A first course on logic

P.D. Welch

April 1996

Contents

Introduction

Since the earliest times people have tried to analyse how they reason, and how secure conclusions can be obtained from a premiss or premisses, and logic may be crudely defined as this science. Attempts were made to abstract formal schemes of deduction from everyday reasoning practice. Aristotle's study of the Syllogism was a paradigm for what was to follow. It was noted that many arguments were considered true quite independently of the material facts about which statements were made, but were considered "true" arguments merely by virtue of some "internal" structure of the reasoning involved, and the study of "logic" is the study of that internal structure. The original realisation that some statements were "true" not because the statement referred to some material fact about the world that was palpably true to others ("It is raining") but because some "correct reasoning" had been employed ("All men are mortal, Socrates is a man, therefore Socrates is mortal"), and this must have been the starting point of this enquiry. We should now say that the first statement is true (or false if it is not raining) whereas the second statement is a "valid" argument. What constitutes a valid argument is part of logic's domain.

But it could be said that not until the nineteenth century were there any further material advances in logic. Boole realised that some deductive laws of logic were algebraic in nature; Frege invented a system of symbolism that is the basis of what we today call predicate calculus, and formalised the theory of quantification which used symbols to represent individuals and properties. The system of predicate logic is the most useful logical system to date.

By mathematical logic sometimes two things are meant: firstly, the application of mathematical types of analysis to these languages and their rules, or secondly, the application of the discoveries of logic back to mathematics itself. Under the first heading, we are able to apply mathematical reasoning to these logical systems, because the languages in which they are expressed, and the rules that they employ are simple enough and regular enough to be construed as mathematical objects themselves and so are amenable to mathematical analysis. As regards the second heading, we should perhaps not be surprised that logic should have something to say about mathematics, after all mathematics is often held up as the "logical science" *par excellence*, but mathematics was not always considered a coherent body of logical thought, of theorems derived logically from one set of axioms or other. However twentieth century discoveries in mathematical logic have had a profound effect on how we can regard mathematics as a whole, and also have contributed many purely mathematical theorems.

Both these aspects will occur in this course. We shall first look at a system for dealing simply with propositions: we shall define a class of formal languages suitable for the study of statements about propositions and the logical interrelationship between them. We shall be particularly interested in those statements are always true, merely by virtue of the structure of the statement, and not because of the truth or falsity of the basic or "atomic" propositions they contain, the "tautologies". We shall then consider far more expressive languages, the "first-order" languages (or "predicate" languages) in which we can express the

idea of individuals having certain properties or relationships to one another. Such a first order language can be interpreted as saying something about a certain structure and a main object of this course is to provide a generalised theory of the internal properties of certain kinds of structures, and the languages with which to describe them. By a structure we mean a set of objects together with a collection of relations and functions on that set. A standard example drawn from mathematics is that of a group, together with the group's operations of multiplication, inverse, an identity element and so on. An example of "internal" property is that of commuiativity. We call it internal since we only have to look "inside" the group to check if the commutative law holds.

The group we could display as $\mathbf{G} = \langle G, \circ_G, {}^{-1}_G, e_G \rangle$ where G is the underlying set of elements, $\circ_\mathbf{G}$ the group multiplication etc. Internal properties turn out to be those that can be expressed in sentences of a formal language. We shall be looking at such languages in general. In this case we can use a language containing symbols such as $\forall, x, y, \circ, (,)$), and = to express commutativity as

$$\forall x \forall y (x \circ y = y \circ x)$$

and we say **G** is commutative if that expression is "true in" **G**.

The formal languages we shall consider are themselves susceptible to mathematical analysis. They are simple enough and concrete enough (as they can usually be written down) so that their features are open to inspection, and proofs concerning them sometimes involve no more than making observations on the way they are built.

One strand to our investigation is *semantic*. That is, it is to do with meaning. This was already alluded to above when I said that the string of symbols "expressing" commutatively was "true in" G. What does it mean to say a symbol string is true in G? We shall give a precise definition of truth-in-a-structure, (due to the polish logician Tarski) and see how we can give definite *meaning* to what is otherwise just a symbol string. The other strand is *syntactic* and is to do with symbols of the languages themselves: the languages are defined in an "inductive" or "recursive" way just as are most computer languages. (Indeed this is exploited to the full in Gödel's First Incompleteness Theorem.) When we come to consideration of "rules of proof" for deriving theorems in our formal language we shall see that they only involve mechanical symbol manipulation. In the example of our group, we find we can write down the three or four axioms which we usually associate with groups and by our rules of proof we can manipulate these axioms, perform "deductions" and finally deduce as a theorem that in a group the identity element is unique. These are purely syntactic operations on formulae in the language: we didn't need at all to look at the groups themselves to discover this. The symbols of our languages will be given to us in a simple straightforward manner, so that we may, for example, use natural numbers as code numbers for the symbols; then using a further simple coding for sequences of symbols, we can think of formulae in our language as given to us by sequences of numbers. Further we have an effective procedure for deciding whether a string of numbers codes a formula. By "effective procedure" here, we mean a mechanical algorithm, or if we wish to be more specific, something we could write a computer program for. Thus we can write a program that, when fed in a sequence of numbers, will return 1 if the sequence codes a formula or 0 otherwise. It turns out that all the syntactic manipulations we perform on formulae in our language can be performed by computer programs on their code numbers. The axiom system for groups above consisted only of a finite number of axioms. We shall also want to consider where we allow

infinitely many axioms that have been given to us in some "effective" way. That is, we have a programme to test whether (a code number of) a formula is one of our list of allowed axioms.
There are two main goals in this course: to show how truth in structures relates to being derivable by syntactic operations, i.e. to being "provable". Gödel's Completeness Theorem shows roughly that what is provable is precisely what is true in all structures of the same type. The second goal relates to the limits of the axiomatic method in mathematics: it turns our that axiom systems to do with number theory, if they're given to us in an effective or mechanical way, cannot provide all the true statements of arithmetic. So, for example, there is no finite list of axioms (or indeed an infinite list given to us in recursive way) for number theory so that everything that is true of the natural numbers is provable from them. This remarkable result is Gödel's First Incompleteness Theorem, and we can regard this as a mathematical result that comes from applying some of the logical discoveries about first order reasoning back to mathematics itself.

Some preliminaries
Sets There are no preferred letters for sets. We write "$x \in y$" or "$x \in A$" to mean the set x is a member of y, or of A. Sets are often specified by writing $\{x| \ldots x \ldots\}$ meaning the set of all x such that $\ldots x \ldots$ holds, or by listing its members, as in $\mathbb{N}$ below. ϕ denotes the empty set; $\mathbb{N} = \{0, 1, 2, \ldots\}$; in logic it is convenient to think of the natural number k as the set of its predecessors, thus $k = \{0, 1, 2, \ldots, k-1\}$; under this convention then 0 is the same as the empty set.
$\langle a, b\rangle$ denotes the *ordered pair* of elements a and b. So $\langle a, b\rangle \neq \langle b, a\rangle$.
We define by induction:
$\langle a_1, a_2, a_3\rangle = \langle\langle a_1, a_2\rangle, a_3\rangle, \ldots \langle a_1, \ldots, a_n\rangle = \langle\langle a_1, \ldots, a_{n-1}\rangle, a_n\rangle$. For sets $A_1, \ldots A_n$

$$A_1 \times \ldots \times A_n = \{\langle a_1, \ldots, a_n\rangle | a_1 \in A_1 \& \ldots \& a_n \in A_n\}$$

This is often written A^n. By convention $A^0 = 1$.
Relations and Functions. If A is a set a binary relation on A, R, is a subset of A^2. So we write $\langle a_1, a_2\rangle \in R$, or $R(a_1, a_2)$. An n-ary relation is accordingly a subset of A^n and we write $\langle a_1, a_2, \ldots, a_n\rangle \in R$ or $R(a_1, \ldots, a_n)$. A function from A *to* B is a subset f of $A \times B$ with the properties
(i) for all $x \in A$ there is $y \in B$ with $\langle x, y\rangle \in f$ [we write $f(\underline{x}) = y$].
(ii) for all $x \in A$, all y, y', $\langle x, y\rangle$ and $\langle x, y'\rangle \in f$ implies $y = y'$.
We write $f : A \longrightarrow B$.
We write $f : A \xrightarrow{(1-1)} B$, or f is *one-to-one*, or *(1- 1)*, or *injective* if $f(x) = f(x\prime)$ implies $x = x\prime$ and f is *onto* if for all $y \in B$ there is $x \in A$ with $f(x) = y$.
We write ran $f = \{y|$ there exists x so that $\langle x, y\rangle \in f\}$
and dom $f = \{x|$ there exists y so that $\langle x, y\rangle \in f\}$
For functions f, g we say g *extends* f and write $g \supseteq f$ if the set g contains the set f. This implies that dom $f \supseteq g$ and g agrees with f on $f's$ domain as you would want.

Order Relations

1. An *equivalence relation* R on a set A is a binary relation with the properties
   (i) (Reflexivity) $R(x, x)$

(ii) (Symmetry) if $R(x, y)$ then $R(y, x)$
(iii) (Transivity) if $R(x, y)$ and $R(y, z)$ then $R(x, z)$.
If R is an equivalence relation on A then the *equivalence* class of x, $[x]_R$, is the set $\{y|R(x, y)\}$.

2. A binary relation R on A is a *strict partial order* if for all $x, y, z \in A$
(i) (Irreflexivity) not $R(x, x)$
(ii) (Transitivity) if $R(x, y)$ and $R(y, z)$ then $R(x, z)$ >

When we're thinking of relations as orders we usually write xRy in the above, or even take over the $<$ symbol to write $x < y$.
A *strict total order* on A is a partial order R so that for all x, y in A $R(x, y)$ or $R(y, x)$.
A *well order* on A is a strict total order so that for all $B \subseteq A$ if $B \neq$ ffl then B has an R-least element, i.e. there is x in B so that for all y in B, $y \neq x, R(x, y)$.
Countability
A set A is *countable* if there is an onto map $f : \mathbb{N} \to A$. [This includes the case of A being finite]. Notice that if $g : A \xrightarrow{(1-1)} \mathbb{N}$ then A is also countable. We denote the size, or cardinality of a set A by $|A|$.
Finally, expressions such as "Lemma 2.3" refer to Lemma 3 of Chapter 2. "Ex 2.3" will abbreviate Exercise 3 of Chapter 2, "Ex.3" and "Lemma 3" will refer to Exercise 3 and Lemma 3 of the current chapter.

Propositional Languages

2.1 Atoms, formulae and connectives

We shall first consider a class of languages simpler than outlined in the introduction, the class of languages suitable for handling *propositions*. We think of a sentence such as "The room is warm" together with such information about the meaning of the words in it, and the circumstance of its utterance which are sufficient to determine what definite statement is being made as a proposition. We shall describe a calculus for handling propositions where we assume every proposition is either *true* or *false*. This is one of the basic assumptions of classical logic and is referred to as the *Principle of Bivalence*. Actually we shall not be concerning ourselves with anything about the proposition other than whether it is true or false and so we shall simply speak of the *truth value* (T or F).

We shall define in general terms a language for manipulating propositions; this may be specified by 1) and 2) below. We shall discuss some of the features of the language and then later give a more 'mathematical' definition of such a language to bring it more into line with the more expressive first order languages to come.

1) We assume the language is built up from a set (finite or infinite) of symbols called *propositional atomic formulae* or more simply *propositional atoms* which we shall denote by

$$P, Q, R, \cdots \text{ or } P_0, P_1, P_2, \cdots \text{etc.}$$

The set of these 'atomic' symbols we shall call ω. We can, if we wish, think of these propositional atoms as propositional "variables" that can range over propositions, and we use the propositional atoms to build up compound formulae. We confine our attention in classical logic to ways of compounding propositional atoms which permit us to calculate the truth value of the built up proposition simply from a knowledge of its components. (This is known as the *Principle of Extensionality* which requires that the truth value of the whole formula should not depend on *how* the truth values of the parts are determined but only on *what* they are. Other logics are possible, for example logics that assign intermediate truth values to indicate "probability" of being true).

We think of the truth value of the whole formula as thus being a *function* of the truth values of the componetns and so the permitted methods of forming compound formulae are said to be *truth functional*. We build up these using *truth functions* which are more usually called *propositional connectives*. Using these we shall be able to build up the whole class of formulae, which we shall individually denote by letters such as $\phi\psi$ and so on with or without subscripts.

2) The two principal propositional connectives or truth functions are negation and implication which we denote by the symbols $\neg, \rightarrow$ (read as "not" and "implies" respectively.)

Using 1) and 2) we define the class of formulae inductively as follows:

(i) The propositional atoms $P, Q, R, \cdots$ etc. are formulae.
(ii) If ϕ and ψ are formulae then so are

$$(\neg\phi) \qquad (\phi \to \psi)$$

For something to be a formulae it must then be built up by using *finitely* many applications of (i) and (ii). The ideas of a propositional connective is that it is a function from the truth values of the formulae it connects to the set of truth values {T,F }. Negation, ¬, only "connects" one formula, we say that it is a "one place truth function". And we specify the way the connectives work with the following *truth tables* for the functions.

ϕ	$\neg\,\phi$
T	F
F	T

ϕ	ψ	$(\phi \to \psi)$
T	T	T
T	F	F
F	T	T
F	F	T

The tables are really displaying how two functions $F_\neg$ and $F_\to$ work. For example $F_\neg(F) = T, F_\to(T, F) = F$. And of course we have designed the tables and the accompanying functions to reflect what we usually think when we say "for $\neg A$ to be true A must be false" and so on. But notice that we have specified that $(\phi \to \psi)$ is always true unless $\phi's$ true and ψ false.
We can use the truth table format to calculate how the truth value of a built up formula depends on the truth values of the atoms it contains.

Example 1 Consider the following table:

ϕ	ψ	$(\neg\,\phi)$	$(\neg(\,\phi \to \psi))$
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

This demonstrates how the built up formula $((\neg\phi) \to \psi)$ gets one of the truth values depending on how the components $(\neg\phi)$ and ψ (and ultimately ϕ and ψ) are awarded truth values. But notice further that $((\neg\phi) \to \psi)$ is true precisely when either ϕ or ψ is true. This shows that what we ordinarily think of as "either ....or" can be *defined* just by using ¬ and → alone. Accordingly we make the following definition: $(\psi \vee \phi)(\text{“}\phi\text{or}\psi'')$ will be an abbreviation for $((\neg\phi) \to \psi)$. Further $(\phi \vee \psi'')(\text{“}\phi\text{and}\psi'')$ will abbreviate $(\neg(\phi \to (\neg\psi)))$. The justification for this is the following table:

ϕ	ψ	$(\neg\,\psi)$	$(\phi \to (\neg\,\psi)$	$(\neg\,(\,\phi \to (\neg\,\psi\,)))$
T	T	F	F	T
T	F	T	T	F
F	T	F	T	F
F	F	T	T	F

Again, $(\neg(\phi \to (\neg\psi)))$ is true precisely when both ϕ and ψ are true. The point of these two examples is that when we come to formally define our language we can be economical with our basic set of propo-

sitional connectives, since we can define "and" and "or" in terms of negation and implication. We make a further abbreviation: $(\phi \longleftrightarrow \psi)$ is short for $(\phi \to \psi) \vee (\psi \to \phi)$ (which of course is itself already an abbreviation.) $\longleftrightarrow$ is called bi-implication. You should check that $(\phi \longleftrightarrow \psi)$ comes out T if both ϕ and ψ are T or both ϕ and ψ are F.

ϕ	ψ	$(\phi \vee \psi)$
T	T	T
T	F	T
F	T	T
F	F	F

ϕ	ψ	$(\phi \longleftrightarrow \psi)$
T	T	T
T	F	F
F	T	F
F	F	T

Here is an example of a truth table of a more complicated expression. Notice here we incorporate $\vee$ into our table directly, saving space by not writing it out in terms of $\neg$ and $\to$.

Example 2 $(\phi \vee (\neg\psi)) \to \chi)$

ϕ	ψ	χ	$\neg\psi$	$(\phi \vee (\neg\psi))$	$(\phi \vee (\neg\psi))$ $\to$ $\chi)$
T	T	T	F	F	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	T	F	F	F	T
F	F	T	T	F	T
F	F	F	T	F	T

Remarks: if ϕ, ψ, and χ had been the propositional atoms, P, Q and R, say (so that we are dealing with the formula $(P \vee (\neg Q) \to R)$) we can think of the table as giving us precisely which alternative conditions on the atoms make the formula come out true (if any). We see here that every line bar one of the table comes out T. Naturally any other formula with 3 propositional atoms in it would also require a truth table with 2^3 lines to look at all the possible alternatives; and with k atoms 2^k lines would be necessary. Notice also that assigning T to U and F to V say makes no difference to the truth or falsity of our formulat: the atoms U and V do not occur there and so their truth value is irrelvant. We think of an assignment of $T's$ and $F's$ to the atoms of the language as a valuation of the language.

Definition 2.1 *A* valuation *of a propositional language L_ω is an assignment, w, of truth values to the propositional atoms in the set ω. A* valuation of a formula *ϕ is an assignment of truth values to the propositional atoms occurring in the formula ϕ.*

We thus think of w as a function whose domain is ω and whose range is contained in the set $\{T, F\}$. Notice that a formula can belong to many different languages: if ϕ contains only the atoms P, Q, and R then ϕ will be a formula of any language L_ω where $\{P, Q, R\} \subseteq \omega$. A valuation of L_ω when restricted to $\{P, Q, R\}$ can then be considered a valuation of ω. What this amounts to is that valuation of ω correspond simply to lines in the truth table associated with ϕ. The import of the remarks above is that if w

and w' are two valuations of L_ω that happen to agree on all the propositional atoms of a formula ϕ then both w and w' make ϕ have the same truth value.

Exercise 1 Draw truth tables for the formulae below
a) $(\neg((\neg\phi) \wedge (\neg\psi)))$ b) $((\phi \to \psi) \to)$ c) $((\psi \to \tau) \wedge (\neg\tau))$
d) $(\neg(\sigma \to (\neg\tau)))$ e) $((\phi \to \psi) \vee (\chi \to (\neg\psi)))$
f) $((\chi \to (\phi \to \psi)) \vee (\neg(\phi \to (\psi \wedge (\neg \wedge (\neg\chi)))))$

Exercise 2 Define a ternary (three-place) connective # so that $\#(\phi, \psi, \chi)$ is T precisely when at least two of ϕ, ψ, and χ are assigned T. Draw a truth table for #.

2.2 Truth functional equivalence and tautologies

In example 2 above suppose ϕ, ψ and χ are the propositional atoms R, Q, R respectively. Consider now the table for the formula τ where τ is $P \to (Q \vee R)))$:

P	Q	R	$(Q \vee R)$	$(P \to (Q \vee R))$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	F	T

This table has a final column precisely that for the table for $((P \vee (\neg Q))) \to R)$; or in other words the formula $((P \vee (\neg Q))) \to R)$; is true under precisely the same conditions as $(P \to (Q \vee R))$. This is important enough to warrant a definition:

Definition 2.2 *Two formulae ϕ and ψ of a propositional language L_ω are* truth-functionally equivalent *if for every valuation w of the propositional atoms occurring in ϕ and ψ then ϕ comes out true under w if and only if ϕ does.*

Example 3
$(\neg(\neg\phi))$ is truth functionally equivalent to ϕ itself
$(P \vee (Q \vee (\neg Q))$ is truth functionally equivalent to P alone
$(P \to (Q \to (\neg P)))$ is truth functionally equivalent to $(\neg(P \vee Q))$.

The usefulness of truth functional equivalence is the following: if ϕ is truth functionally equivalent to ψ and ψ occurs as a "subformula" of χ say, then we can replace the occurrence of ψ by ϕ to get a new formula χ' which is true under precisely the same conditions as χ was (in other words χ and χ' are also truth functionally equivalent). If, for example, ϕ were simpler than ψ then we should have a simplication

of χ to χ'.
It is convenient to make some abbreviations when writing out formulae: it is not necessary to write the exterior parentheses each time around negoatiions or plorations we thus abbreviate $(\neg\phi)$ simply by $\neg\phi$. We can also remove brackets around the other formulae if we agree to the convention that $\neg$ "binds tighter" than $\wedge$ and $\vee$ which in turn bind tighter than $\leftrightarrow$ which in turn binds tighter than $\rightarrow$. Thus $\neg\phi \vee \psi$ is $((\neg\phi) \vee \psi)$ not $\neg(\phi \vee \psi)$ and $\phi \wedge \psi \rightarrow \chi$ is short for $(\phi \wedge \psi) \rightarrow \chi$, and $\psi \rightarrow \phi \leftrightarrow \chi$ is short for $\psi \rightarrow (\phi \leftrightarrow \chi)$, although when there is any possible source of confusion it is better to leave some brackets in. These conventions do not allow us to leave out *all* brackets (what would $\phi \vee \psi \wedge \chi$ be an abbreviation of for example?) but makes reading easier in most cases.
The second example of Example 3 included as a subformula the formula $(Q \vee \neg Q)$. The reason that the formula was truth functionally equivalent to P itself was simply that $Q \vee \neg Q$ is true under any valuation. Such formulae which are always true by the nature of their construction alone are important.

Definition 2.3 *A formula ϕ of a propositional language which is true under every valuation of that language is called a* tautology.

Thus a tautology is simply a formula that when analysed via a truth table always comes out T i.e. the last column is simply a column of $T's$.

Example 4 1 $\phi \vee \neg\phi$

ϕ	$\neg\phi$	$\phi \vee \neg\phi$
T	F	T
F	T	T

2 $(\phi \rightarrow \psi) \longleftrightarrow (\neg\psi \rightarrow \neg\phi)$

ϕ	ψ	$\phi \rightarrow \psi$	$\neg\psi \rightarrow \neg\phi$	$(\phi \rightarrow \psi) \leftrightarrow (\neg\psi \rightarrow \neg\phi)$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

3 $\neg(\phi \wedge \chi) \leftrightarrow (\neg\phi \vee \neg\chi)$
$\neg(\phi \vee \chi) \leftrightarrow (\neg\phi \wedge \neg\chi)$ (De Morgan's Laws)

4 $\neg\neg\phi \leftrightarrow \phi$

5 $\phi \wedge \phi \longleftrightarrow \phi; \phi \longleftrightarrow \phi \vee \phi; (\phi \wedge kl\psi) \longleftrightarrow (\psi \wedge \phi); (\phi \vee \psi) \leftrightarrow (\psi \vee \phi)$

6 $((\phi \wedge \chi) \wedge \psi) \leftrightarrow (\phi \wedge (\chi \wedge \psi)); ((\phi \vee \chi) \vee \psi) \leftrightarrow (\phi \vee (\chi \vee \psi))$

7 $\phi \rightarrow (\chi \rightarrow (\phi \wedge \chi)); \phi \wedge \chi \rightarrow \phi; \phi \rightarrow (\phi \vee \chi)$

8 $(\phi \rightarrow \chi) \rightarrow ((\chi \rightarrow \psi) \rightarrow (\phi \rightarrow \psi))$
$(\phi \rightarrow (\chi \rightarrow \psi)) \rightarrow ((\phi \rightarrow \chi) \rightarrow (\phi \rightarrow \psi))$
$((\phi \rightarrow \chi) \rightarrow \phi) \rightarrow \phi$
$(\neg\phi \rightarrow \chi) \rightarrow ((\neg\phi \rightarrow \neg\chi) \rightarrow \phi)$

9 $(\phi \wedge \neg\phi) \to \chi$

Definition 2.4 *A formula that comes out* F under every valuation is called a *contradiction*.

So ϕ is a tautology iff $\neg\phi$ is a contradiction.

Example 5 $(\phi \wedge \neg\phi), (\phi \longleftrightarrow \neg\phi)$ are contradictions.

Truth tables give us an effective procedure for testing for tautologyhood. "Effective procedure" here means a mechanical algorithm, or to put it another way, a process that we could write a program to do. The following outlines the process for the given ϕ

1 List all propositional variables occurring in ϕ as $P_1, P_2, \ldots, P_n$.

2 Construct a truth table of $T's$ and $F's$ amongst the $P_i (1 \leq i \leq n)$.

3 For reach of the 2^n lines of the table, which we can consider as valuations w from $P_1, \ldots, P_n$ to $\{T, F\}$, build up successive columns of the table using rules given by the truth tables for the connectives $\neg$ and $\to$, building up successively from the values assigned to the P_i, through the various subformulae of ϕ until we have computed the last column of the table.

4 If for each of the $2^n w$, the entry in the last column is T we say ϕ was a tautology. Otherwise ϕ is not a tautology.

We just want to say enough to convince the reader that this is an effective procedure.
In particular cases the following process can be quicker. We illustrate with an example. We wish to check whether ϕ is a tautology where ϕ is as follows:

$((P$	$\to$	$R)$	$\wedge$	$(Q$	$\to$	$R))$	$\to$	$((P$	$\vee$	$Q)$	$\to$	R	$)$
			T				F				F		
			(2)				(1)				(2)		
	T				T				T			F	
	(3)				(3)				(4)			(4)	
		T						T					
		(6)						(5)					
						T				T			
						(8)				(7)			

Step 1 We argue by contradiction and assume that the formula can be false. This means
Step 2 The left hand side (LHS) is T and the RHS F
Step 3 The LHS is a conjunction, so both conjuncts must be T
Step 4 If RHS F then $P \vee Q$ must be T and RF
If $P \vee Q$ is T we have a choice:
Step 5 Suppose P is T. By our assumption at Step 3 ...
Step 6 R must be T; but this contradicts RF at Step 4 so we go back to (4) and suppose instead
Step 7 Q is T since at Step 3 $Q \to R$ is T we have

Step 8 R is T again contradicting (4).
There are now no more alternatives: it's really impossible for the whole formula to be F, so it's a tautology.
Not only is this kind of method usually quick (with practice) since a formula with four propositional atoms needs a $2^4 = 16$ line truth table, but if the formula isn't a tautology this method is extremely useful in revealing a valuation s of the propositional atoms in ϕ to $\{T, F\}$ that will make ϕ come out F. In other words if you wish, if you wish to find a valuation that makes a formula ψ come out T, try and show that $(\neg\psi)$ is not a tautology.

Exercise 3 Replace the omitted brackets in the following formulae:

$$\phi \wedge \neg\psi; \phi \wedge \neg\psi \rightarrow \chi; \phi \rightarrow \psi \vee \neg\chi\phi \rightarrow \psi \leftrightarrow \sigma \wedge \tau$$

Exercise 4 Show the following: if ϕ and $\phi \rightarrow \chi$ are tautologies so is χ
Determine whether the following are tautologies, contradictions or neither.

a $(P \rightarrow Q) \rightarrow ((P \rightarrow \neg R) \rightarrow (\neg R \rightarrow Q))$

b $(P \rightarrow Q) \leftrightarrow \neg(P \wedge \neg Q)$

c $(P \rightarrow Q) \rightarrow ((Q \rightarrow R) \rightarrow (P \rightarrow R))$

d $(P \rightarrow (Q \rightarrow R)) \leftrightarrow ((P \wedge Q) \rightarrow R)$

e $(P \wedge (Q \vee R)) \leftrightarrow ((P \wedge Q) \vee (P \wedge R))$ (Distributive laws)
$(P \vee (Q \wedge R)) \leftrightarrow ((P \vee Q) \wedge (P \vee R))$

f $((P \rightarrow Q) \rightarrow P)$ $((P \leftrightarrow (P \rightarrow Q)) \rightarrow Q$
$(((P \wedge Q) \rightarrow R) \rightarrow ((P \vee \neg Q) \rightarrow R))$ $((P \rightarrow (Q \vee \neg P)) \rightarrow (\neg Q \wedge \neg P))$

Exercise 5 We saw that the truth functions $\vee$ and $\wedge$ could be defined using $\rightarrow$ and $\neg$, show a) how to define $\rightarrow$ in terms of $\neg$ and $\vee$ and b) how to define $\rightarrow$ in terms of $\neg$ and $\wedge$.
Exercise 6 The following binary connective $|$ is defined by means of the following table. Show that $\rightarrow$ and $\neg$ can be defined using this connective alone.

