}(x,, \ldots, x_n) \cdot C_{R_2}(x_1, \ldots, x_n)$; so, $R_1 \vee R_2$ is primitive recursive (or recursive). Since all the propositional connectives are definable in terms of -- and $\vee$, this takes care of them. Now, assume $R(x_1, \ldots, x_n, y)$ primitive recursive (or recursive). If $Q(x_1, \ldots, x_n, z)$ is the relation $(Ey)_{y<z}R(x_1, \ldots, x_n, y)$, then it is easy to verify that $C_Q(x_1, \ldots, x_n, z) = \prod_{y<z} C_R(x_1, \ldots, x_n, y)$, which, by Proposition 3.16, is primitive recursive (or recursive). The bounded quantifier $(Ey)_{y\leqslant z}$ is equivalent to $(Ey)_{y<z+1}$, which is obtainable from $(Ey)_{y<z}$ by substitution. Also, $(y)_{y<z}$ is equivalent to $\sim (Ey)_{y<z} \sim$, and $(y)_{y\leqslant z}$ is equivalent to $\sim (Ey)_{y\leqslant z} \sim$. Doubly bounded quantifiers, such as $(Ey)_{u<y<v}$ can be defined by substitution in the bounded quantifiers already mentioned. Finally, $\prod_{u\leqslant v} C_R(x_1, \ldots, x_n, u)$ has the value 1 for all y such that $R(x_1, \ldots, x_n, u)$ is false for all $u \leqslant y$; it has the value 0 as soon as there is some $u \leqslant y$ such that $R(x_1, \ldots, x_n, u)$ holds. Hence, $\sum_{y<z} (\prod_{u<y} C_R(x_1, \ldots, x_n, u))$ counts the number of integers from 0 up to but not including the first $y < z$ such that $R(x_1, \ldots, x_n, y)$ holds and is z if there is no such y; thus, it is equal to $\mu y_{y<z}R(x_1, \ldots, x_n, y)$ and so the latter function is primitive recursive (or recursive), by Proposition 3.16.

Examples.

(1) Let $p(x)$ be the x^{th} prime number in ascending order, with $p(0) = 2$. We shall write p_x instead of $p(x)$. Then p_x is a primitive recursive function. For

$$p_0 = 2$$

$$p_{x+1} = \mu y_{y\leqslant (p_x)!+1}(p_x < y \wedge Pr(y))$$

Notice that the relation $u < y \wedge Pr(y)$ is primitive recursive. Hence, by Proposition 3.17, the function $\mu y_{y\leqslant v}(u < y \wedge Pr(y))$ is a primitive recursive function $g(u, v)$. If we substitute the primitive recursive functions z and $(z)! + 1$ for u and v respectively in $g(u, v)$, we obtain the primitive recursive function

$$h(z) = \mu y_{y\leqslant z!+1}(z < Y \text{ A } Pr(y))$$

and the right-hand side of the second equation is $h(p_x)$; hence we have an application of the Recursion Rule (V). The bound $(p_x)! + 1$ on the first prime after p_x follows from Euclid's proof of the infinitude of primes (cf. Exercise 3.26, p. 144).

(2) Every positive integer x has a unique factorization into prime powers: $x = p_0^{a_0}p_1^{a_1} \ldots p_k^{a_k}$. Let us denote by $(x)_i$ the exponent a_i in this factorization. If $x = 1$, $(x)_i$ is 0 for all i. If $x = 0$, we arbitrarily let $(x)_i = 0$. Then the function $(x)_i$ is primitive recursive, since $(x)_i = \mu y_{y<x}(p_i^y|x \wedge \sim (p_i^{y+1}|x))$.

(3) Let $1h(x)$ be the number of non-zero exponents in the factorization of x into powers of primes. Let $1h(0) = 0$. Then 1h is primitive recursive. For, let $R(x, y)$ be the primitive recursive predicate $Pr(y) \wedge y|x \wedge x \neq 0$. Then $1h(x) = \sum_{y<x} \overline{sg}(C_R(x, y))$.

(4) If $x = 2^{a_0}3^{a_1} \ldots p_k^{a_k}$ "represents" the sequence of positive integers $a_0, a_1, \ldots, a_k$, and $y = 2^{b_0}3^{b_1} \ldots p_m^{b_m}$ "represents" the sequence $b_0, b_1, \ldots, b_m$, then the number $x * y = 2^{a_0}3^{a_1} \ldots p_k^{a_k} p_{k+1}^{b_0} p_{k+2}^{b_1} \ldots p_{k+1+m}^{b_m}$ "represents" the new sequence a„ a,, . . . , a_k, $b_1, \ldots, b_m$ obtained by juxtaposing the two sequences. But, $k + 1 =$ $1h(x)$, $m + 1 = 1h(y)$, and $b_j = (y)_j$. Hence, $x * y = x \cdot \prod_{j < 1h(y)} (p_{1h(x)+j})^{(y)_j}$, and thus * is a primitive recursive function. We shall omit parentheses in two or more applications of *, since $x * (y * z) = (x * y) * z$ (as long as $y \neq 0$, which will be the only case of interest to us).

EXERCISES

3.19. Using Proposition **3.17**, prove that, if $R(x_1, \ldots, x_n, y)$ is a primitive recursive (or recursive) relation, then $(Ey)_{u<y<v}R(x_1, \ldots, x_n, y)$, $(Ey)_{u\leqslant y\leqslant v}R(x_1, \ldots, x_n, y)$, and $(Ey)_{u\leqslant y<v}R(x_1, \ldots, x_n, y)$ are primitive recursive(or recursive) relations, and $(\mu y)_{u<y<v}R(x_1, \ldots, x_n, y)$, $(\mu y)_{u\leqslant y\leqslant v}R(x_1,$ n Y $(\mu y)_{u\leqslant y<v}R(x_1, \ldots, x_n, y)$, and $(\mu y)_{u<y\leqslant v}R(x_1, \ldots, x_n, y)$ are primitive recursive (or recursive) functions.

3.20. Show that the intersection, union, and complement of primitive recursive (or recursive) sets are also primitive recursive (or recursive). Prove that every finite set is primitive recursive.

3.21. Prove that a function $f(x_1, \ldots, x_n)$ is recursive if and only if its representing relation $f(x_1, \ldots, x_n) = y$ is a recursive relation.

3.22. Let $[\sqrt{n}\,]$ denote the greatest integer $\leqslant \sqrt{n}$, and let $\Pi(n)$ denote the number of primes $\leqslant$ n. Show that $[\sqrt{n}\,]$ and $\Pi(n)$ are primitive recursive.

3.23. Let e be the base of the natural logarithms. Show that $[ne]$, the greatest integer $\leqslant$ ne, is a primitive recursive function of n.

3.24. Let $RP(y, z)$ hold if and only if y and z are relatively prime, that is, y and z have no common factor greater than 1. Let $\varphi(n)$ be the number of positive integers $\leqslant$ n which are relatively prime to n. Prove that RP and φ are primitive recursive.

3.25. Show that, in the definition of the primitive recursive functions, one need not assume that $Z(x) = 0$ is one of the initial functions.

3.26. Prove that $p_{k+1} \leqslant (p_0p_1 \ldots p_k) + 1$. Hence, $p_{k+1} \leqslant p_k! + 1$.

For use in the further study of recursive functions, we prove the following theorem on definition by cases.

PROPOSITION 3.18. *Let*

$$f(x_1, \ldots, x_n) = \begin{cases} g_1(x_1, \ldots, x_n) & \text{if } R(x_1, \ldots, x) \text{ holds} \\ g_2(x_1, \ldots, x_n) & \text{if } R_2(x_1, \ldots, x_n) \text{ holds} \\ \ldots & \\ \ldots & \\ g_k(x_1, \ldots, x_n) & \text{if } R_k(x_1, \ldots, x_n) \text{ holds.} \end{cases}$$

If the functions $g_1, \ldots, g_k$ and the relations R,, . . . , R_k are primitive recursive (*or recursive*), and *if*, for any $x_1, \ldots, x_n$, exactly one of the relations $R_1(x_1, \ldots, x_n), \ldots, R_k(x_1, \ldots, x_n)$ is true, *then* f *is primitive recursive* (*or recursive*).

PROOF. $f(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n) \cdot \overline{sg}(C_{R_1}(x_1, \ldots, x_n)) + \ldots + g_k(x_1, \ldots, x_n) \cdot \overline{sg}(C_{R_k}(x_1, \ldots, x_n))$.

EXERCISES

3.27. Show that in Proposition 3.18 it is not necessary to assume that R_k is primitive recursive (or recursive).

3.28. Let

$$f(x) = \begin{cases} x^2 & \text{if x is even} \\ x + 1 & \text{if x is odd} \end{cases}$$

Prove that f is primitive recursive.

3.29. Let

$$h(x) = \begin{cases} 2 & \text{if Fermat's Last Theorem is true} \\ 1 & \text{if Fermat's Last Theorem is false} \end{cases}$$

Is h primitive recursive?

It is often important to have available a primitive recursive one–one correspondence between the set of ordered pairs of natural numbers and the set of natural numbers. We shall enumerate the pairs as follows:

$$\underbrace{(0, 0)}, \quad \underbrace{(0, 1), (1, 0), (1, 1)} \quad \underbrace{(0, 2), (2, 0), (1, 2), (2, 1), (2, 2)}, \ldots$$

After we have enumerated all the pairs having components $\leqslant$ k, we then add a new group of all the new pairs involving components $\leqslant k + 1$ in the following order: $(0, k + 1), (k + 1, 0), (1, k + 1), (k + 1, 1), \ldots, (k, k + 1), (k + 1, k), (k + 1, k + 1)$. Now, if $x < y$, then (x, y) occurs before (y, x) and both are in the $(y + 1)^{th}$ group. (Note that we start from one in counting groups.) The first y groups contain y^2 pairs, and (x, y) is the (2x + I)'' pair in the $(y + 1)^{th}$ group. Hence, (x, y) is the $(y^2 + 2x + 1)^{th}$ pair in the ordering, and (y, x) is the $(y^2 + 2x + 2)$'' pair. On the other hand, if $x = y$, (x, y) is the ((x + I)')'' pair. This justifies the following definition, in which $0^2(x, y)$ denotes the place of the pair (x, y) in the above enumeration, with (0, 0) considered to be in the 0^{th} place.

$$\sigma^2(x, y) = (sg(x \dot{-} y)) \cdot (x^2 + 2y + 1) + (\overline{sg}(x \dot{-} y)) \cdot (y^2 + 2x)$$

Clearly σ^2 is primitive recursive.

Let us define inverse functions σ_1^2 and σ_2^2 such that $\sigma_1^2(\sigma^2(x, y)) = x$, $\sigma_2^2(\sigma^2(x, y)) = y$, and $\sigma^2(\sigma_1^2(z), \sigma_2^2(z)) = z$. Thus, $\sigma_1^2(z)$ and $\sigma_2^2(z)$ are the first and second components, respectively, of the z^{th} ordered pair in the given enumeration. Note first that $\sigma_1^2(0) = 0$, $\sigma_2^2(0) = 0$,

$$\sigma_1^2(n + 1) = \begin{cases} \sigma_2^2(n) & \text{if } \sigma_1^2(n) < \sigma_2^2(n) \\ \sigma_2^2(n) + 1 & \text{if } \sigma_1^2(n) > \sigma_2^2(n) \\ 0 & \text{if } \sigma_1^2(n) = \sigma_2^2(n) \end{cases}$$

and

$$\sigma_2^2(n+1) = \begin{cases} \sigma_1^2(n) & \text{if } \sigma_1^2(n) \neq \sigma_2^2(n) \\ \sigma_1^2(n)+1 & \text{if } \sigma_1^2(n) = \sigma_2^2(n) \end{cases}$$

Hence,

$$\begin{aligned} \sigma_1^2(n+1) &= \sigma_2^2(n)\cdot\left(sg\left(\sigma_2^2(n) \dot{-} \sigma_1^2(n)\right)\right) + \left(\sigma_2^2(n)+1\right)\cdot\left(sg\left(\sigma_1^2(n) \dot{-} \sigma_2^2(n)\right)\right) \\ &= \varphi\left(\sigma_1^2(n), \sigma_2^2(n)\right) \\ \sigma_2^2(n+1) &= sg\left(|\sigma_1^2(n) - \sigma_2^2(n)|\right)\cdot\sigma_1^2(n) + \overline{sg}\left(|\sigma_1^2(n) - \sigma_2^2(n)|\right)\cdot\left(\sigma_1^2(n)+1\right) \\ &= \psi\left(\sigma_1^2(n), \sigma_2^2(n)\right) \end{aligned}$$

where φ and ψ are primitive recursive functions. Thus, σ_1^2 and σ_2^2 are defined recursively at the same time. We can show that σ_1^2 and σ_2^2 are primitive recursive in the following devious way. Let $\tau(u) = 2^{\sigma_1^2(u)}3^{\sigma_2^2(u)}$. Now, τ is primitive recursive, since $\tau(0) = 2^{\sigma_1^2(0)}3^{\sigma_2^2(0)} = 2^0 \cdot 3^0 = 1$, and $\tau(n+1) = 2^{\sigma_1^2(n+1)} \cdot 3^{\sigma_2^2(n+1)} = 2^{\varphi(\sigma_1^2(n), \sigma_2^2(n))}3^{\psi(\sigma_1^2(n), \sigma_2^2(n))} = 2^{\varphi((\tau(n))_0, (\tau(n))_1)}3^{\psi((\tau(n))_0, (\tau(n))_1)}$. Remembering that the function $(x)_i$ is primitive recursive (cf. Example 2, p. 143), we conclude by Recursion Rule (V) that r is primitive recursive. But $\sigma_1^2(x) = (\tau(x))_0$ and $\sigma_2^2(x) = (\tau(x))_1$; by substitution, σ_1^2 and σ_2^2 are primitive recursive.

One–one primitive recursive correspondences between all n-tuples of natural numbers and all natural numbers can be defined step by step, using induction on n. For n = 2, it has already been established. Assume that, for n = k, we have primitive recursive functions $\sigma^k(x_1, \ldots, x_k), \sigma_1^k(x), \ldots, \sigma_k^k(x)$ such that $\sigma_i^k(\sigma^k(x_1, \ldots, x_k)) = x_i$ for I ⩽ i ⩽ k, and $\sigma^k(\sigma_1^k(x), \ldots, \sigma_k^k(x)) = x$. Now, for n = k + I, define $\sigma^{k+1}(x_1, \ldots, x_k, x_{k+1}) = 0^2(o^k(x,, \ldots, x_k), x_{k+1})$, $\sigma_i^{k+1}(x) = \sigma_i^k(\sigma_1^2(x))$ for I ⩽ i ⩽ k, and $\sigma_{k+1}^{k+1}(x) = \sigma_2^2(x)$. Then $\sigma^{k+1}, \sigma_1^{k+1}, \ldots, \sigma_{k+1}^{k+1}$ are all primitive recursive, and we leave it as an exercise to verify that $\sigma_i^{k+1}(\sigma^{k+1}(x_1, \ldots, x_{k+1})) = x_i$, for $1 \leqslant i \leqslant k+1$, and $\sigma^{k+1}(\sigma_1^{k+1}(x), \ldots, \sigma_{k+1}^{k+1}(x)) = x$.

It is often convenient to define functions by a recursion in which the value of $f(x_1, \ldots, x_n, y + I)$ depends not only upon $f(x_1, \ldots, x_n, y)$ but also upon several or all values of $f(x_1, \ldots, x_n, u)$ with $u \leqslant y$. This type of recursion is called a course-of-values recursion. Let $f\#(x_1, \ldots, x_n, y) = \prod_{u<y} p_u^{f(x_1, \ldots, x_n, u)}$. Note that f can be obtained from f# as follows: $f(x_1, \ldots, x_n, y) = (f\#(x_1, \ldots, x_n, y+1))_y$.

PROPOSITION 3.19. *If* $h(x_1, \ldots, x_n, y, z)$ is primitiue recursiue (or recursiue), and $f(x_1, \ldots, x_n, y) = h(x_1, \ldots, x_n, y, f\#(x_1, \ldots, x_n, y))$, then f is primitiue recursiue (or recursiue).

PROOF.

$$\begin{aligned} f\#(x_1, \ldots, x_n, 0) &= 1 \\ f\#(x_1, \ldots, x_n, y+1) &= f\#(x_1, \ldots, x_n, y)\cdot p_y^{f(x_1, x_2, \ldots, x_n, y)} \\ &= f\#(x_1, \ldots, x_n, y)\cdot (p_y)^{h(x_1, \ldots, x_n, y, f\#(x_1, \ldots, x_n, y))} \end{aligned}$$

Thus, by the Recursion Rule (V), f# is primitive recursive (or recursive); but $f(x_1, \ldots, x_n, y) = (f\#(x_1, \ldots, x_n, y+1))_y$.

Example. The Fibonacci sequence is defined as follows: f(0) = I, f(1) = 2, f(k + 2) = f(k) + f(k + I) for k ⩾ 0. Then f is primitive recursive, since

$$f(k) = \overline{sg}(k) + 2\cdot\overline{sg}(|k-1|) + ((f\#(k))_{k \dot{-} 1} + (f\#(k))_{k \dot{-} 2})\cdot sg(k \dot{-} 1),$$

the function

$$h(y, z) = \overline{sg}(y) + 2 \,.\, \overline{sg}(|y-1|) + ((z)_{y \dot{-} 1} + (z)_{y \dot{-} 2}) \,.\, sg(y \dot{-} 1)$$

is primitive recursive, and

$$f(k) = h(k, f\#(k))$$

EXERCISE 3.30. Let $g(0) = 2$, $g(1) = 4$, and $g(k+2) = 3g(k+1) \dot{-} (2g(k)+1)$. *Show* that g is primitiue recursiue.

COROLLARY 3.20. If $H(x_1, \ldots, x_n, y, z)$ is a primitiue recursiue (or recursive) relation, and $R(x_1, \ldots, x_n, y)$ holds if *and only if* $H(x_1, \ldots, x_n, y, (C_R)\#(x_1, \ldots, x_n, y))$, where C_R is the characteristic function *of* R, then R is primitive recursive (or recursiue).

PROOF. $C_R(x_1, \ldots, x_n, y) = C_H(x_1, \ldots, x_n, y, (C_R)\#(x_1, \ldots, x_n, y))$, where the characteristic function C_H of H is primitive recursive (or recursive). Hence, by Proposition 3.19, C_R is primitive recursive (or recursive), and, therefore, so is the relation R.

Proposition 3.19 and Corollary 3.20 will be drawn upon heavily in the sequel. They are applicable whenever the value of a function or relation for y is defined in terms of values for arguments less than y. Notice in this connection that $R(x_1, \ldots, x_n, u)$ is equivalent to $C_R(x_1, \ldots, x_n, u) = 0$, which, in turn, for $u < y$, is equivalent to $((C_R)\#(x_1, \ldots, x_n, y))_u = 0$.

EXERCISES

331. Prove that the set of recursive functions is denumerable.

332. If $f_0, f,, f_2, \ldots$ is an enumeration of all primitive recursive functions (or all recursive functions) of one variable, prove that the function $f_x(y)$ is not primitive recursive (or recursive).

PROPOSITION 3.21 (GÖDEL'S *B*-FUNCTION). *Let* $\beta(x_1, x_2, x_3) = rm(1 + (x_3 + I) \,.\, x_2, x_1)$. Then β is primitiue recursiue, by Proposition 3.15(n).

Also, $\beta(x_1, x_2, x_3)$ is *strongly* representable in S by the wf $Bt(x_1, x_2, x,, x_4)$:

$$(Ew)(x_1 = (1 + (x_3 + 1)\cdot x_2) . w + x_4 \wedge x_4 < 1 + (x_3 + 1)\cdot x_2)$$

PROOF. By Proposition 3.11, $\vdash (E_1 x_4) Bt(x_1, x_2, x_3, x_4)$. Assume $\beta(k_1, k_2, k_3) = k_4$. Then $k, = (1 + (k_3 + 1) . k_2)$ $k + k_4$ for some k, and $k_4 < I + (k, + 1)$ k_2. So, $\vdash \overline{k_1} = (\bar{1} + (\overline{k_3} + \bar{1}) \cdot \overline{k_2}) \cdot \bar{k} + \overline{k_4}$, by Proposition 3.6(a); and $\vdash \overline{k_4} < \bar{1} + (\overline{k_3} + \bar{1}) \cdot \overline{k_2}$ by the expressibility of $<$ and Proposition 3.6(a). Hence, $\vdash \overline{k_1} = (\bar{1} + (\overline{k_3} \pm \bar{1}) . \bar{k}) \cdot \bar{k} + \overline{k_4} \wedge \overline{k_4} < i + (\overline{k_3} + \bar{1})\overline{k_2}$ from which, by Rule E4, t $Bt(k_1, k_2, k_3, k_4)$. Thus, Bt strongly represents β in **S.**

PROPOSITION 3.22. For any sequence of natural numbers $k_0, k,, \ldots, k_n$, *there* exist natural numbers b, c such that $\beta(b, c, i) = k_i$ for $0 \leqslant \imath \leqslant n$.

PROOF. Let $j = \max(n, k_0, k_1, \ldots, k_n)$ and let $c = j!$. Consider the numbers $u_i = I + (i + 1)c$ for $0 \leqslant i \leqslant n$; they have no factors in common other than one. For, if p were a prime dividing both $1 + (i + 1)c$ and $I + (m + 1)c$ with $0 \leqslant i < m \leqslant n$, then p would divide their difference $(m - i)c$; now, p does not divide c, since, in that case, p would divide both $(i + 1)c$ and $I + (i + 1)c$, and so would divide 1, which is impossible. Hence, p also does not divide $(m - i)$; for $m - i \leqslant n \leqslant j$, and so, $m - i$ divides $j! = c$; if p divided $m - i$, then p would divide c. Hence, p does not divide $(m - i)c$, which yields a contradiction. Thus, the numbers u,, 0 4 i $\leqslant$ n, are relatively prime in pairs. Also, for $0 \leqslant i \leqslant n$, $k_i \leqslant j \leqslant j! = c < 1 + (i + 1)c = u_i$, i.e., $k_i < u_i$. Now, by the Chinese Remainder Theorem (cf. Exercise 3.33, p. 151), there is a number $b < u_0 u_1 \ldots u_n$ such that $rm(u_i, b) = k_i$ for $0 \leqslant i \leqslant n$. But $\beta(b, c, i) = rm(1 + (i + 1)c, b) = rm(u_i, b) = k_i$.

Propositions 3.21 and 3.22 enable us to express within S assertions about finite sequences of natural numbers and this ability is crucial in part of the proof of the following fundamental theorem.

PROPOSITION 3.23. Every recursive function is representable in S.

PROOF. The initial functions Z, N, U_i^n are representable in S, by Examples (a)–(c) on p. 135. The Substitution Rule (IV) does not lead out of the class of representable functions, by Example (d) on p. 136.

The Recursion Rule (V): assume that that $g(x_1, \ldots, x_n)$ and $h(x_1, \ldots, x_n, y, z)$ are representable in S by wfs $\mathcal{A}(x_1, \ldots, x_{n+1})$ and $\mathcal{B}(x_1, \ldots, x_{n+3})$, respectively, and let

$$(I)\begin{cases} f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n) \\ f(x_1, \ldots, x_n, y + 1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \end{cases}$$

Now, $f(x_1, \ldots, x_n, y) = z$ if and only if there is a finite sequence of numbers $b_0, \ldots, b_y$ such that $b_0 = g(x_1, \ldots, x_n)$, $b_{w+1} = h(x_1, \ldots, x_n, w, b_w)$ for $w + I \leqslant y$, and $b_y = z$; but, by Proposition 3.22, reference to finite sequences can be paraphrased in terms of the function β, and, by Proposition 3.21, β is representable in S.

We shall show that $f(x_1, \ldots, x_n, \%+,)$ is representable in S by the wf $\mathcal{C}(x_1, \ldots, x_{n+2})$:

$$\begin{aligned}(Eu)(Ev)[((Ew)(Bt(u, v, 0, w) \wedge \mathcal{A}(x_1, \cdots, x_n, w))) \wedge Bt(u, v, x_{n+1}, x_{n+2}) \\ \wedge (w)(w < x_{n+1} \supset (Ey)(Ez)(Bt(u, v, w, y) \\ \wedge Bt(u, v, w', z) \wedge \mathcal{B}(x_1, \ldots, x_n, w, y, z))\end{aligned}$$

(i) First, assume that $f(k_1, \ldots, k_n, p) = m$. We wish to show that $\vdash \mathcal{C}(\overline{k_1}, \ldots, \overline{k_n}, \bar{p}, \bar{m})$. If $p = 0$, then $m = g(k_1, \ldots, k_n)$. Consider the sequence consisting of m alone. By Proposition 3.22, there exist b, c such that $\beta(b, c, 0) = m$. Hence, $\vdash Bt(\bar{b}, T, 0, \bar{m})$, by Proposition 3.21. Also, $\vdash \mathcal{A}(\overline{k_1}, \ldots, k_n, \bar{m})$ since $m = g(k_1, \ldots, k_n)$. Hence, by Rule E4, (43) $\vdash (Ew)(Bt(\bar{b}, \bar{c}, 0, w) \wedge \mathcal{A}(\overline{k_1}, \ldots, k_n, w))$. We previously obtained (✠✠) $\vdash Bt(\bar{b}, \bar{c}, 0, \bar{m})$. By a tautology, the last conjunction (✠✠✠) of $\mathcal{C}(\overline{k_1}, \ldots, \overline{k_n}, 0, \bar{m})$ is provable, since $\vdash w \not< 0$. Applying Rule E4 to the conjunction of (✠), (✠✠), (✠✠✠), we obtain $\vdash \mathcal{C}(\overline{k_1}, \ldots, k_n, 0, \bar{m})$. Now, for $p > 0$, $f(k_1, \ldots, k_n, p)$ is calculated from the equations (I) in $p + 1$ steps. Let $r_i = f(k_1, \ldots, k_n, i)$. For the sequence of numbers $r_0, r_1, \ldots, r_p$, there are, by Proposition 3.22, numbers b, c such that $\beta(b, c, i) = r_i$ for $0 \leqslant i \leqslant p$. Hence, by Proposition 3.21, $\vdash Bt(\bar{b}, , , \overline{r_i})$. In particular, $\beta(b, c, 0) = r_0 = f(k_1, \ldots, k_n, 0) = g(k_1, \ldots, k_n)$. Therefore, $\vdash Bt(\bar{b}, \bar{c}, 0, \overline{r_0}) \wedge \mathcal{A}(\overline{k_1}, \ldots, k_n, r_0)$, and by Rule E4, (1) t $(Ew)(Bt(\bar{b}, \bar{c}, 0, w) \wedge \mathcal{A}(\overline{k_1}, \ldots, k_n, w))$. Since $r_p = f(k_1, \ldots, k_n, p) = m$, $\beta(b, c, p) = m$; hence, (2) $\vdash Bt(\bar{b}, \bar{c}, \bar{p}, \bar{m})$. For $0 \leqslant i \leqslant p - 1$, $\beta(b, c, i) = r_i = f(k_1, \ldots, k_n, i)$;

$$\begin{aligned}\beta(b, c, i + 1) &= r_{i+1} = f(k_1, \ldots, k_n, i + 1) \\ &= h(k_1, \ldots, k_n, i, f(k_1, \ldots, k_n, i)) = h(k_1, \ldots, k_n, i, r_i).\end{aligned}$$

Hence, $\vdash Bt(\bar{b}, , , \overline{r_i}) \wedge Bt(\bar{b}, , \bar{i}', \overline{r_{i+1}}) \wedge \mathcal{B}(\overline{k_1}, \ldots, \overline{k_n}, \bar{i}, \overline{r_i}, \overline{r_{i+1}})$. BY Rule E4, $\vdash (Ey)(Ez)(Bt(\bar{b}, \bar{c}, \bar{i}, y) \cap Bt(\bar{b}, \bar{c}, \bar{i}', z) \wedge \mathcal{B}(\overline{k_1}, \ldots, k_n, \bar{i}, y, z))$. Hence, by Proposition 3.8(b′), we have (3) t $(w)(w < p \supset (Ey)(Ez)(Bt(b, \bar{c}, w, y)$ A $Bt(\bar{b}, \bar{c}, w', z) \wedge \mathcal{B}(\overline{k_1}, \ldots . k_n, w, y, r)))$. Then, applying Rule E4 twice to the conjunction of (I), (2), and (3), we obtain t $\mathcal{C}(\overline{k_1}, \ldots, k_n, \bar{p}, \bar{m})$. Thus, we have verified clause (1) of the definition of representability in S (cf. p. 135).

(ii) We must show that $\vdash (E_1 x_{n+2})\mathcal{C}(\overline{k_1}, \ldots, k_n, \bar{p}, x_{n+2})$. The proof is by induction on p in the metalanguage. Notice that, by what we have proved above, it suffices to prove only uniqueness. The case for $p = 0$ is easy and is left as an exercise. Now, assume $\vdash (E_1 x_{n+2})\mathcal{C}(k_1, \ldots, k_n, \bar{p}, x_{n+2})$. Let $\alpha = g(k_1, \ldots, k_n)$,

$\beta = f(k_1, \ldots, k_n, p)$, and $\gamma = f(k_1, \ldots, k_n, p + 1) = h(k_1, \ldots\ k_n, p, \beta)$. Then,

(1) $\vdash \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, \bar{p}, \bar{\beta}, \bar{\gamma})$

(2) $\vdash \mathscr{A}(\overline{k_1}, \ldots, \overline{k_n}, \bar{\alpha})$

(3) $\vdash \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \bar{p}, \bar{\beta})$

(4) $\vdash \mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p + 1}, \bar{\gamma})$

(5) $\vdash (E_1 x_{n+2})\mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \bar{p}, x_{n+2})$.

Assume

(6) $\mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \overline{p + 1}, x_{n+2})$

We must prove $x_{n+2} = \bar{\gamma}$. Now from (6) by Rule **C.**

(a) $(Ew)(Bt(b, c, 0, w) \wedge \mathscr{A}(\overline{k_1}, \ldots, \overline{k_n}, w))$

(b) $Bt(b, c, \overline{p + 1}, x_{n+2})$

(c) $(w)(w < \overline{p + 1} \supset (Ey)(Ez)(Bt(b, c, w, y) \wedge Bt(b, c, w', z)$
$\wedge \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, w, y, z))$

From (c),

(d) $(w)(w < \bar{p} \supset (Ey)(Ez)(Bt(b, c, w, y) \wedge Bt(b, c, w', z)$
$\wedge \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, w, y, z))$

From (c) by Rule C,

(e) $Bt(b, c, \bar{p}, d) \wedge Bt(b, c, \overline{p + 1}, e) \wedge \mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, \bar{p}, d, e)$

From (a), (d), (e),

(f) $\mathscr{C}(\overline{k_1}, \ldots, \overline{k_n}, \bar{p}, d)$

From *(f)* and (5),

(g) $d = \bar{\beta}$

From (e), (g),

(h) $\mathscr{B}(\overline{k_1}, \ldots, \overline{k_n}, \bar{p}, \bar{\beta}, e)$

Since $\mathscr{B}$ represents h, we obtain from (1) and (h)

(i) $\bar{\gamma} = e$

From (e), (i),

(j) $Bt(b, c, \overline{p + 1}, \bar{\gamma})$

From (b), (j), and Proposition 3.21,

(k) $x_{n+2} = \bar{\gamma}$.

This completes the induction.

The p-operator (VI). Let us assume that, for any x,, . . . , x_n, there is some y such that $g(x_1, \ldots, x_n, y) = 0$, and let us assume g is representable in S by a wf $\mathscr{D}(x_1, \ldots, x_{n+2})$. Let $f(x_1, \ldots x_n) = \mu y(g(x_1, \ldots, x_n, y) = 0)$. Then f is representable in S by the wf $\mathscr{E}(x_1, \ldots, x_{n+1})$:

$$\mathscr{D}(x_1, \ldots, x_{n+1}, 0) \text{ A } (y)(y < x_{n+1} \supset \sim \mathscr{D}(x_1, \ldots, x_n, y, 0))$$

First, assume $f(k_1, \ldots, k_n) = m$. Then $g(k_1, \ldots,$ k,,, $m) = 0$ and, for $k < m$, $g(k_1, \ldots, k_n, k) \neq 0$. So, $\vdash \mathscr{D}(\overline{k_1}, \ldots\ \overline{k_n}, \bar{m}, 0)$ and, for $k < m$, $\vdash \sim \mathscr{D}(\overline{k_1}, \ldots,,\quad, 0)$ By Proposition 3.8(b′), $\vdash (y)(y < \bar{m} \supset$

$\sim \mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, y, 0))$. Hence, $\vdash \mathscr{E}(\overline{k_1}, \ldots, \overline{k_n}, \bar{m})$. We must also show: $\vdash (E_1 x_{n+1})\mathscr{E}(\overline{k_1}, \ldots, k_n, x_{n+1})$. It suffices, by what we have already shown, to prove the uniqueness. If $\mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, u, 0) \wedge (y)(y < u \supset \sim \mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, y, 0))$, and if $\mathscr{D}(\overline{k_1}, \ldots, k_n, v, 0)$ A $(y)(y < v$ 3 $\sim \mathscr{D}(\overline{k_1}, \ldots, k_n, y, 0))$, then it follows that if $v < u$ we obtain a contradiction $\mathscr{D}(\overline{k_1}, \ldots, \overline{k_n}, v, 0) \wedge \sim \mathscr{D}(\overline{k_1}, \ldots, k_n, v, 0)$, and if $u \leq v$, then we obtain a contradiction $\mathscr{D}(\overline{k_1}, \ldots, k_n, u, 0) \wedge \sim \mathscr{D}(\overline{k_1}, \ldots, k_n, u, 0)$. Hence, since $\vdash (u = v) \vee (u < v) \vee (v < u)$, we conclude $u = v$. This shows the uniqueness.

Thus, we have shown that all recursive functions are representable in S.

COROLLARY 3.24. *Every* recursive relation is *expressible* in S.

PROOF. Let $R(x_1, \ldots, x_n)$ be a recursive relation. Then its characteristic function C_R is recursive. By Proposition 3.23, C_R is representable in S and, therefore, by Proposition 3.12, R is expressible in S-

EXERCISES

3.33^A. (a) Show that, if a and b are relatively prime natural numbers, then there is a natural number c such that $ac \equiv 1 \pmod{b}$. (In general, $x \equiv y \pmod{z}$ means that x and y leave the same remainder upon division by z, or, equivalently, that $x - y$ is divisible by z. This exercise amounts to showing that there exist integers u and v such that $1 = au + bv$.)

(b) Prove the Chinese Remainder Theorem: If $x_1, \ldots, x_k$ are relatively prime in pairs, and y,, . . . , y_k are any natural numbers, there is a natural number z such that $z \equiv y_1 (\text{mod } x_1), \ldots, z \equiv y_k\ (\text{mod } x_k)$. Any two such z's differ by a multiple of $x_1 \ldots x_k$. (Hint: let $x =$ x, . . . x_k and let $x = w_1x_1 = w_2x_2 = \cdots = w_kx_k$. Then, for $1 \leqslant i \leqslant k$, w_i is relatively prime to x_i, and so, by part (a), there is some z_i such that $w_iz_i \equiv 1\ (\text{mod } x_i)$. Now, let $z = w_1z_1y_1 + w_2z_2y_2 + \ldots + w_kz_ky_k$. Then $z \equiv w_iz_iy_i \equiv y_i (\text{mod } x_i)$. In addition, the difference between any two such solutions is divisible by x,, . . . , x_k, and hence by $x_1x_2 \cdots x_k$.)

3.34. Call a relation $R(x_1, \ldots, x_n)$ arithmetical if it is the interpretation of some wf $\mathscr{A}(x_1, \ldots, x_n)$ of S with respect to the standard model. Show that every recursive relation is arithmetical. (Hint: use Corollary 3.24.)

335. Prove that representability implies strong representability, and hence that every recursive function is strongly representable in S (V. H. Dyson).

4. Arithmetization. Gödel Numbers.

For an arbitrary first-order theory K, we correlate with each symbol u of K a positive integer $g(u)$, called the Gödel number of u, in the following way.

$$g(\,(\,) = 3;\ g(\,)\,) = 5;\ g(,) = 7;\ g(\sim) = 9;\ g(\supset) = 11$$

$$g(x_k) = 5 + 8k \text{ for } k = 1, 2, \ldots$$

$$g(a_k) = 7 + 8k \text{ for } k = 1, 2, \ldots$$

$$g(f_k^n) = 9 + 8(2^n3^k) \text{ for } k, n \geqslant 1$$

$$g(A_k^n) = 11 + 8(2^n3^k) \text{ for } k, n \geqslant 1$$

Thus, different symbols have different Gödel numbers, and every Gödel number is an odd positive integer.?

Examples. $g(x_2) = 21$, $g(a_4) = 39$, $g(f_1^2) = 105$, $g(A_2^1) = 155$.

Given an expression $u_1u_2 \cdots u_r$, we define its Gödel number to be $g(u_1u_2 \ldots u_r) = 2^{g(u_1)}3^{g(u_2)} \cdot \ldots p_{r-1}^{g(u_r)}$, where p_i is the i^th^ prime and $p_0 = 2$. For example, $g(A_1^2(x_1, x_2)) = 2^{g(A_1^2)} \cdot 3^{g(()} \cdot 5^{g(x_1)} \cdot 7^{g(,)} \cdot 11^{g(x_2)} \cdot 13^{g())}$ $2^{107}3^35^{13}7^711^{21}13^5$. Observe that different expressions have different Gödel numbers, by the uniqueness of the factorization of integers into primes. In addition, expressions and symbols have different Gödel numbers, since the former have even Gödel numbers and the latter odd Gödel numbers. (A single symbol, considered as an expression, has a different number from its number as a symbol. This situation should cause no confusion.)

If we have an arbitrary finite sequence of expressions $e_1, e_2, \ldots, e_r$, we can assign a Gödel number to this sequence by setting $g(e_1, e_2, \ldots, e_r) = 2^{g(e_1)} \cdot 3^{g(e_2)} \ldots p_{r-1}^{g(e_r)}$. Different sequences of expressions have different Gödel numbers. Since a Gödel number of a sequence of expressions is even and the exponent of 2 in its prime factorization is also even, it differs from Gödel numbers of symbols and expressions.

Thus, g is a one-one function from the set of symbols of K, expressions of K, and finite sequences of expressions of K, into the set of positive integers. The range of g is not the whole set of positive integers; for example, 10 is not a Gödel number.

EXERCISES

3.36. Determine the objects which have the following Gödel numbers: 194.4, 47.

3.37. Show that if n is odd, 4n is not a Gödel number.

3.38. Find the Gödel numbers of the expressions (a) $f_1^1(a_1)$;

(b) $(\sim (A_1^3(a_1, x_3, x_5))) \supset (A_1^1(x_2))$.

This correlation of numbers with symbols, expressions, and sequences of expressions was originally devised by Gödel [1931] in order to arithmetize metamathematics.$ i.e., to replace assertions about a formal system by equivalent number-theoretic statements, and then to express these statements within the formal system. This idea turned out to be the key to a great number of significant problems in mathematical logic.

The assignment of Gödel numbers given here is in no way unique. Other methods may be found in Kleene [1952, Chap. X] and in Smullyan [1961, Chap. I, §6].

†The same numbering was used on p. 66 Lemma 2.10.

‡An *arithmetization* of a theory K is a one-one function g from the set of symbols of K, expressions of K, and finite sequences of expressions of K into the set of positive integers. The following conditions are to be satisfied by the function g: (i) g is effectively computable; (ii) there is an effective procedure which determines whether any given positive integer m is in the range of g, and if m is in the range of g, the procedure finds the object x such that $g(x) = m$.

PROPOSITION 3.25. Let K *be* a *theory* about which we make the assumption *that* the following relations *are primitive recursive* (or recursive):

(a) IC(x) : x is the *Gödel* number of an individual constant of K;

(b) FL(x) : x is the *Gödel* number of a *function* letter of K;

(c) PL(x) : x is the *Gödel* number of a predicate letter of K.

Then the following relations and functions are primitive recursive (or recursive).

(1) EVbl (x) : x is the Gödel number of an expression consisting of a variable. $(Ez)_{z<x}(1 \leqslant z \wedge x = 2^{5+8z})$. By Proposition 3.17, this is primitive recursive.

EIC(x) : x is the Gödel number of an expression consisting of an individual constant. $(Ey)_{y<x}(IC(y) \wedge x = 2^y)$. (Proposition 3.17.)

EFL(x) : x is the Gödel number of an expression consisting of a function letter. $(Ey)_{y<x}(FL(y) \wedge x = 2^y)$. (Proposition 3.17.)

EPL(x) : x is the Gödel number of an expression consisting of a predicate letter. $(Ey)_{y<x}(PL(y) \wedge x = 2^y)$. (Proposition 3.17.)

(2) $Arg_T(x) = (qt(8, x - 9))_0$: If x is the Gödel number of a function letter f_j^n, then $Arg_T(x) = n$.

$Arg_P(x) = (qt(8, x - 11))_0$: If x is the Gödel number of a predicate letter A_j^n, then $Arg_P(x) = n$.

(3) Gd(x) : x is the Gödel number of an expression of K. $EVbl(x) \vee EIC(x) \vee EFL(x) \vee EPL(x) \vee x = 2^3 \vee x = 2^5 \vee x = 2^7 \vee x = 2^9 \vee x = 2^{11} \vee (Eu)_{u<x}(Ev)_{v<x}(x = u*v \wedge Gd(u) \cap Gd(v))$ (Corollary 3.20.)

(4) MP(x, y, z): The expression with Gödel number z is a direct consequence of the expressions with Gödel numbers x and y by modus ponens. $v = 2^3 * x * 2^{11} * z * 2^5 \wedge Gd(x) \wedge Gd(z)$. Here, $*$ is the juxtaposition function defined on p. 144, Example (4).

(5) Gen (x, y): The expression with Gödel number y comes from the expression with Gödel number x by the Generalization Rule. $(Ev)_{v<y}(EVbl(v)$ A $y = 2^3 * 2^3 * v * 2^5 * x * 2^5 \wedge Gd(x))$.

(6) Trm (x): x is the Gödel number of a term of K. This holds when and only when either x is the Gödel number of an expression consisting of a variable or an individual constant or there is a function letter f_k^n and terms $t_1, \ldots,$ t,, such that x is the Gödel number of $f_k^n(t_1, \ldots, t_n)$. The latter holds if and only if there is a sequence of expressions, the last of which having Gödel number x, of the form $f_k^n(f_k^n(t_1, f_k^n(t_1, t_2, \ldots, f_k^n(t_1, t_2, \ldots, t_{n-1}, f_k^n(t_1, \ldots, t_{n-1}, t_n)$. This sequence of n + 1 expressions can be represented by its Gödel number y. Clearly $y < 2^x3^x \cdots p_n^x = (2 \cdot 3 \cdots p_n)^x < (p_n!)^x < (p_x!)^x$. Note that $lh(y) = n + 1$, and also that $n = Arg_T((x)_0)$, since $(x)_0$ is the Gödel number off;. Hence, Trm(x) is equivalent to the following relation.

$$EVbl(x) \vee EIC(x) \vee (Ey)_{y<(p_x!)^x}[x = (y)_{lh(y) \dot{-} 1} \wedge lh(y) = Arg_T((x)_0) + 1 \wedge$$

$$FL(((y)_0)_0) \wedge ((y)_0)_1 = 3 \wedge (u)_{u<lh(y) \dot{-} 2}(Ev)_{v<x}((y)_{u+1}$$

$$= (y)_u * v * 2^7 \wedge Trm(v)) \wedge (Ev)_{v<x}((y)_{lh(y) \dot{-} 1} = (y)_{lh(y) \dot{-} 2} * v * 2^5 \wedge Trm(v))]$$

Thus, Trm(x) is primitive recursive (or recursive), by Corollary 3.20, since the formula above involves Trm(v) only for v < x. In fact, if we replace both occurrences of Trm(v) in the formula by $(z)_v = 0$, then the new formula defines a primitive recursive (or recursive) relation H(x, z), and Trm(x) ≡ H(x, $(C_{Trm})\#$(x)). Therefore, Corollary 3.20 is applicable.

(7) Atfml (x): x is the Gödel number of an atomic wf of K. This holds if and only if there are terms $t_1, \dots, t_n$ and a predicate letter A_k^n such that x is the Gödel number of $A_k^n(t_1, \dots, t_n)$. The latter holds if and only if there is a sequence of expressions, the last of which having Gödel number x, of the form

$$A_k^n(A_k^n(t_1, A_k^n(t_1, t_2, \ldots A_k^n(t_1, t_2, \ldots, t_{n-1}, A_k^n(t_1, \ldots, t_{n-1}, t_n)$$

This sequence of n + 1 expressions can be represented by its Gödel number y. Clearly $y < (p_x!)^x$ (as in (6) above) and $n = \mathrm{Arg}_p((x)_0)$. Hence, Atfml (x) is equivalent to the following relation.

$$(Ey)_{y<(p_x!)^x}[x = (y)_{lh(y) \dot{-} 1} \wedge lh(y) = \mathrm{Arg}_p((x)_0) \wedge PL(((y)_0)_0) \wedge$$
$$((y)_0)_1 = 3 \wedge (u)_{u<lh(y) \dot{-} 2}(Ev)_{v<x}((y)_{u+1} = (y)_u * v * 2^7 \wedge \mathrm{Trm}(v)) \wedge$$
$$(Ev)_{v<x}((y)_{lh(y) \dot{-} 1} = (y)_{lh(y) \dot{-} 2} * v * 2^5 \wedge \mathrm{Trm}(v))]$$

Hence, by Proposition 3.17, Atfml (x) is primitive recursive (or recursive).

(8) Fml (y): y is the Gödel number of a wf of K.

$$\mathrm{Atfml}\ (y) \vee (Ez)_{z<y}[(\mathrm{Fml}\ (z) \wedge y = 2^3 * 2^9 * z * 2^5) \vee$$
$$(\mathrm{Fml}((z)_0) \wedge \mathrm{Fml}((z)_1) \wedge y = 2^3 * (z)_0 * 2^{11} * (z)_1 * 2^5) \vee$$
$$(\mathrm{Fml}((z)_0) \wedge E\mathrm{Vbl}((z)_1) \wedge y = 2^3 * 2^3 * (z)_1 * 2^5 * (z)_0 * 2^5)]$$

As an exercise, check that Corollary 3.20 is now applicable.

(9) (a) Subst (x, y, u, v): x is the Gödel number of the result of substituting in the expression with Gödel number y the term with Gödel number u for all free occurrences of the variable with Gödel number v.

$$\mathrm{Gd}(y) \wedge \mathrm{Trm}(u) \wedge \mathrm{Vbl}(v) \wedge [(y = 2\ \ \wedge x = u)\ V$$
$$(Ew)_{w<y}(y = 2^w \wedge y \neq 2^v \wedge x = y) \vee$$
$$(Ez)_{z<y}(Ew)_{w<y}(\mathrm{Fml}(w) \wedge y = 2^3 * 2'\ \ * 2^5 * w * z \wedge$$
$$(E\alpha)_{\alpha<x}(x = 2^3 * 2\ \ * 2^5 * w * a \wedge \mathrm{Subst}\ (a, z, u, v))) \vee$$
$$((\sim (Ez)_{z<y}(Ew)_{w<y}(\mathrm{Fml}\ (w) \wedge y = 2^3 * 2^v * 2^5 * w * z)) \wedge$$
$$(E\alpha)_{\alpha<x}(E\beta)_{\beta<x}(Ez)_{z<y}(1 < z\ A\ y = (y)_0 *_z A\ x = \alpha * \beta\ A$$
$$\mathrm{Subst}\ (\alpha, (y)_0, u, v)\ A\ \mathrm{Subst}\ (8, z, u, v)))]$$

Check that Corollary 3.20 is applicable.

(b) Sub (y, u, v): the Gödel number of the result of substituting the term with Gödel number u for all free occurrences in the expression with Gödel number y of the variable with Gödel number v. Then Sub(y, u, v) = $\mu x_{x<(p_{uy}!)^{uy}}$ Subst (x, y, u, v), and, therefore, Sub is primitive recursive (or recursive) by Proposition 3.17.

(10) (a) Fr(u, x): u is the Gödel number of a wf or a term of K which contains the variable with Gödel number x free.

$$(\mathrm{Fml}(u) \vee \mathrm{Trm}(u)) \wedge \mathrm{Vbl}(x) \wedge \sim \mathrm{Subst}(u, u, 2^{5+8x}, x)$$

(That is, substitution in the wf with Gödel number u of a variable different from that with Gödel number x for all free occurrences of the variable with Gödel number x yields a different expression.)

(b) Fr_1(u, v, w): u is the Gödel number of a term which is free for the variable with Gödel number v in the wf with Gödel number w.

$$\mathrm{Trm}(u) \wedge \mathrm{Vbl}(v) \wedge \mathrm{Fml}(w) \wedge [\mathrm{Atfml}(w) \vee (Ey)_{y<w}(w = 2^3 * 2^9 * y * 2^5 \wedge$$
$$\mathrm{Fr}_1(u, v, y)) \vee (Ey)_{y<w}(Ez)_{z<w}(w = 2^3 * y * 2^{11} * z * 2^5 \wedge$$
$$\mathrm{Fr}_1(u, v, y)\ A\ \mathrm{Fr}_1(u, v, z))\ V\ (Ey)_{y<w}(Ez)_{z<w}(w = 23 * 2^3 * 2^z * 2^5 * {}^y * 2^5$$
$$\wedge \mathrm{Vbl}(z) \wedge (z \neq v\ 3\ \mathrm{Fr}_1(u, v, y)\ A\ (\mathrm{Fr}(u, z) \supset \sim \mathrm{Fr}(y, v))))]$$

Use Corollary 3.20 again.

(11) (a) Ax_1(x): x is the Gödel number of an instance of Axiom Schema (1).

$$(Eu)_{u<x}(Ev)_{v<x}(\mathrm{Fml}(u) \wedge \mathrm{Fml}(v) \wedge x = 2^3 * u * 2^{11} * 2^3 * v * 2^{11} * a * 2^5 * 2^5)$$

(b) Ax_2(x): x is the Gödel number of an instance of Axiom Schema (2).

$$(Eu)_{u<x}(Ev)_{v<x}(Ew)_{w<x}(\mathrm{Fml}(u)\ A\ \mathrm{Fml}(v)\ A\ \mathrm{Fml}(w)\ A\ x = 2^5\ 2^3 * 2^3 * u * 2^{11} * 2^3 * v * 2^{11} * w * 2^5 * 2^5 * 2^{11} * 2^3 * 2^3 * u * 2^{11} * v * 2^5 * 2^{11} * 2^3 * u * 2^{11} * w * 2^5 * 2^5 * 2^5)$$

(c) Ax_3(x): x is the Gödel number of an instance of Axiom Schema (3).

$$(Eu)_{u<x}(Ev)_{v<x}(\mathrm{Fml}(u)\ n\ \mathrm{Fml}(v)\ A\ x = 2^3 2^5\ 2^3 2^{11} 2^3 * 2^9 * v * 2^5 * 2^{11} * v * 2^5 * 2^3 * 2^9 * v * 2^5 * 2^5 * 2^{11} * 2^3 * 2^3 * 2^3 * 2^9 * v * 2^5 * 2^{11} * u * 2^5 * 2^{11} * v * 2^5 * 2^5)$$

(d) Ax_4(x): x is the Gödel number of an instance of Axiom Schema (4).

$$(Eu)_{u<x}(Ev)_{v<x}(Ey)_{y<x}(\mathrm{Fml}(y)\ A\ \mathrm{Trm}(u)\ A\ \mathrm{Vbl}(v)\ A\ \mathrm{Fr}_3(u, v, y)\ A\ x = 2^3 * 2^3 * 2^3 * 2^v * 2^5 * y * 2^5 * 2^{11} * \mathrm{Sub}(y, u, v) * 2^5)$$

(e) Ax_5(x): x is the Gödel number of an instance of Axion Schema (5).

$$(Eu)_{u<x}(Ev)_{v<x}(Ew)_{w<x}(\mathrm{Fml}(u) \wedge \mathrm{Fml}(w) \wedge \mathrm{Vbl}(v) \wedge \sim \mathrm{Fr}(u, v) \wedge x = 2^3 * 2^3 * 2^3 * 2^v * 2^5 * 2^3 * u * 2^{11} * w * 2^5 * 2^5 * 2^{11} * 2^3 * u * 2^{11} * 2^3 * 2^3 * 2^v * 2^5 * w * 2^5 * 2^5 * 2^5)$$

(f) LAX(y): y is the Gödel number of a logical axiom.

$$\mathrm{Ax}_1(y) \vee \mathrm{Ax}_2(y) \vee \mathrm{Ax}_3(y) \vee \mathrm{Ax}_4(y) \vee \mathrm{Ax}_5(y)$$

Remark. The assumptions (a)–(c) of Proposition 3.25 hold for a first-order theory K which has only a finite number of individual constants, function letters, and predicate letters, since, in that case, IC(x), FL(x), and PL(x) are primitive recursive. For example, if the individual constants of K are a,,, a_{j_2}, . . . , a_{j_n}, then IC(x) if and only if $x = 7 + 8j_1 \vee x = 7 + 8j_2 \vee \cdots \vee x = 7 + 8j_n$. In particular, the assumptions (a)–(c) hold for S.

PROPOSITION 3.26. If a first-order theoty K not *only* satisfies *assumptions* (a)–(c) *of* Proposition 3.25, but also the following assumption:

(d) the property PrAx(y), y is the *Gödel* number of a proper axiom of K, *is* primitive recursiue (or recursiue)

then the *following* relations are primitive recursive (or recursive).

(12) Ax(y): y is the Gödel number of an axiom of K.

$$\mathrm{LAx}(y)\ \mathrm{V}\ \mathrm{PrAx}(y)$$

(13) (a) Prf(y): y is the Gödel number of a proof in K. By Corollary 3.20,

$$(Eu)_{u<y}(Ev)_{v<y}(Ez)_{z<y}(Ew)_{w<y}([y = 2^w \text{ A } \mathrm{Ax}(w)] \vee$$
$$[\mathrm{Prf}(u) \text{ A } \mathrm{Fml}((u)_w) \text{ A } y = u * 2^v \text{ A } \mathrm{Gen}((u)_w, v)]\ \mathrm{V}$$
$$[\mathrm{Prf}(u) \vee \mathrm{Fml}((u)_z) \text{ A } \mathrm{Fml}((u)_w) \text{ A } y = u * 2^v \wedge \mathrm{MP}((u)_z, (u),, \ v)] \vee$$
$$[\mathrm{Prf}(u) \text{ A } y = u * 2 \ \wedge \mathrm{Ax}(v)])$$

which is equivalent to Prf(y), is primitive recursive (or recursive).

(b) Pf(y, x): y is the Gödel number of a proof of the wf with Gödel number x. Pf(y, x) is equivalent to $\mathrm{Prf}(y) \wedge x = (y)_{\mathrm{lh}(y) \dot{-} 1}$.

Notice that S satisfies assumption (d) of Proposition 3.26. Let a,, a_2, . . . , $a_{\circ}$ be the Gödel numbers of Axioms (S1)–(S8). It is easy to see that a number u is the Gödel number of an instance of Axiom Schema (S9) if and only if

$$(Ev)_{v<u}(Ey)_{y<u}(\mathrm{Vbl}(v) \wedge \mathrm{Fml}(y) \wedge u = 2^3 * \mathrm{Sub}(y, 2^{15}, v) * 2^{11} * 2^3 * 2^3 * 2^3$$
$$* 2^v * 2^5 * 2^3 * y * 2^{11} * \mathrm{Sub}(y, 2^{57} * 2^3 * 2^v * 2^5, v) * 2^5 * 2^5$$
$$* 2^{11} * 2^3 * 2^3 * 2^v * 2^5 * 2^5 * y * 2^5 * 2^5).$$

Denote the displayed formula by $A_9(u)$. Then x is the Gödel number of a proper axiom of S if and only if $x = a, \vee x = a, \vee \cdots \vee x = a_8 \vee A_9(x)$. Thus, PrAx(y) is primitive recursive for S.

PROPOSITION 3.27. Let *K* be a theoty having among its symbols *all* the symbols *of S*. If the relations IC, *FL*, and PL of Proposition 3.25 are primitive recursive (or recursive), then (14) and (18) below *are primitive* recursiue (or recursiue). *If*, in addition, the property *PrAx* of Proposition 3.26 *is* primitive recursive (or recursive), then (15)–(17) below are primitive recursive (or recursiue). In particular, for *S* all the functions and relations (1)–(18) are primitive recursiue.

(14) (a) Nu(y): y is the Gödel number of a numeral of **S.**
$y = 2'' \vee (Ex)_{x<y}(\mathrm{Nu}(x) \wedge y = 2^{57} * 2^3 * x * 2^5)$. Use Corollary 3.20.

(b) Num(y) = the Gödel number of $\bar{y}$.

$$\mathrm{Num}(0) = 2^{15}$$
$$\mathrm{Num}(y + 1) = 2^{57} * 2^3 * \mathrm{Num}(y) * 2^5$$

(15) Bw(u, v, x, y): u is the Gödel number of a wf $\mathcal{A}$, v is the Gödel number of free in $\mathcal{A}$, and y is a Gödel number of a proof in K of the wf obtained from $\mathcal{A}$ by substituting the numeral $\bar{x}$ for the free occurrences of the variable with Gödel number v.

$$\mathrm{Fml}(u) \wedge \mathrm{Vbl}(v) \wedge \mathrm{Fr}(u, v) \wedge \mathrm{Pf}(y, \mathrm{Sub}(u, \mathrm{Num}(x), v))$$

(16) Let $\mathcal{A}(x_1, \ldots, x_n)$ be a fixed wf of K containing x,, . . . , x_n as its only free variables, and let m be the Gödel number of $\mathcal{A}(x_1, \ldots, x_n)$. Let $\mathrm{Bw}_{\mathcal{A}}(u_1, \ldots, u_n, y)$ mean: y is the Gödel number of a proof in K of $\mathcal{A}(\bar{u}_1, \ldots, \bar{u}_n)$. Then $\mathrm{Bw}_{\mathcal{A}}(u_1, \ldots, u_n, y)$ is equivalent to:

$$\mathrm{Pf}(y, \mathrm{Sub} \cdot\ .\ \ (\mathrm{Sub}(\mathrm{Sub}(m, \mathrm{Num}(u_1), 5 + 8), \mathrm{Num}(u_2), 5 + 16) \ldots)).$$

(17) (a) $W_1(u, y)$: u is the Gödel number of a wf $\mathcal{A}(x_1)$ containing the free variable x,, and y is the Gödel number of a proof of $\mathcal{A}(\bar{u})$. This is equivalent to:

$$\mathrm{Fml}(u) \wedge \mathrm{Fr}(u, 13) \wedge \mathrm{Pf}(y, \mathrm{Sub}(u, \mathrm{Num}(u), 13)).$$

(b) W,(u, y): u is the Gödel number of a wf $\mathcal{A}(x_1)$ containing the free variable x_1, and y is the Gödel number of a proof of $\sim \mathcal{A}(\bar{u})$. This is equivalent to:

$$\mathrm{Fml}(u) \wedge \mathrm{Fr}(u, 13) \wedge \mathrm{Pf}(y, \mathrm{Sub}(2^3 * 2^9 * u * 2^5, \mathrm{Num}(u), 13)).$$

(18) We wish to define a function D(u) such that, if u is the Gödel number of a wf $\mathcal{A}(x_1)$ with free variable x,, then D(u) is the Gödel number of $\mathcal{A}(\bar{u})$. Let D(u) = Sub(u, Num(u), 13).

The relations and functions of Propositions 3.25–3.27 which relate to the system S should have the subscript "S" attached to the corresponding signs to indicate the dependence upon S. If we were considering another first-order theory S′ with the same symbols as S, then, in general, we would obtain different relations and functions in Propositions 3.25–3.27.

PROPOSITION 3.28. Any function $f(x_1, \ldots, x_n)$ which is representable in S is recursiue.

PROOF. Let $\mathcal{A}(x_1, \ldots, x_n, z)$ be a wf of S representing f. Consider natural numbers k,, . . . , k_n. Let $f(k_1, \ldots, k_n) = m$. Then $\vdash_S \mathcal{A}(\bar{k}_1, \ldots, \bar{k}_n, \bar{m})$. Let j be the Gödel number of a proof in S of $\mathcal{A}(k_1, \ldots, k_n, \bar{m})$. Then $\mathrm{Bw}_{\mathcal{A}}(k_1, \ldots, k_n, m, j)$ (cf. Proposition 3.27(16)). So, for any $x_1, \ldots, x_n$, there is some y such that $Bw_{\mathcal{A}}(x_1, \ldots, x_n, (y)_0, (y)_1)$. Then $f(x_1, \ldots, x_n) = (\mu y(Bw_{\mathcal{A}}(x_1, \ldots, x_n, (y)_0, (y)_1)))_0$. By Proposition 3.27(16), $Bw_{\mathcal{A}}$ is primitive recursive. Hence, by the μ-operator Rule (VI), $\mu y(Bw_{\mathcal{A}}(x_1, \ldots,$ %, $(y)_0, (y)_1))$ is recursive, and, therefore, so is f.

Proposition 3.28, together with Proposition 3.23, shows that the class of recursive functions is identical with the class of functions representable in S. In Chapter 5, it will be made plausible that the notion of recursive function is a precise mathematical equivalent of the intuitive idea of effectively computable function.

COROLLARY 3.29. A number-theoretic relation $R(x_1, \ldots, x_n)$ is recursiue *if* and only *f* $R(x_1, \ldots, x_n)$ is expressible in S.

PROOF. R is recursive if and only if C_R is recursive, by definition. R is expressible in S if and only if C_R is representable in S, by Proposition 3.12.

5. Gödel's Theorem for S

Let K be any theory with the same symbols as S. Then K is said to be o-consistent if and only if, for every wf $\mathcal{A}(x)$ of K, if $\vdash_K \mathcal{A}(\bar{n})$ for every natural number n, then it is not the case that $\vdash_K (Ex) \sim \mathcal{A}(x)$. If we accept the standard interpretation as a model of S, then S is ω-consistent, but we shall always explicitly state the assumption that S is w-consistent whenever it is used in a proof (compare the remarks about consistency on p. 126).

PROPOSITION 3.30. *If* K is o-consistent, then K is consistent.

PROOF. Assume K o-consistent. Consider any wf $\mathcal{A}(x)$ which is provable in K, e.g., $x = x \supset$ x = x. In particular, $\vdash_K \bar{n} =$ ii 3 ii $= \bar{n}$ for all natural numbers n. Hence, (Ex) $\sim$ (x $= x \supset$ x = x) is not provable in K. Therefore, K is consistent (since, by the tautology $\sim A \supset (A \supset B)$, if K were inconsistent, every wf would be provable in K).

By Proposition 3.27, (17a), the relation $W_1(u, y)$ is primitive recursive and so, by Corollary 3.24, W, is expressible in S by a wf $\mathcal{W}_1(x_1, x_2)$ with two free variables x_1, x_2, i.e., if $W_1(k_1, k_2)$, then $\vdash_s \mathcal{W}_1(\bar{k_1}, \bar{k_2})$, and, if not-$W_1(k_1, k_2)$, then $\vdash_s \sim \mathcal{W}_1(\bar{k_1}, \bar{k_2})$. Let us consider the wf

(✠) $(x_2) \sim \mathcal{W}_1(x_1, x_2)$

Let m be the Gödel number of the wf (✠). Substitute iii for x_1 in (✠) to obtain the closed wf

(✠✠) $(x_2) \sim \mathcal{W}_1(\bar{m}, x_2)$

Remember that $W_1(u, y)$ holds if and only if u is the Gödel number of a wf $\mathcal{A}(x_1)$ containing the free variable x_1, and y is the Gödel number of a proof in S of $\mathcal{A}(\bar{u})$. Now, m is the Gödel number of (✠), and (✠Q) comes from (✠) by substituting $\bar{m}$ for the variable $x_,$. Hence,

(I) $W_1(m, y)$ holds if and only if y is the Gödel number of a proof in S of (✠✠).

PROPOSITION 3.31 (Gödel's Theorem for S [1931]).

(1) *If* S is consistent, then the wf (✠✠) is not provable in S.

(2) *If* S is w-consistent, then the wf $\sim$ (✠✠) is not provable in S.

(*Hence*, by Proposition 3.30, if S is o-consistent, the closed wf (✠✠) is neither *provable* nor disprovable in S. Such a closed wf is said to be an undecidable sentence of S.)

PROOF.

(1) Assume S consistent, and assume that $\vdash_S (x_2) \sim \mathcal{W}_1(\bar{m}, x_2)$. Let k be the Gödel number of a proof in S of this wf. By (I) above, $W_1(m, k)$. Since $\mathcal{W}_1$ expresses W_1 in S, we have $\vdash_S \mathcal{W}_1(\bar{m}, \bar{k})$. From $(x_2) \sim \mathcal{W}_1(\bar{m}, x_2)$, by Rule A4, we deduce $\sim \mathcal{W}_1($iii$, \bar{k})$. Thus, $\mathcal{W}_1($iii$, \bar{k})$ and $\sim \mathcal{W}_1($iii$, \bar{k})$ are provable in S, contradicting the consistency of S.

(2) Assume S o-consistent, and assume that $\vdash_S \sim (x_2) \sim \mathcal{W}_1(\bar{m}, x_2)$, i.e., $\vdash_S \sim$ (QQ). By Proposition 3.30, S is consistent, so that not-$\vdash_S$(✠Q). Therefore, for every natural number n, n is not the Gödel number of a proof in S of (✠✠), i.e., by (I), for every n, $W_1(m, n)$ is false. So, for every n, $\vdash_S \sim \mathcal{W}_1(\bar{m},$ ii). If we let $\mathcal{A}(x_2)$ be $\sim \mathcal{W}_1(\bar{m}, x_2)$, then, by the w-consistency of S, it follows that not-$\vdash_S (Ex_2)$ ---- %,(iii, x,); hence, not-$\vdash_S (Ex_2)\mathcal{W}_1(\bar{m}, x_2)$. But this contradicts our assumption that $\vdash_S (Ex_2)\mathcal{W}_1(\bar{m}, x_2)$.

The standard interpretation of the undecidable sentence (✠✠): (x_2) ‒ $\mathcal{W}_1(\bar{m}, x_2)$ is rather remarkable. Since $\mathcal{W}_1$ expresses the relation W, in S, (✠✠) states, according to the standard interpretation, that $W_1(m, x_2)$ is false for every natural number x,. Now, by (I), this means that there is no proof in S of (✠✠). In other words, (✠✠) affirms its own unprovability in S.† Now, by Gödel's Theorem, if S is consistent, then (QQ) is, in fact, unprovable in S, and so, (✠✠) is true under the standard interpretation. Thus, (✠✠) is true for the natural numbers according to the usual interpretation, but is unprovable in S. This might lead us to believe that Gödel's Theorem holds only because the axiom system S that we initially chose just happens to be too weak and that, if we strengthen S by adding new axioms, then the new system might be complete. For example, we might add the true wf (✠✠) to S to obtain a stronger axiom system S_1. However, every recursive function, being representable in S, is also representable in S,; likewise, Propositions 3.25–3.27 obviously hold when S_1 is substituted everywhere for S. But this is all we need for the derivation of Gödel's result; hence, if S_1 is o-consistent, then S_1 also has an undecidable statement $\mathcal{B}$. ($\mathcal{B}$ is of the form $(x_2) \sim (\mathcal{W}_1)_{S_1}(\bar{k}, x_2)$, but, of course, $\mathcal{B}$ will be different from (✠✠), since the relation W, for S, is different from the relation W_1 for S, and hence the wf $(\mathcal{W}_1)_{S_1}$ and the numeral $\bar{k}$ entering into $\mathcal{B}$ are different from $\mathcal{W}_1$ and the numeral $\bar{m}$ of (QQ).)

†Thus, (✠✠) is an analogue of the Liar Paradox (cf. Wang [1955]).

EXERCISES

3.39. Let S_g be the extension of S obtained by adding $\sim$(✠✠) as a new axiom. Show that, if S is consistent, then S_g is consistent and ω-inconsistent.

3.40. A theory K having the same symbols as S is said to be w-incomplete if there is a wf $\mathcal{A}(x)$ such that $\vdash_K \mathcal{A}(\bar{n})$ for all non-negative integers n, but it is not the case that $\vdash_K (x)\mathcal{A}(x)$. Show that, if S is consistent, then S is w-incomplete.

3.41. Prove that w-inconsistency implies ω-incompleteness for consistent theories.

3.42. Using the "fact" that every theorem of S is true in the standard model, and that, according to the standard interpretation, (✠9) says that (99) is unprovable in S, prove that (✠✠) is undecidable in S.

Gödel's Theorem involves the assumption of ω-consistency, but, as Rosser [1936b] has shown, at the cost of complicating the argument we need only assume consistency.

In Proposition 3.27, (17b), the relation $W_2(u, y)$ was shown to be primitive recursive, and so, by Corollary 3.24, W_2 is expressible in S by a wf $\mathcal{W}_2(x_1, x_2)$. Now, consider the wf

$$(\P)\quad (x_2)(\mathcal{W}_1(x_1, x_2) \supset (Ex_3)(x_3 \leqslant x_2 \mathrm{\ A\ } \mathcal{W}_2(x_1, x_3)))$$

Let n be the Gödel number of (7). Substitute $\bar{n}$ for x_1 in (¶) to obtain the closed wf

$$(\P\P)\quad (x_2)(\mathcal{W}_1(\bar{n}, x_2) \supset (Ex_3)(x_3 \leqslant x_2 \mathrm{\ A\ } \mathcal{W}_2(\bar{n}, x_3)))$$

Notice that $W_1(u, y)$ (respectively, $W_2(u, y)$) holds if and only if u is the Gödel number of a wf $\mathcal{A}(x_1)$ containing the free variable x,, and y is the Gödel number of a proof in S of $\mathcal{A}(\bar{u})$ (respectively, $\sim \mathcal{A}(\bar{u})$). Since n is the Gödel number of (¶), we have:

(II) $W_1(n, y)$ holds if and only if y is the Gödel number of a proof in S of (¶¶).
(III) $W_2(n, y)$ holds if and only if y is the Gödel number of a proof in S of $\sim$(¶¶).

PROPOSITION 3.32 (GÖDEL-ROSSER THEOREM [1936b]). *If* S is consistent, then (¶¶) and $\sim$(¶¶) are both unprovable in S; hence, S contains an undecidable sentence.

PROOF. Assume S consistent.

(1) Assume (¶¶) provable in S, i.e., $\vdash_S (x_2)(\mathcal{W}_1(\bar{n}, x_2) \supset (Ex_3)(x_3 \leqslant x_2 \wedge \mathcal{W}_2(\bar{n}, x_3)))$. Let k be the Gödel number of a proof in S of (¶¶). By (II), $W_1(n, k)$. Since $\mathcal{W}_1$ expresses W_1 in S, $\vdash_S \mathcal{W}_1(\bar{n}, \bar{k})$. But, from (¶¶), we obtain by Rule A4, $\vdash_S \mathcal{W}_1(\bar{n}, \bar{k}) \supset (Ex_3)(x_3 \leqslant \bar{k} \mathrm{\ A\ } \mathcal{W}_2(\bar{n}, x_3))$, and then by MP, $\vdash_S (Ex_3)(x_3 \leqslant \bar{k} \wedge \mathcal{W}_2(\bar{n}, x_3))$. Now, since S is consistent, and $\vdash_S$(¶¶), it follows that there is no proof in S of $\sim$(¶¶). So, by (III), $W_2(n, y)$ is false for all natural numbers y. Since $\mathcal{W}_2$ expresses W_2 in S, $\vdash_S - \mathcal{W}_2(\bar{n}, \bar{j})$ for every natural number j. In particular, we deduce $\vdash_S \sim \mathcal{W}_2(\bar{n}, 0) \wedge \sim \mathcal{W}_2(\bar{n}, \bar{1}) \wedge \cdots \wedge \sim \mathcal{W}_2(\bar{\bar{n}}, \bar{k})$.

Hence, by Proposition 3.8(a′), $\vdash_S (x_3)(x_3 \leqslant \bar{k} \supset - \mathcal{W}_2(\bar{n}, x_3))$, and so, $\vdash_S \sim (Ex_3)(x_3 \leqslant \bar{k} \wedge \mathcal{W}_2(\bar{n}, x_3))$ by the Replacement Theorem (Corollary 2.2 1). But this is the negation of a wf we have already derived above, contradicting the consistency of S.

(2) Assume $\vdash_S \sim$(¶¶), i.e., $\vdash_S \sim (x_2)(\mathcal{W}_1(\bar{n}, x_2) \supset (Ex_3)(x_3 \leqslant x_2 \mathrm{\ A\ } \mathcal{W}_2(\bar{n}, x_3)))$. Let r be the Gödel number of a proof of $\sim$(¶¶). By (III), $W_2(n, r)$; therefore, $\vdash_S \mathcal{W}_2(\bar{n}, \bar{r})$. Since S is consistent, there is no proof in S of (¶¶), i.e., by (II), W;(n; y) is false for all natural numbers y. Hence, $\vdash_S \sim \mathcal{W}_1(\bar{n}, \bar{j})$ for all natural numbers j. In particular,

$$\vdash_S \sim \mathcal{W}_1(\bar{n}, 0) \wedge \sim \mathcal{W}_1(\bar{n}, \bar{1}) \wedge \cdots \wedge \sim \mathcal{W}_1(\bar{n}, \bar{r})$$

Then, by Proposition 3.8(a′),

(i) $\vdash_S x_2 \leqslant \bar{r} \supset \sim \mathcal{W}_1(\bar{n}, x_2)$. On the other hand, consider the following deduction.

(1)	$\bar{r} \leqslant x_2$	Hyp
(2)	$\mathcal{W}_2(\bar{n}, \bar{r})$	Already proved above
(3)	$\bar{r} \leqslant x_2 \wedge \mathcal{W}_2(\bar{n}, \bar{r})$	(1), (2), Tautology
(4)	$(Ex_3)(x_3 \leqslant x_2 \mathrm{\ A\ } \mathcal{W}_2(\bar{n}, x_3))$	(3), Rule E4

From (1)–(4), by the Deduction Theorem, we obtain

(ii) $\vdash_S \bar{r} \leqslant x_2 \supset (Ex_3)(x_3 \leqslant x_2 \wedge \mathcal{W}_2(\bar{n}, x_3))$

But, by Proposition 3.7(p),

(iii) $\vdash_S x_2 \leqslant \bar{r} \vee \bar{r} \leqslant x_2$

Now. from (i)–(iii), we obtain, by the appropriate tautology,

$$\vdash_S \sim \mathcal{W}_1(\bar{n}, x_2) \vee (Ex_3)(x_3 \leqslant x_2 \wedge \mathcal{W}_2(\bar{n}, x_3))$$

and then by a tautology, MP and Gen,

$$\vdash_S (x_2)(\mathcal{W}_1(\bar{n}, x_2) \supset (Ex_3)(x_3 \leqslant x_2 \mathrm{\ A\ } \mathcal{W}_2(\bar{n}, x_3)))$$

Thus, $\vdash_S$(¶¶). But, since $\vdash_S \sim$(¶¶) has been assumed, this contradicts the consistency of S.

Rosser's undecidable sentence (¶¶) also has an interesting standard interpretation. By (II) and (III), $W_1(n, x_2)$ means that x_2 is the Gödel number of a proof in S of (IT), and $W_2(n, x_3)$ means that x_3 is the Gödel number of a proof in S of $\sim$(¶¶). Thus, (¶¶) asserts that, if there is a proof in S of (¶¶), then there is a proof in S, with even a smaller Gödel number, of $\sim$(¶¶). Now, Proposition 3.32 shows that, if S is consistent, then (¶¶) is not provable; therefore, if S is consistent, (¶¶) is true under the standard interpretation.

The application of the Godel-Rosser Theorem is not limited to S. Let K be any first-order theory with the same symbols as S. If we analyze the proof above, we obtain the following sufficient conditions for the applicability of the Gödel-Rosser Theorem to K.

(a) The relations W_1 and W_2 (cf. Proposition 3.27(17); replace S everywhere by K in the definitions) should be expressible in K.

(b) There is a wf $u \leqslant v$ such that

(i) for any wf $\mathscr{A}(x)$ and any natural number k,

$$\vdash_K \mathscr{A}(0) \wedge \mathscr{A}(\bar{1}) \wedge \cdots \wedge \mathscr{A}(\bar{k}) \supset (x)(x \leqslant \bar{k} \supset \mathscr{A}(x))$$

(ii) and for any natural number k,

$$\vdash_K x \leqslant \bar{k} \vee \bar{k} \leqslant x$$

Notice that, if K is a theory with equality, then (i) may be replaced by (i'): $\vdash_K x \leqslant \bar{k} \supset (x = 0 \vee x = 1 \vee \cdots \vee x = \bar{k})$.

The condition (a) that W, and W_2 be expressible in K will be satisfied if W, and W_2 are recursive and every recursive relation is expressible in K. From the proofs of Proposition 3.25–3.27, it is obvious that W, and W_2 will be recursive if the assumption (d) of Proposition 3.26 holds for K, i.e., if the property $PrAx_K$ of being a Gödel number of a proper axiom of K is recursive (or, in other words, if the set of Gödel numbers of proper axioms of K is recursive). Thus, we have the following result.

PROPOSITION 3.33. Let **K** be a theory hauing the same symbols as S. Assume also that the following conditions holdfor K.

(1) Every recursive relation is expressible in K.
(2) The set $PrAx_K$ of *Gödel* numbers of proper *axioms* of K is *recursive.*
(3) Conditions (b), (i)–(ii) *above*, hold.

Then the Godel-Rosser Theorem holds for K, *i.e.*, *if* K is consistent, then K *has* an undecidable sentence. (Observe that (1) holds if every recursive function is representable in K, by Proposition 3.12; condition (i) of (3) can be replaced by (i') above if K is a first-order theory with equality.)

Let us call a theory K *recursively* axiomatizable if and only if there is a theory K′ having the same theorems as K such that the set $PrAx_{K'}$ of Gödel numbers of proper axioms of K' is recursive.

COROLLARY 3.34. *Every* consistent *recursively* axiomatizable extension of S is subject to the *Gödel-Rosser* Theorem, and therefore has an undecidable sentence.

PROOF. Since all recursive relations are expressible in S, they are also expressible in any extension of S. Likewise, since conditions (i)–(ii) hold in S, they also hold in any extension of S. So, by Proposition 3.33, the Godel-Rosser Theorem applies to any consistent recursively axiomatizable extension of S.

An *effectively* decidable set of objects is a set for which there is a prescribed mechanical procedure which determines, for any given object, whether or not that object belongs to the set. A mechanical procedure is one which is carried out automatically without any need for originality or ingenuity in its application. It will appear plausible after Chapter 5 that the precise notion of a recursive set corresponds to the intuitive idea of an effectively decidable set of natural numbers. This hypothesis is known as Church's Thesis.

EXERCISE 3.43. *Sometimes* Church's Thesis is taken in the form that a *number-theoretic* function is *effectively* computable *if* and only *if* the function is *recursive.* Prove that this is equivalent to the form of Church's Thesis giuen *above.*

Remember that a theory is said to be axiomatic if the set of its axioms is effectivelydecidable. If we accept Church's Thesis, Corollary 3.34 asserts that S is essentially incomplete, i.e., that every consistent axiomatic extension of S has an undecidable sentence.

EXERCISES

3.44. Prove that the set Tr of Gödel numbers of all wfs of S which are true in the standard model is not recursive.

3.45. From Corollary 3.34, prove that there is no recursively axiomatizable theory having Tr as the set of Gödel numbers of its theorems.

3.46. Let K be a theory with equality satisfying conditions (b), (i)–(ii) (p. 162), and such that every recursive relation is expressible in K. Prove that every recursive function is representable in K.

Let $Neg(x) = 2^3 * 2^9 * x * 2^5$. Then if x is the Gödel number of a wf $\mathscr{A}$, Neg(x) is the Gödel number of $(\sim \mathscr{A})$. Clearly Neg is recursive, and, hence, is representable in S by a wf $\mathfrak{Neg}(x_1, x_2)$. Remember that Pf(y, x) is the relation which holds when and only when x is the Gödel number of a wf $\mathscr{A}$ of S and y is the Gödel number of a proof in S of $\mathscr{A}$. By Proposition 326. Pf is primitive recursive; hence, by Corollary 3.24, Pf is expressible in S by some wf $\mathfrak{Pf}(x_1, x_2)$.

Let Con_S be the wf:

$$(x_1)(x_2)(x_3)(x_4) \sim (\mathfrak{Pf}(x_1, x_3) \wedge \mathfrak{Pf}(x_2, x_4) \wedge \mathfrak{Neg}(x_3, x_4)).$$

Intuitively, according to the standard interpretation, Con_S asserts that there is no proof in S of any wf and its negation, and this is true if and only if S is consistent. Thus, Con_S can be interpreted as asserting the consistency of S. Now, Gödel's undecidable sentence (✠✠) (cf. p. 158) means, according to the standard interpretation, that (✠✠) is not provable in S. Hence, the wf $Con_S \supset$ (✠✠) asserts that if S is consistent, then (✠✠) is not provable in S. But this is just the first half of Gödel's Theorem. The metamathematical reasoning used in Gödel's Theorem can be expressed and carried through within S itself, so that one obtains a proof in S of $Con_S \supset$ (✠✠). (For a proof of this assertion, see Hilbert-Bernays [1939], pages 285–328; Feferman [1960].) Thus, $\vdash_S Con_S \supset$

(✠✠). But, by Gödel's Theorem, if S is consistent, then (✠✠) is unprovable in S. Therefore, if S is consistent, then Con, is unprovable in S, i.e., if S is consistent, a wf which asserts the consistency of S is unprovable in S. This is *Gödel's Second Theorem* [1931]. One can very roughly paraphrase it by stating that if S is consistent, the consistency of S cannot be proved within S; or, equivalently, a consistency proof of S must use ideas and methods which go beyond those available in S. In fact, the consistency proofs for S given by Gentzen [1936, 1938] and Schütte [1951] do employ notions and methods (e.g., a portion of the theory of denumerable ordinal numbers) that apparently are not formalizable in S.

We can state Gödel's Second Theorem approximately as follows: If Con_K is an arithmetization of the statement that the theory K is consistent (where K is a possessing the symbols of S), then, if K is sufficiently strong and consistent, Con_K is not provable in K. Actually, the theorem applies to much general theories (not necessarily first-order). Aside from the vagueness due to the phrase "sufficiently strong" (which can be made precise without much the way in which Con, is constructed also adds an element of This ambiguity is dangerous, because, as Feferman has shown (Feferman [1960], Corollary 5.10), there is a way of defining Con_S so that $\vdash_S Con_S$. Therefore, it is necessary to make the statement of the theorem more precise. This has been done by Feferman [1960] roughly in the following way.†

For any primitive recursive function $f(x_1, \ldots, x_n)$, we showed in the proof of Proposition 3.23 (pp. 148–151) how to find a wf $\mathscr{A}(x_1, \ldots, x_n, y)$ representing f in S. The wfs $\mathscr{A}(x_1, \ldots, x_n, 0)$ obtained in this way are called *PR-formulas*. A wf $\mathscr{B}$ is said to be an *RE-formula* if, and only if, for some PR-formula Q,, $\mathscr{B}$ is of the form $(Ey_1) \ldots (Ey_k)\mathscr{A}$ (with $k \geqslant 0$). In particular, every PR-formula is an RE-formula. If we think of a given wf $\mathscr{A}(x)$ as representing the theory K, the axioms of which are those wfs whose Gödel numbers satisfy $\mathscr{A}$, then we can a proof predicate for K as follows: $Prf_{\mathscr{A}}(y, x)$ is the wf obtained from $= (y)_{lh(y)-1} \wedge y > 1 \wedge (z)(z < lh(y) \supset (Fml((y)_z)) \wedge (LAx((y)_z) \vee \vee (Ev)(Ew)(v < z \wedge w < z \wedge (MP((y)_v, (y)_w, (y)_z) \vee Gen((y)_v, (y)_z)))))$, by all the primitive recursive functions and predicates by the wfs which represent or express them. (For example, if $\mathscr{C}(u, v)$ represents lh(y), then $z < lh(y)$ is replaced by $(Ev)(\mathscr{C}(y, v)$ A $z <$ u).) The wf $Prf_{\mathscr{A}}(y, x)$ expresses in S the relation that y is the Gödel number of a proof in the theory K of a wf having Gödel number x. (See pp. 143, 153–154 for definitions of the relations and functions Fml, lh, $(y)_v$, Gen, MP appearing in B e formula above.) We now can construct a wf corresponding to the notion of a theorem of K: Let $Pr_{\mathscr{A}}(x)$ stand for $(Ey)Prf_{\mathscr{A}}(y, x)$. We then can construct a wf expressing the consistency of K: $Con_{\mathscr{A}}$ for $(x)(Fml(x) \supset \sim Pr_{\mathscr{A}}(x) \vee (Ey)(\mathfrak{Neg}(x, y) \wedge \sim Pr_{\mathscr{A}}(y)))$. One of the consequences of Feferman's work is the following precise version of Gödel's

†For further clarification and development of Gödel's Second Theorem, cf. Jeroslow [1971, 1972, 1973].

Second Theorem: Let K be a consistent extension of S. Let K_1 be any theory such that K is an extension of K_1 and K_1 is an extension of Robinson's system (In particular, K_1 may be S or K itself.) Let T_K be the set of Gödel numbers of theorems of K, and assume that $\mathscr{A}(x)$ is an RE-formula which expresses T_K in K_1. Then not-$\vdash_K Con_{\mathscr{A}}$. (The assumption that $\mathscr{A}(x)$ is an RE-formula is shown be necessary by Feferman's proof that there is a wf $\mathscr{B}(x)$ which expresses T_S in S such that $\vdash_S Con_{\mathscr{B}}$.)

6. Recursive Undecidability. Tarski's Theorem. Robinson's System.

Let K be a theory with equality having the same symbols as S. If u is the Gödel number of wf $\mathscr{A}(x_1)$ with free variable x_1, then the function D(u), as defined in Proposition 3.27(18), has as its value the Gödel number of the wf $\mathscr{A}(\bar{u})$. Since $D(u) = Sub(u, Num(u), 13)$, it is clear that D is primitive recursive. Let T_K be the set of Gödel numbers of theorems of K.

PROPOSITION 3.35. *If* K is consistent and the junction D *is representable in* K, *then* T_K *is not* expressible in K.

PROOF. Assume D representable in K and T_K expressible in K. Then there are wfs $\mathscr{D}(x_1, x_2)$ and $\mathscr{T}(x_2)$ such that

(1) If $D(k) = j$, then $\vdash_K \mathscr{D}(\bar{k}, \bar{j})$
(2) $\vdash_K (E_1 x_2)\mathscr{D}(\bar{k}, x_2)$
(3) If k is in T_K, then $\vdash_K \mathscr{T}(\bar{k})$
(4) If k is not in T_K, then $\vdash_K \sim \mathscr{T}(\bar{k})$.

Consider the wf $\mathscr{A}(x_1) : (x_2)(\mathscr{D}(x_1, x_2) \supset \sim \mathscr{T}(x_2))$. Let p be the Gödel number of this wf. Construct the wf $\mathscr{A}(\bar{p})$:

$$(x_2)(\mathscr{D}(\bar{p}, x_2) \supset \sim \mathscr{T}(x_2)).$$

Let q be the Gödel number of $\mathscr{A}(\bar{p})$. Hence, $D(p) = q$. Therefore, by (1), $\vdash_K \mathscr{D}(\bar{p}, \bar{q})$. Now, either $\vdash_K \mathscr{A}(\bar{p})$ or not-$\vdash_K \mathscr{A}(\bar{p})$. If not-$\vdash_K \mathscr{A}(\bar{p})$, then q is not in T_K, and so, by (4), $\vdash_K \sim \mathscr{T}(\bar{q})$. On the other hand, if $\vdash_K \mathscr{A}(\bar{p})$, then $\vdash_K (x_2)(\mathscr{D}(\bar{p}, x_2) \supset \sim \mathscr{T}(x_2))$. Hence, by Rule A4, $\vdash_K \mathscr{D}(\bar{p}, \bar{q}) \supset \sim \mathscr{T}(\bar{q})$; but $\vdash_K \mathscr{D}(\bar{p}, \bar{q})$. Hence, $\vdash_K \sim \mathscr{T}(\bar{q})$. Thus, in both cases, $\vdash_K \sim \mathscr{T}(\bar{q})$. Now, from $\vdash_K \mathscr{D}(\bar{p}, \bar{q})$ and (2), $\vdash_K \mathscr{D}(\bar{p}, x_2) \supset x_2 = \bar{q}$. But, since $\vdash_K \sim \mathscr{T}(\bar{q})$, $\vdash_K x_2 = \bar{q} \supset \sim \mathscr{T}(x_2)$. Hence, $\vdash_K \mathscr{D}(\bar{p}, x_2) \supset \sim \mathscr{T}(x_2)$, and, by Gen, $\vdash_K (x_2)(\mathscr{D}(\bar{p}, x_2) \supset \sim \mathscr{T}(x_2))$, i.e., $\vdash_K \mathscr{A}(\bar{p})$. Therefore, q is in T_K, and, by (3), $\vdash_K \mathscr{T}(\bar{q})$. Since we also have $\vdash_K \sim \mathscr{T}(\bar{q})$, K is inconsistent.

COROLLARY 3.36. *If* K *is consistent and every recursive function is* representable *in* K, *then* T_K *is not* expressible in K. Hence, T_K *is not recursive.*

D is primitive recursive, and, therefore, would be representable in K. By Proposition 3.35, T_K is not expressible in K. By the proof of Proposition 3.12, the characteristic function C_{T_K} is not representable in K. Hence C_{T_K} is not recursive, and so, T_K is not recursive.

We shall say that K is ***recursively undecidable*** if and only if $\mathbf{T_K}$ is not recursive; and K is called ***essentially recursively undecidable*** if and only if K and every consistent extension of K is recursively undecidable. (If we accept Church's Thesis, then recursive undecidability is equivalent to effective undecidability, i.e., non-existence of a mechanical decision procedure for theorernhood. The non-existence of such a mechanical procedure means that ingenuity is required for determining whether any given wf is a theorem.)

COROLLARY 3.37. ***If*** S ***is consistent, then S is essentially recursively undecidable.***

PROOF. If K is any consistent extension of S (possibly S itself), then, since every recursive function is representable in S, the same holds true for K, and, therefore, by Corollary 3.36, $\mathbf{T_K}$ is not recursive.

COROLLARY 3.38 (Tarski's Theorem [1936]). ***The set*** Tr ***of Gödel numbers of*** wfs ***of S which are true in the standard model is not arithmetical, i.e., there is no*** wf $\mathcal{A}(x)$ ***of*** S ***such that*** Tr ***is the set of numbers k for which*** $\mathcal{A}(\bar{k})$ ***is true in the standard model.***

PROOF. Let K be the extension of S having as its axioms all those wfs which are true in the standard model. Then $\mathbf{T_K}$ = Tr. We assume that K is consistent, since it has the standard model. By Corollary 3.36, since every recursive function is representable in K, Tr is not expressible in K. But a relation is expressible in K if and only if it is the standard interpretation of some wf of S. Hence Tr is not arithmetical. (This result can be roughly paraphrased by saying that the notion of arithmetical truth is not arithmetically definable.)

EXERCISES

3.47. (a) If n is the Gödel number of a wf $\mathcal{A}$, let Cl(n) be the Gödel number of the closure of $\mathcal{A}$; otherwise, let Cl(n) = n. Using Proposition 3.25, show that Cl is primitive recursive.

(b) Show that if the theory K is recursively axiomatizable and complete, then K is recursively decidable, i.e., the set $\mathbf{T_K}$ is recursive; or, equivalently, if K is recursively axiomatizable and recursively undecidable, then K is incomplete.

3.48. Show that, if K is not recursively axiomatizable, then K is recursively undecidable.

3.49. (a) (Fixed Point Theorem) Let K be a theory with equality, with the same symbols as S, in which every recursive function is representable. For any wf $\mathcal{A}(x_1)$ of K, show how to construct a sentence 9, with Gödel number k, such that $\vdash_K \mathcal{F} \equiv \mathcal{A}(\bar{k})$. (Intuitively, $\mathcal{F}$ says that "$\mathcal{A}$ is true of me".) Hint: Let the primitive recursive function D(x) be representable in K by the wf $\mathcal{D}(x_1, x_2)$. Construct the wf ($) $(x_2)\,(\mathcal{D}(x_1, x_2) \supset \mathcal{A}(x_2))$. If m is the Gödel number of ($), let $\mathcal{F}$ be $(x_2)\,(\mathcal{D}(\bar{m}, x_2) \supset \mathcal{A}(x_2))$.

(b) Prove Tarski's Theorem (Corollary 3.38) from the Fixed Point Theorem (Part (a)).

(c) Prove that the set Tr is not recursive. (This already has been proved in another manner in Exercise 3.44.) Hence, by Church's Thesis, arithmetical truth is not decidable.

(d) Let K be any recursively axiomatizable theory with equality, with the same symbols as S, such that all theorems of K are true in the standard model, i.e., $\mathbf{T_K} \subseteq$ Tr. Prove that K has an undecidable sentence.

(e) Let K be a consistent theory with equality, with the same symbols as S, in which every recursive function is representable. Let Ref, be the set of Gödel numbers of refutable wfs of K, that is, $\{x|\mathfrak{Neg}(x) \in \mathrm{T_K}\}$. Prove that there is no recursive set A such that $\mathbf{T_K} \subseteq \mathbf{A}$ and $\mathbf{Ref_K} \subseteq \bar{\mathbf{A}}$ (the complement of A).

Robinson's System: Consider the first-order theory with the same symbols as S and having the following finite number of axioms.

(1) $x_1 = x_1$
(2) $x_1 = x_2 \supset x_2 = x_1$
(3) $x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)$
(4) $x_1 = x_2 \supset$ x; = x;
(5) x, = $x_2 \supset$ (x, + $x_3 = x_2 + x_3$ A x, + x, = $x_3 + x_2$)
(6) $x_1 = x_2 \supset (x_1 \cdot x_3 = x_2 \cdot x_3 \wedge x_3 \cdot x_1 = x_3 \cdot x_2)$
(7) $x_1' = x_2' \supset x_1 = x_2$
(8) $0 \neq (x_1)'$
(9) $x_1 \neq 0 \supset (Ex_2)(x_1 = x_2')$
(10) $x_1 + 0 = x_1$
(11) $x_1 + (x_2)' = (x_1 + x_2)'$
(12) $x_1 \cdot 0 = 0$
(13) $x_1 . (x_2)' = (x_1 \cdot x_2) + x_1$
(14) $(x_2 = x_1 \cdot x_3 + x_4 \wedge x_4 < x_1 \wedge x_2 = x_1 \cdot x_6 + x_5 \wedge x_5 < x_1) \supset x_4 = x_5$
(Uniqueness of remainder)

We shall call this theory RR. (The system Q of Axioms (1)–(13) is due to Raphael Robinson [1950]. Axiom (14) has been added to make one of the proofs below easier.) Clearly, RR is a subtheory of S, since all the axioms of RR are theorems of S. In addition, it follows from Proposition 2.26 and Axioms (1)–(6) that RR is a theory with equality.

PROPOSITION 3.39. ***In*** RR, ***the following are theorems.***

(a) ii + iii =$\underline{\text{n +}}$ m ***for any natural numbers m and*** n.
(b) ii . $\overline{\text{m}}$ =n · m ***for any natural numbers*** m ***and*** n.
(c) ii $\neq$ iii *if* n $\neq$ m, ***for any natural numbers*** n ***and*** m.
(d) x $\leqslant$ ii $\supset$ x = 0 $\vee$ x = 1 $\vee$ · . · $\vee$ x = ii ***for any natural number*** n.
(e) x $\leqslant$ ii $\vee$ ii $\leqslant$ x, ***for any natural number*** n.

PROOF. Parts (a)–(c) are proved just as in Proposition 3.6(a). Parts (d) and (e) are proved by induction on n in the metalanguage, making strong use of Axiom (9). The proofs are left as exercises.

EXERCISES

3.50. Show that RR is a proper subtheory of S. Remark: not only is S different from RR, but it is not finitely axiomatizable at all (i.e., there is no theory K having only a finite number of proper axioms, whose theorems are the same as those of S). This has been proved by Ryll-Nardzewski [1953] and Rabin [1961].

3.51. Show that Axiom (14) is not provable from Axioms (1)–(13). (Hint: let ∞ be an object which is not a natural number. Let $\infty' = \infty$, $\infty + x = x + \infty = \infty$ for all x, $\infty \cdot 0 = 0 \cdot \infty = 0$, and $\infty \cdot x = x \cdot \infty = \infty$ for all $x \neq 0$.)

PROPOSITION 3.40. ***Every recursive junction is representable in*** RR.

PROOF. For the initial functions and the rules of substitution and the p-operator, essentially the same proof holds as was given for S in Proposition 3.23. For the recursion rule, inspection of the proof given for Proposition 3.23 shows that it is still valid for RR if we note that, for the wf Bt defined in Proposition 3.21, if $\beta(k_1, k_2, k_3) = m$, then $\vdash_{RR} Bt(\overline{k_1}, \overline{k_2}, \overline{k_3}, \overline{m})$, and also, by Axiom (14), $\vdash_{RR} Bt(u, v, x, y) \wedge Bt(u, v, x, z) \supset y = z$.

EXERCISE 3.52. ***Carry through the details of the proof of Proposition*** 3.40.

We shall take for granted that RR is consistent, since it has the standard interpretation as a model. However, more constructive consistency proofs can be given along the same lines as the proofs in Beth [1959, §84] or Kleene [1952, §79].

PROPOSITION 3.41

(a) RR ***is essentially recursively undecidable.***
(b) RR ***is essentially incomplete.***

PROOF. (a) By Corollary 3.36 and Proposition 3.40. (b) By Propositions 3.33 and 3.40 (or, from (a), by Exercise 3.47(b), p. 166).

Of course, we already had these results for the theory S. The reason that we have gone to the trouble of obtaining them again for RR is that RR is finitely axiomatizable. It can be shown that Proposition 3.40, and therefore also Proposition 3.41, holds for Robinson's system Q (Axioms (1)–(13)). However, the proof for Proposition 3.40 is more complex (cf. Tarski-Mostowski-Robinson [1953], pages 56–59) than the one given above for RR.

Let K, and K_2 be any two theories having the same symbols. K_2 is called a ***finite extension*** of K_1 if and only if there is a set A of wfs and a finite set B of wfs such that (1) the theorems of K, are precisely the wfs derivable from A; (2) the theorems of K_2 are precisely the wfs derivable from A u B.

We say that K_1 and K_2 are *compatible* if and only if the theory K_1 u K_2, the set of axioms of which is the union of the set of axioms of K, and the set of axioms of K_2, is consistent.

PROPOSITION 3.42. ***Let*** K, ***and*** K_2 ***be theories having the same symbols as*** S. ***If*** K_2 ***is a finite extension oj*** K, ***and if*** K_2 ***is recursively undecidable, then*** K_1 ***is also recursively undecidable.***

PROOF. Let A be a set of axioms of K_1, and A U $\{\mathcal{A}_1, \ldots, \mathcal{A}_n\}$ a set of axioms for K_2. We may assume that $\mathcal{A}_1, \ldots, \mathcal{A}_n$ are closed wfs. Then, by the Deduction Theorem, a wf $\mathcal{B}$ is provable in K_2 if and only if $(\mathcal{A}_1 \wedge \ldots \wedge \mathcal{A}_n) \supset \mathcal{B}$ is provable in K,. Let c be a Gödel number of $(\mathcal{A}_1 \wedge \ldots \wedge \mathcal{A}_n)$. Then b is a Gödel number of a theorem of K_2 when and only when $2^3 * c * 2^{11} * b * 2^5$ is a Gödel number of a theorem of K_1, i.e., b is in T_{K_2} if and only if $2^3 * c * 2^{11} * b * 2^5$ is in T_{K_1}. Hence, $C_{T_{K_2}}(x) = C_{T_{K_1}}(2^3 * c * 2^{11} * x * 2^5)$. So, if T_{K_1} were recursive, T_{K_2} would also be recursive, contradicting the recursive undecidability of K_2.

PROPOSITION 3.43. ***Let*** K ***be a theory having the same symbols as*** S. ***If*** K ***is compatible with*** RR, ***then*** K ***is recursively undecidable.***

PROOF. Since K is compatible with RR, the theory K ∪ RR is a consistent extension of RR. Therefore, by Proposition 3.41(a), K u RR is recursively undecidable. But K ∪ RR is a finite extension of K. Hence, by Proposition 3.42, K is recursively undecidable.

COROLLARY 3.44. ***Let*** K ***be a theory with the same symbols as*** S ***such that all the axioms oj*** K ***are true in the standard model. Then*** K ***is recursively undecidable.***

PROOF. K ∪ RR has the standard interpretation as a model, and is, therefore, consistent, i.e., K is compatible with RR. Now apply Proposition 3.43.

COROLLARY 3.45. ***Let*** P_s ***be the predicate calculus having the same symbols as*** S. ***Then*** P_s ***is recursively undecidable.***

PROOF. P_s ∪ RR = RR. Hence, P, is compatible with RR, and, therefore, by Proposition 3.43, recursively undecidable.

By PF we mean the full first-order predicate calculus containing all predicate letters A_j^n, function letters f_j^n, and individual constants a_j. Let PP be the pure first-order predicate calculus containing all predicate letters, but no function letters or individual constants.

LEMMA 3.46. ***There is a recursive junction h such that, for any*** wf $\mathcal{A}$ ***of*** PF ***having Gödel number u, there is a*** wf $\mathcal{A}'$ ***oj*** PP ***having Gödel number*** $h(u)$ ***such that*** $\mathcal{A}$ ***is provable in*** PF if ***and only*** if $\mathcal{A}'$ ***is provable in*** PP.

PROOF. Let & be a wf of PF. With the distinct function letters f_j^n in $\mathcal{A}$, associate distinct predicate letters A_r^{n+1} not occumng in $\mathcal{A}$, and with the distinct individual constants a, in $\mathcal{A}$, associate distinct predicate letters A_k^1 not occurring in $\mathcal{A}$. Find the first individual constant a, in $\mathcal{A}$; let z be the first variable not in $\mathcal{A}$; and let $\mathcal{A}^\star$ result from & by replacing all occurrences of a, in $\mathcal{A}$ by z. Form the wf $\mathcal{A}_1$: $(Ez)A_k^1(z) \supset (Ez)(A_k^1(z) \wedge \mathcal{A}^\star)$, where A_k^1 is the predicate letter associated with a,. It is easy to check (cf. proof of Proposition 2.29) that $\mathcal{A}$ is logically valid if and only if $\mathcal{A}_1$ is logically valid. Keep on performing similar transformations until a wf $\mathcal{B}$ is reached without individual constants such that $\mathcal{A}$ is logically valid if and only if $\mathcal{B}$ is logically valid. Take the left-most term

$f_l^n(t_1, \ldots, t_n)$ in **I**, where $t_1, \ldots, t_n$ do not contain function letters. Let w be the first variable not in **I**, let $\mathcal{B}^*$ result from **I** by replacing $f_l^n(t_1, \ldots, t_n)$ by w, and let $\mathcal{B}_1$ be the wf $(Ew)A_r^{n+1}(w, t,, \ldots, t_n) \supset (Ew)(A_r^{n+1}(w, t_1, \ldots, t_n) \wedge$ **I***), where A_r^{n+1} is the predicate letter corresponding to f_l^n. It is easy to verify that $\mathcal{B}$ is logically valid if and only if $\mathcal{B}_1$ is logically valid. Repeat the same transformation on $\mathcal{B}_1$, etc., until a wf $\mathcal{A}'$ is reached which contains no function letters. Then $\mathcal{A}'$ is a wf of PP and $\mathcal{A}'$ is logically valid if and only if $\mathcal{A}$ is logically valid. By Gödel's Completeness Theorem (Corollary 2.14), $\mathcal{A}$ is logically valid if and only if $\vdash_{PF}\mathcal{A}$, and $\mathcal{A}'$ is logically valid if and only if $\vdash_{PP}\mathcal{A}'$. Hence, $\vdash_{PF}\mathcal{A}$ if and only if $\vdash_{PP}\mathcal{A}'$. In addition, if u is not the Gödel number of a wf of PF, we define h(u) to be 0; if u is the Gödel number of a wf $\mathcal{A}$ of PF, we let h(u) be the Gödel number of $\mathcal{A}'$. Clearly, h is effectively computable, and we leave it as an exercise for the diligent reader to show that h is recursive.

PROPOSITION 3.47 (Church's Theorem [1936a]). PF ***and*** PP ***are recursively undecidabfe.***

PROOF.

(1) By Gödel's Completeness Theorem, a wf $\mathcal{A}$ of P_s is provable in P_s if and only if $\mathcal{A}$ is logically valid, and $\mathcal{A}$ is provable in PF if and only if $\mathcal{A}$ is logically valid. Hence, $\vdash_{P_s}\mathcal{A}$ if and only if $\vdash_{PF}\mathcal{A}$. However, the set Fml_{P_s} of Gödel numbers of wfs of P_S is recursive. Then, $T_{P_s} = T_{PF} \cap Fml_{P_s}$, where T_{P_s} and T_{PF} are, respectively, the sets of Gödel numbers of the theorems of P_S and PF; and, if T_{PF} were recursive, T_{P_s} would be recursive, contradicting Corollary 3.45. Therefore, PF is recursively undecidable.

(2) By Lemma 3.46, u is in T_{PF} if and only if h(u) is in T_{PP}. Since h is recursive, the recursiveness of T_{PP} would imply the recursiveness of T_{PF}, contradicting (I). Thus, T_{PP} is not recursive, i.e., PP is recursively undecidable.

If we accept Church's Thesis, then "recursively undecidable" can be replaced everywhere by "effectively undecidable". In particular, Proposition 3.47 asserts that there is no decision procedure for the pure predicate calculus PP, nor for the full predicate calculus PF. This implies that there is no effective method for determining whether any given wf is logically valid.

EXERCISE 3.53.

(a) Show that, in contrast to Church's Theorem, the pure monadic predicate calculus is effectively decidable. The pure monadic predicate calculus consists of those wfs of the pure predicate calculus which contain only predicate letters of one argument.

Hint: let $B_1, \ldots, B_k$ be the distinct predicate letters in a wf $\mathcal{A}$. Then $\mathcal{A}$ is valid if and only if $\mathcal{A}$ is true in every interpretation with at most 2^k elements. For, assume $\mathcal{A}$ true in every interpretation with at most 2^k elements, and let M be any interpretation. For any elements b, c of the domain **D** of M, call b and c equivalent if the truth values of $B_1(b), B_2(b), \ldots, B_k(b)$ in M are respectively the same as

$B_1(c), B_2(c), \ldots, B_k(c)$. This defines an equivalence relation in **D**, and the corresponding set of equivalence classes has $\leqslant 2^k$ members and can be made the domain of an interpretation M′ of $\mathcal{A}$ by defining interpretations of $B_1, \ldots, B_k$, in the obvious way, on the equivalence classes. By induction, one can show that $\mathcal{A}$ is true in M if and only if it is true in M'. Since $\mathcal{A}$ is true in M′, it is also true in M. Hence, $\mathcal{A}$ is true in every interpretation, and is, therefore, by Corollary 2.14, provable. Note also that whether $\mathcal{A}$ is true in every interpretation having at most 2^k elements can be effectively determined.

(b) Prove that a wf $\mathcal{A}$ of the pure monadic predicate calculus is logically valid if and only if $\mathcal{A}$ is true for all finite interpretations. This contrasts with the situation in the pure predicate calculus (cf. Exercise 2.38 on p. 72).

The result in this exercise is, in a sense, the best possible. For, by a theorem of Kalmar [1936], there is an effective procedure producing, for each wf $\mathcal{A}$ of the pure predicate calculus, another wf $\mathcal{A}^\star$ of the pure predicate calculus such that $\mathcal{A}^\star$ contains only one predicate letter, a binary one, and such that $\mathcal{A}$ is logically valid if and only if $\mathcal{A}^\star$ is logically valid. (For another proof, cf. Church [1956, § 47].) Hence, by Church's Theorem, there is no decision procedure for logical validity (or provability) of wfs containing only binary predicate letters. (For another proof, cf. Exercise 4.74 on p. 206.)

EXERCISES^D (TARSKI-MOSTOWSKI-ROBINSON [1953], I)

3.54. If a theory K* is consistent, if every theorem of an essentially recursively undecidable theory K_1 is a theorem of K*, and, if the property $Fml_{K_1}(x)$ is recursive, prove that K* is essentially recursively undecidable.

3.55. Let K be a thwry with equality. If a predicate letter A_j^n, a function letter f_j^n, and an individual constant a, are not symbols of K, then by possible *definitions* of A_j^n. f_j^n. and a_j in K we mean, respectively, expressions of the form

(a) $(x_1) \ldots (x_n)(A_j^n(x_1, \ldots, x_n) \equiv \mathcal{A}(x_1, \ldots, x_n))$,

(b) $(x_1) \ldots (x_n)(y)(f_j^n(x_1, \ldots, x_n) = y \equiv \mathcal{B}(x_1, \ldots, x_n, y))$,

(c) $(y)(a_j = Y \equiv \mathcal{C}(y))$,

where $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ are wfs of K, and, in case (b), $\vdash_K (x_1) \ldots (x_n)(E_1 y)\mathcal{B}(x_1, \ldots, x_n, y)$, and, in case (c), $\vdash_K (E_1 y)\mathcal{C}(y)$. If K is consistent, prove that the addition of any possible definitions to K as new axioms (using only one possible definition for each symbol) yields a consistent theory K', and K' is recursively undecidable if and only if K is.

3.56. By a non-logical *constant*, we mean a predicate letter, function letter, or individual constant. Let K_1 be a theory with equality having a finite number of non-logical constants. Then K_1 is said to be interpretable in a theory with equality K if we can associate with each non-logical constant of K_1 which is not a non-logical constant of K a possible definition in K such that, if K* is the theory obtained from K by adding these possible definitions as axioms, then every axiom (and hence every theorem) of K, is a theorem of K*. Notice that, if K_1 is interpretable in K, then it is interpretable in every extension of K. Prove that, if K_1 is interpretable in K and **K** is consistent, and if K, is essentially recursively undecidable, then so is **K**.

3.57. Let K be a theory with equality. and A_j^1 a monadic predicate letter not in K. Given a closed wf $\mathcal{C}$, let $\mathcal{C}^{(A_j^1)}$ (called the **relativization** of $\mathcal{C}$ with respect to A_j^1) be the **wf** obtained from $\mathcal{C}$ by replacing every **subformula** (starting from the smallest **subformulas)** of the form $(x)\mathfrak{B}$ (x) by $(x)(A_j^1(x) \supset \mathfrak{B}$ (x)). **Let** the proper axioms of a new **theory** with equality $\mathbf{K}^{A_j^1}$ be: (1) **all** wfs $\mathcal{C}^{(A_j^1)}$, where $\mathcal{C}$ is the closure of any proper axiom of **K;** (2) $(Ex)A_j^1(x)$; (3) $A_j^1(a_m)$ for each **individual** constant a_m of **K;** (4) $A_j^1(x_1) \wedge \ldots \wedge A_j^1(x_n) \supset A_j^1(f_k^n(x_1, \ldots, x_n))$ for any function letter f_k^n of K. Prove: (a) As proper axioms of $\mathbf{K}^{A_j^1}$ we could have taken all **wfs** $\mathcal{C}^{(A_j^1)}$, where $\mathcal{C}$ is the closure of any theorem of **K. (b)** $\mathbf{K}^{A_j^1}$ is interpretable in **K.** (c) $\mathbf{K}^{A_j^1}$ is consistent **if** and only if **K** is consistent. (d) $\mathbf{K}^{A_j^1}$ is essentially recursively undecidable if and only if K is. (Tarski-Mostowski-Robinson[1953], pp. 27–28.)

3.58. K is said to be ***relatively*** interpretable in K' if there is some predicate letter A_j^1 not in **K** such that $\mathbf{K}^{A_j^1}$ is interpretable in K'. If K is **relatively** interpretable in K' and K is essentially recursively undecidable, prove that K′ is essentially recursively undecidable.

3.59. Call a theory **K** in which **RR** is relatively interpretable ***sufficiently*** strong. Prove that any sufficiently strong consistent theory **K** is **essentially** recursively undecidable, and, if in addition **K** is recursively **axiomatizable,** prove that **K** is incomplete. Roughly speaking, we may say that **K** is sufficiently strong if the notions of natural number, 0, 1, addition, and multiplication are "definable" in **K** in such a way that the axioms of RR **(relativized** to **"natural** numbers" of **K) are** provable in K. Clearly, any theory adequate for present-day mathematics will be sufficiently **strong,** and so, if it is **consistent,** it will be recursively undecidable, and, if it is recursively **axiomatizable,** it **will** be incomplete. If we accept Church's Thesis, this implies that any consistent sufficiently strong theory will be effectively undecidable, and, if it is axiomatic, it will have undecidable sentences. (Similar results also hold for higher-order theories; for example, cf. **Gödel [1931], Scholz-Hasenjaeger [1961], § 237–238.)** This seems to destroy all hope for a consistent and complete **axiomatization** of mathematics.

CHAPTER 4

AXIOMATIC SET THEORY

1. An Axiom System

A prime reason for the increase in importance of mathematical logic in this century was the discovery of the paradoxes of set theory and the need for a revision of intuitive (and contradictory) set theory. Many different axiomatic theories have been proposed to serve as a foundation for set theory, but, no matter how they differ at the fringes, they all have as a common core the fundamental theorems which mathematicians need in their daily work. A choice among the available theories is primarily a matter of taste, and we make no claim about the system we shall use except that it is an adequate basis for present-day mathematics.

We shall describe a first-order theory NBG, which is basically a system of the same type as one originally proposed by von Neumann [1925, 1928] and later thoroughly revised and simplified by R. Robinson [1937], Bernays [1937–1954], and Gödel [1940]. (We shall follow Gödel's monograph to a great extent, though there will be some important differences.) NBG has a single predicate letter A_2^2, but no function letters or individual constants. In order to conform to the notation in Bernays [1937–1954] and Gödel [1940], we shall use capital Latin letters X,, X_2, X_3, . . . as variables, instead of x,, x_2, x_3, ... (As usual, we shall use X, Y, Z, . . . to represent arbitrary variables.) We shall abbreviate $A_2^2(X, Y)$ by $X \in Y$, and $\sim A_2^2(X, Y)$ by $X \notin Y$; intuitively, $\in$ is thought of as the membership relation.

Let us define equality in the following way.

DEFINITION. $X = Y$ for $(Z)(Z \mathrm{E} X \equiv Z \in Y)$

Thus, two objects are equal when and only when they have the same members.

DEFINITION. $X \subseteq Y$ for $(Z)(Z \mathrm{E} X \supset Z \mathrm{E} Y)$ (Inclusion)

DEFINITION. X **c** Y for $X \subseteq Y \wedge X \neq Y$ (Proper inclusion)

As easy consequences of these definitions, we have the following.

PROPOSITION 4.1†

(a) $\vdash X = Y \equiv (X \subseteq Y \wedge Y \subseteq X)$
(b) $\vdash X = X$
(c) $\vdash X = Y \supset Y = X$
(d) $\vdash X = Y \supset (Y = Z \supset X = Z)$
(e) $\vdash X = Y \supset (Z \in X \equiv Z \in Y)$

We shall now present the proper axioms of NBG, interspersing among the statement of the axioms some additional definitions and various consequences of the axioms. First, however, notice that in the "interpretation" we have in mind the variables take classes as values. Classes are the totalities corresponding to some, but not necessarily all, properties.‡ (This "interpretation" is as imprecise as the notions of "totality", "property". etc.)

We define a class to be a set if it is a member of some class, whereas those classes which are not sets are calledproper classes.

DEFINITION. $M(X)$ for $(EY)(X \in Y)$. (X is a set.)

DEFINITION. $Pr(X)$ for $\sim M(X)$. (X is a proper class.)

It will be seen later that the usual derivations of the paradoxes now no longer lead to a contradiction, but only yield the result that various classes are proper classes, not sets. The sets are intended to be those safe, comfortable classes which are used by mathematicians in their daily life and work, whereas proper classes are thought of as monstrously large collections which, if permitted to be sets (i.e., allowed to belong to other classes), would engender contradictions.

EXERCISE 4.1. *Prove*: $\vdash Y \in X \supset M(Y)$

The system NBG is designed to handle classes, not individuals. The reason for this is that mathematics has no need for non-classes, like cows or molecules; all mathematical objects and relations can be formulated in terms of classes alone. If non-classes are required for applications to other sciences, then the system NBG can be modified slightly so as to apply to both classes and non-classes alike (cf. Mostowski [1939]).

Let us introduce small letters x,, x„ . . . as special, restricted variables for sets. In other words, $(x_i)\mathscr{A}(x_i)$ stands for $(X)(M(X) \supset \mathscr{A}(X))$, i.e., & holds for all sets; $(Ex_i)\mathscr{A}(x_i)$ stands for $(EX)(M(X) \wedge \mathscr{A}(X))$, i.e., $\mathscr{A}$ holds for some set. Note that the variable X used in this definition should be one which does not occur in $\mathscr{A}(x_i)$. (As usual, we use x, y, z, . . . to stand for arbitrary set variables.)

†The subscript NBG will be omitted from $\vdash_{NBG}$ in the rest of this chapter.

‡Those properties which actually do determine classes will be partially specified in the axioms. These axioms provide us with the classes we need in mathematics and appear (we hope) modest enough so that contradictions are not derivable from them.

Example. $(X)(x)(Ey)(EZ)\mathscr{A}(X, x, y, Z)$ stands for
$$(X)(W)(M(W) \mathrm{3} (EY)(M(Y) \mathrm{A} (EZ)\mathscr{A}(X, W, Y; Z)))$$

EXERCISE 4.2. Prove: $\vdash X = Y \equiv (z)(z \in X \equiv z \in Y)$

AXIOM T (Axiom of Extensionality). $X = Y \mathrm{3} (X \in Z \equiv Y \in Z)$

PROPOSITION 4.2. NBG is a first-order theory with equality.

PROOF. By Proposition 4.1 and Axiom T, and the discussion on p. 83.

EXERCISE 4.3. *Prove*: $\vdash M(Z) \wedge Z = Y \supset M(Y)$

AXIOM P (Pairing Axiom). $(x)(y)(Ez)(u)(u \in z \equiv u = x \vee u = y)$, *i.e.*, for any sets x, y there is a set z such that z has x and y as its *only* members.

EXERCISES

Prove:

4.4. $\vdash (x)(y)(E_1z)(u)(u \in z \equiv u = x \vee u = y)$, i.e., there is a unique set z, called the unordered *pair* of x and y, such that z has x and y as its only members. This follows easily from Axiom P and the definition of equality.

4.5. $\vdash (X)(M(X) \equiv (Ey)(X \in y))$

AXIOM N (Null Set). $(Ex)(y)(y \notin x)$, *i.e.*, there is a set which *has* no members.

Obviously, from Axiom N and the definition of equality, there is a unique set which has no members, i.e., $\vdash (E_1x)(y)(y \notin x)$. Therefore, we can introduce a new individual constant 0 by means of the following condition.

DEFINITION. $(y)(y \notin 0)$

Since we have the uniqueness condition for the unordered pair, we can introduce a new function letter $g(x, y)$ to designate the unordered pair of x and y. We shall write $\{x, y\}$ for $g(x, y)$. Notice that we have to define a unique value for {X, Y) for any classes X and Y, not only for sets x and y. We shall let (X, Y) = 0 whenever X is not a set or Y is not a set. One can prove: $\vdash (E_1Z)((M(X) \wedge M(Y) \wedge (u)(u \mathrm{E} Z \equiv u = X \vee u = Y)) \vee ((\sim M(X) \mathrm{V} \sim M(Y)) \wedge Z = 0))$. This justifies the introduction of {X, Y}:

DEFINITION. $(M(X) \wedge M(Y) \mathrm{A} (u)(u \in \{X, Y\} \equiv u = X \vee u = Y)) \vee ((\sim M(X) \mathrm{V} \sim M(Y)) \mathrm{A} \{X, Y\} = 0)$.

One can then prove: $\vdash (x)(y)(u)(u \in \{x, y\} \equiv u = x \mathrm{V} u = y)$ and $\vdash (x)(y)(M(\{x, y\}))$.

In connection with these definitions, the reader should review § 9 of Chapter 2, and, in particular, Proposition 2.29, which assures us that the introduction of new individual constants and function letters, such as 0 and $\{X, Y\}$, adds nothing essentially new to the theory NBG.

EXERCISES

4.6. $\vdash \{X, Y) = \{Y, X)$.

4.7. *Define:* $\{X)$ *for* $\{X, X)$. *Prove:* $\vdash (x)(y)(\{x\} = \{y\} \supset x = y)$.

DEFINITION. $(X, Y) = \{\{X), \{X, Y))$

(X, Y) is called the orderedpair of X and Y.

The definition of (X, Y) does not have any intrinsic intuitive meaning. It is just a convenient way (discovered by Kuratowski) to define ordered pairs so that one can prove the characteristic property of ordered pairs expressed in the following proposition.

PROPOSITION 4.3. $\vdash (x)(y)(u)(v)(\langle x, y\rangle = \langle u, v\rangle \supset x = u \wedge y = v)$.

PROOF. Assume $\langle x, y\rangle = \langle u, v\rangle$. Then $\{\{x\}, \{x, y\}\} = \{\{u\}, \{u, v\}\}$. Since $\{x\} \in \{\{x\}, \{x, y\}\}$, $\{x\} \in \{\{u\}, \{u, v\}\}$. Hence, $\{x\} = \{u\}$ or $\{x) = \{u, v\}$. In both cases, $x = u$. Now, $\{u, v\} \in \{\{u), \{u, v\}\}$; so, $\{u, v\} \in \{\{x\}, \{x, y\}\}$. Then $\{u, v\} = \{x\}$ or $\{u, v\} = \{x, y)$. Similarly, $\{x, y) = \{u)$ or $\{x, y) = \{u, v)$. If $\{u, v) = \{x)$ and $\{x, y) = \{u)$, then $x = u = y = v$; if not. $\{u, v\} = \{x, y\}$. Hence, $\{u, v) = \{u, y)$. So, if $v \neq u$, theny $= v$; if $v = u$, then $y = v$. Thus, in all cases, $y = v$.

We now extend the definition of ordered pairs to ordered n-tuples.

DEFINITION.

$$(X) = X$$

$$\langle X_1, \ldots, X_{n+1}\rangle = \langle\langle X_1, \ldots, X_n\rangle, X_{n+1}\rangle$$

Thus,

$$\langle X, Y, Z\rangle = \langle\langle X, Y\rangle, Z\rangle, \quad \text{and} \quad \langle X, Y, Z, U\rangle = \langle\langle\langle X, Y\rangle, Z\rangle, U\rangle$$

One can easily establish the following generalization of Proposition **4.3:**

$$\vdash (x_1) \ldots (x_n)(y_1) \ldots (y_n)(\langle x_1, \ldots, x_n\rangle = \langle y_1, \ldots, y_n\rangle \supset$$

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n)$$

Axioms of *Class* Existence. These axioms state that, for certain properties expressed by wfs, there are corresponding classes of all those sets satisfying the property.

AXIOM B1. $(EX)(u)(v)(\langle u, v\rangle \in X \equiv (u \in v))$ ($\in$-relation)

AXIOM B2. $(X)(Y)(EZ)(u)(u \in Z \equiv u \in X \wedge u \in Y)$ (Intersection)

AXIOM B3. $(X)(EZ)(u)(u \in Z \equiv u \notin X)$ (Complement)

AXIOM B4. $(X)(EZ)(u)(u \in Z \equiv (Ev)(\langle u, v\rangle \in X))$ (Domain)

AXIOM B5. $(X)(EZ)(u)(v)(\langle u, v\rangle \in Z \equiv u \in X)$

AXIOM B6. $(X)(EZ)(u)(v)(w)(\langle u, v, w\rangle \in Z \equiv \langle v, w, u\rangle \in X)$

AXIOM B7. $(X)(EZ)(u)(v)(w)(\langle u, v, w\rangle \in Z \equiv \langle u, w, v\rangle \in X)$

From Axioms B2–B4 and the definition of equality,

$$\vdash (X)(Y)(E_1Z)(u)(u \in Z \equiv u \in X \wedge u \in Y)$$

$$\vdash (X)(E_1Z)(u)(u \in Z \equiv u \notin X)$$

$$\vdash (X)(E_1Z)(u)(u \in Z \equiv (Ev)(\langle u, v\rangle \in X))$$

These results justify the introduction of new function letters: $\cap$, $^-$, $\mathfrak{D}$

DEFINITIONS

$(u)(u \in X \cap Y \equiv u \in X \wedge u \in Y)$ (Intersection of X and Y)

$(u)(u \in \bar{X} \equiv u \notin X)$ (Complement of X)

$(u)(u \in \mathfrak{D}(X) \equiv (Ev)(\langle u, v\rangle \in X))$ (Domain of X)

$X \cup Y = \overline{(\bar{X} \cap \bar{Y})}$ (Union of X and Y)

$V = \bar{0}$ (Universal Class)

$X - Y = X \cap \bar{Y}$ (Difference of X and Y)

EXERCISES

Prove:

4.8. $\vdash (u)(u \in X\ U\ Y \equiv u \in X \vee u \in Y)$

$\vdash (u)(u \in V)$

4.9. $I\cdot X\ n\ Y = Y\ n\ X$

$I\cdot(X\,n\ Y) \cap Z = X \cap (Y \cap Z)$

$\vdash X \cap X = X$

$\vdash X \cap 0 = 0$

$\vdash X \cap V = X$

$I\cdot X \cap (Y\ u\ Z)$
$= (X\ n\ Y) \cup (X\ n\ Z)$

$\vdash \overline{X \cup Y} = \bar{X} \cap \bar{Y}$

$\vdash X - X = 0$

$\vdash \bar{\bar{X}} = X$

$\vdash (u)(u \in X - Y \equiv u \in X \wedge u \notin Y)$

$\vdash X \cup Y = Y \cup X$

$I\cdot(X\,u\ Y) \cup Z = X \cup (Y \cup Z)$

$\vdash X \cup X = X$

$\vdash X \cup 0 = X$

$I\cdot X\,U\ V = V$

$\vdash X \cup (Y \cap Z)$
$= (X\ u\ Y)\ n\ (X\ u\ Z)$

$\vdash \overline{X \cap Y} = \bar{X} \cup \bar{Y}$

$\vdash V - X = \bar{X}$

$\vdash \bar{V} = 0$

4.10. *(a)* $\vdash (X)(EZ)(u)(v)(\langle u, v) \in Z \equiv (v, u\rangle \in X)$. *(Hint: apply successively* B5, *B7*, B6, B4.)

(b) $\vdash (X)(EZ)(u)(v)(w)(\langle u, v, w) \in Z \equiv \langle u, w) \in X)$. *(Hint: use B5 and B7.)*

(c) $\vdash (X)(EZ)(v)(x_1) \ldots (x_n)(\langle x_1, \ldots, x_n, v\rangle \in Z \equiv \langle x_1, \ldots, x_n\rangle \in X)$. *(Hint: use* B5.)

(d) $\vdash (X)(EZ)(v_1) \ldots (v_m)(x_1) \ldots (x_n)(\langle x_1, \ldots, x_n, v_1, \ldots, v_m\rangle \in Z \equiv \langle x_1, \ldots, x,) \in X)$. *(Hint: by iteration of (c).)*

(e) $\vdash (X)(EZ)(v_1) \ldots (v_m)(x_1) \ldots (x_n)(\langle x_1, \ldots, x_{n-1}, v_1, \ldots, v_m, x_n\rangle \in Z \equiv \langle x_1, \ldots, x_n\rangle \in X)$. *(Hint: for* $m = 1$, *from (b), substituting* $\langle x_1, \ldots, x_{n-1}\rangle$ *for* u *and* x_n *for* w*; the general case then follows by iteration.)*

(f) $\vdash (X)(EZ)(x)(v_1) \ldots (v_m)(\langle v_1, \ldots, v_m, x) \in Z \equiv x \in X)$. *(Hint: from B5 and Part (a) above.)*

(g) $\vdash (X)(EZ)(x_1) \ldots (x_n)(\langle x_1, \ldots, x_n\rangle \in Z \equiv (Ey)(\langle x_1, \ldots, x_n, y\rangle \in X))$. *(Hint: from B4, substituting* $(x,, \ldots, x_n\rangle$ *for* u, *and* y *for* v.)

(h) $\vdash (X)(EZ)(u)(v)(w)(\langle v,$ **u, w) $\in$ Z $\equiv$ (u, w) $\in X$). (Hint: substitute (u, w)** for **u in Axiom B5, and apply Axiom B6.)**

(i) $\vdash (X)(EZ)(v_1) \dots (v_k)(u)(w)(\langle v_1, \dots, v_k, u, w\rangle \in Z \equiv \langle u, w\rangle \in X)$. **(Hint: substitute** $\langle v_1, \dots, v_k\rangle$ for v **in** (h).)

Now we can derive a general class existence theorem.

PROPOSITION 4.4. Let $\varphi(X_1, \dots, X_n,$ Y,, $\dots, Y_m)$ be a wf the variables *of* which occur among $X_1, \dots, X_n, Y_1, \dots, Y_m$ and in which only set variables are *quantified* (*i.e.*, φ can be abbreviated in such a way *that* only set variables are quantified). We call such a wf predicative. Then,

$$\vdash (EZ)(x_1) \dots (x_n)(\langle x_1, \dots, x_n\rangle \in Z \equiv \varphi(x_1, \dots, x_n, Y_1, \dots, Y_m))$$

PROOF. We shall consider only wfs φ in which no wf of the form $Y_i \in$ W occurs, since $Y_i \in$ W can be replaced by $(Ex)(x = Y_i \wedge$ x $\in$ W), which is equivalent to $(Ex)((z)(z \in$ x $\equiv z \in Y_i) \wedge$ x $\in$ W). Also, we may assume that φ contains no wf of the form X $\in$ X, since this may be replaced by $(Eu)(u =$ X $\wedge$ u $\in$ X), which is equivalent to $(Eu)((z)(z \in$ u $\equiv z \in$ X) $\wedge$ u $\in$ X). We shall proceed now by induction on the number k of connectives and quantifiers in φ (written with restricted set variables).

Case 1. k = 0. Then φ has the form $x_i \in x_j$ or x, $\in x_i$ or $x_i \in$ Y, where $1 \leqslant i < j \leqslant n$. For x, $\in$ x,, there is, by Axiom B1, some W, such that $(x_i)(x_j)(\langle x_i,$ 4) $\in W_1 \equiv x_i \in x_j)$. For x, $\in$ x,, there is, by Axiom B1, some W_2 such that $(x_i)(x_j)(\langle x_j, x_i\rangle \in W_2 \equiv x_j \in x_i)$, and then, by Exercise 4.10(a), there is some W_3 such that $(x_i)(x_j)(\langle x_i, x_j\rangle \in W_3 \equiv$ x, $\in x_i)$. So, in both cases, there is some W such that $(x_i)(x_j)(\langle x_i, x_j\rangle \in$ W $\equiv \varphi(x_1, \dots, x_n,$ Y,, $\dots, Y_m))$. Then, by Exercise 4.10(i) with W = X, there is some Z_1 such that

$$(x_1) \dots (x_{i-1})(x_i)(x_j)(\langle x_1, \dots, x_{i-1}, x_i, x_j\rangle \in Z_1 \equiv \varphi(x_1, \dots, x_n, Y_1, \dots, Y_m)).$$

Hence, by Exercise 4.10(e) with $Z_1 = X$, there is some Z_2 such that

$$(x_1) \dots (x_i)(x_{i+1}) \dots (x_j)(\langle x_1, \dots, x_j\rangle \in Z_2 \equiv \varphi(x_1, \dots, x_n, Y_1, \dots . Y_m)).$$

Then, by Exercise 4.10(d) with Z_2 = X, there is some Z such that

$$(x_1) \dots (x_n)(\langle x_1, \dots, x_n\rangle \in Z \equiv \varphi(x_1, \dots, x_n, Y_1, \dots, Y_m)).$$

In the remaining case, $x_i \in$ Y, the theorem follows by application of Exercise 4.10(f) and 4.10(d).

Case 2. Let the theorem be provable tor all k < m. and assume that φ has m connectives and quantifiers.

(a) φ is $\sim \psi$. By inductive hypothesis, there is some W such that

$$(x_1) \dots (x_n)(\langle x_1, \dots, x_n\rangle \in W \equiv \psi(x_1, \dots, x_n, Y_1, \dots, Y_m))$$

Let $Z = \overline{W}$.

(b) φ is $\psi \supset$ 8. By inductive hypothesis, there are classes Z_1 and Z_2 such that

$$(x_1) \dots (x_n)(\langle x_1, \dots, x_n\rangle \in Z_1 \equiv \psi(x_1, \dots, x_n, Y_1, \dots, Y_m))$$

and

$$(x_1) \dots (x_n)(\langle x_1, \dots, x_n\rangle \in Z_2 \equiv \theta(x_1, \dots, x_n, Y_1, \dots, Y_m))$$

Let $Z = \overline{(Z_1 \cap \overline{Z}_2)}$.

(c) φ is $(x)\psi$. By inductive hypothesis, there is some W such that

$$(x_1) \dots (x_n)(x)(\langle x_1, \dots, x_n, x\rangle \in W \equiv \psi(x_1, \dots, x_n, x, Y_1, \dots, Y_m))$$

Apply Exercise 4.10(g) with X = $\overline{W}$ to obtain a class Z_1 such that

$$(x_1) \dots (x_n)(\langle x_1, \dots, x_n\rangle \in Z_1 \equiv (Ex) \sim \psi(x_1, \dots, x_n, x, Y_1, \dots, Y_m))$$

Now, let $Z = \overline{Z}_1$, noting that $(x)\psi$ is equivalent to $\sim$ (Ex) $\sim \psi$.

Examples. 1. Let $\varphi(X, Y_1, Y_2)$ be $(Eu)(Ev)(X =$ (u, $v\rangle \wedge u \in Y_1$ A v E $Y_2)$. The only quantifiers in φ involve set variables. Hence, by the Class Existence Theorem, $\vdash (EZ)(x)(x \in Z \equiv (Eu)(Ev)(x = \langle u, v\rangle \wedge u \in Y_1 \wedge v$ E $Y_2)$. By the definition of equality, $\vdash (E_1Z)(x)(x \in Z \equiv (Eu)(Ev)(x =$ (u, $v\rangle \wedge u \in$ Y, $\wedge\ v \in Y_2))$. So, we can introduce a new function letter $\times$:

DEFINITION.

$$(x)(x \in Y_1 \times Y_2 \equiv (Eu)(Ev)(x = \text{(u, v)} \wedge u \in \text{Y,} \wedge v \text{ E } Y_2)$$

(Cartesian Product of Y, and Y_2)

DEFINITIONS

X^2 for X $\times$ X, (In particular, V^2 is the class of all ordered pairs.)
X^n for $X^{n-1} \times X$, (Thus, V^n is the class of all ordered n-tuples.)
$Rel(X)$ for X $\subseteq V^2$ (X is a relation).

2. Let $\varphi(X,$ Y) be X $\subseteq$ Y.

By the Class Existence Theorem and the definition of equality, $\vdash (E_1Z)(x)(x$ E $Z \equiv$ x $\subseteq$ Y). Thus, there is a class Z which has as its members all subsets of Y.

DEFINITION. $(x)(x \in \mathcal{P}(Y) \equiv$ x $\subseteq$ Y). ($\mathcal{P}$(Y): the power class of Y.)

3. Let $\varphi(X,$ Y) be $(Ev)(X \in v \wedge v \in$ Y).

By the Class Existence Theorem and the definition of equality, $\vdash (E_1Z)(x)(x$ E $Z \equiv (Ev)(x \in v \wedge v \in Y))$. Thus, there is a class Z which contains all the elements of the elements of Y.

DEFINITION. $(x)(x \in \bigcup(Y) \equiv (Ev)(x \in$ v $\wedge\ v \in$ Y)).
($\bigcup$(Y): the sum class of Y.)

4. Let $\varphi(X)$ be $(Eu)(X =$ (u, u)).

By the Class Existence Theorem and the definition of equality, there is a unique class Z such that $(x)(x \in Z \equiv (Eu)(x =$ (u, u))).

DEFINITION. $(x)(x \in I \equiv (Eu)(x = (u,\ u))$ (Identity Relation).

COROLLARY 4.5. Given a predicative wf $\varphi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$. *Then* $(E_1 W)(W \subseteq V^n \wedge (x_1) \ldots (x_n)(\langle x_1, \ldots, x,,) \in W$

$$\equiv \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)))$$

PROOF. By Proposition 4.4, there is some Z such that

$$(x_1) \ldots (x_n)(\langle x_1, \ldots, x_n\rangle \in Z \equiv \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m))$$

Clearly, $W = Z \cap V^n$ satisfies the corollary, and the uniqueness follows from the definition of equality.

DEFINITION. Given any predicative wf $\varphi(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$, we use $\{\langle x_1, x_2, \ldots, x_n\rangle | \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)\}$ to denote the class of all n-tuples $\langle x_1, \ldots, x_n\rangle$ satisfying $\varphi(x_1, \ldots, x,,, Y_1, \ldots, Y_m)$, that is

$$\{\langle x_1, \ldots, x_n\rangle | \varphi(x_1, \ldots, x_n, Y_1, \ldots, Y_m)\} \mathrm{E}$$
$$(Ex_1) \ldots (Ex_n)(u = \langle x_1, \ldots, x_n\rangle \wedge \varphi(x_1, \ldots, x,,, Y_1, \ldots, Y_m))).$$

This definition is justified by Corollary 4.5. In particular, when $n = 1$, $(u)(u \in \{x | \varphi(x, Y_1, \ldots, Y_m)\} \equiv \varphi(u, Y_1, \ldots, Y_m))$.

Examples.

1. Take φ to be $\langle x_2, x_1\rangle \in Y$. Let $\check{Y}$ be an abbreviation for $\{(x,, x_2\rangle | \langle x_2, x_1\rangle \in Y\}$. Hence, $\vdash \check{Y} \subseteq V^2 \wedge (x_1)(x_2)(\langle x_1, x_2\rangle \in \check{Y} \equiv \langle x_2, x_1\rangle \in Y)$. Call Y the *inverse* relation of Y.

2. Take φ to be $(Ev)(\langle v, x) \in Y)$. Let $\mathfrak{R}(Y)$ stand for $\{x|(Ev)(\langle v, x) \in Y))$. Then $\vdash (u)(u \in \mathfrak{R}(Y) \equiv (Ev)(\langle v, u) \in Y))$. $\mathfrak{R}(Y)$ is called the range of Y. Clearly, $\vdash \mathfrak{R}(Y) = \mathfrak{D}(\check{Y})$.

Notice that Axioms B1–B7 are special cases of the Class Existence Theorem, Proposition 4.4. Thus, instead of having to assume Proposition 4.4 as an axiom schema, we need only take a finite number of instances of that schema.

Until now, although we can prove, via Proposition 4.4, the existence of a great many classes, the existence of only a few sets, such as 0, {0}, {0, {0}}, {{0}}, etc., is known to us. To guarantee the existence of sets of greater complexity, we require more axioms.

AXIOM *U* (Sum Set). $(x)(Ey)(u)(u \in y \equiv (Ev)(u \in v \wedge v \in x))$.

This axiom asserts that the sum class $\bigcup(x)$ of a set x (cf. Example 3, p. 179) is also a set, which we shall call the sum set of x, i.e., $\vdash (x)(M(\bigcup(x)))$. The sum set $\bigcup(x)$ is usually referred to as the union of all the sets in the set x, and is often denoted $\bigcup_{v \in x}$ u.

EXERCISES

4.11. Show that $\vdash (x)(y)(\bigcup(\{x, y\}) = x\ \mathrm{u}\ y)$. Hence, $\vdash (x)(y)(M(x\ \mathrm{u}\ y))$.

4.12. (a) $\vdash \bigcup(0) = 0$. (b) $\vdash \bigcup(\{0\}) = 0$. (c) $\vdash (x)(\bigcup(\{x\}) = x)$.
(d) $\vdash (x)(y)(\bigcup(\langle x, y\rangle) = \{x, y\})$.

4.13. We can define by induction, $\{x_1, \ldots, x_n\}$ for $\{x_1, \ldots, x_{n-1}\} \cup \{x_n\}$. Prove: $\vdash (x_1)(x_2) \ldots (x_n)(u)(u \in \{x_1, \ldots, x_n\} \equiv u = x_1 \vee u = x_2 \vee \ldots \vee = x_n)$. Thus, for any given sets $x_1, \ldots, x_n$, there is a set which has $x_1, \ldots, x_n$ as its only members.

Another means of generating new sets from old is the formation of the set all subsets of a given set.

AXIOM W (Power Set). $(x)(Ey)(u)(u \in y \quad u \subseteq x)$.

This axiom asserts that the power class $\mathcal{P}(x)$ of a set x (cf. Example 2, p. 179) is also a set, called the power set of x, i.e., $\vdash (x)(M(\mathcal{P}(x)))$.

Examples. $\vdash \mathcal{P}(0) = \{0\}$
$\vdash \mathcal{P}(\{0\}) = \{0, \{0\}\}$
$\vdash \mathcal{P}(\{0, \{0\}\}) = \{0, \{0\}, \{0, \{0\}\}, \{\{0\}\}\}$

A much more general way to produce sets is the following *Axiom of Subsets.*

AXIOM S. $(x)(Y)(Ez)(u)(u \in z \equiv u \in x \wedge u \in Y)$.

Thus, for any set x and class Y, there is a set consisting of the common elements of x and Y. Hence, $\vdash (x)(Y)(M(x \cap Y))$, i.e., the intersection of a set and a class is a set.

PROPOSITION 4.6. $\vdash (x)(Y)(Y \subseteq x \supset M(Y))$ (i.e., any subclass of a set is a set).

PROOF. $t\,(x)(Y \subseteq x \supset Y \cap x = Y)$, and $\vdash (x)M(Y \cap x)$.

Since any predicative wf $\mathcal{A}(y)$ generates a corresponding class (cf. Proposition 4.4), Axiom S implies that, given any set **x**, the class of all elementsy of x which satisfy $\mathcal{A}(y)$ is a set.

A stronger axiom than the Axiom of Subsets (S) will be necessary for the full development of set theory. First, we introduce a few definitions.

DEFINITIONS

$Un(X)$ for $(x)(y)(z)(\langle x, y\rangle \in X \mathrm{A} \langle x, z\rangle \in X \,3\, y = z)$
(X is uniuocal.)

$Fnc(X)$ for $X \subseteq V^2 \wedge Un(X)$. (Xis afunction.)

X: $Y \rightarrow Z$ for $Fnc(X) \wedge \mathfrak{D}(X) = Y \wedge \mathfrak{R}(x) \subseteq Z$.
(X is afunction *from* Y into Z).)

$Y \mathbf{1} X$ for $X \cap (Y \times V)$. (Restriction of X to the domain Y.)

$Un_1(X)$ for $Un(X) \wedge Un(\check{X})$. (Xis one-one.)

$$X`\_ = \begin{cases} z & \text{if } (u)(\langle Y, u) \in X \equiv u = z), \\ 0 & \text{otherwise.} \end{cases}$$

If there is a unique z such that $(y, z) \in X$, then $z = X`y$; otherwise, X'y $= 0$. If X is a function and y is a set in its domain, $X`y$ is the value of the function applied to y.†

$X``Y = \mathfrak{R}(Y \upharpoonleft X)$ (If X is a function, $X``Y$ is the range of X restricted to Y.)

EXERCISE 4.14. Prow: $\vdash Fnc(X) \supset (v)(v \in X``Y \equiv (Eu)(u \in Y \cap \mathfrak{D}(X) \wedge u = X'u))$.

AXIOM R (Replacement).

$$(x)(Un(X) \supset (Ey)(u)(u \in y \equiv (Ev)(\langle v, u\rangle \in X \text{ A } v \in x)))$$

Axiom R asserts that if X is univocal, then the class of second components of ordered pain in X whose first components are in x is a set (or, equivalently, $M(\mathfrak{R}(x \upharpoonleft X))$). When X is a function, this implies that the range of the restriction of the function X to a domain which is a set is also a set.

EXERCISES

4.15, Show that the Axiom of Replacement (R) implies the Axiom of Subsets (S).
4.16. Prove: $\vdash (x)(M(\mathfrak{D}(x)) \text{ A } M(\mathfrak{R}(x)))$.
4.17. (a) Prove: $\vdash x \times y \subseteq \mathcal{P}(\mathcal{P}(x \cup y))$.
(b) Prove: $\vdash (x)(y)M(x \times y)$.
4.18. Prove: $\vdash M(\mathfrak{D}(X)) \wedge M(\mathfrak{R}(X)) \wedge Rel(X) \text{ 3 } M(X)$.
4.19. Prove: $\vdash (y)(Fnc(X) \supset M(X``y))$.

To insure the existence of an infinite set, we add the following axiom.

AXIOM I (Axiom of Infinity).

$$(Ex)(0 \in x \text{ A } (u)(u \in x \supset u \text{ U } \{u\} \in x))$$

Axiom I states that there is a set x which contains 0 and such that, whenever $u \in x$, then $u \text{ U } \{u)$ also belongs to x. Clearly, for such a set x, $\{0\} \in x$, $\{0, \{0\}\}$ E x, $\{0, \{0\}, (0, \{0\}\}\} \in x$, etc. Intuitively, if we let 1 stand for $\{0\}$, 2 for $(0, 1\}$, 3 for $(0, 1, 2\}, \ldots, n$ for $\{0, 1, 2, \ldots, n-1\}, \ldots$, then, for all integers $n \geqslant 0$, $n \in x$; and $0 \neq 1$, $0 \neq 2$, $1 \neq 2$, $0 \neq 3$, $1 \neq 3$, $2 \neq 3, \ldots$.

EXERCISE 4.20. (a) *Prove* that any formula which implies $(EX)M(X)$ would, together with Axiom *S*, *imply* Axiom N.

(b) Show that Axiom (I) is *equivalent* to the *following* sentence ($\mathscr{L}$): $(Ex)((Ey)(y \in x \text{ A } (u)(u \notin y)) \text{ A } (u)(u \in x \supset u \text{ U } \{u\} \in x))$, *and then* prove that ($\mathscr{L}$) implies Axiom *N*. (Hence, *if* we assumed ($\mathscr{L}$) instead of Axiom **I**, Axiom N would become superfluous.)

†From here on, we shall introduce new function letters or individual constants wherever it is made clear that the definition is based upon a uniqueness theorem. In this case, we have introduced a new function letter $h(X, Y)$ abbreviated X'Y.

This completes the list of axioms of NBG, and we see that NBG has only a finite number of axioms: namely, Axiom T (Extensionality), Axiom P (Pairing), Axiom N (Null Set), Axiom S (Subsets), Axiom U (Sum Set), Axiom W (Power Set), Axiom R (Replacement), Axiom I (Infinity), and the seven class existence axioms B1–B7. We have also seen that Axioms N and S are provable from the other axioms; however, they have been included here because they are of interest in the study of certain weaker subtheories of NBG.

Let us verify now that Russell's Paradox is not derivable in NBG. Let $Y = \{x | x \notin x\}$. Hence. $(x)(x \in Y \equiv x \notin x)$. (Such a class Y exists by the Class Existence Theorem, Proposition 4.4, since $x \notin x$ is a predicative wf.) This, in unabbreviated notation, is $(X)(M(X) \supset (X \in Y \equiv X \notin X))$. Assume $M(Y)$. Then $Y \in Y$ $Y \notin Y$, which by the tautology $(A \equiv \sim A) \supset (A \wedge - A)$, implies $Y \in Y \wedge Y \notin Y$. Hence, by the Deduction Theorem, $\vdash M(Y) \supset (Y \in Y \wedge Y \notin Y)$, and so, by the tautology $(B \supset (A \wedge \sim A)) \supset \sim B$, $\vdash \sim M(Y)$. Thus, in NBG, the argument for Russell's Paradox merely shows that Russell's class Y is a proper class, not a set. This is typical of the way NBG avoids the usual paradoxes (Cantor, Burali-Forti).

EXERCISE 4.21. Prove: $\vdash \sim M(V)$. (The uniuersal class is not a set.)

2. Ordinal Numbers

Let us first define some familiar notions concerning relations.

DEFINITIONS

X Irr Y for $(y)(y \in Y \supset \langle y, y\rangle \notin X) \text{ A } Rel(X)$.
(X is an *irreflexive* relation on Y.)

X Tr Y for $Rel(X) \wedge (u)(v)(w)(u \in Y \wedge u \in Y \wedge w \in Y \wedge \langle u, u) \in X \wedge \langle v, w) \in X \supset \langle u, w) \in X)$.
(X is a transitive relation on Y.)

X Part Y for $(X\ Irr\ Y) \wedge (X \text{ Tr } Y)$. (Xpartially orders Y.)

X Con Y for $Rel(X) \wedge (u)(v)(u \in Y \wedge v \in Y \wedge u \neq v \supset \langle u, v\rangle \in X \vee \langle v, u\rangle \in X)$.
(X is a connected relation on Y.)

X *Tot* Y for $(X \text{ Irr } Y) \wedge (X \text{ Tr } Y) \wedge (X \text{ Con } Y)$.
(X totally orders Y.)

X We Y for $(X \text{ Irr } Y) \wedge (Z)(Z \subseteq Y \wedge Z \neq 0 \supset (Ey)(y \in Z \wedge (v)(v \in Z \text{ A } v \neq y \supset \langle y, v\rangle \in X \text{ A } \langle v, y\rangle \notin X))$.
(X well-orders Y, i.e., the relation X is irreflexive on Y and every non-empty subclass of Y has a least element with respect to X.)

EXERCISES

Prove:

4.22. $\vdash (X\ We\ Y) \text{ 3 } (X\ Tot\ Y)$. (Hint: to show X Con Y, let $x, y \in Y$ with $x \neq y$. *Then* $(x, y\}$ has a least element, say x. Then $(x, y\rangle \in X$. To show X Tr Y, let x, y, z $\in Y$ with $\langle x,y\rangle \in X$ **A** $\langle y, z\rangle \in X$. Then $\{x,y,z\}$ has a least element, which must be x.)

4.23. $\vdash (X\ We\ Y) \wedge (Z \subseteq Y) \supset (X\ We\ Z)$.

Examples. (From intuitive set theory.)

I. The relation $<$ on the set of positive integers P well-orders P.

2. The relation $<$ on the set of all integers totally orders, but does not well-order, this set. The set has no least element.

3 The relation c on the set W of all subsets of the set of integers partially orders W, but does not totally order W. For example, $\{1\} \not\subset (2)$ and $\{2\} \not\subset \{I\}$.

DEFINITION. $Sim(Z, W_1, W_2)$ for $(Ex_1)(Ex_2)(Er_1)(Er_2)(Rel(r_1) \wedge Rel(r_2) \wedge W_1 = \langle r_1, x_1\rangle$ A $W_2 = \langle r_2, x_2\rangle$ A $Fnc(Z)$ A $Un_1(Z) \wedge \mathfrak{D}(Z) = x_1 \wedge \mathfrak{R}(Z) = x_2$ A $(u)(v)(u \in x_1 \wedge v \in x_1 \supset$ ((u, $v\rangle$ E $r_1 \equiv$ (Z'U, Z'u) $\in r_2$))). (Z *is* a similarity mapping *of* the relation r, on x, onto the relation r_2 on x_2.)

DEFINITION. $Sim(W_1, W_2)$ for $(Ez)Sim(z$, W,, $W_2)$. (W, and W_2 are similar ordered structures.)

Example. Let r, be the relation $<$ on the set of non-negative integers A, and let r_2 be the relation $<$ on the set of positive integers B. Let z be the set of all ordered pairs (x, x + I) for $x \in$ A. Then z is a similarity mapping of (r,, A)̄ onto $\langle r_2$, B).

EXERCISES

Prove:

4.24. $\vdash Sim(Z, X, Y) \supset Sim(\check{Z}, Y, X)$.

4.25. $\vdash Sim(Z, X, Y) \supset M(Z) \wedge M(X) \wedge M(Y)$.

DEFINITIONS

$Fld(X)$ for $\mathfrak{D}$(X) u $\mathfrak{R}$(X). (The *field* of X.)

$TOR(X)$ for $Rel(X) \wedge$ (X Tot $(Fld(X))$). (X is a total order.)

$WOR(X)$ for $Rel(X) \wedge$ (X We $(Fld(X))$). (X is a well-ordering relation.)

EXERCISES

Prove:

4.26. $\vdash (Sim(X, Y) \supset Sim(Y, X)) \wedge (Sim(X, Y) \wedge Sim(Y, U) \supset Sim(X, U))$.

4.27. $\vdash Sim(\langle X, Fld(X)\rangle, \langle Y, Fld(Y)\rangle) \supset (TOR(X) \equiv TOR(Y)) \wedge (WOR(X) \equiv WOR(Y))$.

If x is a total-order, then, the class of all total orders similar to x is called the order type of x. We are especially interested in the order types of well-ordering relations, but, since, in NBG, it turns out that all order types are proper classes (except the order type $\{0\}$ of 0), it is convenient to find a class W of well-ordered structures such that every well-ordering is similar to a unique element of W. This leads us to the study of ordinal numbers.

DEFINITIONS

E for $\{\langle x, y\rangle | x \in y\}$. (The membership relation)

Trans (X) for $(u)(u \in$ X $\supset u \subseteq X)$. (X is transitive.)

$Sect_Y(X$, Z) for Z $\subseteq$ X $\wedge$ $(u)(v)(u \in$ X $\wedge$ v E Z $\wedge$(u, $v\rangle$ E Y $\supset$ u E Z). (Z is a Y-section of X.)

$Seg_Y(X, U)$ for $\{x|x \in$ X $\wedge$ (x, $U\rangle \in$ Y). (The Y-segment of X determined by U.)

EXERCISES

Prove:

4.28. $\vdash Trans(X) \equiv (u)(v)(v \in u \wedge u \in X \supset v \in X)$.

4.29. $\vdash Trans(X) \equiv \bigcup(X) \subseteq X$.

430. $\vdash Trans(X) \wedge Trans(Y) \supset Trans(X \cup Y) \wedge Trans(X \cap Y)$.

431. $\vdash Seg_E(X, u) = X \cap u \wedge M(Seg_E(X, u))$.

4.32. $\vdash Trans(X) \equiv (u)(u \in X \supset Seg_E(X, u) = u)$.

433. t $E\ We\ X \wedge Sect_E(X, Z) \wedge Z \neq X \supset (Eu)(u$ E $X \wedge Z = Seg_E(X, u))$.

DEFINITIONS

$Ord(X)$ for (E We X) A $Trans(X)$.

(X is an ordinal class if and only if the $\in$-relation well-orders X and any member of X is a subset of X.)

On for $\{x|Ord(x)\}$. (Thus, $\vdash (x)(x \in On \equiv Ord(x))$.)

An ordinal class which is a set is called an ordinal number. On is the class of all ordinal numbers. Notice that a wf x $\in$ On is equivalent to a predicative wf, namely, the conjunction of the following wfs.

(a) $(u)(u \in x \supset$ u $\notin u)$;

(b) $(u)(u \subseteq x \wedge u \neq 0 \supset (Ev)(v \in$ u $\wedge (w)(w \in$ u $\wedge\, w \neq$ v $\supset v \in w \wedge w \notin v)))$;

(c) $(u)(u \in x \supset u \subseteq x)$.

(The conjunction of (a) and (b) is equivalent to E We **x**, and (c) is $Trans(x)$.) Hence, any wf which is predicative except for the presence of "On" is equivalent to a predicative wf, and, therefore, can be used in connection with the Class Existence Theorem. (Any wf On $\in$ Y can be replaced by $(Ey)(y \in$ Y$\wedge (z)(z \in$ y $\equiv z \in$ On)).)

EXERCISES

4.34. Prove: $\vdash 0 \in On$.

435. Let I stand for (0). Prove: $\vdash 1 \in On$.

We shall use small Greek letters a, β, y, $\delta, \tau, \ldots$ as restricted variables for ordinal numbers. Thus, $(\alpha)\mathscr{A}(\alpha)$ stands for $(x)(x \in On \supset \mathscr{A}(x))$, and $(E\alpha)\mathscr{A}(\alpha)$ stands for $(Ex)(x \in On\ A\ \mathscr{A}(x))$.

PROPOSITION 4.7

(1) $\vdash Ord(X) \supset (X \notin X\ A(u)(u \in X\ 3\ u \notin u))$
(2) $\vdash Ord(X) \wedge Y\ C\ X \wedge Trans(Y) \supset Y\ E\ X$
(3) $\vdash (Ord(X) \wedge Ord(Y)) \supset (Y\ C\ X \equiv Y \in X)$
(4) $\vdash Ord(X) \wedge Ord(Y) \supset (X \in Y \vee X = Y \vee Y \in X) \wedge$
$\sim(X \in Y \wedge Y \in X) \wedge \sim(X \in Y \wedge X = Y)$
(5) $\vdash Ord(X) \wedge Y \in X\ 3\ Y \in On$
(6) $\vdash E\ \mathbf{We}\ On$
(7) $\vdash Ord(On)$
(8) $\vdash\sim M(On)$
(9) $\vdash Ord(X) \supset X = On \vee X \in On$
(10) $\vdash y \subseteq On \wedge Trans(y) \supset y \in On.$

PROOF.

(1) If $Ord(X)$, then E is irreflexive on X; so, $(u)(u \in X \supset u \notin u)$; and if $X \in X, X \notin X$. Hence, $X \notin X$.

(2) Assume $Ord(X) \wedge Y\ C\ X \wedge Trans(Y)$. It is easy to see that Y is a proper E-section of X. Hence, by Exercises *4.32–4.33* (p. 185), $Y \in X$.

(3) Assume $Ord(X) \wedge Ord(Y)$. If $Y \in X$, then $Y \subseteq X$, since X is transitive; but $Y \neq X$ by (1); so, Y C X. Conversely, if Y C X, then, since Y is transitive, we have $Y \in X$, by *(2)*.

(4) Assume $Ord(X) \wedge Ord(Y) \wedge X \neq Y$. Now, $X\ n\ Y \subseteq X$ and $X\ n\ Y \subseteq Y$. Since X and Yare transitive, so is X n Y. If $X\ n\ Y\ C\ X$ and $X\ n\ Y\ C\ Y$, then, by (2), X n $Y \in X$ and $X\ n\ Y \in Y$; hence, $X\ n\ Y \in X\ n\ Y$, contradicting the irreflexivity of E on X. Hence, either X n $Y = X$ or $X\ n\ Y = Y$, i.e., $X \subseteq Y$ or $Y \subseteq X$. But $X \neq Y$. Hence, by (3), $X \in Y$ or $Y \in X$. Also, if $X \in Y$ and $Y \in X$, then, by (3), X C Y and $Y\ C\ X$, which is impossible. Clearly, $X \in Y \wedge X = Y$ is impossible, by (1).