ϕ	ψ	$\phi \mid \psi$
T	T	F
T	F	T
F	T	T
F	F	T

(This shows that our original choice of two basic connectives could have reduced to one by using $|$.)

now repeat the exercise for the connective $\downarrow$:

ϕ	ψ	$\phi \downarrow \psi$
T	T	F
T	F	F
F	T	F
F	F	T

Exercise 7 Show that there are infinitely many tautologies. Invent some more of your own.

2.3 A formal definition of propositional languages

The languages we wish to study, both propositional and first order, are sufficiently simple that they are amenable to mathematical analysis. But to do that we need to give a *mathematical* definition of what these languages are. (We shall see that everything in the language is capable of being encoded by natural numbers and actually all the associated manipulations that we shall introduce can also be thought of as manipulations of those code numbers, very much as computers manipulate symbols of a programming language.) We shall emphasis this mathematical nature of the languages by giving the definitions that follow inductively. Just as in a proof by induction we assume that if a property P has been proven for all $k < n$ and then proceed to prove P for n itself, we shall make our definitions such that we give the definition for formulae of simplest complexity, complexity 0, and then we make a definition for formulae of complexity n assuming that we know the definition for all formulae of lesser complexity. We thus have the task now of defining inductively the class of formulae and for any formula the associated natural number which is a measure of its complexity. There are many ways of doing this, we choose one which is rather economical in terms of the number of clauses in the definitions. The advantage of having this complexity measure is the following: suppose we wish to prove that all formulae have a certain property, then we now have a natural way of doing this, we simply use ordinary mathematical induction on the complexity of formulae. We prove the property is good for all formulae of 0 complexity, we then prove it for a formula ϕ assuming that it is proven for all formulae ψ where the complexity of ψ is less than that of ϕ.

We give a formal definition for the formulae of a propositional language given a set of ω of *propositional atoms*. The definition below doesn't assume that ω is countable, but in our applications this will always be the case. We'll commonly use $P_0, P_1, \ldots, Q, R, \ldots$ to range over members of ω. We think of P_i, Q etc., as standing simply for propositions that are either T or F.

Definition 2.5 *Let ω be a set of propositional atoms. We define by recursion the* formulae *of L_ω and simultaneously, their* complexity *which for a formula ϕ we write as* $\mathrm{comp}(\phi)$.
(i) If $P \in \omega$ then P is a formula of complexity 0
(ii) If ϕ is a formula then $(\neg\phi)$ is a formula of complexity that $\mathrm{comp}(\phi) + 1$.
(iii) If ϕ, ψ are formulae then $(\phi \to \psi)$ is a formula of complexity $\max\{\mathrm{comp}(\phi), \mathrm{comp}(\psi)\} + 1$.
(iv) Nothing is a formula except by (i) - (iii) above.

Notice that (i) - (iii) don't allow any way of forming "infinitely long formulae", thus every formula has only finitely many symbols in it and has a finite complexity. The definition given here is consistent with one we shall use for first-order languages; notice here that comp (ϕ) equals the "depth of nesting" of the brackets within ϕ. An alternative measure of complexity is the number of basic propositional connectives in ϕ. An official formula also can only have the same number of left brackets in it as right brackets. (Why? It is pretty obvious given the way formulae are constructed, but if we required a proof, we should argue as follows: It is vacuously true for all formulae of complexity 0; let ϕ be a formula and suppose we have proven this for all formulae with complexity less than comp (ϕ), there are two cases a) ϕ is $(\neg\psi)$ for some formula ψ, now $\mathrm{comp}(\psi < \mathrm{comp}(\phi)$ so by inductive hypothesis ψ has the same number of left as right brackets, but since ϕ *is* $(\neg\psi)$ it is true for ψ too; b) ϕ is $(\psi \to \chi)$; again we apply the inductive hypothesis to ψ and χ since $\mathrm{comp}(\psi), \mathrm{comp}(\chi) < \mathrm{comp}(\psi)$ and the symbol string $\psi \to \chi$ (not an official

formula) has the same number of left brackets as right brackets, therefore so must ϕ. This is a somewhat trivial example but it illustrates the method.) That done we introduce the abbreviation $\wedge, \vee, \longleftrightarrow$ as before with similar conventions concerning bracketing.

Example 6 $\text{comp}((\neg P)) = 1$
$\text{comp}\,((Q \to (\neg P))) = \max\{\text{comp}(Q), \text{comp}((\neg P))\} + 1 = \max\{0,1\} + 1 = 2$
$\text{comp}(((\neg P) \to (Q \to (\neg P))) = \max\{\text{comp}((\neg P)), \text{comp}((Q \to (\neg P)))\} + 1 = \max\{1,2\} + 1 = 3$
$\text{comp}(P \vee Q \to R \wedge \neg Q) = \text{comp}((((\neg P) \to Q) \to (\neg(R \to (\neg(\neg Q))))) = 5.$

Notice if $\text{comp}(\psi) = 23$ then $\text{comp}(\psi \vee P) = 25$ but $\text{comp}(P \vee \psi) = 24$, because $\vee$ is an abbreviation whereas $\text{comp}((\psi \to \phi)) = \text{comp}((\phi \to \psi))$ for any ϕ.
We can now give a mathematical definition of a valuation of the propositional atoms of a language and its extension to the formulae of that language.

Definition 2.6 *A* valuation *of a propositional language is a map $w : \omega \to \{T, F\}$ which assigns to each propositional variable in ω a truth value T or F. We then define by induction on complexity of ϕ a formula of L_ω the valuation of $\omega*$ of ϕ*

(i) *if φ is P $w^*(\varphi) = w(P)$*

(ii) *if φ is $(\neg\psi)$ then $w^*(\varphi)$ is given by*

$w^*(\varphi)$	$w^*(\varphi)$
T	F
F	T

(iii) *if φ is $(\varphi \to \chi)$ then $w^*(\varphi)$ is given by*

$w^*(\varphi)$	$w^*(\chi)$	$w^*(\varphi)$
T	T	T
T	F	F
F	T	T
F	F	T

Of course these are just the truth tables of p. 7. The point is that we have given a formal definition of the truth value of a formula φ, $w^*(\varphi)$, given a valuation $w : \omega \to \{\text{T, F}\}$. We have then $w^* : \{\text{ Formulae of } L_\omega\} \to \{\text{T, F}\}$. This is a prototypical example of a definition by induction on the complexity of a formula. Notice here the advantage of only having two propositional variables as primitive: if we had also taken $\vee$ and $\wedge$ say, then Definition 2.6 would have had an extra two clauses. We can couch the definition of a tautology in this terminology:

Definition 2.7 *If under every valuation $w : \omega \to \{\text{T, F}\}$, $w^*(\varphi)$ =T, then we say φ is a tautology.*

Definition 2.8 *We say a valuation w satisfies a formula φ in L_ω if $w^*(\varphi)$ =T. A formula φ is* satisfiable *if there is a valuation w so that $w^*(\varphi)$ =T; otherwise φ is said to be* unsatisfiable. If Γ is a set of formulae, then we say *w satisfies* Γ if for all $\psi \in \Gamma$, $w^*(\psi)$ =T; and Γ is *satisfiable* if there is some valuation *w* that satisfies Γ. Γ is *unsatisfiable* if no *w* satisfied Γ.

A tautology is thus a formula that is satisfied by every valuation. Note that $\varnothing$ is satisfiable. There is some notiaiton that is useful for representing the relationship between sets of formulae in terms of satisfiability.

Definition 2.9 *Let* $\Gamma \cup \{\varphi\}$ *be a set of formulae in* L_ω. *Then* $\Gamma \vDash \varphi$ *means that every valuation that satisfies* Γ *satisfies* φ.

To say that φ is a tautology is now the same as writing $\varnothing \vDash \varphi$ (because every valuation satisfies $\varnothing$) and we abbreviate this to simply $\vDash \varphi$. For not $(\Gamma \vDash \phi)$ we write $\Gamma \nvDash \varphi$. We write $\Gamma, \psi \vDash \varphi$ rather than $\Gamma \cup \{\psi\} \vDash \varphi$. We allow here the possibility that Γ is infinite.
Another way to write that Γ is unsatisfiable is to write $\Gamma \vDash \varphi \wedge \neg\varphi$ (Why?). Similarly the list of properties of $\vDash$ in the following lemma can all be checked as simple ramifications of this definition.

Lemma 2.10 *Let* $\Gamma, \Delta, \{\phi, \psi, \chi\}$ *be sets of formulae in* L_ω

a) $\Gamma \vDash \varphi$ implies $\Gamma \cup \Delta \vDash \varphi$

b) If $\varphi \in \Gamma$ then $\Gamma \vDash \varphi$

c) If $\Gamma \vDash \varphi$ and $\Gamma, \varphi \vDash \psi$ then $\Gamma \vDash \psi$

d) If $\varphi \vDash \psi$ and $\psi \vDash \chi$ then $\varphi \vDash \chi$

e) $\Gamma \vDash \neg\varphi$ *iff* $\Gamma, \varphi \vDash \psi \wedge \neg\psi$

f) $\Gamma \vDash \varphi$ and $\Gamma \vDash \psi$ iff $\Gamma \vDash \phi \wedge \psi$

g) $\Gamma, \varphi \vDash \psi$ and $\Gamma, \chi \vDash \psi$ iff $\Gamma, \varphi \wedge \chi \vDash \psi$

h) $\Gamma, \varphi \vDash$ *iff* $\Gamma \vDash \varphi \to \psi$

i) $\Gamma, \varphi \vDash \psi$ and $\Gamma, \psi \vDash \varphi$ iff $\Gamma \vDash \varphi \leftrightarrow \psi$

j) $\varphi \to \psi,\ \varphi \vDash \psi$

k) If $\Gamma, \varphi \vDash$ and $\Gamma, \neg\varphi \vDash \psi$ then $\Gamma \vDash \psi$

Proof For example g). $(\Rightarrow)$ Suppose $\Gamma, \varphi \vDash \psi$ and $\Gamma, \chi \vDash \psi$. Now let w be any valuation that satisfied $\Gamma \cup \{\varphi \vee \chi\}$, since "$w^*(\varphi \vee \chi)$ =T either $w^*(\varphi)$ =T or $w^*(\chi)$ =T; suppose the former then w satisfies $\Gamma \cup \{\varphi\}$ and since by hypothesis $\Gamma, \varphi \vDash \psi$ we have $w^*(\psi)$; similarly if $w^*(\chi)$ =T, we'd have $w^*(\psi)$ =T andhence $\Gamma, \varphi \vee \chi \vDash \psi$ · $(\Leftarrow)$ Suppose $\Gamma, \varphi \vee \chi \vDash \psi$ and let w be a valuation that satisfies $\Gamma \cup \{\varphi\}$; in particular $w^*(\varphi)$ =T and so therefore $w^*(\varphi \vee \chi)$ =T. But then by hypothesis $w^*(\psi)$ =T. Thus $\Gamma, \varphi \vDash \psi$. The argument supposing w satisfied $\Gamma \cup \{\chi\}$ is the same. QED

The reader should check that he or she can verify each of the above. Note that (d) is merely a special case of (c); and (e) - (j) really just reflect the natural properties of the connectives. Notice that if φ is truth-functionally equivalent to ψ we can write this as "$\varphi \vDash \psi$ and $\psi \vDash \varphi$", and this is the same as saying that $\varphi \longleftrightarrow \psi$ is a tautology equivalently or $\vDash \varphi \longleftrightarrow \psi$ (this is Lemma 2.10.i)

A *set* of formulae may be unsatisfiable without any member of the set being a contradiction as this example shows:

Example 8 If $\Gamma = \{P \vee Q, P \vee \neg Q,\ \neg P \vee Q,\ \neg P \vee \neg Q\}$ then Γ is unsatisfiable, but every proper subset of Γ is satisfiable. (Check!)
Notice the following: if $\Gamma \subseteq \Delta$ are sets of formulae in L_ω then

a) if Γ is unsatisfiable then Δ is unsatisfiable, or to put it another way

b) if Δ is satisfiable then Γ is satisfiable

The reader should check this and also see the the implication in a) (or in b)) cannot be reversed. (Just look around for a counterexample.)
We've already mentioned that if φ and ψ are truth-functionally equivalent and if χ is a formula in which ψ occurs then replacing ψ by φ will not affect which valuations satisfy χ. We finish off this section by giving a fomral definition of this idea of "replacing subformulae" and then state a result.

Definition 2.11 *The relation "χ' comes from χ by replacing some (or all) occurrences of ψ by φ", which we shall write as Rep$(\varphi, \psi, \chi\ \chi')$, is defined by induction on complexity of χ:*

Rep$(\varphi, \psi, \chi, \chi')$ holds iff χ is an atom and χ' is χ
or χ is ψ and χ' is φ or ψ
or χ is $\chi_1 \to \chi_2$ and χ' is $\chi_1' \to \chi_2'$ and
Rep$(\varphi, \psi, \chi_1, \chi_1')$ and Rep$(\varphi, \psi, \chi_2, \chi_2')$
or χ is $(\neg\chi_1)$, χ' is $(\neg\chi_1')$ and Rep$(\varphi, \psi, \chi_1, \chi_1')$

Lemma 2.12 (The Principle of Substitution) *If φ and ψ are truth-functionally equivalent and Rep$(\varphi, \psi, \chi, \chi')$ then χ and χ' are truth functionally equivalent. Further for any Γ, $\Gamma \vDash \chi$ iff $\Gamma \vDash \chi'$.*

Proof The first sentence is contained in the remark following Exmaple 3. And from this, since precisely the same valuations make χ true as make χ' true, the second sentence is obvious. QED

We remark also that if ω is countable (say ω is enumerated as $\{P_k | k \in \mathbb{N}\}$) then the formulae of L_ω from a countable set: we could consider coding up strings of symbols using digits in the following manner:

Symbol	(	)	→	¬	P_k
Code	1	2	3	4	588...88 (k eights)

Then any symbol string (whether or not it is a proper formula) can be coded into a number. This already shows that there is a (1-1) map of strings into $\mathbb{N}$, thus the set of all strings is countable and hence so is the set of all formulae. Since the rules for forming formulae are inductive we can check, given a number whether it is the code of a proper formula or not. Indeed we could easily write a computer program that would do this for us. So we say there is an algorithm or an "effective procedure" for checking whether "n is the code number of a formula". We've also remarked that it is not hard to see that checking whether a formula is a tautology or not is an effective procedure: we could have a program which given (the code

number of) a formula will draw up its truth table. Thus putting these two processes together we can say that checking whether a number of codes a tautology is an effective procedure. There will be more on this in Chapter 6.

Exercise 8 Use truth tables to find out which of the following entailments is correct

a) $((\varphi \wedge \psi) \to \chi) \vDash (\varphi \to \chi)$
b) $((\sigma \wedge \neg\sigma) \to \varphi) \vDash \neg\varphi$
c) $(\varphi \to \psi), (\neg\varphi \to \psi) \vDash (\tau \wedge \neg\tau)$
d) $\vDash (\psi \to \psi)$
e) $\neg\tau \vDash (\tau \to \sigma)$
f) $\varphi \to \psi, \psi \to \neg\varphi \vDash \varphi$
g) $\neg(\varphi \to \psi), \neg(\psi \to \varphi) \vDash \varphi \wedge \neg\varphi$
h) $\vDash (\tau \to \chi) \leftrightarrow (\neg\chi \to \neg\tau)$

Exercise 9 (The Principle of Duality) Let φ be a formula whose only connectives are $\neg, \wedge$ and $\vee$. Let ϕ^* be the result of interchanging $\wedge$ and $\vee$ and replacing each propositional atom by its negation. Prove that ϕ^* is truth functionally equivalent to $\neg\varphi$. (A few examples should convince you that it is true; look at De Morgan's Laws.) [Hint: to prove this requires an induction on the number of occurrences of $\neg, \vee$, and $\wedge$ in φ.]

Exercise 10 a) Prove that a formula that only contains the connective $\leftrightarrow$ is a tautology iff each propositional atom occurs an even number of times. b) Prove that a formula that contains $\neg$ and $\leftrightarrow$ as its only connectives is a tautology iff $\neg$ and each atom occurs an even number of times. [Hint for a): first consider the case when φ contains a single atom P say; then use the fact that $(P \leftrightarrow (Q \leftrightarrow R))$ is truth functionally equivalent to $(P \leftrightarrow Q) \leftrightarrow R)$.]

Exercise 11 Let $\omega = \{P_n | n \in \mathbb{N}\}$ and let Γ be the set of formulae of L_ω as follows

$$\Gamma = \{P_n \to P_m | m, n \in \mathbb{N}, n < m\}$$

(i) is $\Gamma \cup \{P_0\}$ satisfiable?
(ii) is $\Gamma \cup \{\neg P_0, P_1\}$ satisfiable?
(iii) determine whether $\Gamma \vDash P_n \to P_m$ for each of the three possibilities $n < m, n > m, n = m$.
(iv) is $\{(\neg\varphi) | \varphi \in \Gamma\}$ satisfiable?
(v) is it possible to decide for an arbitrary formula ψ of L_ω, whether $\Gamma \vDash \psi$ or not?

2.4 The Compactness Theorem for L_ω

Suppose ω is a countable collection of propositional variables. Then L_ω is countable; we can ask: when is a set Γ of formulae of L_ω satisfiable? We've seen how to ascertain this for a single formula, and by extension we can do this for a conjunction of a finite set of formulae. [Just perform the process on p.??? to test whether $\neg\varphi$ is a tautology - if it isn't, the valuation thrown up shows that φ is satisfiable with that valuation.] The Compactness Theorem shows remarkably enough, that to test whether an *infinite* set of formulae is *simultaneously* satisfiable, it's enough to test all *finite* subsets *separately*. We use the following lemma, of interest in its own right in the proof.

Let S be a set of finite sequences of 0's and 1's. We can think of a typical element t of S as a finite function, so that if the sequence is of length n then we can write t out as $(t(0), t(1), t(2), \ldots, t(n-1))$. We call S a *tree on* $\{0,1\}$ if it has the property that if $t \in S$ then any initial segment of t is in S. Thus for t above for any i with $0 \leq i \leq n-1 (t(0), \ldots, t(i)) \in S$. (The empty sequence is an initial segment of every sequence and so is also in S.)

Theorem 2.13 (König's Tree Lemma) *Suppose S is a tree on $\{0,1\}$ and it has infinitely many members. Then there is an infinite sequence $(s(0), s(1), \ldots, s(n), \ldots)$ so that:*

$$\forall n \geq 0 (s(0), s(1), \ldots, s(n)) \in S.$$

Proof A sort of proof by induction. The conclusion of the lemma is that there is an infinite "branch" through the tree. Since S is infinite, either infinitely many sequences begin with a 0 or with a 1 (or both). Select a 0 or 1 for which this is true, and call it i_0 say. Set $s(0) = i_0$. Now infinitely many sequences must begin $(i_0, 0)$ or $(i_0, 1)$. Suppose infinitely many start (i_0, i_1). Set $s(1) = i_1$. Then further, infinitely many must start $(i_0, i_1, 0)$ or $(i_0, i_1, 1)$. Suppose it's i_2 and set $s(2) = i_2$. We continue in this way inductively defining s.
(Notice that this is not a straightforward induction: at each stage we may have to make a choice between i_k being 0 or 1 if infinitely many start $(i_0, \ldots, i_{k-1}, 0)$ and $(i_0, \ldots, i_{k-1}, 1)$. We thus potentially have to make infinitely many choices; in our underlying theory of sets we have to have a (rather weak) axiom that allows us to make infinitely many choices in this way.) The notion of a tree on any set rather than $\{0, 1\}$ is defined similarly. We use Lemma 2.13 to show:

Theorem 2.14 (Compactness Theorem for L_ω) *Let L_ω be a countable propositional language, and let Γ be a set of formulae in L_ω. Then Γ is satifsiable iff every finite subset of Γ is satisfiable.*

Proof If Γ is satisfiable by some valuation w, then trivially every finite subset of Γ is simultaneously satisfied by that same w. Conversely if Γ is finite then the result is also trivial so suppose that Γ is infinite. Let Γ be enumerated $\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_n, \ldots$. We wish to show that Γ is satisfiable. Let ψ_k be $\varphi_0 \wedge \ldots \wedge \varphi_k$. Then ψ_k is satisfiable iff $\varphi_0, \ldots, \varphi_k$ are simultaneously satisfiable. This mans it would be enought to show that $\Gamma^* = \{\psi_k | k \in \mathbb{N}\}$ is satisfiable, since then if w satisfies Γ^*, w will satisfy all of Γ. The hypothesis clearly implies every finite subset of Γ^* is satisfiable: let $\Delta \subseteq \Gamma^*$ be finite, let k be largest so that $\psi_k \in \Delta$, then if u satisfies $\varphi_0, \ldots \varphi_k$, u satisfies Δ.
We now define a tree S on $\{\mathrm{T}, \mathrm{F}\}$. Since ω is countable let's suppose the propositional variables are enumerated as $P_1, P_2, \ldots, P_k, \ldots$. We think of a finite valuation u of just the first $n+1$, say, propositional atoms alone as a finite sequence of T's and F's $u(1), \ldots, u(n)$. Let n_k be least such that the atoms of ψ_k are amongst $\{P_1, \ldots, P_{n_k}\}$. Notice that $k \leq k'$ implies that $n_k \leq n_{k'}$, since $\psi_{k'}$ essentially "contains" ψ_k. We put all possible u into S if, for some k, u is a sequence of length n_k and $u^*(\psi_k) = T$.
Remark Notice also that if $u^*(\psi_k)$ =T, then $u^*(\psi_l)$ =T for all $l < k$ because as above, ψ_l is "contained" in ψ_k.
If we put u into S, we also put all initial segments of u into S. This makes S into a tree and then every formula in Γ^* is satisfied by some finite valuation in S. [If S is finite then there is a maximal length to any sequence in S, n say. But that means that for all k ψ_k's atoms are always amongst $\{P_0, \ldots P_n\}$. Since there are at most 2^n sequences in S of length n, and Γ^* is infinite there must be some $n \in S$ of length n so that u satisfies infinitely many ψ_k's. But that means u satisfied *all* the ψ_k's and so all of Γ^*. If S is infinite then notice that since we have put sequences into S of arbitrary length S is infinite. By the Tree Lemma there is an infinite sequence $(w(0), w(1), \ldots)$ of T's and F's, so that for all $n \geq 0$ $(w(0), \ldots, w(n)) \in S$. Let ψ_k be arbitrary; we shall show that $w^*(\psi_k) = T$. Since there are sequences in S of arbitrarily length, let $v \in S$ be a finite initial segment of w of length greater than n_k; then v is an initial segment of some u that satisfied some ψ_k, or other (or v is itself such a u); now this u has length $n_{k'} > n_k$; this means that $k' > k$. But as $u^*(\psi_{k'})$ =T we have as in the remark above that $u^*(\psi_k)$ =T. But since u and v (and hence w) agree on the valuation of the propositional atoms occurring in ψ_k, this means that $w^*(\psi_k)$ =T too! As k was arbitrary, we have that w satisfies all of Γ^* and so all of Γ. QED

We give some examples involving the Compactness Theorem. Consider the following:

Example 9 Let $\Gamma \cup \{\varphi\}$ be formulae in L_ω.
(*) If $\Gamma \vDash \varphi$ the there is a finite $\Gamma_0 \subseteq \Gamma$ so that $\Gamma_0 \cup \{\neg\varphi\}$ is unsatisfiable. By the Compactness Theorem there must be some finite $\Gamma_0 \subseteq \Gamma$ so that $\Gamma_0 \cup \{\neg\varphi\}$ is unsatisfiable. That is $\Gamma_0 \vDash \varphi$
Example 10 Let Δ be a set of formulae in a language L_ω. Suppose every valuation satisfies at least one formula of Δ. Prove that there are $\varphi_1, \ldots, \varphi_n \in \Delta$ so that $\varphi_1 \vee \ldots \vee \varphi_n$ is a tautology.
Proof: $\overline{\Delta} = \{\neg\varphi | \varphi \in \Delta\}$ is unsatisfiable. So by the Compactness Theorem some finite $\neg_0 \subseteq \overline{\Delta}$ is unsatisfiable. Let $\Delta_0 = \{\neg\varphi_1, \ldots, \neg\varphi_n\}$ say. Then every valuation makes $\neg\varphi_1 \wedge \ldots \wedge \neg\varphi_n$ false. But then every valuation makes $\varphi_1 \wedge \ldots \wedge \varphi_n$ true.
The Compactness Theorem has some socially useful applications.

Theorem 2.15 (The Marriage Problem) *Suppose we have an infinite set W of women $w_0, w_1, w_2, \ldots$, each of whom has at most a finite number of male special friends. If for each n, any n of the women have between them at least n boyfriends, then it is possible for each woman to marry (heterosexually) without anybody committing bigamy (or biandry).*

Proof: We shall need the following:

Lemma 2.16 *If U is a set of M women and for each $k \leq m$, any k of the women have at least k boyfriends between them, then it is possible for each woman to marry one of her boyfriends without anybody committing bigamy or biandry.*

This is just the finite case of the theorem to be proved and can be proven by induction on m. We leave it to the reader. Let $M = \{m_j | j \in \mathbb{N}\}$ be the men in question all of whom have at least one of the women as a girlfriend. Choose a set ω of propositional atoms double-indexed as follows: $\omega = \{P_{ij} | i, j \in \mathbb{N}\}$. Let Γ be the set of formulae in Γ_ω consisting of all the formulae specified by:

(A) For each i the formula

$$P_{ij_0} \vee P_{ij_1} \vee \ldots \vee P_{ij_k}$$

where $m_{j_0}, \ldots m_{j_k}$ are all the boyfriends of w_i.

(B) For each $i \in \mathbb{N}$ and each pair j, j' in $\mathbb{N}$ the formula

$$\neg(P_{ij} \wedge P_{ij'})$$

(C) For each $j \in \mathbb{N}$ and each pair i, i' in $\mathbb{N}$ the formula

$$\neg(P_{ij} \wedge P_{i'j}).$$

Let Γ_0 be a finite subset of Γ. We show Γ_0 is satisfiable. Let V be the finite set of w_i such that for some jP_{ij} occurs in a formula in Γ_0. The hypotheses of the theorem imply that whatever the size of V there are enough boyfriends to apply the lemma to marry off the w_i of V with some m_j without bigamy, etc. being

committee. We define a valuation by $u(P_{ij})$ =T if $w_i \in V$ and w_i marries m_j by this process, $u(P_{ij})$ =F otherwise.
The clearly u satisfies Γ_0. So we conclude by the compactness theorem that there is a valuation v that satisfies all of Γ simultaneously. Now let w_i now marry m_j iff $v(P_{ij})$ =T. Since Γ contains all the formulae in (A) each woman marries one of her boyfriends and bigamy (respectively biandry is not committed since Γ contains all of (B) (respectively (C)). QED

Exercise 12 Formulate and prove König's Tree Lemma for trees on any fixed finite set of symbols. What if the set was infinite?
Exercise 13 Show that $(^*)$ of Example 9 implies the Compactness Theorem (so that $(^*)$ is equivalent to this theorem).
Exercise 14 Suppose $\Gamma \subseteq L_\omega$ is satisfiable, let $\Delta = \Gamma \cup \{\neg(P_0 \vee \ldots \vee P_n) | n \in \mathbb{N}\}$. if Δ is unsatisfiable show that for some n $\Gamma \vDash P_0 \vee \ldots \vee P_n$.
Exercise 15 A *graph* is structure $\langle A, R\rangle$ where R is a symmetric relationon a set A. Let us say that two elements a, b of A are *connected* if aRb. A graph is k-coloured if A can be partitioned into k disjoint subsets so that no two connected elements are in the same subset. Show that if A is countable, $\langle A, R\rangle$ is k-colourable iff every finite subgraph is k=colourable. [Hint: let A be enumerated $a_1, a_2, \ldots, a_n, \ldots n \in \mathbb{N}$; choose $\omega = \{P^i_j | i < k, j \in \mathbb{N}\} \cup \{Q_{ij} | i, j \in \mathbb{N}\}$; think of a valuation u giving $u(P^i_j)$ =T if a_j is coloured with colour i, and $u(Q_{ij})$ =T iff $a_j R a_j$; then choose a suitable set Γ; argue similarly to the Marriage Problem]
Exercise 16 Show that if A is a finite set and R a partial ordering on A then there is a total ordering R^* on A extending R, [i.e $R^* \supseteq R$, *or* in other words $aRb \Rightarrow aR^*b$ for all $a,\ b \in A$]. Hence deduce that any countable partially ordered set $\langle A, R\rangle$ can be totally ordered by some R^* extending R. [Hint: the first part asks you to prove the "finite case"; assuming that done choose an enumeration of the countable A as in Ex. 15 and take ω as $\{Q_{ij} | i, j \in \mathbb{N}\}$].