(5) Assume $Ord(X) \wedge Y \in X$. We must show: E $\mathbf{We}$ Y and $Trans(Y)$. Since $Y \in X$ and $Trans(X)$, Y C X. Hence, since E $\mathbf{We}$ X, E $\mathbf{We}$ Y. Moreover, if $u \in Y$ and $v \in u$, then, by $Trans(X)$, $v \in X$. Since $E\ Con\ X$ and $Y \in$ X $\wedge\ v \in$ X, then $v \in Y$ or $v = Y$ or $Y \in v$. If either $v = Y$ or $Y \in v$, then, since E Tr X and $u \in Y \wedge v \in u$, we would have $u \in u$, contradicting (1). Hence, $v \in Y$. So, if $u \in Y$, then $u \subseteq Y$, i.e., $Trans(Y)$.

(6) By (1), E Irr On. Now, assume $X \subseteq On \wedge X \neq 0$. Let $a \in X$. If a is the least element of X, we are done. (By ***least element*** of X, we mean an element $v \in X$ such that $(u)(u \in X \wedge u \neq v \supset v \in u)$.) If not, then E $\mathbf{We}$ a, and $X\ n\ a \neq 0$; let β be the least element of X n a. It is obvious, using (4), that β is the least element of X.

(7) We must show $E\ \mathbf{We}\ On$ and $Trans(On)$. The first part is *(6)*. For the second, if $u \in On$ and $v \in u$, then, by (5), u $\in On$. Hence, $Trans(On)$.

(8) If $M(On)$, then, by (7), $On \in On$, contradicting (1).

(9) Assume $Ord(X)$. Then $X \subseteq On$. If $X \neq On$, then, by (3), $X \in On$.

(10) Substitute On for X and y for Y in *(2)*. By (8), y C On.

We see, from Proposition 4.7(9), that the only ordinal class which is not an ordinal number is the class On itself.

DEFINITION. $x <_0 y$ for $x \in On\ A\ y \in On\ A\ x \in y$
$x \leqslant_0 y$ for $y \in On \wedge (x = y \vee x <_0 y)$

Thus, for ordinals, $<_0$ is the same as $\in$; so, $<_0$ well-orders On. In particular, from Proposition 4.7(5), we see that any ordinal x is equal to the set of smaller ordinals.

PROPOSITION *4.8* (Transfinite Induction)

$$\vdash (\beta)[(\alpha)(\alpha \in \beta \supset a \in X) \supset \beta \in X] \supset On \subseteq X$$

(If, for any β, whenever all ordinals $<_0\beta$ are in X, then β is in X, then all ordinals are in *X.)*

PROOF. Assume that $(\beta)[(\alpha)(\alpha \in \beta \supset a \in X) \supset \beta \in X]$. Assume there is an ordinal in $On - X$. Then, since On is well-ordered by E, there is a least ordinal β in $On - X$. Hence all ordinals $<_0\beta$ are in X. So, by our hypothesis, β is in X, which is a contradiction.

Proposition *4.8* is used to prove that all ordinals have a given property *&(a)*. We let $X = \{x|\mathscr{A}(x) \wedge x \in On)$ and show that $(\beta)[(\alpha)(\alpha \in \beta \supset \&(a))\supset \mathscr{A}(\beta)]$.

DEFINITION. x' for $x \cup \{x\}$

PROPOSITION 4.9

(1) $\vdash (x)(x \in On \equiv x' \in On)$
(2) $\vdash (a)\sim(E\beta)(\alpha <_0 \beta <_0 \alpha')$
(3) $\vdash (\alpha)(\beta)(\alpha' = \beta' \supset \alpha = \beta)$

PROOF.

(1) $x \in x'$. Hence, if $x' \in On$, then $x \in On$, by Proposition 4.7(5). Conversely, assume $x \in On$, We must prove E $\mathbf{We}$ $(x \cup \{x\})$and $Trans(x \cup \{x\})$. Since E $\mathbf{We}$ x and $x \notin x$, E Irr $(x \cup \{x))$. Also, if $y \# 0 \wedge y \subseteq (x\ U\ \{x\})$, then either $y = \{x)$,in which case the least element of y is x, or $y\ n\ x \neq 0$; the least element of $y \cap x$ is then the least element of y. Hence, E $\mathbf{We}$ $(x \cup \{x\})$. Also, if y $\in x \cup \{x)$and $u \in$y, then $u \in x$. Thus, $Trans(x\ U\ \{x))$.

(2) Assume $a <_0 \beta <_0 \alpha'$. Then $a \in \beta \wedge \beta \in a'$. Since $a \in \beta$, $\beta \notin \alpha$, and $\beta \neq a$, by Proposition 4.7(4), contradicting $\beta \in a'$.

(3) Assume a' $=$ I)'. Then I) $<_0$ a', and, by Part (2), I) $\leqslant_0$ a. Similarly, a $\leqslant_0 \beta$. Hence, a $= \beta$.

DEFINITION. $Suc(X)$ for X E On $\wedge\ (E\alpha)(X =$ a'). (X is a successor ordinal)

DEFINITION. K_I for $\{x|x = 0 \vee Suc(x)\}$. (The class of ordinals of the first kind)

DEFINITION. ω for $\{x|x \in K_I \wedge (u)(u \in$ x $\supset u \in K_I)$. ω is the class of all ordinals a of the first kind such that all ordinals $<_0$ a are also of the first kind.

Examples. t $0 \in \omega \wedge 1 \in w$. Remember that $1 = (0)$.

PROPOSITION 4.10.

(I) t $(\alpha)(\alpha \in \omega \equiv$ a' $\in \omega)$
(2) $\vdash M(\omega)$
(3) $\vdash 0 \in X \wedge (u)\ (u \in X \supset u' \in X) \supset \omega \subseteq X$
(4) $\vdash (\alpha)(\alpha \in \omega$ A $\beta <_0 \alpha \supset \beta \in \omega)$.

PROOF.

(1) Assume $\alpha \in$ w. Now, $Suc(\alpha')$. Hence, a' $\in K_I$. Also, if $\beta \in$ a', then $\beta \in \alpha$ or $\beta =$ a. Hence, $\beta \in K_I$. Thus, a' $\in$ w. Conversely, if a' $\in$ w, then, since a $\in$ a', and $(\beta)(\beta \in$ a $\supset \beta \in$ a'), it follows that a $\in \omega$.

(2) By the Axiom of Infinity (I), there is a set x such that $0 \in$ x and (u) $(u \in$ x $\supset$ u' $\in$ x). We shall prove $\omega \subseteq$ x. Assume not. Let a be the least ordinal in $\omega -$ x. Clearly, a $\neq 0$, since $0 \in$ x. Hence, $Suc(\alpha)$. So, $(E\beta)(\alpha =$ I)'). Let S be an ordinal such that a $= \delta'$. Then S $<_0$ a, and, by Part (1), $\delta \in w$. Therefore, S $\in$ x. Hence, $\delta' \in$ x. But a $= \delta'$. Therefore, a $\in$ x, which yields a contradiction. Thus, w $\subseteq$ x. So, $M(\omega)$, by Proposition 4.6.

(3) This is proved by a procedure similar to'that used for Part (2). (4) is left as an easy exercise.

The elements of ω are called *finite ordinals*. We shall use the standard notation: 1 for 0'; 2 for 1'; 3 for 2', etc. Thus, $0 \in \omega$, $1 \in \omega$, $2 \in \omega$, $3 \in \omega, \ldots$. The non-zero ordinals which are not successor ordinals are called *limit* ordinals, or ordinals of the second kind.

DEFINITION. $Lim(x)$ for $x \in$ On $\wedge\, x \notin K_I$.

EXERCISE 4.36. Prove: t $Lim(\omega)$.

PROPOSITION 4.11

(1) $\vdash (x)(x \subseteq On \supset (\bigcup(x) \in On$ A $(\alpha)(\alpha \in x \supset$ a $\leqslant_0 \bigcup(x)) \wedge (\beta)((\alpha)(\alpha \in x \supset \alpha \leqslant_0 \beta) \supset \bigcup(x) \leqslant_0 \beta)))$. (If x is a set of ordinals, then $\bigcup(x)$ is an ordinal which is the least upper bound of x.)

(2) $\vdash (x)(x \subseteq On \wedge x \neq 0$ A $(\alpha)(\alpha \in x \supset (E\beta)(\beta \in x \wedge \alpha <_0 \beta)) \supset Lim(\bigcup(x)))$. (If x is a non-empty set of ordinals without a maximum, then $\bigcup(x)$ is a limit ordinal.)

PROOF.

(1) Assume x $\subseteq$ On. $\bigcup(x)$, as a set of ordinals, is well-ordered by E. Also, if $\alpha \in \bigcup(x) \wedge$ I) $\in$ a, then there is some y with y $\in$ x $\wedge$ a $\in \gamma$. Then I) $\in$ a and $\alpha \in \gamma$; since every ordinal is transitive, $\beta \in$ y. So, $\beta \in \bigcup(x)$. Hence, $\bigcup(x)$ is transitive, and therefore $\bigcup(x) \in$ On. In addition, if a $\in$ x, then a $\subseteq \bigcup(x)$; so, $\alpha \leqslant_0 \bigcup(x)$, by Proposition 4.7(3). Assume now that $(\alpha)(\alpha \in x \supset$ a $\leqslant_0 \beta)$. Clearly, if $\delta \in \bigcup(x)$, then there is some y such that S $\in$ y $\wedge$ y $\in$ x. Hence, $\gamma \leqslant_0 \beta$ and so, $\delta <_0 \beta$. Therefore, $\bigcup(x) \subseteq$ I), and, by Proposition 4.7(3), $\bigcup(x)$ cop.

(2) Assume x $\neq 0 \wedge$ x $\subseteq$ On $\wedge\ (\alpha)(\alpha \in$ x $\supset (E\beta)(\beta$ E x $\wedge$ a $<_0 \beta)$. If $\bigcup(x) = 0$, then, a $\in x$ implies a $= 0$. So, x $= 0$ or x $=$ I, which contradicts our assumption. Hence, $\bigcup(x) \neq 0$. Assume that $Suc(\bigcup(x))$. Then $\bigcup(x) =$ y' for some y. By Part (1), $\bigcup(x)$ is a least upper bound of x. Therefore, γ is not an upper bound of x; there is some S $\in$ x with y $<_0 \delta$. But then $\delta = \bigcup(x)$, since $\bigcup(x)$ is an upper bound of x. Thus, $\bigcup(x)$ is a maximum element of x, contradicting our hypothesis. Hence, $\sim Suc(\bigcup(x))$, and $Lim(x)$ is the only possibility left.

EXERCISE 4.37. *Prove*: $\vdash (\alpha)((Suc(\alpha) \supset (\bigcup(\alpha))' =$ a$) \wedge (Lim(\alpha) \supset \bigcup(\alpha) =$ a$))$.

We can now state and prove another form of transfinite induction.

PROPOSITION 4.12 (Transfinite Induction: Second Form)

(1) t $0 \in$ X $\wedge\ (\alpha)(\alpha \in$ X $\supset$ a' $\in$ X) $\wedge\ (\alpha)(Lim(\alpha)$ A $(\beta)(\beta <_0$ a $\supset \beta \in X) \supset \alpha \in X) \supset On \subseteq X$

(2) (Induction up to δ) $\vdash 0 \in$ X $\wedge\ (\alpha)(\alpha' <_0$ S $\wedge$ a $\in$ X $\supset$ a' E $X)$ A $(\alpha)(\alpha <_0 \delta \wedge Lim(\alpha) \wedge (\beta)(\beta <_0 \alpha \supset \beta \in X) \supset$ a $\in X) \supset \delta \subseteq X$

PROOF.

(1) Assume the antecedent of the proposition. Let $Y = \{x|x \in On \wedge (\alpha)(\alpha \leqslant_0 x \supset \alpha \in$ x)). It is then easy to prove that $(\alpha)(\alpha <_0 \gamma \supset \alpha \in Y) \supset \gamma \in Y$. Hence, by Proposition 4.8, $On \subseteq Y$. But $Y \subseteq X$. Hence, $On \subseteq X$.

(2) is left as an exercise.

Set theory depends heavily upon definitions by transfinite induction, which are justified by the following theorems.

PROPOSITION 4.13

(1) t $(X)(E_1 Y)(Fnc($Y$) \wedge \mathfrak{D}(Y) = On \wedge (\alpha)(Y\ `\alpha = X\ `(\alpha \upharpoonright Y)))$. (Given X, there is a unique function Y defined on all ordinals such that the value of

Y at a is the value of X applied to the restriction of Y to the set of ordinals $<_0 \alpha$.)

(2) $\vdash (x)(X_1)(X_2)(E_1 Y)(Fnc(Y)$ A $\mathfrak{D}(Y)$ = On A YO = x $\wedge$ (a)(Y'(α') $= X_1$ '(Y 'a)) $\wedge$ $(\alpha)(Lim(\alpha) \supset$ Y 'a $= X_2$ '$(\alpha$ 1 Y))).

(3) (Induction up to δ) $\vdash (x)(X_1)(X_2)(E_1 Y)(Fnc(Y)$ A $\mathfrak{D}(Y) = \delta$ A Y '0 = x $\wedge$ $(\alpha)(\alpha' <_0 \delta \supset Y$ '(a') $= X_1$ '(Y 'a)) A $(\alpha)(Lim(\alpha) \wedge$ a $<_0 \delta \supset$ Y 'a = X_2 '$(\alpha$ 1 Y))).

PROOF. Let Y, = $\{u|Fnc(u) \wedge \mathfrak{D}(u) \in$ On $\wedge$ $(\alpha)(\alpha \in \mathfrak{D}(u) \supset u$'$\alpha$ = X '$(\alpha$ 1 u)). Now, if $u_1 \in$ Y, and $u_2 \in Y_1$, then u, $\subseteq u_2$ or $u_2 \subseteq u_1$. For, let $\gamma_1 = \mathfrak{D}(u_1)$ and $\gamma_2 = \mathfrak{D}(u_2)$. Either $\gamma_1 \leqslant \gamma_2$ or $\gamma_2 \leqslant_0$ y,, say $\gamma_1 \leqslant_0 \gamma_2$. Let w be the set of all ordinals a $<_0 \gamma_1$ such that u, 'a $\neq u_2$ 'a; assume w $\neq$ 0, and let η be the least ordinal in w. Then for all $\beta <_0$ q, u, '$\beta = u_2$ 'β. Hence, η 1 u_1 = η 1 u_2. But u_1 'η = X '$(\eta$ 1 u,) and u_2 'η = X '$(\eta$ 1 $u_2)$; and so, u, '$\eta = u_2$ 'η, contradicting our assumption. Therefore w = 0, i.e., for all a $<_0$ y,, u_1 'a = u_2 'α. Hence, $u_1 = \gamma_1$ 1 u, = γ_1 1 $u_2 \subseteq u_2$. Thus, any two functions in Y, agree in their common domain. Let Y = $\bigcup(Y_1)$. We leave it to the reader to prove that Y is a function the domain of which is either an ordinal or the class On, and $(\alpha)(\alpha \in \mathfrak{D}$(Y) $\supset Y$ 'a = X '$(\alpha$ 1 Y)). That $\mathfrak{D}$(Y) = On follows easily from the observation that, if $\mathfrak{D}(Y) = \delta$ and if we let W = Y $\cup$ {$\langle\delta$, X 'Y)), then W $\in$ Y,; so, W $\subseteq$ Y and $\delta \in \mathfrak{D}$(Y) = δ, which contradicts the fact that $\delta \notin$ 6. The uniqueness of Y follows by a simple transfinite induction (Proposition 4.12). The proof of (2) is similar to that of (1), and (3) follows from (2).

Using Proposition 4.13, one can introduce new function letters by transfinite induction.

Examples.

1. Ordinal addition. In Proposition 4.13(2), take

$$x = \beta, \quad X_1 = \{(u, v\rangle | v = u'), \text{ and } X_2 = \{(u, v\rangle | v = \bigcup(\mathfrak{R}(u))\}.$$

Hence, for each ordinal β, there is a unique function Y_β such that Y_β '0 = $\beta \wedge$ $(\alpha)(Y_\beta$ '(a') = $(Y_\beta$ 'a)') $\wedge$ $(\alpha)(Lim(\alpha) \supset Y_\beta$ 'a = $\bigcup(Y_\beta$ ''a))). Hence, there is a unique binary function $+_0$ with domain On^2 such that, for any ordinals β and γ, $+_0(\beta, \gamma) = Y_\beta$ 'γ. As usual, we write $\beta +_0 \gamma$ instead of $+_0(\beta, \gamma)$. Notice that

$$\beta +_0 0 = \beta$$

$$\beta +_0 (\gamma') = (\beta +_0 \gamma)'$$

$$Lim(\alpha) \supset \beta +_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta +_0 \tau).$$

In particular,

$$\beta +_0 1 = \beta +_0 (0') = (\beta +_0 0)' = \beta'.$$

2. Ordinal multiplication. In Proposition 4.13(2), take x = 0, $X_1 = \{\langle u, v\rangle |$ u = $u +_0 \beta)\}$, and X_2 = ((u, $v\rangle | v = \bigcup(\mathfrak{R}(u))$. Then, as in Example 1, one obtains a function β x$_0\gamma$ with the properties

$$\beta \times_0 0 = 0$$

$$\beta \times_0 (\gamma') = (\beta \times_0 \gamma) +_0 \beta$$

$$Lim(\alpha) \supset \beta \times_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta \times_0 \tau)$$

EXERCISE 4.38. *Justify the following definition of ordinal exponentiation.*[†]

$$exp(\beta, 0) = 1$$

$$exp(\beta, \gamma') = exp(\beta, \gamma) \times_0 \beta$$

$$Lim(\alpha) \supset exp(\beta, \text{a}) = \bigcup_{0 <_0 \tau <_0 \alpha} exp(\beta, \tau).$$

For any set X, let E_X be the membership relation restricted to X, that is, $E_X = \{\langle x, y\rangle | x \in y$ A $x \in X \wedge y \in X\}$.

PROPOSITION 4.14.[‡] Let R be a well-ordering relation on a class Y, that is, R We Y. Let F be a function from Y into Y such that, *for* any u, v in Y, *if* (u, u) $\in$ R, then (F 'u, F '$v\rangle \in$ R. Then, *for* all u in Y, u = F 'u $v\langle u$, F 'u) $\in$ R.

PROOF. Let $X = \{u | \langle F$ 'u, u) $\in$ R). We wish to show that X = 0. Assume X $\neq$ 0. Since X $\subseteq$ Y and R well-orders Y, there is an R-least element u_0 of X. Hence, (F 'u_0, $u_0\rangle \in$ R. Therefore, (F '(F 'u_0), F '$u_0\rangle \in$ R. Thus, F '$u_0 \in$ X, but F 'u_0 is R-smaller than u_0, contradicting the definition of u_0.

As a special case of Proposition 4.14, if Y is a class of ordinals, F: Y → Y, and F is increasing on Y (that is, a $\in Y \wedge \beta \in$ Y $\wedge$ a $<_0 \beta \supset$ F 'a $<_0$ F 'β), then a $\leqslant_0$ F 'a for all α in Y.

COROLLARY 4.15. Let a $<_0 \beta$ and y $\subseteq$ a, *i.e.* let y be a subset of a segment *of* β. Then $\langle E_\beta, \beta\rangle$ is not similar to $\langle E_y$, y).

PROOF. Assume f is a function from β onto y such that, for u, u in β, if $u <_0 v$, then f 'u $<_0 f$ 'v. Since the range of f is y, f 'a $\in$ y. But y $\subseteq$ a. Hence, f 'a $<_0$ a. But, by the special case of Proposition 4.14 mentioned above (with y = β and R = E_β), a $\leqslant_0$ f 'a, which yields a contradiction.

COROLLARY 4.16. (1) For a $\neq \beta$, $\langle E_\alpha$, a) and $\langle E_\beta, \beta\rangle$ are not similar. (2) For any a, iff is a similarity mapping *of* $\langle E_\alpha$, a) with $\langle E_\alpha$, a), then f is the identity mapping, *i.e.* f '$\beta = \beta$ for all $\beta <_0$ a.

[†] We use the notation exp(β, *a)* instead of β^α in order to avoid confusion with the notation X^Y to be introduced later (p. 193).

[‡] From this point on we shall express many theorems of NBG in English by using the corresponding informal English translations. This is done to avoid writing mile-long wfs which are difficult to decipher, and only in cases where the reader can easily produce from the English version the precise wf of NBG.

PROOF. (1) By Corollary 4.15. (2) By Proposition 4.14, f $‘\beta \geqslant_0 \beta$ for all $\beta <_0$ a. But, again by Proposition 4.14, $(\check{f})$ $‘\beta \geqslant_0 \beta$ for all $\beta <_0$ a. Hence, $\beta =$ $(\check{f})$ '(f $‘\beta) \geqslant_0 f‘\beta \geqslant_0 \beta$, and, therefore, f $‘\beta = \beta$.

PROPOSITION 4.17. Assume that R is a well-ordering of a non-emply set u, *i.e.* R We $u \wedge u = Fld(R) \wedge u \neq 0$. Then there is a unique ordinal y and a *unique similarity* mapping of $(E_\gamma, \gamma\rangle$ with (R, u), *i.e.* every non-emply *well-ordered set* is similar to a unique ordĭnal.

PROOF. Let $Z = \{\langle v, w\rangle | w \in u - v \wedge (z)(z \in u - v \supset \langle z,$ w) $\notin R)$. Z is a function such that, if v is a subset of u and $u -$ v $\neq$ 0, then Z $‘v$ is the R-least element of $u -$ v. Let X = $((v, w\rangle | \langle \mathfrak{R}(v),$ w) $\in$ Z)). Now we use a definition by transfinite induction (Proposition 4.13) to obtain a function Y with *On* as its domain such that $(\alpha)(Y$ 'a $= X‘(\alpha \rceil$ Y)). Let W = $\{\alpha | Y“\alpha \subseteq u \wedge u - Y“\alpha \neq 0\}$. Clearly, if a $\in$ W and $\beta \in$ a, then $\beta \in$ W. Hence, either W = On or W is some ordinal y. (For, if W # On, let y be the least ordinal in On $- W$.) If a $\in$ W, then Y 'a = X $‘(\alpha \rceil$ Y) is the R-least element of $u - Y''\alpha$; so, Y'a $\in$ u, and, if $\beta \in$ a, then Y'a $\neq$ Y$‘\beta$. Thus, Y is a one-one function on W and the range of Y restricted to W is a subset of u. Now, let f = $(W \rceil$ Y), i.e. let f be the inverse of Y restricted to W. Then f is a one-one function with domain a subset of u and range W. So, by the Replacement Axiom (R), W is a set. Hence, W is some ordinal y. Let g = $\gamma \rceil$ Y. Then g is a one-one function with domain y and range a subset u_1 of u. We must show that $u_1 = u$ and that, if a and β are in γ and $\beta <_0$ a, then (g $‘\beta$, g 'a) $\in$ R. Assume a and β are in y and $\beta <_0$ a. Then g “$\beta \subseteq$ g'' a and, since g 'a $\in u -$ g “α, g 'a $\in u - g“ \beta$. But g $‘\beta$ is the R-least element of $u -$ g'' β. Hence, (g $‘\beta$, g 'a $> \in$ R. It remains to prove that $u_1 =$ u. Now, $u_1 =$ Y'' y. Assume u $- u_1 \neq 0$. Then y $\in$ W. But $W =$ y, which yields a contradiction. Hence $u =$ u,. That y is unique follows from Corollary 4.16.

PROPOSITION 4.18. *Let* R be a well-ordering of a proper class X such that, for each y E X, the class of *all* R-predecessors of y in X (*i.e.* the R-segment in X determined by y) is a set. Then R is similar to E_{On}, *i.e.* there is a one-one mapping h of On onto X such that a $\in \beta$ implies (h 'a, h $‘\beta\rangle \in$ R.

PROOF. Proceed as in the proof of Proposition 4.17. Here, however, W = On; also, one proves that $\mathfrak{R}(Y) =$ X by using the hypothesis that every R-segment of X is a set. (If X $- \mathfrak{R}(Y) \neq 0$, then, if w is the R-least element of X $- \mathfrak{R}(Y)$, the proper class On is the range of $\check{Y}$, while the domain of $\check{Y}$ is the R-segment of X determined by w, contradicting the Replacement Axiom.)

3. Equinumerosity. Finite and Denumerable Sets

We say that two classes X and Y are equinumerous if and only if there is a one-one function F with domain X and range Y. We shall denote this by X $\underset{F}{\cong}$ Y.

DEFINITIONS

$X \underset{F}{\cong} Y$ for $(Fnc(F) \wedge Un_1(F) \wedge \mathfrak{D}(F) = X \wedge \mathfrak{R}(F) = Y\rangle$

X $\cong$ Y for $(EF)(X \underset{F}{\cong}$ v)

Notice that $\vdash (x)(y)(x \cong y \equiv (Ez)(x \underset{z}{\cong}$ y)). Hence, a wf x $\cong y$ is predicative (i.e., is equivalent to a wf using only set quantifiers).

Clearly, if $X \underset{F}{\cong}$ Y, then Y $\underset{\check{F}}{\cong}$ X; and if X $\underset{F}{\cong}$ Y and Y $\cong$ Z, then X $\underset{H}{\cong}$ Z, where H is the composition G ° F of F and G, that is, G ° F = ((x, $y\rangle | (Ez)(\langle x,$ z) $\in$ $F \wedge \langle z, y\rangle \in$ G)). Hence, we have the following theorem.

PROPOSITION 4.19. (1) $X \cong X$. (2) $X \cong Y \supset Y \cong X$. (3) $X \cong Y \wedge Y \cong Z \supset$ $X \cong$ Z.

PROPOSITION 4.20. (1) (X $\cong$ Y $\wedge$ $X_1 \cong Y_1$ A X n $X_1 = 0$ A Y n Y, = 0) $\supset X \cup X_1 \cong Y \cup Y_1$. (2) $(X \cong Y \wedge X_1 \cong Y_1) \supset X \times X_1 \cong Y \times Y_1$. (3) X X $\{y\} \cong$ X. (4) X X Y $\cong$ Y X X. (5) (X X Y) X $Z \cong$ X X (Y X Z).

PROOF. (1) Let $X \underset{F}{\cong}$ Y and X$^1 \underset{G}{\cong}$ Y,. Then X u X_1 $\underset{F \cup G}{\cong}$ Y u Y,. (2) Let $X \underset{F}{\cong}$ Y and $X^1 \underset{G}{\cong}$ Y,. Let

W = $\{\langle u, v\rangle | (Ex)(Ey)(x \in$ X $\wedge y \in X_1 \wedge u = \langle x, y\rangle$ A $v =$ (F'x, $G‘y\rangle)\}$.

Then X $\times$ $X_1 \underset{W}{\cong} Y \times Y_1$.

(3) Let F = $\{(u, v\rangle | u \in X \wedge v = \langle u, y\rangle\}$. Then $X \underset{F}{\cong} X \times \{y\}$.

(4) Let

F = $\{(u, v\rangle | (Ex)(Ey)(x \in$ X $\wedge$y E $Y \wedge u = \langle x, y\rangle$ A $v = \langle y, x\rangle)\}$

Then $X \times Y \underset{F}{\cong} Y \times X$.

(5) Let

F = $\{(u, v\rangle | (Ex)(Ey)(Ez)(x \in$ X $\wedge$y $\in$ Y $\wedge$ z $\in$ Z $\wedge$ $u = \ll x, y >\ z >$ A $v = \langle x, \langle y, z\rangle\rangle)\}$.

Then (X $\times$ Y) $\times$ Z $\underset{F}{\cong}$ X $\times$ (Y $\times$ Z).

DEFINITION. X^Y = $\{u | u :$ Y $\rightarrow$ X$\}$. X^Y is the class of all sets which are functions from Y into X.

EXERCISES

Prove:

4.39. $\vdash (X)(Y)(EX_1)(EY_1)(X \cong X_1$ A $Y \cong Y_1$ A $X_1 \cap Y_1 = 0)$.

4.40. $\vdash \mathcal{P}(x) \cong 2^x$. (Remember that 2 = {0, 1}.)

4.41. $\vdash \sim M(Y) \supset X^Y = 0$.

4.42. $\vdash M(x^y)$.

PROOF. (1) By Corollary 4.15. *(2)* By Proposition *4.14,* $f'\beta \geqslant_0 \beta$ for all $\beta <_0 a$. But, again by Proposition *4.14,* $(\breve{f})'\beta \geqslant_0 \beta$ for all $\beta <_0 a$. Hence, $\beta = (\breve{f})'(f'\beta) \geqslant_0 f'\beta \geqslant_0 \beta$, and, therefore, $f'\beta = \beta$.

PROPOSITION *4.17. Assume that* R *is a well-ordering of a non-empty set u, i.e.* R *We* $u \wedge u = Fld(R) \wedge u \neq 0$. *Then there is a unique ordinal y and a unique similarity mapping of* $\langle E_\gamma, y)$ *with* (R, *u), i.e. every non-empty well-ordered set is similar to a unique ordżnal.*

PROOF. Let $Z = \{\langle v, w\rangle | w \in u - v \wedge (z)(z \in u - v \supset (2, w\rangle \notin R)$. Z is a function such that, if v is a subset of u and $u - v \neq 0$, then $Z'v$ is the R-least element of $u - v$. Let $X = \{(v, w\rangle | \langle \mathfrak{R}(v), w) \in Z))$. Now we use a definition by transfinite induction (Proposition *4.13)* to obtain a function Y with *On* as its domain such that $(\alpha)(Y'a = X'(\alpha \upharpoonleft Y))$. Let $W = \{\alpha | Y''\alpha \subseteq u \wedge u - Y''\alpha \neq 0\}$. Clearly, if $a \in W$ and $\beta \in a$, then $\beta \in W$. Hence, either $W = On$ or W is some ordinal y. (For, if $W \# On$, let y be the least ordinal in $On - W$.) If $a \in W$, then $Y'a = X'(\alpha \upharpoonleft Y)$ is the R-least element of $u - Y''\alpha$; so, $Y'a \in u$, and, if $\beta \in a$, then $Y'a \neq Y'\beta$. Thus, Y is a one-one function on W and the range of Y restricted to W is a subset of u. Now, let $f = (W \upharpoonleft Y)$, i.e. let f be the inverse of Y restricted to W. Then f is a one-one function with domain a subset of u and range W. So, by the Replacement Axiom (R), W is a set. Hence, W is some ordinal y. Let $g = \gamma \upharpoonleft Y$. Then g is a one-one function with domain y and range a subset u_1 of u. We must show that $u_1 = u$ and that, if a and β are in γ and $\beta <_0 a$, then $(g'\beta, g'a) \in$ R. Assume a and β are in y and $\beta <_0 a$. Then $g''\beta \subseteq g''a$ and, since $g'a \in u - g''a, g'a \in u - g''\beta$. But $g'\beta$ is the R-least element of $u - g''\beta$. Hence, $(g'\beta, g'a > \in$ R. It remains to prove that $u_1 = u$. Now, $u_1 = Y''y$. Assume $u - u_1 \neq 0$. Then $y \in W$. But $W = y$, which yields a contradiction. Hence $u = u,$. That y is unique follows from Corollary *4.16.*

PROPOSITION 4.18. *Let* R *be a well-ordering of a proper class* X *such that, for each y* E X, *the class of all R-predecessors of y in X (i.e. the R-segment in X determined by y) is a set. Then* R *is similar to* E_{On}, *i.e. there is a one-one mapping h of On onto X such that* $a \in \beta$ *implies* $(h'a, h'\beta\rangle \in$ R.

PROOF. Proceed as in the proof of Proposition *4.17.* Here, however, $W = On$; also, one proves that $\mathfrak{R}(Y) = X$ by using the hypothesis that every R-segment of X is a set. (If $X - \mathfrak{R}(Y) \neq 0$, then, if w is the R-least element of $X - \mathfrak{R}(Y)$, the proper class *On* is the range of $\check{Y}$, while the domain of $\check{Y}$ is the R-segment of X determined by w, contradicting the Replacement Axiom.)

3. Equinumerosity. Finite and Denumerable Sets

We say that two classes X and Y are *equinumerous* if and only if there is a one-one function F with domain X and range Y. We shall denote this by $X \underset{F}{\cong} Y$.

DEFINITIONS

$$X \underset{F}{\cong} Y \quad \text{for} \quad (Fnc(F) \wedge Un_1(F) \wedge \mathfrak{D}(F) = X \wedge \mathfrak{R}(F) = Y)$$

$$X \cong Y \quad \text{for} \quad (EF)(X \underset{F}{\cong} {}^{V})$$

Notice that $\vdash (x)(y)(x \cong y \equiv (Ez)(x \underset{z}{\cong} y))$. Hence, a wf $x \cong y$ is predicative (i.e., is equivalent to a wf using only set quantifiers).

Clearly, if $X \underset{F}{\cong} Y$, then $Y \underset{\breve{F}}{\cong} X$; and if $X \underset{F}{\cong} Y$ and $Y \underset{G}{\cong} Z$, then $X \underset{H}{\cong} Z$, where H is the composition $G \circ F$ of F and G, that is, $G \circ F = \{(x, y\rangle | (Ez)(\langle x, z) \in F \wedge \langle z, y) \in G))$. Hence, we have the following theorem.

PROPOSITION *4.19.* (1) $X \cong X$. *(2)* $X \cong Y \supset Y \cong X$. *(3)* $X \cong Y \wedge Y \cong Z \supset X \cong Z$.

PROPOSITION *4.20.* (1) $(X \cong Y \wedge X_1 \cong Y_1 \wedge X \cap X_1 = 0 \wedge Y \cap Y_1 = 0) \supset X \cup X_1 \cong Y \cup Y_1$. *(2)* $(X \cong Y \wedge X_1 \cong Y_1) \supset X \times X_1 \cong Y \times Y,$. (3) $X \times \{y\} \cong X$. (4) $X \times Y \cong Y \times X$. (5) $(X \times Y) \times Z \cong X \times (Y \times Z)$.

PROOF. (1) Let $X \underset{F}{\cong} Y$ and $X_1 \underset{G}{\cong} Y,$. Then $X \cup X, \underset{F \cup G}{\cong} Y \cup Y,$. *(2)* Let $X \underset{F}{\cong} Y$ and $X_1 \underset{G}{\cong} Y_1$. Let

$$W = \{\langle u, v\rangle | (Ex)(Ey)(x \in X \wedge y \in X_1 \wedge u = \langle x, y\rangle \wedge v = \langle F'x, G'y\rangle)\}.$$

Then $X \times X_1 \underset{W}{\cong} Y \times Y,$.

(3) Let $F = \{(u, v\rangle | u \in X \wedge v = \langle u, y\rangle\}$. Then $X \underset{F}{\cong} X \times (y)$.

(4) Let

$$F = \{\langle u, v\rangle | (Ex)(Ey)(x \in X \wedge y \in Y \wedge u = \langle x, y\rangle \wedge v = \langle y, x\rangle)\}.$$

Then $X \times Y \underset{F}{\cong} Y \times X$.

(5) Let

$$F = \{\langle u, v\rangle | (Ex)(Ey)(Ez)(x \in X \wedge y \in Y \wedge z \in Z \wedge u = \langle\langle x, y\rangle, z\rangle \wedge v = \langle x, \langle y, z\rangle\rangle)\}.$$

Then $(X \times Y) \times Z \underset{F}{\cong} X \times (Y \times Z)$.

DEFINITION. $X^Y = \{u | u : Y \to X\}$. X^Y is the class of all sets which are functions from Y into X.

EXERCISES

Prove:

439. $\vdash (X)(Y)(EX_1)(EY_1)(X \cong X_1 \wedge Y \cong Y_1 \wedge X_1 \cap Y_1 = 0)$.

4.40. $\vdash \mathcal{P}(x) \cong 2^x$. *(Remember that* $2 = (0, 1\}$.)

4.41. $\vdash \sim M(Y) \supset X^Y = 0$.

4.42. $\vdash M(x^y)$.

4.43. $\vdash X^0 = (0) = 1.$
4.44. $\vdash Y \neq 0 \supset 0^Y = 0.$
4.45. $\vdash X \cong Y \wedge Z \cong Z_1 \subset X^Z \cong Y^{Z_1}.$
4.46. $\vdash X$ n $Y = 0 \supset Z^{X \cup Y} \cong Z^X$ x $Z^Y.$
4.47. $\vdash (X^Y)^Z \cong X^{Y \times Z}$, **except when** $Y = 0 \wedge \sim M(Z).$
4.48. $\vdash (X$ x $Y)^Z \cong X^Z$ x $Y^Z.$
4.49. $\vdash (x)(R)(R\ We\ x \supset (E\alpha)(x \cong a))$. **(Every well-ordered set is equinumerous with some ordinal.)**

One can define a partial order $\preccurlyeq$ on classes such that, intuitively, $X \preccurlyeq Y$ if X has the same number or fewer elements than Y.

DEFINITION. $X \preccurlyeq Y$ for $(EZ)(Z \subseteq Y \wedge X \cong Z)$ (i.e., X is equinumerous with a subclass of Y).

DEFINITION. $X \prec Y$ for $X \preccurlyeq Y \wedge \sim (X \cong Y)$
Hence, $\vdash X \preccurlyeq Y \equiv (X \prec Y \vee X \cong Y)$.

EXERCISES

Prove:
4.50. **t** $X \preccurlyeq Y \wedge \sim M(X) \supset \sim M(Y).$
4.51. **t** $X \preccurlyeq Y \wedge (EZ)(Z\ We\ Y) \supset (EZ)(Z\ We$ **X).**

PROPOSITION 4.21
(1) $\vdash X \preccurlyeq X \wedge \sim (X \prec X)$
(2) $\vdash X \subseteq Y \supset X \preccurlyeq Y$
(3) $\vdash X \preccurlyeq Y \wedge Y \preccurlyeq Z \supset X \preccurlyeq Z$
(4) (Schroder-Bernstein) $\vdash X \preccurlyeq Y \wedge Y \preccurlyeq X \supset X \cong Y$

PROOF.

(3) Assume $X \cong Y, \wedge Y_1 \subseteq Y \wedge Y \cong Z_1 \wedge Z_1 \subseteq Z$. Let H be the composition of F and G. $\overset{F}{\text{T}}$hen $\mathfrak{R}(H) \subseteq Z \wedge X \overset{G}{\cong} \mathfrak{R}(H)$.

(4) There are many proofs of this non-trivial theorem. The following is a new one devised by Hellman [1961]. Lemma: Assume X n $Y = 0$, X n $Z = 0$, $Y \cap Z = 0$, and let $X \cong X \cup Y$ u Z. Then there is a G such that $X \cong X \cup Y$. (Roof. Define a function H on a subclass of X x ω as follows: ((u, k), a) $\in$ H if and only if $u \in X$ and $k \in \omega$ and there is a function f with domain k' such that f '0 = F 'u and, if $j \in k$, then f $'j \in X \wedge$ f '(j') = F '(f 'j) $\wedge$ f 'k = v. Thus, H '((u, 0)) = F 'u, H '($\langle u$, l)) = F '(F 'u) if F '$u \in X$, and H '($\langle u$, 2)) = F '(F '(F 'u)) if F 'u and F '(F 'u) are in X, etc. Let X* be the class of all $u \in X$ such that $(Ey)(y \in \omega \wedge \langle u, y\rangle \in \mathfrak{D}(H) \wedge H$ '($\langle u$, y)) $\in$ Z). Let Y* be the class of all $u \in X$ such that $(y)(y \in \omega \wedge$ (u, y) $\in \mathfrak{D}(H) \supset H$ '($\langle u$, y)) $\notin$ Z). Then X = X* u Y*. Now define G as follows: $\mathfrak{D}(G) =$ X, and, if $u \in$ X*, then G 'u = u, whereas if $u \in$ Y*, then G 'u = F 'u. Then $X \underset{G}{\cong} X \cup Y$

(Exercise).) Now, to prove the Schröder-Bernstein Theorem: assume $X \ncong Y_1 \wedge Y_1 \subseteq Y \wedge Y \underset{G}{\cong} X_1 \wedge X_1 \subseteq X$. Let $A = G$ "$Y_1 \subseteq X_1 \subseteq X$. But $A \cap (X_1 - A) =$ 0, $A \cap (X - X_1) = 0$, and (X – X,) n $(X_1 - A) = 0$. Also, $X = (X - X_1)$ u $(X_1 - A) \cup A$, and the composition H of F and G is a one-one function with domain X and range A. Hence, $A \ncong X$. So, by the Lemma, there is a one-one function D such that $A \ncong X$, (since (X, – A) u A = X,). Let T be the composition of the functions H, D, $\check{G}$, i.e., let T 'u = $(\check{G})$ '(D '(H 'u)). Then $X \ncong Y$, since $X \underset{H}{\cong} A$ and $A \underset{D}{\cong} X_1$ and $X_1 \underset{\check{G}}{\cong}$ Y.

EXERCISES

4.52. Carry out the details of the following proof (due to J. Whitaker) of the Schroder-Bemstein Theorem in the case where X **and** Y **are sets. Let** $X \ncong Y_1 \wedge Y_1 \subseteq Y \wedge Y \ncong X_1 \wedge X_1 \subseteq X$. **We wish to find a set Z $\subseteq$ X such that** G**, restricted to** $Y - F$ "Z**, is a one-one function of** $Y - F$ "Z **onto** $X - Z$. **(If we have such a set** Z**, let** $H = (Z \upharpoonright F) \cup ((X - Z) \upharpoonright G)$**, i.e.** H 'x = F 'x **for** $x \in z$ **and H** 'x = $\check{G}$ 'x **for** $x \in X - Z$. **Then** $X \ncong$ **Y.) Let** $Z = \{x|(Eu)(u \subseteq X \wedge x \in u \wedge G''(Y - F''u) \subseteq X - u\}$. **Notice that this proof does not presuppose the definition of** ω **nor any other part of the theory of ordinals. For still another proof, cf. Kleene [1952, § 4].**

PROPOSITION 4.22. Assume $X \preccurlyeq Y$ and $A \preccurlyeq B$. Then,

(1) $Y \cap B = 0 \supset X \cup A \preccurlyeq Y \cup B$

(2) $X \times A \preccurlyeq Y \times B$

(3) $X^A \preccurlyeq Y^B$ *if* B *is* a set and *it* is not *the* case *that* $X = A = Y = 0 \wedge B \neq 0$.

PROOF. (1) Assume $X \ncong Y_1 \subseteq$ Y and $A \ncong B_1 \subseteq$ B. Let H be a function with domain X u A such that H 'x = F'x if x $\in$ X and H'x = G'x if x $\in$ A – X. Then $X \cup A \underset{H}{\cong} H$" $(X \cup A) \subseteq Y \cup B$. (2) and (3) are left as exercises.

EXERCISES

Prove:
4.53. $\vdash X \preccurlyeq X$ **u** $Y.$
4.54. $\vdash X \prec Y \supset \sim (Y \prec X).$
4.55. $\vdash X \prec Y \wedge Y \preccurlyeq Z \supset X \prec Z.$

PROPOSITION 4.23 (Cantor's Theorem).

(a) $\vdash \sim (Ef)(Fnc(f) \wedge \mathfrak{D}(f) = x \wedge \mathfrak{R}(f) = \mathfrak{P}(x))$. (There *is* no *function from* x onto $\mathfrak{P}(x)$.)

(b) $\vdash x \prec \mathfrak{P}(x)$.

PROOF. (a) Assume $Fnc(f) \wedge \mathcal{D}(f) = x \wedge \mathcal{R}(f) = \mathcal{P}(x)$. *Let* $y = \{u|u \in$ $\wedge\ u \notin f$ 'u). Then $y \in \mathcal{P}(x)$. Hence, there is some z in x such that f 'z $= \overset{x}{y}$. But, $(u)(u \in$ y $\equiv u \in x \wedge u \notin f$ 'u$)$. Hence, $(u)(u \in f$ 'z $\equiv u \in x \wedge u \notin f$ ‘$u)$. By Rule A4, z E f ‘$z \equiv z \in x \wedge z \notin$ f 'z. Since z $\in x$, we obtain $z \in f$ ‘$z \equiv z \notin f$ 'z, which yields a contradiction.

(b) Let f be the function with domain x such that f '$u = \{u)$ for each u in x. Then f '' $x \subseteq \mathcal{P}(x)$and f is one-one. Hence, $x \preccurlyeq \mathcal{P}(x)$. By Part (a), $x \cong \mathcal{P}(x)$is impossible. Hence, $x \prec 9(x)$.

Observe that we have not proved $\vdash (x)(y)(x \preccurlyeq y \vee y \preccurlyeq x)$. This proposition is, in fact, not yet provable, since it turns out to be equivalent to the Axiom of Choice.

EXERCISE 4.56. *Notice that, if NBG is consistent, then it has a denumerable model (Proposition* 2.12). *Explain why this does not contradict Cantor's Theorem, which implies that there exist non-denumerable* **infinite** *sets* (*e.g.*, 2^{ω}). *(This apparent, but not real, contradiction is sometimes called* ***Skolem's*** *Paradox.)*

The equinumerosity relation $\cong$ has all the properties of an equivalence relation. We are inclined, therefore, to partition the class of all sets into equivalence classes under this relation. The equivalence class of a set x would be the class of all sets equinumerous with x. The equivalence classes are called *cardinal numbers*. For example, if u is a set, and $x = \{$u$)$, then the equivalence class of x is the class of all unit sets $\{v\}$ and is called the cardinal number 1_c. Likewise, if $u \neq v$, and $y = \{$u, u$)$, then the equivalence class of y is the class of all sets containing exactly two elements, and is called the cardinal number 2,. i.e., $2_c = \{z|(Ex_1)(Ey_1)(x_1 \neq y_1\ A\ z = \{x_1, y,)))$. Now, notice that all the cardinal numbers, except the cardinal number of 0 (which is $\{0\}$), are proper classes. For example, V $\cong 1_c$, where V is the universal class. (Let F'$x = \{x)$ for each x in V. Then V $\underset{F}{\cong} 1_c$.) But $\sim M(V)$; hence, by the Replacement Axiom, $\sim M(1_c)$.

EXERCISE 4.57. *Prove*: $\vdash\sim M(2_c)$.

Because the cardinal numbers are proper classes, we cannot talk about classes of cardinal numbers, and it is difficult or impossible to say and prove many interesting things about them. Most assertions one should like to make about cardinal numbers can be paraphrased by suitable use of $\cong$ and $\preccurlyeq$. In addition, we shall see later that, given certain additional plausible axioms, there are other ways of defining a notion which does the same job as that of cardinal number.

To see how everything we want to say about cardinal numbers can be said without explicit mention of cardinal numbers, consider the following treatment of the "sum" of cardinal numbers.

DEFINITION. $X +, Y = (X \times \{0\})\ U\ (Y \times \{1\})$. Since $X \times \{0\}$ and $Y \times \{1\}$ are disjoint, their union is a class whose "size" is the "sum" of the "sizes" of X and Y.

EXERCISE 4.58. *Prove*:

(a) $\vdash X \preccurlyeq X +_c Y \wedge Y \preccurlyeq X +_c Y$.

(b) $\vdash X \cong A \wedge Y \cong B \supset X +_c Y \cong A +_c B$.

(c) $\vdash X +_c Y \cong Y +_c X$.

(d) $\vdash M(X +_c Y) \equiv M(X) \wedge M(Y)$.

(e) $\vdash X +_c (Y +_c Z) \cong (X +_c Y) +_c Z$.

(f) $\vdash X \preccurlyeq Y \supset X +_c Z \preccurlyeq Y +_c Z$.

(g) $\vdash X +_c X = X \times 2$.

(h) $\vdash X^{Y +_c Z} \cong X^Y \times X^Z$

(i) $\vdash x \cong x +_c 1 \supset 2^x +_c x \cong 2^x$.

Finite Sets. Remember that w is the set of all ordinals a such that α and all smaller ordinals are successor ordinals or 0. The elements of ω will be called *finite ordinals*. A set will be called *finite* if and only if it is equinumerous with a finite ordinal.

DEFINITION. $Fin(X) \equiv (E\alpha)(\alpha \in$ w $\wedge\ X \cong a)$.

Clearly, by the Replacement Axiom, $\vdash Fin(X)\ \Xi\ M(X)$. Trivially, all finite ordinals are finite sets, and $\vdash Fin(X) \wedge X \cong Y \supset Fin(Y)$.

PROPOSITION 4.24. (1) $\vdash (\alpha)(\alpha \in On -$ w $\supset a \cong a')$.

(2) $\vdash (\alpha)(\beta)(\alpha \in \omega \wedge a \neq \beta \supset\sim a \cong \beta)$. *(No finite ordinal is equinumerous with any other ordinal. Hence, a finite set is equinumerous with exactly one finite ordinal, and a non-finite ordinal, that is, a member of On –* w, *is not finite.)*

(3) $\vdash (\alpha)(x)(\alpha \in \omega \wedge x \subset \alpha \supset\sim a \cong x)$. *(No finite ordinal is equinumerous with a proper subset of itself.)*

PROOF. (1) Assume $a \in On - \omega$. Define a function f with domain a' as follows: f ‘$\delta = \delta'$ if $\delta \in$ w; f ‘$\delta = \delta$ if $\delta \in a' \wedge \delta \notin \omega\ U\ \{a)$; f '$a = 0$. Then α ‘ $\underset{f}{\cong} \alpha$.

(2) Assume false, and let a be the least ordinal such that $a \in$ w, and there is a $\beta \neq \alpha$ such that $a \cong \beta$. Hence, $a <_0 \beta$. (Otherwise, β would be a smaller ordinal than a, and β would be equinumerous with some ordinal $\neq \beta$.) Let $a \underset{f}{\cong} \beta$. If $\alpha = 0$, then $f = 0$ and $\beta = 0$, contradicting $a \neq \beta$. So, $a \neq 0$. Since $\alpha \in$ w, $\alpha = \delta'$ for some $\delta \in$ w. We may assume that $\beta = y'$ for some y. (For, if $\beta \in \omega$, then $\beta \neq 0$; and if $\beta \notin$ o, then, by Part (1), $\beta \cong \beta'$, and we can take β' instead of β.) Thus, $\delta' = a \underset{f}{\cong} y'$. Also, $\delta \neq y$, since $a \neq \beta$. Case I: f '$S = y$. Then $\delta \cong \gamma$. Case 2: f ‘$\delta \neq y$. Then there is some $\mu \in \delta$ such that f ‘$\mu = y$. Let $\overset{\delta 1 f}{h} = ((\delta 1 f) - \{(p, y)))U\{\langle\mu, f‘\delta\rangle\}$, i.e., let h 'r $= f$ ‘τ if $\tau \notin \{\delta, \mu\}$; h‘$\mu = f$‘δ. Then $\delta \underset{h}{\cong} \gamma$. In both cases, δ is a finite ordinal smaller than α which is equinumerous with a different ordinal γ, contradicting the minimality of a.

(3) Assume $\beta\ 6\ \omega \wedge x \subset \beta \wedge \beta \cong x$ holds for some β, and let a be the least such β. Clearly, $a \neq 0$; hence, $a = y'$ for some y; but, as in the proof of Part (2),

one can then show that y is also equinumerous with a proper subset of itself, contradicting the minimality of a.

EXERCISE 4.59. Prove that the Axiom of Infinity (I) is equivalent to *the* following sentence:

$$(*)\ (Ex)((Eu)(u \in x) \wedge (y)(y \in x \supset (Ez)(z \in x \wedge y \subset z))).$$

PROPOSITION 4.25.

(1) $\vdash Fin(X) \wedge$ Y ⊆ X ⊃ $Fin(Y)$.

(2) t $Fin(X) \supset Fin(X \cup$ {y)).

(3) t $Fin(X) \wedge$ Fin(Y) ⊃ $Fin(X$ u Y).

(4) A set is said to be Dedekind-finite *if* and only *if* it is equinumerous with a proper subset of itself. Then every finite set is Dedekind-finite. (The *converse* is not provable without use *of* an additional axiom, the Axiom of Choice.)

PROOF.

(1) Assume $Fin(X) \wedge$ Y ⊆ X. Then X $\underset{f}{\cong}$ a, where a ∈ w. Let $g = Y$ 1f and $W = g$ "Y ⊆ a. W is a set of ordinals, and so, E_W is a well-ordering of W. By Proposition 4.17, $\langle E_W$, W) is similar to $\langle E_\beta, \beta\rangle$ for some ordinal β. Hence, W ≅ β. In addition, $\beta \leqslant_0$ **a.** (For, if $\beta >_0 0$, then $\langle E_\beta, \beta\rangle$ is similar to $\langle E_W$, W), contradicting Corollary 4.15.) Since a ∈ w, β ∈ w. From Y $\underset{g}{\cong}$ W ∧ W ≅ β it follows that Fin (Y).

(2) If y ∈ X, then X u {y} = X and the result is trivial. So, assume y 4 X. From $Fin(X)$ it follows that there is a finite ordinal a and a function f such that a $\underset{f}{\cong}$ X. Let g = f u {(a, y)}. Then ***a'*** $\underset{g}{\cong}$ X u {y). Hence, $Fin(X \cup \{y\})$.

(3) Let $Z = \{u | u \in \omega \wedge (x)(y)(f)(x \overset{g}{\cong}$ u $\wedge\ Fin(y) \supset Fin(x$ u y))}. We must show that Z = w. Clearly, 0 ∈ Z, for, if $x \underset{f}{\cong} 0$, then $x = 0$ and x u y = y. Assume that a ∈ Z. Let $x \underset{f}{\cong}$ a' and $Fin(y)$. Let f 'w = a and $x_1 = x - \{w\}$. Then $x_1 \cong \alpha$. Since a ∈ Z, $Fin(x_1$ u y). But x u y = (x, u y) u {w). Hence, by Part (2), $Fin(x$ u y). Thus, a' ∈ Z. Hence, by Proposition 4.10(3), Z = w.

(4) This follows from Proposition 4.24(3).

DEFINITIONS. $Inf(X)$ for $\sim Fin(X)$. (X is infinite.)
$Den(X)$for X ≅ w. (X is denumerable.)

Clearly, t $Inf(X) \wedge$ X ≅ Y 3 $Inf(Y)$ and $\vdash Den(X) \wedge$ X ≅ Y ⊃ $Den(Y)$. By the Replacement Axiom and the fact that $M(\omega)$, it follows that $\vdash Den(X)$ 3 $M(X)$.

PROPOSITION 4.26

(1) $\vdash Inf(X) \wedge X \subseteq Y \supset Inf(Y)$

(2) $\vdash Inf(X) \equiv Inf(X \cup \{y\})$

(3) A class is called Dedekind-infinite if and only if it is equinumerous with *a proper* subset of *itself*. Then *every Dedekind-infinite* class is infinite.

(4) $\vdash Inf(\omega)$

PROOF.

(I) From Proposition 4.25(1).

(2) t $Inf(X) \supset Inf(X$ u {y}) by Part (1). By Proposition 4.25(3), $\vdash Inf(X \cup \{y\}) \supset Inf(X)$.

(3) Use Proposition 4.25(4).

(4) t ω 4 ω and Proposition 4.24(2).

PROPOSITION 4.27. $\vdash Den(v) \wedge z \subseteq v \supset (Den(z) \vee Fin(z))$

PROOF. It suffices to prove: $z \subseteq \omega \supset (Den(z) \vee Fin(z))$. Assume z ⊆ ω ∧ ‾ $Fin(z)$. Since $\sim Fin(z)$, for any a ∈ z, there is some β ∈ z with a $<_0 \beta$. (Otherwise, z ⊆ a' and, since $Fin(\alpha')$, $Fin(z)$.) Let X be a function such that, for any a ∈ ω, X 'a is the least ordinal β in z with a $<_0 \beta$. Then, by Proposition 4.13(3) (with $\delta = \omega$), there is a function Y with domain ω such that Y '0 is the least ordinal in z, and for any y in ω, Y '(y') is the least ordinal β in z with $\beta >_0 (Y$ 'y). Clearly, Y is one-one, $\mathfrak{D}(Y) = \omega$, and Y "ω ⊆ z. Also, Y "ω = z; for, if z – Y "$\omega \neq 0$, δ is the least ordinal in z – Y "w, and τ is the least ordinal in Y "w with 7 $>_0 \delta$, then 7 = Y 'o for some o in w. Since 6 $<_0$ 7, $\sigma \neq 0$. So, $\sigma = \mu'$ for some p in w. Then τ = Y 'σ = the least ordinal in z which is greater than Y '*p*. But $\delta >_0 Y$ 'μ, since τ is the least ordinal in Y"ω which is greater than 6. Hence $\tau \leqslant_0$ 6, which contradicts 6 $<_0$ 7.

EXERCISES

Prove:

4.60. $\vdash Fin(x) \supset Fin(\mathcal{P}$(x)).

4.61. t $(Fin(x) \wedge (y)(y \in$ x 3 $Fin(y)) \supset Fin(\bigcup(x))$.

4.62. $\vdash$ x $\preccurlyeq$ y $\wedge\ Fin(y) \supset Fin(x)$

4.63. $\vdash Fin(\mathcal{P}$**(x))** $\supset Fin(x)$

4.64. $\vdash Fin(\bigcup(x)) \supset (Fin(x) \wedge (y)(y \in x$ 3 $Fin(y)))$

4.65. $\vdash Fin(x) \supset$ (x $\preccurlyeq y \vee y \preccurlyeq x)$

4.66. t $Fin(x) \wedge Inf($ Y) ⊃ $x \prec Y$

4.67. $\vdash Fin(x) \wedge$ y ⊂ x ⊃ $y \prec x$

4.68. $\vdash Fin(x) \wedge Fin(y) \supset Fin(x \times y)$

4.69. t $Fin(x) \wedge Fin(y) \supset Fin(x^y)$

4.70. $\vdash Fin(x) \wedge$ y 4 x ⊃ x ≺ (x ∪ (y))

4.71. Define x to be a minimal (respectively, maximal) element of Y if and only if x ∈ Y and $(y)(y \in$ Y ⊃ ∼ y ⊂ x) (respectively, $(y)(y \in$ Y ⊃ ∼ x ⊂ y)). Prove that a set Z is finite if and only if every non-empty set of subsets of Z has a minimal (respectively, maximal) element (Tarski [1925]).

4.72. (a) $\vdash Fin(x) \wedge Den(y) \supset Den(x \cup$ y).
(b) $\vdash Fin(x) \wedge Den(y) \wedge$ x ≠ 0 ⊃ $Den(x \times y)$.

(c) A set x contains a denumerable subset if and only if x is Dedekind-infinite.

(d) If $y \notin x$, then x is Dedekind-infinite if and only if $x \cong x \cup \{y\}$.

(e) $\vdash \omega \preccurlyeq x \supset x +_c 1 \cong x$.

4. Hartogs' Theorem. Initial Ordinals. Ordinal Arithmetic.

An unjustly neglected proposition with manifold uses in set theory is Hartogs' Theorem.

PROPOSITION 4.28 (Hartogs [1915]). For any set x, there is an ordinal *which is* not equinumerous with any subset of x (and hence there is a least such *ordinal*).

PROOF. Assume that every ordinal a is equinumerous with some subset y of x. Hence, y $\underset{f}{\cong}$ a for some f. Define a relation R on y by stipulating that $\langle u$, U) ∈ R if and only if (f 'u) ∈ (f 'u). Then R is a well-ordering of y such that (R, $y\rangle$ is similar to $\langle E_\alpha$, a). Now, define a function F with domain On such that, for any a, F 'a is the set w of all pairs (z, y) such that y ⊆ x, is a well-ordering of y, and $\langle E_\alpha$, a) is similar to (z, y). (w is a set, since w $\mathcal{P}(x \times x) \times \mathcal{P}(x)$.) Hence, F ''On ⊆ $\mathcal{P}$($\mathcal{P}$(x × x) × $\mathcal{P}$(x)), and therefore F ''(On) is a set. F is one-one; hence, On = $\breve{F}$ ''(F ''(On)) is a set, by the Replacement Axiom, contradicting Proposition 4.7(8).

Let $\mathcal{H}$ be the function which assigns to each set x the least ordinal α which is not equinumerous with any subset of x. Notice that, to each $\beta <_0 \mathcal{H}$ 'x, we can associate the set of relations r such that r ⊆ x × x, r is a well-ordering of its field y, and $\langle r, y\rangle$ is similar to $\langle E_\beta, \beta\rangle$. This defines a one-one function from $\mathcal{H}$ 'x into $\mathcal{P}\mathcal{P}(x \times x)$. Hence $\mathcal{H}$ 'x $\preccurlyeq \mathcal{P}\mathcal{P}(x \times x)$, and, since $x \times x \subseteq$ $\mathcal{P}\mathcal{P}(x)$ by Exercise 4.17(a), p. 182, we obtain $\mathcal{H}$ '$x \preccurlyeq \mathcal{P}\mathcal{P}\mathcal{P}\mathcal{P}(x)$.

By an *initial* ordinal we mean an ordinal which is not equinumerous with any smaller ordinal. By Proposition 4.24(2), every finite ordinal is an initial ordinal, and ω is the smallest infinite initial ordinal. It is obvious that, for any x, $\mathcal{H}$ 'x is an initial ordinal. Moreover, for any ordinal a, $\mathcal{H}$ 'a is the least initial ordinal greater than a.

By transfinite induction (Proposition 4.13(2)), there is a function G with domain On such that

$$G\text{`}0 = \omega$$

$$G\text{`}(a') = \mathcal{H}\text{`}(G\text{'}a)$$

$$G\text{'}A = \bigcup(G\text{''}A) \text{ if } A \text{ is a limit ordinal.}$$

G is an increasing function, i.e., a ∈ $\beta \supset G$ 'a ∈ G 'β; therefore, if λ is a limit ordinal, and each G 'a, for a $<_0$ A, is an initial ordinal, then $\bigcup$(G ''A) is also an initial ordinal. (For, $\delta = \bigcup(G$ ''A) is the least upper bound of G ''A. Assume $\delta \cong \gamma$ with y $<_0 \delta$. Hence, there is some a $<_0$ A such that y $<_0$ G 'α. But G '(a') $<_0 \delta$. So, by the Schroder-Bernstein Theorem (Proposition 4.21(4)), using G '$\alpha \preccurlyeq G$ '(a') and G '$(\alpha') \preccurlyeq \delta \cong$ y $\preccurlyeq$ G 'a, we have G '$\alpha \cong G$ '$(\alpha') = \mathcal{H}$ '(G 'α), contradicting the definition of $\mathcal{H}$.) Hence G 'a is an initial ordinal, for all α.

In addition, every infinite initial ordinal is equal to G 'α for some α. (Assume not. Let σ be the least infinite initial ordinal not in G "On. By the Replacement Axiom R, G "On is not a set; hence there is some ordinal greater than σ in G "On. Let μ be the least such ordinal, and let $\mu = G$ 'β. Clearly, $\beta \neq 0$; if $\beta = \gamma'$ for some γ, then G '$\gamma <_0$ $\sigma <_0 G$ '$(\gamma') = \mathcal{H}$ '(G 'γ), contradicting the definition of $\mathcal{H}$. If β is a limit ordinal, then there is some $\alpha <_0 \beta$ such that $\sigma <_0 G$ '$\alpha <_0 G$ 'β, contradicting the definition of μ.) Thus, G is an $\in$-preserving "isomorphism" of On with the class of infinite initial ordinals.

We denote G 'α by ω_α. Thus, $\omega_0 = \omega$; $\omega_{\alpha'}$ is the least initial ordinal greater than ω_α; and, for limit ordinals λ, ω_λ is the initial ordinal which is the least upper bound of the set of all $\omega_\sim$ with $\alpha <_0 \lambda$. It follows from Proposition 4.14 that $\omega_\alpha \geqslant_0 \alpha$ for all α. Also, any infinite ordinal a is equinumerous with a unique initial ordinal $\omega_\beta \leqslant_0 \alpha$, namely, with the least ordinal equinumerous with α.

Let us turn now to ordinal arithmetic. We have already defined (see pp. 190–191) addition, multiplication, and exponentiation:

(I)
$$\beta +_0 0 = \beta$$
$$\beta +_0 \gamma' = (\beta +_0 \gamma)'$$
$$Lim(\alpha) \supset \beta +_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta +_0 \tau)$$

(II)
$$\beta \times_0 0 = 0$$
$$\beta \times_0 (\gamma') = (\beta \times_0 \gamma) +_0 \beta$$
$$Lim(\alpha) \supset \beta \times_0 \alpha = \bigcup_{\tau <_0 \alpha} (\beta \times_0 \tau)$$

(III)
$$exp(\beta, 0) = 1$$
$$exp(\beta, \gamma') = exp(\beta, \gamma) \times_0 \beta$$
$$Lim(\alpha) \supset exp(\beta, \alpha) = \bigcup_{0 <_0 \tau <_0 \alpha} exp(\beta, \tau).$$

PROPOSITION 4.29. The *following* wfs *are theorems.*

(1) $\beta +_0 1 = \beta'$

(2) $0 +_0 \beta = \beta$

(3) $\beta >_0 0 \supset \alpha +_0 \beta >_0 \alpha \wedge \alpha +_0 \beta \geqslant_0 \beta$

(4) $\beta <_0 \gamma \supset \alpha +_0 \beta <_0 \alpha +_0 \gamma$

(5) a $+_0 \beta =$ a $+_0 \delta \supset \beta = \delta$

(6) a $<_0 \beta \supset (E_1\delta)(\alpha +_0 \delta = \beta)$

(7) $0 \neq x \subseteq On \supset \alpha +_0 \bigcup_{\beta \in x} \beta = \bigcup_{\beta \in x} (\alpha +_0 \beta)$

(8) $0 <_0 \alpha \wedge 1 <_0 \beta$ 3 $\alpha \times_0 \beta$

(9) $0 <_0$ a $\wedge\, 0 <_0 \beta \supset \alpha \times_0 \beta \geqslant_0 \beta$

(10) y $<_0 \beta \wedge 0 <_0 \alpha$ 3 $\alpha \times_0 \gamma <_0 \alpha \times_0 \beta$

(11) $x \subseteq$ On $\supset$ a $\times_0 \bigcup_{\beta \in x} \beta = \bigcup_{\beta \in x} (\alpha \times_0 \beta)$

PROOF.

(1) $\beta +_0 1 = \beta +_0(0') = (\beta +_0 0)' = (\beta)'$.

(2) Prove $0 +_0 \beta = \beta$ by transfinite induction (Proposition *4.12)*. Let $X = \{\beta | 0 +_0 \beta = \beta\}$. First, $0 \in X$, since $0 +_0 0 = 0$. If $0 +_0 \gamma = \gamma$, then $0 +_0(\gamma') = (0 +_0 \gamma)' = y'$. If $Lim(\alpha)$ and $0 +_0 \tau = \tau$ for all $\tau <_0 a$, then $0 +_0 \alpha = \bigcup_{\tau <_0 \alpha} (0 +_0 \tau) = \bigcup_{\tau <_0 a} \tau = \alpha$, since $\bigcup_{\tau <_0 \alpha} \tau$ is the least upper bound of the set of all $\tau <_0 a$.

(3) Let $X = \{\beta | \beta >_0 0 \supset a +_0 \beta >_0 a)$. Prove $X =$ On by transfinite indue-tion. Clearly, $0 \in X$. If $\gamma \in X$, then $a +_0 \gamma \geqslant_0 a$; hence, $a +_0(\gamma') = (\alpha +, ?)$. $>_0 a +_0 \gamma \geqslant_0 a$. If $Lim(\lambda)$ and $\tau \in X$ for all $r <_0 \lambda$, then $a +_0 \lambda = \bigcup_{\tau <_0 \lambda} (\alpha +_0 \tau) \geqslant_0 a +_0 1 = a' >_0 a$. The second part is left as an exercise.

(4) Use transfinite induction. Let

$$X = \{\gamma | (\alpha)(\beta)(\beta <_0 \gamma \supset \alpha +_0 \beta <_0 \alpha +_0 \gamma)\}.$$

Clearly, $0 \in X$. Assume y $\in X$. Assume $\beta <_0 \gamma'$. Then $\beta <_0 \gamma$ or $\beta = \gamma$. If $\beta <_0 \gamma$, then, since $\gamma \in X$, $a +_0 \beta <_0 \alpha +_0 \gamma <_0 (a +_0 \gamma)' = a +_0 \gamma'$. If $\beta = \gamma$, then $a +_0 \beta = a +_0 \gamma <_0 (\alpha +_0 \gamma)' = a +_0 \gamma'$. Hence, $\gamma' \in X$. Assume $Lim(\lambda)$ and $\tau \in X$ for all $\tau <_0 \lambda$. Assume $\beta <_0 \lambda$. Then $\beta <_0 \tau$ for some $\tau <_0 \lambda$, since $Lim(\lambda)$. Hence, since $\tau \in X$, $a +_0 \beta <_0 a +_0 \tau \leqslant_0 \bigcup_{\tau <_0 \lambda} (a +_0 \tau) = a +_0 \lambda$. Hence, $\lambda \in X$.

(5) Assume $a +_0 \beta = a +_0 \delta$. Now. either $\beta <_0 6$ or $S <_0 \beta$ or $6 = \beta$. If $\beta <_0 6$, then $a +_0 \beta <_0 \alpha +_0 \delta$, and if $\delta <_0 \beta$, then $a +_0 \delta <_0 a +_0 \beta$, by Part **(4)**, contradicting $a +_0 \beta = a +_0 6$. Hence, $6 = \beta$.

(6) The uniqueness follows from Part *(5)*. Prove the existence by induction on β. Let $X = \{\beta | \alpha <_0 \beta \supset (E_1 \delta)(\alpha +_0 6 = \beta)$. Clearly. $0 \in X$. Assume $\gamma \in X$ and $a <_0 \gamma'$. Hence, $a = \gamma$ or $a <_0 \gamma$. If $a = \gamma$, then $(E\delta)(\alpha +_0 \delta = \gamma')$, namely $\delta = 1$. If $a <_0 \gamma$, then $(E_1 \delta)(\alpha +_0 \delta = y)$. Take an ordinal σ such that $a +_0 \sigma = \gamma$. Then a $+_0 \sigma' = (a +_0 \sigma)' = y'$; thus, $(E\delta)(\alpha +_0 6 = y')$, i.e. $\gamma' \in X$. Assume now that $Lim(\lambda)$ and $\tau \in X$ for all $\tau <_0 \lambda$. Assume $a <_0 \lambda$. Now define a function f such that, for $a <_0 \mu <_0 \lambda$, f 'μ is the unique ordinal 6 such that $\alpha +_0 \delta = \mu$. But $\lambda = \bigcup_{\alpha <_0 \mu <_0 \lambda} \mu = \bigcup_{\alpha <_0 \mu <_0 \lambda} (\alpha +_0 f\text{`}\mu)$. Let $\rho = \bigcup_{a <_0 \mu <_0 A} (f\text{`}\mu)$. Notice that, if $a <_0 \mu <_0 \lambda$, then $f\text{`}\mu <_0 f\text{`}(\mu')$; hence, p is a limit ordinal. Then $\lambda = \bigcup_{\alpha <_0 \mu <_0 \lambda} (\alpha +_0 f\text{`}\mu) = \bigcup_{\sigma <_0 \rho} (a +_0 \sigma) = \alpha +_0 \rho$.

(7) Assume $0 \neq x \subseteq On$. By Part (6), there is some δ such that $a +_0 6 = \bigcup_{\beta \in x} (a +_0 \beta)$. We must show that $\delta = \bigcup_{\beta \in x} \beta$. If $\beta \in x$, $a +_0 \beta \leqslant_0 a +_0 \delta$. Hence, $\beta \leqslant_0 \delta$, by Part *(4)*. Therefore, 6 is an upper bound of the set of all $\beta \in x$. So, $\bigcup_{\beta \in x} \beta \leqslant_0 6$. On the other hand, if $\beta \in x$, then $a +_0 \beta \leqslant_0 \alpha +_0 \bigcup_{\beta \in x} \beta$. Hence, $a +_0 \delta = \bigcup_{\beta \in x} (a +_0 \beta) \leqslant_0 a +_0 \bigcup_{\beta \in x} \beta$, and so, by Part (4), $\delta \leqslant_0 \bigcup_{\beta \in x} \beta$. Therefore, $6 = \bigcup_{\beta \in x} \beta$.

(8)–(11) are left as exercises.

PROPOSITION *4.30*. *The following* wfs *are theorems.*

(1) $\beta \times_0 1 = \beta \; A \; 1 \times_0 \beta = \beta$
(2) $0 \times_0 \beta = 0$
(3) $(\alpha +_0 \beta) +_0 \gamma = \alpha +_0(\beta +_0 \gamma)$
(4) $(\alpha \times_0 \beta) \times_0 \gamma = \alpha \times_0(\beta \times_0 \gamma)$
(5) $\alpha \times_0(\beta +_0 \gamma) = (\alpha \times_0 \beta) +_0(\alpha \times_0 \gamma)$
(6) $exp(\beta, 1) = \beta \; A \; exp(1, \beta) = 1$
(7) $exp(exp(\beta, \gamma), \delta) = exp(\beta, \gamma \times_0 \delta)$
(8) $exp(\beta, \gamma +_0 \delta) = exp(\beta, \gamma) \times_0 exp(\beta, \delta)$
(9) $a >_0 1 \; A \; \beta <_0 \gamma \supset exp(\alpha, \beta) <_0 exp(\alpha, \gamma)$.

PROOF.

(1) $\beta \times_0 1 = \beta \times_0 0' = (\beta \times_0 0) +_0 D = 0 \; f_0 p = \beta$, by Proposition 4.29(2). Prove $1 \times_0 \beta = \beta$ by transfinite induction on β.

(2) Prove $0 \times_0 \beta = 0$ by transfinite induction on β.

(3) Let $X = \{\gamma | (\alpha)(\beta)((\alpha +_0 \beta) +_0 \gamma = \alpha +_0(\beta +_0 \gamma))\}$. $0 \in X$, since $(a +_0 \beta) +_0 0 = a +_0 \beta = a +_0(\beta +_0 0)$. Now, assume $\gamma \in X$. Then $(a +_0 \beta) +_0 \gamma' = ((\alpha +_0 \beta) +_0 \gamma)' = (\alpha +_0(\beta +_0 \gamma))' = \alpha +_0(\beta +_0 \gamma)' = a +_0(\beta +_0 \gamma')$. Hence, $\gamma' \in X$. Assume now that $Lim(\lambda)$ and $\tau \in X$ for all $r <_0 \lambda$. Then $(\alpha +_0 \beta) +_0 \lambda = \bigcup_{\tau <_0 \lambda} ((\alpha +_0 \beta) +_0 \tau) = \bigcup_{\tau <_0 \lambda} (\alpha +_0(\beta +_0 \tau)) = \alpha +_0 \bigcup_{\tau <_0 \lambda} (\beta +_0 \tau)$ (by Proposition 4.29(7)), and this is equal to $a +_0(\beta +_0 \lambda)$.

(4)–(9) are left as exercises.

We should like to consider for a moment the properties of ordinal addition and multiplication when restricted to *w*.

PROPOSITION *4.31*. *Assume a, β, γ are in* o. *Then*

(1) $\alpha +_0 \beta \in \omega$
(2) $\alpha \times_0 \beta \in \omega$
(3) $exp(\alpha, \beta) \in \omega$
(4) $\alpha +_0 \beta = \beta +_0 \alpha$
(5) $\alpha \times_0 \beta = \beta \times_0 \alpha$
(6) $(\alpha +_0 \beta) \times_0 \gamma = (\alpha \times_0 \gamma) +_0(\beta \times_0 \gamma)$
(7) $exp(\alpha \times_0 \beta, \gamma) = exp(\alpha, \gamma) \times_0 exp(\beta, \gamma)$.

PROOF.

(1) Induction on β. Let $X = \{\beta | (\alpha)(\alpha \in \omega \supset a +_0 \beta \in \omega)\}$. Clearly $0 \in X$. Assume $\beta \in X$ and $a \in \omega$. Then $a +_0 \beta \in w$. Hence, $\alpha +_0(\beta') = (a +_0 \beta)' \in \omega$ *by* Proposition 4.10(1). So, by Proposition 4.10(3), $\omega \subseteq X$.

(2) and *(3)* are left as exercises.

(4) Lemma: $\vdash a \in \omega \wedge \beta \in \omega \supset a' +_0 \beta = a +_0 \beta'$.

Let $Y = \{\beta | \beta \in \omega \wedge (\alpha)(\alpha \in \omega \supset a' +_0 \beta = a +_0 \beta')\}$. Observe that $0 \in Y$. Assume $\beta \in Y$ and let $a \in w$. So, $a' +_0 \beta = a +_0 \beta'$. Then $a' +_0 \beta' = (\alpha' +_0 \beta)' = (a +_0 \beta')' = a +_0(\beta')'$. Hence, $\beta' \in Y$.

Now, to prove Part (4), let

$$X = \{\beta | \beta \in \omega \wedge (\alpha)(\alpha \in \omega \supset \alpha +_0 \beta = \beta +_0 \alpha)\}.$$

Then $0 \in X$, and, it is easy to prove, using the Lemma, that $\beta \in X \supset \beta' \in X$. (5)–(7) are left as exercises.

The reader will have noticed that we have not stated for ordinals certain well-known laws which hold for other familiar number systems, e.g., the commutative laws for addition and multiplication. In fact, these laws fail for ordinals, as the following examples show.

Examples.

1. $(E\alpha)(E\beta)(\alpha +_0 \beta \neq \beta +_0 \alpha)$

$$1 +_0 \omega = \bigcup_{\alpha <_0 \omega} (1 +_0 \alpha) = \omega$$

$$\omega +_0 1 = \omega' >_0 \omega$$

2. $(E\alpha)(E\beta)(\alpha \times_0 \beta \neq \beta \times_0 \alpha)$

$$2 \times_0 \omega = \bigcup_{\alpha <_0 \omega} (2 \times_0 \alpha) = \omega$$

$$\omega \times_0 2 = \omega \times_0 (1 +_0 1) = (\omega \times_0 1) +_0 (\omega \times_0 1) = \omega +_0 \omega >_0 \omega$$

3. $(E\gamma)(E\alpha)(E\beta)((\alpha +_0 \beta) \times_0 \gamma \neq (\alpha \times_0 \gamma) +_0 (\beta \times_0 \gamma))$

$$(1 +_0 1) \times_0 \omega = 2 \times_0 \omega = \omega$$

$$(1 \times_0 \omega) +_0 (1 \times_0 \omega) = \omega +_0 \omega >_0 \omega$$

4. $(E\alpha)(E\beta)(E\gamma)(exp(\alpha \times_0 \beta, \gamma) \neq exp(\alpha, \gamma) \times_0 exp(\beta, \gamma))$

$$exp(2 \times_0 2, w) = exp(4, w) = \bigcup_{\alpha <_0 \omega} (exp(4, \alpha) = \omega$$

$$exp(2, w) = \bigcup_{\alpha <_0 \omega} exp(2, a) = w.$$

So, $exp(2, w) \times_0 exp(2, w) = \omega \times_0 \omega >_0 \omega$.

Given any wf $\mathcal{A}$ of formal number theory *S* (cf. Chapter 3), we can associate with $\mathcal{A}$ a wf $\mathcal{A}^\star$ of NBG as follows: first, replace every "+" by "$+_0$", and every "·" by "xi'; then, if $\mathcal{A}$ is $\mathcal{B} \supset \mathcal{C}$, or $\sim \mathcal{B}$, respectively, and we already have found $\mathcal{B}^\star$ and $\mathcal{C}^\star$, let $\mathcal{A}^\star$ be $\mathcal{B}^\star \supset C^*$, or $\sim(\mathcal{B}^\star)$, respectively; if $\mathcal{A}$ is $(x)\mathcal{B}(x)$, replace it by $(x)(x \in \omega \supset \mathcal{B}^\star(x))$. This completes the definition of $\mathcal{A}^\star$. Now, if x,, . . . , x,, are the free variables of $\mathcal{A}$, prefix (x, $\in$ w $\wedge$ $x_2 \in \omega$ A . . . Ax,, $\in \omega) \supset$ to $\mathcal{A}^\star$, obtaining a wf $\mathcal{A}\#$. This amounts to restricting all variables to ω and interpreting addition, multiplication, and the successor function on integers as the corresponding operations on ordinals. Then every axiom $\mathcal{A}$ of S is transformed into a theorem $\mathcal{A}\#$ of NBG. (Axioms (S1)–(S3) are obviously transformed into theorems. (S4)# is a theorem, by Proposition

4.9(3), and (S5)#–(S8)# are properties of ordinal addition and multiplication (cf. p. 201). Now, for any wf $\mathcal{A}$ of S, $\mathcal{A}\#$ is predicative. Hence, by Proposition 4.4, all instances of (S9)# are provable by transfinite induction (Proposition 4.12(2)). (In fact, assume $\&\#(0) \wedge (x)(x \in$ w $\supset (8\#(x) \supset \mathcal{A}\#(x')))$. Let $X = \{y | y \in \omega \wedge \mathcal{A}\#(y))\}$. Then, by Proposition 4.12(2), $(x)(x \in \omega \supset \mathcal{A}\#(x))$.) Applications of modus ponens are easily seen to be preserved under the transformation of $\mathcal{A}$ into $\mathcal{A}\#$. As for the Generalization Rule, consider a wf $\mathcal{A}(x)$, and assume that $\mathcal{A}\#(x)$ is provable ın NBG. But $\mathcal{A}\#(x)$ ıs of the form $x \in \omega \wedge y_1 \in \omega \wedge \ldots \wedge y_m \in \omega \supset \mathcal{A}^\star(x)$. Hence, $y_1 \in \omega \wedge \ldots \wedge y_m \in \omega \supset (x)(x \in$ w $\supset \mathcal{A}^\star(x))$ is provable in NBG. But this wf is just $((x)\mathcal{A}(x))\#$. Hence, application of Gen leads from theorems to theorems. Therefore, for every theorem $\mathcal{A}$ of S, $\mathcal{A}\#$ is a theorem of NBG, and we can translate into NBG all the theorems of S proved in Chapter 3.

One can check that the number-theoretic function h such that, if x is the Gödel number of a wf $\mathcal{A}$ of S, then h(x) is the Gödel number of $\mathcal{A}\#$ in NBG, and if x is not the Gödel number of a wf of S, then h(x) = 0, is recursive (in fact, primitive recursive). Let K be any consistent extension of NBG. As we saw above, if x is the Gödel number of a theorem of S, h(x) is the Gödel number of a theorem of NBG, and, hence, also a theorem of K. Let S' be the extension of S obtained by taking as axioms all wfs $\mathcal{A}$ of S such that $\mathcal{A}\#$ is a theorem of K. Since K is consistent, S' must be consistent. Therefore, sınce *S* is essentially recursively undecidable (by Corollary 3.37), *S'* is recursively undecidable, i.e., the set $T_{S'}$ of Gödel numbers of theorems of *S'* is not recursive. Now, assume K is recursively decidable, i.e., the set T_K of Gödel numbers of theorems of K is recursive. But, $C_{T_S}(x) = C_{T_K}(h(x))$ for any x, where C_{T_S} and C_{T_K} are the characteristic functions of $T_{S'}$ and T_K. Hence $T_{S'}$ would be recursive, contradicting the recursive undecidability of S. Therefore K is recursively undecidable, and, thus, if NBG is consistent, NBG is essentially recursively undecidable. Recursive undecidability of a recursively axiomatizable theory implies incompleteness (cf. Exercise 3.47 (b), p. 166). Hence NBG is also essentially incomplete. Thus, we have the following result: *If* NBG is consistent, then NBG is *essentially recursively* undecidable and essentially incomplete. (It is possible to pmve this result directly in the same way that the corresponding result was proved for S in Chapter 3. Also cf. Exercises on page 172.) Since NBG apparently can serve as a foundation for all of present-day mathematics (i.e., it is clear to every mathematician that every mathematical theorem can be translated and proved within NBG, or within extensions of NBG obtained by adding various extra axioms such as the Axiom of Choice), the essential incompleteness of NBG seems to indicate that the "axiomatic approach to mathematics" is inadequate. This conclusion does not depend upon the peculiarities of the theory NBG. Any other consistent theory (including "higher-order theories" as well as first-order theories) in which the theory of natural numbers can be developed far enough so as to include all the theorems of S (or even of RR) must also be essentially recursively undecidable and essentially incomplete, as the proof given above for NBG shows.

EXERCISES

4.73. Verify that the function h defined above is recursive. (Notice that, because $+_0$, $\times_0$, 0 are introduced into NBG as additional function letters and individual constant, one has to prove that the transformation given in Proposition **2.29** is recursive.)

4.74. Prove that a predicate calculus with a single binary predicate letter ■ recursively undecidable. (Hint: Use Proposition **3.42.)**

There are a few facts about the "cardinal arithmetic" of ordinals that we should like to deal with now. By "cardinal arithmetic", we mean properties connected with the operations of union (u) and Cartesian product (x) and X^Y, as opposed to the properties of $+_0$ and $\times_0$ and ordinal exponentiation. Observe that $\times$ is distinct from $\times_0$; also notice that ordinal exponentiation $exp(\alpha, \beta)$, in spite of the ambiguous notation, has nothing to do with the operation of forming X^Y, the class of all functions from Y into X. (From Example 4 on p. 204, we see that exp(2, o), in the sense of ordinal exponentiation, is ω; while, from Cantor's Theorem, $\omega \prec 2^\omega$, where, in the latter formula, we mean by 2^ω the set of functions from ω into 2.)

PROPOSITION 4.32

(a) $\vdash \omega \times \omega \cong \omega$

(b) *If each of X and Y* contains at least two elements, then $X \cup Y \preccurlyeq X \times Y$

(c) $Den(x) \wedge Den(y) \supset Den(x \cup y)$

PROOF.

(a) Let f be a function with domain ω such that, if a $\in \omega$, then f 'a $= (a, 0\rangle$. Then f is a one-one function from ω into a subset of $\omega \times$ o. Hence, $\omega \preccurlyeq \omega$ X ω. Conversely, let g be a function with domain $\omega \times \omega$ such that, for any (a, $\beta\rangle \in$ ω X ω, g '(a, $\beta\rangle$ = 2'' $\times_0 3^\beta$. We leave it as an exercise to show that g is one-one. Hence, ω X $\omega \preccurlyeq$ o. So, by the Schroder-Bernstein Theorem, ω X $\omega \cong$ ω.

(b) Assume a, $\in$ X, $a_2 \in X$, a, $\neq a_2$ and b, $\in Y$, $b_2 \in Y$, and b, $\neq b_2$. Define:

$$f\text{‘}x = \begin{cases} (x, b_1\rangle & \text{if x} \in \text{X} \\ \langle a_1, x\rangle & \text{if } x \in \text{Y} - \text{Xandxfb,} \\ \langle a_2, b_2\rangle & \text{ifx} = b_1 \text{ and } x \in \text{Y} - \text{X} \end{cases}$$

Then f is a one-one function with domain X u Y and range a subset of X x Y. Hence, X u $Y \preccurlyeq X$ X Y.

(c) Assume $Den(A)$ and $Den(B)$. Hence, each of A and B contains at least two elements. Then, by Part (b), A u B $\preccurlyeq$ A $\times$ B. But A $\cong \omega$ and B $\cong \omega$. Hence, $A \times$ B $\cong \omega \times \omega$. Therefore A u B $\preccurlyeq \omega \times \omega \cong \omega$. By Proposition 4.27, either $Den(A$ u B) or $Fin(A$ u B). But A $\subseteq$ A u B and $Den(A)$; hence, $\sim Fin(A$ u B).

For the further study of ordinal addition and multiplication, it is quite useful to obtain concrete interpretations of these operations.

PROPOSITION 4.33 (Addition). Assume thaf (R, A) is similar to $\langle E_\alpha$, a), that $\langle S$, B) is similar to $\langle E_\beta, \beta\rangle$, and that A $\cap$ B = 0. *Define* the relation T on $A \cup$ B as *follows*: $\langle x, y\rangle \in T \equiv (x \in A \wedge y \in B) \vee (x \in A \wedge y \in A \wedge$ $\langle x, y\rangle \in$ R) $\vee$ (x $\in$ B $\wedge$ y $\in$ B $\wedge$ (x, y) $\in$ S); (*i.e.*, T is the some as R in *the* set A, *the* same as S in the set B, and every element *of* A T-precedes *every element of* B). Then T is a well-ordering *of* A $\cup$ B, and (T, A $\cup$ B) *is* similar to $\langle E_{\alpha +_0 \beta}, \alpha +_0 \beta\rangle$.

PROOF. First, it is simple to verify that T is a well-ordering of A $\cup$ B, since R is a well-ordering of A and S is a well-ordering of B. To show that $\langle T, A \cup B\rangle$ is similar to $\langle E_{\alpha +_0 \beta}$, a $+_0 \beta\rangle$, perform transfinite induction on β. For β = 0, B = 0. Hence, T = R, A $\cup$ B = A, and a $+_0 \beta$ = a. So, (T, A u $B\rangle$ is similar to $\langle E_{\alpha +_0 \beta}$, a $+_0 \beta\rangle$. Assume the proposition for γ, and let β = y'. Since (S, B) is similar to $\langle E_\beta, \beta\rangle$, we have a function f with domain B and range β such that, for any x, y in B, $\langle x, y\rangle \in$ S if and only iff ‘$x \in$ f ‘y. Let $b = (\check{f})$ ‘γ, let $B_1 = B$ – {b), and let S, = S $\cap$ (B, $\times$ B_1). Since b is the S-maximum of B, it follows easily that S_1 well-orders B,. Also, $B_1$1f is a similarity mapping of B, onto y. Let T_1 = T $\cap$ ((A $\cup$ B_1) $\times$ (A $\cup$ B_1)). By inductive hypothesis, (T,, $A \cup B_1\rangle$ is similar to $\langle E_{\alpha +_0 \gamma}, \alpha +_0 \gamma\rangle$, by means of some similarity mapping g with domain A u B, and range $a +_0 \gamma$. Extend g to g_T = g $\cup$ {(b, a $+_0 \gamma\rangle$}, which is a similarity mapping of A $\cup$ B onto (a $+_0 \gamma)'$ – a $+_0 \gamma'$ = a $+_0 \beta$. Finally, if $Lim(\beta)$, and our proposition holds for all $\tau <_0 \beta$, assume that f is a similarity mapping of B onto β. Now, for each $\tau <_0 \beta$, let $B_\tau = (\check{f})$ “τ, $S_\tau = S \cap$ (B, x B,), and T_τ = T $\cap$ ((A u B,) $\times$ (A $\cup$ B_τ)). By inductive hypothesis, and Corollary 4.16(2), there is a unique similarity mapping g_τ of (T,, A $\cup$ B,) with $\langle E_{\alpha +_0 \tau}$, a $+_0 \tau\rangle$; also, if $\tau_1 <_0 \tau_2 <_0 \beta$, then, since $A \cup B_{\tau_1}$1g_{τ_2} is a similarity mapping of $\langle T_{\tau_1}$, A u $B_{\tau_1}\rangle$ with $\langle E_{\alpha +_0 \tau_1}, \alpha +_0 \tau_1\rangle$ and, by the uniqueness of g_{τ_1}, $A \cup B_{\tau_1}$1$g_{\tau_2} = g_{\tau_1}$, i.e., g_{τ_2} is an extension of g_{τ_1}. Hence, if $g = \bigcup_{\tau <_0 \rho} \text{a}(g_\tau)$, then g is a similarity mapping of (T, $\bigcup_{\tau <_0 \beta}(A \cup B_\tau)$ with $\langle E_{\bigcup_{\tau <_0 \beta} (\alpha +_0 \tau)}$, $\bigcup_{\tau <_0 \beta} (\alpha +_0 \tau)\rangle$. But, $\bigcup_{\tau <_0 \beta} (A \cup B_\tau) = A \cup B$, and $\bigcup_{\tau <_0 \beta}$ (a $+_0 \tau) = \alpha +_0 \beta$. This completes the transfinite induction.

PROPOSITION 4.34 (Multiplication). Assume that (R, A) is similar to $\langle E_\alpha, \alpha\rangle$ and that (S, B) *is* similar to $\langle E_\beta, \beta\rangle$. *Define the* relation W on A $\times$ B *as* follows: $\langle\langle x, y\rangle, \langle u, v\rangle\rangle \in$ W $\equiv (x \in$ A $\wedge$ $u \in A \wedge y \in B \wedge v \in B) \wedge$ (((y, $v\rangle \in S) \vee$ (y = v $\wedge$ (x, u) $\in$ R)). Then W is a well-ordering of A X B and (W, A X B) is similar to $\langle E_{\alpha \times_0 \beta}$, a $\times_0 \beta\rangle$.†

†The ordering W is called an *inverse lexicographical* ordering because it orders pairs as follows: first, according to the sue of their second components, and, then, if their second components are equal, according to the size of the first components.

PROOF. Exercise. (Proceed as in the proof of Proposition 4.33.)

Examples.

1. $2 \times_0 \omega = \omega$. Let (R, A) $= \langle E_2, 2)$, and (S, B) $= \langle E_\omega, \omega\rangle$. Then the pairs in $2 \times \omega$ can be well-ordered as follows: $(0, 0\rangle$, $(1, 0\rangle$, $(0, 1\rangle$, $(1, 1\rangle$, $(0, 2\rangle$, $\langle 1, 2\rangle, \ldots, \langle 0, n\rangle, \langle 1, n\rangle, \langle 0, n+1\rangle, \langle 1, n+1\rangle, \ldots$.

2. By Proposition 4.30(5), $\omega \times_0 2 = \omega +_0 \omega$. Let (R, A) $= \langle E_\omega, \omega\rangle$ and $(S, B\rangle = \langle E_2, 2)$. Then $\omega \times 2$ can be well-ordered (cf. Proposition 4.34) as follows: $\langle 0, 0\rangle, \langle 1, 0\rangle, \langle 2, 0\rangle, \ldots, \langle 0, 1\rangle, \langle 1, 1\rangle, \langle 2, 1\rangle, \ldots$.

PROPOSITION 4.35. ***For all a**, $\omega_\alpha \times \omega_\alpha \cong \omega_\alpha$.*

PROOF. (Sierpinski [1958]). Assume false, and let a be the least ordinal such that $-(\omega_\alpha \times \omega_\alpha \cong \omega_\alpha)$. Then $\omega_\beta \times \omega_\beta \cong \omega_\beta$ for all $\beta <_0$ ***a.*** By Proposition 4.32(1), a $>_0 0$. Now, let P $= \omega_\alpha \times \omega_\alpha$, and, for $\beta <_0 \omega_\alpha$, let $P_\beta = (($y, $\delta\rangle | \gamma +_0 \delta = \beta\}$. First, we wish to show that P $= \bigcup_{\beta <_0 \omega_\alpha} P_\beta$. Now, if $\gamma +_0 \delta = \beta <_0 \omega_\alpha$, then $\gamma \leqslant_0 \beta <_0 \omega_\alpha$ and 6 $\leqslant_0 \beta <_0 \omega_\alpha$; hence, (y, 6) $\in \omega_\alpha$ X ω_α = P. Thus, $\bigcup_{\beta <_0 \omega_\alpha} P_\beta \subseteq$ P. To show that P $\subsetneq \bigcup_{\beta <_0 \omega_\alpha} P_\beta$, it suffices to show that, if $\gamma <_0 \omega_\alpha$ and $\delta <_0 \omega_\alpha$, then $\gamma +_0 \delta <_0 \omega_\alpha$. Now, γ and δ are equinumerous with initial ordinals $\omega_\sigma \leqslant {}_0\gamma$ and $\omega_\rho \leqslant$ 08, respectively. Let ζ be the larger of a and p. Since $\gamma <_0 \omega_\alpha$ and $\delta <_0 \omega_\alpha$, then $\omega_\zeta <_0 \omega_\alpha$. Hence, by the minimality of ***a,*** $\omega_\zeta \times \omega_\zeta \cong \omega_\zeta$. Let A $= \gamma \times \{0)$, B $= \delta \times (1)$. Then, by Proposition 4.33, A u B $\cong \gamma +_0 \delta$. Since $\gamma \cong \omega_\sigma$ and 6 $\cong \omega_\rho$, A $\cong \omega_\sigma \times \{0\}$ and B $\cong \omega_\rho \times \{1\}$. Hence, since A $\cap B = 0$, A u B $\cong (\omega_\sigma \times \{0\})$ u $(\omega_\rho \times \{1\})$. But, by Proposition 4.32(b), $(\omega_\sigma \times \{0\}) \cup (\omega_\rho$ X $\{1\}) \preccurlyeq (\omega_\sigma$ X $(0))$ X $(\omega_\rho$ X $\{1\}) \cong \omega_\sigma \times \omega_\rho \preccurlyeq \omega_\zeta$ X $\omega_\zeta \cong$ **q**. Hence, $\gamma +_0 \delta \preccurlyeq \omega_\zeta <_0 \omega_\alpha$. Since ω_α is an initial ordinal, y $+_0 \delta <_0 \omega_\alpha$. (For, if $\omega_\alpha \leqslant_0 \gamma +_0 6$, then $\omega_\alpha \preccurlyeq \omega_\zeta$ and $\omega_\zeta \preccurlyeq \omega_\alpha$; so, by the Schroder-Bërnstein Theorem, $\omega_\alpha \approx \omega_\zeta$, contradicting $\omega_\zeta <_0$ **y.**)Thus, P $= \bigcup_{\beta <_0 \omega_\alpha} P_\beta$. Consider P_β for any $\beta <_0 \omega_\alpha$. By Proposition 4.29(6), for each $\gamma \leqslant_0 \beta$, thëre is exactly one ordinal δ such that $\gamma +_0 \delta = \beta$. Hence there is a similarity mapping from β' onto P_β, where P_β is ordered according to the size of the first component γ of the pairs (y, 6). Define the following relation R on P. For any $\gamma <_0 \omega_\alpha$, 6 $<_0 \omega_\alpha$, $\mu <_0 \omega_\alpha \nu <_0 \omega_\alpha$, $\langle\langle\gamma, \delta\rangle$, $(\mu$, Y)) E R if and only if either $\gamma +_0 \delta <_0 \mu +_0 \nu$ or $(\gamma +_0 \delta =$ p $+_0 \nu \wedge \gamma <_0 \mu)$. Thus, if $\beta_1 <_0 \beta_2 <_0 \omega_\alpha$, the pairs in P_{β_1} R-precede the pairs in P_{β_2}, and, within each P_β, the pairs are R-ordered according to the size of their first components. One easily verifies that *R* well-orders *P*. Since P $= \omega_\alpha$ X ω_α, it suffices now to show that (R, P) is similar to $\langle E_{\omega_\alpha}, \omega_\alpha\rangle$. By Proposition 4.17, (R, $P\rangle$ is similar to some $\langle E_\xi, \xi\rangle$, where ξ is an ordinal. Hence, P $\cong \xi$. Assume that $\xi >_0 \omega_\alpha$. There is a similarity mapping *f* between $\langle E_\xi, \xi\rangle$ and (R, P). Let b = f ‘ω_α; then b is an ordered pair $\langle\gamma, \delta\rangle$ with $\gamma <_0 \omega_\alpha$, $\delta <_0 \omega_\alpha$, and ω_α**1**f is a similarity mapping between $\langle E_{\omega_\alpha}, \omega_\alpha\rangle$ and the R-segment Y = $Seg_R(P$, (y, $\delta\rangle)$ of P determined by (y, $\delta\rangle$. Then Y $\cong \omega_\alpha$. Also, letting $\beta =$ y $+_0 \delta$, if (a, ***p)*** $\in$ Y, we have $\sigma +_0 \rho \leqslant_0 \gamma +_0 \delta = \beta$; hence, $\sigma \leqslant_0 \beta$ and p $\leqslant_0 \beta$. Therefore, Y $\subseteq \beta'$ X β'. But $\beta' <_0 \omega_\alpha$. Hence,

$\beta' \cong \omega_\mu$ with $\mu <_0$ ***a.*** By the minimality of ***a,*** $\omega_\mu \times \omega_\mu \cong \omega_\mu$. So, $\omega_\alpha \cong$ Y $\preccurlyeq \omega_\mu$, contradicting $\omega_\mu \prec \omega_\alpha$. Thus, $\xi \leqslant_0 \omega_\alpha$, and, therefore, P $\preccurlyeq \omega_\alpha$. Let *h* be the function with domain ω_α such that $h‘\beta = \langle \beta, 0\rangle$ for every $\beta <_0 \omega_\alpha$. Then *h* is a one-one correspondence between ω_α and the subset $\omega_\alpha \times \{0\}$, and, therefore, $\omega_\alpha \preccurlyeq$ P. By the Schroder-Bemstein Theorem, $\omega_\alpha \cong$ P, contradicting the definition of ***a.*** Hence. $\omega_\beta \times \omega_\beta \cong \omega_\beta$ for all β.

COROLLARY 4.36. If A $\cong \omega_\alpha$ ***and** $B \cong \omega_\beta$, **and if** γ **is the maximum** of **a and** β, **then** $A \times B \cong \omega_\gamma$ **and*** A $\cup$ ***B*** $\cong \omega_\gamma$. In ***particular,*** $\omega_\alpha \times \omega_\beta \cong \omega_\gamma$.

PROOF. By Proposition 4.35 and 4.32(2), $\omega_\gamma \preccurlyeq$ A u B $\preccurlyeq$ A $\times$ B $\cong \omega_\alpha \times \omega_\beta \preccurlyeq \omega_\gamma \times \omega_\gamma \cong \omega_\gamma$. Hence, by the Schröder-Bernstein Theorem, A $\times$ B $\cong \omega_\gamma$ and $A \cup B \cong \omega_\gamma$.

This is really only the beginning of ordinal arithmetic. For further study, cf. Sierpinski [1958] and Bachmann [1955].

EXERCISES

Prove that the following are theorems of NBG.

4.75. (a) x $\preccurlyeq \omega_\alpha \supset$ x u $\omega_\alpha \cong$ w,
(b) $\omega_\alpha +_c \omega_\alpha \cong \omega_\alpha$

4.76. $0 \neq$ x $\preccurlyeq \omega_\alpha \supset$ x X $\omega_\alpha \cong \omega_\alpha$

4.77. $0 \neq$ **x** $\prec \omega \supset \omega_\alpha^x \cong \omega_\alpha$

4.78. (a) $\mathcal{P}(\omega_\alpha) \times \mathcal{P}(\omega_\alpha) \cong \mathcal{P}(\omega_\alpha)$
(b) $x \preccurlyeq 9(\omega_\alpha) \supset x$ U $9(\omega_\alpha) \cong \mathcal{P}(\omega_\alpha)$
(c) 0 $\neq$ **x** $\preccurlyeq \mathcal{P}(\omega_\alpha) \supset x \times \mathcal{P}(\omega_\alpha) \cong \mathcal{P}(\omega_\alpha)$
(d) 0 $\neq$ x $\preccurlyeq \omega_\alpha \supset (\mathcal{P}(\omega_\alpha))^x \cong \mathcal{P}(\omega_\alpha)$
(e) 1 $\prec$ x $\preccurlyeq \omega_\alpha \supset x^{\omega_\alpha} \cong \omega_\alpha^{\omega_\alpha}$ -- $(\mathcal{P}(\omega_\alpha))^{\omega_\alpha} \cong \mathcal{P}(\omega_\alpha)$.

4.79. Assume $y \neq 0 \wedge y \cong y +_c y$. Remember that $y +_c y = (y \times \{0\}) \cup (y \times$ {I)). (This assumption holds for $y = \omega_\alpha$ by Corollary 4.36, and for $y = \mathcal{P}(\omega_\alpha)$ by Exercise 4.78(b). It will turn out to hold for all infinite sets y if the Axiom of Choice holds.)
(a) $Inf(y)$
(b) $y \cong 1 +_c y$
(c) $(Eu)(Ev)(y = u \cup v \wedge u \cap v = 0 \wedge u \cong y \wedge v \cong y)$
(d) $\{z | z \subseteq y \wedge z \cong y\} \cong \mathcal{P}(y)$
(e) $\{z | z \subseteq y \wedge Inf(z)\} \cong \mathcal{P}(y)$
(f) $(Ef)(y \underset{f}{\cong} y \wedge (u)(u \in y \supset f'u \neq u))$.

4.80. Assume $y \cong y$ X $y \wedge 1 \prec y$. (This holds when $y = \omega_\alpha$ by Proposition 4.35 and for $y = \mathcal{P}(\omega_\alpha)$ by Exercise 4.78(a). It is true for all infinite sets y if the Mom of Choice holds.)
(a) Y $\cong$ Y $+_c y$.
(b)^D Let $Perm(y) = \{f | y \not\cong$ y). Then $Perm(y) \cong \mathcal{P}(y)$.

5. The Axiom of Choice. The Axiom of Regularity.

The Axiom of Choice is one of the most celebrated and contested statements of the theory of sets. We shall state it in the next proposition and show its equivalence to several other important assertions.

PROPOSITION 4.37. The following wfs are equivalent.

(I) Axiom of Choice (AC): For any *set* x, there is a *function f* such that, *for* any *non-empty* subset y ofx, *f* ‘*y* ∈ y (f *is* called a choice functionfor x).

(2) Multiplicative Axiom (Mult): If x is a set of disjoint *non-empty* sets, *then* there is a set y (*called* a choice set for x) such *that* y contains *exactly one element of* each set in **x**. $(u)(u \in x \supset u \neq 0 \wedge (v)(v \in x \wedge v \neq u \supset o \cap = 0))$ ɜ $(Ey)(u)(u \in x$ ɜ $(E_1 w)(w \in u \cap y))$. *u*

(3) Well-ordering Principle (*W.O.*): Every *set* can be well-ordered $(x)(Ey)(y\ We\ x)$.

(4) Trichotomy (Trich): $(x)(y)(x \preccurlyeq y \vee y \preccurlyeq x)$.

(5) Zorn's Lemma (Zorn): Any *non-empty partially-ordered* set *x*, in which ***every*** chain (i.e., every totally-ordered *subset*) *has* an upper bound, has *a* maximal element. $(x)(y)((y\ \text{Part}\ x) \wedge ((u)(u \subseteq x \wedge y\ \text{Tot}\ u \supset (Ev)(v \in x \wedge (w)(w \in u \supset w = v \vee \langle w, v\rangle \in y))) $ ɜ $ (Ev)(v \in x$ A $(w)(w \in x \supset \langle v, w) \notin y)))$.

PROOF.

(I) ⊦ (W.O.) ɜ Trich. Given sets x, y, then, by (W.O.), x and y can be well-ordered; hence, by Proposition 4.17, x ≅ a and y ≅ β for some ordinals a, β. **But** a ≼ β or β ≼ a. Hence, x ≼ y or y ≼ **x.**

(2) ⊦ *Trich* ⊃ (W.O.). Given a set x, then, by **Hartogs’** Theorem, there is an ordinal a such that a is not equinumerous with any subset of x. By Trich, *x* is equinumerous with some subset y of a. Hence, by translating the well-ordering E_y of y to x, *x* can be well-ordered.

(3) ⊦ (*W.O.*) ⊃ *Mult*. Let **x** be a set of non-empty disjoint sets. By (W.O.), there is a well-ordering R of $\bigcup(x)$. Hence, there is a function **j** with domain x such that, for any *u* in x, f ‘*u* is the R-least element of u. (Notice that $u \subseteq \bigcup(x)$.)

(4) ⊦ *Mult* ɜ AC. For any set **x,** we may define a one-one function g such that, for each non-empty subset *u* of x, g ‘$u = u \times$ {u). Let x_1 be the range of g. Then ***x*,** is a set of non-empty disjoint sets. Hence, by *Mult*, there is a choice set *y* for x_1. Therefore, if $0 \neq u$ and $u \subseteq$ x, then $u \times \{u\}$ is in x,, and so, *y* contains exactly one element (v, u) in $u \times$ {u). Then the function *f* such that f ‘$u =$ v is a choice function for **x.**

(5) ⊦ AC ⊃ Zorn. Let y partial-order a non-empty set x such that every y-chain in x has an upper bound in x. By AC, there is a choice function *f* for x. Let *b* be any element of x. By transfinite induction (Proposition 4.13), we define a function F such that F'0 = b, and, for any a > 0, F'a is f ‘*u*, where *u* is the set of y-upper bounds *v* in x of F "a such that o ∉ F ***"a.*** Let β be the least ordinal such that the set of y-upper bounds in x of F“β which are not in F“β is empty. (There must be such an ordinal; otherwise, F is a one-one function with domain On and range a subset of x. which, by the Replacement Axiom R, implies that On is a set.) Let g = β ˥ ***F.*** Then it is an easy exercise to check that g is one-one, and, if a $<_0 \gamma <_0 \beta$, ***(g 'a, g*** 'y) ∈ y. Hence, g “β is ay-chain in x; by hypothesis, there is an upper bound w of g “β. Since the set of upper bounds

of F “β (= g “β) which are not in g “β is **empty,** *w* ∈ g “β and w is the only Upper bound of g “β (**because** a set can contain at most one upper bound). **Hence,** w is a y-maximal element. (For, if (w, z) ∈ y and z ∈ *x*, then *z* is a *y*-upper bound of g “β, which is impossible.)

(6) ⊦ Zorn ⊃ (W.O.). Given a set *z*, let X be the class of all one-one functions with domain an ordinal and range a subset of *z*. By **Hartogs’** Theorem, **X** is a set. Clearly, 0 ∈ ***X.*** X is partially-ordered by the proper **inclusion** relation **⊂ .** Given any chain of functions in *X*, of any two, one is an extension of the other. Hence, the union of all the functions in the chain is also a one-one function from an ordinal into z, which is an ⊂ -upper bound of the chain. Hence, by *Zorn*, ***X*** has a maximal element g, which is a one-one function from an ordinal a into *z*. Assume z – g “$\alpha \neq 0$, and let $b \in z - g$ “α. Let $f = g \cup \{\langle \alpha, b\rangle\}$. Then f ∈ ***X*** and g **⊂** *f*, contradicting the **maximality** of g. So, g "a = z. Thus, $\alpha \underset{g}{\cong}$ z. We can transfer by means of g the well-ordering E_α of a to a well-ordering of z.

EXERCISES

4.81. Show that the following are equivalent to the Axiom of Choice.

(a) Any set *x* is equinumerous with some ordinal.

(b) (Special case of **Zorn’s** Lemma) If *x* is a non-empty set, and if the union of each non-empty ⊂ -chain in *x* is also in *x*, then x has a ⊂ -maximal element.

(c) (Hausdorff Maximal **Principle)** If *x* is a set, then **every** ⊂ -chain in x is a subset of some maximal ⊂ -chain in **x.**

(d) (Teichmiiller-Tukey Lemma) Any set of **finite character has** an ⊂ -maximal element. (A non-empty set **x** is said to be of finite character if and only if (i) every finite subset of an element of *x* is also an element of r; (ii) if every finite subset of a set y is a member of x, then *y* ∈ *x*.)

(e) $(x)((Rel(x) \supset (Ey)(Fnc(y)$ A $\mathfrak{D}(x) = \mathfrak{D}(y) \wedge y \subseteq x)$.

(f) For any non-empty sets *x* andy, either there is a function with domain *x* and range y or there is a function with domain y and range **x.**

4.82. Show that the following Finite Axiom of Choice is provable in NBG: if *x* is a finite set of non-empty disjoint sets, then there is a choice set y for x. (Hint: assume ***x*** ≅ a where a ∈ ω. Use induction on ***a.)***

PROPOSITION 4.38. The following are consequences of the Axiom of Choice.

(I) Any infinite set has a denumerable subset.

(II) Any infinite set is Dedekind-infinite.

(III) If x is a *denumerable set* whose elements are denumerable *sets*, then $\bigcup(x)$ is denumerable.

PROOF.

(I) Assume AC. Let *x* be an **infinite set.** By Exercise 4.81(a), x is equinumerous with some ordinal a. Since *x* is infinite, so is a. **Hence,** ω ≼o a; therefore, ω is equinumerous with some subset of *x*.

(II) By (I) and Exercise 4.72(c), p. 200.

(III) Assume x is a denumerable set of denumerable sets. Let f be a function assigning to each $u \in x$ the set of all one-one correspondences between u and ω. Let z be the union of the range of f. Then, by AC applied to z, there is a function g such that g ‘$v \in u$ for each non-empty $u \subseteq$ z. In particular, if $u \in x$, then g ‘$(f'u)$ is a one-one correspondence between u and o. Let h be a one-one correspondence between ω and x. Define a function F on $\bigcup(x)$ as follows: Let $y \in \bigcup(x)$ and let n be the smallest element of ω such that $y \in h$ 'n. Now, h 'n $\in x$; so, g ‘$(f'(h'n))$ is a one-one correspondence between h ‘n and ω. Define F‘$y = (n, (g$‘$(f'(h'n)))$'y). Then F is a one-one function with domain $\bigcup(x)$ and range a subset of $\omega \times \omega$. Hence, $\bigcup(x) \preccurlyeq \omega \times o$. But o × o $\cong \omega$ and, therefore, $\bigcup(x) \preccurlyeq o$. If $u \in$ x, then $u \subseteq \bigcup(x)$ and $u \cong o$. Hence, $\omega \preccurlyeq \bigcup(x)$. By the Schroder-Bernstein Theorem, $\bigcup(x) \cong \omega$.

EXERCISES

4.83. If x is a set, the Cartesian product $\prod$ u is the set of functions f with domain x such that f ‘$u \in u$ for all $u \in x$.“Show that AC is equivalent to the proposition that the Cartesian product of any set x of non-empty sets is also non-empty.

4.84. Show that AC implies that any partial ordering of a set x is included in a total ordering of x.

4.85. Prove that the following assertion is a consequence of AC: for any ordinal a, if x is a set such that $x \preccurlyeq \omega_\alpha$ and such that $(u)(u \in$ X $\supset u \preccurlyeq \omega_\alpha)$, then $\bigcup(x) \preccurlyeq \omega_\alpha$. (Hint: proof is analogous to that of Proposition 4.38(III).)

4.86. (a) Prove: y $\preccurlyeq x \supset (Ef)(Fnc(f) \wedge \mathfrak{D}(f) = x \wedge \mathfrak{R}(f) = y)$.

(b) Prove that AC implies the converse of Part (a):

$$(Ef)(Fnc(f)\ A\ \mathfrak{D}(f) = x\ A\ \mathfrak{R}(f) = y) \supset Y \preccurlyeq x.$$

4.87.'' (a) Prove: $(u +_c v)^2 \cong u^2 +_c 2 \times (u \times$ U$) +_c v^2$.

(b) Assume y is a well-ordered set such that $x \times$ y $\cong x +$y and $\sim(y \preccurlyeq x)$. Prove that $x \preccurlyeq$ y.

(c) Assume y $\cong$ y $\times$ y for all infinite sets y. Prove that, if $Inf(x)$ and $z = \mathcal{H}$ ‘x, then x X z $\cong x +_c z$.

(d) Prove that AC is equivalent to $(y)(Inf(y) \supset$ y $\cong y \times$ y). (Tarski [1923])

A stronger form of the Axiom of Choice is the following sentence. (UCF): $(EX)(Fnc(X) \wedge (u)(u \neq 0 \supset$ X‘$u \in u))$. (There is a *universal choice function*, i.e. a function which assigns to every non-empty set u an element of u.) UCF obviously implies AC, but it was proved by W. B. Easton in 1964 that UCF is not provable from AC if NBG is consistent. However, Felgner [1971] proved that, for any sentence $\mathscr{C}$ in which all quantifiers are restricted to sets, if $\mathscr{C}$ is provable from NBG + (UCF), then $\mathscr{C}$ is also provable in $NBG + (AC)$. (See Felgner [1976] for a thorough treatment of the relations between UCF and AC.)

The theory of cardinal numbers is simplified if we assume AC; for, AC implies that every set is equinumerous with some ordinal, and, therefore, that every set x is equinumerous with a unique initial ordinal, which we shall call the *cardinal number* of x. Thus, the cardinal numbers are identified with the initial ordinals. To conform with the standard notation for ordinals, we let $\aleph_\alpha$ stand for ω_α. Propositions 4.35–4.36 establish some of the basic properties of addition and multiplication of cardinal numbers.

The status of the Axiom of Choice has become less controversial in recent years. To most mathematicians it seems quite plausible and it has so many important applications in practically all branches of mathematics that not to accept it would seem to be a wilful hobbling of the practicing mathematician. We shall discuss its consistency and independence later in this section.

Another hypothesis which has been proposed as a basic principle of set theory is the so-called *Axiom of Regularity* (Axiom D):

$$(X)(X \neq 0 \supset (Ey)(y \in X\ A y\ n\ X = 0)).$$

(Every non-empty class X contains a member which is disjoint from X.)

PROPOSITION 4.39

(1) The Axiom of Regularity implies the Fundierungsaxiom:

$$\sim (Ex)(Fnc(x) \wedge \mathfrak{D}(x) = \omega \wedge (u)(u \in \omega\ 3\ x\text{‘}(u') \in x\,'u))$$

i.e., there is no infinitely-descending $\in$*-sequence* $x_1 \ni x_2 \ni x_3\ 3\ . \ldots$

(2) If we assume the Axiom of Choice, then the Fundierungsaxiom implies the Axiom of Regularity.

(3) The Axiom of Regularity implies the non-existence of finite E*-cycles, i.e., of functions f on a non-zero finite ordinal a' such that* f ‘$0 \in f$ ‘$1 \in \ldots \in f\,'a \in f$ ‘0; *in particular, it implies that there is no set y such that* $y \in y$.

PROOF. (I) Assume $Fnc(x) \wedge \mathfrak{D}(x) = \omega \wedge (u)(u \in \omega\ 3\ x$ ‘$(u')\ E\ x$ 'u). Let $z = x$ "o. By the Axiom of Regularity, there is some element y in z such that $V\ n\ z = 0$. Since $y \in$ z, there is some finite ordinal a such that $y = x\,'a$. Then $x\,'(a') \in y \cap z$, contradicting $y \cap z = 0$.

(2) First, we define the *transitive closure* of a set u. Define by induction a function g on ω such that g ‘$0 = \{u)$, and $g\,'(a') = \bigcup(g\,'a)$ for each $a \in o$. Thus, g ‘$1 = u$, $g\,'2 = \bigcup(u)$, etc. Let $TC(u) = \bigcup(g$ “$\omega)$ be called the transitive closure of u. For any u, $TC(u)$ is transitive, i.e., $(v)(v \in TC(u) \supset u \subseteq TC(u))$. Now, assume AC and the *Fundierungsaxiom;* also, assume $X \# 0$ but there is no y $\in$ X such that y $\cap$ X $= 0$. Let b be some element of X; hence, $b\ n\ X \neq 0$. Let $c = TC(b) \cap X$. *By AC*, let h be a choice function for c. Define a function f on ω such that f ‘$0 = b$, and, for any $a \in o$, $f\,'(a') = h$ ‘$((f\,'a) \cap X)$. It follows easily that, for each $a \in o$, $f\,'(a') \in f$ 'a, contradicting the Fundierungsaxiom. (The proof can be summarized as follows: we start with an element b of X; then, using h, we pick an element f 'I in $b \cap X$; since, by assumption, f ‘1 and X cannot be disjoint, we pick an element f ‘2 in f ‘1 n X, etc.)

(3) Assume given a finite $\in$-cycle: f ‘$0 \in f$ ‘$1 \in \ldots \in f$ ‘$n \in f$ ‘0. Let X be the range of f: {f ‘0, f ‘1, . . . , f ‘n}. By the Axiom of Regularity, there is some

$f\,'i \in$ X such that $f\,‘i \cap X = 0$. But each element of X has an element in common with X.

Remark: The use of the Axiom of Choice in deriving the Axiom of Regularity from the Fundierungsaxiom is necessary. It can be shown (cf. Mendelson [1958]) that, if NBG is consistent, and if we add the Fundierungsaxiom as an axiom, then the Axiom of Regularity is not provable in this enlarged theory.

EXERCISES

4.88. If v is a transitive set such that $u \in v$, prove that $TC(u) \subseteq v$

4.89. By the ***Principle*** of Dependent Choices (PDC) we mean the following assertion: If r is a non-empty relation whose range is a subset of its domain, then there is a function $f : \omega \rightarrow \mathscr{D}$(r) such that $(u)(u \in \omega \supset \langle f‘u, f‘(u')\rangle \in$ r). (Mostowski [1948])

(a) Prove: t AC $\supset PDC$.

(b) Show that PDC implies the following Denumerable Axiom of Choice: $(DAC)\ Den(x) \wedge (u)(u \in x \supset u \neq 0) \supset (Ef)(f :$ x $\rightarrow$ u (x) $\wedge$ $(u)(u \in x \supset f\,$'u $\in u))$.

(c) Prove: $\vdash PDC \supset (x)(Inf(x) \supset \omega \preccurlyeq x)$. (Hence, by Exercise 4.72(c), PDC implies that a set is infinite if and only if it is Dedekind-infinite.)

(d) Prove that the conjunction of PDC and the Fundiemngsaxiom implies the Axiom of Regularity.

Let us define by transfinite induction a function Ψ, which was originally devised by von Neumann.

$$\Psi‘0 = 0$$

$$\Psi‘\ (a') = \mathscr{P}(\Psi‘\alpha)$$

$$Lim(\lambda) \supset \Psi‘\lambda = \bigcup_{\beta <_0 \lambda} (\Psi‘\beta)$$

Let $H = \bigcup(\Psi\ ''On)$, and let H_β stand for $\Psi\ ‘(\beta')$. Define a function ρ on H such that, for any **x** in H, p **'x** is the least ordinal ***a*** such that $x \in \Psi\ ‘\alpha$. $\rho\ ‘x$ is called the ***rank*** of x. Observe that p **'x** must be a successor ordinal.

EXERCISES

Prove:

4.90. $\vdash$ (a) $Trans(\Psi$ 'a).

4.91. $\vdash Trans(H)$.

492. t Ψ 'a $\subseteq \Psi'(a')$.

4.93. $\vdash a <_0 \beta \supset 9\ 'a \subseteq \Psi\ ‘\beta$.

4.94. $\vdash$ On $\subseteq H$.

4.95. $\vdash p\ 'a = a'$.

4.96. $\vdash u \in H \wedge v \in H \wedge u \in v \supset \rho\ ‘u <_0 \rho\ ‘v$.

4.97. $\vdash u \subseteq H \supset u \in H$.

PROPOSITION **4.40.** ***The Axiom of Regularity is equivalent to the assertion that $V = H$, i.e., that every set is a member of H.***

PROOF.

(1) Assume V $= H$, and let $X \# 0$. Let a be the least of the ranks of all the elements of X, and let b be an element of X such that p $‘b = \alpha$. Then $b \cap$ X = 0; for, if $u \in b \cap X$, then, by Exercise 4.96 above, p $'u \in p\ 'b = a$ contradicting the minimality of α.

(2) Assume the Axiom of Regularity, and assume that V – $H \neq 0$. By the Axiom of Regularity, there is some y $\in$ V – H such that y $\cap$ (V – H) = 0. Hence, $y \subseteq$ H, and so, by Exercise 4.97 above, $y \in$ H, contradicting y $\in$ V – H.

EXERCISES

4.98. Show that the Axiom of Regularity is equivalent to the special case: $x \neq 0 \supset (Ey)(y \in x \wedge y$ n $x = 0)$.

4.99. Show that, if we assume the Axiom of Regularity, then $Ord(X)$ is equivalent to: $Trans(X) \wedge$ E Con X, that is, to the wf

$$(u)(u \in X \supset u \subseteq X) \wedge (u)(v)(u \in X \wedge v \in X \wedge u \neq v \supset u \in v \vee v \in u).$$

Thus, with the Axiom of Regularity, a much simpler definition of the notion of ordinal class is possible, a definition in which all quantifiers are restricted to sets.

4.100. Show that the Axiom of Regularity implies that every non-empty transitive class contains 0.

Proposition 440 certainly increases the attractiveness of adding the Axiom of Regularity as a new axiom to NBG. The proposition V= H asserts that every set can be obtained by starting with 0 and applying the power set and union operations any transfinite number of times, and the assumption that this is so would clarify our rather hazy ideas about sets. By Exercise 4.99 above, the Axiom of Regularity would also simplify the definition of ordinal numbers. In addition. we can develop the theory of cardinal numbers on the basis of the Axiom of Regularity: namely, just define the cardinal number of a set **x** to be the set of all those y of lowest rank such that y $\cong$ **x**. (The basic requirement of the theory of cardinal numbers is that there be a function ***Card*** whose domain is V such that ***Card*** $'x =$ ***Card*** $‘y \equiv x \cong$ y.) There is no unanimity among mathematicians about whether we have sufficient grounds for adding the Axiom of Regularity as a new axiom, for, although it has great simplifying power, it does not have the immediate plausibility that even the Axiom of Choice has, nor has it had any mathematical applications.

The class H defined above determines an ***inner model*** of NBG in the following sense. For any wf $\mathscr{A}$ (written in unabbreviated notation) containing the free variables Y,, . . . , Y_n, let $\mathrm{Rel}_H(\mathscr{A})$ be the wf obtained from $\mathscr{A}$ by replacing every subformula (X)$\mathscr{B}$(X) by $(X)(X \subseteq$ H $\ni \mathscr{B}$(X)) (in making the replacements, we start with the innermost subformulas), and then prefixing $(Y_1 \subseteq H \wedge Y_2 \subseteq H \wedge \ldots \wedge Y_n \subseteq$ H$) \supset$. In other words, in forming $\mathrm{Rel}_H(\mathscr{A})$, we interpret "class" as "subclass of H". Then, for any theorem $\mathscr{A}$ of NBG, $\mathrm{Rel}_H(\mathscr{A})$ is also a theorem of NBG.

EXERCISE 4.101. *Verify* that, for each axiom $\mathcal{A}$ of NBG, $Rel_H(\mathcal{A})$ is a theorem of *NBG*. Notice that $Rel_H((x)\mathcal{B})$ is *equivalent* to $(x)(x \in H \supset \mathcal{B}^{\#})$, where $\mathcal{B}^{\#}$ is $Rel_H(\mathcal{B})$. *In particular*, $Rel_H(M(X))$ is $(EY)(Y \subseteq H \wedge X \in Y)$, which *is* equivalent to X ∈ H; thus, the "sets" of the model are the elements of *H*. If we adopt a semantic approach, then one need *only* observe that, if N is a model for NBG (in the usual *sense* of "model"), then the objects X of N that *satisfy* the wf X ⊆ H also form a model for NBG. In addition, one can *verify* that the Axiom of Regularity holds in this model; this is just Part (1) of Proposition 4.40. A direct consequence of this fact is the consistency of the Axiom of Regularity, *i.e.*, if NBG is *consistent*, so is the *theory* obtained by adding the Axiom of *Regularity* as a new axiom. That the Axiom of *Regularity* is *independent* of NBG can also be proved (cf. Bernays [1954], Part *VII*) by means *of* a suitable model, though the model is more complex than that giuen *above* for the *consistency* proof. Thus, the Axiom of *Regularity* is both *consistent* and *independent* with respect to *NBG*: we can *consistently* add either it or its negation as an axiom to NBG, if NBG is consistent. (Practically the same proofs *also* show the independence and consistency of the Axiom of Regularity with respect *to* NBG + (AC).)

EXERCISES

4.102. Consider the model whose domain is H_α and whose interpretation of ∈ is E_{H_α}, the membership relation restricted to H_α. Notice that the "sets" of this model are the sets of rank $\leqslant_0$ a, and the "proper classes" are the sets of rank a'. Show that the model H_α satisfies all axioms of NBG (except possibly the Axioms of Infinity and Replacement) if and only if $Lim(\alpha)$. Prove also that H satisfies the Axiom of Infinity if and only if a $>_0 \omega$.

4.103. Show that the Axiom of Infinity is not provable from the other axioms of NBG, if the latter are consistent.

4.104. Show that the Axiom of Replacement R is not provable from the other axioms (T, P, N, B1 – B7, U, W, S) if these latter are consistent.

4.105.^{D} **An** ordinal a such that H_α is a model for NBG is called *inaccessible*. Since NBG has only a finite number of proper axioms, the assertion that a is inaccessible can be expressed by the conjunction of the relativization to H_α of the proper axioms of NBG. Show that the existence of inaccessible ordinals is not provable in NBG if the latter is consistent, and the same is true even if the Axiom of Choice and the Generalized Continuum Hypothesis are added as axioms. (Compare Shepherdson [1951–1953], Montague-Vaught [1959], and, for related results, Bernays [1961] and Levy [1960].) Inaccessible ordinals have been shown to have connections with problems in measure theory and algebra (cf. Ulam [1930], Zeeman [1955], and Erdos-Tarski [1961]).† The consistency of the theory obtained from NBG by adding an axiom asserting the existence of an inaccessible ordinal is still an open question.

†Inaccessible ordinals are involved also with attempts to provide a suitable set-theoretic foundation for category theory (cf. Maclane [1971], Gabriel [1962], Sonner [1962], Kruse [1966], Isbell [1966]).

The Axiom of Choice turns out to be consistent and independent with respect to NBG + (Axiom of Regularity); more precisely, if NBG is consistent, AC is an undecidable sentence of the theory NBG + (Axiom of Regularity). In fact, Gödel ([1938], [1939], [1940]) showed that, if NBG is consistent, then the theory NBG + (AC) + (Axiom of Regularity) + (GCH) is also consistent, where (GCH) stands for the Generalized Continuum Hypothesis:

$$(x)(Inf(x) \supset \sim (Ey)(x \prec y \wedge \prec \mathcal{P}(x))).$$

(Our statement of Gödel's result is a bit redundant, since ⊢(GCH) 3 (AC) has been proved by Sierpinski [1947] and Specker [1954]. This result will be proved below.) The unprovability of AC from (NBG) + (Axiom of Regularity), if NBG is consistent, has been proved by P. J. Cohen [1963], who also has shown the independence of the special Continuum Hypothesis,

$$2'' \cong \omega_1, \text{ from NBG + (AC) + (Axiom of Regularity).}$$

For expositions of the ingenious work of Cohen and its further development, see Cohen [1966] and Shoenfield [1971] (as well as Rosser [1969], Felgner (19711, Jech [1971], Takeuti-Zaring [1973]).

We shall present here a modified form of the proof in Cohen [1966] of Sierpinski's proof that (GCH) implies (AC).

DEFINITION. For any set v, let $\mathcal{P}^0(v) = v$, $\mathcal{P}^1(v) = \mathcal{P}(v)$, $\mathcal{P}^2(v) = \mathcal{P}(\mathcal{P}(v)), \ldots, \mathcal{P}^{k+1}(v) = \mathcal{P}(\mathcal{P}^k(v))$ for all k in *w*.

LEMMA 4.41. *If* $\omega \preccurlyeq v$, *then* $\mathcal{P}^k(v) +_c \mathcal{P}^k(v) \cong \mathcal{P}^k(v)$ for all k $\geqslant_0 1$.

PROOF. Remember that $\mathcal{P}(x) \cong 2^x$ (Exercise 4.40, p. 193). From $\omega \preccurlyeq$ v, we obtain $w \preccurlyeq \mathcal{P}^k(v)$ for all k in ω. Hence, $\mathcal{P}^k(v) +_c 1 \cong \mathcal{P}^k(v)$ for all k in ω, by Exercise 4.72(e). Now, for any k $\geqslant_0 1$,

$$\mathcal{P}^k(v) +_c \mathcal{P}^k(v) = \mathcal{P}^k(v) \times 2 = \mathcal{P}(\mathcal{P}^{k-1}(v)) \times 2 \cong 2^{\mathcal{P}^{k-1}(v)} \times 2$$
$$= 2^{\mathcal{P}^{k-1}(v)} \times 2^1 \cong 2^{\mathcal{P}^{k-1}(v)+_c 1} \cong 2^{\mathcal{P}^{k-1}(v)} \cong \mathcal{P}(\mathcal{P}^{k-1}(v)) = \mathcal{P}^k(v).$$

LEMMA 4.42. If $y +_c x \cong \mathcal{P}(x +_c x)$, then $\mathcal{P}$(x) $\preccurlyeq$ y.

PROOF. Notice that $\mathcal{P}(x +_c x) \cong 2^{x+_c x} \cong 2^x \times 2^x \cong \mathcal{P}(x) \times \mathcal{P}$(x). Let y* = y × {0} and x* = x × {1}. Since $y +_c x \cong \mathcal{P}(x +_c x) \cong \mathcal{P}(x) \times \mathcal{P}(x)$, there is a function **j** such that $y^* \cup x^* \overset{f}{\cong} \mathcal{P}(x) \times \mathcal{P}(x)$. Let h be the function which takes each *u* in x^* into the first component w of the pair *f* 'u. Thus, $h : x^* \rightarrow \mathcal{P}(x)$. By Proposition 4.23(a), there must exist c ∈ $\mathcal{P}$(x) – $h``x^*$. Then, for all z in $\mathcal{P}$(x), there exists a unique *v* in y^* such that *f* '*v* = (c, z). This determines a one-one function from $\mathcal{P}$(x) into y. Hence, $\mathcal{P}$(x) $\preccurlyeq$ *y*.

PROPOSITION 4.43. Assume GCH.

(a) For any ordinal *β*, *if* *u* cannot be well-ordered, $u +_c u \cong u$, and $\beta \preccurlyeq 2^u$, then $\beta \preccurlyeq u$.

(b) The Axiom of Choice AC *holds*.

PROOF.

(a) Notice that $u +_c u \cong u$ implies 1 $+_c u \cong$ u, by Exercise 4.79(b); therefore, by Exercise 4.58(i), 2'' $+_c u \cong$ 2''. Now, $u \preccurlyeq \beta +_c u \preccurlyeq$ 2'' $+_c u \cong$ 2''. By GCH, either (i) $u \cong \beta +_c u$ or (ii) $\beta +_c u \cong 2^u$. If (ii) holds, $\beta +_c u \cong 2^u +_c u$,- $\mathcal{P}(u +_c u)$. Hence, by Lemma 4.42, $\mathcal{P}(u) \preccurlyeq \beta$, and, therefore, $u \preccurlyeq \beta$. Then, since u would be equinumerous with a subset of an ordinal, u could be well-ordered, contradicting our assumption. Hence, (i) must hold. But then, $\beta \preccurlyeq \beta +_c u \cong u$.

(b) We shall prove AC by proving the equivalent sentence (W.O.) asserting that every set can be well-ordered. To that end, consider any set x, and assume, for the sake of contradiction, that x cannot be well-ordered. Let v = $2^{x \cup \omega}$. Then $\omega \preccurlyeq$ x $\cup$ $\omega \preccurlyeq v$. Hence, by Lemma 4.41, $\mathcal{P}^k(v) +, \mathcal{P}^k(v) \cong \mathcal{P}^k(v)$ for all k $\geqslant_0$1. Also, since x $\preccurlyeq$ x u $\omega \preccurlyeq$ v $\prec \mathcal{P}(v) \prec \mathcal{P}\mathcal{P}(v) \prec \ldots$, and x cannot be well-ordered, each $\mathcal{P}^k(v)$ cannot be well-ordered,for k $\geqslant_0$ 0. Let $\beta = \mathcal{H}$ 'v. We know that $\beta \preccurlyeq \mathcal{P}^4(v)$ (p. 200). Hence, by Part (a), with $u = \mathcal{P}^3(v)$, we obtain $\beta \preccurlyeq \mathcal{P}^3(v)$. Using Part (a) twice more (successively with $u = \mathcal{P}^2(v)$ and $u = \mathcal{P}(v)$), we obtain X '$v = \beta \preccurlyeq v$. But this contradicts the definition of X 'v as the least ordinal not equinumerous with a subset of v.

EXERCISE 4.106. An a-sequence is a function w whose domain is a. *If* the range of w consists of ordinals, w is called an ordinal a-sequence, and if, in addition, $\beta <_0 \gamma <_0$ a implies $w(\beta) <_0 w(\gamma)$, w is called an increasing ordinal a-sequence. By Proposition 4.11, if w is an increasing ordinal a-sequence, then $\bigcup(w$ "$\alpha)$ *is* the least upper bound of the range of w. An ordinal 6 is said *to* be regular if, for any increasing ordinal a-sequence w such that a $<_0 \delta$ and the ordinals in the range of w are all $<_0$ 6, then $\bigcup(w$ "a) $+_0 1 <_0$ 6. Non-regular ordinals are called singular ordinals.

(i) Which *finite* ordinals are regular?

(ii) Show that ω_0 is regular and that ω_ω is singular.

(iii) Prove that every regular ordinal is an initial ordinal.

(iv) Assuming the Axiom of Choice (AC), prove that every ordinal *of* the form $\omega_{\gamma +_0 1}$ is regular.

(v) If ω_α is regular and $Lim(\alpha)$, prove that $\omega_\alpha =$ a. (A regular ordinal ω_α such that $Lim(\alpha)$ is called a weakly inaccessible ordinal.)

(vi) Show that, if ω_α has the property that $\gamma <_0 \omega_\alpha$ implies $\mathcal{P}(\gamma) \prec \omega_\alpha$, then $Lim(\alpha)$. The converse is implied by the Generalized Continuum Hypothesis. A regular ordinal ω_α such that a $>_0$ 0, and $\gamma <_0 \omega_\alpha$ implies $\mathcal{P}(\gamma) \prec \omega_\alpha$, is called strongly inaccessible. Thus, every strongly inaccessible ordinal is weakly inaccessible, and, if the (GCH) *holds*, the strongly inaccessible ordinals coincide with the weakly inaccessible ordinals.

(vii) (*Shepherdson* [1951–53], Montague-Vaught [1959]) (a) If γ is inaccessible (*i.e.*, if H_γ is a model of NBG), then γ is weakly inaccessible. ^{D}(b) In the theory NBG + (AC), γ is inaccessible if and *only* if γ is strongly inaccessible.

(viii) If (NBG) is consistent, then in the theory NBG + (AC) + (GCH) it is impossible to prove the existence *of* weakly inaccessible ordinals.

We have chosen to develop axiomatic set theory on the basis of NBG because it is simple and convenient for the practicing mathematician. Of course, there are many other varieties of axiomatic set theory.

(1) Strengthening NBG, we can replace Axioms B1–B7 by the Axiom Schema: $(EX)(y_1)(y_2)\ldots(y_n)(\langle y_1,\ldots,y_n\rangle \in X \equiv \phi(y_1,\ldots,y_n))$, where ϕ is any wf (not necessarily predicative) of NBG. This new theory MK, called Morse-Kelley set theory because it was originally proposed by A. Morse (cf. Morse [1965]) and became widely known through its publication in Kelley [1955], is a proper extension of NBG. Although MK is simpler and more powerful than NBG, its strength makes its consistency a riskier gamble. (However, if we add to NBG + (AC) the axiom In asserting the existence of a strongly inaccessible ordinal θ, then the model H_θ is a model of MK. Hence, MK involves no more risk than NBG + (AC) + (In).) Mostowski [1951] proved that MK is stronger than NBG; in fact, the consistency of NBG is provable in MK. A development of set theory based upon MK may be found in Rubin [1967], and Chuquai [1972] has extended Cohen's independence results to MK.

(2) Zermelo-Skolem-Fraenkel (ZSF) set theory is essentially the part of NBG which refers only to sets. We use x,, x„ . . . as variables in ZSF. There is a single binary predicate $\in$. The axioms are Axioms T (Extensionality), P (Pairing), N (Null Set), U (Sum Set), W (Power Set), I (Infinity), plus an axiom schema corresponding to Axiom R (Replacement): for any wf $\varphi(v, u)$, the following is an axiom.

$$((v)(w)(u))\varphi(v,u) \wedge \varphi(v,w) \supset u = w))$$
$$\supset (Ey)(u)(u \in y \equiv (Ev)(v \in x \text{ A } \varphi(v,u)))$$

Every wf of ZSF can be considered a wf of NBG, with the variables of ZSF playing the role of restricted set variables in NBG. It has been proved (cf. Novak-Gál [1951], Rosser-Wang [1950], Shoenfield [1954]) that, for any closed wf $\mathcal{Q}$ of ZSF, if $\vdash_{NBG}\mathcal{Q}$, then $\vdash_{ZSF}\mathcal{Q}$; therefore, ZSF is consistent if and only if NBG is consistent. For a detailed development of ZSF, consult Suppes [1960], Zuckerman [1974], Krivine [1971].

For a survey of various axiomatic set theories, cf. Fraenkel-Bar Hillel [1958] and Hatcher [1968]. To obtain more detailed treatments of the theory of types, consult Church [1940] and Quine [1938]; for Quine's New Foundations (NF), cf. Rosser [1953] and Specker [1953] (where it is shown that the strong Axiom of Choice is disprovable in NF), and, for Quine's system ML, cf. Quine [1951]. Drake [1974] is an account of many recent developments in axiomatic set theory.

CHAPTER 5

EFFECTIVE COMPUTABILITY

1. Markov Algorithms

A function $f(x_1, \ldots, x_n)$ is thought of as being effectively computable if there is a mechanical procedure for determining the value $f(k_1, \ldots, k_n)$ when the arguments $k_1, \ldots, k_n$ are given. The phrase "mechanical procedure" is not at all precise; what we mean is a process which requires no ingenuity for its performance. An obvious example is the addition of two integers expressed in decimal notation. Another well-known case is the Euclidean algorithm for obtaining the greatest common divisor of two integers. In these two examples, it seems intuitively clear that the given functions are effectively computable. This is generally the case when an effective procedure has already been discovered. However, more and more in mathematics, we are faced with the task of showing that there is no effectively computable function of a certain kind or that there is no effective procedure for solving a large class of problems. To illustrate, we can cite on the one hand the well-known effective way of determining whether or not any given polynomial $f(x)$ in one variable with integral coefficients has an integral root.† On the other hand, the famous Tenth Problem of Hilbert asked whether there is an effective procedure for determining whether or not any given polynomial $f(x_1, \ldots, x_n)$ with integral coefficients, in any finite number of variables, has integral roots. This problem recently has been solved by Matiyasevich [1970], whose proof was the culmination of previous work by M. Davis, J. Robinson, and H. Putnam. (Cf. Davis [1973] for a complete exposition.) If we attempt to prove that there is no effective procedure or operation of a certain kind, it is apparent that we have to give a precise, mathematical definition of the notion of effective computability. The situation is analogous to that which prevailed in mathematics before notions like continuity, curve, surface, and area were explicated.

Any particular problem of a general class of problems can be formulated as an expression of some language. Any expression of a language can be considered as a sequence of symbols of that language, provided that the blank which is

†If $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, then any integral solution of $f(x) = 0$ must be a divisor of a_0. Each of the finite number of divisors of a_0 can be tested to see whether it satisfies $f(x) = 0$.

usually used to separate words is assumed to be a symbol in its own right. By an alphabet we mean a non-empty finite set of symbols. Most natural languages use only a finite number of symbols, and, for our purposes, it also suffices to treat only such alphabets. (Indeed, anything that can be done with an infinite alphabet a,, a,, . . . can be accomplished with a two-symbol alphabet {b, c}, if we let $b\underbrace{cc\ldots cc}_{n\text{ times}}b$ play the role of a,.) For uniformity, we assume that the symbols of all alphabets are taken from the denumerable sequence S_0, S,, S_2, . . . , though, sometimes, for convenience, we shall use other letters.

A word in an alphabet A is any finite sequence of symbols of A. The empty sequence of symbols is called the empty word, and is denoted by A. If P denotes a word $S_{j_1} \ldots S_{j_k}$ and Q denotes a word $S_{r_1} \ldots S_{r_m}$, then we use PQ to denote the juxtaposition $S_{j_1} \ldots S_{j_k} S_{r_1} \ldots S_{r_m}$ of the two words. In particular, PA = ΛP = P; also, $(P_1P_2)P_3 = P_1(P_2P_3)$.

An alphabet A is an extension of an alphabet B if and only if B ⊆ A. If A is an extension of B, any word of B is a word of A.

By an algorithm in an alphabet A, we mean an effectively computable function $\mathfrak{A}$ whose domain is a subset of the set of words of A and the values of which are also words in A. If P is a word in A, $\mathfrak{A}$ is said to be applicable to P if P is in the domain of $\mathfrak{A}$; if $\mathfrak{A}$ is applicable to P, we denote its value by $\mathfrak{A}(P)$. By an algorithm over an alphabet A we mean an algorithm $\mathfrak{A}$ in an extension B of A. Of course, the notion of algorithm is as hazy as that of effectively computable function.

Most familiar algorithms can be broken down into a few simple steps. Starting from this observation, and following Markov [1954], we select a particularly simple operation, substitution of one word for another, as the basic unit from which algorithms are to be constructed. To this end, if P and Q are words of an alphabet A, then we call the expressions P → Q and P → . Q productions in the alphabet A. We assume here that "→" and the dot "·" are not symbols of A. Notice that P or Q can be the empty word. P → Q is called a simple production, while P → . Q is a terminal production. Let us use $P \to (\cdot)Q$ to denote either P → Q or P → · Q. A finite list of productions in A

$$\begin{array}{l} P_1 \to (\cdot)Q_1 \\ P_2 \to (\cdot)Q_2 \\ \quad\vdots \\ P_r \to (\cdot)Q_r \end{array}$$

is called an algorithm schema and determines the following algorithm $\mathfrak{A}$ in A. As a preliminary definition, we say that a word T occurs in a word Q if there are words U, V (possibly empty) such that Q = UTV. Now, given a word P in A: (1) We write $\mathfrak{A}$: P $\sqsupset$ if none of the words $P_1, \ldots, P_r$ occurs in P. (2) Otherwise, if m is the least integer, with 1 ⩽ m ⩽ r, such that P_m occurs in P, and if R is the word which results from replacing the left-most occurrence of P_m in P by Q_m, then we write

(a) $$\mathfrak{A} : P \vdash R$$

if $P_m \to (\cdot)Q_m$ is simple (and we say that $\mathfrak{A}$ simply transforms P into R);

(b) $$\mathfrak{A} : P \vdash \cdot R$$

if $P_m \to (\cdot)Q_m$ is terminal (and we say that $\mathfrak{A}$ terminally transforms P into R).

We then define $\mathfrak{A}$: P ⊧ R to mean that there is a sequence $R_0, R_1, \ldots, R_k$ such that P = R_0; R = R_k; if 0 ⩽ j ⩽ k − 2, $\mathfrak{A}$: R, ⊢ R_{j+1}; and either $\mathfrak{A}$: $R_{k-1} \vdash R_k$ or $\mathfrak{A}$: $R_{k-1} \vdash . R_k$. (In the second case, we write $\mathfrak{A}$: P ⊧ · R.) We set $\mathfrak{A}(P)$ = R if and only if either $\mathfrak{A}$: P ⊧ · R, or $\mathfrak{A}$: P ⊧ R and $\mathfrak{A}$: R $\sqsupset$. The algorithm thus defined is called a normal algorithm (or Markov algorithm) in the alphabet A.

The action of $\mathfrak{A}$ can be described as follows: given a word P, we find the first production $P_m \to (\cdot)Q_m$ in the schema such that P_m occurs in P. We then substitute Q_m for the left-most occurrence of P_m in P. Let R_1 be the new word obtained in this way. If $P_m \to (\cdot)Q_m$ is a terminal production, the process stops and the value of the algorithm is R,. If $P_m \to (\cdot)Q_m$ is simple, then we apply the same process to R, as was just applied to P, and so on. If we ever obtain a word R_i such that $\mathfrak{A}$: $R_i \sqsupset$, i.e., no P_m occurs in R, for 1 ⩽ m ⩽ r, then the process stops and the value of $\mathfrak{A}$ is R,. It is possible that the process just described never stops. In that case, $\mathfrak{A}$ is not applicable to the given word P.

Our exposition of the theory of normal algorithms will closely follow that of Markov [1954].

Examples.

1. Let A be the alphabet {b, c). Consider the schema

$$\begin{array}{l} b \to \cdot\Lambda \\ c \to c \end{array}$$

The normal algorithm $\mathfrak{A}$ defined by this schema transforms any word containing at least one occurrence of b into the word obtained by erasing the left-most occurrence of b. $\mathfrak{A}$ transforms the empty word A into itself. $\mathfrak{A}$ is not applicable to any non-empty word not containing b.

2. Let A be the alphabet {a,, a,, . . . , a_n}. Consider the schema

$$\begin{array}{l} \text{a,} \to \text{A} \\ \text{a,} \to \Lambda \\ \quad \vdots \\ \text{a,} \to \Lambda \end{array}$$

We can abbreviate this schema as follows:

$$\xi \to \text{A} \quad (\xi \text{ in A})$$

(Whenever we use such abbreviations, the productions intended may be listed in any order.) The corresponding normal algorithm transforms every word into the empty word. For example, $\mathfrak{A} : a_1a_2a_1a_3a_0 \vdash a_1a_2a_1a_3 \vdash a_2a_1a_3 \vdash a_2a_3 \vdash$ a, $\vdash \Lambda$ and 8 : Λ ⌉. Hence $\mathfrak{A}(a_1a_2a_1a_3a_0) = $ A.

3. Let A be an alphabet containing the symbol S_1, which we shall abbreviate 1. For natural numbers n, we define ii inductively as follows: $\bar{0} = 1$ and $\overline{n+1}$ = iil. Thus, $\bar{1}$ = 11, $\bar{2}$ = 111, etc. The words ii are called numerals. Now consider the schema A → . 1, defining a normal algorithm 8. For any word P in A, $\mathfrak{A}(P) = 1P\cdot$ † In particular, for every natural number n, $\mathfrak{A}(\bar{n}) = \overline{n+1}$.

4. Let A be an arbitrary alphabet {a,, a,, . . . , a,,). Given a word $P = a_{j_0}a_{j_1} \ldots a_{j_k}$, let P = $a_{j_k} \ldots a_{j_1}a_{j_0}$ be the inverse of P. We seek a normal algorithm $\mathfrak{A}$ such that $\mathfrak{A}(P) = \check{P}$. Consider the following (abbreviated) algorithm schema in the alphabet B = A u {a, β}.

(a)	$\alpha\alpha \to \beta$	
(b)	$\beta\xi \to \xi\beta$	(ξ in A)
(c)	$\beta\alpha \to \beta$	
(d)	$\beta \to \cdot\Lambda$	
(e)	$\alpha\eta\xi \to \xi\alpha\eta$	(ξ, η in A)
(f)	$\Lambda \to \alpha$	

This determines a normal algorithm $\mathfrak{A}$ in B. Let $P = a_{j_0}a_{j_1} \ldots a_{j_k}$ be any word in A. Then, $\mathfrak{A} : P \vdash \alpha P$ by production (f); $\alpha P \vdash a_{j_1}\alpha a_{j_0}a_{j_2} \ldots a_{j_k} \vdash$ $a_{j_1}a_{j_2}\alpha a_{j_0}a_{j_3} \ldots a_{j_k} \ldots \vdash a_{j_1}a_{j_2} \ldots a_{j_k}\alpha a_{j_0}$ by production (e). Thus, $\mathfrak{A} : P \vDash a_{j_1}a_{j_2} \ldots a_{j_k}\alpha a_{j_0}$. Then, by production (f), $\mathfrak{A} : P \vDash \alpha a_{j_1}a_{j_2} \ldots a_{j_k}\alpha a_{j_0}$. Applying, as before, production (e), $\mathfrak{A} : P \vDash a_{j_2}a_{j_3} \ldots a_{j_k}\alpha a_{j_1}\alpha a_{j_0}$. Iterating this process, we obtain 8 : $P \vDash \alpha a_{j_k}\alpha a_{j_{k-1}}\alpha \ldots \alpha a_{j_1}\alpha a_{j_0}$. Then, by production (f), $\mathfrak{A} : P \vDash \alpha\alpha a_{j_k}\alpha a_{j_{k-1}}$a $\ldots \alpha a_{j_1}\alpha a_{j_0}$, and, by production (a), $\mathfrak{A} : P \vDash \beta a_{j_k}\alpha a_{j_{k-1}}\alpha \ldots \alpha a_{j_1}\alpha a_{j_0}$; applying productions (b) and (c), and, finally, (d), we arrive at 8 : $P \vDash . \check{P}$. Thus, $\mathfrak{A}$ is a normal algorithm over A which inverts every word of A.‡

EXERCISES

5.1. Let **A** be an alphabet. Describe the action of the normal algorithms given by the following schemas.

(a) Let Q be a fixed word in **A**, and let the algorithm schema be: A → . Q.

(b) Let Q be a fixed word in A, and let a be a symbol not in **A**. Let **B** = **A u** (a). Consider the schema

$$\begin{array}{ll} \alpha\xi \to \xi\alpha & (\xi \text{ in A}) \\ \alpha \to \cdot Q & \\ \Lambda \to \alpha & \end{array}$$

(c) Let Q be a fixed word in **A**. Take the schema

$$\begin{array}{ll} \xi \to \Lambda & (\xi \text{ in A}) \\ \Lambda \to \cdot Q & \end{array}$$

(d) Let **B** = **A** ∪ {1}. Consider the schema

$$\begin{array}{ll} \xi \to 1 & (\xi \text{ in A} - \{1\}) \\ \text{A+} \ \cdot 1 & \end{array}$$

5.2. Let **A** be an alphabet not containing the symbols a, β, y. Let B = **A** ∪ **(a)** and C = **A** ∪ {α, β, γ}.

(a) Construct a normal algorithm $\mathfrak{A}$ in **B** such that $\mathfrak{A}(\Lambda)$ = A and $\mathfrak{A}(\xi P)$ = P for any symbol ξ in **A** and any word P in **A.** Thus, $\mathfrak{A}$ erases the first letter of any non-empty word in **A.**

(b) Construct a normal algorithm G in B such that $\mathfrak{D}(\Lambda)$ = A and $\mathfrak{D}(P\xi)$ = P for any symbol ξ in **A** and word P in A. Thus, G erases the last letter of any non-empty word in A.

(c) Construct a normal algorithm $\mathfrak{C}$ in **B** such that $\mathfrak{C}(P)$ = A if P contains exactly two occurrences of a, and $\mathfrak{C}(P)$ is defined and ≠ A in all other cases.

(d) Construct a normal algorithm $\mathfrak{B}$ in C such that, for any word P of **A,** $\mathfrak{B}(P)$ = PP.

53. Let **A** and **B** be alphabets, and let a be a symbol in neither **A** nor B. For certain symbols $a,, \ldots, a_k$ in **A,** let $Q_1, \ldots, Q_k$ be corresponding words in B. Consider the algorithm which associates with each word of **A** the word $\mathrm{Sub}^{a_1,\ldots,a_k}_{Q_1,\ldots,Q_k}(P)$ obtained by simultaneous substitution of each Q_i for a_i (i = 1, . . . , k). Show that this is given by a normal algorithm in **A** ∪ **B** ∪ (a).

5.4. Let H = (l} and **M** = (1, * }. Every natural number n is represented by its numeral $\bar{n}$, which is a word in H. We represent every k-tuple (n,, n_2, . . . , n_k) of natural numbers by the word $\bar{n}_1 * \bar{n}_2 * \ldots \bullet \bar{n}_k$ in **M.** We shall denote this word by $\overline{(n,, \ldots, n_k)}$. For example, (3, 1, 2) is 1111 * 11 * 111.

(a) Show that the schema

$$\begin{array}{c} * + * \\ \text{a}11 \to \alpha 1 \\ \alpha 1 \to \cdot 1 \\ \Lambda \to \alpha \end{array}$$

defines a normal algorithm $\mathfrak{A}_Z$ over **M** such that $\mathfrak{A}_Z(\bar{n}) = \bar{0}$ for any n, and $\mathfrak{A}_Z$ is applicable only to numerals in **M.**

(b) Show that the schema

$$\begin{array}{c} * + * \\ \alpha 1 \to \cdot 11 \\ \Lambda \to \alpha \end{array}$$

defines a normal algorithm $\mathfrak{A}_Z$ over **M** such that $\mathfrak{A}_N(\bar{n}) = \overline{n+1}$ for all n, and $\mathfrak{A}_N$ is applicable only to numerals in M.

†To see this, observe that *A* occurs at the beginning of any word *P*, since *P* = *AP*.

‡The distinction between a normal algorithm in A and a normal algorithm over A is important. A normal algorithm in A uses only symbols of A, while a normal algorithm over A may employ additional symbols not in A. Every nonnal algorithm in A is a normal algorithm over A, but there are algorithms in A which are determined by normal algorithms over A but which are not normal algorithms in A (cf. Exercise 5.9(d), p. 240).

(c) Let $a,, \dots, \alpha_{2k}$ be symbols not in M. Let $1 \leq j$ 6 k. Let $\mathfrak{S}_i$ be the list

$$\alpha_{2i-1} * \to \alpha_{2i-1} *$$
$$\alpha_{2i-1} 1 \to \alpha_{2i} 1$$
$$\alpha_{2i} 1 \to \alpha_{2i}$$
$$\alpha_{2i} * \to \alpha_{2i+1}$$

If $1 < j < k$, consider the algorithm schema

$$\mathfrak{S}_1$$
$$\vdots$$
$$\mathfrak{S}_{j-1}$$
$$\alpha_{2j-1} * \to \alpha_{2j-1} *$$
$$\alpha_{2j-1} 1 \to \alpha_{2j} 1$$
$$\alpha_{2j} 1 \to 1 \alpha_{2j}$$
$$\alpha_{2j} * \to \alpha_{2j}+1$$
$$\mathfrak{S}_{j+1}$$
$$\vdots$$
$$\mathfrak{S}_{k-1}$$
$$\alpha_{2k-1} * \to \alpha_{2k-1} *$$
$$\alpha_{2k-1} 1 \to \alpha_{2k} 1$$
$$\alpha_{2k} 1 \to \alpha_{2k}$$
$$\alpha_{2k} * \to \alpha_{2k} *$$
$$\alpha_{2k} \to \cdot \Lambda$$
$$\Lambda \to \alpha_1$$

If $j = 1$, consider the schema

$$\alpha_1 * \to \alpha_1 *$$
$$\alpha_1 1 \to \alpha_2 1$$
$$\alpha_2 1 \to 1 \alpha_2$$
$$\alpha_2 * \to \alpha_3$$
$$\mathfrak{S}_2$$
$$\vdots$$
$$\mathfrak{S}_{k-1}$$
$$\alpha_{2k-1} * \to \alpha_{2k-1} *$$
$$\alpha_{2k-1} 1 \to \alpha_{2k} 1$$
$$\alpha_{2k} 1 \to \alpha_{2k}$$
$$\alpha_{2k} * \to \alpha_{2k} *$$
$$\alpha_{2k} \to \cdot \Lambda$$
$$\Lambda \to \alpha_1$$

If $j = k$, consider the schema

$$\mathfrak{S}_1$$
$$\vdots$$
$$\mathfrak{S}_{k-1}$$
$$\alpha_{2k-1} * \to \alpha_{2k-1} *$$
$$\alpha_{2k-1} 1 \to \alpha_{2k} 1$$
$$\alpha_{2k} 1 \to 1 \alpha_{2k}$$
$$\alpha_{2k} * \to \alpha_{2k} *$$
$$\alpha_{2k} * \to \alpha_{2k} *$$
$$\alpha_{2k} \to \cdot \Lambda$$
$$\Lambda \to \alpha_1$$

Show that the corresponding normal algorithm $\mathfrak{A}_j^k$ is such that $\mathfrak{A}_j^k(\overline{(n_1, \dots, n_k)}) = \overline{n}_j$; and $\mathfrak{A}_j^k$ is applicable only to words of the form $\overline{(n_1, \dots, n_k)}$.

(d) Construct a schema for a normal algorithm in M transforming $\overline{(n_1, n_2)}$ into $\overline{|n_1 - n_2|}$.