2.5 Normal Forms and Truth Functional Completeness

It is often useful to know that a formula can be written out in some uniform, or canonical way, usually called "normal form".

Definition 2.17 *A formula of the form $(\neg\varphi)$ is called a* negation*; a* conjunction *is a formula of the form $\psi_1 \wedge \psi_2 \wedge \ldots \wedge \psi_n$ for some formulae $\psi_1, \ldots, \psi_n$; a* disjunction *is a formula of the form $\psi_1 \wedge \psi_2 \wedge \ldots \wedge \psi_n$ for some formulae $\psi_1, \ldots, \psi_n$.*

Definition 2.18 *A formula φ is in* disjunctive normal form*, (dnf), if it is a disjunction $\psi_1 \vee \psi_2 \vee \ldots \vee \psi_n$, where each $\psi_i (l \leq i \leq n)$ is a conjunction of propositional atoms or negations of propositional atoms.*

We give an example of a formula which is in dnf in the proof of the following theorem

Theorem 2.19 (Disjunctive Normal Form Theorem) *Every formula is truth functionally equivalent to one in dnf.*

Proof We illustrate by means of an example. Let φ be the formula $P \rightarrow (Q \wedge R)$. Consider the truth table for φ:

P	Q	R	(Q ∧ R)	(P→ (Q ∧ R))
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F
F	T	T	T	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

We simply read off from the final column those lines where φ comes out true and see what assignments are necessary for this to happen. Thus φ is then truth functionally equivalent to:

$$(P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$$

The convenience of this normal form is that it displays precisely the alternative truth conditions that are necessary to make φ true. Notice that if φ had been a contradiction then φ is truth functionally equivalent to $S \wedge \neg S$ which is also in dnf. QED

Definition 2.20 *A formula is in* conjunctive normal form, *(cnf), if it is a conjunction $\psi_1 \wedge \psi_2 \wedge \ldots \wedge \psi_n$, where each $\psi_i (1 \leq i \leq n)$ is a disjunction of propositional atoms or negations of propositional atoms.*

Theorem 2.21 (Conjunctive Normal Form Theorem) *Every formula is truth functionally equivalent to one in conjunctive normal form.*

Proof Using the same example as for the Disjunction Normal Form Theorem, we now look at those lines where φ comes out F. So φ is equivalent to *none* of them holding, i.e.

$$\varphi \longleftrightarrow \neg((P \wedge Q \neg R) \wedge (P \wedge \neg Q \wedge R)) \wedge (P \wedge \neg Q \wedge \neg R))$$

Using De Morgan's Laws (and the Principle of Substitution, Lemma 2.12) we get

$$\varphi \longleftrightarrow \neg(P \wedge Q \wedge \neg R) \wedge \neg(P \wedge \neg R) \wedge \neg(P \wedge \neg Q \wedge R) \wedge \neg Q \wedge \neg R)$$

and again

$$\varphi \longleftrightarrow (\neg P \vee \neg Q \vee \neg\neg R) \wedge (\neg P \vee \neg\neg Q \vee \neg R) \wedge (\neg P \vee \neg\neg Q \vee \neg\neg R)$$

We now use the tautology of Example 4 (4) (and Lemma 2.12 again) to get

$$\varphi \longleftrightarrow (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R)$$

We can use the DNF Theorem to show that the set $\{\neg, \rightarrow\}$ is complete in the following sense. QED

Definition 2.22 *A set G of truth functions is* truth functionally complete*, or simply complete, if every truth function is a composition of functions from the set G.*

We are thinking of a truth function here as a function from $\{\mathrm{T}, \mathrm{F}\}^n$ to $\{\mathrm{T}, \mathrm{F}\}$ for some n. (Thus the propositional connective $\to$ is essentially a function $\mathrm{F}_\to : \{\mathrm{T}, \mathrm{F}\}^2 \to \{\mathrm{T}, \mathrm{F}\}$ given by the relevant table; so for example $\mathrm{F}_\to(\mathrm{T}, \mathrm{F})$ =F). We saw that the tables for the two place connectives $\wedge$, $\vee$, and $\to$ required 2^2 lines. In general for a table representing a two place truth function 2^2 lines are necessary, each with a choice of T of F in the final column, thus giving $2^{2^2} = 16$ possible such tables altogether. A truth table corresponding to a three place truth function would have 2^3 lines, and there are $2^{2^3} = 256$ such tables; and similarly there are 2^{2^n} n-place truth functions. We say by means of tables how $\wedge$ and $\vee$ can be expressed in terms of $\neg$ and $\to$. And the idea in the proof of the DNF Theorem shows how any truth function can be expressed using $\vee$, $\wedge$, and $\neg$.

Example 11 A three place connective or truth function, ζ, is defined by the table

φ	ψ	χ	$\zeta(\varphi, \psi, \chi)$
T	T	T	T
T	T	F	F
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	F
F	F	F	T

$\zeta(\varphi, \psi, \chi)$ is equivalent to $(\varphi \wedge \psi \wedge \chi) \vee (\neg\varphi \wedge \neg\psi \wedge \neg\chi)$. Since we can express $\wedge$, and $\vee$ in terms of $\neg$ and $\to$, we can do the same for ζ. And this approach would work for any other 3 or n place truth fucntion. We have thus shown

Theorem 2.23 (Truth Functional Completeness Theorem) *The set $\{\neg, \to\}$ is truth functionally complete.*

Exercise 6 showed that in fact $\neg, \to$ could be defined in terms of either $|$ or $\downarrow$. We thus have that both the sets $\{|\}$ and $\{\downarrow\}$ are complete. Exercise 5 showed that $\to$ could be defined in terms of $\neg$ and $\wedge$. This means that $\{\neg, \wedge\}$ is also a complete set.

Example 12 The set $\{\to, \vee\}$ is incomplete. The reason being that any formula built up using only these connectives will have a truth value T whenever the atoms within it are assigned T. Thus there can be no way that we can represent the one place negation function $\mathrm{F}_\neg$.
In general showing that a set is incomplete is harder than showing completeness: one has to notice some feature of the functions built up from the given set that precludes defining e.g., $\neg$, as in the last example. These examples show that our choice of $\to$ and $\neg$ as primitive is arbitrary to a certain extent; the choice is a balance between economy so as not to have too many clauses in inductive definitions and proofs, and over zealous economy (formulae built up from $\downarrow$ alone rapidly become unreadable.)

Exercise 17 Express $\varphi \to (\psi \vee \chi)) \longleftrightarrow (\chi \to (\psi \vee \tau))$ in cnf.
Exercise 18 Express the majority connective $\zeta(\varphi, \psi, \chi)$ in both cnf and dnf (See Exercise 2).

Exercise 19 Call a formula φ *full cnf* if it is in cnf and there is a natural number k and distinct propositional atoms $P_1, \ldots, P_k$ so that every conjunct in φ is of the form $\gamma_1 \vee \gamma_2 \vee \ldots \vee_{\gamma k}$ where each γ_i is either P_i or $\neg P_i$. (So every conjunct mentions the same set of atoms.) Show that any formula ψ, if is not a tautology, then it is equivalent to some ψ^* in full cnf. Show that any ψ which is not a tautology is a contradiction iff ψ^* (containing the same atoms) has 2^n distinct conjuncts.

Exercise 20 Show that the following are incomplete sets: $\{\rightarrow, \wedge\}$, $\{\zeta(\varphi, \psi, \chi)\}$, $\{\longleftrightarrow, \neg\}$.

Exercise 21 (i) Show that $\{\rightarrow, \nrightarrow\}$ where $\nrightarrow$ is "does not imply" (its truth table is that for $\rightarrow$ with the final column having T's and F's reversed), is a complete set.

(ii) Show that the 3 place truth function F defined by F(X, Y, Z) = "the value in the final column of the truth table for $(\varphi \vee \psi) \rightarrow \neg\chi$ corresponding to the line X Y Z" forms a complete set by itself.

Exercise 22 Show that $|$ and $\downarrow$ are the only binary connectives that are complete by themselves. [Hint: Suppose G(X, Y) is a binary truth function; argue that G(T, T) must be F and G(F, F) must be T (or $\neg$ would be indefinable) and then deduce that the truth table for G(X, Y) must correspond to one of the two alternatives]

Exercise 23 Show that only half the truth functions can be built up using the set $\{\neg, \wedge, \vee\}$.

First order languages and their Structures

We intend to give a definition of a class of languages that are considerably more expressive than the propositional languages, the so called *first order languages*. The atoms of our propositional languages were essentially variables that stood in for any proposition we cared to substitute in for them. We shall have variables in these new languages, but they will range over individuals. And these individuals will be considered to be elements of the domain of some structure, the domain of discourse so to speak. So first we must specify what kinds of structures we are referring to, and then we shall give inductive definitions of the terms and formulae of our languages, and then give tha all important definition of the Satisfaction Relation, which shows how we intend to give meaning to our syntactic formulae.

3.1 First order structures

The goal of this section is to define what kind of structures our languages will be able to refer to. The definition is sufficiently all encompassing that almost any structure of mathematics and indeed many in the world of computer science or the real world can be considered as first order structures. It is this fact that makes our theorems relating languages to these structures have the widest possible applicability. Further, the logic associated to such languages is much developed and is probably the most successful of all logics.

We want to give a general definition of structure that covers a very wide class of the objects we ever meet in mathematics or elsewhere. Obviously mathematical structures can be very dissimilar and the languages we need to talk about these different structures, albeit having many common features, will also be different. In particular what relations or functions occur in the structure will be a differentiating factor. What the idea of a similarity type (to be defined presently) does is indirectly collect together all structures with similar kinds of functions and relations.

We think of an n-ary relation on a set A as a set of ordered n-tuples, that is a subset of A^n. Likewise an n-ary function on a set A is a map $h : A^n \to A$. We allow here the idea of a 0-ary function, $h : A^0 \to A$, but actually this is just a way of picking an element, or in other words a *constant* from A. (This is because in set theory we have the convention that $X^0 = 1 = \{0\}$, so that then if $h : X^0 \to X$ there is only one element in the domain of X, namely 0, so h picks out a unique element of X, $h(0)$.)

F as a *constant symbol* if $f(F) = 0$. We often use $c, d, \ldots$, etc. as constant symbols rather than 0-ary $F, G, \ldots$.

Definition 3.1 *A* similarity type *is an ordered pair* $\Omega = \langle \boldsymbol{r}, \boldsymbol{f} \rangle$ *where* $\mathbf{r}$ *and* f *are functions with range contained in* $\mathbb{N}$. *The elements of* $\operatorname{dom} \boldsymbol{r}$ *are called the* relation symbols *of* Ω, *those of* $\operatorname{dom} \boldsymbol{f}$ *the* function symbols. *We say* R *is an* n-ary *relation (or* F *an* n*-ary function symbol) if* $\mathbf{r}(R) = n$ (*or* $\boldsymbol{f}(F) = n$); *if* $\boldsymbol{f}(F) = 0$ *we call* F *a* constant symbol.

The idea is thus that Ω specifies the kind of structures we can use the symbols in $\operatorname{dom} \mathbf{r}$ and $\operatorname{dom} \mathbf{f}$ to talk about. Referring to the discussion above when we allow F to be 0-ary function symbol, (and so are thinking of it as a constant symbol) we use the letters c, d, e, and os on instead. Usually there will not be any ambiguity in simply saying "R is an n-ary relation symbol" rather than the more pedantic "$R \in \operatorname{dom} \mathbf{r}$ and $\mathbf{r}(R) = n$", and similarly for functions. It is worth emphasising that the R's and F's in this discussion are *not* relations and functions, they are simply syntactic symbols that we shall later *interpret* as relations and functions; alternatively we could say that they will be used to *denote* relations or functions. This is just analogous with the idea that "2" is not a number, it is merely a *numeral* that we interpret as the number two.

Definition 3.2 *Let* $\Omega = \langle \boldsymbol{r}, \boldsymbol{f} \rangle$ *be a similarity type. An* Ω*-structure is an ordered triple*

$$\boldsymbol{A} = \langle A, \langle R_{\boldsymbol{A}} \rangle_{R \in \operatorname{dom} \boldsymbol{r}}, \ \langle F_{\boldsymbol{A}} \rangle_{F \in \operatorname{dom} \boldsymbol{f}} \rangle$$

where A *is a non-empty set; for each* $R \in \operatorname{dom} \mathbf{r}$, $R_{\boldsymbol{A}}$ is an $r(R)$-ary relation on A, *and* $F_{\boldsymbol{A}}$ *is an* $\boldsymbol{f}(F)$*-ary function on* $\boldsymbol{A}$. A *is called the* domain *of* $\boldsymbol{A}$ *and members of* A *are* elements *of* A. *The* cardinality *of* $\boldsymbol{A}$ *is that of* A, *and in particular we say* $\boldsymbol{A}$ *is infinite if* A *is an infinite set.*

When we have an Ω-structure in mind we often simply write it out as

$$\mathbf{A} = \langle A, H_1, H_2, H_3, \ldots \rangle$$

where the H_i are the various relations and functions $R_{\mathbf{A}}, \ F_{\mathbf{A}}$.

Examples

Groups

1. Take $\mathbf{r}$ as empty and $\mathbf{f}$ as the function with $\operatorname{dom} f = \{\bullet\}$ with $\mathbf{f}(\bullet) = 2$. Every group is then an $\langle \mathbf{r}, \mathbf{f} \rangle$ structure:
   $tmstrongG = \langle G, \bullet_G \rangle$ where the elements of the group $\mathbf{G}$ is the set of G and $\bullet_G$ is the group multiplication.

2. Groups have more than just a multiplication action in them. Take $\mathbf{r}$ as empty, but $\mathbf{f}$ now has $\operatorname{dom} \mathbf{f} = \{\bullet, ^{-1}, e\}$ with $\mathbf{f}(\bullet) = 2, \ \mathbf{f}(^{-1}) = 1, \ \mathbf{f}(e) = 0$. Notice here that e is an 0-ary function symbol, or in other words a constant symbol.

   Then again a group is an $\langle \mathbf{r}, \mathbf{f} \rangle$ structure. $\mathbf{G} = \langle G, \bullet_{\mathbf{G}}, \ ^{-1}_{\mathbf{G}}, e_{\mathbf{G}} \rangle$ where $\bullet_{\mathbf{G}}$ is as before, $^{-1}_{G}$ is the inverse function, and $e_{\mathbf{G}}$ is the identity element.

3. The following way of presenting groups illustrates a general fact of structures: n-ary functions can be thought of as $n+1$-ary relations. Let $\mathbf{f}$ be empty but $\mathbf{r}$ have $\operatorname{dom}\mathbf{r} = \{\bullet\}$. Then if $\mathbf{r}(\bullet) = 3$ we can represent Example 1 as $\mathbf{G} = \langle G, \bullet_{\mathbf{G}}\rangle$ where now $\bullet$ is a ternary relation where if $a, b, c \in G$, $\bullet_{\mathbf{G}}(a, b, c)$ holds if the group multiplication of a followed by b results in c.

   Thus structures can be presented in a variety of ways depending on the similarity type chosen, some with more, some with less information in the form of displayed functions or relations.

Number systems

4. We may present a structure $\mathbb{N}_0 = \langle \mathbb{N}, <_{\mathbb{N}_0}, 0_{\mathbb{N}_0}\rangle$ which is an $\langle \mathbf{r}, \mathbf{f}\rangle$-structure where $\operatorname{fom}\mathbf{r} = \{<\}$, $\mathbf{r}(<) = 2$, $\operatorname{dom}\mathbf{f} = \{0\}$, $\mathbf{f}(0) = 0$. $<_{\mathbb{N}_0}$ is the usual binary relation on $\mathbb{N}$, and $0_{\mathbb{N}_0}$ is of course zero.

5. $\mathbb{N} = \langle \mathbb{N}, +_{\mathbb{N}}, \bullet_{\mathbb{N}}, {}'_{\mathbb{N}}, 0_{\mathbb{N}}\rangle$ where now $\operatorname{dom}\mathbf{f} = \{+, \bullet, {}', 0\}$ with $f(0) = 0$ as before, $f(+) = \mathbf{f}(\bullet) = 2$, $\mathbf{f}({}') = 1$; $+_{\mathbb{N}}, \bullet_{\mathbb{N}}$ are the usual addition and multiplication, ${}'_{\mathbb{N}}$ is the successor function.

Other algebraic systems

6. *Fields*. Let $\operatorname{dom}\mathbf{f} = \{+, -, \bullet, {}^{-1}0, 1\}$ with $\mathbf{f}(+) = \mathbf{f}(\bullet) = \mathbf{f}(-) = 2, \mathbf{f}({}^{-1}) = 1, f(0) = \mathbf{f}(1) = 0, \mathbf{r}$ is empty; then any field is an $\langle \mathbf{r}, \mathbf{f}\rangle$-structure

$$\mathbf{f} = \langle F, +_{\mathbf{f}}, -_{\mathbf{f}}, 0_{\mathbf{f}}, 1_{\mathbf{f}}\rangle.$$

   The careful reader will notice something wrong here: $0_{\mathbf{f}}^{-1}$ doesn't exist but our definition of structure does not allow the possibility for functions that are not defined everywhere. Accordingly we give $0_{\mathbf{f}}^{-1}$ some default value, $0_{\mathbf{f}}$ say, and then we are careful about statements we wish to make concerning inverses in the field.

7. *Binary relations*. Let A be any non-empty set, R any binary relation on A (for example it might be a linear order) then $A = \langle A, R\rangle$ can be thought of as Ω-structure where $\Omega = \langle \mathbf{r}, \mathbf{f}\rangle$, f empty, $\mathbf{r}$ has a symbol $\dot{R}$ in it and $\mathbf{r}(\dot{R}) = 2$, and we set $\dot{R}_{\mathbf{A}} = R$.

   The last example shows that given a structure $\mathbf{A} = \langle A, H_1, \ldots\rangle$ say we can look at $H_1, \ldots$ and think of $\mathbf{A}$ as an $\langle \mathbf{r}, \mathbf{f}\rangle$-structure by constructing $\mathbf{r}, \mathbf{f}$ from a suitable stock of symbols. An easy way to write down such sym;bols being to place dots over the relations and functions of the given structure, that is $\dot{H}_1, \ldots, \dot{H}_n, \ldots$, etc. We often do this implicitly, by talking about the language of $\mathbf{A}$ or of fields, rings, etc., which we can obtainin this manner.

3.2 Relations between structures

The previous definition of structure in a very generalised sense encompasses any of the usual mathematical, and many non-mathematical, structures. Normally we look at certain classes of structures, groups, fields, vector spaces, etc., and look at relationships between members of that class, i.e. between groups, or between vector spaces. Further we are often interested when given a group say to look at all of its

subsets which are in the same class of structures, i.e. at all of its subgroups. And similarly at subrings of a given ring and so on. The first definition looks at a precise description of this idea of "subsets of the same type" or a *substructure*. Later definitions will generalise between arbitrary structures the idea of homomorphism.

Definition 3.3 *Let $\boldsymbol{A}$ be a structure of similarity type $\Omega = \langle \boldsymbol{r}, \boldsymbol{f} \rangle$. We say $\boldsymbol{B}$ is a* substructure *of $\boldsymbol{A}$, $\boldsymbol{B} \subseteq \boldsymbol{A}$, if $\boldsymbol{B}$ is an Ω-structure and*

(i) $B \subseteq A$

(ii) For each $R \in \operatorname{dom} r$, if $\mathbf{r}(R) = n$ then $R_A \cap B^n = R_{\boldsymbol{B}}$

(iii) For each $F \in \operatorname{dom} f$, if $\mathbf{f}(F) = n$ then for any $b_1, \ldots, b_n \in \boldsymbol{B}$ $F_{\boldsymbol{B}}(b_1, \ldots, b_n) = F_A(b_1, \ldots, b_n)$.

Remark 1 $\mathbf{B}$ an Ω-structure implies that it is closed under the functions $F_{\mathbf{B}}$ for $F \in \operatorname{dom} f$, so in (iii) above $F_{\mathbf{B}}(b_1, \ldots, b_n) \in B$ by definition.

2 When $f(F) = 0$ then F is a constant symbol, (iii) then says that $F_{\mathbf{A}} = F_{\mathbf{B}}$ (and so is also in B by the first remark.)

We also say, if $\mathbf{B}$ is a substructure of $\mathbf{A}$, that $\mathbf{A}$ is an *extension* of B.

Examples

8. Consider Example 1. Suppose $\mathbf{G} = \langle G, \bullet_{\mathbf{G}} \rangle$ is a group and that $\mathbf{H} = \langle H, \bullet_H \rangle$ is a subgroup of $\mathbf{G}$. Then according to the above definition $\mathbf{H} \subseteq \mathbf{G}$. On the other hand if $\mathbf{H} \subseteq \mathbf{G}$, it's not necessarily the case that $\mathbf{H}$ is a subgroup of $\mathbf{G}$. H will be closed under group multiplication, but will not necessarily be closed under the group inverse function.

9. Example 2 gives a presentation of groups so that all substructures are subgroups: by including $^{-1}$ in dom $\mathbf{f}$ we ensure any substructure is closed under inverses.

10. Let $\mathbf{E} = \langle \{Evens\}, <_E, 0_E \rangle$ and $\mathbf{O} = \langle \{Odds\}, <_{\mathbf{O}}, 0_{\mathbf{O}} \rangle$. Then $E \subseteq \mathbb{N}_0 = \langle \mathbb{N}, <_{\mathbb{N}_0}, 0_{\mathbb{N}_0} \rangle$ and $\mathbf{O} \subseteq \mathbb{N}_0$. Indeed even $1 = \langle \{0\}, <_1, 0 \rangle \subseteq \mathbb{N}_0$. But if $\mathbb{N}_0 = \langle \mathbb{N}, +_{\mathbb{N}_1}, \bullet_{\mathbb{N}_1}, {}'_{\mathbb{N}_1}, 0_{\mathbb{N}_1} \rangle$ is the structure of Example 5, the only substructure of $\mathbb{N}_1$ is $\mathbb{N}_1$ itself. (Why?)

Definition 3.4 *let A and B be two Ω-structures, a map $h : A \to B$ is a* homomorphism from $\mathbf{A}$ to $\mathbf{B}$ *iff (where $\Omega = \langle \boldsymbol{r}, \boldsymbol{f} \rangle$)*
(i) $\forall R \in \operatorname{dom} \boldsymbol{r}$, $\forall a_1, a_2, \ldots, a_{\boldsymbol{r}(R)} \in A$ $\langle a_1, \ldots, a_{\boldsymbol{r}(R)} \rangle \in R_{\boldsymbol{A}} \Rightarrow \langle h(a_1), \ldots, h(a_{r(R)}) \rangle$ R_B;
(ii) $\forall F \in \operatorname{dom} \boldsymbol{f}$, $\forall a, a_1, \ldots, a_{\boldsymbol{f}(F)} \in A$ $F_{\boldsymbol{A}}(a_1, \ldots, a_{\boldsymbol{f}(F)}) = a \Rightarrow F_B(h(a_1), \ldots, h(a_{f(F)})) = h(a)$.

The idea is that such a mapping preserves structure. Note again when $\mathbf{f}(F) = 0$, that this says simply $h(F_{\mathbf{A}}) = F_{\mathbf{B}}$. If h is a homomorphism from $\mathbf{A}$ to $\mathbf{B}$ we write $h : \mathbf{A} \to \mathbf{B}$.

Example 11 If $\mathbf{G}_1 = \langle G_1, \bullet_{G_1}, e_{G_1} \rangle$ and $G_2 = \langle G_2, \bullet_{\mathbf{G}_2}, e_{\mathbf{G}_2} \rangle$ are groups and h a homomorphism between them, then h is a group homomorphism in the usual sense. [Notice we don't need $^{-1}$ to be a function in the similarity type for this to happen.]

Definition 3.5 *If $h : \boldsymbol{A} \to \boldsymbol{B}$ and $h : A \to B$ is one-to-one then h is called an* embedding. *If $h : A \to B$ is (1-1), onto* and *in addition, in clause (i) of the previous definition we write*

$$\langle a_1, \ldots, a_{\boldsymbol{r}(R)} \rangle \in R_{\boldsymbol{A}} \Leftrightarrow \langle h(a_1), \ldots, h(a_{\boldsymbol{r}(R)}) \rangle \in R_B.$$

Then h is called an isomorphism *and write $h : \boldsymbol{A} \cong \boldsymbol{B}$. We write $\boldsymbol{A} \cong \boldsymbol{B}$ iff there's an h so that $h : \boldsymbol{A} \cong \boldsymbol{B}$.*

Example 12 $\mathbb{N} = \langle \mathbb{N}, < \rangle$ and $\mathbb{N}^+ = \langle \mathbb{N}^+, < \rangle$ where $\mathbb{N}^+ = \mathbb{N} \backslash \{0\}$ and $<$ is the usual "less than" relation. These two structures are isomorphic via the function $h : \mathbb{N} \to \mathbb{N}^+$ defined by $h(n) = n + 1$. However $\langle \mathbb{N}, <, + \rangle$ is not isomorphic to $\langle \mathbb{N}^+, <, + \rangle$ [since in $\mathbb{N}$ there is c so that $c + a = a$ for all $a \in \mathbb{N}$, but in $\mathbb{N}^+$ there is no such thing.]

Exercise 1 If $h : \mathbf{A} \to \mathbf{B}$ and if we write $h[A]$ for the set of b in B in the range of h, is $h[A]$ a substructure of $\mathbf{B}$, with the relations and functions on $h[A]$, those inherited from $\mathbf{B}$?
Exercise 2 In Ex 3 where group multiplication was represented by a ternary $\bullet_G$, if $\mathbf{G}_1$ and $\mathbf{G}_2$ are two groups and $h : \mathbf{G}_1 \to \mathbf{G}_2$ is a homomorphism, is h a group homomorphism?
Exercise 3 Check that "is isomorphic to" is an equivalence relation.
Exercise 4 Find an example of structures $\mathbf{A}$ and $\mathbf{B}$ of the same type, with $h : \mathbf{A} \to \mathbf{B}$, $h : A \to B$, (1-1) and onto, but not $\mathbf{A} \cong \mathbf{B}$.