(e) Construct a normal algorithm in M for addition.

(f) Construct a normal algorithm over M for multiplication.

Given algorithms $\mathfrak{I}$ and $\mathfrak{B}$ and a word P, we write $\mathfrak{A}(P) \approx \mathfrak{B}(P)$ if and only if either $\mathfrak{I}$ and $\mathfrak{B}$ are both applicable to P and $\mathfrak{A}(P) = \mathfrak{B}(P)$ or neither $\mathfrak{I}$ nor $\mathfrak{B}$ is applicable to P. More generally, if C and D are expressions, then $C \approx D$ is to hold if and only if neither C nor D is defined or both C and D are defined and denote the same object. If $\mathfrak{I}$ and $\mathfrak{B}$ are algorithms over an alphabet A, then we say that $\mathfrak{A}$ and $\mathfrak{B}$ are ***fully equivalent*** relative to A if and only if $\mathfrak{A}(P) \approx \mathfrak{B}(P)$ for every word P in A; we say that $\mathfrak{A}$ and $\mathfrak{B}$ are *equivalent* relative to A if and only if, for any word P in A, whenever $\mathfrak{A}(P)$ or $\mathfrak{B}(P)$ exists and is in A, then $\mathfrak{A}(P) \approx \mathfrak{B}(P)$.

Let M be the alphabet (I, $*$), as in Exercise 5.4 above; let w be the set of natural numbers. Given a partial effectively computable number-theoretic function φ of k arguments, i.e., a function from a subset of ω^k into w, we denote by $\mathfrak{B}_\varphi$ the corresponding algorithm in M; that is, $\mathfrak{B}_\varphi(\overline{(n_1, \dots, n_k)}) = \overline{\varphi(n_1, \dots, n_k)}$ whenever either of the two sides of the equation is defined; $\mathfrak{B}_\varphi$ is assumed to be inapplicable to words not of the form $\overline{(n_1, \dots, n_k)}$. The function φ is said to be ***partially Markov-computable*** if and only if there is a normal algorithm $\mathfrak{S}$ over M which is fully equivalent to $\mathfrak{B}_\varphi$ relative to M.† If the function φ is total, i.e., if φ is defined for all k-tuples of natural numbers, and if φ is partially Markov-computable, then φ is said to be ***Markov-computable***.

Let us generalize the notion of recursive function (cf. p 138). A partial function φ of k arguments is called ***partial recursive*** if and only if φ can be obtained from the initial functions Z (zero function), U_j^n (projection functions), and N (successor function) by means of substitution, recursion, and the unrestricted p-operator. (We say that ψ comes from τ by means of the unrestricted p-operator if and only if $\psi(x_1, \dots, x_n) = \mu y(\tau(x_1, \dots, x_n, y) = 0)$. More precisely, $\mu y(\tau(x_1, \dots, x_n, y) = 0)$ is the least number k (if such exists) such that, if $0 \leqslant i < k$, $\tau(x_1, \dots, x_n, i)$ exists and is not 0, and $\tau(x_1, \dots, x_n, k) = 0$. Notice that ψ may not be defined for certain n-tuples; in particular, for those n-tuples $(x,, \dots, x_n)$ for which there is no y such that $\tau(x_1, \dots, x_n, y) = 0$.) Clearly, every recursive function is partial recursive. The assertion that every total partial recursive function is recursive is true, but not at all obvious, and will be proved later. We shall show that the partial recursive functions coincide with the partially Markov-computable functions and that the recursive functions are identical with the Markov-computable functions.

A normal algorithm is said to be ***closed*** if and only if one of the productions in its schema has the form $A \to \cdot Q$. Such an algorithm can only end terminally, i.e., by an application of a terminal production. Given an arbitrary normal algorithm $\mathfrak{S}$, add on at the end of the schema for $\mathfrak{A}$ the new production $A \to . A$, and denote by $\mathfrak{A}\cdot$ the normal algorithm determined by this enlarged schema. $\mathfrak{A}\cdot$ is closed, and '21$\cdot$ is fully equivalent to $\mathfrak{A}$ relative to the alphabet of $\mathfrak{A}$.

Let us show now that the composition of two normal algorithms is again a normal algorithm. Let $\mathfrak{A}$ and $\mathfrak{B}$ be normal algorithms in an alphabet A. For each symbol b in A, form a new symbol $\bar{b}$, called the correlate of b. Let $\bar{A}$ be the alphabet consisting of the correlates of the symbols of A. Let a and β be two symbols not in $A \cup \bar{A}$. Let $\mathfrak{S}_{\mathfrak{A}}$ be the schema of $\mathfrak{A}$. except that the terminal dot in terminal productions is replaced by a. Let $\mathfrak{S}_{\mathfrak{B}}$ be the schema of $\mathfrak{B}$. except that every symbol is replaced by its correlate, every terminal dot by β, productions of the form $A \to Q$ are replaced by $a \to \alpha Q$, and productions $A \to \cdot Q$ are

† In this and in all other definitions in this chapter, the existential quantifier "there is" is meant in the ordinary, "classical" sense. When we assert that there exists an object of a certain kind, we do not necessarily imply that any human being has found or ever will find such an object. Thus, a function φ may be partially Markov-computable without our ever knowing it to be so.

replaced by $\alpha \to \alpha\beta Q$. Consider the abbreviated schema

$$\begin{array}{ll}
a\alpha \to \alpha a & (a \text{ in A}) \\
\alpha a \to \alpha\bar{a} & (a \text{ in A}) \\
\bar{a}b \to \bar{a}\bar{b} & (a, b \text{ in A}) \\
\bar{a}\beta \to \beta\bar{a} & (a \text{ in A}) \\
\beta\bar{a} \to \beta a & (a \text{ in A}) \\
a\bar{b} \to ab & (a, b \text{ in A}) \\
\alpha\beta \to \cdot\Lambda & \\
\mathfrak{S}_{\mathfrak{B}} & \\
\mathfrak{S}_{\mathfrak{A}} &
\end{array}$$

This schema determines a normal algorithm $\mathfrak{C}$ over A such that $\mathfrak{C}(P) \approx \mathfrak{B}(\mathfrak{A}(P))$ for any word P in A. (Exercise.) $\mathfrak{C}$ is called the *composition* of $\mathfrak{A}$ and $\mathfrak{B}$, and is denoted $\mathfrak{B} \circ \mathfrak{A}$. In general, by $\mathfrak{A}_n \circ \ldots \circ \mathfrak{A}_1$, we mean $\mathfrak{A}_n \circ (\ldots \circ (\mathfrak{A}_3 \circ (\mathfrak{A}_2 \circ \mathfrak{A}_1)) \ldots)$.

Let $\mathfrak{D}$ be a normal algorithm in an alphabet A, and let B be an extension of A. If we take a schema for $\mathfrak{D}$ and prefix to it the productions $b \to b$ for each symbol b in B − A, then the new schema determines a normal algorithm $\mathfrak{D}_{\text{B}}$ in B such that $\mathfrak{D}_{\text{B}}(P) \approx \mathfrak{D}(P)$ for every word P in A, and $\mathfrak{D}_{\text{B}}$ is not applicable to any word in B containing any symbol of B − A. $\mathfrak{D}_{\text{B}}$ is fully equivalent to $\mathfrak{D}$ relative to A and is called the *propagation* of $\mathfrak{D}$ onto B.

Assume that $\mathfrak{A}$ is a normal algorithm in an alphabet A_1 and $\mathfrak{B}$ is a normal algorithm in an alphabet A_2. Let $\text{A} = \text{A}_1 \cup \text{A}_2$. Let $\mathfrak{A}_{\text{A}}$ and $\mathfrak{B}_{\text{A}}$ be the propagations of $\mathfrak{A}$ and $\mathfrak{B}$, respectively, onto A. Then the composition $\mathfrak{C}$ of $\mathfrak{A}_{\text{A}}$ and $\mathfrak{B}_{\text{A}}$ is called the *normal composition* of $\mathfrak{A}$ and $\mathfrak{B}$, and is denoted by $\mathfrak{B} \circ \mathfrak{A}$. (When $\text{A}_1 = \text{A}_2$, the normal composition of $\mathfrak{A}$ and $\mathfrak{B}$ is identical with the composition of $\mathfrak{A}$ and $\mathfrak{B}$; hence the notation $\mathfrak{B} \circ \mathfrak{A}$ is unambiguous.) $\mathfrak{C}$ is a normal algorithm over A such that $\mathfrak{C}(P) \approx \mathfrak{B}(\mathfrak{A}(P))$ for any word P in A_1, and $\mathfrak{C}$ is applicable only to those words P of A such that P is a word of A_1, $\mathfrak{A}$ is applicable to P, and $\mathfrak{B}$ is applicable to $\mathfrak{A}(P)$.

Let an alphabet B be an extension of an alphabet A. Given a word P in B, the *projection* P^{A} of P on A is the word obtained by erasing in P all symbols in B − A. The abbreviated schema $\xi \to \Lambda$ (ξ in B − A) determines the *projection algorithm* $\mathfrak{B}$ of B on A, i.e., $\mathfrak{B}(P) = P^{\text{A}}$ for all words P in B.

Let A and C be alphabets without any symbols in common, and let $\text{B} = \text{A} \cup \text{C}$. Then the abbreviated schema $ca \to ac$ (a in A; c in C) determines a normal algorithm $\mathfrak{L}_{\text{A, C}}$ in B such that, for any word P in B, $\mathfrak{L}_{\text{A, C}}(P) = P^{\text{A}}P^{\text{C}}$.

Given a normal algorithm $\mathfrak{A}$ in an alphabet A, and an extension B of A, then the *natural extension* $\mathfrak{B}$ of the algorithm $\mathfrak{A}$ to B is the normal algorithm in B

determined by the given schema for $\mathfrak{A}$. Clearly, $\mathfrak{B}(P) \approx \mathfrak{A}(P)$ for any word P in A, and, in addition, if P is a word in A and Q is a word in B − A, then $\mathfrak{B}(PQ) \approx \mathfrak{A}(P)Q$. Notice that the natural extension of $\mathfrak{A}$ to B generally is different from the propagation of $\mathfrak{A}$ onto B, since the latter is not applicable to any word containing symbols of B − A.

PROPOSITION 5.1. *Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ be normal algorithms, and let* A *be the union of their alphabets. Then there is a normal algorithm $\mathfrak{B}$ over* A, *called the* juxtaposition *of the algorithms $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ such that*

$$\mathfrak{B}(P) \approx \mathfrak{A}_1\#(P)\mathfrak{A}_2\#(P) \ldots \mathfrak{A}_k\#(P) \textit{ for any word } P \textit{ in } \text{A},$$

where $\mathfrak{A}_i\#$ is the natural extension of $\mathfrak{A}_i$ to A.

PROOF. By induction on k. Clearly, it suffices to prove the result for k = 2. For each symbol a in A, introduce a new symbol $\bar{a}$. Let $\overline{\text{A}}$ be the alphabet made up of these new symbols, and let $\text{B} = \text{A} \cup \overline{\text{A}}$. Let $\overline{\mathfrak{A}}_1$ be the normal algorithm in $\overline{\text{A}}$ corresponding to the algorithm $\mathfrak{A}_1\#$ in A. (The schema for $\overline{\mathfrak{A}}_1$ is obtained from that for $\mathfrak{A}_1$ by replacing each symbol a by $\bar{a}$.) Let $\overline{\mathfrak{A}}_1\#$ and $\mathfrak{A}_2\#$ be the natural extensions, respectively, of $\overline{\mathfrak{A}}_1$ and $\mathfrak{A}_2$ to B. Let $\text{A} = \{a_1, \ldots, a_n\}$. By Exercise 5.3 (p. 225), there exist normal algorithms $\mathfrak{W}_1 = \text{Sub}^{a_1, a_2, \ldots, a_n}_{a_1\bar{a}_1, a_2\bar{a}_2, \ldots, a_n\bar{a}_n}$ and $\mathfrak{W}_2 = \text{Sub}^{\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n}_{a_1, a_2, \ldots, a_n}$ over B such that $\mathfrak{W}_1$ simultaneously substitutes $a_1\bar{a}_1$ for a_1, $a_2\bar{a}_2$ for $a_2, \ldots,$ and $\mathfrak{W}_2$ substitutes a_1 for $\bar{a}_1$, a_2 for $\bar{a}_2$,. . . . We also have normal algorithms $\mathfrak{L}_{\text{A}, \overline{\text{A}}}$ and $\mathfrak{L}_{\overline{\text{A}}, \text{A}}$ such that $\mathfrak{L}_{\text{A}, \overline{\text{A}}}(P) = P^{\text{A}}P^{\overline{\text{A}}}$ and $\mathfrak{L}_{\overline{\text{A}}, \text{A}}(P) = \text{P}^{\overline{\text{A}}}P^{\text{A}}$. Then, take the normal composition $\mathfrak{B} = \mathfrak{W}_2 \circ \overline{\mathfrak{A}}_1\# \circ \mathfrak{L}_{\overline{\text{A}}, \text{A}} \circ \mathfrak{A}_2\# \circ \mathfrak{L}_{\text{A}, \overline{\text{A}}} \circ \mathfrak{W}_1$. It is easy to verify that $\mathfrak{B}(P) \approx \mathfrak{A}_1\#(P)\mathfrak{A}_2\#(P)$ for any word P in A.

COROLLARY 5.2. *Let $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ be normal algorithms; let* A *be the union of their alphabets. Then there is a normal algorithm $\mathfrak{B}$ over* $\text{A} \cup \{ * \}$ *such that $\mathfrak{B}(P) \approx \mathfrak{A}_1\#(P) * \mathfrak{A}_2\#(P) * \ldots * \mathfrak{A}_k\#(P)$ for any word P in* A, *where $\mathfrak{A}_i\#$ is the natural extension of $\mathfrak{A}_i$ to* A. *(Hence, $\mathfrak{B}(P) \approx \mathfrak{A}_1(P) * \mathfrak{A}_2(P) * \ldots * \mathfrak{A}_k(P)$ for any word P common to the alphabets of all the $\mathfrak{A}_i$'s.)*

PROOF. There is a normal algorithm $\mathfrak{D}$ in $\text{A} \cup \{ * \}$ such that $\mathfrak{D}(P) = *$ for any word P in $\text{A} \cup \{ * \}$. Take as its defining schema

$$\begin{array}{ll}
a \to \Lambda & (a \text{ in A}) \cdot \\
\Lambda \to \cdot * &
\end{array}$$

Let $\mathfrak{B}$ be the juxtaposition of $\mathfrak{A}_1, \mathfrak{D}, \mathfrak{A}_2, \mathfrak{D}, \ldots, \mathfrak{D}, \mathfrak{A}_k$, as in Proposition 5.1. Then $\mathfrak{B}(P) \approx \mathfrak{A}_1\#(P) * \mathfrak{A}_2\#(P) * \ldots * \mathfrak{A}_k\#(P)$ for any word P in $\text{A} \cup \{ * \}$ (and $\mathfrak{B}(P) \approx \mathfrak{A}_1(P) * \mathfrak{A}_2(P) * \ldots * \mathfrak{A}_k(P)$ for any word P in the intersection of the alphabets of the $\mathfrak{A}_i$'s).

LEMMA 5.3

(1) *Let $\mathfrak{C}$ be a normal algorithm in an alphabet A and let a be any symbol. Then there is a normal algorithm* 6 *over A U { a) such that*

$$\mathfrak{D}(P) = \begin{cases} \alpha P & \textit{if } P \textit{ is a word in } A \textit{ such that } \mathfrak{C}(P) = A \\ P & \textit{if } P \textit{ is a word in } \mathrm{A} \textit{ such that } \mathfrak{C}(P) \neq A \end{cases}$$

and 6 *applies only to those words to which* (5 *applies.*

(2) If 1 *and $\mathfrak{B}$ are normal algorithms in an alphabet A and a is a symbol not in A, then there is a normal algorithm $\mathfrak{G}$ over $A \cup$ { a) such that*

$$\begin{aligned} \mathfrak{G}(\mathrm{P}) \approx \mathfrak{A}(\mathbf{P}) & \quad \text{if } P \text{ is a word in } A, \text{ and} \\ \mathfrak{G}(\alpha \mathrm{P}) \approx \mathfrak{B}(\mathrm{P}) & \quad \text{if } P \text{ is a word in } A. \end{aligned}$$

PROOF.

(1) There is a normal algorithm $\mathfrak{H}_1$ over A U { a) taking A into a and any other word of A U { a) into A. Let β be any symbol not in A U { a). Consider the abbreviated schema for $\mathfrak{H}_1$

$$\begin{array}{ll} a \to \beta & (a \text{ in } \mathrm{A}\ U\ \{ a)) \\ \beta\beta \to \beta & \\ \beta \to \cdot\Lambda & \\ \Lambda \to \cdot\alpha & \end{array}$$

Let $\mathfrak{H}_2 = \mathfrak{H}_1 \circ \mathfrak{C}$. For any word P in A, if $\mathfrak{C}(P) = A$, then $\mathfrak{H}_2(P) = a$ and if $\mathfrak{C}(P) \neq A$, then $\mathfrak{H}_2(P) = A$. Let $\mathfrak{J}$ be the identity algorithm in A (with the schema A → . A). Let $\mathfrak{D}$ be the juxtaposition of $\mathfrak{H}_2$ and $\mathfrak{J}$. If $\mathfrak{C}(P) = A$, then $\mathfrak{D}(P) = \alpha P$, and, if $\mathfrak{C}(P) \neq$ A, then $\mathfrak{D}(P) = P$.

(2) For each,symbol a of A, let $\bar{a}$ be a new symbol, and let $\bar{\mathrm{A}}$ be the alphabet consisting of these $\bar{a}$'s. Let B = $A \cup \bar{\mathrm{A}}$ U { a , β }, where β is not in A u $\bar{\mathrm{A}}$ u { a }. If we replace in the schema of algorithm $\mathfrak{B}$. all symbols a by the corresponding symbols a, all terminal dots by β, every production $A \to Q$ by $\alpha \to \alpha Q$, and every production $A \to .\, Q$ by $a \to \alpha\beta Q$, we obtain a new algorithm schema $\mathfrak{S}_{\mathfrak{B}}$. Let $\mathfrak{S}_{\mathfrak{A}}$. be the schema for 1 · . Form the schema

$$\begin{array}{ll} aa \to \alpha\bar{a} & (a \text{ in } A) \\ \bar{a}b \to \text{a6} & (a, b \text{ in } A) \\ \bar{a}\beta \to \beta\bar{a} & (a \text{ in } A) \\ \beta\bar{a} \to \beta a & (a \text{ in } A) \\ a\bar{b} \to ab & (a, b \text{ in } A) \\ \alpha\beta \to \cdot\Lambda & \\ \mathfrak{S}_{\mathfrak{B}} & \\ \mathfrak{S}_{\mathfrak{A}}. & \end{array}$$

This determines a normal algorithm $\mathfrak{G}$ over A U { a) such that $\mathfrak{G}(P) \approx \mathfrak{A}(P)$ and $\mathfrak{G}(\alpha P) \approx \mathfrak{B}(P)$ if P is a word in A.

PROPOSITION 5.4. *Let $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ be normal algorithms and A the union of their alphabets. Then there is a normal algorithm $\mathfrak{E}$ over A such that*

$$\mathfrak{E}(P) \quad \begin{cases} \mathfrak{B}(P) & \textit{if } P \textit{ is a word in } A \textit{ and } \quad \mathfrak{C}(P) = A \\ \mathfrak{A}(P) & \textit{if } P \textit{ is a word in } A \textit{ and } \quad \mathfrak{C}(P) \neq A \end{cases}$$

and $\mathfrak{E}$ applies only to those words in A to which $\mathfrak{C}$ is applicable. The algorithm $\mathfrak{E}$ is called the ramification *of* 1 *and $\mathfrak{B}$ governed by 0:.*

PROOF. Let $\mathfrak{A}_1$, $\mathfrak{B}_1$, $\mathfrak{C}_1$ be the propagations of $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ to A. Let a be a symbol not in A. By Lemma 5.3(1), there is a normal algorithm 6 over $A \cup$ { a) such that

$$\mathfrak{D}(P) = \begin{cases} \alpha P & \text{if } P \text{ is a word in } \mathbf{A} \text{ and } \mathfrak{C}(P) = \Lambda \\ P & \text{if } P \text{ is a word in } A \text{ and } \mathfrak{C}(P) \neq A \end{cases}$$

By Lemma 5.3(2), there is a normal algorithm $\mathfrak{G}$ over A u { a) such that $\mathfrak{G}(P) \approx \mathfrak{A}_1(P)$, and $\mathfrak{G}(\alpha P) \approx \mathfrak{B}_1(P)$ if P is a word in A. Let $\mathfrak{E} = \mathfrak{G} \circ \mathfrak{D}$.

Suppose that $\mathfrak{A}$ and $\mathfrak{C}$ are algorithms in an alphabet A and that P_0 is a word in A. First, apply $\mathfrak{A}$ to P_0, and, if a word P_1 results, apply $\mathfrak{C}$ to P_1. If $\mathfrak{C}(P_1) = A$, stop; if $\mathfrak{C}(P_1) \neq A$, apply 1 to P_1. If a word P_2 results, test P_2 by $\mathfrak{C}$: if $\mathfrak{C}(P_2) = A$, stop; if $\mathfrak{C}(P_2) \neq A$, apply $\mathfrak{A}$ to P_2, and so on. The algorithm $\mathfrak{B}$ defined in this way is called the *iteration* of $\mathfrak{A}$ governed by 0:. Clearly, $\mathfrak{B}(P_0) = Q$ when and only when there is a sequence of words $P_0, P_1, \ldots, P_n$ $(n > 0)$ such that $P_n = Q$, $\mathfrak{C}(P_n) = A$, $P_i = \mathfrak{A}(P_{i-1})$ if $0 < \mathrm{i} \leq n$, and $\mathfrak{C}(P_i) \neq A$ if $0 < \mathrm{i} < \mathrm{n}$.

PROPOSITION 5.5. *Let* 1 *and $\mathfrak{C}$ be normal algorithms, A the union of their alphabets, and $\mathfrak{A}_1$ and $\mathfrak{C}_1$ the propagations of* 1 *and $\mathfrak{C}$ to A. Then the iteration of $\mathfrak{A}_1$ governed by $\mathfrak{C}_1$ is a normal algorithm over A.*

PROOF. It clearly suffices to prove the result when 1 and 0: have the same alphabet A, in which case 1 , = 1 and $\mathfrak{C}_1 = \mathfrak{C}$. Let a be a symbol not in A. By Lemma 5.3(1), there is a normal algorithm $\mathfrak{D}$ over B = $A \cup$ { a) such that

$$\mathfrak{D}(P) = \begin{cases} \alpha P & \text{if } P \text{ is a word in } A \text{ such that } \quad \mathfrak{C}(P) = A \\ P & \text{if } P \text{ is a word in } \mathbf{A} \text{ such that } \quad \mathfrak{C}(P) \neq A \end{cases}$$

Let $\mathfrak{F}$ = 6 ∘ 1. $\mathfrak{F}$ is a normal algorithm in an extension F of B. Let β be a symbol not in the alphabet F. Consider the following schema.

$$\begin{array}{ll} \xi\beta \to \beta\xi & (\xi \text{ in F}) \\ \beta\alpha \to \cdot\Lambda & \\ \beta \to \Lambda & \\ \mathfrak{S}_{\mathfrak{F}^\beta} & \end{array}$$

where $\mathfrak{S}_{\mathfrak{F}^\beta}$ is a schema for 3 . in which all terminal dots are replaced by β. The normal algorithm $\mathfrak{G}$ defined by this schema is the desired normal algorithm.

COROLLARY 5.6. ***Let $\mathfrak{A}$ and (5 be normal algorithms and*** A ***the union of their alphabets. Then there is a normal algorithm $\mathfrak{H}$ over*** A ***such that, for any word P_0 in*** A, $\mathfrak{H}(P_0) = Q$ if ***and only if there is a sequence $P_0, \ldots, P_n$*** (n $\geqslant$ 0) ***such that P_n*** = Q, $\mathfrak{C}(P_n)$ = A, $P_{i+1} = \mathfrak{A}(P_i)$ ***and*** $\mathfrak{C}(P_i) \neq$ A ***for $0 \leqslant i < n$.***

PROOF. Let $\mathfrak{J}$ be the identity algorithm and 23 the iteration of $\mathfrak{A}$ governed by (5. Take $\mathfrak{H}$ to be the ramification of 23 and $\mathfrak{J}$ governed by (5 (cf. Proposition 5.4). This algorithm $\mathfrak{H}$ is called the ***full iteration*** of $\mathfrak{A}$ governed by (5.

PROPOSITION 5.7. ***Let $\mathfrak{A}$ be a normal algorithm in an alphabet*** A. ***Then there is a normal algorithm $\mathfrak{A}^I$ over the alphabet*** B = A $\cup$ M ***(where*** M = ($*$, 1}) ***such that, for any word P_0 in*** A ***and any natural number*** n, $\mathfrak{A}^I(\bar{n} * P_0) = Q$ ***if and only if there is a sequence $P_0, \ldots, P_n$*** (n $\geqslant$ 0) ***with P_n*** = Q ***and $P_i = \mathfrak{A}(P_{i-1})$ for $0 < i \leqslant n$.***

PROOF. Let a be a symbol not in B, and let C = B u (a}. Consider the normal algorithms in C given by the following schemas.

$$\mathfrak{H}_1 : \left|\begin{array}{l} a11 \rightarrow \cdot 1 \\ \alpha 1 * \rightarrow \alpha\, * \\ \alpha * \xi \rightarrow a* \qquad (\xi \text{ in B}) \\ a* \rightarrow \cdot \Lambda \\ \Lambda \rightarrow \alpha \end{array}\right.$$

Clearly, $\mathfrak{H}_1(\bar{0} * P) = A$ and $\mathfrak{H}_1(\bar{n} * P) \neq A$, for n > 0, where P is any word in B.

$$\mathfrak{H}_2 : \begin{cases} *\xi \rightarrow * & (\xi \text{ in B}) \\ * \rightarrow \Lambda \end{cases}$$

If P does not contain $*$, then $\mathfrak{H}_2(P * Q) = P$.

$$\mathfrak{H}_3 : \quad \begin{cases} \alpha 1 \rightarrow \alpha \\ \alpha * \rightarrow \cdot \Lambda \\ \Lambda \rightarrow \alpha \end{cases}$$

Then $\mathfrak{H}_3(\bar{n} * P) = P$.

$$\mathfrak{H}_4 : \quad 1 \rightarrow \cdot \Lambda$$
$$\mathfrak{H}_5 : \quad 1* \rightarrow \cdot \Lambda$$

Clearly, $\mathfrak{H}_4(\bar{n} * P) = \overline{(n-1)} * P$ if n > 0, and $\mathfrak{H}_4(\bar{0} * P) = * P$. Also, $\mathfrak{H}_5(\bar{0} * P) = P$.

Let $\mathfrak{E}$ be the normal algorithm given by Corollary 5.2 such that $\mathfrak{E}(P) = (\mathfrak{H}_2 \circ \mathfrak{H}_4)(P) * (\mathfrak{A} \circ \mathfrak{H}_3)(P)$ for any word P in C. For any word P in A,

$$\mathfrak{E}(\bar{n} * P) = \left(\begin{array}{ll} \overline{n-1} * \mathfrak{A}(P) & \text{if n is a positive integer} \\ \overline{* \mathfrak{A}(P)} \text{ if } n = 0 \end{array} \right.$$

Let E be the alphabet of $\mathfrak{E}$. By Corollary 5.6, let $\mathfrak{F}$ be a normal algorithm over E such that $\mathfrak{F}(P_0) = Q$ if and only if there is a sequence $P_0, \ldots, P_k$ (k $\geqslant$ 0) with $P_k = Q$, $\mathfrak{H}_1(P_k) = A$, $P_i = \mathfrak{E}(P_{i-1})$ for $0 < i \leqslant k$, and $\mathfrak{H}_1(P_i) \neq \Lambda$ for $0 \leqslant i < k$. Now let $\mathfrak{A}^1 = \mathfrak{H}_5 \circ \mathfrak{F}$. We leave as an exercise the verification that this is the required normal algorithm.

PROPOSITION 5.8. ***Every partial recursive function is partially Markov-computable, and every recursive function is Markov-computable.***

PROOF.

(1) The initial functions Z, N, I_j^k ($1 \leqslant j \leqslant k$) are Markov-computable (cf. Exercise 5.4, pp. 225–226).

(2) Substitution. Assume that ψ arises from $\tau, \varphi_1, \ldots, \varphi_k$ by substitution: $\psi(x_1, \ldots, x_n) = \tau(\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_k(x_1, \ldots, x_n))$, where $\tau, \varphi_1, \ldots, \varphi_k$ are partial recursive. Suppose that there are normal algorithms $\mathfrak{A}_\tau, \mathfrak{A}_{\varphi_1}, \ldots, \mathfrak{A}_{\varphi_k}$ over M = {1, $*$ } which partially compute the functions $\tau, \varphi_1, \ldots, \varphi_k$. By Corollary 5.2, there is an algorithm 23 over M such that $\mathfrak{B}(P) \approx \mathfrak{A}_{\varphi_1}(P) * \mathfrak{A}_{\varphi_2}(P) * \ldots * \mathfrak{A}_{\varphi_k}(P)$ for any word P in M. In particular,

$$\mathfrak{B}(\overline{(x_1, \ldots, x_n)}) \approx \overline{\varphi_1(x_1, \ldots, x_n)} * \overline{\varphi_2(x_1, \ldots, x_n)} * \ldots * \overline{\varphi_k(x_1, \ldots, x_n)}$$

for any natural numbers x,, . . . , x_n. Now, let $\mathfrak{C} = \mathfrak{A}_\tau \circ$ 23. Then

$$\mathfrak{C}(\overline{(x_1, \ldots, x_n)}) \approx \mathfrak{A}_\tau(\overline{\varphi_1(x_1, \ldots, x_n)} * \ldots * \overline{\varphi_k(x_1, \ldots, x_n)})$$
$$\approx \overline{\tau(\varphi_1(x_1, \ldots, x_n), \ldots, \varphi_k(x_1, \ldots, x_n))}$$

for any natural numbers x,, . . . , x_n.

(3) Recursion. Assume that ψ arises from 7 and φ by recursion:

$$\psi(x_1, \ldots, x_k, 0) = \tau(x_1, \ldots, x_k)$$
$$\psi(x_1, \ldots, x_k, y+1) = \varphi(x_1, \ldots, x_k, y, \psi(x_1, \ldots, x_k, y))$$

Suppose that 7 and φ are partial recursive and that $\mathfrak{A}_\tau$ and $\mathfrak{A}_\varphi$ are normal algorithms over M which partially compute τ and φ. Let $\mathfrak{A}_Z$ be the normal algorithm computing the zero function, $\mathfrak{A}_N$ the normal algorithm computing the successor function, and let $\mathfrak{A}_j^k$ be the normal algorithm computing the projection function U_j^k. By Corollary 5.2, using the algorithms $\mathfrak{A}_i^{k+1}$, there is a normal algorithm 23, over M such that $\mathfrak{B}_1(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y}) = \bar{x}_1 * \ldots * \bar{x}_k$. Let $\mathfrak{K} = \mathfrak{A}_\tau \circ \mathfrak{B}_1$. Again by Corollary 5.2, applied to $\mathfrak{A}_{k+1}^{k+1}, \mathfrak{A}_1^{k+1}, \ldots, \mathfrak{A}_k^{k+1}, \mathfrak{A}_Z, \mathfrak{K}$, there is a normal algorithm 23, over M such that $\mathfrak{B}_2(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y}) \approx \bar{y} * \bar{x}_1 * \ldots * \bar{x}_k * 0 * \overline{\tau(x_1, \ldots, x_k)}$. Let $\mathfrak{B}_3 = \mathfrak{A}_N \circ \mathfrak{A}_{k+1}^{k+2}$. Thus, $\mathfrak{B}_3(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y} * \bar{x}) = y + 1$. By Corollary 5.2, applied to $\mathfrak{A}_1^{k+2}, \ldots, \mathfrak{A}_k^{k+2}, \mathfrak{B}_3, \mathfrak{A}_\varphi$, we obtain the juxtaposition algorithm $\mathfrak{B}_4$ over M such that

$$\mathfrak{B}_4(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y} * \bar{z}) \approx \bar{x}_1 * \ldots * \bar{x}_k * \overline{y+1} * \overline{\varphi(x_1, \ldots, x_k, y, z)}$$

By Proposition 5.7, there is a normal algorithm $\mathfrak{B}_4^{I}$ such that, if n $\geqslant$ 0, $\mathfrak{B}_4^{I}(\bar{n} * P_0)$ = Q when and only when there is a sequence $P_0, \ldots,$ P„ such that Q = P_n and $P_i = \mathfrak{B}_4(P_{i-1})$ for $0 < i \leqslant n$. Then $\mathfrak{B} = \mathfrak{A}_{k+2}^{k+2} \circ \mathfrak{B}_4^{I} \circ \mathfrak{B}_2$ is a normal algorithm over M computing I). Notice that

$$\mathfrak{B}_2(\bar{x}_1 * \ldots * \bar{x}_k * \bar{y}) \approx \bar{y} * \bar{x}_1 * \ldots * \bar{x}_k * \bar{0} * \overline{\tau(x_1, \ldots, x_k)}$$

If we then apply $\mathfrak{B}_4^{I}$, this produces a y-fold iteration of $\mathfrak{B}_4$ starting with $\bar{x}_1 * \ldots * \bar{x}_k * \bar{0} * \overline{\tau(x_1, \ldots, x_k)}$. It is easy to see that the result is then $\bar{x}_1 * \ldots * \bar{x}_k * \bar{y} * \overline{\psi(x_1, \ldots, x_k, y)}$. Then, applying $\mathfrak{A}_{k+2}^{k+2}$, we obtain $\overline{\psi(x_1, \ldots, x_k, y)}$.

(4) p-operator. Suppose that $\psi(x_1, \ldots, x_n) = \mu y(\varphi(x_1, \ldots, x_n, y) = 0)$ and assume that φ is partially computable by a normal algorithm $\mathfrak{A}_\varphi$ over M. By Corollary 5.2, applied to the algorithms $\mathfrak{A}_1^{n+1}, \ldots, \mathfrak{A}_n^{n+1}$, $\mathfrak{A}_N \circ \mathfrak{A}_{n+1}^{n+1}$, there is a normal algorithm $\mathfrak{W}$ such that $\mathfrak{W}(\bar{x}_1 * \ldots * \bar{x}_n * \bar{y}) = \bar{x}_1 * \ldots * \bar{x}_n * \overline{y+1}$. Let $\mathfrak{S}$ be the normal algorithm over M given by the schema

$$\begin{aligned} 11 &\rightarrow \cdot 11 \\ 1 &\rightarrow \Lambda \end{aligned}$$

Then $\mathfrak{D}(\bar{n}) = \Lambda$ if n = 0 and $\mathfrak{D}(\bar{n}) \neq \Lambda$ if n > 0. Let O = $\mathfrak{S} \circ \mathfrak{U}_\varphi$. Then

$$\mathfrak{C}(\bar{x}_1 * \ldots * \bar{x}_n * \bar{y}) \begin{cases} = \Lambda & \text{if } \varphi(x_1, \ldots, x_n, y) = 0 \\ \neq \Lambda & \text{if } \varphi(x_1, \ldots, x_n, y) \neq 0 \end{cases}$$

Let $\mathfrak{K}$ be a normal algorithm over M such that

$$\mathfrak{K}(\bar{x}_1 * \ldots * \bar{x}_n) = \bar{x}_1 * \ldots * \bar{x}_n * \bar{0}$$

By Corollary 5.6, applied to $\mathfrak{W}$ and 0, there is a normal algorithm $\mathfrak{H}$ over M such that $\mathfrak{H}(P_0)$ = Q if and only if there is a sequence $P_0, \ldots,$ P„ (n $\geqslant$ 0) such that P„ = Q, $\mathfrak{C}(P_n) = \Lambda$, $P_{i+1} = \mathfrak{W}(P_i)$ and $\mathfrak{C}(P_i) \neq \Lambda$ for $0 \leqslant i < n$. Let $\mathfrak{B} = \mathfrak{A}_{n+1}^{n+1} \circ \mathfrak{H} \circ \mathfrak{K}$. Then

$$\mathfrak{B}(\bar{x}_1 * \ldots * \bar{x}_n) \approx \overline{\mu y(\varphi(x_1, \ldots, x_n, y) = 0)} \approx \overline{\psi(x_1, \ldots, x_n)}$$

From Parts (1)–(4), if ψ is a partial recursive function of k arguments, there is a normal algorithm $\mathfrak{A}_\psi$ over M such that

$$\mathfrak{A}_\psi(\bar{x}_1, * \ldots * \bar{x}_k) \approx \overline{\psi(x_1, \ldots, x_k)}$$

Let $\mathfrak{R}$ be a normal algorithm over M such that $\mathfrak{R}$ is defined only for words of M of the form $\bar{x}_1 * \ldots * \bar{x}_k$, where x,, . . . , x_k are natural numbers, and $\mathfrak{R}(\bar{x}_1 * \ldots * \bar{x}_k) = \bar{x}_1 * \ldots * \bar{x}_k$. (We leave the construction of a schema for $\mathfrak{R}$ as an exercise.) Take $\mathfrak{E}_\psi = \mathfrak{A}_\psi \circ$ W. Then $\mathfrak{E}_\psi(\bar{x}_1 * \ldots * \bar{x}_k) \approx \overline{\psi(x_1, \ldots, x_k)}$ and $\mathfrak{E}_\psi$ is defined only for those words of M of the form $\bar{x}_1 * \ldots * \bar{x}_k$ such that $\psi(x_1, \ldots, x_k)$ is defined. Hence, every partial recursive function is partially Markov-computable. Every recursive function is, a fortiori, partially Markov-computable, and, since it is total, it is Markov-computable.

We shall now assign Gödel numbers to the symbols S_0, S,, S„ . . . out of which alphabets are constructed: $g(S_i) = 2i + 3$. Then, to any word P = $S_{j_0} \ldots S_{j_k}$ we assign the number

$$g(P) = 2^{g(S_{j_0})} 3^{g(S_{j_1})} \ldots p_k^{g(S_{j_k})} = 2^{2j_0+3} 3^{2j_1+3} \ldots p_k^{2j_k+3}$$

where p_k is the k^th prime number; we define $g(\Lambda) = 1$. To a sequence of words $P_0, \ldots, P_k$, we assign the number $2^{g(P_0)} 3^{g(P_1)} \ldots p_k^{g(P_k)}$.

We make the convention that S, is abbreviated by 1, and S_2 by * . Considering the numerals as words, we have $g(\bar{0}) = 2^5$; $g(\bar{1}) = 2^5 \cdot 3^5$, and, in general, $g(\bar{n}) = \prod_{i=0}^{n} p_i^5$.

There are normal algorithms $\mathfrak{T}_1$, $\mathfrak{T}_2$ over A ∪ M such that $\mathfrak{T}_1(P) = \overline{g(P)}$ for any word P in the alphabet A, and $\mathfrak{T}_2(\overline{g(P)}) = P$ for any word P in A. First, there is a normal algorithm $\mathfrak{B}_1$ over A u M such that, for any non-empty word $P = a_{m_0} a_{m_1} \ldots a_{m_r}$ of A,

$$\mathfrak{B}_1(P) = \overline{g(a_{m_0})} * \overline{g(a_{m_1})} * \ldots * \overline{g(a_{m_r})} * \text{ and } \mathfrak{B}_1(a_{m_0}) = \overline{g(a_{m_0})} *$$

If A = $\{S_{j_0}, \ldots, S_{j_k}\}$, then the schema for $\mathfrak{B}_1$ is

$$\begin{aligned} \alpha S_{j_0} &\rightarrow \overline{2j_0 + 3} * \alpha \\ \alpha S_{j_1} &\rightarrow \overline{2j_1 + 3} * \alpha \\ &\vdots \\ \alpha S_{j_k} &\rightarrow \overline{2j_k + 3} * \alpha \\ \alpha &\rightarrow \cdot \Lambda \\ \Lambda &\rightarrow \alpha \end{aligned}$$

Second, there is a normal algorithm $\mathfrak{B}_2$ such that $\mathfrak{B}_2(\bar{n} * Q) = \bar{0} * \overline{2^n} * Q$. (Exercise. Note that the function 2^x is recursive; so, by Proposition 5.8, there is a normal algorithm computing it.) Let $\mathfrak{B}_3 = \mathfrak{B}_2 \circ \mathfrak{B}_1$. Then, for any non-empty word P = $S_{m_0} \ldots S_{m_r}$,

$$\mathfrak{B}_3(P) = \bar{0} * \overline{{}_2 g(S_{m_0})} * \overline{g(S_{m_1})} * \ldots * \overline{g(S_{m_r})} *$$

Let $\mathfrak{A}$ be a normal algorithm such that

$$\mathfrak{A}(\bar{n} * \bar{u} * \bar{v} * Q) = \overline{n+1} * \overline{u \cdot (p_{n+1})^v} * Q$$

(Exercise. Notice that the function $f(x, y, n) = x \,.\, (p_{n+1})^y$ is recursive and hence computable by a normal algorithm.) Let O be a normal algorithm such that $\mathfrak{C}(P) = \Lambda$ when and only when P contains exactly two occurrences of * . Using Corollary 5.6, let $\mathfrak{H}$ be the full iteration of $\mathfrak{A}$ governed by $\mathfrak{C}$; let $\mathfrak{E}$ be a normal algorithm such that O(R * $\bar{y}$ *) = $\bar{y}$, and let 5 = $\mathfrak{E} \circ \mathfrak{H} \circ \mathfrak{B}_3$. Then, for any non-empty word P of A, $\mathfrak{F}(P) = \overline{g(P)}$. Hence, if we use Proposition 5.4 to take care of the case P = A, there is a normal algorithm $\mathfrak{T}_1$ over A ∪ M such that $\mathfrak{T}_1(P) = \overline{g(P)}$ for any word P in A. (Remember that $g(\Lambda) = 1$.)

EXERCISES

5.5. Prove that there is a normal algorithm $\mathfrak{T}_2$ over A u M such that $\mathfrak{T}_2(\overline{g(P)}) = P$ for any word P in A.

Hint: construct a normal algorithm $\mathfrak{D}$ such that $\mathfrak{D}(\overline{2i+3}) = S_i$ for each symbol S_i of A, but $\mathfrak{D}$ is not defined for any other words. Construct a normal algorithm $\mathfrak{K}$ such that $\mathfrak{K}(\bar{u}) = 6 * \bar{u} *$, for any positive integer u but $\mathfrak{K}$ is not defined for any other words. Construct a normal algorithm 5 such that

$$\mathfrak{F}(\bar{n} * \bar{u} * P) = \overline{n+1} * \overline{Qt(p_n^{(u)_n}, u)} * P\mathfrak{D}(\overline{(u)_n})$$

for any non-negative integers n, u and any word P. Let $\mathfrak{C}$ be a normal algorithm such that $\mathfrak{C}(\bar{n} * \bar{I} * P) = A$ for any non-negative integer n and word P, and 4 is defined but not equal to A for words not of the form $\bar{n} * \bar{I} * P$. By Proposition 5.5, let $\mathfrak{R}$ be the normal algorithm which is the iteration of 5 governed by 4. Let $\mathfrak{G}$ be a normal algorithm such that $\mathfrak{G}(\bar{n} * \bar{I} * P) = P$ for any non-negative integer n and any word P of A. Let $\mathfrak{L} = \mathfrak{G} \circ \mathfrak{R} \circ \mathfrak{K}$. Then $\mathfrak{L}(\overline{g(Q)}) = Q$ for any non-empty word Q of A. Use Proposition 5.4 to take care of the empty word.

Let $\mathfrak{A}$ be any algorithm (not necessarily normal) over an alphabet A. We can associate with $\mathfrak{A}$ a partial function $\psi_{\mathfrak{A}}$ such that $\psi_{\mathfrak{A}}(n) = m$ if and only if either n is not the Gödel number of a word of A and $m = 0$ or n and m are Gödel numbers of words P and Q of A such that $\mathfrak{A}(P) = Q$. Suppose that $\psi_{\mathfrak{A}}$ is partial recursive. (We then call 8 a ***recursiue algorithm.)*** By Proposition 5.8, there is a normal algorithm $\mathfrak{B}$ over M such that $\mathfrak{B}(\bar{n}) \approx \overline{\psi_{\mathfrak{A}}(n)}$ for any natural number n and $\mathfrak{B}$ is defined only for those ii for which $\psi_{\mathfrak{A}}(n)$ is defined. Let $\mathfrak{A}'$ be the normal algorithm $\mathfrak{T}_2 \circ \mathfrak{B} \circ \mathfrak{T}_1$. Then $\mathfrak{A}'$ is a normal algorithm over A which is fully equivalent to $\mathfrak{I}$ relative to A. Thus:

Proposition 5.9. ***If $\mathfrak{A}$ is any algorithm over A, and $\psi_{\mathfrak{A}}$ is partial recursive, then $\mathfrak{A}$ is fully equivalent relative to*** A ***to some normal algorithm over A.***

Proposition 5.10. ***If $\mathfrak{A}$ is a normal algorithm over*** A, ***then $\psi_{\mathfrak{A}}$ is partial recursiue, and, if I is applicable to all words in A, $\psi_{\mathfrak{A}}$ is recursiue.***

PROOF. Given a simple production $P \to Q$, we call $2^1 3^{g(P)} 5^{g(Q)}$ its index; given a terminal production $P \to \cdot Q$, we let $2^2 3^{g(P)} 5^{g(Q)}$ be its index. If $P_0 \to (\cdot)Q_0, \ldots, P_r \to (\cdot)Q_r$ is an algorithm schema, we let its ***index*** be the number $2^{k_0} 3^{k_1} \ldots p_r^{k_r}$, where k_i is the index of $P_i \to (\cdot)Q_i$. Let Word (u) be the recursive predicate which holds if and only if u is the Gödel number of a word: $u = 1 \vee (z)(z < lh(u) \supset (Ey)(y < u \wedge (u)_z = 2y + 3))$. Let SI(u) be the recursive predicate which holds if and only if u is the index of a simple production: $lh(u) = 3$ A $(u)_0 = 1$ A $Word((u)_1) \wedge Word((u)_2)$. Similarly, let TI(u) be the recursive predicate which holds if and only if u is the index of a terminal production: $lh(u) = 3 \wedge (u)_0 = 2 \wedge Word((u)_1) \wedge Word((u)_2)$. Let Ind(u) be the recursive predicate which holds if and only if u is the index of an algorithm schema: $u > 1 \wedge (z)(z < lh(u) \supset SI((u)_z) \vee TI((u)_z))$. Let $x \square y$ stand for the recursive function which we denoted $x * y$ on p. 144(4). Then, if $x = \prod_{i=0}^{n} p_i^{\alpha_i}$

and each $\alpha_i > 0$, and $y = \prod_{i=0}^{m} p_i^{\beta_i}$, $x \square y = \prod_{i=0}^{n} p_i^{\alpha_i} \cdot \prod_{i=0}^{m} p_{i+n+1}^{\beta_i}$. In addition, $x \square 1 = 1 \square x = x$.

$\square$ corresponds to the juxtaposition operation on words. Let Lsub(x, y, e) be the recursive predicate which holds if and only if e is the index of a production $P \to (\cdot)Q$ and x and y are Gödel numbers of words U and V such that P occurs in U, and V is the result of substituting Q for the left-most occurrence of P in U: $Word(x)$ A $Word(y)$ A $(SI(e) \vee TI(e))$ A $(Eu)_{u \leqslant x}(Ev)_{v \leqslant x}(x = u \square (e)_1 \square v$ A $y = u \square (e)_2 \square v \wedge \sim (Ew)_{w \leqslant x} (Ez)_{z \leqslant x} (x = w \square (e)_1 \square z \wedge w < u))$. Let Occ(x, y) be the recursive predicate which holds if and only if x and y are Gödel numbers of words U and V, and V occurs in U: $Word(x) \wedge Word(y) \wedge (Ev)_{v \leqslant x}(Ez)_{z \leqslant x}(x = v \square y \square z)$. Let End(e, z) be the recursive predicate holding if and only if z is the Gödel number of a word P, e is the index of an algorithm schema, and any algorithm $\mathfrak{A}$ defined by this schema cannot be applied to P (i.e., $8: P\square$): $Ind(e)$ A $Word(z)$ A $(w)_{w < lh(e)}(\sim Occ(z, ((e)_w)_1))$. Let SCons (e, y, x) be the recursive predicate which holds if and only if e is the index of an algorithm schema and y and x are Gödel numbers of words V and U such that V arises from U by a simple production of the schema:

$$Ind(e) \wedge Word(x) \wedge Word(y) \wedge (Ev)_{v < lh(e)}(SI((e)_v)$$
$$\wedge\ Lsub(x, y, (e)_v) \wedge (z)_{z < v}(\sim Occ(x, ((e)_z)_1)))$$

Similarly, one defines the recursive predicate TCons(e, y, x) which differs from SCons(e, y, x) only in that the production in question is terminal. Let Der(e, x, y) be the recursive predicate which is true when and only when e is the index of an algorithm schema, x is the Gödel number of a word U_0, y is the Gödel number of a sequence of words $U_0, \ldots, U_k$ $(k \geqslant 0)$ such that, for $0 \leqslant i < k \dot{-} 1$, U_{i+1} arises from U_i according to an algorithm $\mathfrak{A}$ determined by the schema, and, either $\mathfrak{I}: U_{k \dot{-} 1} \vdash \cdot U_k$, or $\mathfrak{A}: U_{k \dot{-} 1} \vdash U_k$ and $\mathfrak{A}: U_k \sqsupset$ (or, if $k = 0$, just $\mathfrak{A}: U_k \sqsupset$): $Ind(e) \wedge Word(x)$ A $(z)_{z < lh(y)}(Word((y)_z)$ A

$$(y)_0 = x \wedge (z)_{z < lh(y) \dot{-} 2}(SCons(e, (y)_{z+1}, (y)_z)) \wedge$$
$$((lh(y) = 1 \wedge End(e, (y)_0)) \vee (lh(y) > 1 \wedge (TCons(e, (y)_{lh(y) \dot{-} 1}, (y)_{lh(y) \dot{-} 2})$$
$$\vee\ (SCons(e, (y)_{lh(y) \dot{-} 1}, (y)_{lh(y) \dot{-} 2}) \wedge End(e, (y)_{lh(y) \dot{-} 1})))))$$

Let A be any alphabet $\{S_{j_0}, \ldots, S_{j_m}\}$, and let $W_A(u)$ be the recursive predicate which holds if and only if u is the Gödel number of a word of A: $u = 1 \vee (z)_{z < lh(u)}((u)_z = 2j_0 + 3 \vee \ldots \vee (u)_z = 2j_m + 3)$. Now, let $\mathfrak{I}$ be any normal algorithm over the alphabet A, and let e be the index of the algorithm schema for P. Define the partial recursive function $\varphi(x) = \mu y((W_A(x) \wedge Der(e, x, y))$ V $\neg W_A(x))$. But, $\psi_{\mathfrak{A}}(x) = (\varphi(x))_{lh(\varphi(x)) \dot{-} 1}$, and so, $\psi_{\mathfrak{A}}$ is partial recursive. If $\mathfrak{A}$ is applicable to every word in A, then φ is recursive; hence, so is $\psi_{\mathfrak{A}}$.

EXERCISES

5.6. Let A be an alphabet. Show that there is a normal algorithm $\mathfrak{B}$ over A ∪ M such that, for any normal algorithm $\mathfrak{A}$ in *A* determined by an algorithm schema with index e, $\mathfrak{B}(\overline{e} * P) \approx \mathfrak{A}(P)$ for any word *P* in A. ($\mathfrak{B}$ can be considered a universal algorithm for A.)

COROLLARY 5.11. *Let φ be a* partial function. *If φ is partially Markov-computable, then φ is partial recursive*, and, *if φ* is *Markov-computable, then φ recursive.*

PROOF. Let $\mathfrak{A}$ be a normal algorithm over M such that $\varphi(n_1, \ldots, n_k) = m$ if and only if $\mathfrak{A}(\overline{(n_1, \ldots, n_k)}) = \overline{m}$. By Proposition 5.10, the function $\psi_{\mathfrak{A}}$ is partial recursive. Define the recursive function $\gamma(x) = lh(x) \dot{-} 1$. If $x = \prod_{i=0}^{n}(p_i)^5$, then $n = \gamma(x)$. Let

$$\ldots, n_k) = g(\overline{(n_1, \ldots, n_k)}) = g(1^{n_1+1} * 1^{n_2+1} * \cdots * 1^{n_k+1})$$

$$= \left[\prod_{i=0}^{n_1+1}(p_i)^5\right] \cdot (p_{n_1+2})^7 \cdot \left[\prod_{i=0}^{n_2+1}(p_{i+n_1+3})^5\right] \cdot (p_{n_1+n_2+5})^7 \cdot \ldots$$

$$\ldots \cdot (p_{n_1+\ldots+n_{k-1}+2k \dot{-} 3})^7 \cdot \left[\prod_{i=0}^{n_k+1}(p_{i+n_1+\ldots+n_{k-1}+2k \dot{-} 2})^5\right]$$

ξ is clearly recursive. Then $\varphi = \gamma \circ \psi_{\mathfrak{A}} \circ \xi$ is partial recursive. If φ is Markov-computable, then $\mathfrak{A}$ can be assumed applicable to every word in M. (Set up the algorithm schema for $\mathfrak{A}$ so that it takes every word in M not of the form $\overline{n}_1 * \ldots * \overline{n}_k$ into the empty word.) Then, by Proposition 5.10, $\psi_{\mathfrak{A}}$ is recursive. Hence $\varphi = \gamma \circ \psi_{\mathfrak{A}} \circ \xi$ is recursive.

EXERCISE 5.7. *Show that every total* partial *recursive function is recursive.*

the equivalence between partial recursiveness and partial Markov-computability (and between recursiveness and Markov-computability) has been by Corollary 5.11 and Proposition 5.8. Church's Thesis asserts that recursiveness is equivalent to effective computability (and, in an extended form, that partial recursiveness is equivalent to partial effective computability). In terms of algorithms, Markov has formulated the corresponding *Normalization Principle*: Every algorithm in A is fully equivalent relative to A to some normal over A. Now, Church's Thesis (in the extended form) and Markov's Principle are equivalent. First, assume Church's Thesis. Let $\mathfrak{A}$ be an algorithm in an alphabet A. Then $\psi_{\mathfrak{A}}$ is a partial effectively computable function. Hence, by Church's Thesis, $\psi_{\mathfrak{A}}$ is partial recursive, and so, by Proposition 5.9, $\mathfrak{A}$ is fully equivalent relative to A to some normal algorithm $\mathfrak{B}$, i.e., Markov's Principle assume Markov's Principle. Let φ be a partial effectively computable function. Let $\mathfrak{B}_\varphi$ be the corresponding algorithm in M. By Markov's Principle, $\mathfrak{B}_\varphi$ is fully equivalent to a normal algorithm relative to M. Hence, φ is partially Markov-computable, and, by Corollary 5.11, φ is partial recursive. Thus, Church's Thesis holds.

Of course, because of the vagueness of the intuitive notions of computable function and algorithm, it is impossible to *prove* the validity of Thesis or Markov's Principle. Nor is there any a priori reason to support these hypotheses. There is no apparent reason why the use of productions alone should account for all effective operations. One can only expect incomplete confirmation, not a rigorous proof. It is clear that every partial recursive function is a partial effectively computable function.† The converse assertion, that every partial effectively computable function is partial recursive (or, equivalently, that every algorithm in an alphabet A is fully equivalent relative to A to some normal algorithm) has been confirmed for every known partial effectively computable function. There is some additional evidence in favor of Church's Thesis, namely, the odd fact that quite dissimilar attempts to precisely define the notion of partial effectively computable function have proved to be equivalent. We have seen this already for partial recursiveness and partial Markov-computability. Other approaches, by Turing and by Herbrand and Gödel, will be shown later to lead to the same result. In addition, Church's theory of λ-computability [1941] and Post's theory of normal systems yield notions equivalent to that of partial-recursive function or normal akarithm. (Arguments for Church's Thesis may be found in Kleene [1952], §§ 62, 70. Also consult Hermes [1965].)

EXERCISES

5.8. Show that the Normalization Principle is equivalent to the assertion that every algorithm in an alphabet A is equivalent relative to A to some algorithm over *A*.

5.9. Given an alphabet B and an alphabet $A = \{a_1, \ldots, a_k\}$ disjoint from B. Let *b*, *c* be distinct symbols not in B ∪ A. For any symbol *a*, we denote by a^i the word $\underbrace{aa\cdots a}_{i\text{ time}}$. The *translation* $T(a_i)$ of a, is defined to be the word cb^ic, and the translation $T(u)$ of any symbol *u* in *B* is u itself; the translation $T(P)$ of a word $P = d_1 \cdots d_n$ in B ∪ A is defined to be $T(d_1) \ldots T(d_n)$, while $T(\Lambda) = \Lambda$. Note that $T(P) = P$ for any word *P* in B.

(a) Show that the schema

$$\begin{aligned} &\alpha\xi \to T(\xi)\alpha \qquad (\xi \text{ in } B \cup A) \\ &\alpha \to \cdot\Lambda \\ &\Lambda \to \alpha \end{aligned}$$

defines a normal algorithm $\mathfrak{T}$ over $B \cup A \cup \{b, c\}$ such that $\mathfrak{T}(P) = T(P)$ for any word *P* in B ∪ A. (Assume that a is not in $B \cup A \cup \{b, c\}$.)

†The reader should notice that partial effective computability does not necessarily imply human computability. Partial effective computability means that the values of the function can be computed, according to a fixed procedure, in a finite number of steps. Some of the computations needed to obtain the values of a partial recursive function involve so many steps that the human race may not exist long enough to carry them out.

(b) Give the schema for a normal algorithm $\mathfrak{B}$ over B u A u $\{b, c)$ such that $\mathfrak{B}(\mathrm{T}(P)) = \mathrm{P}$ for any word P in B ∪ A.

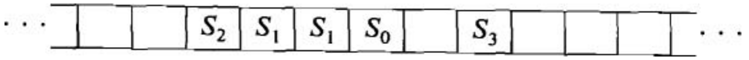
(c) Let $\mathfrak{C}$ be any normal algorithm in B u A. For any production $\mathrm{P} \rightarrow (\cdot) Q$ of the schema for $\mathfrak{C}$, the translation of this production is taken to be the production $\mathrm{T}(P) \rightarrow (\cdot)\mathrm{T}(Q)$. The translation of all the productions in the schema for $\mathfrak{C}$ gives an algorithm schema defining a normal algorithm $\mathrm{T}(\mathfrak{C})$ in B ∪ $\{b, c)$. If $\mathfrak{T}$ is the algorithm of Part (a), show that $(\mathrm{T}(\mathfrak{C}))(\mathfrak{T}(P)) \approx \mathfrak{T}(\mathfrak{C}(P))$.

(d) Prove that any normal algorithm over B is fully equivalent relative to B to some normal algorithm in B ∪ $\{b, c)$. (That the number of additional symbols can be reduced from two to one has been shown by Nagornyi [1953]. However, in the same paper, Nagornyi states that there is a normal algorithm over B, the doubling algorithm (Exercise 5.2(d), page 225), which is not equivalent relative to B to any normal algorithm in B itself. This is an easy exercise for the reader.)

2. Turing Algorithms

Attempting to give a precise definition of effective computability, Turing [1936] proposed that a certain class of abstract machines could perform any "mechanical" computing procedure. Such machines are now called Turing machines in honor of their inventor, and can be described in the following way.

There is a two-way potentially infinite tape divided up into squares.



The tape is said to be potentially infinite in the sense that, although at any moment it is finite in length, additional squares always can be added to the right- and left-hand ends of the tape. There is a finite set of ***tape symbols*** S_0, S,, . . . , S_n called the ***alphabet*** of the machine; at every moment, each square of the tape is occupied by at most one symbol. The machine has a finite set of ***internal states*** $\{q_0, q_1, \ldots, q_m\}$. At any given moment, the machine is in exactly one of these states. Finally, there is a reading head which, at any given time, stands over some square of the tape. The machine does not act continuously, but only at discrete moments of time. If, at any moment t, the reading head is scanning (i.e., is standing over) a square containing a symbol S_i and the machine is in the internal state q_j, then the action of the machine is determined, and it will do one of four things: (1) it may erase the symbol S,.and print a new symbol S_k; (2) it may move left one square; (3) it may move right one square; (4) it may stop. In cases (1)–(3), the machine goes into a new internal state q_r, and is ready to act again at time t + 1. We shall assume that the symbol S_0 represents a blank, so that the reading head may always be assumed to be scanning a symbol. The first three actions of the machine just described can be represented by quadruples: either (1) $q_j S_i S_k q_r$, or (2) $q_j S_i L q_r$, or (3) $q_j S_i R q_r$. The first two symbols stand for the present internal state and scanned symbol, the third symbol represents the action of the machine (print S_k, or move left, or move right one square), and the fourth symbol gives the internal state of the machine after the action has been performed.

If a tape is put into a Turing machine and the reading head is placed on a certain square, and if the machine is started off in one of its internal states, then the machine begins to operate on the tape: printing and erasing symbols and moving from one square to an adjacent one. If the machine ever stops, the resulting tape is said to be the output of the machine applied to the given tape. Now we can associate with any Turing machine T the following algorithm $\mathfrak{B}$ in the alphabet A of T. Take any word P in the alphabet A and print it from left to right in the squares of an empty tape. Place this tape in the machine with the reading head scanning the left-most square. Start the machine in the internal state q_0. If the machine ever stops, the word of A appearing on the tape is the value of the algorithm $\mathfrak{B}$. $\mathfrak{B}$ is called a ***Turing algorithm.*** (The word appearing on the tape is defined to be the sequence of symbols beginning with the left-most symbol and moving right to the right-most symbol. Remember that a blank square encountered in this motion is assumed to have the symbol S_0 printed in it.) We have not specified yet the mechanism by which a machine knows when to stop; this will be done below.

Any Turing machine can be determined precisely by a finite set of quadruples of the three kinds: (1) $q_j S_i S_k q_r$; (2) $q_j S_i L q_r$; (3) $q_j S_i R q_r$, such that no two quadruples have the same first two symbols. In fact, we now shall define a ***Turing machine*** to be such a finite set of quadruples. The ***alphabet*** of any Turing machine T is the set of tape symbols S_m appearing in any of the quadruples. The ***internal states*** of the machine are the symbols q_s appearing in the quadruples. We assume that q_0 is an internal state of every Turing machine.

An ***instantaneous tape description*** of a Turing machine T is a word such that (i) all symbols in the word but one are tape symbols S_m; (ii) the only symbol which is not a tape symbol is an internal state q_s; (iii) q_s is not the last symbol of the word.† We say that T ***moves*** one instantaneous tape description a into another one β (abbreviated a $\nrightarrow \beta$) if and only if either (a) a is of the form $P q_j S_i Q$, β is of the form $P q_r S_k$ Q, and $q_j S_i S_k q_r$ is one of the quadruples of T; or (b) a is of the form $P S_s q_j S_i Q$, β is $P q_r S_s S_i Q$, and $q_j S_i L q_r$ is one of the quadruples of T; or (c) a is of the form $q_j S_i Q$, β is $q_r S_0 S_i Q$, and $q_j S_i L q_r$ is one of the quadruples of T; or (d) a is of the form $P q_j S_i S_k Q$, β is $P S_i q_r S_k Q$, and $q_j S_i R q_r$ is one of the quadruples of T; or (e) a is of the form $P q_j S_i$, β is $P S_i q_r S_0$, and $q_j S_i R q_r$ is one of the quadruples of T.‡

†An instantaneous tape description describes the condition of the machine and the tape at a given moment. When read from left to right, the tape symbols in the description represent the symbols on the tape at the moment. The internal state q_s in the description is the internal state of the machine at the moment, and the tape symbol occurring immediately to the right of q_s in the tape description represents the symbol being scanned by the machine at the moment.

‡Observe that, according to our intuitive picture, "T moves a into β" implies that if the condition at time t of the Turing machine and tape is described by a, then the condition at time t + 1 is described by β. Notice that, according to clause (c), whenever the machine reaches the left-hand end of the tape and is ordered to move left, a blank square is attached to the tape on the left; similarly, by clause (e), a blank square is added on the right when the machine reaches the right-hand end of the tape and has to move right.

We say that T ***stops*** at an instantaneous tape description a if and only if there is no instantaneous tape description β such that a $\xrightarrow[T]{} \beta$. (This happens when q_jS_i occurs in a but q_jS_i are not the first two symbols of a quadruple of T.)

A ***computation*** of a Turing machine T is a finite sequence of instantaneous tape descriptions $\alpha_0, \ldots,$ a, (m $\geqslant$ 0) such that the internal state occurring in α_0 is q_0; for $0 \leqslant i <$ m, a, $\xrightarrow[T]{}$ α_{i+1}; and T stops at a,. This computation is said to begin with α_0 and end with a. The algorithm $\mathfrak{B}_{T,C}$ in any alphabet C containing the alphabet A of T is defined as follows: for any words P, Q in C, $\mathfrak{B}_{T,C}(P) =$ Q if and only if there is a computation of T which begins with the instantaneous tape description q_0P and ends with an instantaneous tape description of the form R,q_jR_2, where Q = R,R_2. An algorithm $\mathfrak{A}$ in an alphabet D is called ***Turing-computable*** if and only if there is a Turing machine T with alphabet A and an alphabet C containing A $\cup$ D such that $\mathfrak{B}_{T,C}$ and $\mathfrak{A}$ are fully equivalent relative to D.

We let 1 stand for S,. Remember that iii stands for 1^{m+1}, for any natural number m. Also, let * be an abbreviation of S_2. Given a partial number-theoretic function $f(x_1, \ldots, x_n)$, we say that a Turing machine T (whose alphabet A includes {1, *)) ***computes*** f if and only if, for any natural numbers k,, . . . , k_n, and any word Q, $\mathfrak{B}_{T,A}(\overline{k_1} * \overline{k_2} * \cdots * \overline{k_n}) =$ Q if and only if Q is $R_1\overline{f(k_1, \ldots, k_n)}R_2$, where both R_1 and R, are certain (possibly empty) words consisting only of S_0's. (The form $R_1\overline{f(k_1, \ldots, k_n)}R_2$ is allowed for the result since S_0 is interpreted as a blank.) The function f is called ***Turing-computable*** if and only if there is a Turing machine T which computes f.

Examples

1. Consider the Turing machine T defined by the following quadruples.

$$q_01Lq_1$$
$$q_1S_01q_2$$

The alphabet of T is $\{1, S_0\}$. T computes the successor function, since $q_0\bar{k} \xrightarrow[T]{} q_1S_0\bar{k} \xrightarrow[T]{} q_2\overline{k+1}$. In general, T takes any q_01P into q_211P, and T takes any word not beginning with 1 into itself.

2. The machine defined by the quadruples

$$q_01Lq_1$$
$$q_1S_01q_0$$

when started on a word beginning with 1 keeps on adding 1's to the left and never stops.

3. The Turing machine given by the quadruples

$$q_0S_0Rq_0$$
$$q_0S_2Rq_0$$
$$q_0\dot{S}_kRq_0$$
$$q_01\ 1q_1$$

moves right until it locates the first occurrence (if any) of the symbol 1 and then stops.

4. Let us find a Turing machine T which computes the addition function. Take as the quadruples for T:

$$q_01S_0q_0$$
$$q_0S_0Rq_1$$
$$q_11Rq_1$$
$$q_1{*}\ 1q_2$$
$$q_21Rq_2$$
$$q_2S_0Lq_3$$
$$q_31S_0q_3$$

Then

$$q_0\overline{m} * a = q_01^{m+1} * 1^{n+1} \xrightarrow[T]{} q_0S_01^m \blacksquare 1^{n+1} \xrightarrow[T]{} S_0q_11^m * 1^{n+1} \xrightarrow[T]{} S_01q_11^{m\dot{-}1} * 1^{n} \cdots$$
$$\xrightarrow[T]{} \ - \ - \xrightarrow[T]{} S_01^mq_1 * 1^{n+1} \xrightarrow[T]{} S_01^mq_211^{n+1} \xrightarrow[T]{} S_01^{m+1}q_21^{n+1} \xrightarrow[T]{} S_01^{m+1}1q_21^n \xrightarrow[T]{}$$
$$\ldots \xrightarrow[T]{} S_01^{m+1}1^{n+1}q_2S_0 \xrightarrow[T]{} S_01^{m+1}1^nq_31S_0 \xrightarrow[T]{} S_01^{m+1}1^nq_3S_0S_0 =$$
$$S_01^{m+n+1}q_3S_0S_0 = S_0\overline{m+n}q_3S_0S_0.$$

EXERCISES

5.10. What function f(x) is computed by the following Turing machine?

$$q_01S_0q_0$$
$$q_0S_0Rq_1$$
$$q_111q_0$$
$$q_1S_01q_2$$

5.11. Show that the initial primitive recursive functions $U_i^n(x_1, \ldots, x_n)$ are Turing computable.

5.12. Write down the quadruples of a Turing machine which computes the function $f(x) = [x/2]$, the greatest integer $\leqslant x/2$.

5.13. Show that the function $m \dot{-} n$ is Turing-computable. (For more examples, cf. Davis [1958, Chapter 1].)

PROPOSITION 5.12. ***Let*** T ***be a Turing machine with alphabet*** A. ***Let*** C ***be an extension of*** A, ***i.e.***, C $\supseteq$ A. ***Then there is a normal algorithm*** $\mathfrak{A}$ ***over*** C ***which is fully equivalent to the Turing algorithm*** $\mathfrak{B}_{T,C}$ ***relative to*** C.

PROOF. Let D = C $\cup$ $\{q_{k_0}, \ldots, q_{k_m}\}$, where $q_{k_0}, \ldots, q_{k_m}$ are the internal states of T, and $q_{k_0} = q_0$. Write down the algorithm schema for $\mathfrak{A}$ as follows: first, for all quadruples $q_jS_iS_kq_r$ of T, take the productions $q_jS_i \rightarrow q_rS_k$. Second, for each quadruple $q_jS_iLq_r$, take the productions $S_lq_jS_i \rightarrow q_rS_lS_i$ for all symbols S_l of C; then take the production $q_jS_i \rightarrow q_rS_0S_i$. Third, for each quadruple

$q_jS_iRq_r$, take the productions $q_jS_iS_l \rightarrow S_iq_rS_l$ for all symbols S_l of C; then take the production $q_jS_i \rightarrow S_iq_rS_0$. Fourth, write down the productions $q_{k_i} \rightarrow \cdot$ A for each internal state q_{k_i} of T, and, finally, take A → q_0. This schema defines an algorithm $\mathfrak{A}$ over C, and it is easy to see that, for any word P of C, $\mathfrak{B}_{T, C}(P) \approx \mathfrak{A}(P)$.

COROLLARY 5.13. ***Every Turing-computable function f is partially Markov-*** **,** ***computable; hence*** (by ***Corollary*** 5.1 1), ***f is partial recursive, and, i f f is total,*** ' ***then f is recursiue.***

PROOF. Let $f(x_1, \ldots, x_n)$ be Turing-computable by a Turing machine T with alphabet A ⊇ {1, * }. Then by Proposition 5.12, there is a normal algorithm $\mathfrak{A}$ over A such that $\mathfrak{A}$ is fully equivalent to $\mathfrak{B}_{T, A}$ relative to A, where $\mathfrak{B}_{T, A}(\overline{k_1} * \cdot \ldots * \overline{k_n}) \approx R_1\overline{f(k_1, \ldots, k_n)}R_2$, R, and R_2 being (possibly empty) sequences of S_0's. Let $\mathfrak{C}_1$ be a normal algorithm over {1, * , S_0} such that (15, erases all S_0's occurring before the first 1 or * ; as a schema for $\mathfrak{C}_1$ we may take

$$\alpha S_0 \rightarrow \alpha$$
$$\alpha 1 \rightarrow \cdot 1$$
$$\alpha * \rightarrow \cdot *$$
$$\alpha \rightarrow \cdot \Lambda$$
$$\Lambda \rightarrow \alpha$$

Also, let $\mathfrak{C}_2$ be a normal algorithm over {1, * , S_0} such that $\mathfrak{C}_2$ erases all S_0's occurring after the last 1 or * of a word in {1, * }; a schema for $\mathfrak{C}_2$ is

$$a * \rightarrow * a$$
$$a 1 \rightarrow 1\alpha$$
$$\alpha S_0 \rightarrow \alpha$$
$$\alpha \rightarrow \cdot \Lambda$$
$$\Lambda \rightarrow \alpha$$

Now, let $\mathfrak{C}$ be the normal algorithm $\mathfrak{C}_2 \circ \mathfrak{C}_1 \circ \mathfrak{A}$. Then for any k,, . . . , k_n, $\mathfrak{A}(\overline{k_1} * \ldots * k_n) \approx \mathfrak{B}_{T, A}(\overline{k_1} * \ldots * \overline{k_n}) \approx R_1\overline{f(k_1, \ldots, k_n)}R_2$, where R, and R_2 are sequences of S_0's. Then

$$\mathfrak{C}_1(R_1\, \overline{f(k_1, \ldots, k_n)}\, R_2) = \overline{f(k_1, \ldots, k_n)}\, R_2$$

and $\mathfrak{C}_2(\overline{f(k_1, \ldots, k_n)}R_2) = \overline{f(k_1, \ldots, k_n)}$. Hence, f is partially Markov-computable by $\mathfrak{C}$.

PROPOSITION 5.14. ***Let $\mathfrak{A}$ be a normal algorithm in an alphabet A not containing S_0 or 6. Then there is a Turing machine*** T ***such that the Turing algorithm $\mathfrak{B} = \mathfrak{B}_{T, (A \cup \{S_0, \delta\})}$ in the alphabet*** A ***u*** {S_0, 6) ***has the following property: for any word*** W ***in A, $\mathfrak{B}$ is applicable to*** W ***if and only if $\mathfrak{A}$ is, and***

$\mathfrak{B}(W)$ is of the form $S_0^m\mathfrak{A}(W)S_0^n$, where m and n are non-negatiue integers. (The reason for the difference between $\mathfrak{A}$ and $\mathfrak{B}$ is that, while we agree to consider S_0 as a blank on a Turing machine tape, S_0 is treated like any other symbol in the theory of algorithms.)

PROOF. We may assume, by suitable reindexing, that A = {S,, S_2, . . . , S_k}. Let $P \rightarrow (\cdot)Q$ be an arbitrary production. We shall construct Turing machine quadruples which will have the effect of replacing the left-most occurrence (if any) of P in a word W by Q. If P ≠ A, let P be $b_0 \ldots b_r$. Then, take the following quadruples.

q_0	S_i	R	q_0	(S_i ∈ A, S_i # b_0)
q_0	b_0	δ	q_0	
q_0	δ	R	q_2	
q_2	b_1	R	q_3	
q_2	S_i	S_i	q_{r+2}	(S_i ∈ A ∪ {S_0}, S_i ≠ b_1)
43	b_2	R	44	
q_3	S_i	S_i	q_{r+2}	(S_i ∈ A ∪ {S_0}, S_i ≠ b_2)
q_r	b_{r-I}	R	q_{r+1}	
q_r	S_i	S_i	q_{r+2}	(S_i ∈ A U {S_0}, S_i ≠ b_{r-1})
q_{r+1}	b_r	R	q_{r+4}	
q_{r+1}	S_i	S_i	q_{r+2}	(S_i E A u {So), S_i ≠ b_r)
q_{r+2}	S_i	L	q_{r+2}	(S_i ∈ A ∪ {S_0})
q_{r+2}	δ	b_0	q_{r+3}	
q_{r+3}	b_0	R	q_0	
q_0	S_0	L	q_{r+5}	
q_{r+5}	S_i	L	q_{r+5}	(S_i ∈ A)
q_{r+5}	δ	b_0	q_{r+5}	
q_{r+5}	S_0	R	q_Y	(where Y is an integer greater than all the other indices, to be specified later)

These quadruples have the following effect on a word W. (Notice that we have not used q_1; q_1 will have a special purpose later on.) If W has no occurrence of P, then we wind up with the instantaneous tape description q_YW; if W has an occurrence of P, and W = W_1PW_2, where the indicated P is the left-most occurrence of P in W, then we wind up with $W_1Pq_{r+4}W_2$. In the latter case, we must now add some quadruples which will replace the indicated occurrence of P by Q. Let Q be $c_0 \ldots c_s$. There are three cases:

(1) s = r, i.e., P and Q have the same length. Then we add:

$$\begin{array}{lllll}
q_{r+4} & S_i & L & q_{r+7} & (S_i \in A \cup \{S_0\}) \\
q_{r+7} & b_r & c_r & q_{r+8} & \\
q_{r+8} & c_r & L & q_{r+9} & \\
q_{r+9} & b_{r-1} & c_{r-1} & q_{r+10} & \\
q_{r+10} & c_{r-1} & L & q_{r+11} & \\
 & & & & \\
q_{3r+7} & b_0 & c_0 & q_{3r+8} & \\
q_{3r+8} & S_i & L & q_{3r+8} & (S_i \in A) \\
q_{3r+8} & S_0 & R & q_u & u = \begin{cases} 0 & \text{if } P \to (\cdot)Q \text{ is simple} \\ 1 & \text{if } P \to (\cdot)Q \text{ is terminal} \end{cases}
\end{array}$$

Then, applying these quadruples to $W_1Pq_{r+4}W_2$, we obtain $q_uW_1QW_2$.

(2) s < r. Q is shorter than P. Add the quadruples

$$\begin{array}{lllll}
q_{r+4} & S_i & L & q_{r+7} & (S_i \in A \, U \, \{S_0\}) \\
q_{r+7} & b_r & c_s & q_{r+8} & \\
q_{r+8} & c_s & L & q_{r+8} & \\
 & \cdot & & & \\
q_{r+7+2s} & b_{r-s} & c_0 & q_{r+7+2s+1} & \\
q_{r+7+2s+1} & c_0 & L & q_{r+7+2s+2} & \\
q_{r+7+2s+2} & b_{r-s-1} & S_0 & q_{r+7+2s+2} & \\
q_{r+7+2s+2} & S_0 & L & q_{r+7+2s+3} & \\
q_{r+7+2s+3} & b_{r-s-2} & S_0 & q_{r+7+2s+3} & \\
q_{r+7+2s+3} & S_0 & L & q_{r+7+2s+4} & \\
 & & & & \\
q_{2r+s+8} & b_0 & S_0 & q_{2r+s+8} &
\end{array}$$

After these quadruples work on $W_1Pq_{r+4}W_2$, we have

$$W_1q_{2r+s+8}S_0^{r-s}QW_2$$

Now we must provide some quadruples which will move W, r – s squares to the right to obtain W_1QW_2 (preceded by some S_0's). Let M be an integer larger than all the indices of the q_i's and S_i's above, say, M = 3r + 9.

$$\begin{array}{lllll}
q_{2r+s+8} & S_0 & L & q_M &
\end{array}$$

$$(j = 1, 2, \ldots, k)\left\{\begin{array}{lllll}
q_M & S_j & \delta & q_{M+j} & (S_j \in A) \\
q_{M+j} & \delta & R & q_{M+j} & \\
q_{M+j} & S_0 & R & q_{M+j} & \\
q_{M+j} & S_l & L & q_{2M+j} & (S_l \in A) \\
q_{2M+j} & S_0 & S_j & q_{2M+j} & \\
q_{2M+j} & S_j & L & q_{3M+j} & \\
q_{3M+j} & S_0 & L & q_{3M+j} & \\
q_{3M+j} & \delta & S_0 & q_{4M+j} & \\
q_{4M+j} & S_0 & L & q_{5M+j} & \\
q_{5M+j} & S_0 & R & q_{6M+j} & \\
q_{6M+j} & S_0 & R & q_{6M+j} & \\
q_{6M+j} & S_l & S_l & q_u & (S_l \in A) \\
 & & & & u = \begin{cases} \text{Oif } P \to (\cdot)Q \\ \quad \text{is simple} \\ 1 \text{ if } \mathrm{P} \to (\cdot)Q \\ \quad \text{is terminal} \end{cases} \\
q_{5M+j} & S_l & S_l & q_M & (S_l \in A)
\end{array}\right.$$

Beginning with $W_,q_{2r+s+8}S_0^{r-s}QW_2$, these quadruples produce $(S_0)^pq_uW_,QW_2$ (where p is a positive integer).