3.3 First order Languages

We shall construct formal languages L_Ω for talking about Ω-structures. Thus for each similarity type we shall have a different language. We shall single out certain expressions of L_Ω called *terms*, and then define formulae of L_Ω. The expressions themselves will be finite sequences built up from the symbols in $\mathrm{dom}\,\mathbf{r} \cup dom\mathbf{f}$ together with parenthesis (,), arrow $\to$, negation symbol $\neg$ and the universal quantifier $\forall$. To avoid ambiguities we shall assume the relation and function symbols different from these and from each other, and are not themselves sequences of length greater than 1. At the same time as defining terms and formulae we shall again define a complexity function *comp*. This will assign to each term and formula a natural number which is a measure of the complexity of the term or formula.

Definition 3.6 *We simultaneously define the* terms *t of L_Ω and their* complexity *comp(t) by recursion*

(i) For $n \in \mathbb{N}$ v_n is a term of complexity 0. It is called a variable.

(ii) *If* $F \in \mathrm{dom}\,\mathbf{f}$, $\mathbf{f}(F) = n$, *and* $t_1, \ldots, t_n$ are terms then

$$F(t_1, \ldots, t_n) \text{ is a term of complexity } max\{0, \mathrm{comp}(t_1), \ldots, \mathrm{comp}(t_n)\} + 1$$

(iii) Nothing is a term unless built up by clauses (i) and (ii).

Remark If $\mathbf{f}(F) = 0$, i.e. F a constant symbol, then $\mathrm{comp}(F) = 1$. Assume that $\mathrm{dom}\,\mathbf{f}$ contains the function symbols F (binary) and G (ternary) and the constant symbols a, b; then examples of terms are: $F(a, v_0)$ and $\mathrm{comp}(F(a, v_0)) = \max\{\mathrm{comp}(a), \mathrm{comp}(v_0)\} + 1 = \max\{1, 0\} + 1 = 2$. $G(F(a, v_0), v_1, b)$ whose complexity is $\max\{\mathrm{comp}(F(a, v_0)), \mathrm{comp}(v_1), \mathrm{comp}(b)\} + 1 = \max\{2, 0, 1\} + 1 = 3$.
$G(F(a, F(a, v_0)), v_1, b)$ has complexity 4. $G(a, b)$ and $F(F, a)$ are not terms.

Definition 3.7 *We simultaneously define* formula φ *of* L_Ω *and* $\mathrm{comp}(\varphi)$

(i) If s and t are terms then $s = t$ is a formula of complexity 0. *We call this formula an equation.*

(ii) If $R \in \mathrm{dom}\,\mathbf{r}$, $\mathbf{r}(R) = n$, and $t_1, \ldots, t_n$ are terms then $R(t_1, \ldots, t_n)$ is a formula also of complexity o.

(iii) φ is a formula then $(\neg\varphi)$ is a formula and $\mathrm{comp}((\neg\varphi)) = \mathrm{comp}(\varphi) + 1$.

(iv) If φ, ψ are formulae then $(\varphi \to \psi)$ is a formula and

$$\mathrm{comp}((\varphi \to \psi)) = \max\{\mathrm{comp}(\varphi), \mathrm{comp}(\psi)\} + 1.$$

(v) If φ is a formula and v_n a variable then $\forall v_n \varphi$ is a formula of complexity $\mathrm{comp}(\varphi) + 1$.

(vi) Nothing is a formula except as built up by clauses (i) - (v).

Formulae of complexity o are called *atomic formulae.*

Example 13 Let us suppose that dom **r** contains the relation symbols R (binary) and S (unary); then $R(F(a, v_0), a)$ is a formula of complexity o. $(R(v_0, v_1) \to \forall v_5 S(v_0))$ is a formula of complexity $\max \mathrm{comp}(R(v_0, v_1))$, $\mathrm{comp}(\forall v_5 S(v_0) + 1 = \max\{0, 1\} + 1 = 2$ $\forall v_0(\neg(R(v_0, v_1) \to \forall v_5 S(v_0)))$ has then complexity 4; the following are not formulae:

$$v_0\,;\ F(v_0, v_1)\,; \qquad \forall v_0(\neg(R(v_0, v_1 \to \forall v_5 S(v_0)))\,; \qquad S v_k\,; \qquad \forall b S(b).$$

Remark Clause (i) here shows that we are very much building the equality symbol = into every language L_Ω. This isn't necessary, many authors would omit clause (i), and if they wanted an equality relation symbol they would simple put = into dom **r**. Since equations are such a basic part of mathematical experience we decided to build it into the language so that it is there whenever we neet it, without having to make any further specifications. It is worth pointing out that the complexity of a formula is nothing to do with the complexity of any terms it may contain; (the complexity meansures the height of the implicit tree structure from which the formula is built). As with propositional languages, no formulae can be infinitely long.

The idea is that if **A** is an Ω-structure the terms of L_Ω are nouns, a term names an element of A: a constant symbol c names c_A, a variable v_k may name any element of A, and if $t_1, \ldots, t_n$ are terms naming $a_1, \ldots, a_n$ of A, then $F(t_1, \ldots, t_n)$ names $F_A(a_1, \ldots, a_n)$. The formulae of L_Ω then express statement about **A**. If s, t name a, b in A then $s = t$ says a is the same element as b. If R is an n-ary relation symbol then $R(t_1, \ldots, t_n)$ says that $\langle a_1, \ldots, a_n \rangle \in R_{\mathbf{A}}$ (where we're assuming that t_1 names a_i). If φ is a formula built up from certain terms then φinterpreted in a structure A will say something about the objects in the domain of the structure that the terms denote. The intention is that $\forall v_k \varphi$ will say that for every possible interpretation of v_k as an element of A φ is true in **A**.

Again it will be convenient to extend our list of various abbreviations, we write

$$\exists v_k \varphi \ \text{ for } \ (\neg \forall v_k (\neg \varphi)).$$

The binding rules for our defined connectives $\wedge$, $\vee$, and $\leftrightarrow$ remain in force. Thus $\forall v_0\varphi \wedge \psi \rightarrow \chi$ is $(\forall v_0\varphi \wedge \psi) \rightarrow \chi$, $\exists v_0\neg\varphi \rightarrow \forall v_0\psi \vee \chi$ is short for $\exists v_0\neg\varphi \rightarrow (\forall v_0\psi \vee \chi)$. Notice that $(\forall v_0\varphi \wedge \psi)$ is itself shor for $(\neg(\forall v_0\varphi \rightarrow (\neg\psi)))$. there is no sense of the quantifier $\forall v_0$ having anything to do with ψ. Note again that to calculate the complexity of a formula we must write it out in its official unabbreviated form.

Remark The set of expressions of L_Ω is countable if $\operatorname{dom}\mathbf{f} \cup \operatorname{dom}\mathbf{r}$ is. For, suppose we can enumerate $\operatorname{dom}\mathbf{r}$ as $R_1, R_2, \ldots, R_n, \ldots$ and $\operatorname{dom} f$ as $F_1, F_2, \ldots, F_n, \ldots$ we can assign positive integers to the symbols of the language as follows:

Symbol	,	(	)	$\rightarrow$	$\neg$	=	$\forall$	v_k
Code	0	1	2	3	4	7	49	599...9 (k nines)

R_k	F_k
788...899...99 ($\mathbf{r}(R_k)$ eights, k nines)	688...899...9 ($\mathbf{f}(F_k)$ eights, k nines)

Then, to each string of symbols we can associate a number (the "gödel number" or "gn"), for example $(R_1(v_0, v_1) \rightarrow \neg R_2(F_0(v_0), v_1))$ is then coded by the sequence of digits 178891505923478899168815205922. So we can enumerate all formulae, (indeed all symbol strings) in the order of these code numbers. In particular all the terms are countable, as are all the formulae. (The method of coding here is totally unimportant; in fact the rather idiosyncratic choice of digits reflects a coding we shall be using in a later chapter. But notice that a formula may be decoded in a completely mechanical way from a code number. It is also completely mechanical to check whether any string of digits does in fact code a term or a formula).

Examples

14. In Ex. 5 with $\Omega = \langle \mathbf{r}, \mathbf{f}\rangle$ as there, we have the formulae of L_Ω

$$\forall v_0\neg v_0' = 0 \qquad \forall v_0\forall v_1\ v_0 + v_0' = (v_0 + v_1)' \qquad \forall v_0\ v_0 \bullet 0 = v_0$$

These formulae will be intended to express the two facts true in $\mathbb{N}$ that zero is not the successor of any number, that the successor of b added to a, is the successor of (a plus b), and the false fact that anything times zero is that thing itself. But actually we haven't yet said anything about how we intend to interpret our formulae and terms in a structure. The same is true in the following three examples.

15. Ex. 2 gave a presentation of groups.

$\forall v_0\forall v_1\forall v_2(v_0 \bullet v_1) \bullet v_2 = v_0 \bullet (v_1 \bullet v_2)$ expresses the associative law whilst $\forall v_0(\forall v_1 v_1 \bullet v_0 = v_1 \rightarrow v_0 = e)$ expresses the fact that the identity is unique.

16. If $\mathbf{A} = \langle A, R_\mathbf{A}\rangle$ is a structure with R binary, (i.e., where $\mathbf{f}$ is empty, $\operatorname{dom}\mathbf{r} = \{R\}$, $\mathbf{r}(R) = 2$), then we can specify in L_Ω, that $R_\mathbf{A}$ is a strict partial ordering by requiring

(i) $\forall v_0 \neg R(v_0, v_0)$ (ii) $\forall v_0 \forall v_1 \forall v_2 [R(v_0, v_1) \wedge R(v_1, v_2) \rightarrow R(v_0, v_2)]$

By further requiring (iii) $\forall v_0 \forall v_1 [R(v_0, v_1) \wedge R(v_1, v_0) \wedge v_1 = v_0]$ we specify R as a (strict) total order.

17. We can specify that a structure has at least 3 elements in its domain:

$$\exists v_0 \exists v_1 \exists v_2 (v_0 \neq v_1 \wedge v_0 \neq v_2 \wedge v_1 \neq v_2).$$

Notice in the above we have taken some further liberty with our expressions; we've included [,] and have written $\neq$ as an abbreviation for $\neg v_0 = v_1$. Where R is an ordering relation we often write aRb for $R(ab)$ If Ω is a similarity type with a constant symbol c and $\mathbf{A}$ is an Ω-structure the formula $v_0 = c$ has no fixed meaning in $\mathbf{A}$ since the variable v_0 can name any element of A whilst c names $c_{\mathbf{A}}$. Such a variable is called free. We give a precise definition by induction on complexity of terms and formulae of when a variable is free in a term or formula.

Definition 3.8

$FV(v_n) = \{v_n\}$
$FV(F(t_1, \ldots, t_n)) = FV(t_1) \cup \ldots \cup FV(t_n)$
$FV(s = t) = FV(s) \cup FV(t)$
$FV(R(t_1, \ldots, t_n)) = FV(t_1) \cup \ldots \cup FV(t_n)$
$FV((\neg\varphi)) = FV(\varphi)$
$FV((\varphi \rightarrow \psi)) = FV(\varphi) \cup FV(\psi)$
$FV(\forall v_n \varphi) = FV(\varphi) - \{v_n\}$

Remark FV is then a function that is specified by recursion: it defines FV for terms (on the first two lines, note that if F is a constant symbol that $FV(F) = \varnothing$), then FV for formulae of complexity o then FV for formulae of complexity $k+1$ given the definition for formulae of complexity $\leq k$. The reason we bother defining complexityis that it makes definitions like the above simple and concise.

Definition 3.9 *If $FV(\varphi) = \varnothing$ we say φ is a* sentence. *If $FV(t) = \varnothing$ we say t is a* closed term.

Remark We can say informally that if $\forall v_k$ occurs in φ that v_k is "bound" in φ. In our original example $v_0 = c$, $v_0 \in FV(\varphi)$, but in $\forall v_0 v_0 = c\ v_0$ has been "bound" by the quantifier $\forall v_0$ and the resulting formula now has determinate meaning in any structure. Sentences are formulae which when interpreted in a structure have a determinate meaning. A closed term likewise is completely specified and identifies a unique element of the domain. Notice that the definition of $\exists$ too implies that $FV(\exists v_k \varphi) = FV(\varphi) - \{v_k\}$.

Example 18 Let R be binary, then in L_Ω $R(v_0, v_1)$ has v_0, v_1 free variables;
$FV(\forall v_0 \forall v_1 R(v_0, v_1)) = \varnothing$
$FV(\forall v_0 (R(v_0, v_1) \rightarrow \forall v_0 \exists v_1 R(v_1, v_0))) = FV((R(v_0, v_1) \rightarrow \forall v_0 \exists v_1 R(v_1, v_0))) = \{v_0\} =$
$= \{FV(R(v_0, v_1)) \cup FV(\forall v_0 \exists v_1 R(v_1, v_0\} - \{v_0\} = \{\{v_0, v_1\} \cup \varnothing\} = \{v_0\} = \{v_1\}.$

$FV(\forall v_0 R(v_1, v_0) \to \forall v_0 R(v_0, a)) = FV(\forall v_0 R(v_0, v_1)) = \{v_1\}$. $FV(\forall v_0 R(v_1, v_0) \to \forall v_0 R(v_0, a)) = FV(\forall v_0 R(v_0, v_1)) = \{v_1\}$.
Note that $FV(\forall v_0 R(v_1, v_2)) = \{v_1, v_2\}$.

If φ is a formula and $v_k \in FV(\varphi)$ then we think of φ as saying something about v_k– whichever element that is, for example if φ is $\neg(\forall v_1 v_1 = v_k)$. This says "there is something besides v_k". This clearly would have the same effect as saying 'there is something besides v_k' *as long as* $k \neq 1$ since we shall obviously want $\neg(\forall v_1 v_1 = v_1)$ to be interpreted as something that is always false. We want in general given a formula φ id about v_k. The above example shows that it is not always safe to simply substitute a t such as v_1 for v_k: the point being that the term t has a free variable in it when r equals v_1 itself, namely v_1, that is 'captured' by the quantifier $\forall v_1$. The following definition says precisely when a term may safely be substituted for a variable in a formula.

Definition 3.10 *t is* substitutable *for v_k in φ if*

φ is atomic
or: φ is $(\neg\psi)$ and t is substitutable for v_k in ψ
or: φ is $(\psi \to \chi)$ and t is substitutable for v_k in ψ and χ
or: φ is $\forall v_n \psi$ where t is substitutable for v_k in ψ and
(if $v_n \in FV(t)$ then $v_k \notin FV(\varphi)$).

Remark Again a definition by recursion on the complexity of φ. Some author write 'free' rather than 'substitutable'. Notice a couple of consequences of this definition. If a term is not substitutable for a variable in a formula χ, it won't be be substitutable in any other formula in which χ is a part; on the other hand a term may be substitutable in χ but may not be substitutable in a formula in which χ is a part; secondly, we allow ourselves to say t is substitutable for v_k in φ whenever v_k appears nowhere in φ; the intention of the definition is that it tells us when a term may safely be substituted for a variable, which we shall *usually* be thinking of as a free variable. However the definition also specifies some "defaults" when v_k appears but is not free. This leads to some peculiarities when v_k is not free: just because a variable is not free in a formula does not mean in general that a term is substitutable for it in that formula (see Example 19(ii) and (vii) below.). But there are no oddities when v_k is free and the definition functions perfectly.

Example 19 To check substitutability one can use the recursive clauses of Definition 18 with a little practice one can "read off" from the formula when variables are free, and what is substitutable for what, and you are advised to try the exercises below to develop this skill.

(i) v_0 is substitutable for v_0, v_1, and v_2 in $R(v_0, v_1)$ and likewise in $R(F(v_0, v_1), v_1)$

(ii) v_0 and v_2 are both substitutable for v_0 in $\forall v_1 R(v_1, v_0)$. However v_1, although not substitutable for v_0 (see also next item) is declared by default, but somewhat trivially, substitutable for v_1.

(iii) v_1 is not substitutable for v_0 in $\forall v_1 R(v_0, v_1)$ nor is any term t such as $F(v_1)$ in which v_1 is a free variable: looking at the last clause of Def 3.10, although v_1 and such t are substitutable for v_0 in $R(v_0, v_1)$ both $v_1 \in FV(v_1)$ (or more generally $v_1 \in FV(t)$), and $v_0 \in FV(\forall v_1 R(v_0, v_1))$.

(iv) Since v_1 is not substitutable for v_0 in $\forall v_1 R(v_0, v_1)$ it will not be in $\forall v_0 \forall v_1 R(v_0, v_1)$ either; nor will it be in $\forall v_1 \forall v_0 R(v_0, v_1)$ either; nor will it be in $\forall v_1 R(v_0, v_1) \to S(v_0, v_1)$

(v) any constant symbol is substitutable for any variable in any formula

(vi) $G(v_0, a, v_1)$ is substitutable for v_1 and v_2 in $\forall v_1 R(v_0, v_1)$ but not for v_0 since $v_1 \in FV(G(v_0, a, v_1))$ (and $v_0 \in FV(\forall v_1 R(v_0, v_1))$); but it is substitutable for v_1 in $\forall v_3 R(v_3, v_1)$.

(vii) $F(v_2, v_1)$ is not substitutable for v_1 in $\forall v_1 \forall v_2 R(v_2, v_1)$ [notwithstanding that $v_1 \notin FV(\forall v_1 \forall v_2 R(v_2, v_1))$] since it is not substitutable in $\forall v_2 R(v_2, v_1)$.

The intention is that we only want to substitute terms for free variables for which they are substitutable according to the above definition. It's probably fairly clear what this means given any one formula but we can give a precise inductive definition of what the result of performing the substitution of t for v_k in φ is.

Definition 3.11 *For x a formula or a term, $Sub(t, v_k, x)$* ["the result of substituting t for v_k in x"] *is defined by induction on complexity of terms and formulae as follows:*

(i) $Sub(t, v_k, v_n)$ *is* $\begin{cases} t & \text{if } k = n \\ v_n & \text{if } k \neq n \end{cases}$

(ii) $Sub(t, v_k, R(t_1, \ldots, t_n))$ *is* $R(Sub(t, v_k, t_1), \ldots, Sub(t, v_k, t_n))$ $\quad (R \in dom\mathbf{r})$
$Sub(t, v_k, F(t_1, \ldots, t_n))$ *is* $F(Sub(t, v_k, t_1), \ldots, Sub(t, v_k, t_n))$ $\quad (F \in dom\mathbf{f})$

(iii) $Sub(t, v_k, t_1 = t_2)$ *is* $Sub(t, v_k, t_1) = Sub(t, v_k, t_2)$

(iv) $Sub(t, v_k, (\neg\chi))$ *is* $(\neg Sub(t, v_k, \chi))$

(v) $Sub(t, v_k, (\psi \to \chi))$ *is* $(Sub(t, v_k, \psi) \to Sub(t, v_k, \chi))$

(vi) $Sub(t, v_k, \forall v_n, \forall v_n \psi)$ *is* $\begin{cases} \forall v_n \psi & \text{if } k = n \\ \forall v_n \mathrm{Sub}(t, v_k, \psi) & \text{if } k \neq n \end{cases}$

Note: The above definition is made without prejudice as to whether t *actually* is substitutable for v_k in φ (see Example 20(vi) below). But an induction on the complexity of x shows that if $v_k \notin FV(x)$ (even if v_k occurs in x), then $\mathrm{Sub}(t, v_k, x) = x$ (and see Exercise 10). But if t is substitutable for v_k in φ, and $v_k \in FV(\varphi)$, then $\mathrm{Sub}(t, v_k, \varphi)$ does "the right thing" and returns the formula with the correct substitution made without any clash of variables with quantifiers.

Example 20

(i) $\mathrm{Sub}(v_n, v_k, v_k) = v_n$; Now consider $\mathrm{Sub}(F(v_0, v_1), v_2, \varphi)$ for various φ:

(ii) φ is $R(v_1, v_2)$: $\mathrm{Sub}(F(v_0, v_1), v_2, \varphi) = R(\mathrm{Sub}(F(v_0, v_1), v_2, v_0), \mathrm{Sub}(F(v_0, v_1), v_2, v_1))$
$= R(v_0, F(v_0, v_1))$

(iii) φ is $R(v_0, v_2) \to S(v_0)$: $\mathrm{Sub}(F(v_0, v_1), v_2, \varphi) =$
$= \mathrm{Sub}(F(v_0, v_1), v_2, R(v_0, v_2)) \to \mathrm{Sub}(F(v_0, v_1), v_2, S(v_0)) = R(v_0, F(v_0, v_1)) \to S(v_0)$

(iv) φ is $\forall v_3 R(v_3, v_2)$: $\mathrm{Sub}(F(v_0, v_1), v_2, \varphi) = \forall v_3 R(v_3, F(v_0, v_1))$

(v) φ is $\forall v_2 R(v_0, v_2)$: $\mathrm{Sub}(F(v_0, v_1), v_2, \varphi) = \varphi$

(vi) φ is $\forall v_1 R(v_1, v_2)$: $\mathrm{Sub}(F(v_0, v_1), v_2, \varphi) = \forall v_1 R(v_1, F(v_0, v_1))$

Remark Again, the procedure of taking a formula and a term, and checking whether the term is substitutable for a particular occurrence of a variable and performing the substitutions are all effective procedures when considering their code numbers: we could feasibly write a programme which when fed in a gn checked it was the gn of a formula and gave as output (in the form of a gn the result of the suitable substitution.
As a shorthand for the Sub notation we write $x(t/v_k)$ instead of $\mathrm{Sub}(t, v_k, x)$ (x *a* t or φ).
One or more substitutions can be handled by writing $x(t_0/v_0, \ldots, t_n/v_n)$ for the result of successively substituting t_0 for $v_0, \ldots, t_n$ for v_n; so for example $v_k(v_1/v_n)$ is v_1 if $n = k$ and is v_k otherwise; $G(v_0, v_2)(F(v_1)/v_0) = G(F(v_1), v_2)$.

Exercise 5 For those of the following that are terms, calculate their complexity (a and b are constant symbols)

$$G(v_0, v_0, G(v_0, v_0, v_0)) \quad F(a, b) \quad F(S(a), b) \quad v_2 \quad G(F(b, F(G(a, v_1, v_2),)), b, t)$$

where t is a term with $\mathrm{comp}(t) = 4$.
Exercise 6 In the following φ, ψ, χ have complexity 5, 7, 2; putting brackets back where necessary, calculate the complexities of some or all of the following formulae: $\neg\neg\varphi \wedge \psi$; $\forall v_0 \varphi \to (\psi \wedge \chi)$; $(\exists v_0 \neg\varphi \wedge \psi) \to \chi$; $(\neg\varphi \vee \exists v_0 \psi) \to \chi$; $(\neg\exists v_0 \forall v_1 P(v_0, v_1) \to \exists v_0 \neg\forall v_1 R(v_0, v_1) \wedge (\exists v_0 \neg\forall v_1 R(v_0, v_1) \to \neg\exists v_0 \forall v_1 P(v_0, v_1)))$.
Exercise 7 Let $\mathbb{N} = \langle \mathbb{N}, +_{\mathbb{N}}, \times_{\mathbb{N}}, 0_{\mathbb{N}}, 1_{\mathbb{N}} \rangle$. Translate the following formulae into words and determine whether they are true or false in $\mathbb{N}$

a) $\forall v_1 \exists v_0 (v_0 = +(v_1, v_1) \vee v_0 = +(+(v_1, v_1), 1)))$

b) $\forall v_0 \forall v_1 (\times(v_0, v_1) = 0 \to v_0 = 0 \ \vee \ v_1 = 0)$

c) $\exists v_1 (\times(v_1, v_1) = 1)$

Exercise 8 Find out $FV(\varphi)$ for φ in the following cases

(i) $\forall v_0 R(v_1, v_0) \to R(v_0, v_1)$ (ii) $\forall v_0 P(v_0) \to \forall v_1 R(v_0, v_1)$
(iii) $P(v_2) \to \neg\forall v_1 \forall v_2 Q(v_1, v_2, v_1)$ (iv) $\forall v_2 R(F(v_1, v_2), v_1) \to \forall v_1 S(v_3, G(v_1, v_2))$

Exercise 9

(i) For which occurrences of v_1 in the formulae of Exercise 8, is $F(v_0, v_1)$ substitutable? Perform the suitable substitutions.

(ii) Consider the formulae

a) $\forall v_0 \forall v_2 (P(v_2) \to P(v_0))$ b) $\forall v_1 Q(v_0, F(v_0), v_1) \to \forall v_2 P(G(v_0, v_2))$
c) $\forall v_1 P(F(v_1)) \to \forall v_2 Q(v_0, v_1, v_2)$

Form $\mathrm{Sub}(G(v_0, v_2), v_0, \varphi)$ for each of the formulae above. For which φ is $G(v_0, v_2)$ substitutable for v_0?
Exercise 10 If x is a term or a formula prove that if $v_k \notin FV(x)$ then for any term t, $\mathrm{Sub}(t, v_k, x) = x$.

3.4 The Definition of Truth

We have defined languages L_Ω and several syntactical operations on formulae and terms for the languages. In doing so we've alluded to the intention behind these purely syntactical L_Ω: it is a language suitable for describing features in structures of a particular type or signature. We use *valuations* to connect formulae of a language L_Ω to a structure of type Ω: a valuation is simply a function that maps variables to elements of the domain A.

Definition 3.12 (valuations) $W^A = \{w \mid w \text{ is a function } w : \mathbb{N} \longrightarrow A\}$.

We use $w \in W^A$ to get such a mapping by declaring that v_k is mapped to $w(k)$. We extend such valuations to all the terms of the language;

Definition 3.13 (extended valuations) $w^*_A(v_k) = w(k)$;
$w^*_A(v_k) = F_{\mathbf{A}}(w^*_{\mathbf{A}}(t_1), \ldots, w^*_{\mathbf{A}}t_k))$ *if* F *is* k*-ary, and* $t_1, \ldots, t_k$ *are terms for which* w^*_A *has been defined.*

If the $\mathbf{A}$ is given or understood, then we drop the subscript and simply write w^* of u^* etc. The following definition is just a piece of notation:

Definition 3.14 *Let* $w \in W^{\mathbf{A}}$*, and let* $a \in A$*. Then* $w(a/i) \in W^{\mathbf{A}}$ *is defined by*

$$w(a/i)(j) = w(j) \qquad \text{if } j \neq i$$
$$w(a/i)(i) = a \qquad \text{if } j = i$$

Thus $w(a/i)$ *is a valuation that assigns* a *to* v_i *irrespective of what* w *did, but leaves all other values of* w *unaltered; it thus differs from* w *only at the "*i*'th place".*

Example based on above
The following is the central definition of this section, which shows that we can give a precise definition to truth in a structure.