(3) $s > $ r, i.e., Q is longer than P. This is left to the reader as an exercise. The treatment is analogous to that of case (2). (If P or Q is empty, the slight modifications necessary in the above constructions are left to be filled in by the reader.)

Now, let us assume that 𝔄 is a normal algorithm in the alphabet A = $\{S,, \ldots, S_k\}$ not containing S_0 or 8, and that the algorithm 𝔄 is defined by the algorithm schema $P, \to (\cdot)Q_1, \ldots, P_h \to (\cdot)Q_h$. We define a Turing machine T as follows: in the work above, take $P \to (\cdot)Q$ to be $P_1 \to (\cdot)Q_1$ and list the appropriate quadruples (it will suffice to take Y to be a number 100 times greater than the sum of k and the number of occurrences of symbols in the schema). These quadruples have the following effect: given q, W, if W does not contain P_1, we wind up with q_YW; if W = W_1PW_2, and this indicates the left-most occurrence of P in W, then we finally obtain $(S_0)^v q_u W_1QW_2$ (where v is a non-negative integer; and u = 0 if P, $\rightarrow (\cdot)Q_1$ is simple, and u = 1 if $P_1 \rightarrow (\cdot)Q_1$ is terminal). Next, we consider P, $\rightarrow (\cdot)Q_2$ and form the quadruples for this production as indicated above, except that we raise the subscripts on all q_i's by the amount Y (but q_u is left untouched). The subscripts are raised by Y so that these quadruples will not interfere with the action of the quadruples corresponding to $P_1 \rightarrow (\cdot)Q_1$. The new quadruples will go into action only after a word W has been found not to contain P_1; they have the effect of searching W for an occurrence of P„ and, if one is found, replacing the left-most occurrence of P_2 by Q_2, and winding up back in the initial state q_0 ready for action again by the first group of quadruples if $P_2 \rightarrow (\cdot)Q_2$ is simple or winding up in the terminal state q_1 if $P_2 \rightarrow (\cdot)Q_2$ is terminal. We now repeat the same process with $P_3 \rightarrow (\cdot)Q_3$, this time adding 2Y to the subscripts of the q_i's, etc. It should be clear that the Turing machine T so defined mimics the action of the normal algorithm $\mathfrak{A}$ in such a way that, for any word W in A, $\mathfrak{B} = \mathfrak{B}_{T, A \cup \{S_0, \delta\}}$ is applicable to W if and only if $\mathfrak{A}$ is, and $\mathfrak{B}$(W) is of the form $(S_0)^m \mathfrak{A}(W)(S_0)^n$, where m and n are non-negative integers. (For a similar proof, cf. Asser [1959]. An indirect proof could have been given by showing that every partial recursive function is Turing-computable and then using Corollary 5.11. Study of Hermes' method of linking Turing machines and his flow-charts (cf. Hermes [1965], § 7) would clarify the procedures used in the proof above).

COROLLARY 5.15. *Every partially Markov-computable function is Turing-computable.* (Hence, every partial recursive function is Turing-computable. For another proof, cf. Kleene [1952], § 68.)

PROOF. From Proposition 5.14 and the definition of Turing-computable function.

Thus, the Turing-machine approach to effective computability is equivalent to that by means of normal algorithms or by recursive functions. A Turing machine seems to be an abstract form of a digital computer (except that no attention is given to speed or convenience of operation). Intuitively, then, the fact that Turing-computable functions are identical with partial recursive functions further substantiates Church's Thesis. In addition, one can show that making additional complications in the structure of Turing machines (such as adding more tapes and reading heads, or using a two-dimensional tape) does not change the class of Turing-computable functions. (Further arguments along these lines may be found in Kleene [1952], pp. 317–323 and 376–381.)

3. Herbrand-Gödel Computability. Recursively Enumerable Sets.

The idea of defining all computable functions in terms of fairly simple systems of equations was proposed by Herbrand and developed by Gödel [1934]. The exposition given here is a version of the presentation in Kleene [1952], Chapter XI.

We define first the terms.

(a) All variables are terms.
(b) 0 is a term.
(c) If t is a term, then (t)' is a term.
(d) If $t_1, \ldots, t_n$ are terms and f_j^n is a function letter, $f_j^n(t_1, \ldots, t_n)$ is a term.

For every natural number n, we define the corresponding numeral $\bar{n}$ as follows: (1) $\bar{0}$ is 0; (2) n + 1 is $(\bar{n})'$. Thus, every numeral is a term.

An equation is a formula r = s where r and s are terms. A system E of equations is a finite sequence r, = s,, $r_2 = s_2, \ldots, r_k = s_k$ of equations such that r_k is of the form $f_j^n(t_1, \ldots, t_n)$. The function letter f_j^n is called the *principal* letter of the system E. Those function letters (if any) which appear only on the right side of equations of E are called the initial letters of E; any function letter other than the principal letter which appears on the left side of some equations and also on the right side of some equations is called an auxiliary letter of E.

We have two rules of inference:

R,: *An* equation e_2 is a consequence of an equation e_1 by R, if and only if e_2 arises from e_1 by substituting any numeral $\bar{n}$ for all occurrences of a variable.

R_2: *An* equation e is a consequence by R_2 of equations $f_h^m(\bar{n}_1, \ldots, \bar{n}_m) = \bar{p}$ and r = s if and only if e arises from r = s by replacing one or more occurrences of $f_h^m(\bar{n}_1, \ldots, \bar{n}_m)$ in s by $\bar{p}$, and r = s contains no variables.

A proof of an equation e from a set B of equations is a sequence $e_0, \ldots, e_q$ of equations such that e_q = e and, if $0 \leqslant i \leqslant q$, then either (1) e, is an equation of B, or (2) e_i is a consequence by R, of a preceding equation e_j (j < i), or (3) e_i is a consequence by R_2 of two preceding equations e_j and e_m (j < i, m < i). We use the notation B ⊢ e to state that there is a proof from B of e (or, in other words, that e is derivable from B).

Example. Let E be the system

$$f_1^1(x_1) = (x_1)'$$
$$f_1^2(x_1, x_2) = f_1^3(\bar{2}, x_2, f_1^1(x_1))$$

The principal letter of E is f_1^2; f_1^1 is an auxiliary letter, and f_1^3 an initial letter. The sequence of equations

$$f_1^2(x_1, x_2) = f_1^3(\bar{2}, x_2, f_1^1(x_1))$$
$$f_1^2(\bar{2}, x_2) = f_1^3(\bar{2}, x_2, f_1^1(\bar{2}))$$
$$f_1^2(\bar{2}, \bar{1}) = f_1^3(\bar{2}, \bar{1}, f_1^1(\bar{2}))$$
$$f_1^1(x_1) = (x_1)'$$
$$f_1^1(\bar{2}) = (\bar{2})' \quad \left(\text{i.e., } f_1^1(\bar{2}) = \bar{3}\right)$$
$$f_1^2(\bar{2}, \bar{1}) = f_1^3(\bar{2}, \text{T}, \bar{3})$$

is a proof of $f_1^2(\bar{2}, \bar{1}) = f_1^3(\bar{2}, \bar{1}, \bar{3})$ from E.

A number-theoretic partial function $\varphi(x_1, \ldots, x_n)$ is said to be computable by a system E of equations if and only if the principal letter of E is a letter$ with n arguments, and, for any natural numbers k,, . . . , k_n, p,

$$E \text{ t } f_j^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p} \text{ if and only if } \varphi(k_1, \ldots, k_n) = p.$$

The function φ is called Herbrand-Godel computable (for short, HG-computable) if and only if there is some system E of equations by which φ is computable.

Examples.

I. Let E be the system $f_1^1(x_1) = 0$. Then E computes the zero function Z. Hence, Z is HG-computable.

2. Let E be the system $f_1^1(x_1) = (x_1)'$. Then E computes the successor function N. Hence, N is HG-computable.

3. Let E be the system $f_i^n(x_1, \ldots, x_n) = x_i$. Then E computes the projection function U_i^n. Hence, U_i^n is HG-computable.

4. Let E be the system

$$f_1^2(x_1, 0) = x_1$$

$$f_1^2(x_1, (x_2)') = (f_1^2(x_1, x_2))'$$

Then E computes the addition function.

5. Let E be the system

$$f_1^1(x_1) = 0$$

$$f_1^1(x_1) = x_1.$$

The function $\varphi(x_1)$ computed by E is the partial function with domain {0) such that $\varphi(0) = 0$. For every k # 0, E t $f_1^1(\bar{k}) = \bar{0}$ and E t $f_1^1(\bar{k}) = \bar{k}$. Hence, $\varphi(x_1)$ is not defined for x, $\neq$ 0.

EXERCISES

5.14. What functions are HG-computable by the followingsystems of equations?

(a) $f_1^1(0) = 0 \quad f_1^1((x_1)') = x_1$
(b) $f_1^2(x_1, 0) = x_1 \quad f_1^2(0, x_2) = 0 \quad f_1^2((x_1)', (x_2)') = f_1^2(x_1, x_2)$
(c) $f_1^1(x_1) = 0 \quad f_1^1(x_1) = 0'$
(d) $f_1^2(x_1, 0) = x_1 \quad f_1^2(x_1, (x_2)') = (f_1^2(x_1, x_2))' \quad f_1^1(f_1^2(x_1, x_1)) = 0$

5.15. Show that the following functions are HG-computable.

(a) $|x_1 - x_2|$
(b) $x_1 \cdot x_2$
(c) $\varphi(x) = \begin{cases} 0 & \text{when x is even} \\ 1 & \text{when x is odd} \end{cases}$.

PROPOSITION 5.16. *Every* partial recursive function is *HG-computable.*

PROOF.

(1) Examples 1–3 above have shown that the initial functions Z, N, U_i^n are HG-computable.

(2) Substitution (Rule IV). Let $\varphi(x_1, \ldots, x_n) = \eta(\psi_1(x_1, \ldots, x_n), \ldots, \psi_m(x_1, \ldots, x_n))$ where $\eta, \psi_1, \ldots, \psi_m$ have been shown to be HG-computable. Let E, be a system of equations computing ψ_i, with principal letter f_i^n, and let E_{m+1} be a system of equations computing η, with principal letter f_{m+1}^m. By changing indices, we may assume that no two of $E_1, \ldots, E_m, E_{m+1}$ have any function letters in common. Construct a system E for φ by listing $E_1, \ldots, E_{m+1}$, and then adding the equation $f_{m+2}^n(x_1, \ldots,$ x„) = $f_{m+1}^m(f_1^n(x_1, \ldots, x_n), \ldots, f_m^n(x_1, \ldots,$ x„)). (We may assume that f_{m+2}^n does not occur in $E_1, \ldots, E_{m+1}$.) It is clear that, if $\varphi(k_1, \ldots, k_n) = p$, then E⊢ $f_{m\pm2}^n(\bar{k}_1, \ldots, \bar{k}_n) = \bar{p}$. Conversely, if E t $f_{m+2}^n(\bar{k}_1, \ldots, k_n) = \bar{p}$, then E ⊢ $f_1^n(k_1, \ldots, k) = \bar{p}_1, \ldots,$ E⊢ $f_m^n(\bar{k}_1, \ldots, k_n) = \bar{p}_m$ and E ⊢ $f_{m+1}^m(\bar{p}_1, \ldots, \bar{p}_m) = \bar{p}$. Hence, it readily follows that $E_1 \vdash f_1^n(\bar{k}_1, \ldots, k_n) = \bar{p}_1, \ldots, E_m \vdash f_m^n(\bar{k}_1, \ldots, k_n) = \bar{p}_m$ and E_{m+1} t $f_{m+1}^n(\bar{p}_1, \ldots, \bar{p}_m) = \bar{p}$. Consequently, $\psi_1(k_1, \ldots, k_n) = p_1, \ldots,$ $\ldots, k_n) = p_m$ and $\eta(p_1, \ldots, p_m) = p$. So, $\varphi(k_1, \ldots, k_n) = p$. (The details of this proof are left as an exercise. Hints may be found in Kleene 119521. Chapter XI, especially pages 262–270.) Hence φ is HG-computable.

(3) Recursion (Rule V). Let

$$\varphi(x_1, \ldots, x_n, 0) = \psi(x_1, \ldots, x_n)$$

$$\varphi(x_1, \ldots, x_n, (x_{n+1}) + 1) = \theta(x_1, \ldots, x_{n+1}, \varphi(x_1, \ldots, x_{n+1}))$$

where ψ and θ are HG-computable. Assume that E, is a system of equations computing ψ with principal letter f_1^n, and that E_2 is a system of equations computing 8, with principal letter f_1^{n+2}. Then form a system for computing φ by adding to E_1 and E_2

$$f_1^{n+1}(x_1, \ldots, x_n, 0) = f_1^n(x_1, \ldots, x_n)$$

$$f_1^{n+1}(x_1, \ldots, x_n, (x_{n+1})') = f_1^{n+2}(x_1, \ldots, x_{n+1}, f_1^{n+1}(x_1, \ldots, x_{n+1}))$$

(We assume that E_1 and E_2 have no function letters in common.) Clearly, if $\varphi(k_1, \ldots, k_n, k) = p$, then E⊢ $f_1^{n+1}(\bar{k}_1, \ldots, \bar{k}_n, \bar{k}) = \bar{p}$. Conversely, one can prove easily by induction on k that, if E t $f_1^{n+1}(k_1, \ldots, \bar{k}_n, \bar{k}) = \bar{p}$, then $\varphi(k_1, \ldots, k_n, k) = p$. Therefore, φ is HG-computable. (The case when the recursion has no parameters is even easier to handle, and is left as an exercise.)

(4) p-operator (Rule VI). Let $\varphi(x_1, \ldots, x_n) = \mu y(\psi(x_1, \ldots, x_n, y) = 0)$ and assume that ψ is HG-computable by a system E_1 of equations with principal letter f_1^{n+1}. By Parts (1)–(3), we know that every primitive recursive function is HG-computable. In particular, multiplication is HG-computable; hence there is a system E_2 of equations, having no function letters in common with E_1, and with principal letter f_2^2 such that E_2 t $f_2^2(k_1, k_2) = \bar{p}$ if and only if k, . k_2 = p. We form a system E_3 by adding to E_1 and E_2 the equations

$$f_3^{n+1}(x_1, \ldots, x_n, 0) = 1$$

$$f_3^{n+1}(x_1, \ldots, x_n, (x_{n+1})') = f_2^2(f_3^{n+1}(x_1, \ldots, x_n, x_{n+1}), f_1^{n+1}(x_1, \ldots, x_n, x_{n+1}))$$

One can prove by induction that E_3 computes the function $\Pi_{y<z}\psi(x_1, \ldots, x_n, y)$, i.e., $E_3 \vdash f_3^{n+1}(\overline{k_1}, \ldots, \overline{k_n}, \bar{k}) = \bar{p}$ if and only if $\Pi_{y<k}\psi(k_1, \ldots, k_„\ y) = p$. Now construct the system E by adding to E_3 the equations

$$f_4^3((x_1)', 0, x_3) = x_3$$

$$f_3^n(x_1, \ldots, x_n) = f_4^3(f_3^{n+1}(x_1, \ldots, x_n, x_{n+1}), f_3^{n+1}(x_1, \ldots, x_n, (x_{n+1})'), x_{n+1})$$

Then E computes the function $\varphi(x_1, \ldots, x_n) = \mu y(\psi(x_1, \ldots, x_n, y) = 0)$. For, if $\mu y(\psi(k_1, \ldots, k_n, y) = 0) = q$, then E_3 t $f_3^{n+1}(\overline{k_1}, \ldots, \overline{k_n}, \bar{q}) = \bar{p}'$, where p + I $= \Pi_{y<q}\psi(k_1, \ldots, k_n, y)$, and E_3 t $f_3^{n+1}(\overline{k_1}, \ldots, \overline{k_n}, \bar{q}') = 0$. Hence $E \vdash f_3^n(\overline{k_1}, \ldots, \overline{k_)} = f_4^3(\bar{p}', 0, \bar{q})$. But, $E \vdash f_4^3(\bar{p}', 0, \bar{q}) = \bar{q}$, and so, $E \vdash f_3^n(\overline{k_1}, \ldots, \overline{k_n}) = \bar{q}$. Conversely, if $E \vdash f_3^n(\overline{k_1}, \ldots, \overline{k_n}) = \bar{q}$, then $E \vdash f_4^3(\bar{m}', 0, \bar{q}) = \bar{q}$, where $E_3 \vdash f_3^{n+1}(\overline{k_1}, \ldots, \overline{k_n}, \bar{q}) = (\bar{m})'$ and $E_3 \vdash f_3^{n+1}(\overline{k_1}, \ldots, \overline{k_n}, \bar{q}') = 0$. Hence $\Pi_{y<q}\psi(k_1, \ldots, k_n, y) = m + 1 \neq 0$ and $\Pi_{y<q+1}\psi(k_1, \ldots, k_n, y) = 0$. So, $\psi(k_1, \ldots, k_n, y) \neq 0$ for $y < q$, and $\psi(k_1, \ldots, k_n, q) = 0$ Thus, $\mu y(\psi(k_1, \ldots, k_„\ y) = 0) = q$. Therefore, φ is HG-computable.

We now shall proceed to show that every Herbrand-Godel computable function is partial recursive, by means of an arithmetization of the apparatus of Herbrand-Godel computability. We shall use the same arithmetization that was used for first-order theories (cf. Chapter 3, § 4). (We take the symbol ′ to be an abbreviation for f_1^1. Remember that $r = s$ is an abbreviation for $A_1^2(r, s)$. The only individual constant is 0.) In particular (cf. pp. 153–154), the following relations and functions are primitive recursive:

FL(x): x is the Gödel number of a function letter.

$$(Ey)_{y<x}(Ez)_{z<x}(x = 9 + 8(2^y \cdot 3^z) \wedge y > 0 \wedge z > 0)$$

EVbl(x): x is the Gödel number of an expression consisting of a variable.
EFL(x): x is the Gödel number of an expression consisting of a function letter.
Nu(x): x is the Gödel number of a numeral.
Trm(x): x is the Gödel number of a term.
Num(x) = the Gödel number of the numeral $\bar{x}$.
$\mathrm{Arg_T}(x)$ = the number of arguments of a function letter f, if x is the Gödel number of f.
x * y = the Gödel number of an expression AB if x is the Gödel number of the expression A and y is the Gödel number of the expression B.
Subst(a, b, u, v): v is the Gödel number of a variable x_i, u is the Gödel number of a term t, b is the Gödel number of an expression $\mathcal{Q}$, and a is the Gödel number of the result of substituting t for all occurrences of x_i in $\mathcal{Q}$.

The following are also primitive recursive.

Eqt(x): x is the Gödel number of an equation:

$$1h(x) = 3 \wedge \mathrm{Trm}((x)_1) \wedge \mathrm{Trm}((x)_2) \wedge (x)_0 = 107$$

(Remember that = is A_1^2, whose Gödel number is 107.)

Syst(x): x is the Gödel number of a system of equations:

$$(y)_{y<1h(x)}\mathrm{Eqt}((x)_y) \wedge \mathrm{FL}((((x)_{1h(x)\dot{-}1})_1)_0)$$

Occ(u, v): u is the Gödel number of a term t or equation $\mathfrak{B}$ and v is the Gödel number of a term which occurs in t or $\mathfrak{B}$.

$$(\mathrm{Trm}(u) \vee \mathrm{Eqt}(u)) \wedge \mathrm{Trm}(v) \wedge (Ex)_{x<u}(Ey)_{y<u}(u = x * v * y \vee$$
$$u = x * v \vee u = v * y \vee u = v)$$

$\mathrm{Cons_1}(u, v)$: u is the Gödel number of an equation e_1, and v is the Gödel number of an equation e_2, and e_2 is a consequence of e, by Rule $\mathbf{R}_1$:

$$\mathrm{Eqt}(u) \wedge \mathrm{Eqt}(v) \wedge (Ex)_{x<u}(Ey)_{y<v}(\mathrm{Nu}(y) \wedge \mathrm{Subst}(v, u, y, x) \wedge \mathrm{Occ}(u, x))$$

$\mathrm{Cons_2}(u, z, v)$: u, z, v are Gödel numbers of equations e_1, e_2, e_3, respectively, and e_3 is a consequence of e_1 and e_2 by Rule $\mathbf{R}_2$.

$$\mathrm{Eqt}(u) \wedge \mathrm{Eqt}(z) \wedge \mathrm{Eqt}(v) \wedge \sim (Ex)_{x<z}(\mathrm{EVbl}(x) \wedge \mathrm{Occ}(z, x)) \wedge$$
$$\mathrm{FL}(((z)_1)_0) \wedge (x)_{0<x<1h((z)1)} \sim \mathrm{FL}(((z)_1)_x) \wedge$$
$$(x)_{x<1h((z)2)} \sim \mathrm{FL}(((z)_2)_x) \wedge \mathrm{Occ}((u)_2, (z)_1) \wedge ((Ey)_{y<u}$$
$$(Ew)_{w<u}((u)_2 = y * (z)_1 * w \wedge v = 2^{107}3^{(u)_1}5^{y * (z)_2 * w}) \vee$$
$$((u)_2 = (z)_1 \wedge v = 2^{107}3^{(u)_1}5^{(z)_2})))$$

Ded(u, z): u is the Gödel number of a system of equations E, and z is the Gödel number of a proof from E.

$$\mathrm{Syst}(u) \wedge (x)_{x<1h(z)}((Ew)_{w<1h(u)}(u)_w = (z)_x \vee$$
$$(Ey)_{y<x}\mathrm{Cons_1}((z)_y, (z)_x) \vee (Ey)_{y<x}(Ev)_{v<x}\mathrm{Cons_2}((z)_y, (z)_v, (z)_x))$$

$S_n(u, x_1, \ldots, x_n, z)$: u is the Gödel number of a system of equations E whose principal letter is of the form f_j^n, and z is the Gödel number of a proof from E of an equation of the form $f_j^n(\bar{x}_1, \ldots, \bar{x}_n) = \bar{p}$.

$$\mathrm{Ded}(u, z) \wedge \mathrm{Arg_T}((((u)_{1h(u)\dot{-}1})_1)_0 = n \wedge (((z)_{1h(z)\dot{-}1})_1)_0 =$$
$$(((u)_{1h(u)\dot{-}1})_1)_0 \wedge (y)_{0<y<1h(((z)_{1h(z)-1})_1)} \sim \mathrm{FL}((((z)_{1h(z)\dot{-}1})_1)_y)$$
$$\wedge \mathrm{Nu}(((z)_{1h(z)\dot{-}1})_2) \wedge ((z)_{1h(z)\dot{-}1})_1 = 2^{(((u)_{1h(u)\dot{-}1})_1)_0} * 2^3 * 2^{\mathrm{Num}(x_1)} * 2^7 *$$
$$2^{\mathrm{Num}(x_2)} * 2^7 * \cdots * 2^7 * 2^{\mathrm{Num}(x_n)} * 2^5$$

Remember that g(( ) = 3, g( )) = 5, g(,) = 7.

$U(x) = \mu y_{y<x}(\mathrm{Num}(y) = ((x)_{1h(x) \dot{-} 1})_2)$. (If x is the Gödel number of a proof of an equation $r = \bar{p}$, then $U(x) = p$.)

PROPOSITION 5.17 (Kleene [1936a]). *If* $\varphi(x_1, \ldots, x_n)$ is HG-computable by *a* system of equations E with *Gödel* number e, then

$$\varphi(x_1, \ldots, x_n) = U(\mu y(S_n(e, x_1, \ldots, x_n, y)))$$

Hence, *every* HG-computable function φ is partial recursive, and, if φ is total, then φ is recursive.

PROOF. $\varphi(k_1, \ldots, k_n) = p$ if and only if $E \vdash f_j^n(\overline{k_1}, \ldots, \overline{k_n}) = \bar{p}$, where f_j^n is the principal letter of E. $\varphi(k_1, \ldots, k_n)$ is defined if and only if $(Ey)S_n$ $(e, k_1, \ldots, k_n, y)$. If $\varphi(k_1, \ldots, k_n)$ is defined, $\mu y(S_n(e, k_1, \ldots$, k„ y)) is the Gödel number of a proof from E of an equation $f_j^n(\overline{k_1}, \ldots, \overline{k_n}) = \bar{p}$. Hence, $U(\mu y(S_n(e, k_1, \ldots$, k„ y))) $= p = \varphi(k_1, \ldots, k_n)$. Also, since S, is primitive recursive, $\mu y(S_n(e$, x,, $\ldots, x_n, y))$ is partial recursive. If φ is total, then $(x_1) \ldots (x_n)(Ey)S_n(e, x_1, \ldots, x_n, y)$; hence, $\mu y(S_n(e, x_1, \ldots, x_n, y))$ is recursive, and then, so is $U(\mu y(S_n(e$, x,, $\ldots, x_n, y)))$.

Thus, the class of Herbrand-Gödel computable functions is identical with the class of partial recursive functions. This is further evidence for Church's Thesis.

It is sometimes more convenient to use instead of S, the primitive recursive predicate

$$T_n(z, x_1, \ldots, x_n, y): S_n(z, x_1, \ldots, x_n, y) \text{ A } (u)_{u<y} \sim S_n(z, x_1, \ldots, x_n, \text{U})$$

Clearly, if $T_n(z, x_1, \ldots, x_n, y)$, then $S_n(z, x_1, \ldots, x_n, y)$. In addition, in contrast to S_n, if $T_n(z, x_1, \ldots, x_n, y)$ and $T_n(z$, x,, $\ldots, x_n, v)$, then $y = v$. It is obvious that

$$(Ey)S_n(z, x_1, \ldots, x_n, y) \equiv (Ey)T_n(z, x_1, \ldots, x_n, y)$$

and

$$U(\mu y S_n(z, x_1, \ldots, x_n, y)) = U(\mu y T_n(z, x_1, \ldots, x_n, y))$$

whenever either side is defined. From Propositions 5.16 and 5.17, it follows that every partial recursive function is expressible in the form $U(\mu y T_n(e$, x,, $\ldots, x_n, y))$ where e is the Gödel number of a system of equations computing the function. Conversely, for any natural number e, $U(\mu y T_n(e$, x,, $\ldots$, x„ y)) is a partial recursive function. Thus, as z varies over all natural numbers, $U(\mu y T_n(z, x_1, \ldots, x_n, y))$ gives an enumeration (with repetitions) of all partial recursive functions of n arguments. A number e such that $\varphi(x_1, \ldots, x_n) = U(\mu y T_n(e, x_1, \ldots, x_n, y))$ is called an index of the function φ. The Gödel number of any system of equations computing φ is an index of φ; there are infinitely many indices of φ. (Exercise.)

By an index of a recursive relation R we mean an index of the characteristic function of R. Then

$$R(x_1, \ldots, x,) \equiv (Ey)(T_n(e, x_1, \ldots, x_n, y) \text{ A } U(y) = 0)$$

where e is an index of R.

LEMMA 5.18

(1) *For* $n > 0$, if $R(x_1, \ldots$, x„ y) is a recursive predicate, then there exist natural numbers e_1, e_2 such that

$$(Ey)R(x_1, \ldots, x_n, y) \equiv (Ey)T_n(e_1, x_1, \ldots, x_n, y)$$

and

$$(y)R(x_1, \ldots, x_n, y) \equiv (y) \sim T_n(e_2, x_1, \ldots, x_n, y)$$

(2) For $n > 0$, if $R(x_1, \ldots, x_n, z, y)$ is a recursive predicate, there exist natural numbers e,, e_4 such that

$$(z)(Ey)R(x_1, \ldots, x_n, z, y) \equiv (z)(Ey)T_{n+1}(e_3, x_1, \ldots, x_n, z, y)$$

and

$$(Ez)(y)R(x_1, \ldots, x_n, z, y) \equiv (Ez)(y) \sim T_{n+1}(e_4, x_1, \ldots, x_n, z, y)$$

and so on, for three or more *quantifiers.*

PROOF.

(1) Let $\varphi(x_1, \ldots, x_n, y)$ be the characteristic function of R; then φ is recursive, and $\mu y(\varphi(x_1, \ldots, x_n, y) = 0)$ is partial recursive. Let e_1 be the Gödel number of a system of equations computing $\mu y(\varphi(x_1, \ldots, x_n, y) = 0)$. Then, $(Ey)R(x_1, \ldots, x_n, y)$ if and only if $\mu y(\varphi(x_1, \ldots, x_n, y) = 0)$ is defined; hence, $(Ey)R(x_1, \ldots, x_n, y) \equiv (Ey)(T_n(e_1, x_1, \ldots, x_n, y))$. Applying this result to $\sim R$, we obtain a number e_2 such that $(Ey) \sim R(x_1, \ldots, x_n, y) \equiv (Ey)T_n(e_2$, x,, $\ldots, x_n, y)$. Hence, $(y)R(x_1, \ldots, x_n, y) \equiv (y) \sim T_n(e_2$, x,, $\ldots$, x,, y). (2) follows from (1), taking $n + 1$ instead of n.

Thus, as u varies, $(Ey)T_n(u$, x,, $\ldots, x_n, y)$ enumerates all relations $(Ey)R(x_1, \ldots, x_n, y)$, where R is recursive, and $(y) \sim T_n(u, x_1, \ldots, x_n, y)$ enumerates all relations $(y)R(x_1, \ldots, x_n, y)$, where R is recursive; etc.

PROPOSITION 5.19 (Kleene [1943; 1952, § 57], Mostowski [1947])

(1) If $R(x, y)$ is recursive, there are natural numbers e,, e_2 such that

$$\sim ((Ey)R(e_1, y) \equiv (y) \sim T_1(e_1, e_1, y))$$

and

$$\sim ((y)R(e_2, y) \equiv (Ey)T_1(e_2, e_2, y))$$

(2) ***If*** $R(x)$ ***is recursive, there are natural numbers*** e_1, e_2 ***such that***

$$\sim (R(e_1) \equiv (y) \sim T_1(e_1, e_1, y))$$

and

$$\sim (R(e_2) \equiv (Ey)T_1(e_2, e_2, y))$$

(3) ***Both*** $(y) \sim T_1 nx, x, y)$ ***and*** $(Ey)T_1(x, x, y)$ ***are not recursive.***

(4) ***Consider the following list*** (where R is any recursive relation):

$$\begin{array}{lll} (R(x_1, \ldots, x_n) & (Ey_1)R(x_1, \ldots, x_n, y_1) & (Ey_1)(y_2)R(x_1, \ldots, x_n, y_1, y_2) \\ & (y_1)R(x_1, \ldots, x_n, y_1) & (y_1)(Ey_2)R(x_1, \ldots, x_n, y_1, y_2) \end{array}$$

$$\begin{array}{l} (Ey_1)(y_2)(Ey_3)R(x_1, \ldots, x_n, y_1, y_2, y_3) \ldots \\ (y_1)(Ey_2)(y_3)R(x_1, \ldots, x_n, y_1, y_2, y_3) \ldots \end{array}$$

If we let $\Pi_0^n = \Sigma_0^n =$ the set of all recursive relations with n arguments; and, for $k > 0$, $\Sigma_k^n =$ the set of all relations with n arguments expressible in the "prenex form" $(Ey_1)(y_2) \ldots (Qy_k)R(x_1, \ldots, x_n, y,, y_2, \ldots, y_k)$, consisting of k alternating quantifiers beginning with an existential quantifier and followed by a recursive relation R; and $\Pi_k^n =$ the set of all relations with n arguments expressible in "prenex form" $(y_1)(Ey_2) \ldots (Qy_k)R(x_1, \ldots, \%, y,, y_2, \ldots, y_k)$, consisting of k alternating quantifiers beginning with a universal quantifier and followed by a recursive relation R, then the list above can be written

$$\begin{array}{ccccc} & \Sigma_1^n & \Sigma_2^n & \Sigma_3^n & \ldots \\ \Sigma_0^n & & & & \\ & \Pi_1^n & \Pi_2^n & \Pi_3^n & \ldots \end{array}$$

(In the "prenex form," (Qy_k) represents either a universal or existential quantifier.)

(a) Every relation of any form listed above is expressible in any form indicated in any of the succeeding columns on the right, i.e., $\Sigma_k^n \subseteq \Sigma_j^n \cap \Pi_j^n$ and $\Pi_k^n \subseteq \Sigma_j^n \cap \Pi_j^n$ for all $j > k$.

(b) There is a relation of each form, except the left-most, which is not expressible in the other form indicated in the same column, and, hence, by (a), not in any of the previous columns on the left, i.e., $\Sigma_k^n - \Pi_k^n \neq 0$ and $\Pi_k^n - \Sigma_k^n \neq 0$ for $k > 0$.

(c) Every arithmetic relation (cf. p. 151, Exercise 3.34) is expressible in at least one of these forms.

(d) (Post) For any relation $Q(x_1, \ldots, x_n)$, Q is recursive if and only if both Q and $\sim Q$ are both expressible in the form $(Ey_1)R(x_1, \ldots, x_n, y,)$, where R is recursive, i.e., $\Sigma_1^n \cap \Pi_1^n = \Sigma_0^n$.

(e) If $Q_1 \in \Sigma_k^n$ and $Q_2 \in \Sigma_k^n$, then $Q_1 \vee Q_2$ and Q_1 A Q_2 are in Σ_k^n; if Q_1 and Q_2 are in Π_k^n, then $Q, \bigvee Q_2$ and $Q, \bigwedge Q_2$ are in Π_k^n.

(f) In contradistinction to (d), if $k > 0$,

$$(\Sigma_{k+1}^n \cap \Pi_{k+1}^n) - (\Sigma_k^n \cup \Pi_k^n) \neq 0$$

PROOF.

(1) Assume $R(x, y)$ recursive. Then, by Lemma 5.18, there are numbers e_1, e_2 such that $(Ey)R(x, y) \equiv (Ey)T_1(e_1, x, y)$ and $(y)R(x, y) \equiv (y) \sim T_1(e_2, x, y)$. In the first equivalence, let $x = e_1$, and, in the second, let $x = e_2$.

(2) Assume $R(x)$ recursive. Then $R(x) \wedge y = y$ is recursive; clearly, $(Ey)(R(x)$ A $y = y) \equiv R(x)$ and $(y)(R(x)$ A $y = y) \equiv R(x)$. Apply (1).

(3) Assume $(y) \sim T_1(x, x, y)$ is recursive. By (2), there is an integer e, such that $\sim ((y) \sim T_1(e_1, e_1, y) \equiv (y) \sim T_1(e_1, e_1, y))$, which is a contradiction. Similarly, if $(Ey)T_1(x, x, y)$ is recursive, then, by (2), there is an integer e_2 such that $\sim ((Ey)T_1(e_2, e_2, y) \equiv (Ey)T_1(e_2, e_2, y))$, which is a contradiction.

(4) (a) $(Ez_1)(y_1)(Ez_2)(y_2) \ldots (Ez_k)(y_k)R(x_1, \ldots, x_n, z_1, y_1, \ldots, z_k, y_k) \equiv (u)(Ez_1)(y_1) \ldots (Ez_k)(y_k)(R(x_1, \ldots, x_n, z_1, y_1, \ldots, z_k, y_k)$ A $u = u) \equiv (Ez_1)(y_1) \ldots (Ez_k)(y_k)(Eu)(R(x_1, \ldots, x_n, z_1, y_1, \ldots, z_k, y_k)$ A $u = u)$. Hence any relation expressible in one of the forms in the list is expressible in both forms in any succeeding column.

(b) Let us just take a typical case. Consider $(Ev)(z)(Ey)T_{n+2}(x_1, x_1, x_2, \ldots, x_n, v, z, y)$. Assume that this is expressible in the form $(v)(Ez)(y)R(x_1, \ldots, x_n, v, z, y)$, where R is recursive. By Lemma 5.18, this relation is equivalent to $(v)(Ez)(y) \sim T_{n+2}(e, x,, \ldots, x_n, v, z, y)$ for some e. But when $x, = e$, this is a contradiction.

(c) Every wf of the first-order theory S can be put into prenex normal form. It suffices to note that, if R is recursive, then $(Eu)(Ev)R(u, v)$ is equivalent to $(Ez)R(\sigma_1^2(z), \sigma_2^2(z))$, where σ_1^2, σ_2^2 are the recursive inverse mappings of the one-one correspondence a^2 between pairs of natural numbers and natural numbers (cf. 145–146). Also, $(u)(v)R(u, v)$ is equivalent to $(z)R(\sigma_1^2(z), \sigma_2^2(z))$. Hence, successive quantifiers of the same kind (existential or universal) can be condensed into one such quantifier.

(d) If Q is recursive, so is $\sim Q$; if $P(x_1, \ldots, x_n)$ is recursive, then $P(x_1, \ldots, x_n) \equiv (Ey)(P(x_1, \ldots, x_n) \wedge y = y)$. Conversely, assume Q is expressible as $(Ey)R_1(x_1, \ldots, x_n, y)$, and -- Q as $(Ey)R_2(x_1, \ldots, \%, y)$, where R, and R_2 are recursive. Hence, $(x,) \ldots (x_n)(Ey)(R_1(x_1, \ldots, x_n, y) \vee R_2(x_1, \ldots, x_n, y))$. So, $\varphi(x_1, \ldots, x_n) = \mu y(R_1(x_1, \ldots, x_n, y) \vee R_2(x_1, \ldots, x_n, y))$ is recursive. Then $Q(x_1, \ldots, x_n) \equiv R_1(x_1, \ldots, x_n, \varphi(x_1, \ldots, x,,))$, and, therefore, Q is recursive.

(e) Use the following facts; If x is not free in $\mathfrak{A}$, $\vdash (Ex)(\% \vee \mathfrak{B}) \equiv (\mathfrak{A}$ V $(Ex)\mathfrak{B})$, $\vdash (Ex)(\mathfrak{A}$ A $\mathfrak{B}) \equiv (\mathfrak{A}$ A $(Ex)\mathfrak{B})$, $\vdash (x)(\mathfrak{A}$ V $\mathfrak{B}) \equiv (\mathfrak{A}$ V $(x)\mathfrak{B})$, $\vdash (x)(\mathfrak{A}$ A $\mathfrak{B}) \equiv (\mathfrak{A}$ A $(x)\mathfrak{B})$.

(f) We shall suggest here a proof in the case n = 1; the other cases are then easy consequences. Let $Q(x) \in \Sigma^1_k - \Pi^1_k$. Define $P(x)$ as $(Ez)((x = 2z \wedge Q(z)) \vee (x = 2z + 1 \wedge \sim Q(z)))$. It is easy to prove that $P \notin \Sigma^1_k \cup \Pi^1_k$ and that $P \in \Sigma^1_{k+1}$. To show that $P \in \Pi^1_{k+}$,, note that $P(x)$ holds if and only if

$$(Ez)(x = 2z \wedge Q(z)) \vee ((Ez_{z<x}(x = 2z + 1) \wedge (z)(x = 2z + 1 \supset \sim Q(z)))$$

(Cf. Rogers [1959]).

EXERCISES

5.16. This exercise will show the existence of a recursive, non-primitive recursive function.

1. Let $[\sqrt{n}\,]$ be the largest integer $\leqslant \sqrt{n}$. Show that $[\sqrt{n}\,]$ is defined by the recursion

$$\kappa(0) = 0$$
$$\kappa(n + 1) = \kappa(n) + \overline{sg}\,|(n + 1) - (\kappa(n) + 1)^2|$$

Hence, $[\sqrt{n}\,]$ is primitive recursive.

2. The function $\text{Quadrem}(n) = n \dot{-} [\sqrt{n}\,]^2$ is primitive recursive and represents the difference between n and the largest square $\leqslant$ n.

3. Let $\rho(x, y) = ((x + y)^2 + y)^2 + x$; $\rho_1(n) = \text{Quadrem}(n)$ and $\rho_2(n) = \text{Quadrem}([\sqrt{n}\,])$. These functions are primitive recursive. Prove:

(a) $\rho_1(\rho(x, y)) = x$ and $\rho_2(\rho(x, y)) = y$.

(b) $\rho(\rho_1(n), \rho_2(n)) = n$.

(c) p is a one-one function from w^2 onto w.

(d) $\rho_1(0) = \rho_2(0) = 0$ and

$$\left.\begin{array}{l}\rho_1(n + 1) = \rho_1(n) + 1 \\ \rho_2(n + 1) = \rho_2(n)\end{array}\right\} \text{if } \rho_1(n + 1) \neq 0$$

(e) Define for each $n \geqslant 3$, $\rho^n(x_1, \ldots, x_n) = \rho(\rho^{n-1}(x_1, \ldots, x_{n-1}), x_n)$. Let $\rho^2 = p$. Then each ρ^n is primitive recursive. Define $\rho^n_i(k) = \rho^{n-1}_i(\rho_1(k))$ for $1 \leqslant i \leqslant n - 1$, and $\rho^n_n(k) = \rho_2(k)$. Then each $\rho^n_i(1 \leqslant i \leqslant n)$ is primitive recursive, $\rho^n_i(\rho^n(x_1, \ldots, x_n)) = x_i$ and $\rho^n(\rho^n_1(k), \rho^n_2(k), \ldots, \rho^n_n(k)) = k$. Hence, ρ^n is a one-one mapping of ω^n onto w, and the ρ^n_i's are the corresponding "inverse" functions. The ρ^n's and ρ^n_i's are obtained from p, ρ_1, ρ_2 by substitution.

4. The recursion rule (V) (cf. page 138) can be limited to the form

$$\psi(x_1, \ldots, x_{n+1}, 0) = x_{n+1} \qquad (n \geqslant 0)$$
$$\psi(x_1, \ldots, x_{n+1}, y + 1) = \varphi(x_1, \ldots, x_{n+1}, y, \psi(x_1, \ldots, x_{n+1}, y))$$

Suggestion: given

$$\theta(x_1, \ldots, x_n, 0) = \gamma(x_1, \ldots, x_n)$$
$$\theta(x_1, \ldots, x_n, y + 1) = \delta(x_1, \ldots, x_n, y, \theta(x_1, \ldots, x„ \; y))$$

Define ψ as above, letting $\varphi(x_1, \ldots, x_{n+1}, y, z) = \delta(x_1, \ldots, x„ \; y, z)$. Then $\theta(x_1, \ldots, x_n, y) = \psi(x_1, \ldots, x_n, \gamma(x_1, \ldots, x_n), y)$.

5. Assuming p, p,, ρ_2 as additional initial functions, we can limit uses of the recursion rule (V) to the one-parameter form:

$$\psi(x, 0) = \alpha(x)$$
$$\psi(x, Y + 1) = \beta(x, y, \psi(x, y))$$

Hint: Let $n \geqslant 2$. Given

$$\theta(x_1, \ldots, x_n, 0) = \gamma(x_1, \ldots, x_n)$$
$$\theta(x_1, \ldots, x„ \; y + 1) = \delta(x_1, \ldots, x_n, y, \theta(x_1, \ldots, x_n, y)$$

Let $\eta(u, y) = \theta(\rho^n_1(u), \ldots, \rho^n_n(u), y)$. Define η by a permissible recursion.

6. Assuming p, ρ_1, ρ_2 as additional initial functions, we can use $\delta(y, \psi(x, y))$ instead of $\beta(x, y, \psi(x, y))$ in Part (5). (Hint: given

$$\psi(x, 0) = \alpha(x)$$
$$\psi(x, y + 1) = \beta(x, y, \psi(x, y))$$

let $\psi_1(x, y) = \rho(x, \psi(x, y))$. Then $x = \rho_1(\psi_1(x, y))$ and $\psi(x, y) = \rho_2(\psi_1(x, y))$. Define ψ_1 by an appropriate recursion.)

7. Assuming p, ρ_1, ρ_2 as additional initial functions, we can limit uses of the recursion rule (V) to the form

$$\psi(x, 0) = x$$
$$\psi(x, Y + 1) = \beta(y, \psi(x, y))$$

Hint: use Part (6). Given

$$\varphi(x, 0) = \alpha(x)$$
$$\varphi(x, Y + 1) = \beta(y, \varphi(x, y))$$

Define ψ as above. Then $\varphi(x, y) = \psi(\alpha(x), y)$.

8. Assuming p, ρ_1, ρ_2, $+, \cdot$, $\overline{sg}$, as additional initial functions, we can limit all uses of the recursion rule (V) to those with one parameter of the form

$$f(0) = 0$$
$$f(y + 1) = h(y, f(y))$$

Hint: given, by Part (7),

$$\psi(x, 0) = x$$
$$\psi(x, Y + 1) = \beta(y, \psi(x, y))$$

Let $f(n) = \psi(\rho_2(n), \rho_1(n))$. Then

$$
\begin{aligned}
f(0) &= \psi(\rho_2(0), \rho_1(0)) = \psi(0, 0) = 0 \\
f(n + 1) &= \psi(\rho_2(n + 1), \rho_1(n + 1)) \\
&= \begin{cases} \rho_2(n + 1) \text{ if } \rho_1(n + 1) = 0 \\ \beta(\rho_1(n + 1) \dot{-} 1, \psi(\rho_2(n + 1), \rho_1(n + 1) \dot{-} 1)) \text{ if } \rho_1(n + 1) \neq 0 \end{cases} \\
&= \begin{cases} \rho_2(n + 1) \text{ if } \rho_1(n + 1) = 0 \\ \beta(\rho_1(n), \psi(\rho_1(n), \rho_2(n))) \text{ if } \rho_1(n + 1) \neq 0 \end{cases} \\
&= \begin{cases} \rho_1(n + 1) \text{ if } \rho_2(n + 1) = 0 \\ \beta(\rho_1(n), f(n)) \text{ if } \rho_1(n + 1) \neq 0 \end{cases} \\
&= \rho_2(n + 1) \cdot \overline{sg}(\rho_1(n + 1)) + \beta(\rho_1(n), f(n)) \cdot sg(\rho_1(n + 1)) \\
&= h(n, f(n))
\end{aligned}
$$

(Note that sg is obtainable by a recursion of the appropriate kind.)

Then $\psi(x, y) = f(\rho(y, x))$.

9. All primitive recursive functions are obtainable from the initial functions Z, N, U_i^n, ρ, ρ_1, ρ_2, $+$, $\cdot$, $\overline{sg}$ by substitution and the recursion rule (V) in the form

$$\begin{aligned} f(0) &= 0 \\ f(y+1) &= h(y, f(y)) \end{aligned}$$

(Restatement of Part (8).)

10. In Part (9), $h(y, f(y))$ can be replaced by $h(f(y))$. Hint: given

$$\begin{aligned} f(0) &= 0 \\ f(y+1) &= h(y, f(y)) \end{aligned}$$

Let $g(u) = \rho(u, f(u))$, and $\varphi(w) = \rho(\rho_1(w) + 1, h(\rho_1(w), \rho_2(w)))$. Then

$$\begin{aligned} g(0) &= 0 \\ g(y+1) &= \varphi(g(y)) \end{aligned}$$

and

$$f(u) = \rho_2(g(u))$$

11. Show that the equations

$$\begin{aligned} \psi(n, 0) &= n + 1 \\ \psi(0, m+1) &= \psi(1, m) \\ \psi(n+1, m+1) &= \psi(\psi(n, m+1), m) \end{aligned}$$

define a recursive function. (Hint: show that ψ is Herbrand-Godel computable by the given equations, and then use Proposition 5.17.) In addition, prove:

(I) $\psi(n, m) > n$.

(II) ψ is monotonic in each variable, i.e., if $x < z$, then $\psi(x, y) < \psi(z, y)$ and $\psi(y, x) < \psi(y, z)$.

(III) $\psi(n, m+1) \geqslant \psi(n+1, m)$.

(IV) For every primitive recursive function $f(x_1, \ldots, x_n)$, there is some fixed m such that $f(x_1, \ldots, x_n) < \psi(\max(x_1, \ldots, x_n), m)$ for all $x_1, \ldots, x_n$. (Hint: prove this first for the initial functions Z, N, U_i^n, p, p,, ρ_2, $+$, $\cdot$, $\overline{sg}$, and then show that it is preserved by substitution and the recursion of Part (10) above.) Hence, for every primitive recursive function $f(x)$ of one argument, there is some m such that $f(x) < \psi(x, m)$ for all x.

(V) Prove that $\psi(x, x) + 1$ is recursive, but not primitive recursive. (Hint: Part (IV).)

For other proofs of the existence of recursive, non-primitive recursive functions, cf. Ackermann [1928], Peter [1935, 1951], R. Robinson [1948].

A very important metamathematical notion is that of recursively enumerable set. A set of natural numbers is called ***recursively enumerable*** (r.e.) if and only if it is either empty or the range of a recursive function. Intuitively, if we accept Church's Thesis, then a recursively enumerable set is a collection of natural numbers which is generated by some mechanical process.

PROPOSITION 5.20

(I) ***A set*** B ***is*** r.e. *if* ***and only if*** *x* $\in$ B ***is expressible in the form*** (Ey)R(x, y), ***where R is recursive. (We can also allow*** R ***here to be primitiue recursive.)***

(2) A set B is r.e. ***if and only if it is empty or the range of a partial recursive function (or of a primitiue recursive function).***

(3) A ***set*** B ***is*** r.e. *if* ***and only if it is the domain of definition of a partial recursive function.***

(4) A set B ***is recursive if and only if both*** B ***and its complement*** $\overline{B}$† ***are*** r.e.

(5) ***The set*** $\{x|(Ey)T_1(x, x, y))$ ***is*** r.e., ***but not recursive***.‡

PROOF.

(1) Assume B is r.e. If B is empty, then x E B $\equiv (Ey)(x \neq x \wedge y \neq y)$. If B is non-empty, it is the range of a recursive function φ. Then $x \in B \equiv (Ey)(\varphi(y) = x)$. Conversely, assume $x \in B \equiv (Ey)R(x, y)$. If B is empty, B is r.e. If B is non-empty, let k be a fixed element of B. Define:

$$\theta(z) = \begin{cases} k & \text{if} \sim R((z)_0, (z)_1) \\ (z)_0 & \text{if } R((z)_0, (z)_1) \end{cases}$$

Clearly, B is the range of 8, and 8 is recursive. (By Lemma 5.18, if R is recursive, $(Ey)R(x, y) \equiv (Ey)T_1(e, x, y)$ for some e; but $T_1(e, x, y)$ is primitive recursive.)

(2) Assume B is the range of a partial recursive function φ. If B is empty, then B is r.e. If B is non-empty, let k be a fixed element of B. Now, there is a number e such that $\varphi(x) = U(\mu y T_1(e, x, y))$. Let

$$\theta(z) = \begin{cases} U((z)_1) & \text{if } T_1(e, (z)_0, (z)_1) \\ k & \text{if} \sim T_1(e, (z)_0, (z)_1) \end{cases}$$

Then 8 is primitive recursive and B is the range of 8. Hence, B is r.e. This proof also shows that every non-empty r.e. set is the range of a primitive recursive function.

(3) Assume B r.e. If B is empty, B is the domain of the partial recursive function $\mu y(x + y + 1 = 0)$. If B is non-empty, B is the range of a recursive function f. Let g be the partial recursive function such that $g(y) = \mu x(f(x) = y)$. Then B is the domain of g. Conversely, assume B is the domain of a partial recursive function φ. Then there is a number e such that $\varphi(x) = U(\mu y T_1(e, x, y))$. Hence $\varphi(x) = z \equiv (Ey)(T_1(e, x, y) \wedge U(y) = z)$. But $x \in B \equiv (Ez)(\varphi(x) = z)$. So, x E B if and only if $(Ez)(Ey)(T_1(e, x, y) \wedge U(y) = z)$, and the latter is equivalent to $(Eu)(T_1(e, x, (u),) \wedge U((u)_1) = (u)_0)$; moreover, $T_1(e, x, (u),) \wedge U((u)_1) = (u)_0$ is recursive. Thus, by (1), B is r.e.

(4) From (1) and Proposition 5.19(4(d)). (The intuitive meaning of Part (4) is the following: if there are mechanical procedures for generating B and $\overline{B}$, then to

†I.e., $\omega - B$, where ω is the set of non-negative integers.

‡Remember that $\{x|P(x)\}$ stands for the set of all x such that P(x) holds.

determine whether any number n is in B we need only wait until n is generated by one of the machines and then observe which machine produced it.)

(5) From (1) and (4), and Proposition 5.19(3).

EXERCISES

Prove:

5.17. The inverse image of an r.e. set under a recursive function is r.e. (i.e., if f is recursive and B r.e., then $\{x|f(x) \in B\}$ is r.e.). The inverse image of a recursive set under a recursive function is recursive. The image of an r.e. set under a recursive function is r.e., but the image of a recursive set under a recursive function is not necessarily a recursive set.

5.18. An infinite set is recursive if and only if it is the range of a strictly increasing recursive function. (g is ***strictly increasing*** if $x < y$ implies $g(x) < g(y)$.)

5.19. Any infinite set is r.e. if and only if it is the range of a one-one recursive function.

5.20. Every infinite r.e. set contains an infinite recursive subset.

5.21. If A and B are r.e. sets, so are $A \cup B$ and $A \cap B$, but there exists an r.e. set A such that $o - A$ is not r.e.

5.22. Show that the assertion

> (‡) A set B is r.e. if and only if B is effectively enumerable (i.e., there is a mechanical procedure for generating all the elements of B)

is equivalent to Church's Thesis.

5.23. Let **K** be a first-order theory with equality containing all the symbols of formal number theory S. A relation $B(x_1, \ldots, x_n)$ is said to be ***weakly expressible*** in ***K*** if and only if there is a wf $\mathscr{B}(x_1, \ldots, x_n)$ of K such that, for any natural numbers $k_1, \ldots, k_{,,}$ $B(k_1, \ldots, k_n)$ if and only if $\vdash_K \mathscr{B}(\bar{k}_1, \ldots, \bar{k}_n)$.

(a) If K is consistent, show that every relation expressible in K is weakly expressible in K.

(b) If every recursive relation is expressible in K and K is o-consistent, prove that every r.e. set is weakly expressible in K. (Remember that, when we refer here to an r.e. set B, we mean the corresponding relation "$x \in B$".)

(c) If K is such that the relations (a)–(d) of Propositions 3.25–3.26 are recursive, prove that any set which is weakly expressible in K is r.e.

(d) If formal number theory S is o-consistent, prove that a set B is r.e. if and only if B is weakly expressible in S.

5.24. (a) (Craig [1953]) Let K be a first-order theory such that the set T_k of Gödel numbers of theorems of K is r.e. Show that K is recursively axiomatizable.

(b) For any wf $\mathscr{C}$ of formal number theory S, let $\mathscr{C}\#$ represent its translation into axiomatic set theory NBG (cf. p. 204). Let K be the set of wfs $\mathscr{C}$ such that $\vdash_{NBG}\mathscr{C}$ #. Prove that K is a (proper) recursively axiomatizable extension of S. (However, no "natural" set of axioms for K is known.)

By Proposition 5.20(3), a set is r.e. if and only if it is the domain ζ_n of the partial recursive function $U(\mu y T_1(n, x, y))$ for some n; hence, $x \in \zeta_n$ if and only if $(Ey)T_1(n, x, y)$. We call n an ***index*** of the r.e. set ζ_n. We thus have an enumeration (with repetitions) $\zeta_0, \zeta_1, \ldots$ of all r.e. sets.

An example of an r.e. set which is not recursive is the set of all x such that $(Ey)T_1(x, x, y)$. That it is r.e. follows from Proposition 5.20(2), and that it is not recursive follows from Proposition 5.19(3). By Proposition 5.20(4), it also follows that $(y) \sim T_1(x, x, y)$ is not r.e.

EXERCISES

5.25. A set B is called ***creative*** if and only if B is r.e. and there is a partial recursive function φ such that, for any n, if 5, $\subseteq \bar{B}$, then $\varphi(n) \in B - \zeta_n$. Prove that $\{x|(Ey)T_1(x, x, y))$ is creative. Show that every creative set is non-recursive.

5.26. A partial recursive function φ is called ***potentially recursive*** if and only if there is a recursive function ψ such that $\varphi(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_n)$ whenever $\varphi(x_1, \ldots, x_{})$ is defined. Prove that $\mu y T_1(x, x, y)$ is not potentially recursive.

5.27.^{D} **A** set B is called ***simple*** if and only if B is r.e., B is infinite, and B contains no infinite r.e. set. Every simple set is non-recursive. Show that a simple set exists.

5.28. A ***recursive permutation*** is a one-one recursive function from o onto o. Sets X and Y are called ***isomorphic*** (written $X \cong Y$) if there is a recursive permutation which maps X onto Y. Prove:

^{A}(a) The recursive permutations form a group under the operation of composition.

(b) $\cong$ is an equivalence relation.

(c) If X is recursive (r.e., creative, simple) and $X \cong Y$, then Y is recursive (r.e., creative, simple).

Myhill [1955] has shown that any two creative sets are isomorphic. (Also cf. Bernays [1957].)

5.29. X is ***many-one reducible*** to Y (written X R, Y) if there is a recursive function f such that $u \in X$ if and only if $f(u) \in Y$. X and Y are called ***many-one equivalent*** (written $X \equiv_m Y$) if X R, Y and Y R_m X. X is ***one-one reducible*** to **Y** (written X R_1 Y) if there is a one-one recursive function f such that $u \in X$ if and only if $f(u) \in Y$. X and Y are called ***one-one equivalent*** (written $X \equiv_1 Y$) if X R_1 **Y** and Y R, X. Prove:

(a) $\equiv_m$ and $\equiv_1$ are equivalence relations.

(b) If X is creative, Y is r.e., and X R_m Y, then Y is creative. It can be shown (Myhill [1955]) that if X is creative and Y is r.e. then Y R_mX.

(c) (Myhill [1955]) If X R_1 Y then X R_mY, and if $X \equiv_1 Y$ then $X \equiv_m Y$. However, many-one reducibility does not imply one-one reducibility, and many-one equivalence does not imply one-one equivalence. (Hint: let **X** be a simple set, Z an infinite recursive subset of X, and $Y = X - Z$. Then X R_1 Y, Y R_m X, but not (Y R_1 X).) It can be proved that $X \equiv_1 Y$ if and only if $X \cong Y$.

5.30. (Dekker [1955]) X is said to be ***productive*** if there is a partial recursive function f such that if $\zeta_n \subseteq X$ then $f(n) \in X - \zeta_n$. Prove: (a) If X is productive, then X is not r.e.; hence, both X and $\bar{X}$ are infinite. ^{D}(b) If X is productive, then $\bar{X}$ has an infinite r.e. subset. Hence, if X is productive, $\bar{X}$ is not simple. (c) If X is r.e., then X is creative if and only if $\bar{X}$ is productive. ^{D}(d) There exist $2^{\aleph_0}$ productive sets.

531. (Dekker-Myhill [1960]) X is ***recursively equivalent*** to ***Y*** (written $X \sim Y$) if there is a one-one partial-recursive function which maps X onto Y. Prove: (a) $\sim$ is an equivalence relation. ^{D}(b) X is said to be ***immune*** if X is infinite and X has no infinite r.e. subset. X is said to be ***isolated*** if X is not recursively equivalent to a proper subset of X. (The isolated sets may be considered the recursive counterparts of the Dedekind-finite sets.) An infinite set is isolated if and only if it is immune. ^{D}(c) There exist $2^{\aleph_0}$ immune sets.

Recursively enumerable sets are also important because, if we assume Church's Thesis, the set T_K of Gödel numbers of theorems of any axiomatizable first-order theory K is r.e. (The same holds true of arbitrary formal axiomatic systems.) For, the relation Pf(y, x) (y is the Gödel number of a proof in K of a wf with Gödel number x, cf. p. 156) is recursive, if the set of Gödel numbers of the axioms is recursive, i.e., if the theory is axiomatic and Church's Thesis holds. Hence, $x \in T_K$ if and only if (Ey)Pf(y, x), and therefore, T_K is r.e. If we accept Church's Thesis, then K is effectively decidable if and only if the r.e. set T_K is recursive. We showed in Corollary 3.41 that every consistent extension K of the theory RR is recursively undecidable, i.e., T_K is not recursive.

Much more general results along these lines can be proved (cf. Smullyan [1961], Feferman [1957], Putnam [1957], Ehrenfeucht and Feferman [1960], Myhill [1955]). For example, (1) if every recursive set is expressible in K, then K is essentially recursively undecidable, i.e., for every consistent extension of K, T_K is not recursive (cf. Exercise 5.33 below); (2) for any consistent first-order theory with equality K in which every recursive function is representable and which satisfies (i') and (ii) of p. 162, the set T_K is creative. (We assume that K has among its terms the numerals $\bar{0}, \bar{1}, \bar{2}, \ldots$.) For further study of r.e. sets, cf. Post [1944] and Rogers [1967].

EXERCISES

532. Given a set A of natural numbers, define A* as follows: $u \in A^*$ if and only if u is a Gödel number of a wf $\mathscr{B}(x_1)$ and the Gödel number of $\mathscr{B}(\bar{u})$ is in A. Prove that, if A is recursive, then A* is recursive.

533. Let K be a consistent theory having the same symbols as S.

(a) Let T_K be the set of Gödel numbers of theorems of K. Prove that $(\bar{T}_K)^\star$ is not weakly expressible in K (cf. Exercise 5.23, p. 262).

(b) If every recursive set is weakly expressible in K, show that K is recursively undecidable.

(c) If every recursive set is expressible in K, prove that K is essentially recursively undecidable.

4. Undecidable Problems

A general class of problems is said to be undecidable if and only if there is no general effective (or mechanical) procedure for solving each problem in the given class. For example, given any polynomial in any number of variables with integral coefficients, is there a set of integral values of the variables for which the polynomial has the value 0? We may be able to answer this question for certain special polynomials, but it turns out that there is no general procedure which will solve this problem for all polynomials (cf. Matiyasevich [1970]).

If we can arithmetize the formulation of a general class of problems and thus assign to each problem a natural number, then this class is undecidable if and only if there is no effectively computable function h such that, if n is the number of a given problem, then h(n) gives the solution of the problem. If we accept Church's Thesis (as we shall do-in this section) the function h has to be partial recursive, and we then have a precise mathematical question. Examples of important mathematical decision problems which have been solved (negatively) are the word problem for semi-groups (Post [1947], Kleene [1952], § 71), and the very difficult word problem for groups (Boone [1959], Novikov [1955], Britton [1958], Higman [1961]). In addition, the decision problem for various first-order theories has been shown to have a negative solution, i.e., the general problem as to whether any given wf is provable in the theory is undecidable (cf. Corollary 3.36, Corollary 3.37, Proposition 3.41, Corollary 3.45, Proposition 3.46). We shall now present some more examples of undecidable problems.

The sequence of functions $\psi_n(x) = U(\mu y T_1(n, x, y))$ gives an enumeration of all partial recursive functions of one variable. Is there an effective procedure to determine for any n whether ψ_n is recursive (i.e., whether ψ_n is defined for all x)? A positive answer is equivalent to the recursiveness of the set A of all numbers n such that ψ_n is recursive. We shall show that A is not even r.e. Assume A r.e., and let h be a recursive function with range A. Define a new function $f(x) = [\psi_{h(x)}(x)] + 1 = [U(\mu y T_1(h(x), x, y))] + 1$. Hence, f is recursive and so there is some m such that $f = \psi_m$ and $m \in A$. Then $\psi_m(x) = \psi_{h(x)}(x) + 1$. Since $m \in A$, there is some k such that $m = h(k)$. Taking $x = k$, we have $\psi_m(k) = \psi_m(k) + 1$, which is a contradiction. Thus, there is no effective procedure by which we can tell whether any system of equations determines a recursive function.

We can obtain a "local" form of this result. Is there an effective procedure determining for any given m, n whether $\psi_n(m)$ is defined? The answer is negative. For, assume that $\theta(x, y)$ is a recursive function such that

$$\theta(x, y) = \begin{cases} 0 & \text{if } \psi_x(y) \text{ is defined} \\ 1 & \text{if } \psi_x(y) \text{ is not defined} \end{cases}$$

Now, let $\alpha(z) = \mu y(\theta(z, z) = 1 \wedge y = y)$. Clearly,

$$\alpha(z) = \begin{cases} 0 & \text{if } \psi_z(z) \text{ is undefined} \\ \text{undefined} & \text{if } \psi_z(z) \text{ is defined} \end{cases}$$

But a is partial recursive, and so, a = ψ_k for some k. Then

$$\psi_k(k) = \alpha(k) = \begin{cases} 0 & \text{if } \psi_k(k) \text{ is undefined} \\ \text{undefined} & \text{if } \psi_k(k) \text{ is defined} \end{cases}$$

which is a contradiction. (Other undecidable problems can be found in Rogers [19671.)

EXERCISES

5.34. Given a Turing machine T, can one effectively decide, given any instantaneous description ***a,*** whether or not there is a computation of T beginning with ***a?*** (Halting problem for T.) Show that there is a Turing machine with undecidable halting problem. For further discussion of this and similar problems, cf. Davis [1958], Chapter 5.

535. Prove: There is no normal algorithm $\mathfrak{B}$ over M = {1, *} such that $\mathfrak{B}$ is applicable to exactly those words $\bar{n}$ such that n is an index of a normal algorithm $\mathfrak{A}$ over M such that $\mathfrak{A}$ is not applicable to $\bar{n}$.

For further examples of undecidable problems in the theory of algorithms, cf. Markov [1954], Chapter V. Because of the essential equivalence of normal algorithms, Turing machines, and Herbrand-Godel systems of equations, any undecidability result established in terms of one of these approaches usually can be translated into corresponding results for the other two.

536. The function f such that

$$f(x) = \begin{cases} 0 & \text{if } \psi_x(x) \text{ is defined} \\ 1 & \text{otherwise} \end{cases}$$

is not recursive.

5.37.^{D} Show that there is a recursive function $\eta(x)$ such that, for any x, $\eta(x)$ is the index of the partial recursive function v, where

$$v(y) = \begin{cases} 0 & \text{if } \psi_x(x) \text{ if defined} \\ \text{undefined} & \text{if } \psi_x(x) \text{ is undefined} \end{cases}$$

5.38.^{D} (Rogers [1967]) Show that the following relations are not recursive (and, therefore, by Church's Thesis, are undecidable).

(a) y is in the range of ψ_x.

(b) $\psi_x(y) = z$.

(c) $\psi_x = \psi_y$. (Hint: use 5.37 and 5.36.)

The reader should not get the impression that all decision problems have a negative solution. In Chapter 1 it was shown that truth tables provide an effective procedure to determine whether any given statement form is a tautology. On p. 170, it was shown that the pure monadic predicate calculus is effectively decidable (cf. Ackermann [1954] and Suranyi [1959] for many positive results of a similar kind). Presburger [1929] showed that the first-order theory obtained from first-order theory number theory S by omitting the multiplication symbol and the recursion axioms for multiplication is decidable (cf. p. 134, Exercise 3.7); Szmielew [1955] proved the decidability of the first-order theory of abelian groups; and Tarski [1951] established the decidability of the first-order theory of real-closed fields, which is the elementary part of the theory of real numbers.

BIBLIOGRAPHY

Listed here are not only books and papers mentioned in the text but also other material which will be helpful in a further study of mathematical logic. Additional references may be found in the reviews in the *Journal of Symbolic Logic* and *Mathematical Reviews*. We shall use the following abbreviations.

AML for *Annals of Mathematical Logic.*
AMS for *American Mathematical Society.*
Arch for *Archiv fur mathematische Logik und Grundlagenforschung.*
FM for *Fundamenta Mathematicae.*
JSL for *Journal of Symbolic Logic.*
N-H for *North-Holland Publishing Company.*
ZML for *Zeitschrift fur mathematische Logik und Grundlagen der Mathematik.*

Ackermann, W.
1928. Zum Hilbertschen Aufbau der reelen Zahlen, *Math. Annalen*, 99, 118–133.
1940. Zur Widerspruchsfreiheit der Zahlentheorie, *Math. Annalen*, 117, 162–194.
1954. *Solvable Cases of the Decision Problem*, *N-H*.
See Hilbert, D., and W. Ackermann.

Asser, G.
1955. Das Reprasentantenproblem im Prädikatenkalkül der ersten Stufe mit Identitat, *ZML*, 1, 252–263.
1959. Turing-Maschinen und Markowsche Algorithmen, *ZML*, 5, 346–365.

Bachmann, H.
1955. *Transfinite Zahlen.* Springer.

Bar-Hillel, Y. See Fraenkel, A., and Y. Bar-Hillel.

Barwise, J.
1975. *Admissible Sets and Structures.* Springer.
1977. (Editor) *Handbook of Mathematical* Logic. Springer.

Bell, J. L., and A. B. Slomson.
1969. *Models and Ultraproducts. N-H.*

Bernays, P.
1937–1954. A system of axiomatic set theory. *JSL*. I. Vol. 2 (1937), 65–77; II. Vol. 6 (1941), 1–17; III. Vol. 7 (1942), 65–89; IV. Vol. 7 (1942), 133–145; V. Vol. 8 (1943), 89–106; VI. Vol. 13 (1948), 65–79; VII. Vol. 19 (1954), 81–96.

1957. Review of Myhill [1955], *JSL*, 22 73–76.

1958. *Axiomatic Set Theory, N-H.*

1961. Zur Frage der Unendlichkeitsschemata in der axiomatischen Mengenlehre, *Essays on the Foundationr of Mathematics,* Jerusalem, 3–49.

See Hilbert, D., and P. Bernays.

Bernstein, A. R.

1973. Non-standard analysis, *Studies in Model Theory,* Math. Assoc. of America, 35–58.

Beth, E.

1951. A Topological Proof of the Theorem of Löwenheim-Skolem-Gödel, *Indag. Math.,* 13, 436–444.

1953. Some consequences of the theorem of Löwenheim-Skolem-Gödel-Malcev, *Indag. Math.,* 15, 66–71.

1959. *The Foundationr of Mathematics, N-H.*

Bezboruah, A., and J. C. Shepherdson.

1976. Gödel's second incompleteness theorem for Q, *JSL,* 41, 1976, 503–512.

Birkhoff, G.

1948. *Lattice Theory.* AMS Colloquium Publications.

Bishop, E.

1967. *Foundationr of Constructive Analysis.* McGraw-Hill.

1970. Mathematics as a numerical language, *Intuitionism and Proof Theory, N-H,* 53–71.

Boffa, M.

1969. Sur la theorie des ensembles sans axiome de fondement, *Bull. Soc. Math. Belgique,* 21, 16–56.

Boone, W.

1959. The Word Problem, *Annals of Math.,* 70, 207–265.

Bourbaki, N.

1947. *Algebre.* Livre II, Chap. II, Hermann, Paris.

Bridge, J.

1977. *Beginning Model Theory.* Oxford.

Britton, J. L.

1958. The Word Problem for Groups. *Proc. London Math. Soc.,* 8, 493–506.

Bruijn, N. G. de, and P. Erdos.

1951. A colour problem for infinite graphs and a problem in the theory of relations, *Indag. Math.,* 13, 369–373.

Carnap, R.

1934. *The Logical Syntax of Language.* Routledge & Kegan Paul. (English translation, 1937).

Chang, C. C., and H. J. Keisler

1966. *Continuous Model Theory.* Princeton *U.* Press.

1973. *Model Theory. N-H.*

Cherlin, G.

1976. *Model Theoretic Algebra, Selected Topics.* Springer.

Chuquai, R.

1972. Forcing for the impredicative theory of classes, *JSL,* 37, 1–18.

Church, A.

1936a. A note on the Entscheidungsproblem, *JSL,* 1, 40–41; Correction, ibid., 101–102.

1936b. An unsolvable problem of elementary number theory, *Am. J. Math.,* 58, 345–363.

1940. A formulation of the simple theory of types. *JSL,* 5, 56–68.

1941. *The Calculi of Lambda-Conversion,* Princeton, Second printing 1951.

1956. *Introduction to Mathematical Logic, I,* Princeton.

Cohen, P. J.

1963. A minimal model for set theory, *Bull. AMS,* 69, 537–540.

1963–64. The independence of the continuum hypothesis, *Proc. Natl. Acad. Sci. USA,* 50, 1143–1148; 51, 105–110.

1966. *Set Theory and the Continuum Hypothesis.* Benjamin.

1969. Decision procedures for real and p-adic fields, *Comm. Pure and Applied Math.,* 22, 131–151.

Cohn, P. M.

1965. *Universal Algebra.* Harper & Row.

Collins, G. E., and J. D. Halpern

1970. On the interpretability of arithmetic in set theory, *Notre Dame J. Formal Logic,* 11, 477–483.

Comfort, W. W., and S. Negrepontis

1974. *The Theory of Ultrafilters.* Springer.

Cowen R.

1973. Some combinatorial theorems equivalent to the prime ideal theorem, *Proc. AMS,* 41,268–273.

Craig, W.

1953. On axiomatizability within a system, *JSL,* 18, 30–32.

Crossley, J. N.

1969. *Constructiw Order Types. N-H.*

Curry, H. B.

1963. *Foundationr of Mathematical Logic.* McGraw-Hill.

Curry, H. B., and R. Feys

1958. *Combinatory Logic. N-H.*

Da Costa, N. C. A.

1965. On two systems of set theory, *Proc. Koninkl. Nederl. Akad. Wetensch., A,* 68, 95–99.

Davis, M.

1958. *Computability and Unsolvability.* McGraw-Hill.

1965. (Editor) *The Undecidable: Basic Papers on Undecidable Propositions, Unsolvable Problem, and Computable Functionr.* Raven.

1973. Hilbert's tenth problem is unsolvable, *Amer. Math. Monthly,* 80, 233–269.

1977. *Applied Nonstandard Analysis.* Wiley.

Dedekind, R.

1901. *Essays on the Theory of Numbers.* Open Court. (Dover 1963).

Dekker, J. C. E.

1953. Two notes on recursively enumerable sets, *Proc. AMS,* 4, 495–501.

1955. Productive Sets, *Trans. AMS,* 78, 129–149.

1966. *Les Fonctionr Combinatoires et les Isols.* Gauthiers-Villars.

Dekker, J. C. E., and J. Myhill
1960. ***Recursive Equivalence Types.*** Univ. Calif. Publ. Math., 3, 67–213.
Detlovs, V. K.
1958. Equivalence of normal algorithms and recursive functions, ***Tr. Mat. Inst. Steklov, LII,*** 75–139 (in Russian).
Devlin, K. J.
1973. ***Aspects of Constructibility.*** Springer.
1977. ***The Axiom of Conrtructibility.*** Springer.
Dickmann, M.
1976. ***Large Infinitary Languages. N-H.***
Di Paola, ***R.***
1967. Some theorems on extensions of arithmetic, ***JSL,*** 32, 180–189.
Drake, F.
1974. ***Set Theory. N-H.***
Dreben, B.
1952. On the completeness of quantification theory, ***Proc. Natl. Acad. Sci. USA,*** 38, 1047–1052.
Dummett, M.
1977. ***Elements of Intuitionism.*** Oxford.
Easton, W. B.
1970. Powers of regular cardinals, ***AML,*** 1, 139–178.
Ehrenfeucht, A.
1957. On theories categorical in power, ***FM,*** 44, 241–248.
1958. Theories having at least continuum non-isomorphic models in each infinite power (abstract), ***Notices AMS,*** 5, 680.
1961. An application of games to the completeness problem for formalized theories, ***FM,*** 49, 129–141.
Ehrenfeucht, A., and S. Feferman
1960. Representability of recursively enumerable sets in formal theories, ***Arch.,*** 5, 37–41.
Ehrenfeucht, A., and **A.** Mostowski
1957. Models of axiomatic theories admitting automorphisms, ***FM,*** 43, 50–68.
Eilenberg, S., and C. C. Elgot
1970. ***Recursiveness.*** Academic.
Eisenberg, M.
1971. ***Axiomatic Theory of Sets and Classes.*** HRW.
Eklof, P. C., and E. R. Fischer
1972. The elementary theory of abelian groups, ***AML,*** 4, 115–171.
Elgot, C. C. See Eilenberg, S., and C. C. Elgot.
Engeler, E.
1968. ***Formal Languages: Automata & Structures.*** Markham.
1973. ***Introduction to the Theory of Computability.*** Academic.
1975. On the solvability of algorithmic problems, ***Logic Colloquium*** '73, Springer, 231–251.
Erdos, P. See Bruijn, N. G. de, and P. Erdos.
Erdos, P., and **A.** Tarski
1961. On some problems involving inaccessible cardinals. ***Essays on the Foundations of Mathematics,*** Magnes, Jerusalem, 50–82.

Feferman, S.
1960. Arithmetization of metamathematics in a general setting, ***FM,*** 49, 35–92.
1965. Some applications of the notion of forcing and generic sets, ***FM,*** 56, 325–345.
Feferman, S., and A. Ehrenfeucht. See Ehrenfeucht, A., and S. Feferman.
Felgner, U.
1971a. ***Models of ZF-Set Theory.*** Springer.
1971b. Comparison of the axioms of local and universal choice, ***FM,*** 71, 43–62.
1976. Choice functions on sets and classes, ***Sets and Classes, N-H.,*** 217–255.
Feys, R., and H. B. Curry. See Curry, H. B., and R. Feys.
Fischer, E. R., and P. C. Eklof. See Eklof P. C., and E. R. Fischer.
Fraenkel, A., and Y. Bar-Hillel
1958. ***Foundations of Set Theory. N-H.***
Frayne, T., A. Morel, and D. Scott
1956. Reduced direct products, ***FM,*** 51, 195–228.
Freidberg, R.
1957. Two recursively enumerable sets of incomparable degrees of unsolvability, ***Proc. Natl. Acad. Sci. USA,*** 43, 236–238.
Friedman, H.
1971. Higher set theorv and mathematical practice, ***AML,*** 2, 325–357.
1975. One hundred and two problems in mathematical logic, ***JSL,*** 40, 113–129.
Friedman, J.
1969. Proper classes as members of extended sets, ***Math. Ann.,*** 183, 232–246.

Gabriel, P.
1962. Des categories abeliennes, ***Bull. Soc. Math. France, 90,*** 323–448.
Gaifman, H.
1972. A note on models and submodels of arithmetic, ***Conf. in Math. Logic-London*** 1970, Springer, 128--144.
1976. Models and types of Peano arithmetic, ***AML,*** 9, 223–306.
Galler, B. A.
1957. Cylindric and polyadic algebras, ***Proc. AMS,*** 8, 176–183.
Geiser, J. R.
1970. Nonstandard analysis, ***ZML,*** 16, 297–318.
Gentzen, G.
1936. Die Widerspruchsfreiheit der reinen Zahlentheorie, ***Math. Ann.*** 112, 493–565.
1938. Neue Fassung des Widerspruchsfreiheitsbeweises fur die reine Zahlentheorie, ***Forschungen zur Logik,*** 4, 5–18.
1969. ***Collected Papers*** (Edited by M. E. Szabo), ***N-H.***
Gödel, K.
1930. Die Vollstandigkeit der Axiome des logischen Funktionenkalküls, ***Monatsh, Math. Phys.,*** 37, 349–360.
1931. Ueber formal unentscheidbare Satze der Principia Mathematica und verwandter Systeme, I, ibid., 38, 173–198. (English translation in Davis [1965]).
1933. Zum intuitionistischen Aussagenkalkül; Zur intuitionistischen Arithmetik und Zahlentheorie, ***Ergeb. Math. Koll.,*** 4, 34–38 and 40.
1936. Über die Länge der Beweise, ibid., 7, 23–24.
1938. The consistency of the axiom of choice and the generalized continuum hypothesis, ***Proc. Natl. Acad. Sci. USA,*** 24, 556–557.

1939. Consistency proof for the generalized continuum hypothesis, ibid., 25, 220–226.

1940. *The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory,* Princeton.

1947. What is Cantor's continuum problem? *Amer. Math. Monthly,* 54, 515–525.

1958. Über eine bisher noch nicht benutzte Erweiterung des finiten Standpunktes, *Dialectica*, 12, 280–287.

Gratzer, G.

1968. *Universal Algebra.* Van Nostrand.

Grzegorczyk, A., A. Mostowski, and C. Ryll-Nardzewski

1958. The classical and the a-complete arithmetic, *JSL,* 23, 188–206.

Hajek, P. See Vopenka, P.

Halmos, P.

1960. *Naive Set Theory.* Van Nostrand.

1962. *Algebraic Logic.* Chelsea.

1963. *Lectures on Boolean Algebra.* Van Nostrand. (Springer 1977)

Halmos, P., and H. Vaughn

1950. The marriage problem, *Amer. J. Math.,* 72, 214–215.

Halpern, J. D.

1964. The independence of the axiom of choice from the Boolean prime ideal theorem, *FM,* 55, 57–66.

Halpern, J. D., and G. E. Collins. See Collins, G. E., and J. D. Halpern.

Halpern, J. D., and P. E. Howard

1970. Cardinals m such that 2m = m, *Proc. AMS,* 26, 487–490.

Halpern, J. D., and A. Levy

1971. The Boolean prime ideal theorem does not imply the axiom of choice, *Proc. Symp. in Pure Math.,* 13, *AMS,* 83–134.

Hanf, W.

1965. Models-theoretic methods in the study of elementary logic, *The Theory of Models, N-H,* 132–145.

Hartogs, F.

1915. Ueber das Problem der Wohlordnung, *Math. Ann.,* 76, 438–443.

Hasenjaeger, G.

1952. Über ω-Unvollständigkeit in der Peano-Arithmetik, *JSL,* 17, 81–97.

1953. Eine Bemerkung zu Henkin's Beweis fur die Vollstandigkeit des Prädikatenkalkuls der ersten Stufen, *JSL,* 18, 42–48.

Hasenjaeger, G., and H. Scholz

1961. *Grundzüge der mathematischen Logik,* Springer.

Hatcher, W.

1968. *Foundations of Mathematics.* Saunders.

Hechler, S.

1973. Powers of singular cardinals and a strong form of the negation of the generalized continuum hypothesis, *ZML,* 19, 83–84.

Heijenoort, J. van

1967. (Editor) *From Frege to Gödel (A Source Book in Mathematical Logic, 1879–1931).* Harvard.

Hellman, M.

1961. A short proof of an equivalent form of the Schroder-Bernstein Theorem, *Arner. Math. Monthly,* 68, 770.

Henkin, L.

1949. The completeness of the first-order functional calculus, *JSL,* 14, 159–166.

1950. Completeness in the theory of types, ibid., 15, 81–91.

1953. Some interconnections between modern algebra and mathematical logic, *Trans. Am. Math. Soc.,* 74,410–427.

1954. Boolean representation through propositional calculus, *FM,* XLI, 89–96.

1955a. The representation theorem for cylindrical algebras, *Mathematical Interpretations of Formal Systems, N-H,* 85–97.

1955b. On a theorem of Vaught, *JSL,* 20, 92–93.

Henkin, L., J. D. Monk, and A. Tarski

1971. *Cylindric Algebras, I. N-H.*

Herbrand, J.

1930. Recherches sur la theorie de la demonstration, *Travaux de la Soc. des Sci. et des Lettres de Varsovie,* III, 33, 33–160.

1971. *Logical Writings.* Harvard & Reidel.

Hermes, H.

1965. *Enumerability, Decidability, Computability.* Springer.

Heyting, A.

1956. *Intuitionism.* N-H.

Higman, G.

1961. Subgroups of finitely presented groups, *Proc. Roy. Soc.,* Ser. *A.* 262, 455–475.

Hilbert, D., and W. Ackermann

1950. *Principles of Mathematical Logic,* Chelsea.

Hilbert, D., and P. Bernays

1934, 1939. *Grundlagen der Mathematik,* Vol. I (1934), Vol. II (1939), Springer.

Hintikka, K. J.

1954. An application of logic to algebra, *Math. Scand.,* 2, 243–246.

1955a. Form and Content in Quantification Theory, *Acta Phil. Fennica,* 11–55.

1955b. Notes on the Quantification Theory, Comment. Phys.-Math., *Soc. Sci. Fennica,* 17, 1–13.

Hirschfeld, J., and W. H. Wheeler

1975. *Forcing, Arithmetic, Division Rings.* Springer.

Howard, P. E., and J. D. Halpern. See Halpern, J. D., and P. E. Howard.

Isbell, J.

1966. Structure of categories, *Bull. AMS,* 72, 619–655.

Jaśkowski, S.

1936. Recherches sur le systeme de la logique intuitioniste, *Act. Sci. Ind.,* 393, Paris, 58–61.

Jech, T.

1971. *Lectures in Set Theory.* Springer.

1973. *The Axiom of Choice. N-H.*

Jensen, R. B.

1967. *Modelle der Mengenlehre.* Springer.

Jeroslow, R. G.

1971. Consistency statements in formal theories, ***FM,*** 72, 17–40.

1972. On the encodings used in the arithmetization of mathematics, Unpublished manuscript.

1973. Redundancies in the Hilbert-Bernays derivability conditions for Gödel's second incompleteness theorem, ***JSL,*** 38, 359–367.

Jonsson, B.

1962. Algebraic extensions of relational systems, ***Math. Scandinavica,*** 11, 179–205.

Kalmár, L.

1936. Zuruckführung des Entscheidungsproblems auf den Fall von Formeln mit einer einziger binaren Funktionsvariablen, ***Comp. Math.,*** 4, 137–144.

Kamke, E.

1950. ***Theory of Sets.*** Dover.

Karp, C.

1964. ***Languages with Expressions of Infinite Length. N-H.***

1967. *A* proof of the relative consistency of the continuum hypothesis, ***Sets, Models, and Recursion Theory, N-H,*** 1–32.

Keisler, H. J.

1971. ***Model Theory for Infinitary Logic. N-H.***

1976. ***Elementary Calculus: An Approach Using Infinitesimals,*** Prindle, Weber, & Schmidt.

Keisler, H. J., and C. C. Chang. See Chang, C. C. & H. J. Keisler.

Keisler, H. J., and M. Morley

1968. Elementary extensions of models of set theory, ***Israel J. of Math., 6,*** 49–65.

Keisler, H. J., and A. Tarski

1964. From accessible to inaccessible cardinals, ***FM,*** 53, 225–308.

Kelley, J.

1955. ***General Topology.*** Van Nostrand.

Kemeny, J.

1948. Models of logical systems, ***JSL,*** 13, 16–30.

1958. Undecidable problems of elementary number theory, ***Math. Ann.,*** 135, 160–169.

Kent, C. F.

1973. The relation of A to Prov $\ulcorner A \urcorner$ in the Lindenbaum sentence algebra, ***JSL,*** 38, 295–298.

Kleene, S. C.

1936a. General Recursive Functions of Natural Numbers, ***Math. Ann.,*** 112, 727–742.

1936b. λ-definability and recursiveness, ***Duke Math. J.,*** 2, 340–353.

1943. Recursive predicates and quantifiers, ***Trans. Amer. Math. Soc.,*** 53, 41–73.

1945. On the interpretation of intuitionistic number theory, ***JSL,*** 10, 109–124.

1952. ***Introduction to Metamathematics,*** Van Nostrand.

1955a. Hierarchies of number-theoretic predicates, ***Bull. Amer. Math. Soc.,*** 61, 193–213.

1955b. Arithmetical predicates and function quantifiers, ***Trans. Amer. Math. Soc.,*** 79, 312–340.

1976. The work of Kurt Gödel, ***JSL,*** **41, 761–778.**

Kleene, S. C., and E. L. Post

1954. The upper semi-lattice of degrees of recursive unsolvability, ***Ann. of Math.,*** 59, 379–407.

Kleene, S. C., and R. E. Vesley

1965. ***The Foundations of Intuitionistic Mathematics. N-H.***

Kneale, W., and M. Kneale

1962. ***The Development of Logic.*** Clarendon Press, Oxford.

Knight, J. F.

1975. Types omitted in uncountable models of arithmetic, ***JSL,*** 40, 307–320.

Kochen, S.

1961. Ultraproducts in the theory of models, ***Ann. of Math.,*** 74, 221–261.

Kopperman, R.

1972. ***Model Theory and its Applications.*** Allyn & Bacon.

Kreider, D. L., and H. Rogers, Jr.

1961. Constructive versions of ordinal number classes, ***Trans. AMS,*** 100, 325–369.

Kreisel, G.

1950. Note on arithmetic models for consistent formulae of the predicate calculus, ***FM,*** 37, 265–285.

1951–52. On the interpretation of non-finitist proofs, ***JSL,*** 16, 241–267; 17, 43–58.

1952a. On the concepts of completeness and interpretation of formal systems, ***FM,*** 39, 103–127.

1952b. Some concepts concerning formal systems of number theory, ***Math. Zeitschr.,*** 57, 1–12.

1953b. On a problem of Henkin's, ***Indag. Math.,*** 15, 405–406.

1955. Models, translations, and interpretations, ***Mathematical Interpretations of Formal System, N-H,*** 26–50.

1958a. Mathematical significance of consistency proofs, ***JSL,*** 23, 155–182.

1958b. Hilbert's programme, ***Dialectica,*** 12, 346–372.

1965. Mathematical logic, ***Lectures on Modern Mathematics (T.*** L. Saaty, Editor), Vol. 3, Wiley, 95–195.

1968. A survey of proof theory, I, ***JSL,*** 33, 321–388.

1971. A survey of proof theory, II, ***Proc. Second Scandinavian Logic Symp., N-H,*** 109–170.

Kreisel, G., and A. Levy

1968. Reflection principles and their use for establishing the complexity of axiomatic systems. ***ZML,*** 14, 97–191.

Kreisel, G., and H. Wang.

1955. Some applications of formalized consistency proofs, ***FM,*** 42, 101–110.

Krivine, J.-L.

1971. ***Introduction to Axiomatic Set Theory.*** Reidel.

Kruse, A. H.

1966. Grothendieck universes and the super-complete models of Shepherdson, ***Comp. Math,*** 17, 96–101.

Kunen, K.

1970. Some applications of iterated ultrapowers in set theory, ***AML,*** 1, 179–227.

Langford, C. H.

1927. Some theorems on deducibility, ***Ann. of Math.,*** I, 28, 16–40; II, 28, 459–471.

Lauchli, H.
1962. Auswahlaxiom in der Algebra, ***Comment. Math. Helvetica,*** 37, 1–18.

Lawvere. F. W.
1964. An elementary theory of the category of sets, ***Proc. Natl. Acad. Sci. USA,*** 52, 1506–1511.

Levy, A.
1960. Axiom schemata of strong infinity, ***Pacific J. Math.,*** 10, 223–238.
1964. The interdependence of certain consequences of the axiom of choice, ***FM,*** 54, 135–157.
1965. ***A Heirarchy of Formulas in Set Theory,*** Memoirs AMS, No. 57.
1969. The definability of cardinal numbers, ***Foundations of Mathematics, Gödel-Festschrift,*** Springer, 15–38.

Ltvy, A., and J. D. Halpern. See Halpern, J. D., and A. Lévy.

Ltvy, A., and G. Kreisel. See Kreisel, G., and A. Levy.

Löb, M. H.
1955. Solution of a problem of Leon Henkin, ***JSL,*** 20, 115–118.

Lorenzen, P.
1951. Algebraische und logistische Untersuchungen über freie Verbande, ***JSL,*** 16, 81–106.
1955. ***Einführung in die operative Logik und Mathematik,*** Springer.

Loś, J.
1954a. Sur le théorème de Gödel pour les théories indénombrables, ***Bull, de l'Acad. Polon. des Sci.,*** III, 2, 319–320.
1954b. On the existence of linear order in a group, ***Ibid.,*** 21–23.
1954c. On the categoricity in power of elementary deductive systems and some related problems, ***Coll. Math.,*** 3, 58–62.
1955a. The algebraic treatment of the methodology of elementary deductive systems, ***Studia Logica,*** 2, 151–212.
1955b. Quelques remarques, théorèmes et problemes sur les classes définissables d'algebres, ***Math. Interpretations of Formal System, N-H,*** 98–113.

Loś, J., and C. Ryll-Nardzewski
1954. Effectiveness of the representation theory for Boolean algebras, ***FM,*** 41, 49–56.

Löwenheim, L.
1915. Ueber Moglichkeiten im Relativkalkül, ***Math. Ann.,*** 76, 447–470.

Luxemburg, W. A. J.
1962. ***Non-Standard Analysis.*** Caltech Bookstore, Pasadena.
1969. (Editor) ***Applications of Model Theory to Algebra, Analysis, and Probability.*** Holt, Rinehart, Winston.
1973. What is Non-Standard Analysis? ***Papers in the Foundations of Mathematics, Amer. Math. Monthly,*** 80, No. 6, Part II, 38–67.

Luxemburg, W. A. J., and K. D. Stroyan. See Stroyan, K. D., and W. A. J. Luxemburg.

Lyndon, R. C.
1959. Properties preserved under algebraic constructions, ***Bull. AMS,*** 65, 287–299.

Macdowell, R., and E. Specker
1961. Modelle der Arthmetik, ***Infinitistic Methods,*** Pergamon, 257–263.

Machtey, M., and P. Young
1978. ***An Introduction to the General Theory of Algorithms. N-H.***

MacIntyre, A., and H. Simmons
1973. Gödel's diagonalization technique and related properties of theories, ***Colloq. Math.,*** 28, 165–180.

Maclane, S.
1971. Categorical algebra and set-theoretic foundations, ***Proc. Symp. Pure Math., AMS,*** XIII, Part 1, 231–240.

Maclaughlin, T.
1961. A muted variation on a theme of Mendelson, ***ZML,*** 17, 57–60.

Magari, R.
1975. The diagonalizable algebras, ***Boll. Unione Mat. Italiana*** (4), 12, 117–125.

Makkai, M., and G. Reyes
1977. ***First Order Categorical Logic.*** Springer.

Malcev, A.
1936. Untersuchungen aus dem Gebiet der mathematischen Logik, ***Mat. Sbornik,*** 2, 323–336.

Marek, W.
1973. On the metamathematics of impredicative set theory, ***Dissertationes Math.*** 98.

Margaris, A.
1967. ***First-Order Mathematical Logic.*** Blaisdell.

Markov, A.
1954. The Theory of Algorithms, ***Tr. Mat. Inst. Steklov.,*** XLII. (Translation: Office of Technical Services, U.S. Department of Commerce, Washington, D.C., 1962.)

Markwald, S.
1954. Zur Theorie der konstruktiven Wohlordnungen, ***Math. Ann.,*** 127, 135–149.

Martin-Lof, P.
1970. ***Notes on Constructive Mathematics.*** Almqvist & Wiksell, Stockholm.

Matiyasevich, Yu.
1970. Enumerable sets are Diophantine, ***Doklady Akad. Nauk SSSR,*** 191, 279–282. (English translation: ***Soviet Math. Doklady,*** 1970, 354–357).
1971. Diophantine representation of recursively enumerable predicates, (in Russian), ***Izv. Akad. Nauk SSSR,*** Ser. Mat. 35, 3–30.

McKinsey, J. C. C., and A. Tarski
1948. Some theorems about the sentential calculi of Lewis and Heyting, ***JSL,*** 13, 1–15.

Mendelson, E.
1956a. Some proofs of independence in axiomatic set theory, ***JSL,*** 21, 291–303.
1956b. The independence of a weak axiom of choice, ibid., 350–366.
1958. The Axiom of Fundierung and the Axiom of Choice, ***Arch,*** 4, 65–70.
1961. On Non-standard Models for Number Theory, ***Essays on the Foundations of Mathematics,*** Jerusalem, 259–268.
1970. ***Introduction to Boolean Algebra and Switching Circuits.*** Schaum-McGraw-Hill.
1973. ***Number System and the Foundations of Analysis.*** Academic.

Meredith, C. A.
1953. Single axioms for the systems (C, N), (C, O) and (A, N) of the two-valued propositional calculus, ***J. Comp. Syst.,*** 3, 155–164.

Minsky, M. L.

1967. *Computation: Finite and Infinite Machines.* Prentice-Hall.

Monk, J. D. See Henkin, L., J. D. Monk, and A. Tarski.

Montague, R., and R. L. Vaught

1959. Natural models of set theories, *FM,* 47, 219–242.

Morel, A. See Frayne, T., A. Morel, and D. Scott.

Morley, M.

1965. Categoricity in Power, *Trans. AMS,* 114, 514–538.

Morley, M., and H. J. Keisler. See Keisler, H. J., and M. Morley.

Morse, A.

1965. *A Theory of Sets.* Academic.

Moschovakis, Y. N.

1974. *Elementary Induction on Abstract Structures. N-H.*

Mostowski, A.

1939. Ueber die Unabhangigkeit des Wohlordnungsatzes vom Ordnungsprinzip, *FM,* 32, 201–252.

1947. On definable sets of positive integers, *FM,* 34, 81–112.

1947a. On absolute properties of relations, *JSL,* 12, 33–42.

1948. On the principle of dependent choices, *FM,* 35, 127–130.

1949. An undecidable arithmetic statement, *FM,* 36, 143–164.

1951. Some impredicative definitions in the axiomatic set theory, *FM,* 37, 111–124 (also, 38 (1952), 238).

1952. On models of axiomatic systems, *FM,* 39, 133–158.

1952. On direct powers of theories, *JSL,* 17, 1–31.

1956. *Thirty Years of Foundational Studies,* Blackwell, Oxford.

1957. On a generalization of quantifiers, *FM,* 44, 12–36.

1969. *Constructible Sets with Applications. N-H.*

Mostowski, A., and A. Ehrenfeucht, See Ehrenfeucht, A., and A. Mostowski.

Mostowski, A., A. Grzegorczyk, and C. Ryll-Nardzewski. See Grzegorczyk, A., A. Mostowski, and C. Ryll-Nardzewski.

Mostowski, A., A. Tarski, and R. Robinson. See Tarski, A., A. Mostowski, and R. Robinson.

Myhill, J.

1955. Creative Sets, *ZML,* 1, 97–108.

Myhill, J., and J. Dekker. See Dekker, J., and J. Myhill.

Nagornyi, N.

1953. Stronger reduction theorems for the theory of normal algorithms, *Dokl. Adad. Nauk SSSR, 90,* 341–342. (In Russian).

Negrepontis, S. See Comfort, W. W., and S. Negrepontis.

Nelson, E.

1977. Internal set theory: a new approach to nonstandard analysis, *Bull. AMS,* 83, 1165–1198.

Nerode, A.

1961. Extensions to isols, *Ann. of Math.,* 73, 362–403.

von Neumann, J.

1925. Eine Axiomatisierung der Mengenlehre, *J. fur Math.,* 154, 219–240 (also, 155, 128).

1928. Die Axiomatisierung der Mengenlehre, *Math. Zeitschr.,* 27, 669–752.

Nicod, J. G.

1917. A reduction in the number of primitive propositions of logic, *Proc. Camb. Phil. Soc.,* 19, 32–41.

Novak, I. L. (Gal, L. N.)

1951. A construction for models of consistent systems, *FM,* 37, 87–110.

Novikov, P.

1955. On the algorithmic unsolvability of the word problem for group theory, *Tr. Mat. Inst. Steklov.,* 44 *(Amer. Math Soc. Translations,* Series 2, 9, 1–124).

Oberschelp, A.

1964. Eigentliche Klassen als Urelemente in der Mengenlehre, *Math. Ann.,* 157, 234–260.

Orey, S.

1956. On ω-consistency and related properties, *JSL,* 21, 246–252.

1961. Relative interpretations, *ZML,* 7, 146–153.

Parikh, R.

1971. Existence and feasibility in arithmetic, *JSL,* 36, 494–508.

Paris, J. B.

1972. On models of arithmetic, *Conference in Math. Logic-London* 1970, Springer, 251–280.

Peano, G.

1891. Sul concetto di numero, *Rivista di Mat.,* 1, 87–102.

Peter, R.

1935. Konstruktion nichtrekursiver Funktionen, *Math. Ann.,* 111, 42–60.

1967. *Recursive Functions.* Academic.

Phillips, R. G.

1971. On the structure of nonstandard models of arithmetic, *Proc. AMS,* 27, 359–363.

Pincus, D., and R. M. Solovay

1977. Definability of measures and ultrafilters, *JSL,* 42, 179–190.

Post, E.

1921. Introduction to a general theory of elementary propositions, *Amer. J. Math.,* 43, 163–185.

1936. Finite combinatory process—formulation 1, *JSL,* 1, 103–105.

1943. Formal reductions of the general combinatorial decision problem, *Amer. J. Math.,* 65, 197–215.

1944. Recursively enumerable sets of positive integers and their decision problems, *Bull. Amer. Math. Soc.,* 50, 284–316.

1947. Recursive unsolvability of a problem of Thue, *JSL,* 12, 1–11.

Post, E., and S. C. Kleene. See Kleene, S. C., and E. Post.

Prawitz, D.

1971. Ideas and results of proof theory, *Proc. Second Scandinavian Logic Symp., N-H,* 235–307.

Presburger, M.

1929. Ueber die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen in welchem die Addition als einzige Operation hervortritt, *Comptes Rendus, I Congrès des Math. des Pays Slaves,* Warsaw, 192–201, 395.

Putnam, H.
1957. Decidability and Essential Undecidability, *JSL*, 22, 39–54.

Quine, W. V.
1937. New foundations for mathematical logic, *Amer. Math. Monthly*, 44, 70–80.
1950. *Methods of Logic*, Holt.
1951. *Mathematical Logic*, Harvard.
1953. *From a Logical Point of View*, Harvard.
1963. *Set Theory and its Logic*. Harvard.
1965. *Selected Logical Papers*. Random House.

Rabin, M.
1958. On recursively enumerable and arithmetic models of set theory, *JSL*, 23, 408–416.
1959. Arithmetical extensions with prescribed cardinality, *Indag. Math.*, 21,439–446.
1960. Computable algebra, general theory and theory of computable fields, *Trans. Amer. Math. Soc.*, 95, 341–360.
1961. Non-standard Models and Independence of the Induction Axiom, *Essays in the Foundations of Mathematics*, Jerusalem, 287–299.
1962. Diophantine Equations and Non-Standard Models of Arithmetic, *Logic, Methodology, and Philosophy of Science* (Proc. Int. Cong., 1960), Stanford, 151–158.
Rasiowa, H.
1956. On the ε-theorems, *FM*, 43, 156–165.
Rasiowa, H., and R. Sikorski
1951. A proof of the completeness theorem of Gödel, *FM*, 37, 193–200.
1952. A proof of the Skolem-Löwenheim theorem, *FM*, 38, 230–232.
1953. Algebraic treatment of the notion of satisfiability, *FM*, 40, 62–95.
1963. *The Mathematics of Metamathematics*. Warsaw.
Reinhardt, W. N.
1974. Set existence principles of Shoenfield, Ackermann, and Powell, *FM*, 84, 5–34.
Rescher, N.
1969. *Many-Valued Logic*. McGraw-Hill.
Ressayre, J. P.
1969. Sur les theories du premier ordre categorique en un cardinal, *Trans. AMS.*, 142, 481–505.
Reyes, G., and M. Makkai. See Makkai, M., and G. Reyes.
Rice, H. G.
1953. Classes of recursively enumerable sets and their decision problems, *Trans. Amer. Math. Soc.*, 74, 358–366.
Robinson, A.
1951. *On the metamathematics of algebra*, *N-H*.
1952. On the application of symbolic logic to algebra, *Int. Cong. Math.*, Cambridge, Mass., I., 686–694.
1955. On ordered fields and definite functions, *Math. Ann.*, 130, 257–271.
1956. *Complete Theories*, *N-H*.
1961. Model theory and non-standard arithmetic, *Infinitistic Methods*, Warsaw, 266–302.
1965. *Introduction to Model Theory and to the Metamathematics of Algebra*. *N-H*.
1966. *Non-Standard Analyais*. *N-H*.

Robinson, J.
1949. Definability and decision problems in arithmetic, *JSL*, 14, 98–114.
1950. General recursive functions, *Proc. Amer. Math. Soc.*, 1, 703–718.
1952. Existential definability in arithmetic, *Trans. Amer. Math. Soc.*, 72, 437–449.
Robinson, R. M.
1937. The theory of classes. A modification of von Neumann's system, *JSL*, 2, 69–72.
1947. Primitive recursive functions, *Bull. Amer. Math. Soc.*, 53, 925–942.
1948. Recursion and double recursion, ibid., 54, 987–993.
1950. An essentially undecidable axiom system, *Proc. Int. Cong. Math.*, Cambridge, 1950, 1, 729–730.
1956. Arithmetical representation of recursively enumerable sets, *JSL*, 21, 162–186.
Robinson, R., A. Tarski, and A. Mostowski. See Tarski, A., A. Mostowski, and R. Robinson.
Rogers, H., Jr.
1958. Gödel numberings of partial recursive functions, *JSL*, 23, 331–341.
1959. Computing degrees of unsolvability, *Math. Annalen*, 138, 125–140.
1967. *Theory of Recursiw Functions and Effective Computability*. McGraw-Hill.
Rogers, H., Jr., and D. L. Kreider. See Kreider, D. L., and H. Rogers Jr.
Rosenbloom, P.
1950. *Elements of Mathematical Logic*. Dover.
Rosser, J. B.
1936a. Constructibility as a criterion for existence, *JSL*, 1, 36–39.
1936b. Extensions of some theorems of Gödel and Church, ibid., 87–91.
1937. Gödel theorems for non-constructive logics, *JSL*, 2, 129–137.
1939a. On the consistency of Quine's "New foundations for mathematical logic," *JSL*, 4, 15–24.
1939b. An informal exposition of proofs of Gödel's Theorem and Church's Theorem, ibid., 53–60.
1953. *Logic for Mathematicians*, McGraw-Hill.
1954. The relative strength of Zermelo's Set Theory and Quine's New Foundations, *Proc. Int. Cong. Math.*, Amsterdam, III, 289–294.
1955. *Deux esquisses de logique*, Gauthier-Villars.
1969. *Simplified Independence Proofs*. Academic.
Rosser, J. B., and A. Turquette
1952. *Many-valued Logics*. *N-H*.
Rosser, J. B., and H. Wang
1950. Non-standard models for formal logics, *JSL*, 15, 113–129.
Rubin, H., and J. Rubin
1963. *Equivalents of the Axiom of Choice*. *N-H*.
Rubin, J.
1967. *Set Theory for the Mathematician*. Holden-Day.
Russell, B.
1908. Mathematical logic as based on the theory of types, *Amer. J. Math.*, 30, 222–262.
Russell, B., and A. N. Whitehead
1910–1913. *Principia Mathematica*, Vols. I–III, Cambridge Univ. Press.
Ryll-Nardzewski, C.
1953. The role of the axiom of induction in elementary arithmetic, *FM*, 39, 239–263.

Ryll-Nardzewski, C., A. Grzegorczyk, and A. Mostowski. See Grzegorczyk, A., A. Mostowski, and C. Ryll-Nardzewski.

Ryll-Nardzewski, C., and J. Łoś. See Łoś, J., and C. Ryll-Nardzewski.

Sacks, G. E.

1963. *Degrees of Unsolvability*. Princeton.

1972. *Saturated Model Theory.* Benjamin.

Šanin, N. A.

1958. On the constructive interpretation of mathematical judgments, *Trudy Mat. Inst. Steklov*, 52, 226–311. (English translation, *AMS Translations* (2), 23, 1963, 109–189.)

Scarpellini, B.

1969. On the metamathematics of rings and integral domains, *Trans. AMS,* 138, 71–96.

Schmidt, A.

1960. *Mathemutische Gesetze der Logik I, Vorlesungen iiber Aussagenlogik*, Springer.

Scholz, H., and G. Hasenjaeger. See Hasenjaeger, G., and H. Scholz.

Schiitte, K.

1951. Beweistheoretische Erfassung der unendlichen Induktion in der Zahlentheorie, *Math, Ann.,* 122, 369–389.

1960. *Beweistheorie*, Springer (English translation: *Proof Theory,* 1977).

Scott, D.

1961. On constructing models for arithmetic, *Infinitistic Methods,* Warsaw, 235–255.

1967. A proof of the independence of the continuum hypothesis, *Math. Systems Theory,* 1, 89–111.

1974. Axiomatizing set theory, *Proc. Symp. Pure Math.* 13, *AMS,* II, 207–214.

Scott, D., T. Frayne, and A. Morel. See Frayne, T., A. Morel, and D. Scott.

Seidenberg, A.

1954. A new decision method for elementary algebra, *Ann. of Math.,* 60, 365–374.

Shannon, C.

1938. A symbolic analysis of relay and switching circuits, *Trans. Amer. Inst. Elect. Eng.,* 57, 713–723.

Shapiro, N.

1956. Degrees of computability, *Trans. Amer. Math. Soc.,* 82, 281–299.

Shelah, S.

1971. Every two elementarily equivalent models have isomorphic ultrapowers, *Israel J. of Math.,* 10, 224–233.

Shepherdson, J.

1951–1953. Inner models for set theory, *JSL*, I, 16, 161–190; II, 17,225–237; III, 18, 145–167.

1961. Representability of recursively enumerable sets in formal theories, *Arch.,* 5, 119–127.

Shepherdson, J. C., and A. Bezboruah. See Bezboruah, A., and J. C. Shepherdson.

Shoenfield, J.

1954. A relative consistency proof, *JSL,* 19, 21–28.

1958. Degrees of formal systems, *JSL,* 23, 389–392.

1959. On a restricted ω-rule. *Bull. Acad. Pol. Sci., Ser. Sci. Math. Astr. Phys.,* 7, 405–407.

1961. Undecidable and creative theories. *FM,* 49, 171–179.

1961b. The problem of predicativity, *Essays on the Foundations of Mathematics,* Magnes, Jerusalem, 132–139.

1967. *Mathematical Logic*. Addison-Wesley.

1971a. *Degrees of Unsolvability*. *N-H*.

1971b. Unramified forcing, *Proc. Symp. Pure Math.* 13, *AMS,* 357–381.

Sierpinski, W.

1947. L'hypothèse généralisée du continu et l'axiome du choix, *FM,* 34, 1–5.

1958. *Cardinal and-ordinal Numbers,* Warsaw, Polska Akad. Nauk.

Sikorski, R.

1960. *Boolean algebras,* Springer.

Sikorski, R., and H. Rasiowa. See Rasiowa, H., and R. Sikorski.

Silver, J.

1971. Some applications of model theory in set theory, *AML,* 3, 45–110.

Simmons, H. See MacIntyre, A., and H. Simmons.

Skolem, T.

1919. Logisch-kombinatorische Untersuchungen iiber die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze, *Skrifter-Vidensk,* Kristiana, I, 1–36.

1934. Ueber die Nicht-Charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschliesslich Zahlenvariablen, *FM,* 23, 150–161.

1955. Peano's axioms and models of arithmetic, *Mathematical Interpretations of Formal Systems, N-H,* 1–14.

1970. *Selected Works in Logic* (Edited by J. E. Fenstad). Universitetsforlaget, Oslo.

Slomson, A. B. See Bell, J. L., and A. B. Slomson.

Smullyan, R.

1961. *Theory of Formal Systems.* Princeton.

1968. *First-Order Logic.* Springer.

Solovay, R. M.

1970. A model of set theory in which every set of reals is Lebesgue measurable, *Ann. of Math.,* 92, 1–56.

Solovay, R. M., and D. Pincus. See Pincus, D., and R. M. Solovay.

Sonner, J.

1962. On the formal definition of categories, *Math.* Z., 80, 163–176.

Specker, E.

1949. Nicht-konstruktiv beweisbare Satze der Analysis, *JSL,* 14, 145–148.

1953. The axiom of choice in Quine's "New foundations for mathematical logic," *Proc. Acad. Sci. U.S.A.,* 39, 972–975.

1954. Verallgemeinerte Kontinuumshypothese und Auswahlaxiom, *Archiu der Math.,* 5, 332–337.

1957. Zur Axiomatik der Mengenlehre (Fundierungs und Auswahlaxiom), *ZML,* 3, 173–210.

1962. Typical Ambiguity. *Logic, Methodology, and Philosophy of Science (Proc. Int. Cong.,* 1960), Stanford, 116–124.

Specker, E., and R. Macdowell. See Macdowell, R., and E. Specker.

Spector, C.

1955. Recursive well-ordering, *JSL,* 20, 151–163.

Stone, M.

1936. The representation theorem for Boolean algebras, *Trans. Amer. Math. Soc.,* 40, 37–111.

Stroyan, K. D., and W. A. J. Luxemburg

1976. ***Introduction to the Theoty of Infinitesimals***. Academic.

Suppes, P.

1960. ***Axiomatic Set Theoty,*** Van Nostrand.

Suranyi, J.

1959. ***Reduktionstheorie des Entscheidungproblems im Pradikatenkalkiil der ersten Stufe,*** Budapest, Akademiai Kiado.

Szmielew, W.

1955. Elementary properties of abelian groups, ***FM,*** 41, 203–271.

Takeuti, G., and W. M. Zaring

1971. ***Introduction to Axiomatic Set Theory.*** Springer.

1973. ***Axiomatic Set Theoty.*** Springer.

Tarski, A.

1923. Sur quelques théorèmes qui equivalent a l'axiome de choix, ***FM,*** 5, 147–154.

1925. Sur les ensembles finis, ***FM,*** 6, 45–95.

1933. Einige Betrachtungen uber die Begriffe der w-Widerspruchsfreiheit und der w-Vollstandigkeit, ***Monats. Math. Phys., 40,*** 97–112.

1936. Der Wahrheitsbegriff in den formalisierten Sprachen, ***Studia Philos.,*** 1, 261–405 (also in [1956]).

1938. Ueber unerreichbare Kardinalzahlen, ***FM,*** 30, 68–89.

1944. The semantic conception of truth and the foundations of semantics, ***Philos. and Phenom. Res.,*** 4, 341–376.

1951. ***A Decision Method for Elementary Algebra and Geometry***, Berkeley.

1952. Some notions and methods on the borderline of algebra and metamathematics, ***Int. Cong. Math.,*** Cambridge, Mass., 705–720.

1954–55. Contributions to the Theory of Models, ***Indag. Math.,*** 16, 572–588; 17, 56–64.

1956. ***Logic, Semantics, Metamathematics,*** Oxford.

Tarski, A., and P. Erdos. See Erdos, P., and A. Tarski.

Tarski, A., L. Henkin, and J. D. Monk. See Henkin, L., J. D. Monk, and A. Tarski.

Tarski, A., and H. J. Keisler. See Keisler, H. J., and A. Tarski.

Tarski, A., and J. C. C. McKinsey. See McKinsey, J. C. C., and A. Tarski.

Tarski, A., A. Mostowski, and R. Robinson.

1953. ***Undecidable Theories, N-H.***

Tarski, A., and R. Vaught.

1957. Arithmetical extensions of relational systems, ***Comp. Math.,*** 18, 81–102.

Tennenbaum, S.

1968. Souslin's problem, ***Proc. Natl. Acad. Sci. USA,*** 59, 60–63.

Truss, J. K.

1973. The well-ordered and well-orderable subsets of a set, ***ZML,*** 19, 211–214.

Turing, A.

1936–37. On computable numbers, with an application to the Entscheidungsproblem, ***Proc. London Math. Soc.***, 42, 230–265; 43, 544–546.

1937. Computability and λ-definability, ***JSL,*** 2, 153–163.

1939. Systems of logic based on ordinals, ***Proc. London Math. Soc.,*** 45, 161–228.

1950a. The word problem in semigroups with cancellation, ***Ann. of Math.,*** 52, 491–505.

1950b. Computing Machinery and Intelligence, ***Mind,*** 59, 433–460.

Turquette, A., and J. B. Rosser. See Rosser, J. B., and A. Turquette.

Ulam, S.

1930. Zur Masstheorie in der allgemeinen Mengenlehre, ***Fund. Math.,*** 16, 140–150.

Vaughn, H., and P. Halmos. See Halmos, P., and H. Vaughn.

Vaught, R.

1954. Applications of the Löwenheim-Skolem-Tarski theorem to problems of completeness and decidability, ***Indag. Math.,*** 16, 467–472.

1963. Models of complete theories, ***Bull. AMS,*** 69, 299–313.

Vaught, R. L., and R. Montague. See Montague, R., and R. L. Vaught.

Vaught, R. L., and A. Tarski. See Tarski, A., and R. L. Vaught.

Vesley, R. E., and S. C. Kleene. See Kleene, S. C., and R. E. Vesley.

Vopenka, P., and P. Hajek

1972. ***The Theoty of Semisets. N-H.***

Waerden, B. van der

1949. ***Modern Algebra.*** Ungar.

Wang, H.

1955. Undecidable sentences generated by semantical paradoxes, ***JSL,*** 20, 31–43.

1957. The axiomatization of arithmetic, ***JSL,*** 22, 145–158.

1970. ***Logic, Computers, and Sets.*** Chelsea.

Wang, H., and G. Kreisel. See Kreisel, G., and H. Wang.

Wang, H., and J. B. Rosser. See Rosser, J. B., and H. Wang.

Whitehead, A. N., and B. Russell. See Russell, B., and A. N. Whitehead.

Yasuhara, A.

1971. ***Recursive Function Theoty and Logic.*** Academic.

Young, P. See Machtey, M., and P. Young.

Zaring, W. M. See Takeuti, G., and W. M. Zaring.

Zeeman, E. C.

1955. On direct sums of free cycles, ***J. London Math. Soc.***, 30, 195–212.

Zermelo, E.

1908. Untersuchungen uber die Grundlagen der Mengenlehre, ***Math. Ann.,*** 65, 261–281.

Zuckerman, M.

1974. ***Sets and Transfinite Numbers.*** Macmillan.

NOTATION

$\overline{\overline{X}}$	2
$\mathcal{P}$	2, 179
$\in$, $\notin$	5, 173
$\subseteq$, $\subset$, $\subsetneq$	5, 104, 173
$=$, $\neq$	5, 79, 173
$\cup$, $\cap$	5, 163
$\{x \mid P(x)\}$	5
0	5, 102, 175
$X - Y$	5, 177
$\{x, y\}$, $\{b_1, \ldots, b_k\}$, $\{x\}$	5, 175, 180
$\langle b_1, \ldots, b_k \rangle$	5
$Y \times Z$	5, 179
X^k	5, 179
R^{-1}	6
ω	6, 188
I_X	6
$[y]$	6
$f(x_1, \ldots, x_n)$	7
f_Z	7
$f \circ g$	7
1–1	7
$X \cong Y$	8, 192
$\aleph_0$, $2^{\aleph_0}$	8
$\sim$, $\wedge$	11
$\vee$, $\supset$	12
$\equiv$	13, 103
T, F	11
$\downarrow$, $\mid$	27
$\vdash$	30
L	31
MP	31
$\mathrm{L}_1 - \mathrm{L}_4$	40
(x), (Ex)	45
A_j^n, f_j^n, a_j	46
$(A_j^n)^M$, $(f_j^n)^M$, $(a_j)^M$	50
Σ	51
$s\bigstar$	51
$\models_M \mathcal{A}$	52
$\models_M \mathcal{A}[b_{i_1}, \ldots, b_{i_k}]$	54
Gen	60
g	66, 151, 235
$\vdash_C$	77
K_1, K_2	81
G, F, G_C, R_C	82
$(E_1 x)$	83
$(E_n x)$	84
ι	88
$\approx$	93, 117, 226
K^2, K^n	94
$\leqslant_e$	105
$\prod_{j \in J} \mathrm{D}_j$	110
$=_{\mathcal{F}}$	110
$f_{\mathcal{F}}$	111
$\prod_{j \in J} \mathrm{D}_j / \mathcal{F}$	111
$\{c_j\}_{j \in J}$	111
$\prod_{j \in J} \mathrm{M}_j / \mathcal{F}$	112
$\mathrm{N}^J / \mathcal{F}$	112
$c^{\#}$, $\mathrm{M}^{\#}$	114
R, $\mathcal{R}$	115
$\mathrm{R}\bigstar$, $\mathcal{R}\bigstar$, $\mathrm{R}^{\#}$, $\mathcal{R}^{\#}$	116

ANSWERS TO SELECTED EXERCISES

Chapter 1

1.1.

A	B	
T	T	F
F	T	T
T	F	T
F	F	F

1.2.

A	B	$—A$	$A \supset B$	$(A \supset B) \vee \sim A$
T	T	F	T	T
F	T	T	T	T
T	F	F	F	F
F	F	T	T	T

13.

$((A \supset B) \wedge A)$

$T\,T\,T\ \ T\,T$

$F\,T\,T\ \ F\,F$

$T\,F\,F\ \ F\,T$

$F\,T\,F\ \ F\,F$

1.4. (*a*) $((A \supset \sim B) \wedge (\sim A \supset \sim B))$

(*d*) $A \supset B.$ A : *Fiorello goes to the movies.*

(*e*) $A \supset B.$ A : *x is prime.*

(f) $A \supset B.$ A : *s converges.*

(h) $-\ A \supset B.$ A : *The Dodgers win today.*

B : *The Giants will win the pennant.*

1.5. (*a*) *No.* (*c*) *Yes.* (*e*) *No.*

1.8. *All except* (*i*).

1.10. *Yes:* (*c*) *and* (*e*).

1.12. (*a*) *All parentheses may be dropped.*

(*c*) $(A \supset B \vee C) \vee \sim (C \supset D).$

(*e*) $(A \supset B \supset (C \supset D)) \wedge \sim A \vee C.$

1.13. $((C \supset ((\sim (A \vee C)) \wedge A)) \equiv B).$

1.14. (*a*) $(((\sim (\sim A)) \equiv A) \equiv (B \vee C)).$

(*c*) *No. Extra right parenthesis.*

(e) $((((\sim (A \supset B)) \vee C) \vee D) \supset B).$

1.15. (a) $\vee C \supset \wedge B$ ▬ DC.

(b) To prove that (i)–(ii) imply that it is a statement form, use induction with respect to the number of symbols in $\mathcal{A}$. (A proper initial segment of $\mathcal{A}$ is, by definition, an expression made up of all the symbols in $\mathcal{A}$ to the left of some specific symbol.)

(d) (ii) $(A \supset B) \supset ((B \supset C) \supset (\sim A \supset C))$.

1.18. (a) T (b) T (c) Nothing

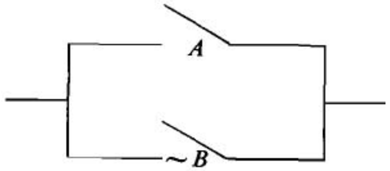
1.19. (a)

```
~A∨(A ⊃ B)
       F
       T   F
F
    F
```

1.20. (a) If & is a tautology, replace all statement letters by their negations, and then move all the new negation signs outward by using Exercise 1.24(a). The result is $\sim \mathcal{A}'$.

If $\sim \mathcal{A}'$ is a tautology, let $\mathcal{B}$ be $\sim \mathcal{A}'$. By the first part, $\sim \mathcal{B}$' is a tautology. But --%'is $\sim\sim \mathcal{A}$.

1.28. (a) For Figure 1.4:



1.29. (a) Not logically correct:

```
((C⊃A)∧A)⊃C
          F
      T     F
  T     T
```

Let A be T, and let C be F.

(b) Logically correct. Assume all the premises true and the conclusion false, and show that this leads to a contradiction.

1.30. (a) Consistent. Let A, B, C be F, and let D be T.

131. (b) Inconsistent.

```
(B∧H)∨(B ∧ W)   H⊃~B    ~W
      T           T      T
                          F
            F
    T
  T   T
                T   F
                  F
```

1.32. $(A_1 \wedge A_2 \wedge A_3) \vee (\sim A_1 \wedge A_2 \wedge A_3) \vee (\sim A_1 \wedge \sim A_2 \wedge \sim A_3)$.

1.34. (a) Any statement form built up using $\supset$ and $\vee$ will always take the value T when the statement letters in it are T.

(b) Using only the statement letters A and B, find all the truth functions of two variables that can be generated by applying $\sim$ and $\equiv$ any number of times.

136. (b) For $\sim (A \supset B) \vee (\sim A \wedge C)$, a disjunctive normal form is $(A \wedge \sim B) \vee (\sim A \wedge C)$, and a conjunctive normal form ɪs $(A \vee C) \wedge (\sim B \vee \sim A) \wedge (\sim B \vee C)$.

(c) For $\sim (A \supset B) \vee (\sim A \wedge C)$, a full disjunctive normal form is $(A \wedge \sim B \wedge C) \vee (A \wedge \sim B \wedge \sim C) \vee (\sim A \wedge B \wedge C) \vee$ $(—A \wedge \sim B \wedge C)$, and a full conjunctive normal form is $(A \vee B \vee C) \wedge (A \vee \sim B \vee C) \wedge (\sim A \vee \sim B \vee C) \wedge (\sim A \vee \sim B \vee \sim C)$.

(e) (i) $—(—A \wedge \sim B) \wedge \sim (B \wedge \sim C)$.

1.38. (b)

1. $\mathcal{B} \supset \mathcal{C}$	Hypothesis
2. $\mathcal{A} \supset \mathcal{B}$	Hypothesis
3. $(\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})) \supset ((\mathcal{A} \supset \mathcal{B}) \supset (\mathcal{A} \supset \mathcal{C}))$	(A2)
4. $(\mathcal{B} \supset \mathcal{C}) \supset (\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C}))$	(A1)
5. $\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})$	1, 4, **MP**
6. $(\mathcal{A} \supset \mathcal{B}) \supset (\mathcal{A} \supset \mathcal{C})$	3, 5, **MP**
7. $\mathcal{A} \supset \mathcal{C}$	1, 6, **MP**

139. (a)

1. $\mathcal{A} \supset \sim\sim \mathcal{A}$	Lemma 1.10(b)
2. $\sim\sim \mathcal{A} \supset (\sim \mathcal{A} \supset \mathcal{B})$	Lemma 1.10(c)
3. $\mathcal{A} \supset (\sim \mathcal{A} \supset \mathcal{B})$	1, 2, Cor. 1.9(i).
4. $\mathcal{A} \supset (\mathcal{A} \vee \mathcal{B})$	3, Abbreviation

(c)

1. $\sim \mathcal{B} \supset \mathcal{A}$	Hypothesis
2. $(\sim \mathcal{B} \supset \mathcal{A}) \supset (\sim \mathcal{A} \supset \sim\sim \mathcal{B})$	Lemma 1.10(e)
3. $\sim \mathcal{A} \supset \sim\sim \mathcal{B}$	1, 2, **MP**
4. $\sim\sim \mathcal{B} \supset \mathcal{B}$	Lemma 1.10(a)
5. $\sim \mathcal{A} \supset \mathcal{B}$	3, 4, Cor. 1.9(i).
6. $\sim \mathcal{B} \supset \mathcal{A} \vdash \sim \mathcal{A} \supset \mathcal{B}$	1–5
7. $\vdash (\sim \mathcal{B} \supset \mathcal{A}) \supset (\sim \mathcal{A} \supset$ 93)	1–6, Deduction Theorem
8. $\vdash (\mathcal{B} \vee \mathcal{A}) \supset (\mathcal{A} \vee \mathcal{B})$	7, Abbreviation

1.42. Hint: Take an assignment of truth values to the statement letters of $\mathcal{A}$ which makes $\mathcal{A}$ false. Replace in $\mathcal{A}$ each letter having the value T by $A_1 \vee \sim A_1$, and each letter having the value F by A, $\wedge \sim$ A,. Call the resulting statement form $\mathcal{B}$.

Chapter 2

2.1. $(((x_2)(\sim A_1^1(x_1))) \supset (A_2^3(x_1, x_1, x_2) \vee ((x_1)A_2^1(x_1))))$

2.2. (a) $((((x_1)((x_3)((x_4)A_1^1(x_1)))) \supset (A_2^1(x_3) \wedge (\sim A_1^1(x_1))))$

(b) $((Ex_1)((x_2)((Ex_3)(A_1^1(x_1) \vee ((Ex_2)(\sim ((x_3)A_1^2(x_3, x_2))))))))$

2.3. (a) $(x_1)(A_1^1(x_1) \supset A_2^1(x_1)) \vee (Ex_1)A_1^1(x_1)$.

24. (a) The only free occurrence of a variable is that of x_2.

(b) The first occurrence of x_3 is free, as is the last occurrence of x_2.

2.6. *In* **2.2(a)**, x_1 *and* x_3 *are both free and bound, while* x_4 *is bound. In* **2.2(b)**, all *variables are bound; no variable is free.*

2.8. *Yes: (a),(c),(e). No:* (b), *(d).*

2.10. (a) $(x)(F(x)$ A $\sim S(x) \supset (y)(C(y) \supset K(x,y)))$

(c) $\sim (x)(B(x) \supset F(y))$

(d) $[((x)(Ey)L(x,y))$ *A* $\sim (Ex)(y)L(x,y)]$ *V* $[((Ex)(y)L(x,y))$ *A* $(Ex)(y) \sim L(x,y)]$

2.11. *(a) Every student has at least one course with a bad teacher.*

(b) *The sum of two sides of a triangle is greater than the third.*

2.12. *(a) (1) is satisfied by all ordered pairs of positive integers. (2) translates into* $x, \geqslant x_2$ *3* $x_2 \geqslant x_1$, *and is satisfied by all pairs of positive integers* (n,k) *such that* $n \leqslant k$. *(Remember that a wf* $\mathscr{A} \supset \mathscr{B}$ *is true when* $\mathscr{A}$ *is false or* $\mathscr{B}$ *is true.) (3) is true; it asserts the transitivity of the relation* $\geqslant$ *in the set of positive integers.*

2.13. *(c) (i) There is no largest integer. (ii) There is an integer greater than every integer. (iii) Every integer has an "immediate successor".*

2.14. *(I) A sequence* **s** *satisfies* $\sim \mathscr{A}$ *if and only* if *s does not satisfy* $\mathscr{A}$. *Hence, all sequences satisfy* $\sim \mathscr{A}$ *if and only if no sequence satisfies* $\mathscr{A}$, i.e., $\sim \mathscr{A}$ *is true if and only if* $\mathscr{A}$ *is false.*

(II) *There is at least one sequence* **s** *in* Σ. *If* **s** *satisfies* $\mathscr{A}$, $\mathscr{A}$ *cannot be false for* M. *If* **s** *does not satisfy* $\mathscr{A}$, $\mathscr{A}$ *cannot be true for* M.

(III) *If a sequence* **s** *satisfies both* $\mathscr{A}$ *and* $\mathscr{A} \supset \mathscr{B}$, *then* **s** *satisfies* $\mathscr{B}$, *by clause (iii) of the definition.*

(V) *(i)***s** *satisfies* $\mathscr{A} \wedge \mathscr{B}$ *if and only if s satisfies* $\sim (\mathscr{A} \supset \sim \mathscr{B})$
if and only if **s** *does not satisfy* $\mathscr{A} \supset \sim \mathscr{B}$
if and only if **s** *satisfies* $\mathscr{A}$ *but not* $\sim \mathscr{B}$
if and only if **s** *satisfies* $\mathscr{A}$ *and* **s** *satisfies* $\mathscr{B}$

(VI) (a) Assume $\vDash_{\mathbf{M}} \mathscr{A}$. *Then every sequence satisfies* $\mathscr{A}$. *In particular, every sequence differing from a sequence* **s** *in at most the* i^{th} *place satisfies* $\mathscr{A}$. *So, every sequence satisfies* $(x_i)\mathscr{A}$, *that is,* $\vDash_{\mathbf{M}} (x_i)\mathscr{A}$.

(b) *Assume* $\vDash_{\mathbf{M}} (x_i)\mathscr{A}$. *If* **s** *is a sequence, then any sequence differing from* **s** *in at most the ith place satisfies* $\mathscr{A}$, *and, in particular,* **s** *satisfies* $\mathscr{A}$. *Then every sequence satisfies* $\mathscr{A}$, *that is,* $\vDash_{\mathbf{M}} \mathscr{A}$.

(VIII) LEMMA *A. If all the variables in a term t occur in the list* $x_{i_1}, \dots, x_{i_k}$ $(k \geqslant 0$; *when* $k = 0$, *t has no variables), and if the sequences s and* s' *have the same components in the* $i_1^{\text{th}}, \dots, i_k^{\text{th}}$ *places, then* $s^\star(t) = (s')^\star(t)$.

Proof. Induction on the number m of function letters in t. Assume the result holds for all integers $< m$.

Case 1. t is an individual constant a_p. *Then* $\mathbf{s}^\star(a_p) = (a_p)^{\mathrm{M}} = (\mathbf{s}')^\star(a_p)$.

Case 2. t is a variable x_{i_j}. *Then* $\mathbf{s}^\star(x_{i_j}) = \mathbf{s}_{i_j} = \mathbf{s}'_{i_j} = (\mathbf{s}')^\star(x_{i_j})$.

Case 3. t is of the form $f_j^n(t_1, \dots, t_n)$. *For* $q \leqslant n$, *each* t_q *has fewer than* m *function letters and all its variables occur among* $x_{i_1}, \dots, x_{i_k}$. *By inductive hypothesis,* $\mathbf{s}^\star(t_q) = (\mathbf{s}')^\star(t_q)$. *Then* $\mathbf{s}^\star(f_j^n(t_1, \dots, t_n)) = (f_j^n)^{\mathrm{M}}(\mathbf{s}^\star(t_1), \dots, \mathbf{s}^\star(t_n)) = (f_j^n)^{\mathrm{M}}((\mathbf{s}')^\star(t_1), \dots, (\mathbf{s}')^\star(t_n)) = (\mathbf{s}')^\star(f_j^n(t_1, \dots, t_n))$.

Proof of (VIII). Induction on the number r of connectives and quantifiers in $\mathscr{A}$. *Assume the result holds for all* $q < r$.

Case 1. $\mathscr{A}$ *is of the* form $A_j^n(t_1, \dots, t_n)$, i.e. $r = 0$. *All the variables of each* t_i *occur among* $x_{i_1}, \dots, x_{i_k}$. *Hence, by Lemma A,* $\mathbf{s}^\star(t_i) = (\mathbf{s}')^\star(t_i)$. *But* **s** *satisfies* $A_j^n(t_1, \dots, t_n)$ *if and* only *if* $(\mathbf{s}^\star(t_1), \dots, \mathbf{s}^\star(t_n))$ *is in* $(A_j^n)^{\mathrm{M}}$, *that is, if and only if* $((\mathbf{s}')^\star(t_1), \dots, (\mathbf{s}')^\star(t_n))$ *is in* $(A_j^n)^{\mathrm{M}}$, *which is equivalent to* s' *satisfying* $A_j^n(t_1, \dots, t_n)$.

Case 2. $\mathscr{A}$ *is of the* form $-$ *3*.

Case 3. $\mathscr{A}$ *is of the* form $\mathscr{B} \supset \mathscr{C}$. *Both cases 2 and 3 are easy.*

Case 4. $\mathscr{A}$ *is of the form* $(x_j)\mathscr{B}$. *The free variables of* $\mathscr{B}$ *occur among* $x_{i_1}, \dots, x_{i_k}$ *and* x_j. *Assume* **s** *satisfies* $\mathscr{A}$. *Then every sequence differing from* **s** *in at most the* j^{th} *place satisfies* $\mathscr{B}$. *Let* **s#** *be any sequence differing from* $\mathbf{s}'$ *in at most the* j^{th} *place. Let* s^b *be a sequence which has the same components as* **s** *in all but the* j^{th} *place, where it has the same component as* **s#**. *Hence,* $\mathbf{s}^b$ *satisfies* $\mathscr{B}$. *Since* s^b *and* **s#** *agree in the* $i_1^{\text{th}}, \dots, i_k^{\text{th}}$, *and* j^{th} *places, it follows by inductive hypothesis, that* s^b *satisfies* $\mathscr{B}$ *if and only* if **s#** *satisfies* $\mathscr{B}$. *Hence,* **s#** *satisfies* $\mathscr{B}$. *Thus,* s' *satisfies* $\mathscr{A}$. *By symmetry, the converse also holds.*

(IX) Assume $\mathscr{A}$ *closed. By (VIII), for any sequences* **s** *and* $\mathbf{s}'$, **s** *satisfies* $\mathscr{A}$ *if and only if* $\mathbf{s}'$ *satisfies* $\mathscr{A}$. *If* $\sim \mathscr{A}$ *is not true for M, some sequence* $\mathbf{s}'$ *does not satisfy* $\sim \mathscr{A}$, i.e., $\mathbf{s}'$ *satisfies* $\mathscr{A}$. *Hence, every sequence* **s** *satisfies* $\mathscr{A}$, i.e. $\vDash_{\mathbf{M}} \mathscr{A}$.

(X) *Proof of the Lemma. Induction on the number m of function letters in t.*

Case 1. t is a_j. *Then* t' *is* a_j. *Hence*

$$\mathbf{s}^\star(t') = \mathbf{s}^\star(a_j) = (a_j)^{\mathrm{M}} = (\mathbf{s}')^\star(a_j) = (\mathbf{s}')^\star(t).$$

Case 2. t is x_j, *where* $j \neq i$. *Then* t' *is* x_j. *By Lemma A of (VIII),* $\mathbf{s}^\star(t') = (\mathbf{s}')^\star(t)$, *since* **s** *and* $\mathbf{s}'$ *have the same component in the* j^{th} *place.*

Case 3. t is x_i. *Then* t' *is u. Hence,* $\mathbf{s}^\star(t') = \mathbf{s}^\star(u)$, *while* $(\mathbf{s}')^\star(t) = (\mathbf{s}')^\star(x_i) = \mathbf{s}'_i = \mathbf{s}^\star(u)$.

Case 4. t is of the form $f_j^n(t_1, \dots, t_n)$. *For* $1 \leqslant q \leqslant n$, *let* t'_q *result from* t_q *by the substitution of* u *for* x_i. *By inductive hypothesis,* $\mathbf{s}^\star(t'_q) = (\mathbf{s}')^\star(t_q)$. *But* $\mathbf{s}^\star(t') = \mathbf{s}^\star(f_j^n(t'_1, \dots, t'_n)) = (f_j^n)^{\mathrm{M}}(\mathbf{s}^\star(t'_1), \dots, \mathbf{s}^\star(t'_n)) = (f_j^n)^{\mathrm{M}}((\mathbf{s}')^\star(t_1), \dots, (\mathbf{s}')^\star(t_n)) = (\mathbf{s}')^\star(f_j^n(t_1, \dots, t_n)) = (\mathbf{s}')^\star(t)$.

Proof of Corollary (i). Induction on the number m of connectives and quantifiers in $\&(x_i)$.,

Case 1. $m = 0$. *Then* $\mathscr{A}(x_i)$ *is* $A_j^n(t_1, \dots, t_n)$. *Let* t'_q *be the result of substituting t for all* occurrences *of* x_i *in* t_q. *Thus,* $\mathscr{A}(t)$ *is* $A_j^n(t'_1, \dots, t'_n)$. *By the* Lemma *above,* $\mathbf{s}^\star(t'_q) = \mathbf{s}')^\star(t_q)$. *Now,* **s** *satisfies* $\mathscr{A}(t)$ if *and only if* $(\mathbf{s}^\star(t'_1), \dots, \mathbf{s}^\star(t'_n))$ *belongs to* $(A_j^n)^{\mathrm{M}}$, *which is equivalent to* $((\mathbf{s}')^\star(t_1), \dots, (\mathbf{s}')^\star(t_n))$ *belonging to* $(A_j^n)^{\mathrm{M}}$, *that is, to* s' *satisfying* $\mathscr{A}(x_i)$.

Case 2. $\mathscr{A}(x_i)$ *is* $\sim \mathscr{B}(x_i)$. *Straightforward.*

Case 3. $\mathscr{A}(x_i)$ *is* $\mathscr{B}(x_i) \supset \mathscr{C}(x_i)$. *Straightforward.*

Case 4. $\mathscr{A}(x_i)$ *is* $(x_j)\mathscr{B}(x_i)$.

Case 4a. x_j *is* x_i. *Then* x_i *is not free in* $\mathscr{A}(x_i)$, *and* $\mathscr{A}(t)$ *is* $\mathscr{A}(x_i)$. *Since* x_i *is not free in* $\mathscr{A}(x_i)$, *it follows by (VIII) that* **s** *satisfies* $\mathscr{A}(t)$ *if and only if* $\mathbf{s}'$ *satisfies* $\mathscr{A}(x_i)$.

Case 4b. x_j *is different from* x_i. *Since t is free for* x_i *in* $\mathscr{A}(x_i)$, *t is also free for* x_i *in* $\mathscr{B}(x_i)$.

Assume **s** *satisfies* $(x_j)\mathscr{B}(t)$. *We must show that* s' *satisfies* $(x_j)\mathscr{B}(x_i)$. *Let* **s#** *differ from* $\mathbf{s}'$ *in at most the* j^{th} *place. It suffices to show that* **s#** *satisfies* $\mathscr{B}(x_i)$. *Let* s^b *be the same as* **s#** *except that it has the same* i^{th} *component as s. Hence,* $\mathbf{s}^b$

is the same as s except in its j^{th} component. Since s satisfies $(x_j)\mathfrak{B}(t)$, s^b satisfies $\mathfrak{B}(t)$. Now, since t is free for x_i in $(x_j)\mathfrak{B}(x_i)$, t does not contain x_j. (The other possibility, that x_i is not free in $\mathfrak{B}(x_i)$, is handled as in Case 4a.) Hence, by Lemma A of **(VIII)**, $(s^b)^*(t) = s^\star(t)$. Hence, by the inductive hypothesis and the fact that s# is obtained from s^b by substituting $(s^b)^*(t)$ for the i^{th} component of s^b, it follows that s# satisfies $\mathfrak{B}(x_i)$ if and only if s^b satisfies $\mathfrak{B}(t)$. Since s^b satisfies $\mathfrak{B}(t)$, s# satisfies $\mathfrak{B}(x_i)$.

Conversely, assume s′ satisfies $(x_j)\mathfrak{B}(x_i)$. Let s^b differ from s in at most the j^{th} place. Let s# be the same as s′ except in the j^{th} place, where it is the same as s^b. Then s# satisfies $\mathfrak{B}(x_i)$. As above, $s^\star(t) = (s^b)^*(t)$. Hence, by the inductive hypothesis, s^b satisfies $\mathfrak{B}(t)$ if and only if s# satisfies $\mathfrak{B}(x_i)$. Since s# satisfies $\mathfrak{B}(x_i)$, s^b satisfies $\mathfrak{B}(t)$. Therefore, s satisfies $(x_j)\mathfrak{B}(t)$.

Proof of Corollary (ii). Assume s satisfies $(x_i)\mathfrak{A}(x_i)$. We must show that s satisfies $\mathfrak{A}(t)$. Let s′ arise from s by substituting $s^\star(t)$ for the i^{th} component of s. Since s satisfies $(x_i)\mathfrak{A}(x_i)$ and s′ differs from s in at most the i^{th} place, s' satisfies $\mathfrak{A}(x_i)$. By Corollary (i), s satisfies $\mathfrak{A}(t)$.

2.15. Assume $\mathfrak{A}$ is satisfied by a sequence s. Let s′ be any sequence. By **(VIII)**, s′ also satisfies $\mathfrak{A}$. Hence, $\mathfrak{A}$ is satisfied by all sequences, i.e., $\models_M \mathfrak{A}$.

2.16. (a) x is a common divisor of y and z.

(d) x_1 is a bachelor.

2.17. (a) (i) Every non-negative integer is even or odd. True.

(ii) If the product of two non-negative integers is zero, at least one of them is zero. True.

(iii) 1 is even. False.

2.18. (a) Consider an interpretation with domain the set of integers. Let $A_1^1(x)$ mean that x is even, and let $A_2^1(x)$ mean that x is odd. Then $(x_1)A_1^1(x_1)$ is false, and so, $(x_1)A_1^1(x_1) \supset (x_1)A_2^1(x_1)$ is true. However, $(x_1)(A_1^1(x_1) \supset A_2^1(x_1))$ is false, since it asserts that all even integers are odd.

2.19. (a) $[(x_i)^{-}\,\mathfrak{A}(x_i) \supset \sim \mathfrak{A}(t)] \supset [\mathfrak{A}(t) \supset \sim (x_i)^{-}\,\mathfrak{A}(x_i)]$ is logically valid because it is an instance of the tautology $(A \supset^{-} B) \supset (B >^{-} A)$. By (X), $(x_i) \sim \mathfrak{A}(x_i) \supset \sim \mathfrak{A}(t)$ is logically valid. Hence, by (111), $\mathfrak{A}(t) \supset \sim (x_i)^{-}\,\mathfrak{A}(x_i)$ is logically valid.

(b) Intuitive proof: If $\mathfrak{A}$ is true for all x_i, then $\mathfrak{A}$ is true for some x_i. Rigorous proof: Assume $(x_i)\mathfrak{A} \supset (Ex_i)\mathfrak{A}$ is not logically valid. Then there is an interpretation M for which it is not true. Hence, there is a sequence s in Σ such that s satisfies $(x_i)\mathfrak{A}$ and s does not satisfy $\sim (x_i)^{-}\,\mathfrak{A}$. From the latter, s satisfies (x,) $\sim \mathfrak{A}$. Since s satisfies $(x_i)\mathfrak{A}$, s satisfies $\mathfrak{A}$, and, since s satisfies $(x_i) \sim 8$, s satisfies $\sim \mathfrak{A}$. But then, s satisfies $\mathfrak{A}$ and s satisfies $^{-}\,\mathfrak{A}$, which is impossible.

2.21. (a) Let the domain be the set of integers, and let $A_1^2(x, y)$ mean that either $x < y$ or ($x = y$ and x is even). Verify that the negation of the given wf is true for this interpretation.

(b) Let $A_1^2(x, y)$ mean that $x < y$ in the domain of integers.

2.23. (a) The premises are: (i) $(x)(S(x) \supset U(x))$, (ii) $(x)(H(x) \supset \sim U(x))$, (iii) $(x)(\sim S(x) \supset \sim V(x))$, and the conclusion is (iv) $(x)(H(x) \supset \sim V(x))$. Intuitive proof: Assume $H(x)$. By (ii), $\sim U(x)$, and, therefore, by (i), $\sim S(x)$. Hence, by (iii), $\sim V(x)$. Thus, $\sim V(x)$ follows from $H(x)$, and

(iv) holds. A more rigorous proof can be given along the lines of (I)-(XI), but a better proof will become available after the study of predicate calculi.

2.24. (a) Let the domain consist of just one object, and let A_1^2 be the identity relation.

2.26. (a)

1.	$(x_i)(\mathfrak{A} \supset \mathfrak{B})$	**Hyp**
2.	$(x_i)\mathfrak{A}$	**Hyp**
3.	$(x_i)(\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \mathfrak{B})$	Axiom (4)
4.	$\mathfrak{A} \supset \mathfrak{B}$	1, 3, MP
5.	$(x_i)\mathfrak{A} \supset \mathfrak{A}$	Axiom (4)
6.	$\mathfrak{A}$	2, 5, MP
7.	$\mathfrak{B}$	4, 6, MP
8.	$(x_i)\mathfrak{B}$	7, Gen
9.	$(x_i)(\mathfrak{A} \supset \mathfrak{B}), (x_i)\mathfrak{A} \vdash (x_i)\mathfrak{B}$	1-8
10.	$(x_i)(\mathfrak{A} \supset \mathfrak{B}) \vdash (x_i)\mathfrak{A} \supset (x_i)\mathfrak{B}$	1-9, Cor. 2.5
11.	$\vdash (x_i)(\mathfrak{A} \supset 4) \supset ((x_i)\mathfrak{A} \supset (x_i)\mathfrak{B})$	1-10, Cor. 2.5

2.27. Hint: Assume $\vdash_K \mathfrak{A}$. By induction on the number of steps in a proof of $\mathfrak{A}$ in K, prove that, for any variables $y_1, \ldots,$ y, $(n \geqslant 0)$, $\vdash_{K\#}(y_1) \ldots (y_n)\mathfrak{A}$.

231. (a) Assume K complete, and let $\mathfrak{A}$ and $\mathfrak{B}$ be closed **wfs** of K such that $\vdash_K \mathfrak{A} \vee \mathfrak{B}$. Assume not-$\vdash_K \mathfrak{A}$. Then, by completeness, $\vdash_K {}^{-}\,\mathfrak{A}$. Hence, by the tautology $\sim A \supset ((A \vee B) \supset B)$, $\vdash_K \mathfrak{B}$.

(b) Assume K is not complete. Then there is a sentence $\mathfrak{A}$ of K such that not-$\vdash_K \mathfrak{A}$ and not-$\vdash_K {}^{-}\,8$. However, $\vdash_K \mathfrak{A} \vee {}^{-}\,8$.

232. See Tarski-Mostowski-Robinson [1953], pp. 15–16.

235. Assume $\mathfrak{A}$ not logically valid. Then the closure 4 of $\mathfrak{A}$ is not logically valid. Hence, the theory K with $^{-}\,\mathfrak{B}$ as its only proper axiom has a model. By the Skolem-Lowenheim Theorem, K has a denumerable model, and, by the Lemma in the proof of Corollary 2.17, K has a model of cardinality a. Hence, $\mathfrak{B}$ is false in this model, and, therefore, $\mathfrak{A}$ is not true in some model of cardinality a.

237. (b) It suffices to assume $\mathfrak{A}$ is a closed wf. (Otherwise, look at the closure of d.) We can effectively write down all the interpretations on a finite domain $\{b,, \ldots, b_k\}$. (We need only specify the interpretations of the symbols occurring ın d.) For every such interpretation, replace every wf $(x)\mathfrak{B}(x)$, where $\mathfrak{B}(x)$ has no quantifiers, by $\mathfrak{B}(b_1) \wedge \ldots \wedge \mathfrak{B}(b_k)$, and continue until no quantifiers are left. One can then evaluate the truth of the resulting wf for the given interpretation.

2.41. Assume K_1 not finitely **axiomatizable.** Let the axioms of K_1 be $\mathfrak{A}_1, \mathfrak{A}_2, \ldots,$ and let the axioms of K_2 be $\mathfrak{B}_1, \mathfrak{B}_2, \ldots$. Then $\{\mathfrak{A}_1, \mathfrak{B}_1, \mathfrak{A}_2, \mathfrak{B}_2, \ldots)$ is consistent. (For, if not, some finite subset $\{\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k, \mathfrak{B}_1, \ldots, \mathfrak{B}_m\}$ is inconsistent. **Since** K_1 is not finitely **axiomatizable**, there is a theorem $\mathfrak{A}$ of K, such that $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k \vdash \mathfrak{A}$ does not **hold.** Hence, the theory with axioms $\{\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k, \sim \mathfrak{A}\}$ has a model M. Since $\vdash_{K_1}\mathfrak{A}$, M must be a model of K_2, and, therefore, M is a model of $\{\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k, \mathfrak{B}_1, \ldots, \mathfrak{B}_m\}$, contradicting the inconsistency of this set of **wfs.)** Since $\{\mathfrak{A}_1, \mathfrak{B}_1, \mathfrak{A}_2, \mathfrak{B}_2, \ldots)$ is consistent, it has a model, which must be a **model** of both K, and K_2.

2.42. Hint: Let the closures of the axioms of K be $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$. Choose a *subsequence* $\mathcal{A}_{j_1}, \mathcal{A}_{j_2}, \ldots$ such *that* $\mathcal{A}_{j_{n+1}}$ *is the first sentence (if any) after* $\mathcal{A}_{j_n}$ *which is not deducible from* $\mathcal{A}_{j_1} \wedge \ldots \wedge \mathcal{A}_{j_n}$. *Let* $\mathcal{B}_k$ *be* $\mathcal{A}_{j_1} \wedge \mathcal{A}_{j_2} \wedge \ldots \wedge \mathcal{A}_{j_k}$. *Then the* $\mathcal{B}_k$'s *form an axiom set for the theorems of K such that* $\vdash \mathcal{B}_{k+1} \supset \mathcal{B}_k$ *but not-I-* $\mathcal{B}_k \supset \mathcal{B}_{k+1}$. *Then* $\{\mathcal{B}_1, \mathcal{B}_1\ 3\ \mathcal{B}_2, \mathcal{B}_2 \supset \mathcal{B}_3, \ldots)$ *is an independent axiomatization of K.*

2.44. *(c) Use Proof by Contradiction (Exercise* 2.43(e)).

1. $(y) \sim (A_1^1(y) \supset (y)A_1^1(y))$	Hyp
2. $\sim (A_1^1(y) \supset (y)A_1^1(y))$	*1, Rule A4*
3. $A_1^1(y)$	*2, Tautology*
4. $\sim (y)A_1^1(y)$	*2, Tautology*
5. $(y)A_1^1(y)$	*3, Gen*
6. $(y)A_1^1(y) \wedge \sim (y)A_1^1(y)$	*4, 5, Conjunction* Introduction

By Proof by Contradiction, $\vdash \sim (y) \sim (A_1^1(y) \supset (y)A_1^1(y))$, i.e., $\vdash (Ey)(A_1^1(y) \supset (y)A_1^1(y))$.

2.46. *(i) (a) Assume* I- $\mathcal{A}$. *By moving the negation step-by-step inward to the atomic wfs, show that* $\sim \mathcal{A}^\star$ *is logically equivalent to the wf* $\mathcal{B}$ *obtained from* $\mathcal{A}$ *by replacing all atomic wfs by their negations. But, from* $\vdash \mathcal{A}$ *it can be shown that* I- $\mathcal{B}$. *Hence,* **t—** $\mathcal{A}^\star$. *The converse follows by noting that* $(\mathcal{A}^\star)^\star$ *is* $\mathcal{A}$.

(b) *Apply Part (a) to* $\sim \mathcal{A} \vee \mathcal{B}$.

2.48. (b) $(E\varepsilon)(\varepsilon > 0$ **A** $(\delta)(\delta > 0 \supset (Ex)(|x - c| < \delta$ **A** $^{-}$ $|f(x) - f(c)| < \varepsilon)))$

2.52.

1. $(Ey)(x)(A_1^2(x,y) \equiv \sim A_1^2(x,x))$	Hyp
2. $(x)(A_1^2(x,b) \equiv \sim A_1^2(x,x))$	*1, Rule C*
3. $A_1^2(b,b) \equiv \sim A_1^2(b,b)$	*2, Rule A4*
4. $\mathcal{C} \wedge \sim \mathcal{C}$	*3, Tautology*

($\mathcal{C}$ *is any wf not containing b.)*
Use Proposition 2.23 and Proof by Contradiction.

2.59. *(a) In step 4, b is not a new individual constant. It was used in step 2.*

2.61. *(c)*

1. $x = x$	*Proposition* 2.24(a)
2. $(Ey)(x = y)$	*1, Rule* E4
3. $(x)(Ey)(x = y)$	*2, Gen*

2.64. *(a) The problem obviously reduces to the case of substitution for a single variable at a time:*

$\vdash x_1 = y_1 \supset t(x_1) = t(y_1)$. *From* (7),

$\vdash x_1 = y_1 \supset (t(x_1) = t(x_1) \supset t(x_1) = t(y_1))$. *By Proposition* 2.24(a),

$\vdash t(x_1) = t(x_1)$. *Hence,* $\vdash x_1 = y_1\ 3\ (t(x_1) = t(y_1))$.

2.66. *By Exercise* 2.61(c), $\vdash (Ey)(x = y)$. *By Proposition* 2.24(b), *(c),* I- $(y)(z)(x = y \wedge x = z \supset y = z)$. *Hence,* $\vdash (E_1 y)(x = y)$. *By Gen,* I- $(x)(E_1 y)(x = y)$.

2.70. (b) *(i) Let* $\bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j$ *stand for the conjunction of all wfs of the form* $x_i \neq x_j$, *where* $1 \leqslant i < j \leqslant n$. *Let* $\mathcal{B}_n$ *be* $(Ex_1) \ldots (Ex_n) \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j$.

(ii) Assume there is a theory with axioms $\mathcal{A}_1, \ldots, \mathcal{A}_n$, *having the same theorems as K. Each of* $\mathcal{A}_1, \ldots, \mathcal{A}_n$ *is provable from* $\mathbf{K}_1$ *plus a finite number of the wfs* $\mathcal{B}_1, \mathcal{B}_2, \ldots$. *Hence,* $\mathbf{K}_1$ *plus a finite number of the wfs* $\mathcal{B}_{j_1}, \ldots, \mathcal{B}_{j_n}$ *sufficesto prove all theorems of K. We may assume* $j_1 < \ldots < j_n$. *Then an interpretation whose domain consists of* j_n *objects would be a model of K, contradicting the fact that* $\mathcal{B}_{j_n+1}$ *is an axiom of K.*

2.75.

$$(x)(Ey)((Ez)(\mathcal{A}(z,x,y,\ldots,y) \wedge A_1^3(x,y,z)) \supset (Ez)(\mathcal{A}(z,y,x,\ldots,x) \wedge z = x)).$$

2.76.

$$(Ez)(w)(Ex)\big([A_1^1(x) \supset A_1^2(x,y)] \supset [A_1^1(w) \supset A_1^2(y,z)]\big).$$

2.80. $\mathcal{B}$ *has the form* $(Ex)(Ey)(z)([A_1^2(x,y) \supset A_1^1(x)] \supset A_1^1(z))$. *Let the domain D be* $\{1, 2)$, *let* A_1^2 *be* $<$, *and let* $A_1^1(u)$ *stand for* $u = 2$. *Then* $\mathcal{B}$ *is true, but* $(x)(Ey)A_1^2(x,y)$ *is false.*

2.81. *Let g be a one-one correspondence between D' and D. Define:* $(a_j)^{M'} = g((a_j)^M)$; $(f_j^n)^{M'}(b_1, \ldots, b_n) = g^{-1}[(f_j^n)^M(g(b_1), \ldots, g(b_n))]$ $\vDash_{M'} A_j^n[b_1, \ldots, b_n]$ *if and only if* $\vDash_M A_j^n[g(b_1), \ldots, g(b_n)]$.

2.88. *Hint: Extend K by adding axioms* $\mathcal{B}_n$, *where* $\mathcal{B}_n$ *asserts that there are at least* n *elements. The new theory has no finite models.*

2.89. *Hint: Consider the wfs* $\mathcal{B}_n$, *where* $\mathcal{B}_n$ *asserts that there are at least* n *elements. Use elimination of quantifiers, treating the* $\mathcal{B}_n$'s *as* if *they were atomic wfs.*

2.94. *Let W be any set. For each b in W, let* a_b *be an individual constant. Let the theory K have as its proper axioms:* $a_b \neq a_c$ *for all b,* c *in W such that* $b \neq c$, *plus the axioms for a total order. K is consistent, since any finite subset of its axioms has a model. (For, any such finite subset contains only a finite number of individual constants. One can define a total order on any finite set B by using the one-one correspondence between B and a set* $\{1, 2, 3, \ldots, n\}$ *and carrying over to B the total order* $<$ *on* $\{1, 2, 3, \ldots, n)$.) *Since K is consistent, K has a model M by the Generalized Completeness Theorem. The domain D of M is totally ordered by the relation* $<^M$; *hence, the subset* $\mathbf{D_W}$ *of D consisting of the objects* $(a_b)^M$ *is totally ordered by* $<^M$. *This total ordering of* $\mathbf{D_W}$ *can then be* carried *over to a total ordering of W :* $b <_W c$ *if and only if* $a_b <^M a_c$.