Definition 3.15 (The Satisfaction Relation) *Let* $\boldsymbol{A}$ *be an* Ω*-structure and* φ *a formula of* L_Ω*. If* w *is a valuation in* $\boldsymbol{A}$ *we define* w *satisfies* φ *in* $\boldsymbol{A}$ (and write $\mathbf{A} \vDash \varphi[w]$) by recursion on complexity of φ

$$\begin{array}{ll}
\boldsymbol{A} \vDash s = t[w] & \textit{iff } w^*_{\mathbf{A}}(s) = w^*_{\mathbf{A}}(t) \\
\boldsymbol{A} \vDash R(t_1, \ldots, t_n)[w] & \textit{iff } \langle w^*_{\mathbf{A}}(t_1), \ldots, w^*_{\mathbf{A}}(t_n)\rangle \in R_{\mathbf{A}} \textit{ for } R \in \text{dom } \boldsymbol{r} \textit{ with} \\
 & \quad \boldsymbol{r}(R) = n, \textit{ and } t_1, \ldots, t_n \textit{ terms of } L_\Omega. \\
\boldsymbol{A} \vDash (\neg\psi)[w] & \textit{iff it's not the case that } \boldsymbol{A} \vDash \psi[w] \\
\boldsymbol{A} \vDash (\psi \to \chi)[w] & \textit{iff whenever } \boldsymbol{A} \vDash \psi[w] \textit{ then } \boldsymbol{A} \vDash \chi[w] \\
\boldsymbol{A} \vDash \forall v_k \varphi[w] & \textit{iff for any } a \in A,\ \boldsymbol{A} \vDash \varphi[w(a/k)]
\end{array}$$

Remark The last clause shows that we're intending this as a simultaneous definition for all valuations w.
The next example shows how the mechanics of this definition works.
Example 21 Let $\mathbb{N} = \langle \mathbb{N}, +_{\mathbb{N}}, \times_{\mathbb{N}}, 0_{\mathbb{N}}, '_{\mathbb{N}} \rangle$, let $w \in W^{\mathbb{N}}$ have the property that $w(0) = 23,\ w(1) = 106$.

a) Let φ be $v_0 + v_1 = 0''$. Then it is not the case that $\mathbb{N} \vDash v_0 + v_1 = 0''[w]$ since $w^*(0'') = 2$, but $w^*(v_0 + v_1) = w^*(v_0) +_{\mathbb{N}} w^*(v_1) = 23 +_{\mathbb{N}} 106 = 129 \neq 2$.

b) Let φ be $\forall v_0\ v_0 + v_1 = v_1 + v_0$. Then $\mathbb{N} \vDash \varphi[w]$ since this holds iff

$$\forall k \in \mathbb{N}(\mathbb{N} \vDash v_0 + v_1 = v_1 + v_0[w(k/0)]) \text{ iff } \forall k \in \mathbb{N}(w(k/0)^*(v_0 + v_1) = w(k/0)^*(v_1 + v_0))$$

$$\text{iff } \forall k \in \mathbb{N}\ (k +_{\mathbb{N}} 106 = 106 +_{\mathbb{N}} k).$$

c) Let φ be $\forall v_1 \forall v_0\ v_0 + v_1 = v_1 + v_0$, now φ has no free variables. $\mathbb{N} \vDash \varphi[w]$ iff for all $k \in \mathbb{N}$ $\mathbb{N} \vDash \forall v_0\ v_0 + v_1 = v_1 + v_0[w(k/1)]$ iff for all $k,\ l \in \mathbb{N}$ $\mathbb{N} \vDash v_0 + v_1 = v_1 + v_0[w(k/1, 1/0)]$ iff for all $k, l \in \mathbb{N}$ $w(k/1, 1/0)^*(v_0 + v_1) = w(k/1, 1/0)^*(v_1 + v_0)$. Notice that here what the values of the original w were is irrelevant, we have that for this φ $\mathbb{N} \vDash \varphi[w]$ for any valuation $w \in W^{\mathbb{N}}$. This observation leads us to the following piece of shorthand: If $FV(\varphi) = \varnothing$ (so φ is a sentence) we simply write

$$\mathbf{A} \vDash \varphi \Longleftrightarrow \text{for any } w \in W^{\mathbf{A}}\ \mathbf{A} \vDash \varphi[w].$$

For Γ a set of sentences we write $\mathbf{A} \vDash \Gamma$ iff for all $\varphi \in \Gamma$ $\mathbf{A} \vDash \varphi$.
Some facts are readily seen about the satisfaction relation:

(i) $\mathbf{A} \vDash \neg\varphi[w]R$ iff not $(\mathbf{A} \vDash \varphi[w])$ (written $\mathbf{A} \nvDash \varphi[w]$)

(ii) Not both $\mathbf{A} \vDash \varphi[w]$ and $\mathbf{A} \vDash \neg\varphi[w]$

(iii) If $\mathbf{A} \vDash \varphi[w]$ and $\mathbf{A} \vDash (\varphi \to \psi)[w]$ then $\mathbf{A} \vDash \psi[w]$.

The same considerations as above immediately give the following

Lemma 3.16

a)	$\boldsymbol{A} \vDash (\varphi \wedge \psi)[w]$	*iff* $\boldsymbol{A} \vDash \varphi[w]$ *and* $\boldsymbol{A} \vDash \psi[w]$
b)	$\boldsymbol{A} \vDash (\varphi \vee \psi)[w]$	*iff* $\boldsymbol{A} \vDash \varphi[w]$ *or* $\boldsymbol{A} \vDash \psi[w]$
c)	$\boldsymbol{A} \vDash (\varphi \leftrightarrow \psi)[w]$	*iff* $\boldsymbol{A} \vDash \varphi[w]$ *if and only if* $\boldsymbol{A} \vDash \psi[w]$
d)	$\boldsymbol{A} \vDash \exists v_k \varphi[w]$	*iff for some* $a \in A$ $\boldsymbol{A} \vDash \varphi[w(a/k)]$

Proof The lemma is just a rewriting of the definition of $\vDash$ for these abbreviations. QED

The next observations says that essentially the truth of a formula in a structure, or the denotation of a term *only* depends on the interpretation of the free variables: everything else is irrelevant.) In Example 21, the interpretation of the term $v_0'' \times 0'$ should only depend on what a valuation assigns to v_0 and nothing else; likewise whether the formula $v_0 + v_1 = v_1 + v_1$ ends up being satisfied should only depend on what the valuation assigns to v_0 and v_1 and nothing else. The mathematical nature of our definitions, in particular that of the satisfaction relation allows us to actually *prove* that this is the case, and that is the content of part a) of the next lemma. Further although $0'' + v_1$ and $v_1 + (0' + 0')$ are different terms under any valuation they will both get interpreted as the same natural number; if I now substitute each of them separately for the variable v_0 in the term $v_0 \times v_0$ (to get $(0'' + v_1) \times (0'' + v_1)$ and $(v_1 + (0' + 0')) \times (v_1 + (0' + 0'))$ respectively) then if my definitions are sound and I now interprete these two terms I ought to get the same final interpretation; part b) below assures this. And lastly if I substitute these in for the variable v_2

in any formula (note both these terms *are* substitutable for v_2 in any formula) then the truth or falsity of the resulting formulae are the same; this is what part c) says. So:

Remark b) and c) together show that w^* as defined in Definition 3.13 does the right things: substituting different terms that w^* evaluates as the same object in A doesn't affect the valuation of terms or evaluation of formulae in which we substitute those terms.

Lemma 3.17 *Let $\mathbf{A}$ be a Ω-structure, t a term and φ a formula of L_Ω*

a) If $w, u \in W^{\mathbf{A}}$ and $w(i) = u(i)$ whenever $v_i \in FV(t)$ then $w^*(t) = u^*(t)$. Similarly with φ in place of t, $\mathbf{A} \vDash \varphi[w] \iff \mathbf{A} \vDash \varphi[u]$.

b) Suppose also s_0, s_1 are terms of L_Ω such that $w^*(s_0) = w^*(s_1)$. Then $w^*(t(s_0/v_k)) = w^*(t(s_1/v_k))$.

c) If in addition s_0, s_1 are substitutable for v_k in φ then $\mathbf{A} \vDash \varphi(s_0/v_k)[w]$ iff $\mathbf{A} \vDash \varphi(s_1/v_k)[w]$.

Proof

a) By induction on the complexity of t or φ. We let the reader do t as an exercise, assuming the results for terms we do φ.

$\mathbf{A} \vDash s = t[w]$ iff $w^*(s) = w^*(t)$ iff $u^*(s) = u^*(t)$ iff $\mathbf{A} \vDash s = t[u]$

$\mathbf{A} \vDash R(t_1, \ldots, t_n)[w]$ iff $\langle w^*(t_1), \ldots, w^*(t_n)\rangle \in R_{\mathbf{A}}$
iff $\langle u^*(t_1), \ldots, u^*(t_n)\rangle \in R_{\mathbf{A}}$
iff $\mathbf{A} \vDash R(t_1, \ldots, t_n)[u]$.

$\mathbf{A} \vDash (\neg\varphi)[w]$ iff it's not the case that $\mathbf{A} \vDash \varphi[w]$
iff (by the inductive hypothesis) it's not the case that $\mathbf{A} \vDash \varphi[u]$
iff $\mathbf{A} \vDash (\neg\varphi)[u]$.

$\mathbf{A} \vDash (\varphi \to \chi)[w]$: Similar.

$\mathbf{A} \vDash \forall v_k \varphi[w]$ iff for any $a \in A$ $\mathbf{A} \vDash \varphi[w(a/k)]$.

Now $u(j) = w(j)$ for any $v_j \in FV(\varphi)$. So, by inductive hypothesis, the line above holds iff for any $a \in A$:

$$\mathbf{A} \vDash \varphi[u(a/k)] \; iff \; \mathbf{A} \vDash \forall v_k \varphi[u]$$

b) If t is v_k then $w^*(t(s_0/v_k)) = w^*(s_0) = w^*(s_1) = w^*(t(s_1/v_k))$
If t is v_i $(i \neq k)$ then $w^*(t(s_0/v_k)) = w^*(t) = w^*(t(s_1/v_k))$
If t is $F(t_1, \ldots, t_n)$ then

$$\begin{aligned} w^*(t(s_0/v_k)) &= F_{\mathbf{A}}(w^*(t_1(s_0/v_k)), \ldots, w^*(t_n(s_0/v_k))) \\ &= F_{\mathbf{A}}(w^*(t_1(s_1/v_k)), \ldots, w^*(t_n(s_1/v_k))) \quad \text{(by inductive hypothesis)} \\ &= w^*(t(s_1/v_k)). \end{aligned}$$

c) Again induction on complexity of φ using b):

$\mathbf{A} \vDash t_0 = t_1(s_0/v_k)[w]$ iff $\mathbf{A} \vDash t_0(s_0/v_k) = t_1(s_0/v_k)[w]$
iff $w^*(t_0)(s_0/v_k)) = w^*(t_1)(s_0/v_k)$
iff $w^*(t_0(s_1/v_k)) = w^*(t_1(s_1/v_k))$ by b)
iff $\mathbf{A} \vDash t_0(s_1/v_k) = t_1(s_1/v_k)[w]$
iff $\mathbf{A} \vDash t_0 = t_1(s_1/v_k)[w]$.

If φ is $R(t_1, \ldots, t_n)$, $\psi \to \chi$, or $\neg\psi$. Similar.

If φ is $\forall v_k \psi$ then $\mathbf{A} \vDash \varphi(s_0/v_k)[w]$ iff $\mathbf{A} \vDash \varphi(s_1/v_k)[w]$ since $\varphi(s_0/v_k)$ is φ.

If φ is $\forall v_j \psi$ $(j \neq k)$ then $\mathbf{A} \vDash \forall v_j(\psi(s_0/v_k))[w]$ iff for all $a \in A$, $\mathbf{A} \vDash \psi(s_0/v_k)[w(a/j)]$
Now by assumption s_0, s_1 are substitutable for v_k in φ. This means either
(i) $v_k \notin FV(\psi)$ or (ii) $v_j \notin FV(s_0) \cup FV(s_1)$
If (i) holds: $\mathbf{A} \vDash \psi(s_0/v_k)[w(a/j)]$ iff $\mathbf{A} \vDash \psi[w(a/j)]$
iff $\mathbf{A} \vDash \psi(s_1/v_k)[w(a/j)]$
since $\psi(s_0/v_k)$ is just ψ.
If (ii) holds: $w(a/j)^*(s_0) = w^*(s_0) = w^*(s_1) = w(a/j)^*(s_1)$ by part a). Now $\psi(s_0/v_k)$ has complexity less than that of $\forall v_j \varphi$ so our inductive hypothesis holds, so

$$\text{for all } a \in A \quad \mathbf{A} \vDash \psi(s_0/v_k)[w(a/j)]$$

iff for all $a \in A$ $\mathbf{A} \vDash \psi(s_1/v_k)[w(a/j)]$ iff $\mathbf{A} \vDash \forall v_j \psi(s_1/v_k)[w]$ as required. QED

Definition 3.18 *a) If φ is an L_Ω formula, then φ is* universally valid *iff for all Ω-structures $\mathbf{A}$ and valuations $w \in W^{\mathbf{A}}$ $\mathbf{A} \vDash \varphi[w]$*

b) If φ is an L_Ω sentence, $\mathbf{A}$ an Ω- structure, then $\mathbf{A}$ is a model of φ *iff $\mathbf{A} \vDash \varphi$. If Γ is a set of sentences and $\mathbf{A} \vDash \Gamma$, we say $\mathbf{A}$ is* a model of Γ.

c) If φ is an L_Ω is satisfiable *if there is an Ω- structure $\mathbf{A}$ and $w \in W^{\mathbf{A}}$ so that $\mathbf{A} \vDash \varphi[w]$. Otherwise it's* unsatisfiable.

d) If Γ is a set of L_Ω formulae, we say Γ is satisfiable *if there's an Ω-structure $\mathbf{A}$ and $w \in W^{\mathbf{A}}$ so that $\mathbf{A} \vDash \varphi[w]$ for all $\varphi \in \Gamma$. Otherwise it's* unsatisfiable.

We may also use the symbol $\vDash$ in exactly the same way that we did as a relation between sets of formulae of some L_Ω.

Definition 3.19 *Let $\Gamma \cup \{\varphi\}$ be a set of formulae in L_Ω. Then $\Gamma \vDash \varphi$ means that for every Ω- structure, every valuation in that structure that satisfies Γ must satisfy φ.*

We may now express some of Definition 16 in this notation: φ is universally valid now becomes simply $\varnothing \vDash \varphi$ (which we write as $\vDash \varphi$) because every formula in $\varnothing$ is true in every Ω-structure (vacuously). For not $(\Gamma \vDash \varphi)$ we write $\Gamma \nvDash \varphi$. Again we write $\Gamma, \psi \vDash \varphi$ rather than $\Gamma \cup \{\psi\} \vDash \varphi$. We allow here the possibility that Γ is infinite.

Lemma 3.20 *Let $\Gamma, \Delta, \{\phi, \psi, \chi\}$ be sets of formulae in L_Ω, then all the entailments of Lemma 1.1 hold for L_Ω.*

Lemma 3.21 *Let t be a term, and φ, ψ formulae of L_Ω. Then*

(i) $\forall v_i \varphi \to \varphi(t/v_i)$ is universally valid, if t is substitutable for v_i in φ

(ii) $\forall v_i(\varphi \to \psi) \to (\varphi \to \forall v_i \psi)$ is universally valid if $v_i \notin FV(\varphi)$.

Before proving the lemma let us see why the restrictions are necessary.
For (i) simply let φ be $\neg\forall v_j v_i = v_j$ and let t be v_j; then t is not substitutable for v_i in φ. Now

$$(\forall v_i(\neg\forall v_j v_i = v_j) \to (\neg\forall v_j v_j = v_j))$$

is then false in any Ω-structure $\mathbf{A}$ as long as A has at least two elements.
For (ii) suppose P is a unary relation symbol of the language; take both φ and ψ as $P(v_i)$. Then $v_i \in FV(\varphi)$ and (ii) now reads

$$\forall v_i(P(v_i) \to P(v_i)) \to (P(v_i) \to \forall v_i P(v_i))$$

The antecedent of this is clearly universally valid, but the consequent isn't: let $\mathbf{A} = \langle \mathbb{N}, P_{\mathbf{A}} \rangle$ where $P_{\mathbf{A}}$ is the set of even natural numbers. If $w \in W^{\mathbf{A}}$ has $w(i) = 2$ say then $A \not\models P(v_i) \to \forall v_i P(v_i)[w]$.

Proof of Lemma 3.21

(i) Let $\mathbf{A}$ be an arbitrary Ω-structure and w an arbitrary valuation in $W^{\mathbf{A}}$. To show $\mathbf{A} \models \forall v_i \varphi \to \varphi(t/v_i)[w]$ it's enough to show $\mathbf{A} \models \forall v_i \varphi[w]$ implies $\mathbf{A} \models \varphi(t/v_i)[w]$. So suppose the former. We have to be slightly careful since we may have $v_i \in FV(t)$. Let v_k be a variable that occurs nowhere in φ or t. Let $a = w^*(t)$. By assumption

$\mathbf{A} \models \varphi[w(a/i)]$ — But this holds

$\iff \mathbf{A} \models \varphi[w(a/i, a/k)]$ — (by Lemma 3.17 a) as $k \notin FV(\varphi)$) with s_0 as v_i, s_1 as v_k, but

$\iff \mathbf{A} \models \varphi(v_k/v_i)[w(a/i, a/k)]$ — (by 3.17 c)
substituting in here for v_i in φ. Note that v_i is substitutable for v_i in any formula, and v_k is substitutable for v_i here because v_k occurs nowhere in φ, see Exercise 10)

$\iff \mathbf{A} \models \varphi(v_k/v_i)[w(a/k)]$ — (by 3.17 a) again as now $v_i \notin FV(\varphi(v_k/v_i))$

$\iff \mathbf{A} \models \varphi(i/v_i)[w(a/k)]$ — (by 3.17 c) with s_0 as v_k, s_1 as t
since $w^*(a/k)(v_k) = a = w^*(a/k)(t)$ by 3a))

$\iff \mathbf{A} \models \varphi(t/v_i)[w]$ — (again by 3a))

which was what we were after.

(ii) Again let $\mathbf{A}$ and w be arbitrary and suppose $\mathbf{A} \models \forall v_i(\varphi \to \psi)[w]$ then for any $a \in A$ we have $\mathbf{A} \models \varphi \to \psi[w(a/i)]$. The latter holds *iff* $\mathbf{A} \models \varphi[w(a/i)]$ implies $A \models \psi[w(a/i)]$. But $v_i \notin FV(\varphi)$, so by Lemma 3a) *either* for any $a \in A$ whatsoever $\mathbf{A} \models \varphi[w(a/i)]$ *or*, in particular, it's not the case that $\mathbf{A} \models [w]$. If the first possibility holds, then by the above for any $a \in A$ $\mathbf{A} \models \psi[w(a/i)]$; that is $\mathbf{A} \models \forall v_i \psi[w]$ and we conclude $\mathbf{A} \models \varphi \to \forall v_i \psi[w]$;

The second case is then trivial, we have $\mathbf{A} \models \varphi \to \forall v_i \psi[w]$ since $\mathbf{A} \models \neg\varphi[w]$. QED

In general we should like to know how to determine whether a formula φ is universally valid or not.

Definition 3.22 *Let φ be a formula in a first order language L_Ω is an* instance *of ψ if ψ is a formula of a propositional language L_Ω and ψ contains the propositional variables $P_1, \ldots, P_N$, and there are formulae $\varphi_1, \ldots, \varphi_n$ of L_Ω such that φ is the result of substituting φ_i for each occurence of P_i in φ for $1 \leq i \leq n$.*

Example 22

(i) $\forall v_0\varphi \to (\exists v_1\varphi \to \forall v_0\varphi)$ is an instance of the tautology $P_1 \to (P_2 \to P_1)$

(ii) $(\forall v_0\forall v_1\varphi \wedge \exists v_2\forall v_3\varphi) \to (\forall v_0\forall v_1\varphi \vee \exists v_2\chi)$ is an instance of the tautology $(P \wedge Q) \to (P \vee R)$

(iii) $\forall v_0\varphi$ can never be an instance of a tautology (although φ itself may be). Nor can an atomic formula of L_Ω be an instance of a tautology.

The relevance of tautology instances in first order languages is the following.

Lemma 3.23 *Every instance of a tautology is universally valid.*

Proof Let φ be an instance of φ' in L_ω, where φ arises from φ' by substituting $\varphi_1, \ldots, \varphi_n$ in L_Ω for $P_1, \ldots, P_n$- The propositional variables occuring in φ'. Let $\mathbf{A}$ be an interpretation of L_Ω, let $w \in W^{\mathbf{A}}$. Define a valuation of $L_{\{P_1,\ldots,P_n\}}$ by

$$\begin{aligned} w_0(P_i) &= T \text{ if } \mathbf{A} \vDash \varphi_i[w] \\ &= F \text{ if not } \mathbf{A} \vDash \varphi_i[w] \end{aligned}$$

Claim $\mathbf{A} \vDash \varphi[w] \iff w_0^*(\varphi') = T$
Proof By induction on complexity of φ'.
φ' *is* P_k then $w_0^*(P_k) = T \iff \mathbf{A} \vDash \varphi[w]$
φ' *is* $\neg\psi'$ (and so φ is $\neg\psi$ for some ψ)

$$\begin{aligned} \mathbf{A} \vDash \varphi[w] &\iff \text{not } \mathbf{A} \vDash \phi[w] \\ &\iff w_0^*(\psi') = F \qquad \text{(by Induction hypothesis)} \\ &\iff w_0^*(\phi') = T \end{aligned}$$

φ' *is* $\psi' \to \chi'$ (and so φ is $\psi \to \chi$ some ψ, χ)

$$\begin{aligned} \mathbf{A} \vDash \iff \varphi[w] &\iff \text{whenever } \mathbf{A} \vDash \psi[w] \text{ then } \mathbf{A} \vDash \chi[w] \\ &\iff \text{whenever } w_0^*(\psi') = T \text{ then } w_0^*(\chi') = T \quad \text{(by the inductive hypothesis)} \\ &\iff w_0^*(\varphi') = T \end{aligned}$$

This completes the proof of the claim. Now if our original φ was an instance of a tautology φ', but $\mathbf{A}$ were an interpretation of L_Ω, $W \in W^{\mathbf{A}}$, so that $\mathbf{A} \vDash \neg\varphi[w]$ then we should have according to the construction above $w_0^*(\varphi') = F$. But φ' is a tautology. A contradiction and so φ must be universally valid. QED

If the only universally valid formulae were instances of tautologies life would be simple: we've already remarked that testing a formula of L_ω for "tautologyhood" is an effective procedure; we could then generate

all universally valid formulae, by generating all the formulae of L_ω where ω has variables $P_1, P_2, \ldots, P_n, \ldots$ ($n \in \mathbb{N}$), testing each in turn for tautologousness, and then substituting in each tautology all the possible substitutions of formulae in L_Ω for the relevant P_i. An infinite process of course, but one for which a programme could be written. Unfortunately, this isn't the case.

Example 23 The formulae of Lemma 3.21(i) and (ii) are universally valid but are not instances of tautologies. e.g. $\forall v_i \varphi \to \varphi(t/v_i)$ can only be thought of as an instance of $P_1 \to P_2$ which isn't a tautology.

Definition 3.24 *Let $\Omega \subseteq \Omega'$, that is, if Ω is $\langle \boldsymbol{r}', \boldsymbol{f} \rangle$, $\Omega' = \langle \boldsymbol{r}', \boldsymbol{f}' \rangle$ then* $\mathrm{dom}\, r \subseteq \mathrm{dom}\, r', \mathrm{dom}\, f \subseteq \mathrm{dom}\boldsymbol{f}'$, *and for all $R \in \mathrm{dom}\, \boldsymbol{r}$, $F \in \mathrm{dom}\boldsymbol{f}$ $\boldsymbol{r}(R) = r'(R)$ $f(F) = \boldsymbol{f}'(F)$. If $\boldsymbol{A}$ is an Ω'-structure, the* reduct *of $\boldsymbol{A}$ to Ω, $\boldsymbol{A}|\Omega$, is the structure obtained by discarding the relations R_A and functions F_A that are in $dom\boldsymbol{r}'$ - $tmopdom\boldsymbol{r}$* and $\mathrm{dom}\boldsymbol{f}'$ - $\mathrm{dom}\boldsymbol{f}$.

Note that A stays the same, i.e. $\mathbf{A}$ and $\mathbf{A}|\Omega$ have the same domains. Example 1 is a reduct of Example 2.
Example 24 Let $\mathbb{N} = \langle \mathbb{N}, +_{\mathbb{N}}, \cdot_{\mathbb{N}}, {}'_{\mathbb{N}}, 0_{\mathbb{N}} \rangle$. Then $\mathbb{N}^-$ is a reduct of $\mathbb{N}$ where $\mathbb{N}^- = \langle \mathbb{N}, +_{\mathbb{N}}, \cdot_{\mathbb{N}}, {}'_{\mathbb{N}} \rangle$

Lemma 3.25 *Let $\Omega \subseteq \Omega'$ and let $\boldsymbol{A}$ be on Ω'-structure, t a term of L_Ω and $w \in W^A$. Then $w^*_{\mathbf{A}}(t) = w^*_{A|\Omega}(t)$. Similarly if φ if a formula of L_Ω, $\boldsymbol{A} \vDash \varphi[w] \iff \boldsymbol{A}|\Omega \vDash \varphi[w]$.*

Proof By induction on complexity of t or φ. The intuitive idea is simply that the valuation of a term doesn't depend on function symbols not mentioned in it. Nor is the truth of a formula affected by relation symbols not in it.

Definition 3.26 *a)* If A is an Ω-structure then the *theory* of $\mathbf{A}$, $Th(\mathbf{A})$ is the set

$$\{\varphi \in L_\Omega \mid \boldsymbol{A} \vDash \varphi,\ \varphi \text{ a sentence}\}$$

b) If $\mathbf{A}, \mathbf{B}$ are Ω-structures, then $\mathbf{A}$ is *elementarily equivalent* to $\boldsymbol{B}$, $A \equiv B$, $\iff Th(\boldsymbol{A}) = Th(\boldsymbol{B})$

For example number theorists study $Th(\langle \mathbb{N}, +_{\mathbb{N}}, \times_{\mathbb{N}}, 0_{\mathbb{N}}, {}'_{\mathbb{N}} \rangle)$, another interesting theory is $Th(\langle \mathbb{R}, +_{\mathbb{R}}, \times_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}}, e_{\mathbb{R}} \rangle)$ where e is a two place function symbol and $e_{\mathbb{R}}(n, m)$ is n^m.

Lemma 7 a) $\equiv$ *is an equivalence relation*;
b) *If* $\mathbf{A}, \mathbf{B}$ are Ω structures and $\mathbf{A} \cong \mathbf{B}$ then $\mathbf{A} \equiv \mathbf{B}$.

Proof: Exercise. [Hint for b): if $h : \mathbf{A} \cong \mathbf{B}$ show by an induction on complexity that for any φ, w that $\mathbf{A} \vDash \varphi[w] \iff \mathbf{B} \vDash \varphi[h(w)]$ where $h(w) \in W^{\mathbf{B}}$ is defined by $h(w)(k) = h(w(k))$; then deduce $Th(A) = Th(\mathbf{B})$.]
Warning: the converse is false, one can show that if $<$ is the usual ordering of the reals that $\langle \mathbb{Q}, < \rangle \equiv \langle \mathbb{R}, < \rangle$ but as $\mathbb{Q}$ is countable and $\mathbb{R}$ is uncountable they clearly can't isomorphic. There is a theorem that states that given any structure $\mathbf{A}$ there is a structure $\mathbf{B}$ with $\mathbf{A}$ not isomorphic to $\mathbf{B}$, but $\mathbf{A} \equiv \mathbf{B}$. We shall see a vivid example of this later.

Exercise 11

(i) φ is universally valid if $\neg\varphi$ is unsatisfiable

(ii) If $FV(\varphi) \subseteq \{v_0, \ldots, v_n\}$ then φ is satisfiable *iff* $\exists v_0 \ldots \exists v_n \varphi$ is satisfiable

(iii) With φ as in (ii) then φ is universally valid *iff* every Ω-structure is a model of $\forall v_0 \ldots \forall v_n \varphi$.

Exercise 12 Find interpretations for each of the following formulae in which they are not satisfied (thus showing that they are not universally valid).

a) $[\forall v_0 P(v_0) \to \forall v_0 Q(v_0)] \to [\forall v_0 (P(v_0) \to Q(v_0))]$

b) $[\forall v_0 (P(v_0) \vee Q(v_0))] \to [\forall v_0 P(v_0) \vee \forall v_0 Q(v_0)]$

c) $[\exists v_0 P(v_0) \leftrightarrow \exists v_0 Q(v_0] \to \forall v_0 (P(v_0, v_1) \vee P(v_1, v_2))) \to \exists v_1 \forall v_2 P(v_1, v_2))$

Exercise 13

(i) Show that $\varphi(t/v_i) \to \exists v_i \varphi$ is universally valid if t is substitutable for v_i in φ

(ii) Show $\forall v_i \varphi \to \exists v_i \varphi$ is universally valid. Showing that a formula is not universally valid is usually most easily done by thinking up a structure and a valuation in which it comes out false. To show $\varphi \not\models \psi$ one must find a structure and valuation in which φ is true but ψ is false etc., as in the next exercise

(iii) Let φ be $\forall v_0 \forall v_1 (R(v_0, v_1) \to (R(v_1, v_2) \to R(v_0, v_2)))$.
Let ψ be $\forall v_0 \exists v_1 R(v_0, v_1) \to \exists v_1 \forall v_0 R(v_0, v_1)$
Show that neither $\varphi \models \psi$ nor $\psi \models \varphi$.

(iv) Check whether the following sets of formulae are satisfiable:

a) $\{\exists v_0 \forall v_1 R(v_0, v_1),\ \forall v_0 \forall v_1 \exists v_2 (R(v_0, v_2) \wedge R(v_2, v_1))\}$

b) $\{\forall v_0 \exists v_1 R(v_1, v_0,\ \forall v_0 \forall v_1 (v_0 \neq v_1 \to (R(v_0, v_1) \to \neg R(v_1, v_0)))\}$.

c) $\{\forall v_0 \neg R(v_0, v_0),\ \forall v_0 \forall v_1 [v_0 \neq v_1 \to (R(v_0, v_1) \wedge R(v_1, v_0))],\ \forall v_0 \forall v_1 \forall v_2 [(R(v_0, v_1) \wedge R(v_1, v_2)) \to R(v_0, v_2)]\}$

d) The same set as in c) with the addition of $\exists v_0 \exists v_1 v_0 \neq v_1$.

(v) Determine whether the following formulae are universally valid:

a) $\neg \exists v_0 \forall v_1 (v_0 \neq v_1 \to (R(v_1, v_0) \leftrightarrow \neg R(v_0, v_1)))$

b) $[\exists v_0 P(v_0) \to \exists v_0 Q(v_0)] \to \exists v_0 (P(v_0) \to Q(v_0))$

c) $\exists v_0 (P(v_0) \to \forall v_1 P(v_1))$

d) $\forall v_0 (P(v_0) \vee Q(v_0)) \to \forall v_0 P(v_0) \vee \exists v_0 Q(v_0)$.

Exercise 14 Find an interpretation for the following set of sentences
$\forall v_0 \neg R(v_0, v_0)$; $\forall v_0 \forall v_1 [v_0 = v_1 \vee R(v_0, v_1) \vee R(v_1, v_0)]$;
$\forall v_0 \exists v_2 \exists v_1 [R(v_0, v_1) \wedge R(v_2, v_0)] \wedge R(v_2, v_0]$; $\forall v_0 \forall v_1 \forall v_2 [(R(v_0, v_1) \wedge R(v_1, v_2)) \to R(v_0, v_2)]$
$\forall v_0 \forall v_1 [R(v_0, v_1) \to \exists v_2 [R(v_0, v_2) \wedge R(v_2, v_1)]]$

Exercise 15 Find an interpretation for the following sets of sentences

(i) $\forall v_0 \neg R(v_0, v_0)$; $\forall v_0 \forall v_1 \forall v_2 [(R(v_0, v_1) \wedge R(v_1, v_2)) \to R(v_0, v_2)]$; $\forall v_0 R(v_0, F(v_0))$;

(ii) $\forall v_0 \neg R(v_0, v_0$; $\forall v_0 \forall v_1 \forall v_2 [(R(v_0, v_1) \wedge R(v_1, v_2)) \to R(v_0, v_2)]$; $\forall v_0 [c = v_0 \vee \neg R(v_0, c)]$ $\forall v_0 (v_0 \neq c \to R(F(v_0, v_0))$; $\forall v_0 \forall v_1 [\neg (R(v_0, v_1) \wedge R(F(v_1), v_0))]$; $\forall v_0 \exists v_1 [v_0 \neq c \to (v_0 \neq v_1 \wedge F(v_0) = F(v_1)]$.

A formal system for predicate calculus

The last chapter considered generalised structures and the possibility of expressing in a first order language propositions that might or might not be satisfiable in, or true in, those structures. We gave a rigorous definition of what a formal language was depending on a set of relation and function symobls, given by a similarity type Ω, and gave another rigorous definition of satisfiability or truth, in an interpretation $\mathbf{A}$ of L_Ω. A universally valid sentence was something true in every suitable interpretation. We continue the search for a characterisation of universally valid formulae, and our study of mathematical structures by looking at the idea of "proof" itself. In §3.1 a formal deductive systemis defined whereby a first order formula may be deduced or inferred according to a fixed set of rules of inference from a given set of hypotheses. This formalisation is completely *syntactic*, that is it has nothing to do with "meaning", "truth", *etc.*, that is with any *semantic* concept. The rules of proof can be viewed as simple symbol manipulation procedures on strings of symbols, without any reference to intended interpretations. Again something machines could (and indeed do) do. The formalisation we shall give is deceptively simple, and in fact is actually rather restrictive in the kinds of rules of deduction we allow in the system. There are many ways of formalising the system, but they all turn out to lead to the same set of provable formulae (that is if the formalisation is a sensible one). We choose one that is useful for our purposes. In fact we want to establish theorems *about* the system, rather than actually *doing* the symbol manipulation procedures on strings of symbols, without any reference to intended interpretations. Indeed the system is so chosen with a view to making these theorems about the system simpler but even at the expense of making derivations *within* the system rather complicated.
The system is *sound* in that any formula φ that is derivable in the system from a set of axioms $\Gamma \subseteq L_\Omega$, is such that $\Gamma \vDash \varphi$. In particular when $\Gamma = \varnothing$ if φ is derivable then φ is universally valid. Our system is adequate in that we shall later be able to show (in the Completeness Theorem) that every *universally valid formula* φ is derivable. This gives us our sought after characterisation: the universally valid formulae are *precisely* those provable in our system.

4.1 Predicate calculus

Definition 4.1 *Given a first order language* L_Ω predicate calculus for L_Ω *consists of a set of* axioms *and a set of* rules of inference*:*
The (Logical) Axioms*:* Let $\varphi,\ \psi,\ \chi$ be any formulae of L_Ω then the following are axioms of PC

A1 $(\varphi \to (\psi \to \varphi))$

A2 $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$

A3 $(\neg\varphi \to \psi) \to ((\neg\varphi \to \neg\psi) \to \varphi)$

A4 Let t be any term substitutable for v_i in φ then

$$\forall v_i \varphi \to \varphi(t/v_i) \text{is an axiom}$$

A5 If $v_i \notin FV(\varphi)$ then

$$\forall v_i(\varphi \to \psi) \to (\varphi \to \forall v_i \psi) \text{is an axiom}$$

A6

$$\forall v_1(v_1 = v_1)$$

A7 Let s, t be any terms of L_Ω substitutable for both v_0 and v_1 in φ. Then

$$s = t \to (\varphi(s/v_0,\ s/v_1) \to \varphi(s/v_0,\ t/v_1)) \text{is an axiom.}$$

Remark Axioms A1-A3 are the propositional axioms, A6 and A7 the axioms for equality. As an example of the latter φ might be the ternary atomic formula $R(v_0,\ v_1,\ v_2)$. Then the axiom reads

$$s = t \to (R(s, s, v_2) \to R(s, t, v_2))$$

Some authors treat predicate calculus us having axioms of the form A1-A5 only, and then deal with the additional case of languages with an equality symbol. Since we've insisted that = be a symbol in the language we need axioms to ensure that the symbol "behaves properly" in proofs; but it's to be emphasised that predicate calculus, the Completeness Theorem and so on can be developed without this. To complete the definition of PC we need to define the:

The Rules of Inference

R1 (Modus Ponens) For any two formulae φ, ψ of L_Ω, ψ is an immediate consequence of φ and $(\varphi \to \psi)$.
R2 (Generalisation) For any formula φ of L_Ω and any variable v_k $\forall v_k \varphi$ is an immediate consequence of φ .

Lemma 4.2 *All the axioms of PC are universally valid.*

Proof A1-A3 are instances of tautologies and so universally valid by Lemma 2.6. A4-A5 by Lemma 2.5; A6 and A7 by the actual definition of satisfaction (and Lemma 2.3) QED

Definition 4.3 *Suppose* $\Gamma \cup \{\varphi\} \subseteq L_\Omega$. *A* proof *(or* deduction*, or* derivation*)* of φ from Γ *(where possibly* Γ *is empty) is a finite sequence of formulae* $\varphi_1, \varphi_2, \ldots, \varphi_n = \varphi$ *such that for each* $i \leq n$ either

	(i)	φ_i is an axiom
or	(ii)	$\varphi_i \in \Gamma$
or	(iii)	For some $j, k < i$ φ_i is an immediate consequence of φ_m, φ_k by R1
or	(iv)	For some $j < i$ φ_i is an immediate consequence of φ_j by R2 and where, if φ_i is $\forall v_k \varphi_j$, then $v_k \notin FV(\Gamma)$.

If there is a proof of φ from Γ we write $\Gamma \vdash \varphi$
If $\Gamma = \varnothing$, then we write $\vdash \varphi$ for $\varnothing \vdash \varphi$ and call φ a *theorem* of PC

Remark If $\Gamma \vdash \varphi$ and $\Sigma \supseteq \Gamma$ then trivially $\Sigma \vdash \varphi$.
The restriction in the use of *R2* comes from semantical considerations. Our aim is that if $\Gamma \vdash \varphi$ then $\Gamma \vDash \varphi$. Suppose $\mathbb{N}$ and Ω are as in Example 1.4 (p.31). Let $\Gamma = \{\nu_i = 0\}$. If the restriction of R2 were not in place we'd have $\Gamma \vdash \forall \nu_i \nu_i = 0$ but clearly $\mathbb{N} \nvDash \forall \nu_i \nu_i = 0$.
Similar reasons prompt the restrictions on A4 and A5: see Lemma 2.6.
Remark A proof of φ from Γ, being a finite sequenc eof formulae, can only quote a finite number of hypotheses from Γ, so if $\Gamma_0 \subseteq \Gamma$ is finite is such that $\Gamma_0 \vdash A$, we can loosen the restriction on R2 somewhat: it need only apply to those free variables ν_k appearing in Γ_0. The comments following the next example illustrate this.

Example 1 Let $\Gamma = \{\varphi\}$ where $\nu_1 \notin FV(\varphi)$. consider the following proof

1	$\varphi \to (\psi \to \varphi)$	Instance of A1
2	φ	Hypothesis from Γ
3	$\psi \to \varphi$	R1 on 1, 2
4	$\forall \nu_1(\psi \to \varphi)$	R2 on 3.

The application of R2 on A3 was correct since $\nu_1 \notin FV(\varphi)$. But 1-4 should also count as a proof of $\forall \nu_1(\psi \to \varphi)$ from $\Gamma_1 \supseteq \Gamma$ where $\Gamma_1 = \{\varphi, \chi\}$ say, and possibly $\nu_1 \in FV(\chi)$. This is simply because χ wasn't quoted in the proof. We implicitly allow this relaxation of Def. 3(iii) in derivations that follow.
The following example shows that proofs of even rather trivial formulae are rather complicated in our system.
Example 2 For any formula $\varphi \vdash \varphi \to \varphi$

1	$(\varphi \to ((\varphi \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$	Instance of A2
2	$\varphi \to ((\varphi \to \varphi) \to \varphi)$	Instance of A1
3	$(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$	R1 on 1, 2
4	$\varphi \to (\varphi \to \varphi)$	Instance of A1
5	$\varphi \to \varphi$	R1 on 3, 4

We quickly introduce some lemmas that enable us to speed up our proofs by deriving some additional rules. Example 1 above shows $\varphi \vdash \forall \nu_1(\psi \to \varphi)$. Even proving $\vdash \varphi \to \forall \nu_1(\psi \to \phi)$ is rather difficult using our minimal rules. The following theorem shows we can conclude it immediately.

Theorem 4.4 (Deduction Theorem) *If* $\Gamma \cup \{\varphi, \psi\} \subseteq L_\Omega$ *and* $\Gamma, \varphi \vdash \psi$ *then* $\Gamma \vdash \varphi \to \psi$.

Proof Let $\varphi_1, \ldots, \varphi_n = \psi$ be a proof of ψ from $\Gamma \cup \{\varphi\}$. By induction on i we show that $\Gamma \vdash \varphi_i$. $i = n$ is our desired result.
Suppose for $j < i$ we have shown $\Gamma \vdash \varphi \to \varphi_j$.
If $\varphi_i = \varphi$ then as in Example 2 $\vdash \varphi \to \varphi$, so $\Gamma \vdash \varphi \to \varphi$
If φ_i is an axiom, or is in Γ, then as $\varphi_i \to (\phi \to \varphi_i)$ is an instance of A1, we have $\Gamma \vdash \phi_i \to (\varphi \to \varphi_i)$ and we have $\Gamma \vdash \varphi_i$, and by R1, we get $\Gamma \vdash \varphi \to \varphi_i$
If φ_i followed from φ_j and φ_k by R1, so then φ_k, say, was $\varphi_j \to \varphi_i$. by our by inductive hypothesis

$\Gamma \vdash \varphi \to \varphi_j$ and $\Gamma \vdash \varphi \to \varphi_k$.
But $\vdash (\varphi \to (\varphi_j \to \varphi_i)) \to ((\varphi \to \varphi_j) \to (\varphi \to \varphi_i))$ (Instance of A2)

Apply R1 twice, to get $\Gamma \vdash \varphi \to \varphi_i$.
Lastly if φ_i is $\forall v_n \varphi_j$ where $j < i$, by inductive hypothesis $\Gamma \vdash \varphi \to \varphi_j$. Now φ_i arose by applying R2 on φ_j; by our restrictions on proof in Def 3(iii) $v_n \notin FV(\varphi)$. So, we may apply

R2 to get $\Gamma \vdash \forall v_n(\varphi \to \varphi_j)$
But $\vdash \forall v_n(\varphi \to \varphi_j) \to (\varphi \to \forall v_n \varphi_j)$ (Instance of A5)

So by applying R1 we have

$$\Gamma \vdash \varphi \to \forall v_n \varphi_j \text{ as required.}$$

So $\Gamma \vdash \varphi_i$ and the i'th stage of the induction is complete. QED

Example 3 $\vdash \forall v_0 \forall v_1 \varphi \to \forall v_1 \forall v_0 \varphi$

1	$\forall v_0 \forall v_1 \varphi$	Hypothesis
2	$\forall v_0 \forall v_1 \varphi \to \forall v_1 \varphi$	A4 $t = v_0$ φ as $\forall v_1 \varphi$
3	$\forall v_1 \varphi$	R1 on 1, 2
4	$\forall v_1 \varphi \to \varphi$	A4 $t = v_1$
5	φ	R1 on 3, 4
6	$\forall v_0 \varphi$	R2 on 5
7	$\forall v_1 \forall v_0 \varphi$	R2 on 6.

Thus we've shown $\forall v_0 \forall v_1 \varphi \vdash \forall v_1 \forall v_0 \varphi$. by the Deduction Theorem we conclude

$$\vdash \forall v_0 \forall v_1 \varphi \to \forall v_1 \forall v_0 \varphi$$

LEMMA 4.5 *a) (Particularisation Rule) If t is substitutable for v_0 in φ then $\forall v_0 \varphi \vdash \varphi(t/v_0)$*
b) (Existential or E-Rule) If t is substitutable for v_0 in φ then $\varphi(t/v_0) \vdash \exists v_0 \varphi$

Note In the above t can be v_0 itself

Proof a)

1	$\forall v_0 \varphi$	Hypothesis
2	$\forall v_0 \varphi \to \varphi(t/v_0)$	Instance of A4
3	$\varphi(t/v_0)$	R1 1, 2

b) We show $\vdash \varphi(t/v_0) \to \exists v_0 \varphi$, since then using R1 we get $\varphi(t/v_0) \vdash \exists v_0 \varphi$.

1	$\forall v_0 \neg \varphi \to \neg \varphi(t/v_0)$	A4
2	$(\forall v_0 \neg \varphi \to \neg \varphi(t/v_0)) \to (\varphi(t/v_0) \to \neg \forall v_0 \neg \varphi)$	Taut. Instance
3	$\varphi(t/v_0) \to \exists v_0 \varphi$	R1 on 1,2 QED

We need to explain the second line in the above. What we've done is introduce an instance of a tautology, in face the tautology $(\psi \to \neg\chi) \to (\chi \to \neg\psi)$. That we're allowed to do this follows from the next theorem.

THEOREM 4.6 *Every instance of a tautology is a theorem of PC.*

If we grant the theorem, then line 2 above has a proof from the axioms. Instead of working out and writing down that proof and inserting it in place of line 2, we've simply appealed to the theorem and written down the justification on the right hand side. (We shall do this in other cases in the future when we appeal to previous results.) Many authors take as axioms for PC all instances of tautologies. The theorem then merely says there's no advantage to doing this.

Proof. Let φ be an instance of a formula ψ in L_ω where ψ contains $P_1, \ldots, P_n$ say and φ comes from ψ by replacing P_i by φ_i $(1 \leq i \leq n)$. Define, for any valuation $w : \{P_1, \ldots, P_n\} \to \{T, F\}$

$$\begin{aligned}\varphi_i' &= \varphi_i \text{ if } w(P_i) = T\\ &= \neg\varphi_i \text{ if } w(P_i) = F\\ \varphi' &= \varphi \text{ if } w^*(\psi) = T\\ &= \neg\varphi \text{ if } w^*(\psi) = F.\end{aligned}$$

Claim 1 With the notiation as above $\Gamma = \{\varphi_1', \ldots, \varphi_n'\} \vdash \varphi'$.
Proof of Claim By induction on comp(ψ):
ψ *is* $\neg\chi$ and so φ is of the form $\neg\gamma$. γ' is γ if $w^*(\chi) = T$ and is $\neg\gamma$ otherwise. By the inductive hypothesis $\Gamma \vdash \gamma'$. If $w^*(\chi) = F$ then $\gamma' = \neg\gamma = \varphi'$, so $\Gamma \vdash \varphi'$; if $w^*(\chi) = T$ then $\gamma' = \gamma$ and $\varphi' = \neg\varphi - \neg\neg\gamma$, since $\Gamma \vdash \gamma'$ and $\vdash \gamma \to \neg\neg\gamma$ (slightly tricky Exercise) we have $\Gamma \vdash \varphi'$ (using R1).
ψ *is* $\chi_1 \to \chi_2$ and so φ is of the form $\gamma_1 \to \gamma_2$.
By inductive hypothesis $\Gamma \vdash \gamma_1'$ and $\Gamma \vdash \gamma_2'$ where

$$\begin{aligned}\gamma_1' &= \gamma_1 \quad \text{if } w^*(\chi_1) = T\\ &= \neg\gamma_1 \quad \text{if } w^*(\chi_1) = F\end{aligned}$$

and similarly for γ_2'
If $w^*(\chi_1) = F$ we have $\Gamma \vdash \neg\gamma_1$ and by Claim 2a) $\vdash \neg\gamma_1 \to (\gamma_1 \to \gamma_2)$; so we have $\Gamma \vdash \gamma_1 \to \gamma_2$. But $w^*(\chi_1) = F$ so $w^*(\psi) = R$ and thus φ' is $\gamma_1 \to \gamma_2$, so $\Gamma \vdash \varphi'$.
If $w^*(\chi_2) = T$ again φ' is $\gamma_1 \to \gamma_2$, γ_2', γ_2' is γ_2 and $\Gamma \vdash \gamma_2$ by the inductive hypothesis. But $\vdash \gamma_2 \to (\gamma_1 \to \gamma_2)$ is an instance of A1 so by R1 $\Gamma \vdash \gamma_1 \to \gamma_2$.
If $w^*(\chi_1) = T$ *and* $w^*(\chi_2) = F$ then φ' is $\neg\varphi$, γ_1' is γ_1, γ_2' is $\neg\gamma_2$ and by the inductive hypothesis $\Gamma \vdash \gamma_1$ and $\Gamma \vdash \neg\gamma_2$. By Claim 2b) and two applications of R1 $\Gamma \vdash \neg(\gamma_1 \to \gamma_2)$.
Claim 2 For any formulae φ, *psi* of L_Ω

a) $\vdash \neg\varphi \to (\varphi \to \psi)$
b) $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$.

Proof

a)	1	φ	Hyp
	2	$\neg\varphi$	Hyp
	3	$\varphi \to (\neg\psi \to \varphi)$	A1
	4	$\neg\psi \to \varphi$	R1 1, 3
	5	$\neg\psi \to \neg\varphi$	A1

6	$\neg\psi \to \neg\varphi$	R1 2, 5
7	$(\neg\psi \to \varphi) \to ((\neg\psi \to \neg\varphi) \to \psi)$	A3
8	ψ	R1 twice 4, 6, 7.

So $\varphi,\ \neg\varphi \vdash \psi$. Apply the Deduction Theorem twice.

b) Since $\varphi,\ \varphi \to \psi \vdash \psi$ the Deduction Theorem gives

(1) $\vdash \varphi \to ((\varphi \to \psi) \to \psi)$. Now $\vdash (\gamma \to \delta) \to (\neg\delta \to \neg\gamma)$ (proof omitted) we have

(2) $\vdash ((\varphi \to \psi) \to \psi) \to (\neg\psi \to \neg(\varphi \to \psi))$.

But $\gamma \to \delta,\ \delta \to \varepsilon \vdash \gamma \to \varepsilon$ (easy application of Deduction Theorem); applying this to (1) and (2) gives $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$. This finishes off the Claim.

Let φ be an instance of the tautology ψ, where ψ has propositional variables $P_1, \ldots, P_n$ and φ is the result of substituting $\varphi_1, \ldots, \varphi_n$ for $P_1, \ldots, P_n$. With the notation above for any valuation w of the propositional variables φ' is φ (since ψ is a tautology).
If $w(P_n) = T$ $\varphi'_n = \varphi_n$ and by Claim 1 $\{\varphi'_1, \ldots, \varphi'_{n-1} \vdash \neg\varphi_n \to \varphi$. Applying the theorem $\vdash 9\varphi_n \to \varphi) \to ((\neg\varphi_n \to \varphi) \to \varphi)$ and R1 gives $\{\varphi'_1, \ldots, \varphi'_{n-1}\} \vdash \varphi$. Repeating the process another $n-1$ times yields $\vdash \varphi$.

Corollary 4.7 *(to Lemma 3)* $\vdash \forall v_0\varphi \to \exists v_0\varphi$

Proof We show $\forall v_0\varphi \vdash \exists v_0\varphi$ and then we use the Deduction Theorem.

1	$\forall v_0\varphi$	Hyp
2	$\forall v_0\varphi \to \varphi(v_0/v_0)$	A4 with $t = v_0$
3	$\varphi(v_0/v_0)$	R1 on 1, 2
4	$\exists v_0\varphi$	E-Rule on 3 (with r as v_0) QED

The following lemma lists some results of derivations which we can consider as *derived rules* which we can later use as further justifications for lines in derivations.

a)	*Negation*	$\neg\neg\varphi \vdash \varphi$; $\quad \varphi \vdash \neg\neg\varphi$
b)	*Conjuction*	$\varphi \wedge \psi \vdash \varphi$; $\quad \varphi \wedge \psi \vdash \psi$
		$\neg(\varphi \wedge \psi) \vdash \neg\varphi \wedge \neg\psi$
		$\varphi,\ \psi \vdash \varphi \wedge \psi$
c)	*Disjunction*	$\varphi \to \psi,\ \chi \to,\ \varphi \wedge \chi \vdash \psi$
		$\neg(\varphi \wedge \psi) \vdash \neg\varphi \wedge \neg\psi$
		$\varphi \wedge \psi,\ \neg\varphi \vdash \psi; \varphi \wedge \psi,\ \neg\psi \vdash \varphi$
		$\varphi \vdash \varphi \wedge \psi; \psi \vdash \varphi \wedge \psi$
d)	*Conditional*	$\varphi \to \psi,\ \neg\psi \vdash \neg\varphi$
		$\neg(\varphi \to \psi) \vdash \varphi$; $\quad \neg(\varphi \to \psi) \vdash \neg\psi$
e)	*Biconditional*	$\varphi \leftrightarrow \psi,\ \varphi \vdash \psi$; $\quad \varphi \leftrightarrow \psi,\ \psi \vdash \varphi$
		$\varphi \leftrightarrow \psi,\ \neg\varphi \vdash \neg\psi$; $\quad \varphi \leftrightarrow \psi, \neg\psi \vdash \neg\varphi$

		$\varphi \leftrightarrow \psi \vdash \varphi \to \psi$; $\quad \varphi \leftrightarrow \psi \vdash \psi \to \phi$
		$\varphi \to \psi,\ \psi \to \varphi \vdash \varphi \leftrightarrow \psi$
f)	*Proof by Contradiction*	$\Gamma,\ \neg\varphi \vdash \psi \wedge \neg\psi$ then $\Gamma \vdash \varphi$
g)	*Contraposition*	$\varphi \to \psi \vdash\ \neg\psi \to \neg\varphi$; $\quad \neg\psi \to \neg\varphi \vdash \varphi \to \psi$
h)	*Proof by cases*	$\Gamma,\ \varphi \vdash \psi$ *and* $\Gamma,\ \varphi \vdash\ \neg\psi$ *then* $\Gamma \vdash \neg\varphi$

Proof All can be shown by using suitable instances of tautologies, for example we prove $\varphi \to \psi,\ \chi \to \psi,\ \varphi \wedge \chi \vdash \psi$.

1	$\varphi \to \psi$	Hyp
2	$\chi \to \psi$	Hyp
3	$\varphi \wedge \chi$	Hyp
4	$(\varphi \to \psi) \to ((\chi \to \psi) \to\ ((\varphi \wedge \chi) \to \psi))$	Tautology
5	ψ	R1 3 times on 1-4

The rest are similar and are left as an exercise. QED

Definition 4.8 *a) We say* φ *and* ψ *are* provably equivalent *if* $\varphi \vdash \psi$ *and* $\psi \vdash \varphi$

b) "χ' *comes from* χ *by replacing some (or all or no) occurrences of* ψ *by* φ*",* $\mathrm{Rep}(\varphi, \psi, \chi, \chi')$*, is defined by induction on complexity of* φ $\mathrm{Rep}(\varphi, \psi, \chi, \chi')$ *holds*

iff χ *is atomic and* χ' *is* χ

or χ *is* φ *and* χ' *is* ψ *of* φ

or χ *is* $\chi_1 \to \chi_2$ *and* χ' *is* $\chi_1' \to \chi_2'$ *and* $\mathrm{Rep}(\varphi, \psi, \chi_1, \chi_1')$ *and* $\mathrm{Rep}(\varphi, \psi, \chi_2, \chi_2')$

or χ *is* $\neg\chi_1$, χ' *is* $\neg\chi_1'$ *and* $\mathrm{Rep}(\varphi, \psi, \chi_1, \chi_1')$

or χ *is* $\forall v_n \chi_1$, χ' *is* $\forall v_n \chi_1'$ *and* $\mathrm{Rep}(\varphi, \psi, \chi_1, \chi_1')$

Notice that the definition of Rep is simply that of Definition 1.10 with an extra clause added to take care of $\forall v_n \varphi$. Lemma 7c) below then is analogous to the Principle of Substitution for truth functional equivalence, Lemma 1.2.

Lemma 4.9

a) Provable equivalence is an equivalence relation
b) φ, ψ are provably equivalent iff $\quad \vdash \varphi \leftrightarrow \psi$
c) φ, ψ provably equivalent and *Rep*$(\varphi, \psi, \chi, \chi')$ then χ, χ' are provably equivalent.