2.97. *Assume* $\mathbf{M}_1$ *finite and* $\mathbf{M}_1 \equiv \mathbf{M}_2$. *Let the domain* $\mathbf{D}_1$ *of* $\mathbf{M}_1$ *have* n *elements. Then, since the assertion that a model has exactly* n *elements can be written as a sentence, the domain* $\mathbf{D}_2$ *of* $\mathbf{M}_2$ *must also have* n *elements. Let* $D_1 = \{b_1, \ldots, b_n\}$ *and* $\mathbf{D}_2 = \{c_1, \ldots, c_n\}$. *Assume* $\mathbf{M}_1$ *and* $\mathbf{M}_2$ *not isomorphic. Let* φ *be any one of the n! one-one correspondences between* $\mathbf{D}_1$ *and* $\mathbf{D}_2$. *Since* φ *is not an isomorphism, either: (1) there is an individual constant a and an element* b_j *of* $\mathbf{D}_1$ *such that either (i)* $b_j = a^{M_1} \wedge \varphi(b_j) \neq a^{M_2}$, *or* (ii) $b_j \neq a^{M_1} \wedge \varphi(b_j) = a^{M_2}$; *or (2) there is a function letter* f_k^m *and* $b_l, b_{j_1}, \ldots, b_{j_m}$ *in* $\mathbf{D}_1$ *such that*

$$b_l = (f_k^m)^{M_1}(b_{j_1}, \ldots, b_{j_m}) \text{ and } \varphi(b_l) \neq (f_k^m)^{M_2}(\varphi(b_{j_1}), \ldots, \varphi(b_{j_m}));$$

or (3) there is a predicate letter A_j^{n} *and* $b_{j_1}, \ldots, b_{j_m}$ *in* $\mathbf{D}_1$ *such that either*

(i) $\models_{M1} A_k^m[b_{j_1}, \ldots, b_{j_m}]$ and $\models_{M_2} \sim A_k^m[\varphi(b_{j_1}), \ldots, \varphi(b_{j_m})]$, or (ii)$\models_{M_1} \sim A_k^m[b_{j_1}, \ldots, b_{j_m}]$ and $\models_{M_2} A_k^m[\varphi(b_{j_1}), \ldots, \varphi(b_{j_m})]$. *Construct a* **wf** $\mathfrak{B}_\varphi$ *as follows:*

$$\mathfrak{B}_\varphi \text{ is } \left|\begin{array}{l} x_j = a \text{ if } (1), (i) \text{ holds} \\ x_j \neq a \text{ if } (1), (ii) \text{ holds} \\ x_l = f_k^m(x_{j_1}, \ldots, x_{j_m}) \text{ if } (2) \text{ holds} \\ A_k^m(x_{j_1}, \ldots, x_{j_m}) \text{ if } (3), (i) \text{ holds} \\ \sim A_k^m(x_{j_1}, \ldots, x_{j_m}) \text{ if } (3), (ii) \text{ holds} \end{array}\right.$$

Let $\varphi_1, \ldots, \varphi_{n!}$ *be the one-one correspondences between* $\mathbf{D}_1$ *and* D_2. *Let* $\mathfrak{C}$ *be the wf*

$$(Ex_1)\ldots(Ex_n)\Big(\underset{1 \leqslant i < j \leqslant n}{A} x_i \neq x_j \; A\, \mathfrak{B}_{\varphi_1} \; A\, \mathfrak{B}_{\varphi_2} \; A \ldots A\, \mathfrak{B}_{\varphi_{n!}}\Big).$$

Then $\mathfrak{C}$ *is true for* $\mathbf{M}_1$ *but not for* $\mathbf{M}_2$.

2.98. *(a) There are* $\aleph_\alpha$ *sentences of K. Hence, there are* $2^{\aleph_\alpha}$ *sets of* sentences.If $\mathbf{M}_1 \not\equiv \mathbf{M}_2$, *then the set of sentences true for* $\mathbf{M}_1$ *is differentfromthe set of sentences true for* $M_,$.

2.99. *Let K' be the theory with* $\aleph_\gamma$ *new symbols* b_τ *and, as axioms, all sentences true for M and all* $\mathrm{b}_\tau \neq \mathrm{b}_\rho$ *for* $\tau \neq$ p. *Prove K' consistent and apply Corollary 2.35.*

2.102. *(a) Let M be the field of rational numbers, and* $x = \{-1)$.

2.105. *Consider the wf* $(Ex_2)(x_2 < x_1)$.

2.106. *(a) (ii) Introduce a new individual constant b, and forma new theory by adding to the complete diagram of M all the sentences* $b \neq t$ *for all closed terms of K.*

2.107. *If* 0 4 $\mathfrak{F}$, $\mathfrak{F} \neq \mathfrak{P}(A)$. *Conversely, if* $0 \in 4$, *then, by clause* (iii) *of the definition of filter,* $\mathfrak{F} = 9(A)$.

2.108. *If* $4 = \mathfrak{F}_B$, *then* $\bigcap_{C \in 9} C = B \in 9$. *Conversely,* if $B = \bigcap_{C \in \mathfrak{F}} C \in 9$, *then* $\mathfrak{F} = \mathfrak{F}_B$.

2.109. *Use Exercise 2.108.*

2.110. *(i)* $A \in \mathfrak{F}$, *since* $A = A - 0$. *(ii) If* $B = A - W_1 \in \mathfrak{F}$ *and* $C = A - W_2 \in 4$, *where* W_1 *and* W_2 *are finite, then* $B \cap C = A - (W_1 \cup W_2) \in 4$, *since* W_1 u W_2 *is finite.(iii) If* $B = A - W \in 9$, *where W is finite,and if* $B \subseteq C$, *then* $C = A - (W - C) \in \mathfrak{F}$, *since* $W - C$ *is finite.* (iv) **Let** $B \in \mathfrak{F}$. So, $B = A - W$, *where W is finite. Let* $b \in B$. *Then* $W \cup \{b)$ *is finite. Hence,* $C = A - (W$ u $\{b)) \in \mathfrak{F}$. *But* $B \nsubseteq C$, *since* $b \notin C$. *Therefore,* $\mathfrak{F} \neq \mathfrak{F}_B$.

2.113. *Let* $\mathfrak{F}' = \{DID \subseteq A \wedge (EC)(C \in \mathfrak{F} \wedge B \cap C \subseteq D))$.

2.114. *Assume that, for every* $B \subseteq A$, *either* $B \in \mathfrak{F}$ *or* $A - B \in \mathfrak{F}$. *Let* $\mathfrak{G}$ *be a filter such that* $\mathfrak{F} \subset \mathfrak{G}$. *Let* $B \in \mathfrak{G} - \mathfrak{F}$. **Then** $A - B \in 9$. *Hence,* $A - B \in \mathfrak{G}$. *So,* $0 = B \cap (A - B) \in \mathfrak{G}$, *and* $\mathfrak{G}$ *is improper.The converse follows from Exercise 21 13.*

2.115. *Assume* $\mathfrak{F}$ *is an ultrafilter, and* $B \notin \mathfrak{F}$, $C \notin \mathfrak{F}$. *By Exercise 2.114,* $A - B \in \mathfrak{F}$ *and* $A - C \in 4$. *Hence,* $A - (B \cup C) = (A - B) \cap (A - C) \in \mathfrak{F}$. *Since* 4 *is proper,* B u C 4 4.

Conversely, assume B 4 $\mathfrak{F}$ A C 4 $\mathfrak{F} \supset$ B u $C \notin \mathfrak{F}$. *Since* $B \cup (A - B) = A \in 9$, *this implies that, if* **B** 4 $\mathfrak{F}$, *then* $A - B \in \mathfrak{F}$. *Use Exercise 21 14.*

2.116. *(a) Assume* $\mathfrak{F}_C$ *a principal ultrafilter. Let* $a \in C$, *and assume* $C \neq \{a)$. *Then* $\{a)$ 4 $\mathfrak{F}_C$ *and* $C - \{a)$ 4 $\mathfrak{F}_C$. *By Exercise 2.115,* $C = \{a) \cup (C - \{a))$4 $\mathfrak{F}_C$, *which yields a contradiction.*

(b) *Assume a non-principal ultrafilter* $\mathfrak{F}$ *contains a finite set, and let B be a finite set in* 9 *of least cardinality. Since* 4 *is non-principal, the cardinality of* **B** *is* > 1. *Let* $b \in B$. *Then* $B - \{b\} \neq 0$. *Both* $\{b)$ *and* $B - \{b)$ *are finite sets of lower cardinality than B. Hence,* $\{b)$ 4 9 *and* $B - \{b)$ 4 9. *By Exercise 2.115,* $B = \{b) \cup (B - \{b))$4 $\mathfrak{F}$, *which contradicts the definition of B.*

2.119. *Let* **J** *be the set of all finite subsets of* Γ. *For each A in J,; choose a model* $\mathbf{M}_\Delta$ *of A. For A in J, let* $A^* = \{\Delta' | \Delta' \in J \wedge \Delta \subseteq A')$. *The collection* $\mathfrak{G}$ *of all* Δ^*'s *has the finite-intersection property. By Exercise 2.112, there is a proper filter* $\mathfrak{F} \supseteq \mathfrak{G}$. *By the Ultrafilter Theorem, there is an ultrafilter* $9' \supseteq \mathfrak{F} \supseteq \mathfrak{G}$. *Consider* $\prod_{\Delta \in J} \mathbf{M}_\Delta/\mathfrak{F}'$. *Let* $\mathfrak{C} \in \Gamma$. *Then* $\{\mathfrak{C}\}^* \in \mathfrak{G} \subseteq \mathfrak{F}'$. *Therefore,* $\{\mathfrak{C}\}^* \subseteq \{\Delta | \Delta \in J \wedge \models_{M_\Delta} \mathfrak{C}\} \in \mathfrak{F}'$. *By* **Łoś's** *Theorem,* $\mathfrak{C}$ *is true in* $\prod_{\Delta \in J} \mathbf{M}_\Delta/\mathfrak{F}'$.

2.120. *(a) Assume* $\mathfrak{W}$ *is closed under elementary equivalence and ultraproducts. Let A be the set of all sentences of K which are true in every model in* $\mathfrak{W}$. *Let M be any model of A. We must show that M is in* $\mathfrak{W}$. *Let* Γ *be the set of all sentences true for M. Let J be the set of finite subsets of* Γ. *For* $\Gamma' = \{\mathfrak{C}_1, \ldots, \mathfrak{C}_n\} \in J$, *choose a model* $\mathbf{N}_{\Gamma'} \in \mathfrak{W}$ **such** *that* $\mathfrak{C}_1 \wedge \ldots \wedge \mathfrak{C}_n$ *is true in* $\mathbf{N}_{\Gamma'}$. *(If there were no such model,* $\sim(\mathfrak{C}_1 \wedge \ldots \wedge \mathfrak{C}_n)$, *although false in M, would be in A.) As in Exercise 21 19, there is an ultra-filter* $\mathfrak{F}'$ *such that* $N^* = \prod_{\Gamma' \in J} \mathbf{N}_{\Gamma'}/\mathfrak{F}'$ *is a model of* Γ. *Now,* $N^* \in \mathfrak{W}$. *Moreover,* $M \equiv N^*$. *Hence,* $M \in \mathfrak{W}$.

(b) *Use Part (a) and Exercise 2.41.*

(c) Let $\mathfrak{W}$ *be the class of all fields of characteristic zero. Let J be a non-principal ultrafilter on the set P of primes, and consider* $M = \prod_{p \in \mathrm{P}} \mathbf{Z}_p/\mathfrak{F}$, *where* Z_p *is the field of integers modulop. Apply Part* (b).

2.121. $\mathrm{R}^\# \subseteq R^*$. *Hence, the cardinality of* R^* *is* $\geqslant 2^{\aleph_0}$. *On the other hand,* R^w *is equinumerous with* 2^ω, *and, therefore,has cardinality* $2^{\aleph_0}$. *But the cardinality of* R^* *is at most that of* R^w.

2.122. *Assume x and y are infinitesimals. Let* ε *be any positive real. Then* $|x| < \varepsilon/2$ *and* $|y| < \varepsilon/2$. *So,* $|x + y| \leqslant |x| + |y| < \varepsilon/2 + \varepsilon/2 = \varepsilon$; $|xy| = |x|\,|y| < 1 \cdot \varepsilon = \varepsilon$; $|x - y| \leqslant |x| + |-y| < \varepsilon/2 + \varepsilon/2 = \varepsilon$.

2.123. *Assume* $|x| < r_,$, *and* $|y| < \varepsilon$ *for all positive real* ε. *Let* ε *be a positive real. Then* ε/r_1 *is a positive real. Hence* $|y| < \varepsilon/\mathrm{r}_1$, *and so,* $|xy| = |x|\,|y| < \mathrm{r}_1(\varepsilon/\mathrm{r}_1) = \varepsilon$.

2.125. *Assume* $x - r$, *and* $x - \mathrm{r}_2$ *are infinitesimals, with* r_1 *and* r_2 *real. Then* $(x - r,) - (x - \mathrm{r}_2) = \mathrm{r}_2 - \mathrm{r}_1$ is *infinitesimal and real. Hence,* $\mathrm{r}_2 - \mathrm{r}_1 = 0$.

2.126. *(a)* $x - \mathrm{st}(x)$ *and* $y - \mathrm{st}(y)$ *are infinitesimals. Hence, their sum* $(x + y) - (\mathrm{st}(x) + \mathrm{st}(y))$ *is an infinitesimal. Since* $\mathrm{st}(x) + \mathrm{st}(y)$ *is real,* $\mathrm{st}(x) + \mathrm{st}(y) = \mathrm{st}(x + y)$ *by Exercise 2.125.*

2.127. (a) By Proposition 2.46, $\mathbf{s}^*(n) \approx c_1$ and $\mathbf{u}^*(n) \approx c_2$ for all $n \in \omega^* -$ w. Hence, $\mathbf{s}^*(n) + \mathbf{u}^*(n) \approx c_1 + c_2$ for all $n \in \omega^* -$ w. But $\mathbf{s}^*(n) + \mathbf{u}^*(n) =$ (s $+$ u)$^*(n)$. Apply Proposition 2.46.

2.128. Assume f continuous at c. Take any positive real E. Then there is a positive real δ such that $(x)(x \in$ B $\wedge |x - c| < \delta \supset |f(x) - f(c)| <$ E) holds in $\mathfrak{R}$. Therefore, $(x)(x \in$ B* $\wedge |x - c| < \delta \supset |f^*(x) - f(c)| <$ E) holds in $\mathfrak{R}^*$. So, if $x \in B^*$ and $x \approx$ c, then $|x - c| < \delta$, and, therefore, $|f^*(x) - f(c)| <$ E. Since E was arbitrary, $f^*(x) \approx f(c)$.

Conversely, assume $x \in$ B* $\wedge\, x \approx$ c $\supset f^*(x) \approx f(c)$. Take any positive real E. Let δ_0 be a positive infinitesimal. Then $(x)(x \in$ B* $\wedge |x - c| < \delta_0 \supset |f^*(x) - f(c)| <$ E) holds for $\mathfrak{R}^*$. Hence, $(E\delta)(\delta > 0 \wedge (x)(x \in B^* \wedge |x - c| < \delta \supset |f'(x) - f(c)| <$ E)) holds for $\mathfrak{R}^*$, and so, $(E\delta)(\delta > 0 \wedge (x)(x \in$ B A $|x - c| < \delta \supset |f(x) - f(c)| <$ E)) holds in $\mathfrak{R}$.

2.129. Since $x \in B^* \wedge x \approx$ c $\supset (f^*(x) \approx f(c) \wedge g^*(x) \approx g(c))$ by Proposition 2.47, we can conclude $x \in$ B* $\wedge\, x \approx$ c $\supset$ (f $+$ $g)^*(x) \approx$ (f $+$ $g)(c)$, and so, by Proposition 2.47, f $+$ g is continuous at c.

2.134. Consider $\mathbf{s}_{\mathfrak{F}} \in$ R*. Since $\mathbf{s}$ is bounded by b, $|\mathbf{s}_{\mathfrak{F}}| <$ b. So, $\mathbf{s}_{\mathfrak{F}} \in \mathbf{R}_1$. Let $r = \mathrm{st}(\mathbf{s}_F)$. Let E be any positive real. Then $|r - \mathbf{s}_{\mathfrak{F}}| <$ E, since $r - \mathbf{s}$ is an infinitesimal. Hence, $\{j|\ |\mathbf{s}_j - r| \leqslant \varepsilon\} \in 5$ (remembering that r stands for $(r^{\#})_{\mathfrak{F}}$). Since the empty set does not belong to 5, there exists j such that $|\mathbf{s}_j - r| < \varepsilon$.

Chapter 3

3.4. Consider the interpretation having as its domain the set of polynomials with integral coefficients such that the leading coefficient is non-negative. The usual operations of addition and multiplication are the interpretations of $+$ and . . Verify that (S1)–(S8) hold, but that Proposition 3.11 is false (substituting the polynomial x for x and 2 for y).

3.5. (a) Form a new theory S' by adding to S a new individual constant b and the axioms b $\neq \mathbf{0}$, b $\neq \bar{1}$, b $\neq \bar{2}$ . . . , b $\neq \bar{n}$, ... Show that S' is consistent, and apply Proposition 2.27 and Corollary 2.35(3).

(b) By a *cortège* let us mean any denumerable sequence of 0's and 1's. There are $2^{\aleph_0}$ corttges. An element c of a denumerable model M of S determines a cortege $(s_0, s_1, s_2, \ldots)$ as follows: $s_i = 0$ if $\vdash_{\mathbf{M}} p_i|c$, and $s_i = 1$ if $\vdash_{\mathbf{M}} \sim (p_i|c)$. Consider now any cortège s. Add a new constant b to S, together with the axioms $\mathfrak{B}_i(b)$, where $\mathfrak{B}_i(b)$ is $p_i|b$ if $s_i = 0$, and $\mathfrak{B}_i(b)$ is $\sim(p_i|b)$ if $s_i = 1$. This theory is consistent and, therefore, has a denumerable model M_s, in which the interpretation of b determines the cortège s. Thus, each of the $2^{\aleph_0}$ cortèges is determined by an element of some denumerable model. Every denumerable model determines denumerably many cortèges. Therefore, if a maximal collection of mutually non-isomorphic denumerable models had cardinality $\mathfrak{m} < 2^{\aleph_0}$, then the total number of cortèges represented in all denumerable models would be $\leqslant \mathfrak{m} \times \aleph_0 < 2^{\aleph_0}$. (We use the fact that the elements of a denumerable model determine the same corteges as the elements of an isomorphic model.)

3.6. Let (D, 0, ') be one model of Peano's Postulates, with $0 \in$ D, and $'$ the successor operation, and let (D#, 0#, $\star$) be another such model. For each x in D, by an x-mapping we mean a function f from $\mathbf{S}_x = \{u|u \in \mathbf{D} \wedge$ u $\leqslant x\}$ into D# such that $f(0) = 0\#$ and $f(u') = (f(u))^\star$ for all u $<$ x. Show by induction that, for every x in D, there is a unique x-mapping (which will be denoted f_x). It is easy to see that, if $x_1 < x_2$, then the restriction of f_{x_2} to $\mathbf{S}_{x_1}$ must be f_{x_1}. Define $F(x) = f_x(x)$ for all x in D. Then F is a function from D into D# such that $F(0) = 0\#$ and $F(x') = (F(x))^\star$ for all x in D. It is easy to prove that F is one-one. (If not, a contradiction results when we consider the least x in D for which there is some y in D such that $x \neq$ y and $F(x) = F(y)$.) To see that F is an isomorphism, it only remains to show that the range of F is D#. If not, let z be the least element of D# not in the range of F. Clearly z $\neq$ 0#. Hence, z = w* for some w. Then w is in the range of F, and so w = $F(u)$ for some u in D. Therefore, $F(u') = (F(u))^\star =$ w* = z, contradicting the fact that z is not in the range of F.

The reason that this proof does not work for models of first-order number theory S is that the proof employs mathematical induction and the least number principle several times, and these uses involve properties which cannot be formulated within the language of S. Since the validity of mathematical induction and the least number principle in models of S is guaranteed to hold, by virtue of Axiom (S9), only for wfs of S, the categoricity proof is not applicable. For example, in a non-standard model for S, the property of being the interpretation of one of the standard integers $\bar{0}$, $\bar{1}$, $\bar{2}$, $\bar{3}$, . . . is not expressible by a wf of S. If it were, then, by Axiom (S9), one could prove that {0, 1, 2, 3, . . . } constitutes the whole model.

3.8. (a) Hint: Show that, for any term r not containing variables, there is a natural number m such that $\vdash_{\mathbf{S}} \mathbf{r} = \bar{\mathrm{m}}$. (b) Use Part (a) and Proposition 1.12.

3.15. Assume $f(x_1, \ldots, x_n) = x_{n+1}$ is expressible in S by $\mathfrak{B}(x_1, \ldots, x_{n+1})$. Let $\mathcal{C}(x_1, \ldots, x_{n+1})$ be $\mathfrak{B}(x_1, \ldots, x_{n+1})$ A $(z)(z < x_{n+1} \supset \sim \mathfrak{B}(x_1, \ldots, x_{n+1}))$. Show that $\mathcal{C}$ represents $f(x_1, \ldots, x_n)$ in S. (Use Proposition 3.8(b).)

Assume, conversely, that $f(x_1, \ldots, x_n)$ is representable in S by $\mathcal{C}(x_1, \ldots, x_{n+1})$. Show that the same wf expresses $f(x_1, \ldots, x_n) = x_{n+1}$ in S.

3.18. To see that $\vdash_{\mathbf{K}} 0 \neq 1$ is necessary, consider the consistent theory K with equality having the same symbols as S and with $(x)(y)(x =$ y) as its only other axiom. Then all functions are representable in K, but $x_1 = x_2$ is not expressible in K.

3.19. $(Ey)_{u<y<v}\mathrm{R}(x_1, \ldots, x_n,$ y) is equivalent to $(Ez)_{z<v \dot{-} (u+1)}\mathrm{R}(x_1, \ldots, x_n,$ z $+$ u $+$ 1), and similarly for the other cases.

3.21. If the relation $\mathrm{R}(x_1, \ldots, x_n,$ y) : $f(x_1, \ldots, x_n) =$ y is recursive, then $C_{\mathbf{R}}$ is recursive, and, therefore, so is $f(x_1, \ldots, x_n) = \mu y(C_{\mathbf{R}}(x_1, \ldots, x_n, y) = 0)$. an versely, if $f(x_1, \ldots, x_n)$ is recursive, $C_{\mathbf{R}}(x_1, \ldots, x_n, y) = \mathrm{sg}|f(x_1, \ldots,$ %) $- y|$ is recursive.

3.22.

$$[\sqrt{n}\,] = \delta\big(\mu y_{y<n+1}(y^2 > n)\big).$$

$$\Pi(n) = \sum_{y<n} \overline{\mathrm{sg}}\,(C_{\mathrm{Pr}}(\mathrm{y})).$$

3.23. $[ne] = \left[n\left(1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!}\right)\right]$, since $n\left(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \ldots\right) < \frac{1}{n!}$. Let $1 + 1 + \frac{1}{2!} + \cdots + \frac{1}{n!} = \frac{g(n)}{n!}$. Then $g(0) = 1$, and $g(n+1) = (n+1)g(n) + 1$. Hence, g is primitive recursive. Therefore, so is $[ne] = \left[\frac{ng(n)}{n!}\right] = \mathrm{qt}(n!, ng(n))$.

3.24. $\mathrm{RP}(y, z)$ stands for $(x)_{x \leqslant y+z}(x|y \wedge x|z \supset x = 1)$.

$$\varphi(n) = \sum_{y \leqslant n} \overline{\mathrm{sg}}(C_{\mathrm{RP}}(y, n)).$$

3.25. $Z(0) = 0, Z(y + 1) = U_2^2(y, Z(y))$.

3.26. Let $v = (p_0p_1 \ldots p_k) + 1$. Some prime q is a divisor of v. Hence $q \leqslant v$. But q is different from $p_0, p_1, \ldots, p_k$. For, if $q = p_j$ then $p_j|v$ and $p_j|p_0p_1 \ldots p_k$ would imply that $p_j|1$, and, therefore, $p_j = 1$. Thus, $p_{k+1} \leqslant q \leqslant (p_0p_1 \ldots p_k) + 1$.

3.29. If Fermat's Last Theorem is true, h is the constant function 2. If Fermat's Last Theorem is false, h is the constant function 1. In either case, h is primitive recursive.

331. List the recursive functions step-by-step in the following way. In the first step, start with the finite list consisting of $Z(x)$, $N(x)$, and $U_1^1(x)$. At the $(n + 1)'''$ step, make one application of substitution, recursion, and the p-operator to all appropriate sequences of functions already in the list after the n^{th} step, and then add the $n + 1$ functions $U_j^{n+1}(x_1, \ldots, x_{n+1})$ to the list. Every recursive function eventually appears in the list.

332. Assume $f_x(y)$ is primitive recursive (or recursive). Then so is $f_x(x) + 1$. Hence, $f_x(x) + 1$ is equal to $f_k(x)$ for some k. Therefore, $f_k(x) = f_x(x) + 1$ for all x, and, in particular, $f_k(k) = f_k(k) + 1$.

333. (a) Let d be the least positive integer in the set Y of integers of the form $au + bv$, where u and v are arbitrary integers; say, $d = au_0 + bv_0$. Then $d|a$ and $d|b$. (To see this for a, let $a = qd + r$, where $0 \leqslant r < d$. Then $r = a - qd = a - q(au_0 + bv_0) = (1 - qu_0)a + (-qv_0)b \in Y$. Since d is the least positive integer in Y and $r < d$, r must be 0. Hence $d|a$.) If a and b are relatively prime, then $d = 1$. Hence, $1 = au_0 + bv_0$. Therefore, $au_0 \equiv 1 \pmod b$.

335. Assume that a function $f(x_1, \ldots, x,)$ is representable in S by the wf $\mathcal{A}(x_1, \ldots, x_n, y)$. Then the wf $\mathcal{B}(x_1, \ldots, x_n, y)$:

$$[((E_1y)\mathcal{A}(x_1, \ldots, x_n, y)) \wedge \mathcal{A}(x_1, \ldots, x_n, y)] \vee$$
$$[(\sim(E_1y)\mathcal{A}(x_1, \ldots, x_n, y)) \wedge y = 0]$$

strongly represents $f(x_1, \ldots, x_n)$.

3.36. $1944 = 2^33^5$. Hence, 1944 is the Gödel number of the expression ( ). $47 = 7 + (8 \cdot 5)$. So, 47 is the Gödel number of the symbol $a_,$.

3.38. (a) $g(f_1^1) = 9 + 8(2^1 \cdot 3^1) = 57$ and $g(a_1) = 15$. So, $g(f_1^1(a_1)) = 2^{57}3^35^{15}7^5$.

339. Assume S consistent. By Proposition 3.31(1), (✠✠) is not provable in S. Hence, by Lemma 2.9, the theory S_g is consistent. Now, $\sim$(✠✠) is equivalent to $(Ex,) \sim\sim \mathfrak{W}_1(\overline{m}, x_2)$. Since there is no proof of (✠✠) in S, $W_1(m, k)$ is false for all natural numbers k, by (I) on p. 159. Hence, $\vdash_S \sim \mathfrak{W}_1(\overline{m}, \overline{k})$ for all natural numbers k. Therefore, $\vdash_{S_g} \sim \mathfrak{W}_1(\overline{m}, \overline{k})$. But, $\vdash_{S_g}(Ex_2) \sim\sim \mathfrak{W}_1(\overline{m}, x_2)$. Thus, S_g is w-inconsistent.

3.40. Assume S consistent. By Proposition 3.31(1), $(x) \sim \mathfrak{W}_1(\overline{m}, x_2)$ is not provable in S. As in the answer to Exercise 3.39, $\vdash_S \sim \mathfrak{W}_1(\overline{m}, \overline{k})$ for all natural numbers k. Thus, S is w-incomplete.

3.42. (a) Assume $\vdash_S$(✠✠). Hence, (✠✠) is true for the standard model. Thus, since (✠✠) says that (✠✠) is unprovable in S, (✠✠) is actually unprovable in S, contradicting our assumption that $\vdash_S$(✠✠).

(b) Assume $\vdash_S \sim$(✠✠). Hence, $\sim$(✠✠) is true for the standard model. Since (✠✠) says that (✠✠) is unprovable in S, (✠✠) must actually be provable in S. But then, what (✠✠) asserts is false, and (✠✠) is a theorem of S which is false in the standard model.

3.43. (a) Assume the "function" form of Church's Thesis, and let A be an effectively decidable set of natural numbers. Then the characteristic function C_A is effectively computable, and, therefore, recursive. Hence, by definition, A is a recursive set.

(b) Assume the "set" form of Church's Thesis, and let $f(x_1, \ldots, x_n)$ be any effectively computable function. Then the relation $f(x_1, \ldots, x_n) = y$ is effectively decidable. Using the functions o^k, σ_i^k of p. 146, let A be the set of all z such that $f(\sigma_1^{n+1}(z), \ldots, \sigma_n^{n+1}(z)) = \sigma_{n+1}^{n+1}(z)$. Then A is an effectively decidable set, and, therefore, recursive. Then $f(x_1, \ldots, x,) = \sigma_{n+1}^{n+1}(\mu z(C_A(z) = 0))$ is recursive.

3.44. Let K be the extension of S having as proper axioms all wfs which are true in the standard model. Apply Corollary 3.34.

3.46. Let $f(x_1, \ldots, x_n)$ be a recursive function. So, $f(x_1, \ldots, x_n) = y$ is a recursive relation, expressible in K by a wf $\mathcal{A}(x_1, \ldots, x_n, y)$. Then f is representable by

$$\mathcal{A}(x_1, \ldots, x_n, y) \wedge (z)(z < y \supset \sim \mathcal{A}(x_1, \ldots, x_n, z)),$$

where $z < y$ stands for $z \leqslant y \wedge z \neq y$.

3.47. (a) Let

$$G(n) = \begin{cases} \text{the Gödel number of } (x_j)\mathcal{A} \text{ if } n \text{ is the Gödel} \\ \text{number of a wf } \mathcal{A} \text{ and } x_j \text{ is the first (in order} \\ \text{of subscripts) variable free in } \mathcal{A} \\ n, \text{ otherwise.} \end{cases}$$

Let $h(n, 0) = n$ and $h(n, y + 1) = G(h(n, y))$. Then $\mathrm{Cl}(n) = h(n, n)$. It suffices to show that $G(n)$ is primitive recursive. Let $v(n) = \mu y_{y<n}(\mathrm{Fml}(n) \wedge \mathrm{Vbl}(y) \wedge \mathrm{Fr}(n, y))$. Then

$$G(n) = \begin{cases} 2^3 * 2^3 * 2^{v(n)} * n * 2^5 \text{ if } \mathrm{Fml}(n) \\ n \text{ otherwise.} \end{cases}$$

(b) If n is the Gödel number of a wf $\mathcal{A}$, then there is a proof either of the closure of $\mathcal{A}$ or of the negation of the closure of $\mathcal{A}$, i.e., $(Ey)(\mathrm{Pf}(y, \mathrm{Cl}(n)) \vee \mathrm{Pf}(y, 2^3 * 2^9 * \mathrm{Cl}(n) * 2^5) \vee \overline{}\ \mathrm{Fml}(n))$. (Here, the proof predicate Pf is defined with respect to a theory K' which, by the recursive **axiomatizability** of K, has the same theorems as K and has a recursive set of axioms. By Proposition **3.26(13(b)),** this insures that Pf is recursive.) Abbreviating this last formula by $(Ey)\mathfrak{B}(y, \mathrm{n})$, we know, by the p-operator Rule (VI), that $\mu y(\mathfrak{B}(\mathrm{y}, \mathrm{n}))$ is a recursive function. Therefore, $\mathrm{Pf}(\mu y(\mathfrak{B}(\mathrm{y}, \mathrm{n})), \mathrm{Cl}(n))$ is recursive, but it is equivalent to $\mathrm{Cl}(n)$ being in T_K, which, in turn, is equivalent to n being in T_K. An intuitive result corresponding to the one just proved, namely, that any complete, axiomatic theory is effectively decidable, already has been proved on pp. 96–97. Of course, if one assumes Church's Thesis, this intuitive result and the result of Exercise **3.47(b)** are equivalent.

3.48. If K is recursively decidable, the set of **Gödel** numbers of theorems of K **is** recursive. Taking the theorems of K as axioms, we obtain a **recursive axiomatization.**

3.49. (a) Let k be the **Gödel** number of the wf $\mathfrak{F}$. Then $\mathbf{D(m)} = \mathrm{k}$. Hence, $\vdash_K \mathfrak{D}(\bar{\mathrm{m}}, \bar{\mathrm{k}})$ and $\vdash_K (E_1 x_2)\mathfrak{D}(\bar{m}, x_2)$. Then, $\vdash_K (x_2)(\mathfrak{D}(\bar{\mathrm{m}}, x_2) \supset x_2 = \bar{\mathrm{k}})$. It is now easy to prove $\vdash_K \mathfrak{F} \equiv \mathfrak{A}(\bar{\mathrm{k}})$.

(b) Let K be the theory whose axioms are all true sentences of arithmetic. Assume $\mathfrak{A}$ is a wf such that $\mathfrak{A}(\bar{\mathrm{n}})$ is true if and only if n $\in$ Tr. By Part (a), take a "fixed point" 5 , with **Gödel** number k, for $\sim \mathfrak{A}(x_1)$. Then $\mathfrak{F} \equiv \sim \mathfrak{A}(\bar{\mathrm{k}})$ is true. Hence, $\mathfrak{F}$ is true if and only if $\mathfrak{A}(\bar{\mathrm{k}})$ is false, that is, $\mathfrak{F}$ is true if and only if k $\notin$ Tr. Thus, $\mathfrak{F}$ is true if and only if $\mathfrak{F}$ is false.

(c) Use **Tarski's** Theorem and Exercise 3.34.

(d) Assume K complete. Then $T_K = \mathrm{Tr}$. By Exercise **3.47(b),** K is recursively decidable. Hence, **Tr** is recursive, contradicting Part (a).

(e) Assume there is such a recursive set A, and let it be expressed in K by $\mathfrak{A}(\mathbf{x})$. Let $\mathfrak{F}$, with **Gödel** number k, be a fixed point for $\sim \mathfrak{A}(\mathbf{x})$. Then $\vdash_K \mathfrak{F} \equiv \sim \mathfrak{A}(\bar{\mathrm{k}})$. Since $\mathfrak{A}(\mathbf{x})$ expresses A in K, $\vdash_K \mathfrak{A}(\bar{\mathrm{k}})$ or $\vdash_K \sim \mathfrak{A}(\bar{\mathrm{k}})$. (i) If $\vdash_K \mathfrak{A}(\bar{\mathrm{k}})$, then $\vdash_K \sim \mathfrak{F}$. Therefore, $\mathrm{k} \in \mathbf{Ref}_K \subseteq \bar{\mathrm{A}}$. Hence, $\vdash_K \sim \mathfrak{A}(\bar{\mathrm{k}})$, contradicting the consistency of K. (ii) If $\vdash_K \sim \mathfrak{A}(\bar{\mathrm{k}})$, then $\vdash_K \mathfrak{F}$. So, $\mathrm{k} \in T_K \subseteq$ A, and, therefore, $\vdash_K \mathfrak{A}(\bar{\mathrm{k}})$, contradicting the consistency of K.

3.50. Take as a **normal** model for RR, but not for S, the set of polynomials with integral coefficients such that the leading coefficient is non-negative. Note that $(Ey)(x = \mathrm{y} + \mathrm{y} \vee \mathrm{x} = \mathrm{y} + \mathrm{y} + 1)$ is false in this model but is provable in S.

3.54. Let K_2 be the theory whose axioms are those wfs of K_1 which are provable in K*. The theorems of K_2 are the axioms of K_2. Hence, $\mathrm{x} \in T_{K_2}$ if and only if $\mathrm{Fml}_{K_1}(\mathrm{x}) \wedge \mathrm{x} \in T_{K^\star}$. So, if K* were recursively decidable, **i.e.,** if $T_{K\star}$ were recursive, T_{K_2} **would** be recursive. Since K_2 is a consistent extension of K_1, this would contradict the essential recursive undecidability of K,.

3.55. Compare the proof of Proposition 2.29 (p. 86).

3.56. Hint: By Exercise 3.55, K* is consistent. So, by Exercise **3.54**, K* is essentially recursively undecidable. Hence, by Exercise 3.55, K is recursively undecidable.

3.57. (b) Take $(x)(A_j^1(x) \equiv \mathrm{x} = \mathrm{x})$ as a possible definition of A_j^1.

3.58. Use Exercises 3.56–3.57.

3.59. Use Proposition **3.41(a),** Exercise 3.58, and Exercise **3.47(b).**

Chapter 4

4.15. Let $\mathrm{X} = ((\mathrm{y}_1, y_2\rangle | \mathrm{y}_, = y_2 \wedge \mathrm{y}_1 \in \mathrm{Y})$, **i.e.** X is the class of all ordered pairs (u, u) with $u \in$ Y. Clearly $\mathrm{Un}(X)$ and, for any set x, $(Ev)(\langle v, \mathrm{u}) \in \mathrm{X} \wedge v \in \mathrm{x}) \equiv u \in$ Y n x. so, by Axiom R, M(Y n x).

4.16. $\mathfrak{D}(x) \subseteq \bigcup(\bigcup(x))$ and $\mathfrak{R}(x) \subseteq \bigcup(\bigcup(x))$. Apply Proposition 4.6.

4.17. (a) Assume $u \in \mathrm{x} \times \mathrm{y}$. Then $u = (\mathrm{v}, \mathrm{w}) = ((\mathrm{v}), (\mathrm{v}, \mathrm{w}))$ for some v $\in$ x, $w \in$ y. Then $v \in \mathrm{x} \cup \mathrm{y}$ and $\mathrm{w} \in \mathbf{x} \cup \mathrm{y}$. So, $(\mathrm{v}) \in \mathfrak{P}(x$ u y) and $\{v, w\} \in \mathfrak{P}(x$ u $y)$. Hence, $\{\{v\}, (\mathrm{v}, w\}\} \in \mathfrak{P}(\mathfrak{P}(x$ u $y))$.

(b) Use Part (a), Exercise 4.11, Axiom W, and Proposition 4.6.

4.W. If $\mathrm{Rel}(X)$, then $\mathrm{X} \subseteq \mathfrak{D}(X) \times \mathfrak{R}(X)$. Use Exercise **4.17(b)** and Proposition 4.6.

4.19. Assume $\mathrm{Fnc}(X)$. Then $\mathrm{Fnc}(y1X)$ and $\mathfrak{D}(y1X) \subseteq y$. By Axiom R, M(X"y).

4.20. (a) Let **0** be the class $\{u|u \neq \mathrm{u})$. Assume $M(X)$. Then $\mathbf{0} \subseteq$ X. So, 0 = **0** n X. By **Axiom** S, **M(0).**

4.21. Assume $\mathbf{M}(V)$. Let $\mathrm{Y} = \{x|x \notin \mathrm{x})$. It was proved above that $\sim \mathbf{M}(Y)$. But Y $\subseteq$ V. Hence, by Proposition 4.6, $\sim$ **M(** V).

4.33. Let u be the least $\in$**-element** cf X – Z.

4.36. By Proposition **4.10(4),** Trans (w). By Proposition **4.10(2)** and Proposition **4.7(10),** $\omega \in$ On. If $\omega \in K_I$, then $\omega \in \omega$, contradicting Proposition **4.7(1).** Hence, $\omega \notin K_I$.

4.39. Let $X_1 = X \times (0)$ and $Y_1 = \mathrm{Y} \times (1)$.

4.40. For any $u \subseteq$ x, let the characteristic function C_u be the function with domain x such that $C_u`y = \mathbf{0}$ if $\mathrm{y} \in u$ and $C_u`y = 1$ if $\mathrm{y} \in \mathrm{x} - u$. Let F be the function with domain $\mathfrak{P}(x)$, taking u into C_u. Then $\mathfrak{P}(\mathrm{x}) \underset{F}{\cong} 2^x$.

4.41. For any set u, $\mathfrak{D}(u)$ is a set, by Exercise 4.16.

4.42. If $u \in \mathrm{x}^\mathrm{Y}$, then $u \subseteq \mathrm{y} \times \mathbf{x}$. So, $\mathrm{x}^\mathrm{Y} \subseteq \mathfrak{P}(y \times \mathrm{x})$.

4.43. (a) **0** is the only function with domain **0.**

(b) Define a function F with domain X such that, for any x_0 in X, $F(x_0)$ is the function g in $X^{\{u\}}$ such that $g`u = x_0$. Then $\mathrm{X} \underset{F}{\cong} X^{\{u\}}$.

4.44. If $\mathfrak{D}(u) \neq 0$, then $\mathfrak{R}(u) \neq 0$.

4.45. Assume $\mathrm{X} \underset{F}{\cong} \mathrm{Y}$ and $Z \underset{G}{\cong} Z_1$. If $\sim M(Z_1)$, then $\sim \mathbf{M}(Z)$ and $X^Z = Y^{Z_1} = 0$, by Exercise 4.41. Hence, we may assume $\mathbf{M}(Z_1)$ and $\mathbf{M}(Z)$. Define a function Φ on X^Z: If $f \in X^Z$, let $\Phi`f = F \circ f \circ G^{-1}$. Then $X^Z \underset{\Phi}{\cong} Y^{Z_1}$.

4.46. If X or Y is not a set, then $Z^{X \cup Y}$ and $Z^X \times Z^Y$ are both **0.** We may assume then that X and Y are sets. Define a function Ψ with domain $Z^{X \cup Y}$ as follows: iff $\in Z^{X \cup Y}$, let $\Psi`f = \langle X 1 f, Y 1 \mathrm{f})$. Then $Z^{X \cup Y} \underset{\Psi}{\cong} Z^X \times Z^Y$.

4.47. (a) When $Y = 0 \wedge \sim M(Z)$, $(X^Y)^Z = 0$ and $X^{Y\times Z} = X^0 = \{0\}$.
(b) When $Y \neq 0 \wedge \sim \mathrm{M}(Z)$, then $\sim \mathrm{M}(Y\ x\ Z)$ and $(X^Y)^Z = 0 = X^{Y\times Z}$
(c) When $\sim \mathrm{M}(Y) \wedge Z = 0$, $(X^Y)^Z = 1 = X^0 = X^{Y\times Z}$.
(d) When $\sim \mathrm{M}(Y) \wedge Z \neq 0$, $\sim \mathrm{M}(Y \times Z)$ and $(X^Y)^Z = 0^Z = 0 = X^{Y\times Z}$.
(e) Finally, when $\mathrm{M}(Y)\ A\ \mathrm{M}(Z)$, define a function Θ with domain $(X^Y)^Z$ as follows: For any $f \in (X^Y)^Z$,

$\Theta'f$ is the functionin $X^{Y\times Z}$ such that $(\Theta'f)'(y,z) = (f'z)'y$

for all $(y,z) \in Y \times Z$. Then $(X^Y)^Z \underset{\Theta}{\cong} X^{Y\times Z}$.

4.48. If $\sim \mathrm{M}(Z)$, $(X \times Y)^Z = 0 = 0 \times 0 = X^Z \times Y^Z$. Assume then that $\mathrm{M}(Z)$. Define a function $F : X^Z \times Y^Z \rightarrow (X \times Y)^Z$ as follows: For any $f \in X^Z$, $g \in Y^Z$, $(F`\langle f, g\rangle)'z = (f'z, g'z)$ for all z in Z. Then $X^Z \times Y^Z \underset{F}{\cong} (X \times Y)^Z$.

4.49. This is a direct consequence of Proposition 4.17.

4.54. Use the Schroder-Bernstein Theorem (Proposition 4.2 l(4)).

455. Use Proposition 4.2 l((3)–(4)).

4.56. Assume M is a model of NBG with denumerable domain D. Let z be the element of D satisfying the wf $x = 2^\omega$. Hence, z satisfies the wf $\sim(x \simeq \omega)$. This means that there is no object in D which satisfies the condition of being a one–one correspondence between z and w. Since D is denumerable, there is a one–one correspondence between the set of "elements" of z (that is, the set of objects v in D such that $\models_{\mathrm{M}} \mathrm{v} \in z$) and the set of natural numbers. However, no such one–one correspondence exists within M.

4.57. Define a function F from V into 2, as follows: $F'u = \{u, 0\}$ if $u \neq 0$; $F`0 = \{1, 2)$. Since F is one–one, $V \preccurlyeq 2_c$ Hence, by Exercises 4.21 and 4.50, $\sim \mathrm{M}(2_c)$.

4.58. (h) Use Exercise 4.46.

(i) $2'' \preccurlyeq 2' +_c \mathrm{x} \preccurlyeq 2' +_c 2^{\mathrm{x}} = 2' \times 2 \simeq 2^{\mathrm{x}} \times 2^{1} \simeq 2^{\mathrm{x}+_c 1} \simeq 2''$. Hence, by the Schroder–Bernstein Theorem, $2' +_c \mathrm{x} \simeq 2''$.

4.59. Under the assumption of the Axiom of Infinity, ω is a set such that $(Eu)(u \in \omega)\ A(y)(y \in \omega \supset (Ez)(z \in \omega \wedge y\ C\ z))$. Conversely, assume (*) and let b be a set such that (i) $(Eu)(u \in b)$, and (ii) $(y)(y \in b \supset (Ez)(z \in b \wedge y\ C\ z))$. Let $d = \{u | (Ez)(z \in b \wedge u \subseteq z))$. Since $d \subseteq \mathscr{P}(\bigcup(b))$, d is a set. Define a relation $\mathrm{R} = \{\langle n, v\rangle | n \in \omega \wedge v = \{u | u \in d \wedge u \simeq n))$. Thus, $(n, u) \in R$ if and only if $n \in \omega$ and v consists of all elements of d that are equinumerous with n. R is a one–one function with domain ω and range a subset of $\mathscr{P}(d)$. Hence, by the Replacement Axiom applied to R^{-1}, ω is a set, and, therefore. Axiom I holds.

4.60. Induction on **a** in $(x)(x \simeq a \wedge a \in \omega \supset \mathrm{Fin}(\mathscr{P}(x)))$.

4.61. Induction on a in $(x)(x \simeq a \wedge a \in \omega \wedge (y)(y \in x \supset \mathrm{Fin}(y)) \supset \mathrm{Fin}(\bigcup(x)))$.

4.62. Use Proposition 4.25(1).

4.64. $x \subseteq \mathscr{P}(\bigcup(x))$ and $y \in x \supset y \subseteq \bigcup(x)$.

4.65. Induction on **a** in $(x)(x \simeq a \wedge a \in \omega \supset (x \preccurlyeq y \vee y \preccurlyeq x))$.

4.66. Induction on a in $(x)(x \simeq a \wedge a \in \omega \wedge \mathrm{Inf}(Y) \supset x \preccurlyeq Y)$.

4.67. Use proposition 4.24(3).

4.68. Use Exercise 4.17(2).

4.69. $x^y \subseteq \mathscr{P}(y \times x)$.

4.71. (a) Let Z be a set such that every non-empty set of subsets of Z has a minimal element. Assume $\mathrm{Inf}(Z)$. Let Y be the set of all infinite subsets of Z. Then Y is a non-empty set of subsets of Z without a minimal element.
(b) Prove by induction that, for all a in ω, any non-empty subset of $\mathscr{P}(\alpha)$ has a minimal element. The result then carries over to non-empty subsets of $\mathscr{P}(\mathrm{z})$, where z is any finite set.

4.72. (a) Induction on a in $(x)(x \simeq a \wedge a \in \omega \wedge \mathrm{Den}(y) \supset \mathrm{Den}(x\ U\ y))$.
(b) Induction on a in $(x)(x \simeq a \wedge x \neq 0 \wedge \mathrm{Den}(y) \supset \mathrm{Den}(x \times y))$.
(c) Assume $z \subseteq x$ and $\mathrm{Den}(z)$. Let $z \underset{f}{\simeq} \omega$. Define a function g on x: $g`u = u$ if $u \in x - z$; $g`u = (\check{f})`((f`u)')$ if $u \in z$. (ii) Assume x Dedekind-infinite. Assume $z \subset x$ and $x \underset{J}{\simeq} z$. Let $v \in x - z$. Define a function h on ω such that $h`0 = v$ and $h`(\alpha') = f`(h`\alpha)$ if $a \in w$. Then h is one–one; so, $\mathrm{Den}(h``\omega)$ and $h``\omega \subseteq x$.
(d) Assume $y \notin x$. (i) Assume $x \cup \{y) \underset{f}{\simeq} x$. Define by induction a function g on ω such that $g`0 = y$ and $g`(n+1) = f`(g`n)$. g is a one–one function from ω into x. Hence, x contains a denumerable subset, and, by Part (c), x is Dedekind-infinite. (ii) Assume x Dedekind-infinite. Then, by Part (c), there is a denumerable subset z of x. Assume $z \underset{f}{\simeq} \omega$. Let $c_0 = (f^{-1})`0$. Define a function F as follows: $F'u = u$ for $u \in x - z$; $F`c_0 = y$; $F`u = (f^{-1})`((f`u) - 1)$ for $u \in z - \{c_0\}$. Then $x \underset{F}{\simeq} x \cup \{y)$. If z is $\{c_0, c_1, c_2, \ldots\}$, F takes c_{i+1} into c_i and moves c_0 into y.
(e) Assume $\omega \preccurlyeq x$. By Part (c) x is Dedekind-infinite. Choose $y \notin x$. By Part (d), $x \simeq x \cup \{y)$. Hence, $x +_c 1 = (x \times \{0\}) \cup \{\langle 0, 1\rangle\} \simeq x \cup \{y\} \simeq x$.

4.74. NBG is finitely axiomatizable and has only the binary predicate letter A_2^2. The argument on p. 205 shows that NBG is recursively undecidable. Hence, by Proposition 3.47, the predicate calculus with A_2^2 as its only predicate letter is recursively undecidable.

4.75. (a) Assume $x \preccurlyeq \omega_\alpha$. If $2 \preccurlyeq x$, then, by Proposition 4.32(b) and Proposition 4.35, $\omega_\alpha \preccurlyeq x \cup \omega_\alpha \preccurlyeq x \times \omega_\alpha \preccurlyeq \omega_\alpha \times \omega_\alpha \simeq \omega_\alpha$. If x contains one element, use Exercise 4.72(c), (d).
(b) Use Corollary 4.36.

4.78. (a) $\mathscr{P}(\omega_\alpha) \times \mathscr{P}(\omega_\alpha) \simeq 2^{\omega_\alpha}\ X\ 2^{\omega_\alpha} \simeq 2^{\omega_\alpha +_c \omega_\alpha} \simeq 2^{\omega_\alpha} \simeq \mathscr{P}(\omega_\alpha)$.
(b) $(9(\omega_\alpha))^x \simeq (2^{\omega_\alpha})^x \simeq 2^{\prime\prime\text{-}\times x} \simeq 2^{\omega_\alpha} \simeq \mathscr{P}(\omega_\alpha)$.

4.79. (a) If y were non-empty and finite, $y \simeq y +_c y$ would contradict Exercise 4.67.
(d) By Part (c), let $y = u \cup v$, $u \cap v = 0$, $u \simeq y$, $v \simeq y$. Let $y \underset{J}{\simeq} u$. Define a function g on $\mathscr{P}(y)$ as follows: for $x \subseteq y$, let $g'x = u \cup (f``x)$. Then

g'x $\subseteq$ y and y $\simeq u \preccurlyeq$ g'x $\preccurlyeq$ y. Hence, g'x $\simeq$ y. So, g is a one–one function from $\mathcal{P}(y)$ into $A = \{z|z \subseteq y \wedge z \simeq y)$. **Thus,** $\mathcal{P}(y) \preccurlyeq A$. Since A $\subseteq \mathcal{P}(y)$, $\mathcal{A} \preccurlyeq \mathcal{P}(y)$.

(e) Use Part (d). $\{z|z \subseteq y \wedge z \simeq y) \subseteq \{z|z \subseteq y \wedge \mathrm{Inf}(z)\}$.

(f) By Part (c), let y = u U u, $u \cap$ u = 0, $u \simeq$ y, u $\simeq$ y. Let $u \underset{h}{\simeq}$ u. Define f on y as follows: fx = h'x if x $\in u$ and f'x = (h^{-1})'x if x $\in$ u.

4.80. (a) Use Proposition **4.32(b)**.

(b) (i) $\mathrm{Perm}(y) \subseteq y^y \preccurlyeq (2^y)^y \simeq 2^{y \times y} \simeq 2^y \simeq \mathcal{P}(y)$.

(ii) By Part (a), we may use Exercise **4.79(c)**. Let y = $u \cup$ u, $u \cap$ u = 0, $u \simeq y$, $v \simeq y$. Let $u \underset{H}{\simeq} v$ and $y \underset{G}{\simeq} u$. Define a function F : $\mathcal{P}(y) \rightarrow \mathrm{Perm}(y)$ in the following way. Assume z $\in \mathcal{P}(y)$. Let ψ_z : y $\rightarrow$ y be defined as follows: ψ_z'x = H'x if x $\in G$"z; ψ_z'x = (H^{-1})'x if (H^{-1})'$x \in G$"z; ψ_z'x = x otherwise. Then $\psi_z \in \mathrm{Perm}(y)$. Let F'z = ψ_z. F is one–one. Hence, $\mathcal{P}$(y) $\preccurlyeq \mathrm{Perm}(y)$.

4.81. (a) Use (W.O.) and Proposition 4.17.

(b) The proof of $\vdash$ Zorn $\supset$ (W.O.) in Proposition 4.37 uses only this special case of Zorn's Lemma.

(c) To prove the Hausdorff Maximal Principle (HMP) from Zorn, consider some $\subset$ -chain C_0 in x. Let y be the set of all $\subset$ -chains C in x such that $C_0 \subseteq$ C, and apply Part (b) to y.

Conversely, assume (HMP). To prove (b), assume that the union of each non-empty $\subset$ -chain in a given non-empty set x is also in x. By (HMP) applied to the $\subset$ -chain 0, there is some maximal $\subset$ -chain C in x. Then $\bigcup(C)$ is an $\subset$ -maximal element of x.

(d) Assume the **Teichmüller–Tukey** Lemma (TT). To prove Part (b), assume that the union of each non-empty $\subset$ -chain in a given non-empty set x is also in x. Let y be the set of all $\subset$ -chains in x. y is easily seen to be a set of finite character. Therefore, y contains an $\subset$-maximal element C. Then $\bigcup(C)$ is an $\subset$ -maximal element of x.

Conversely, let x be any set of finite character. In order to prove (TT) by means of Part (b), we must show that, if C is an $\subset$ -chain in x, then $\bigcup(C) \in$ x. By the finite character of x, it suffices to show that every finite subset z of $\bigcup(C)$ is in x. Now, since z is finite, z is a subset of the union of a finite subset W of C. Since C is an $\subset$ -chain, W has an $\subset$ -greatest element w $\in$ x, and z is a subset of w. Since x is of finite character, z $\in$ x.

(e) Assume $\mathrm{Rel}(x)$. Let $u = \{z|(Ev)(v \in \mathcal{D}(x) \wedge$ z = $\{v\} 1 x\}$, that is, z $\in$ u if z is the set of all ordered pairs (u, w) in x, for some fixed u. Apply the Multiplicative Axiom to u. The resulting choice set y $\subseteq$ x is a function with domain $\mathcal{D}$(x).

Conversely, the given property easily yields the Multiplicative Axiom. If x is a set of disjoint non-empty sets, let r be the set of all ordered pairs (u, u) such that $u \in$ x and u $\in$ u. By Part (e), there is a function f $\subseteq$ r such that $\mathcal{D}(f) = \mathcal{D}(r)$ = x. The range $\mathcal{R}(f)$ is the required choice set for x.

(f) By Trichotomy, either x $\prec$ y or y $\prec$ x. If x $\prec$ y, there is a function with domain y and range x. (Assume x $\underset{f}{\simeq}$ y, $\subseteq$ y. Take $c \in$ x. Define g'u = c if $u \in$ y $- y_1$, and g'u = (f^{-1})'u if $u \in y_1$.) Similarly, if y $\prec$ x, there is a function with domain x and range y.

Conversely, to prove (W.O.), apply the assumption *(f)* to x and $\mathcal{H}$'$(\mathcal{P}(x))$. Note that, if $(Ef)(f{:}u \rightarrow$ u $\wedge$ $\mathcal{R}(f)$ = u), then $\mathcal{P}(v) \prec \mathcal{P}(u)$. Therefore, if there were a function f from x onto $\mathcal{H}$'$(\mathcal{P}(x))$, we would have $\mathcal{H}$'$(\mathcal{P}$(x)) $\prec \mathcal{P}(\mathcal{H}$'$(\mathcal{P}$(x))) $\prec \mathcal{P}$(x), contradicting the definition of $\mathcal{H}$'$(\mathcal{P}(x))$. Hence, there is a function from $\mathcal{H}$'$(\mathcal{P}(x))$ onto x. Since $\mathcal{H}$'$(\mathcal{P}$(x)) is an ordinal, one can define a one–one function from x into $\mathcal{H}$'$(\mathcal{P}$(x)). Thus, x $\prec \mathcal{H}$'$(\mathcal{P}$(x)), and, therefore, x can be well-ordered.

4.84. If $<$ is a partial ordering of x, use Zorn's Lemma to obtain a maximal partial ordering $<^*$ of x with $< \subseteq <^*$. But a maximal partial ordering must be a total ordering. (For, if u, u were distinct elements of x unrelated by $<^*$, we could add to $<^*$ all pairs $\langle u_1, v_1 \rangle$ such that $u_1 \leqslant^* u$ and u $\leqslant^* v_1$. The new relation would be a partial ordering properly containing $<^*$.)

4.87. (b) Since $x \times y \simeq x +_c y$, $x \times y = a \cup b$ with $a \cap b = 0$, $a \simeq x$, $b \simeq y$. Let r be a well-ordering of y. (i) Assume there exists u in x such that (u, u) $\in$ a for all u in y. Then y $\preccurlyeq$ a. Since a $\simeq$ x, y $\preccurlyeq$ x, contradicting – (y $\preccurlyeq$ x). Hence, (ii) for any u in x, there exists u in y such that (u, u) $\in$ b. Define **j** : x $\rightarrow$ b such that f'u = (u, u), where u is the r-least element of y such that (u, u) $\in$ b. Since f is one–one, x $\preccurlyeq$ b $\simeq$ y.

(c) Clearly $\mathrm{Inf}(z)$ and $\mathrm{Inf}(x +_c z)$. Then

$$x +_c z \simeq (x +_c z)^2 \simeq x^2 +_c 2 \times (x \times z) +_c z^2 \simeq x +_c 2 \times (x \times z) +_c z.$$

Therefore, x $\times$ z $\preccurlyeq$ 2 $\times$ (x $\times$ z) $\preccurlyeq$ x $+_c 2 \times$ (x $\times$ z) $+_c z \simeq$ x $+_c z$. Conversely, x $+_c z \preccurlyeq$ x $\times$ z by Proposition **4.32(b)**.

(d) If (AC) holds, $(y)(\mathrm{Inf}(y) \supset$ y $\simeq$ y X y) follows from Proposition 4.35 and Exercise **4.81(a)**. Conversely, if we assume y $\simeq y \times$ y for all infinite y, then, by Parts (c) and (b), it follows that x $\preccurlyeq \mathcal{H}$'x for **any** infinite set x. Since $\mathcal{H}$'x is an ordinal, x can be well-ordered. **Thus,** (W.O) holds.

4.89. (a) Let $<$ be a well-ordering of the range of r. Let f'0 be the $<$ **-least** element of $\mathcal{R}(r)$, and let f'(n') be the $<$ **-least** element of those u in $\mathcal{R}(r)$ such that $\langle f$'n, u) $\in$ r.

(b) Assume $\mathrm{Den}(x) \wedge (u)(u \in$ x $\supset u \neq 0)$. Let $\omega \underset{g}{\simeq}$ x. Let r be the set of all pairs (a, b) such that a and b are finite sequences $\langle v_0, v_1, \ldots, v_n \rangle$ and $\langle v_0, v_1, \ldots, v_{n+1} \rangle$ such that, for $0 \leqslant$ i $\leqslant n +$ 1, $v_i \in$ g'i. Since $\mathcal{R}(r) \subseteq \mathcal{D}$(r), (PDC) produces a function h : $\omega \rightarrow \mathcal{D}$(r) such that $\langle h$'n, h'$(n') \rangle \in$ r for all n in o. Define the choice function f by taking, for each u in x, f'u to be the $(g$'$u)^{\text{th}}$ component of the sequence h'$(g$'$u)$.

(c) Assume (PDC) and **Inf**(x). Let r consist of all ordered pairs (u, $u \cup$ (a)), where u U (a) $\subsetneq$ x, **Fin**$(u$ U $(a))$, and a $\notin$ u. By (PDC), there is a function $f : \omega \rightarrow \mathfrak{D}(r)$ such that (f'n, $f`(n')\rangle \in$ r for all $n$ in $\omega$. Define g : $\omega \rightarrow$ x by setting g'n equal to the unique element of $f`(n')$ – f'n. Then g is one–one, and so, $\omega \preccurlyeq$ x.

(d) In the proof of Proposition **4.39(2)**, instead of using the choice function h, apply (PDC) to obtain the **function** f. As the relation r, use the set of all pairs $\langle u$, o) such that u $\in$ c, o $\in$ c, $v \in$ u n X.

4.90. Use transfinite induction.

4.93. Induction on β.

4.94.–4.95. Use transfinite induction and Proposition 4.90.

4.97. Assume u $\subseteq$ H. Let o be the set of ranks p'x of elements x in u. Let $\beta = \bigcup(v)$. Then u $\subseteq \Psi`\beta$. Hence, u $\in \mathscr{P}(\Psi`\beta) = \Psi`(\beta') \subseteq H$.

4.98. Assume $X \neq 0$ A $\sim(Ey)(y \in$ X A y n X $= 0)$. Choose u $\in$ X. Define a function g : $g`0 =$ u n X, $g`(n') = (\bigcup(g`n))$ n X. Let x $= \bigcup(\mathfrak{R}(g))$. Then x $\neq 0$ and $(y)(y \in$ x $\supset y$ n x $\neq$ 0).

4.103. Hint: Assume that the other axioms of NBG are consistent and that the Axiom of Infinity is provable from them. Show that H_ω is a model for the other axioms but not for the Axiom of Infinity.

104. Use $H_{\omega +_0 \omega}$.

Chapter 5

5.1. (a) Any word P is transformed into QP.
(b) Any word P in A is transformed into PQ.
(c) Any word P in A is transformed into Q.
(d) Any word P in A is transformed into $\bar{n}$, where n is the number of symbols in P.

5.2. (a)

$$\begin{array}{ll}
\alpha\xi \rightarrow \cdot\Lambda & (\xi \text{ in } A) \\
\text{a} + \text{-}\,\text{A} & \\
\Lambda \rightarrow \alpha &
\end{array}$$

(b)

$$\begin{array}{ll}
\alpha\xi \rightarrow \xi\alpha & (\xi \text{ in } A) \\
\xi\alpha \rightarrow \cdot\Lambda & (\xi \text{ in } A) \\
\alpha \rightarrow \cdot\Lambda & \\
\Lambda \rightarrow \alpha &
\end{array}$$

(c)

$$\begin{array}{ll}
\xi \rightarrow \Lambda & (\xi \text{ in } A) \\
\alpha\alpha \rightarrow \cdot\Lambda & \\
\Lambda \rightarrow \cdot\alpha &
\end{array}$$

(d)

$$\begin{array}{ll}
\xi\eta\beta \rightarrow \eta\beta\xi & (\xi, \eta \text{ in } A) \\
\alpha\xi \rightarrow \xi\beta\xi\alpha & (\xi \text{ in } A) \\
\beta \rightarrow \gamma & \\
\gamma \rightarrow \Lambda & \\
\alpha \rightarrow \cdot & \\
\rightarrow \alpha &
\end{array}$$

5.3.

$$\begin{array}{ll}
\alpha a_i \rightarrow Q_i\alpha & (i = 1, \ldots, k) \\
\alpha\xi \rightarrow \xi\alpha & (\xi \text{ in } A - \{a_1, \ldots, a_k\}) \\
\alpha \rightarrow \cdot\Lambda & \\
\Lambda \rightarrow \alpha &
\end{array}$$

5.4. (d) $1 \bullet 1 \rightarrow \bullet$
$\bullet \rightarrow 1$
(e) $1 \bullet 1 + 1$
(f) Let a, β, δ be new symbols.

$$\begin{array}{c}
\beta 1 \rightarrow 1\beta \\
\alpha 1 \rightarrow 1\beta\alpha \\
\alpha \rightarrow \Lambda \\
11\delta \rightarrow 1\delta\alpha \\
1\delta \rightarrow 1 \\
\delta 11 \rightarrow \delta 1 \\
\delta 1 \rightarrow 1 \\
\delta \rightarrow 1 \\
\beta \rightarrow 1 \\
1 \bullet 1 \rightarrow \delta
\end{array}$$

5.6. In the notation of the proof of Proposition 5.10, let $\varphi(\text{e}, \text{x}) = \mu\text{y}(W_A(\text{x}) \wedge \text{Der}(\text{e}, \text{x}, \text{y})) \vee \sim W_A(\text{x}))$ and $\psi(\text{e}, \text{x}) = (\varphi(e, x))_{1h(\varphi(e, x)) - 1}$. If e is the index of an algorithm schema for an algorithm $\mathfrak{A}$ in A and if x is the **Gödel** number of a word P in A, then ψ(e, x) is the **Gödel** number of the word $\mathfrak{A}(P)$ if $\mathfrak{A}(P)$ is defined; otherwise, ψ(e, x) is not defined. Let 6 be a normal algorithm over M computing ψ(e, x). Let $\mathfrak{T}_1$ be the normal algorithm over M of p. 235, and let $\mathfrak{I}$ be the identity algorithm in A $\cup$ M. By Corollary 5.2, there is a juxtaposition algorithm 3 such that, for any natural number e and any word P in A, $\mathfrak{J}(\bar{\text{e}} \bullet \text{P}) = \bar{\text{e}} \bullet g(P)$. Let $\mathfrak{T}_2$ be the algorithm of Exercise 5.5. Let $\mathfrak{B}$ be the composition $\mathfrak{T}_2 \circ 6 \circ 3$.

5.7. Let $\varphi(x_1, \ldots, x_n)$ be a total partial recursive function. By Proposition **5.8**, φ is Markov-computable. Hence, by Corollary 5.11, φ is recursive.

5.8. Since two fully equivalent algorithms are equivalent, one direction is easy. Assume that every algorithm in A is equivalent relative to A to some normal algorithm over A. Let $\mathfrak{A}$ be an algorithm in A. Then $\mathfrak{A}$ is equivalent relative to A to some normal algorithm b. Let the alphabet of $\mathfrak{B}$ be B $\supseteq$ A. Let 3 be a normal algorithm in B such that $\mathfrak{J}(P)$ is defined only for words P in A, and $\mathfrak{J}(P)$ = P for all words P in A. (Its schema is $\xi \rightarrow \xi$ (ξ in B – A).) Then $\mathfrak{A}$ is fully equivalent relative to A to $\mathfrak{J} \circ \mathfrak{B}$.

5.9. (b)

$$\begin{array}{ll}
\alpha\xi \rightarrow \xi\alpha & (\xi \text{ in } B) \\
\alpha T(\xi) \rightarrow \xi\alpha & (\xi \text{ in } A) \\
\alpha \rightarrow \cdot\Lambda & \\
\Lambda \rightarrow \alpha &
\end{array}$$

5.10. δ(x).

5.11. For example, U_2^3 is computable by the Turing machine

$q_0\, 1\, S_0 q_0$
$90 S_0\, Rq_1$
$q_1\, 1 1\, q_0$
$q_1\, S_0\, Rq_2$

$q_2\, 1\, Rq_2$
$q_2\, S_0\, Rq_3$
$q_3\, 1\, S_0 q_4$
$94\, 1 1\, q_3$

5.12.

$q_0\, 1\, S_2 q_1$
$q_1\, S_2\, Rq_1$
$q_1\, 1\, Rq_1$
$q_1\, S_0\, Lq_2$
$q_2\, 1\, S_0 q_2$

$q_2\, S_0\, Lq_3$
$q_3\, 1\, Lq_3$
$q_3\, S_2\, 1 q_4$
$q_4\, 1\, Rq_0$
$q_0\, S_0\, Lq_5$

5.13

$q_0\, 1\, S_0\, q_0$
$q_0\, S_0\, R\, q_1$
$q_1\, 1\, R\, q_1$
$q_1\, S_0\, R\, q_2$
$q_2\, 1\, R\, q_3$
$92\, S_0\, 1\, q_8$
$q_8\, 1\, R\, q_8$
$q_8\, S_0\, 1\, q_9$
$q_3\, 1\, R\, 93$
$93\, S_0\, L\, 94$
$94\, 1\, S_0\, 94$

$94\, S_0\, L\, 95$
$95\, 1\, L\, 95$
$q_5\, S_0\, L\, q_6$
$q_6\, 1\, L\, q_7$
$q_6\, S_0\, R\, q_{10}$
$q_{10}\, S_0\, R\, q_{11}$
$q_{11}\, 1\, S_0\, q_{12}$
$912\, S_0\, R\, q_{11}$
$q_{11}\, S_0\, R\, 99$
$97\, 1\, L\, 97$
$97\, S_0\, R\, q_0$

5.14. (a) $\delta(x)$
(b) $x_1 \dot{-} x_2$
(c) The function with empty domain.
(d) The function with domain the set of even natural numbers and with value 0.

5.15. (a)

$$f_1^2(x_1, 0) = x_1$$
$$f_1^2(0, x_2) = x_2$$
$$f_1^2((x_1)', (x_2)') = f_1^2(x_1, x_2)$$

(b)

$$f_1^2(x_1, 0) = x_1$$
$$f_1^2(x_1, (x_2)') = (f_1^2(x_1, x_2))'$$
$$f_2^2(x_1, 0) = 0$$
$$f_2^2(x_1, (x_2)') = f_1^2(f_2^2(x_1, x_2), x_1)$$

(c)

$$f_1^2(x_1, 0) = x_1$$
$$f_1^2(x_1, (x_2)') = (f_1^2(x_1, x_2))'$$
$$f_1^1(f_1^2(x_1, x_1)) = 0$$
$$f_1^1((f_1^2(x_1, x_1))') = 0'$$

5.17. Let $f(x)$ be a recursive function.

(a) Assume B **r.e.**, and let C be the inverse image of B under f. By Proposition 5.20(1), $(u)(u \in B \equiv (Ey)R(u, y))$, for some recursive relation R. Then $R(f(x), y)$ is recursive, and $(x)(x \in C \equiv (Ey)(R(f(x), y)))$. By Proposition 5.20(1), C is **r.e.**

(b) Let B be a recursive set, and let D be the inverse image of B under f. Then $x \in D$ if and only if $C_B(f(x)) = 0$, and $C_B(f(x)) = 0$ is a recursive relation.

(c) Let B be **r.e.**, and let A be the image of B under f, that is, the range off restricted to B. If B is empty, so is A. If B is non-empty, then B is the range of a recursive function g. Then A is the range of the recursive function $f(g(x))$.

(d) Any non-empty **r.e.** set which is not recursive (such as that of Proposition 5.20(5)) is the range of a recursive function g, and is, therefore, the image of the recursive set ω of all natural numbers under the function g.

5.18. (a) Let **A** be an infinite recursive set. Then A is the range of a recursive function f, by Proposition 5.20(4). Since A is infinite, $h(u) = \mu y(f(y) > u)$ is recursive. Let a_0 be the least element of A. Define $g(0) = a_0$, $g(n + 1) = f(h(g(n)))$. Then g is a strictly increasing function with range A.

(b) Let A be the range of a strictly increasing recursive function g. Then $g(x) \geqslant x$ for all x (by the special case of Proposition 4.14, p. 191). Hence, $x \in A$ if and only if $(Eu)_{u \leqslant x} g(u) = x$. So, A is recursive by Proposition 3.17.

5.19. Assume **A** is an infinite **r.e.** set. Let A be the range of the recursive function $g(x)$. Define the function f by the following course-of-values recursion (p. 146):

$$f(n) = g(\mu y((z)_{z<n}\, g(y) \neq f(z))) = g(\mu y((z)_{z<n}\, g(y) \neq (f\#(n))_z)).$$

Then A is the range of h, h is one-one, and h is recursive by Propositions 3.17 and 3.19. Intuitively, $f(0) = g(0)$ and, for $n > 0$, $f(n) = g(y)$, where y is the least number for which $g(y)$ is different from $f(0), f(1), \dots, f(n - 1)$.

5.20. Let A be an infinite **r.e.** set, and let A be the range of the recursive function g. Since A is infinite, $F(u) = \mu y(g(y) > u)$ is a recursive function. Define $G(0) = g(0)$, $G(n + 1) = g(\mu y(g(y) > G(n))) = g(F(G(n)))$. G is a strictly increasing recursive function whose range is infinite and included in A. By Exercise 5.18, the range of G is an infinite recursive subset of A.

5.21. Assume **A** and B are **r.e.** Then, by Proposition 5.20(1), $x \in A \equiv (Ey)R(x, y)$ and $x \in B \equiv (Ey)S(x, y)$, where R and S are recursive relations. Then $x \in A \cup B \equiv (Ey)(R(x, y) \vee S(x, y))$, and so, $A \cup B$ is **r.e.** by Proposition 5.20(1). Moreover, $x \in A \cap B \equiv (Ey)(Ez)(R(x, y) \wedge S(x, z))$, and the right-hand side of this equivalence is equivalent to $(Eu)(R(x, (u)_0) \wedge S(x, (u),))$. So, $A \cap B$ is **r.e.** by Proposition 5.20(1). The existence of an **r.e.** set A for which $w - A$ is not **r.e.** follows from Proposition 5.20(4, 5).

5.22. Assume (‡). Let $f(x_1, \dots, x_n)$ be effectively computable. Then the set $B = \{u \mid f((u)_1, \dots, (u)_n) = (u)_{n+1}\}$ is effectively enumerable, and, therefore, by (‡), r.e. Hence, $u \in B \equiv (Ey)R(u, y)$ for some recursive relation R. Then

$$f(x_1, \ldots, x_n) = ([\mu v(((v)_0)_1 = x_1 \wedge \ldots \wedge ((v)_0)_n = x_n \wedge R((v)_0, (v)_1))]_0)_{n+1}.$$

So, f is recursive. Conversely, assume Church's Thesis and let W be an effectively enumerable set. If W is empty, then W is r.e. If W is non-empty, let W be the range of the effectively computable function g. By Church's Thesis, g is recursive. But $x \in$ W $\equiv (Eu)(g(u) = x)$. Hence, W is r.e. by Proposition 5.20(1).

5.23. (b) Let A be r.e. Then $x \in$ A $\equiv (Ey)R(x, y)$, where R is recursive. Let $\mathfrak{R}(x, y)$ express $R(x, y)$ in K. Then

$$\mathrm{k} \in A \equiv \vdash_K (Ey)\mathfrak{R}(\bar{\mathrm{k}}, y).$$

(c) Assume k $\in$ A $\equiv \vdash_K \mathscr{Q}(\bar{\mathrm{k}})$ for all natural numbers k.Then k $\in$ A $\equiv$ $(Ey)Bw_{\mathscr{Q}}(\mathrm{k}, y)$, and $Bw_{\mathscr{Q}}(x, y)$ is recursive (cf. p. *157).*

5.24. (a) Clearly T_K is infinite. Let $f(x)$ be a recursive function with range T_K. Let $\mathfrak{B}_0$, A,, . . . be the theorems of K, where $\mathfrak{B}_j$ is the wf of K with Gödel number $f(j)$. Let $g(x, y)$ be the recursive function such that, if x is the Gödel number of a wf $\mathscr{C}$, then $g(x, \mathrm{j})$ is the Gödel number of the conjunction $\mathscr{C} \wedge \mathscr{C} \wedge \ldots \wedge \mathscr{C}$ consisting of J conjuncts; and, otherwise, $g(x, j) = 0$. Then $g(f(j), j)$ is the Gödel number of the j-fold conjunction A, $\wedge$ A, $\wedge \cdot \cdot .\wedge$ A,. Let K' be the theory whose axioms are all these *j*-fold conjunctions, for J = 0, 1, 2, ... Then K' and K have the same theorems. Moreover, the set of axioms of K' is recursive. In fact, x is the Gödel number of an axiom of K' if and only if $x \neq 0 \wedge (Ey)_{y<x}(g(f(y), y) = x)$. From an intuitive standpoint using Church's Thesis, we observe that, given any wf $\mathscr{Q}$, one can decide whether $\mathscr{Q}$ is a conjunction $\mathscr{C} \wedge \mathscr{C} \wedge \cdot\, .\, .\wedge \mathscr{C}$; if it is such a conjunction, one can determine the number J of conjuncts and check whether $\mathscr{C}$ is A,.

Part (b) follows from Part (a).

5.25. Let $\varphi(\mathrm{n}) = \mathrm{n}$ for all n.

5.26. If $\psi(x)$ were a recursive function which is an extension of $\mu y \mathrm{T}_1(x, x, y)$, then $(Ey)\mathrm{T}_1(x, x, y)$ would be equivalent to $\mathrm{T}_1(x, x, \psi(x))$, which is recursive.

5.27. Let $\varphi(z) = \sigma_1^2(\mu y[\mathrm{T}_1(z, \sigma_1^2(y), \sigma_2^2(y)) \wedge \sigma_1^2(y) > 2z])$, and let B be the range of φ.

5.33. (a) Assume $A(x,)$ weakly expresses $(\bar{\mathrm{T}}_K)^\star$ in K. Then, for any n, $\vdash_K \mathfrak{B}(\bar{\mathrm{n}})$ if and only if n $\in (\bar{\mathrm{T}}_K)^\star$. Let p be the Gödel number of $A(x,)$. Then $\vdash_K \mathfrak{B}(\bar{\mathrm{p}})$ if and only if p $\in (\bar{\mathrm{T}}_K)^\star$. Hence, $\vdash_K \mathfrak{B}(\bar{\mathrm{p}})$ if and only if the Gödel number of A@) is in $\bar{\mathrm{T}}_K$. I.e., $\vdash_K \mathfrak{B}(\bar{\mathrm{p}})$ if and only if not-$\vdash_K \mathfrak{B}$@)-

(b) If K is recursively decidable, T_K is recursive. Hence, $\bar{\mathrm{T}}_K$ is recursive, and, by Exercise *5.32,* $(\bar{\mathrm{T}}_K)^\star$ is recursive. So, $(\bar{\mathrm{T}}_K)^\star$ is weakly expressible in K, contradicting Part (a).

(c) Use Part (b); every recursive set is expressible, and, therefore, weakly expressible, in everv consistent extension of K.

5.34. Let T be a Turing machine which computes $\mu y \mathrm{T}_1(x, x, y)$. Use Proposition 5.19(3).

5.36. Assume f is recursive. Let $h(z) = \mu y(y < z)$. Then h is partial recursive, and $h(z) = 0$ if $z \neq 0$, and $h(z)$ is undefined if $z = 0$. Hence, the composition $h(f(z))$ is partial recursive, and

$$h(f(z)) \text{ is } \begin{cases} \text{undefined if } \psi_z(z) \text{ is defined} \\ 0 \text{ if } \psi_z(z) \text{ is undefined} \end{cases}$$

Then $h(f(z)) = \psi_k(z)$ for some k. So, we obtain the contradiction:

$$\psi_k(k) = h(f(k)) = \begin{cases} \text{undefined if } \psi_k(k) \text{ is defined,} \\ 0 \text{ if } \psi_k(k) \text{ is undefined.} \end{cases}$$

INDEX