Proof

a) Reflexivity is trivial; transitivity follows from "$\varphi \vdash \psi$ and $\psi \vdash \chi$ implies $\varphi \vdash \chi$"; symmetry is trivial

b) If φ, ψ are provably equivalent, by the Deduction Theorem we have $\vdash \varphi \to \psi$ and $\vdash \psi \to \varphi$. By Lemma 6 e) we have $\vdash \varphi \leftrightarrow \psi$. Conversely $\varphi \leftrightarrow \psi \vdash \varphi \to \psi$ and $\varphi \leftrightarrow \psi \vdash \psi \to \varphi$ (again by Lemma 6e)). So $\vdash \varphi \leftrightarrow \psi$ yields $\vdash \varphi \to \psi$ and $\vdash \psi \to \varphi$. But $\vdash \varphi \to \psi$ implies $\varphi \vdash \psi$ [because $\vdash \varphi \to \psi$ implies $\varphi \vdash \varphi \to \psi$, which by R1 gives $\varphi \vdash \psi$]. Similarly $\psi \vdash \varphi$.

c) By induction on complexity of χ. Only if χ is $\chi_1 \to \chi_2$ of is $\forall v_n \chi_1$ is it not trivial.

$\underline{\chi \text{ is } \chi_1 \to \chi_2}$ and χ' is $\chi_1' \to \chi_2'$ and by definition $\mathrm{Rep}(\varphi, \psi, \chi_1, \chi_1')$ $\mathrm{Rep}\varphi, \psi, \chi_2, \chi_2')$. By induction hypothesis $\chi_1 \vdash \chi_1$ and $\chi_2 \vdash \chi_2'$. So

$\chi_1 \to \chi_2, \chi_1' \vdash \chi_2$ (since $\chi_1' \vdash \chi_1$ we can use R1 on χ_1, and $\chi_1 \to \chi_2$). So
$\chi_1 \to \chi_2, \chi_1' \vdash \chi_2'$ (using $\chi_2 \vdash \chi_2'$)

So $\chi_1 \to \chi_2 \vdash \chi_1' \to \chi_2'$ using the Deduction Theorem. The converse is similar.
$\underline{\chi \text{ is } \forall v_n \chi_1}$ and χ' is $\forall v_n \chi_1'$, and $\mathrm{Rep}(\varphi, \psi, \chi_1, \chi_1')$
$\forall v_n \chi_1 \vdash \chi_1$ (using $\vdash \ \forall v_n \chi_1 \to \chi_1$, and R1) and $\chi_1 \vdash \chi_1'$ by inductive hypothesis. So $\forall v_n \chi_1 \vdash \chi_1'$. But $v_n \notin FV(\forall v_n \chi_1)$ so apply R2 and get $\forall v_n \chi_1 \vdash \forall v_n \chi_1'$. The converse is similar. QED
Thus: if we can *prove* two formulae equivalent, then the above result shows that if we take any other formula in which one of these formulae occur we can *prove* that it's equivalent in our system to that with the replacement made. A major use of Lemma 7 is that when developing proofs if φ is on line n and φ is provably equivalent to ψ, we allow ourselves to write ψ on any later line.

Example 4 Suppose $\vdash \varphi \leftrightarrow \psi$, then $\vdash \exists v_1(\varphi \wedge \chi) \leftrightarrow \exists v_1(\psi \wedge \chi)$
We collect together in the next few lemmas some useful theorem of our system.

Lemma 4.10

i)	If $v_i \notin FV(\varphi)$ and v_i is substitutable for v_j in φ then	
ii) a)	$\vdash \forall v_j \varphi \leftrightarrow \forall v_i \varphi(v_i/v_j)$	*b)* $\vdash \exists v_j \varphi \leftrightarrow \exists v_i \varphi(v_i/v_j)$
iii) a)	$\vdash \neg \forall v_i \varphi \leftrightarrow \exists v_i (\neg \varphi)$	*b)* $\vdash \exists v_i \exists v_j \varphi \leftrightarrow \exists v_i \varphi$

Proof i)

1	$\forall v_j \varphi \to \varphi(v_i/v_j)$	A4 using $t = v_i$
2	$\forall v_i(\forall v_j \varphi \to \varphi(v_i/v_j))$	R2 1 since $v_i \notin FV(\varphi)$
3	$\forall v_i(\forall v_j \varphi(v_i/v_j)) \to (\forall v_j \varphi \to \forall v_i \varphi(v_i/v_j))$	A5
4	$\forall v_j \varphi \to \forall v_i \varphi(v_i/v_j)$	R1 2, 3.

Conversely

1	$\forall v_i \varphi(v_i/v_j)$	Hyp
2	φ	Particularisation [Note v_j subst. for v_i in $\varphi(v_i/v_j)$]
3	$\forall v_j \varphi$	R2, 2

We thus have $\forall v_i \varphi(v_i/v_j) \vdash \forall v_j \varphi$ and above $\vdash \forall v_j \varphi \to \forall v_i \varphi(v_i/v_j)$ and so the result follows by the Deduction Theorem and Lemma 6 e).
ii a) $\exists v_i \neg \varphi$ is by definition of $\exists$ an abbreviation of $\neg \forall v_i \neg \neg \varphi$. But $\vdash \varphi \leftrightarrow \neg \neg \varphi$ (Lemma 6a)) so by Lemma 7 $\vdash \neg \forall v_i \neg \neg \varphi \leftrightarrow \neg \forall v_i \varphi$ as required. ii b) Similar

iii)	1	$\forall v_i \forall v_j \varphi$	Hyp
	2	$\forall v_j \varphi$	Part. (with $t = v_i$)
	3	φ	Part. (with $t = v_j$)
	4	$\forall v_i \varphi$	R2
	5	$\forall v_j \forall v_i \varphi$	R2.

So $\forall v_i \forall v_j \vdash \forall v_j \forall v_i \varphi$. The other deduction is identical.

LEMMA 4.11

i *a)* $\vdash \forall v_i(\varphi \wedge \psi) \leftrightarrow \forall v_i \varphi \wedge \forall v_i \psi$
b) $\vdash \exists v_i(\varphi \wedge \psi) \leftrightarrow \exists v_i \varphi \wedge \exists v_i \psi$
c) $\vdash \forall v_i \varphi \wedge \forall v_i \psi \rightarrow \forall v_i(\varphi \wedge \psi)$
d) $\vdash \exists v_i(\varphi \wedge \psi) \rightarrow \exists v_i \varphi \wedge \exists v_i \psi$
ii If $v_i \notin FV(\varphi)$ then
a) $\vdash \varphi \wedge \exists v_i \psi \leftrightarrow \exists v_i(\varphi \wedge \psi)$
b) $\vdash \varphi \vee \forall v_i \psi \leftrightarrow \forall v_i(\varphi \vee \psi)$
c) $\vdash \varphi \leftrightarrow \exists v_i \varphi$ $\qquad\qquad$ $\vdash \varphi \leftrightarrow \forall v_i \varphi$
d) $\vdash (\varphi \rightarrow \exists v_i \psi) \leftrightarrow \exists v_i(\varphi \rightarrow \psi)$
e) $\vdash (\exists v_i \psi \rightarrow \varphi) \leftrightarrow \forall v_i(\psi \rightarrow \varphi)$
f) $\vdash (\varphi \rightarrow \forall v_i \psi) \leftrightarrow \forall v_i(\varphi \rightarrow \psi)$
g) $\vdash (\forall v_i \psi \rightarrow \varphi) \leftrightarrow \exists v_i(\psi \rightarrow \varphi)$

Proof We do some samples.

i a)	1	$\forall v_i(\varphi \wedge \psi)$	Hyp
	2	$\varphi \wedge \psi$	Part.
	3	φ	Lemma 6 b) Conjunction
	4	ψ	Similarly
	5	$\forall v_i \varphi$	R2, 3
	6	$\forall v_i \psi$	R2, 4
	7	$\forall v_i \varphi \wedge v_i \psi$	Lemma 6 b)

Thus $\forall v_i(\varphi \wedge \psi) \vdash \forall v_i \varphi \wedge v_i \psi$. Converse not too dissimilar.
i d) We prove $\vdash \neg(\exists v_i \varphi \wedge \exists v_i \psi) \rightarrow \neg \exists v_i(\varphi \wedge \psi)$ and use contraposition, Lemma 6 b).

	1	$\neg(\neg \forall v_i \neg \varphi \wedge \neg \forall v_i \neg \psi)$	Hyp
	2	$\neg\neg \forall v_i \neg \varphi \vee \neg\neg \forall v_i \psi$	Lemma 6 b) Conjunction
	3	$\forall v_i \neg \varphi \vee \forall v_i \neg \psi$	Provably equivalent to 2 by Lemmas 6 a) and 7 c)
	4	$\forall v_i(\neg \varphi \vee \neg \psi$	Lemma 9 i c).
	5	$\forall v_i \neg(\varphi \wedge \psi)$	Lemma 7.
	6	$\neg\neg \forall v_i \neg(\varphi \wedge \psi)$	Provably equivalent ot 5 using Lemma 6 a)
ii e)	1	$\neg \forall v_i \neg \varphi \wedge \neg \forall v_i \neg \psi)$	Hyp

	2 $\neg\neg\forall v_i\neg\varphi \vee \neg\neg\forall v_i\psi$	Lemma 6b) Conunction
	3 $\forall v_i\neg\varphi \wedge \forall v_i\neg\psi$	Provably equivalent to 2 by Lemmas 6a) and 7c)
	4 $\forall v_i(\neg\varphi \wedge \neg\psi)$	Lemma 9 i c).
	5 $\forall v_i\neg(\varphi \wedge \psi)$	Lemma 7.
	6 $\neg\neg\forall v_i\neg(\varphi \wedge \psi)$	Provably equivalent to 5 using Lemma 6a)
ii e)	1 $\neg\forall v_i\neg\psi \rightarrow \varphi$	Hyp
	2 $\forall v_i\neg\psi \vee \varphi$	Prov. equiv. to 1 using def. of $\vee$ and Lemma 6a)
	3 $\forall v_i(\neg\psi \vee \varphi)$	By Part ii b)
	4 $\forall v_i(\psi \rightarrow \varphi)$	Definition of $\vee$.

Since each step here is a provable equivalence or a definition, it is reversibly giving the required equivalence.

ii b)	1 $\forall v_i(\varphi \vee \psi)$	Hyp
	2 $\forall v_i(\neg\varphi \rightarrow \psi)$	Def. of $\vee$.
	3 $\forall v_i(\neg\varphi \rightarrow \psi) \rightarrow (\neg\varphi \rightarrow \forall v_i\psi)$	A5 $v_i \notin FV(\varphi)$
	4 $\neg\varphi \rightarrow \forall v_i\psi$	R1 2, 3
	5 $\varphi \vee \forall v_i\psi$	Def. of $\vee$.

Thus $\forall v_i(\varphi \vee \psi) \vdash \varphi \vee \forall v_i\psi$

Conversely

	1 $\varphi \vee \forall v_i\psi$	Hyp
	2 $\neg\varphi \rightarrow \forall v_i\psi$	Def. of $\vee$
	3 $\neg\varphi$	Hyp
	4 $\forall v_i\psi$	R1 on 2, 3
	5 ψ	Part

Thus $\varphi \vee \forall v_i\psi,\ \neg\varphi \vdash \psi$ By Deduction Theorem
$\varphi \vee \forall v_i\psi \vdash \neg\varphi \rightarrow \psi$
But $v_i \notin FV(\varphi)$ so we can apply R2 to get
$\varphi \vee \forall v_i\psi \vdash \forall v_i(\neg\varphi \rightarrow \psi)$ as required. QED

None of our lemmas have yet said much about the equality symbol.

Lemma 4.12

a) $\vdash \forall v_n(v_n = v_n)$ *For any terms s, t, u:*
b) $\vdash s = t \rightarrow t = s$
c) $\vdash (s = t \wedge t = u) \rightarrow s = u$

Proof a)	1	$\forall v_1(v_1 = v_1)$	A6
	2	$v_n = v_n$	Part. $(t = v_n)$
	3	$\forall v_n(v_n = v_n)$	R2 on 2.

b) Let φ be the formula $v_1 = v_0$

1	$\forall v_1(v_1 = v_1)$	A6
2	$s = s$	Part. $(t = s)$
3	$s = t \to (s = s \to t = s)$	A7 with φ as above.
4	$s = t$	Hyp
5	$t = s$	R1 twice on 2, 3, 4.

Thus $s = t \vdash t = s$. Now use the Deduction Theorem

c)

1	$s = t$	Hyp
2	$t = u$	Hyp
3	$s = t \to t = s$	Lemma 10 b)
4	$t = s$	R1 on 1, 3.
5	$t = s \to (t = u \to s = u)$	A7 with φ as $v_1 = u$
6	$s = u$	R1 twice 2, 4, 5

Thus $s = t,\ t = u \vdash s = u$. So (Lemma 6) $s = t \wedge t = u \vdash s = u$, and again the result follows from the Deduction Theorem. QED

LEMMA 4.13 *Suppose v_1 does not occur anywhere in φ. Show*

a) $\vdash \forall v_0[\varphi \leftrightarrow \exists v_1(v_0 = v_1 \wedge \varphi(v_1/v_0))]$

b) $\vdash \forall v_0[\varphi \leftrightarrow \forall v_1(v_0 = v_1 \to \varphi(v_1/v_0))]$.

Proof a)

1	$\forall v_1\ \neg(v_0 = v_1 \wedge \varphi(v_1/v_0))$	Hyp
2	$\neg(v_0 = v_0 \wedge \varphi)$	Part. $t = v_0$.
3	$v_0 = v_0$	Part. from Lemma 10 a)
4	$\neg\varphi$	Taut. $P \to (\neg(P \wedge Q) \to \neg Q))$ and R1 twice on 3, 2

So $\forall v_1 \neg(v_0 = v_1 \wedge \varphi(v_1/v_0)) \vdash \neg\varphi$. Or by contraposition, Lemma 6 g) and R1.
$\varphi \vdash \exists v_1(v_0 = v_1 \wedge \varphi(v_1/v_0))$ and by Deduction Theorem
$\vdash \varphi \to \exists v_1(v_0 - v_1 \wedge \varphi(v_1/v_0))$ Now use R2 on v_0.

Conversely

1	$v_0 = v_1 \wedge \varphi(v_1/v_0)$	Hyp
2	φ	Exercise 5 and R1 on 1

So

$v_0 = v_1 \wedge \varphi(v_1/v_0) \vdash \varphi$	Or again using Lemma 6
$\neg\varphi \vdash \neg(v_0 = v_1 \wedge \varphi(v_1/v_0))$	Now apply R2, knowing $v_1 \notin FV(\varphi)$:
$\neg\varphi \vdash \forall v_1 \neg(v_0 = v_1 \wedge \varphi(v_1/v_0))$	Or as above
$\vdash \exists v_1(v_0 = v_1 \wedge \varphi(v_1/v_0)) \to \varphi$	Hence by Lemma 6 e)
$\vdash \varphi \leftrightarrow \exists v_1(v_0 = v_1 \wedge \varphi(v_1/v_0))$	Thus result follows applying R2 again on v_0.

QED

Remark Given a sequence $s_1, \ldots, s_n$ of gödel numbers of formulae it's a mechanical matter to check whether there is i or j so that s_i and s_j code formulae φ_i, φ_j such that we can apply R1 to them. Given s_i say we look and see if s_j codes a formula beginning $(\varphi_i \to$ and we know that applying R1 to φ_i and φ_j would then result in ψ when s_j codes $(\varphi_i \to \psi)$.
Suppose then we have a finite set Γ of formulae, with gn's $t_1, \ldots, t_k$. And suppose that we are provided with a list of gn's $s_1, \ldots, s_n$. I claim that it's a mechanical procudre to *check* whether $s_1, \ldots, s_n$ constitutes a proof in PC from Γ. Each s_i must equal some t_j or it must be an instance of a tautology (I've already argued that we can mechanically generate code numbers of such formulae) or s_i must "follow from" two earlier code numbers by begin the result of an application of R1 on the two formulae so coded, or lastly s_i codes $\forall v_\ell \varphi$ where φ has a code s_j for some $j < i$; we can further check that we apply Def 3(iii) properly, and that v_ℓ is not a free variable of the $s_{j'}$ in the list where $s_{j'}$ is one of the t's.
Thus: Checking a proof is an effective procedure. Furthermore, we can expand this idea and allow Γ to be an infinite set of formulae and still check effectively whether $s_1, \ldots, s_n$ is a proof from Γ *as long as* we have an effective method to check whether s_i codes a formula in Γ.

4.2 The Soundness Theorem

We've said little so far about relating proof procedures to meaning. Lemma 1 stated that all axioms of PC are universally valid and Theorem 4 claimed that all instances of tautologies are provable. The next theorem shows that our purely symbolic manipulations have a "sensible" meaning: the rules of inference preserve universal validity; in other words the system is sound. In fact it shows more than this; it shows that the rules of inference cannot lead to a formula which is not satisfiable in any structure in which the hypotheses of the derivation are true. [In fact it shows more than this, it shows that our rules of inference cannot lead to a formula which is not satifiable in any structure in which the hypotheses are true].

Theorem 4.14 (The Soundness Theorem) *Let* $\Gamma \cup \{\varphi\} \subseteq L_\Omega$. *Then*

$$\Gamma \vdash \varphi \implies \Gamma \vDash \varphi.$$

Proof Let $\Gamma_0 \subseteq \Gamma$ be finite so that $\Gamma_0 \vdash \varphi$. Let $\varphi_1, \ldots, \varphi_n = \varphi$ be a proof of φ from Γ_0. We show by induction on $i \leq n$ that $\Gamma_0 \vDash \varphi_i$ whence $\Gamma \vDash \varphi$. Suppose this is proven for $j < i$.

(i) φ_i *an axiom*: then $\vDash \varphi_i$ by Lemma 1, so $\Gamma_0 \vDash \varphi$

(ii) $\varphi_i \in \Gamma_0$: again trivially $\Gamma_0 \vDash \varphi$

(iii a) φ_i *follows from* φ_j and $\varphi_k (j, k < i)$ by R1. Then by our inductive hypothesis $\Gamma_0 \vDash \varphi_j$ and $\Gamma_0 \vDash \varphi_k$. Suppose φ_k is $\varphi_j \to \varphi_i$. Let $\mathbf{A}$ be any interpretation of L_Ω, w any valuation in W^A so that $\mathbf{A} \vDash \psi[w]$ for all $\psi \in \Gamma_0$. By inductive hypothesis

$$\mathbf{A} \vDash \varphi_j[w] \text{ and } \mathbf{A} \vDash \varphi_k[w], \qquad \text{so by Def. 2.15, } \mathbf{A} \vDash \varphi_i[w].$$

Hence $\Gamma_0 \vDash \varphi_i$.

Definition 4.15 *a) A theory T is* deductively closed*, if for any sentence φ if $T \vdash \varphi$ then $\varphi \in T$.*
b) The deductive closure *of a theory T, is the smallest theory $T' \supseteq T$ so that T' is deductively closed.*

Hence The deductive closure of a theory T is the set of all sentences
derivable from T in PC. (*Warning* being deductively closed is not the same as being complete.)

Definition 4.16 *a) Let T be a theory. T' is an* axiomatisation *of T if for all sentences φ $T' \vdash \varphi$ iff $T \vdash \varphi$.*
b) A theory T is finitely axiomatisable *if there is an axiomatisation T' of T with T' a finite set.*

Clearly 8 a) is only going to be interesting when there's something special about $T' : T$ axiomatises itself! 3 b) gives one way for it to be interesting. Alternatively the members of T' could be given to us in some effective way.
We look at some examples of theories and their axiomatisations.

Example 5 *The Theory of groups* is the deductive closure of the following three axioms in L_Ω

(i) $\forall v_1 \forall v_2 \forall v_3 [(v_1 \circ v_2) \circ v_3 = v_1 \circ (v_2 \circ v_3)]$

(ii) $\forall v_1 (v_1 \circ e = e \circ v_1 = v_1)$

(iii) $\forall v_1 \exists v_2 (v_1 \circ v_2 = v_2 \circ v_1 = e)$

where $\Omega = \langle \mathbf{r}, \mathbf{f} \rangle$, dom $\mathbf{r}$ empty, and $\mathbf{f}$ has a two place and a constant symbol only. The theory of groups is obviously finitely axiomatisable, because we have *defined* it to be the set of sentences provable from the three axioms above! But it is not complete since some groups are commutative and others are not.
Example 6 *The Theory of dense linear order without endpoints* is the deductive closure of the sentences in Exercise 2.14. Here the language contains just the 2-place relation symbol R.
Example 7 *The Theory of strict partial order* has axioms

(i) $\forall v_0 \neg R(v_0, v_0)$

(ii) $\forall v_0 \forall v_1 [R(v_0, v_1) \to \neg R(v_1, v_0)]$

(iii) $\forall v_0 \forall v_1 \forall v_2 [R(v_0, v_1) \wedge R(v_1, v_2) \to R(v_0, v_2)]$

in the same language as Example 6. Formally speaking the *theory* is again the set of sentences deducible from these two.
Example 8 *The Theory of graphs* is the deductive closure of $\forall v_1 \forall v_2 (R(v_1, v_2) \to R(v_2, v_1))$. (A graph is simple a set with a symmetric relation.)
Example 9 *The Theory of commutative fields*
Let $\Omega = \langle \mathbf{r}, \mathbf{f} \rangle$ with dom $\mathbf{r}$ empty, dom $\mathbf{f}$ with two constant symbols 0, 1, two one-place function symbols $-$, $^{-1}$, and two binary function symbols $+$, $.$; commutative fields are then Ω-structures (where we give 0^{-1} the default value 0) which satisfy the following axioms

(i) Three axioms as in Ex. 5 that say $+$ is a group operation

(ii) Three axioms saying that $.$ is a group oeration on $F \backslash \{0_F\}$:

a) $\forall v_1 \forall v_2 \forall v_3 [v_1, v_2, v_3 \neq 0 \to (v_1.v_2).v_3 = v_1, (v_2 c v_3)]$

b) $\forall v_1 [v_1 \neq 0 \to v_1.1 = 1.v_1 = v_1]$

c) $\forall v_1 [v_1 \neq 0 \to v_1.v_1^{-1} = v_1^{-1}.v_1 = 1]$

(iii) (Commutativity) $\forall v_1 \forall v_2 [v_1 + v_2 = v_2 + v_1 \wedge v_1.v_2 = v_2.v_1]$

(iv) A sentence expressing distributivity of muliplication over addition (Exercise).

(v) $\neg 0 = 1$ (non-triviality)

Let σ_F be the conjunction of (i)-(v). Then the theory of commutative fields is the deductive closure of σ_F.

Example 10 Commutative fields of characteristic p.

Let $p > 0$. In the language of Example 9, let px abbreviate $x + x + \ldots + x$ (p x's) [It's to be emphasised that the symbol strings 'p' and 'px' are themselves not in L_Ω.] A field **f** is of *characteristic p* if p is the least integer such that for all $x \in F$, $px = 0_F$. One can show that there are fields of characteristic p precisely when p is prime. We can express the above condition by

$$\gamma_p : \quad \forall v_0 p v_0 = 0 \wedge \neg [\forall v_0 2 v_0 = 0 \vee \forall v_0 3 v_0 = 0 \vee \ldots \vee \forall v_0 (p-1) v_0 = 0].$$

Then the theory of fields of characteristic p are axiomatised by $\sigma_F \wedge \gamma_p$.

A field is of *characteristic o* if it's not of any prime characteristic. The theory of such fields is characterised by $\sigma_F \cup \{\neg \gamma_p | p \in \mathbb{N}\}$

Example 11 Theory of groups where all elements have order less than some fixed p. Use the language of Example 5. An element has order n if

$$\mu_n : \quad e = v_0 \circ v_0 \circ \ldots \circ v_0 (n\ v_0's)$$

The theory of such groups is axiomatised by (i)-(iii) of Ex. 5 plus: $\forall v_0 [\mu_1 \vee \mu_2 \vee \mu_3 \ldots \vee \mu_{p-1}]$.

Example 12 Peano's Axioms

These are expressed in the language with symbols for o and the successor operation $'$ and has axioms

(i) $\forall v_0 \neg v_0' = 0$

(ii) $\forall v_0 \forall v_1 (v_0' = v_1' \to v_0 = v_1)$

(iii) If φ is any formula with $v_0 \in FV(\varphi)$ then

$$[\varphi(0) \wedge \forall v_0 (\varphi(v_0) \to \varphi(v_0'))] \to \forall v_0 \varphi(v_0)$$

The latter induction scheme is clearly an infinite group of axioms, one for each such formula φ.

Example 13 Formal number theory: the system Q

This is an important axiomatisation of a number theory. The language contains in addition to 0, $'$, symbols for + and $\times$. The axioms are

Q1 $\forall v_0 \forall v_1 (v_0' = v_1' \to v_0 = v_1)$

Q2 $\forall v_0(v_0' \neq 0)$

Q3 $\forall v_0(v_0 \neq 0 \to \exists v_1(v_0 = v_1'))$

Q4 $\forall v_0(v_0 + 0 = v_0)$

Q5 $\forall v_0 \forall v_1(v_0 + v_1' = (v_0 + v_1)')$

Q6 $\forall v_0(v_0 \times 0 = 0)$

Q7 $\forall v_0 \forall v_1(v_0 \times v_1' = (v_0 \times v_1) + v_0)$

The difference between Q and Peano's axioms is that Q only has a finite number of axioms. The axioms of Q are all true in the standard interpretation of this language:
$\mathbb{N} = \langle \mathbb{N},\ +_{\mathbb{N}},\ \times_{\mathbb{N}},\ 0_{\mathbb{N}},\ {}'_{\mathbb{N}} \rangle$ the natural numbers, and those of PA in $\langle \mathbb{N},\ 0_{\mathbb{N}},\ {}'_{\mathbb{N}} \rangle$.

Example 14 Arithmetic
Arithmetic is the set of sentences true in $\mathbb{N}$ above i.e. $Th(\mathbb{N})$.
Is there a reasonable axiomatisation of arithmetic? We shall see that the answer is no. Given a set of sentences Γ (such as Q above) is there $\Gamma' \supseteq \Gamma$ which is complete? We shall see how we can find such a complete extension. Of course if Γ is inconsistent, there's a trivial way to make Γ complete according to the definition of complete: throw in all sentences. We want to do this in a way that preserves Γ's consistency. Given a consistent set of sentences is it possible to fina a model for it? We shall answer this too in the next chapter.

Exercise 1 Prove some (or all) of the following

(i) $\vdash \forall v_0 \forall v_1(P(v_0, v_1) \to \forall v_0 P(v_0, v_0)$

(ii) $\vdash \neg\exists v_0 \varphi \leftrightarrow \forall v_0 \neg\varphi$

(iii) $\vdash \forall v_0 \varphi \to \forall v_0(\varphi \wedge \psi)$

(iv) $\vdash \forall v_0 \forall v_1[P(v_0, v_1) \to \neg P(v_1, v_0)] \to \forall v_0 \neg P(v_0, v_0)$

(v) $\vdash \forall v_0 P(v_0, v_0) \to \exists v_1 P(v_0, v_1)$

(vi) $\vdash \exists v_1[Q(v_1) \to \forall v_1 Q(v_1)]$

Exercise 2 Prove Lemma 8 iii b).
Exercise 3 Prove the remaining cases of Lemma 9.

Exercise 4 a) $\forall v_1(R(v_1) \to S(v_1)),\ \forall v_1(S(v_1) \to T(v_1)) \vdash \forall v_1(R(v_1) \to T(v)1))$
b) $\forall v_0 \forall v_1(R(v_0, v_1) \to \neg R(v_1, v_0)) \vdash \forall v_1 \neg R(v_1, v_1)$

Exercise 5 a) Let φ, s, t be as in A7. Show
$\vdash (s = t \wedge \varphi(x/v_0, t/v_1)) \to \varphi(s/v_0, s/v_1)$
b) Let u, s, t be terms. Show $\vdash s = t \to u(s/v_0) - u(t/v_0)$

Exercise 6 a) Prove Lemma 11 b).
b) Show $\vdash \forall v_0 \exists v_1)(v_0 = v_1)$

Exercise 7 a) Show that $\vdash \varphi$ iff $\vdash \forall v_i \varphi$
b) Does this mean $\vdash \varphi \leftrightarrow \forall v_i \varphi$?

Exercise 8 Suppose c is a constant that appears nowhere in $\Gamma \cup \{\varphi\}$. If $\Gamma \vdash \varphi(c/v_0)$. Show that $\Gamma \vdash \forall v_i \varphi(v_i/v_0)$ where v_i is a variable not appearing on any line of such a proof. [Hint: This is to be shown, by looking at the proof of $\varphi(c/v_0)$ from Γ. The constant c can't play any dynamical role, so if v_i doesn't appear in any part of the proof, replace c by v_i. This is then a derived rule of a slightly different kind from those previous considered.]

Exercise 9 a) The empty set is consistent
b) If Γ is inconsistent, then for *every* $\psi \in L_\Omega$ $\Gamma \vdash \psi$ and $\Gamma \vdash \neg\psi$.
c) $\{\varphi\}$ is consistent iff $\{\exists v_0 \exists v_1 \ldots \exists v_n \varphi\}$ is consistent. [Hint: for ($\Leftarrow$): suppose $\varphi \vdash \psi$ and $\varphi \vdash \neg\psi$ for some *sentence* ψ.]
d) Γ is consistent iff for every finite $\Gamma_0 \subseteq \Gamma$ is consistent.
e) Suppose Γ, φ are formulae, and $\Gamma \nvdash \neg\varphi$. Show that $\Gamma \cup \{\varphi\}$ is consistent. Conclude that for every consistent Γ, and every φ either $\Gamma \cup \{\varphi\}$ or $\Gamma \cup \{\neg\varphi\}$ is consistent.

Exercise 10 a) Let $T = Th(A)$ for some structure A. Show that T is complete.
b) Show that T is complete iff for every pair of sentences φ, χ if $T \vdash \varphi \wedge \chi$ then $T \vdash \varphi$ or $T \vdash \chi$.

Exercise 11 a) Let T be a theory, then the deductive closure of T is simply $\{\varphi | T \vdash \varphi, \varphi$ a sentence$\}$.
b) If $T = Th(\mathbf{A})$ for some $\mathbf{A}$ then T is deductively closed.

Exercise 12 Try and write down axiomatisations for all groups which have in addition the property that
a) they have less than n elements;
b) no elements have finite order ["Torsion-free groups"];
c) all elements have finite order ["Torsion groups"].

Note Your answers in a), b) may require infinite sets of axioms. The question is, can we find finite sets that will also do the job? [Actually there is no axiomatisation for torsion groups (see Exercise 5.5), but it is instructive to try.]

Exercise 13 Show that the theories in Examples 7 - 9 are incomplete. [However the theory of Example 6 is complete.]

The Completeness Theorem

It's now, at last, possible to prove the first major theorem. It is a converse to the Soundness Theorem, but more than that, it implies that in a language, the universally valid formulae are precisely those provable in our deductive calculus. If in the statement of the theorem, you take Γ to be any of the sets of axioms i the examples of the last section of §3, what you have is, e.g., if Γ is the axioms for groups, that *every sentence that is true in every group is provable in PC from the group axioms.* As a preliminary we prove the following lemma that shows that any consistent theory can be enlarged to a complete theory which is still consistent.

Lemma 5.1 (The Lindenbaum Lemma) *Let $\Gamma \subseteq L_\Omega$ be a consistent theory. Then there is $\Gamma' \supseteq \Gamma$, which is a complete, consistent theory.*

Proof L_Ω is countable. So let $\varphi_1, \varphi_2, \ldots, \varphi_n, \ldots (n \in \mathbb{N})$ enumerate all sentences of the language. We define
$\Gamma_0 \subseteq \Gamma_1 \ldots \subseteq \Gamma_n \subseteq \ldots$ by recursion:

$$\Gamma_0 = \Gamma$$

$$\Gamma_{n+1} = \Gamma_n \cup \{\varphi_{n+1}\} \quad \text{if} \quad \nvdash \neg\varphi_{n+1}$$

$$= \Gamma_n \quad \text{otherwise}$$

Let $\Gamma' = \cup_n \Gamma_n$.
Claim 1 Each Γ_n is consistent.
Proof By induction on n: Γ_0 is consistent, assume Γ_k consistent but Γ_{k+1} not consistent. Then $\Gamma_{k+1} = \Gamma_k \cup \{\varphi_{k+1}\}$. By Exercise 3.9e) Γ_{k+1} is consistent. Contradiction.
Claim 2 Γ' is consistent.
Proof If not then for some finite $\Delta \subseteq \Gamma'$, Δ is inconsistent (Exercise 3.9d)). But for some $k\Delta \subseteq \Gamma_k$. But then Γ_k is inconsistent.
Claim 3 Γ' is complete.
Let φ be an arbitrary sentence. Then φ is φ_{i+1} some i. So if $\Gamma_i \nvdash \neg\varphi_{i+1}$, then $\varphi_{i+1} \in \Gamma'$. So $\Gamma' \vdash \varphi_{i+1}$
But if $\Gamma_i \vdash \neg\varphi_{i+1}$, then $\Gamma' \vdash \neg\varphi_{i+1}$. So Γ' is complete. QED

Theorem 5.2 (The Completeness Theorem for countable languages with equality) *Let $\Gamma \cup \{\varphi\}$ be a set of sentences in L_Ω, and Ω contains (as we've always specified up to now) at most a countable collection of predicate and function symbols. Then*

$$\Gamma \vDash \varphi \quad \textit{implies} \quad \Gamma \vdash \varphi.$$

We establish this as a corollary of the following theorem.

THEOREM 5.3 *Any consistent set of* sentences $\Gamma \subseteq L_\Omega$ *has a model.*

We make a couple of definitions and then outline how the proof goes.

DEFINITION 5.4 *We say that* L_Ω*, is an* extension by constants *of* L_Ω *if* Ω' *is* Ω *together with a collection of new constant symbols alone. We write* $L_\Omega \subseteq_c L_{\Omega'}$.

DEFINITION 5.5 *If* $\Gamma \subseteq L_\Omega$ *is a set of sentences,* $L_\Omega \subseteq_c L_{\Omega'}$, $L_{\Omega'}$ *is also a set of sentences, then* Γ' *is a full extension of* Γ *in* $L_{\Omega'}$
if a) $\Gamma \subseteq \Gamma'$ *b) For all* $\varphi \in L_\Omega$ *with* $FV(\varphi) = \{v_i\}$ *(for some i) and such that* $\Gamma \vdash \exists v_i \varphi$*, there is a constant symbol* $c \in dom f'$ *so that* $\varphi(c/v_i) \in \Gamma'$
(ii) $\Gamma \subseteq L_\Omega$, Γ *a set of sentences, is* full*, if* Γ *is a full extension of itself in* L_Ω.

Thus if Γ' is a full extension of Γ in $L_{\Omega'}$ and φ and c are as in b) $\Gamma' \vdash \exists v_0 \varphi \to \varphi(c/v_0)$. The constant symbol c is called a *Henkin witness* or *constant*.

Example 1 $\forall v_0(v_0 = v_0 0$ is an axiom, A6, so $\vdash \exists v_1(v_1 = v_1)$ by the E-Rule, so if a theory is to have the chance of being full in any language, that language must contain a constant symbol.
Example 2 Let Γ be a theory true in $\mathbb{N} =< \mathbb{N}, +, \times, 0 >$. Let $\mathbb{N}* =< \mathbb{N}, +, \times, 0, 1, 2, \ldots >$. If $\Gamma \vdash \exists v_0 \varphi$ then by Soundness $\Gamma \vDash \exists v_0 \varphi$. But $\mathbb{N}* \vDash \Gamma$ so $\mathbb{N}* \vDash \exists v_0 \varphi$. Suppose $n \in \mathbb{N}$ is such that $\mathbb{N}* \vDash \varphi(m/v_0$. From this we see that if we extend the language for $\mathbb{N}$ to L' say, by adding in the constant symbols $1, 2, \ldots$ and let Γ' be the $Th(\mathbb{N}*)$, then Γ' contains things like $\varphi(n)$. Hence Γ' is a full extension of Γ in L'.
Example 3 The Γ' from Example 2 is not just a full extension of Γ in Γ', but is itself full in L'.

The steps we take in the plan for proving Theorem 3 are:

(A) For any consistent set of sentences $\Delta \subseteq L_\Omega$, there is $\Delta' \supseteq \Delta$, where Δ' is a consistent full extension of Δ in $L_{\Omega'}$, where $L_\Omega \subseteq_c L_{\Omega'}$.

(B) (The Lindenbaum Lemma) For any consistent set of sentences $\Gamma \subseteq L_\Omega$ there is $\Gamma' \supseteq \Gamma$, where $\Gamma' \subseteq L_\Omega$ is a consistent, *complete* set of sentences.

(C) Use (A) and (B) alternately to show for any $\Gamma \subseteq L_\Omega$, a consistent set of sentences, there is a complete, consistent, and full $\Gamma^+ \subseteq L_{\Omega+}$, $\Gamma^+ \supseteq \Gamma$ where $L_\Omega \subseteq_c L_{\Omega+} \supseteq \Gamma^+$.

(D) Show that a complete, consistent, full $\Gamma^+ \subseteq L_{\Omega+}$ has a model.

(E) Using (D) and (C) we conclude if $\Gamma \subseteq L_\Omega$ is a consistent set of sentences then Γ has a model.

LEMMA 5.6 *Let* Δ *be a consistent theory in* L_Ω*. Then there is a consistent full extension of* Δ, Δ'*, in* $L_\Omega \subseteq_c L_{\Omega'}$.

Proof We wish to add constant symbols to $dom\,\mathbf{f}_\Omega$ which will be Henkin witnesses for existential statements of L_Ω. The problem is just to check that we can do this in a way to preserve consistency. Suppose $\langle\varphi_i|i\in\omega\rangle$ is an enumeration of all formulae in L_Ω with one free variable; suppose that the free variable of φ_i is v_{n_i}. Now let

$$\Delta^1 = \{\varphi_i|\Delta\vdash\exists v_{n_i}\varphi_i\}$$

For each $\varphi_i\in\Delta^1$ add a constant symbol c_i to $\mathrm{dom}\,\mathbf{f}_\Omega$. (This defines our new language $L_{n'}$). Let $\Delta' = \Delta\cup\{\varphi(c_i/v_{n_i})|\varphi_i\in\Delta^1\}$. Trivially Δ^1 is a full extension of Δ in $L_{\Omega'}$.

Claim Δ' is consistent.
Proof Suppose not and let $\Delta_0\subseteq\Delta'$ be finite so that for some (any) $\psi\Delta_0\vdash\psi\wedge\neg\psi$. Let $\Delta_0=\Gamma\cup\bar\Delta$ where Γ contains none of the new constants c_i, but $\bar\Delta\subset\{\varphi_i(c_i/v_{n_i})|\varphi_i\in\Delta^1\}$. Let χ be the conjunction of the finitely many formulae in $\bar\Delta$

Then	$\Gamma,\chi\vdash\varphi\wedge\neg\psi$	
i.e.	$\Gamma\vdash\chi\to(\psi\wedge\neg\psi)$.	Deduction Theorem
	$\Gamma\vdash\neg\chi$	Taut. Instance $(P\to(Q\wedge\neg Q))\to\neg P$

Suppose χ is $\varphi_1(c_1/v_n-1)\wedge\varphi_2(c_2/v_{n_k})$ without loss of generality.
Since none of the c_i appear in Γ we apply the derived rule of Exercise 3.8 k times using new variables $v'_1,\ldots,v'_k$ not occurring in Γ or χ to get

$\Gamma\vdash\forall v'_1\ldots\forall v'_k\neg[\varphi_1(v'_1/c_1)\wedge\ldots\wedge\varphi_k(v'_k/c_k)]$ we note that $\varphi_k(v'_k/c_k)$ is the same as $\varphi_k(v'_k/v_{n_k}$
or $\Gamma\vdash\neg\exists v'_1\ldots\exists v'_k[\varphi_1(v'_1/v_{n_1})\wedge\ldots\wedge\varphi_k(v'_k/v_{n_k})]$
or $\Gamma\vdash\neg\exists v_{n_1}\ldots\exists v_{n_k}(\varphi_1\wedge\ldots\wedge\varphi_k)$ by changing variables as in Lemma 3.8(i)
or $\Gamma\vdash\neg[\exists v_{n_1}\varphi_1\wedge\exists v_{n_2}\varphi_2\wedge\ldots\wedge\exists v_{n_k}\varphi_k]$ Discarding unnecessary quantifier using Lemma 3.9 i (d) and ii (c)
or $\Gamma\vdash\neg\exists v_{n_1}\varphi_1\vee\ldots\vee\neg\exists v_{n_k}\varphi_k$ $(*)$
But $\Delta\vdash\exists v_{n_i}\varphi_i$ for all $i\le k$ since each of the φ_i here derives ultimately from Δ^1 This contradicts $(*)$ since $\Gamma\subseteq\Delta$ and this in turn means that our original assumption of Δ' being inconsistent was false.
QED

This completes (A), we now do (C).

Lemma 5.7 *Let $\Gamma\subseteq L_\Omega$ be a consistent set of sentences. There is $L_{\Omega*}$ so that $L_\Omega\subseteq_c L_{\Omega*}$, and there is $\Gamma^*\subseteq\Gamma$, so that Γ^* is a consistent, full, complete set of sentences of $L_{\Omega*}$.*

Proof Use Lemmas 5.1 and 5.6 alternately, countably often, constructing languages $L_{\Omega_n}\subseteq_c L_{\Omega_{n+1}}$, sets of sentences $\Gamma_i\subseteq\Delta_{i+1}\subseteq\Gamma_{i+1}$ with $\Gamma_{i+1}\cup\Delta_{i+1}$ sentences in $L_{\Omega_{i+1}}$. Let $\Omega_1=\Omega,\Gamma_1=\Gamma$. Suppose Ω_n,Γ_n are defined. By lemma 4 choose $L_{\Omega_{n+1}}\supseteq_c L_{\Omega_n}$ and Δ_{n+1} a consistent, full extension of Γ_n in $L_{\Omega_{n+1}}$. By the Lindenbaum lemma, choose Γ_{n+1} a consistent, complete set of sentences containing Δ_{n+1}, in $L_{\Omega_{n+1}}$.
Let $L_{\Omega*}=\bigcup_n L_{\Omega_n}$, and $\Gamma^*=\bigcup_n\Gamma_n$. Clearly $L_\Omega\subseteq_c L_{\Omega*}$, $\Gamma\subseteq\Gamma^*$. Each Γ_n is consistent, and so, as in the proof of the Lindenbaum Lemma, is Γ^*.
Γ^* *is complete*: for if φ is a sentence of $L_{\Omega*}$, and so either $\Gamma_n\vdash\varphi$ or $\Gamma_n\vdash\neg\varphi$. So Γ^* is complete.

Γ^* *is full*: Suppose $\Gamma^* \vdash v_i\varphi$ where $\varphi \in L_{\Omega *}$ with only free variable v_i. For some m, then $\Gamma_m \vdash \exists v_i \varphi$, so there is some new constant c of Ω_{m+1} so that $\varphi(c/v_i) \in \Delta_{m+1} \supseteq \Gamma^*$. QED

This now completes (A), (B), & (C) of our plan. We now have a complete, full, consistent set of sentences Γ^* containing our original consistent Γ. We need a model. Where should we find it? The neat trick here is that we build the model out of the terms of the language $L_{\Omega *}$ itself.

Definition 5.8 *Let $\Gamma \subseteq L_\Omega$ be a consistent set of sentences such that Ω contains at least one constant symbol. The* canonical interpretation determined by Γ *is*

$$I_r = I = \langle I, \langle P_1\rangle_{P\in domr}, \langle F_1\rangle_{F\in domf}\rangle \qquad (\Omega = \langle r, f\rangle)$$

where I is the set of equivalence classes of closed terms, $[t]_-$ of L_Ω for the equivalence relation $\sim$.

$$\begin{array}{rcll} t_1 \sim t_2 & \iff & \Gamma \vdash t_1 = t_2. & \\ P_1([t_1], \ldots, [t_i]) & \iff & \Gamma \vdash P(t_1, \ldots, t_i) & (P \in domr) \\ F_1([t_1], \ldots [t_i]) = [t] & \iff & \Gamma \vdash F(t_1, \ldots, t_i) = t & (F \in domf) \end{array}$$

The properties of completeness and fullness are just what's required to show that the canonical structure determined by Γ is a model of Γ. Notice that if there are no closed terms in the language I would be empty; that is why we stipulate that Ω contain at least one constant symbol. Note also that the $\sim$ is well-defined: we should show that if $t_j \sim t'_j (1 \leq j \leq i)$ then $\Gamma \vdash P(t_1, \ldots, t_i)$ iff $\Gamma \vdash P(t'_1, \ldots, t'_i)$ (and similarly for functions) but this follows by A7 and the definition of $\sim$.

Lemma 5.9 *Let $\Gamma \subseteq L_\Omega$ be a complete, full and consistent set of sentences. Then for each sentence φ of L_Ω* $\quad I_\Gamma \vDash \varphi \iff \Gamma \vdash \varphi$.

Proof Note that as $\vdash \exists v_1(v_1 = v_1)$ for any $R \in \Omega$, fullness of Γ implies there is at least one constant in Ω. Proof is by induction on the complexity of the *sentence*.
φ atomic This is then just part of the definition of canonical interpretation since the denotation of t in I_Γ is $[t]$; for example $\Gamma \vdash t_1 = t_2$ iff $t_1 \sim t_2$ iff $[t_1] = [t_2]$ iff $I_\Gamma \vDash t_1 = t_2$.
φ is $\neg\psi I_\Gamma \vDash \neg\psi$ iff it's not the case that $I \vDash \psi$
iff not $\Gamma \vdash \psi$ by Inductive Hypothesis.
iff $\Gamma \vdash \neg\psi$ as Γ is complete
φ is $\psi \to \chi$ Similar.
φ is $\forall v_m\psi$ *Case 1* $v_m \notin FV(\psi$. Then ψ is a sentence and by Ind.Hyp:
$I_\Gamma \vDash v_m\psi$ iff $I_\Gamma \vDash$ iff $\Gamma \vdash \psi$ iff (by Lemma 3.9iic)) $\Gamma \vdash \forall v_m\psi$
Case 2 $FV(\psi) = \{v_m\}$. then
$I_\Gamma \vDash \varphi$ iff for all valuations $wI_\Gamma \vDash \forall v_m\psi[w]$
iff for all $[t] \in I$ and valuations $wI_\Gamma \vDash \psi[w([t]/m]$
iff for all closed terms t in Γ_Ω and all valuations w
$I_\Gamma \vDash \psi(t/v_m)$ (since every $[t] \in I$ is the denotation of such a term t in Γ_Ω)
iff for all closed terms t in L_Ω
$\Gamma \vdash \psi(t/v_m)$ by Inductive Hypothesis (since now $\psi(t/v_m)$ is a sentence).

Suppose not $\Gamma \vdash \varphi$. Then by completeness $\Gamma \vdash \neg\varphi$ or $\Gamma \vdash \exists v_m \neg\psi$. Γ is full so for some $c \in L_\Omega \Gamma v dash \neg\psi(c/v_m)$. By the equivalence above not $I \vDash \varphi$. Conversely if $\Gamma \vdash \varphi$ then by A4 for all closed terms without variables $\Gamma \vdash \psi(t/v_m)$ so again by the above $I \vDash \varphi$. This completes *Case 2* and induction. QED

Proof of Theorem 5.3: Let $\Gamma \subseteq L_\Omega$ by a consistent set of sentences. By Lemma 5.6 $\exists \Gamma' \supseteq \Gamma, \Gamma \subseteq L_{\Omega'}$ where Γ' is a consistent, complete, full set of sentences. By Lemma 5 $\underline{I}_{\Gamma'}$ is a model Γ'. The *reduct* of $\underline{I}_{\Gamma'}$ to the language L_Ω is a model of Γ of similarity type Ω. QED

Proof of Theorem 5.2 Let Γ, φ, Ω be as stated in the theorem. Suppose not $\Gamma \vdash \varphi$. Then not $\Gamma \vdash \neg\neg\varphi$. By 3.9e) $\Gamma \cup \{\neg\varphi\}$ is consistent and by Theorem 5.2 has a model. thus not $\Gamma \vDash \varphi$ QED

Putting Theorem 5.2 and the Soundness Theorem together gives

Theorem 5.10 *Let $\Gamma \cup \{\varphi\}$ be sentences on L_Ω, where L_Ω is a countable language. Then*

$$\Gamma \vDash \varphi \Longleftrightarrow \Gamma \vdash \varphi$$

Thus formal provability from a set of sentences is as strong a concept as semantic entailment.

Corollary 5.11 *The Theorems of PC are precisely the universally valid formulas.*

Proof Let Γ = fi and φ a formula with $FV(\varphi) \subseteq \{v_1, \ldots, v_n\}$. Then $\forall v_1 \ldots \forall v_n \varphi$ is a sentence. Theorem 6 gives $\vDash \forall v_1 \ldots \varphi$ iff $\vdash \forall v_1 \ldots \varphi$. But φ is universally valid iff $\forall v_1 \ldots \forall v_n \varphi$ is universally valid Ex. 2.4) and $\vdash \varphi$ iff $\vdash \forall v_1 \ldots \forall v_n \varphi$ (by R2 and, A4 with R1). QED

Theorem 5.12 *Since Γ be a consistent set of sentences in L_Ω, a countable language. Then Γ has a countable model.*

Proof In Lemma 5.6 each of the languages $L_{\Omega_{n+1}}$ was obtained by adding countably many constants to dom *f*; thus by induction each L_{Ω_n} is countable. Thus $L_{\Omega *} = \cup L_{\Omega_n}$ is also countable. The canonical interpretation uses equivalence classes of terms of $L_{\Omega *}$, of which there are only countably many, and so is itself countable. QED

Remark (1) There are generalisations of theorem 3.3 to uncountable languages, but then the models may have to be uncountable too.
Remark (2) Theorems 5.2, 5.3 are due to Gödel (1930). The proof here is due to Henkin.
Exercise 1 Let T_0 and T_i be theories in L_Ω such that for any interpretation **A** of L_Ω.
$\mathbf{A} \vDash T_0$ iff $\mathbf{A} \nvDash T_1$. Show that both T_0 and T_1 are finitely axiomatisable.
Exercise 2 (Very similar to Ex.1). Let T_0 and T_1 be theories such that nothing is a model of both T_0 and T_1. Show that there is a sentence φ so that

$$\forall \mathbf{A}[(\mathbf{A} \vDash T_0 \Rightarrow \mathbf{A} \vDash \varphi) \wedge (\mathbf{A} \vDash T_1 \Rightarrow \mathbf{A} \vdash \neg\varphi)].$$

The Compactness and Löwenheim Skolem Theorems

The theorems of the title are corollaries of the Completeness Theorem.

Theorem 6.1 (The Downward Löwenheim-Skolem Theorem) *Let $\Gamma \subseteq L_\Omega$ be a set of sentences in a countable language with equality. If Γ has a model then Γ has a countable model.*

Proof If Γ has a model then Γ is consistent. Theorem 4.8 gives the conclusion. QED

Example 1 Let $\mathbb{R} = \langle \mathbb{R}, +_{\mathbb{R}}, \times_{\mathbb{R}}, -1_{\mathbb{R}}, 0_{\mathbb{R}} \rangle$ be the fields of the reals. Let $\Gamma = Th(\mathbb{R})$. Then Γ is countable. By Theorem 4.9 Γ has a countable model $\mathbb{R}^*$, and by design $Th(\mathbb{R}^*) = Th(\mathbb{R})$. *Conclusion*: any theorem about the reals as a field doesn't depend in any essential way on the uncountability of $\mathbb{R}$.
In the above we can in fact arrange for $\mathbb{R}^* \subseteq \mathbb{R}$ (although Theorem 1 doesn't give us this).
Example 2 The underlying foundation of mathematics is the theory of sets. This is expressed using a countable set of axioms, called ZF, in a countable language with equality and a single binary relation symbol which is used to denote set membership. From these axioms any theorem about sets that mathematicians (normally) need can be devised: e.g. the usual construction of the reals from the rationals can be couched in terms of this basic set theory. A *model* for the axioms is a collection,**M**, of sets which satisfy the axioms.
Theorem 1 then gives us the following "paradoxical" fact: If **M** is a model of the axioms, then the axioms are consistent. So there is a countable model $\mathbf{M}^*$ of the axioms. But then as the existence of the set of reals is a theorem of ZF
ZF$\vdash$ $(\exists x)(x$ is the set of real numbers). Further $ZF \vdash$ (the reals are uncountable), since the axioms prove also that the reasl are uncountable (our usual Cantor diagonal argument). This was the so-called *Skolem Paradox*. $\mathbf{M}^*$ thinks its collection of real numbers is uncountable. But $\mathbf{M}^*$ is itself countable! The point is simply that the interpretation $\underline{M^*}$ does not have a function $f \in \mathbf{M}^*$ which is a bijection between its reals and its natural numbers. We know "from outside" there is an f *outside* $\mathbf{M}^*$! The next theorem is probably the most important result for applications in mathematics, and the theory of models that we've been developing.

Theorem 6.2 (The Compactness Theorem; Mal'cev, 1936) *Let L_Ω be a countable language. Let $\Gamma \subseteq L_\Omega$ be a set of sentences. Γ has a model iff every finite $\Gamma_0 \subseteq \Gamma$ has a model.*

Proof ($\rightarrow$) If Γ has a model then trivially so does every finite $\Gamma_0 \subseteq \Gamma$. ($\rightarrow$) Suppose however Γ has no model. By Theorem 4.3 Γ is inconsistent. So some finite subset $\Gamma_0 \subseteq \Gamma$ is also inconsistent; and thus cannot have a model QED

Remark (1) Note the theorem as stated is formulated using only semantic concepts. Although the proof via the Completeness Theorem relates semantic and syntactic concepts, purely semantic proofs without reference to deductive systems are possible. Note also that the proof is entirely non-constructive k(as opposed to that for propositional languages): given models for all finite subsets, there's no way to string them together to get a model for all of Γ.
Remark (2) Again the theorem is true even if L_Ω doesn't have equality. It is also true if we have uncountable languages.
The applications of Compactness are legion. The following shows that elementary equivalence, $\equiv$, and $\cong$, isomorphism are different, in a very striking way.

Definition 6.3 *Let* **A,B** *be two* Ω*-structures, and* $h : \mathbf{A} \to \mathbf{B}$ *an embedding. Then* h *is an* elementary embedding *if for all formulae all valuations* $w \in \mathbf{W}^{\mathbf{A}}$

$$A \vDash \varphi[w] \quad \Longleftrightarrow \quad \mathbf{B} \vDash \varphi[h(w)]$$

where $h(w) \in \mathbf{W}^{\mathbf{B}}$ *is such that* $h(w)(j) = h(w(j))$

Remark If $h : \mathbf{A} \to \mathbf{B}$ is an elementary embedding then $\mathbf{A} \equiv \mathbf{B}$. Note that h is not necessarily onto

Theorem 6.4 (Elementary Extension Theorem) *Let A be a countable interpretation of* L_Ω. *Then there is* $h, \mathbf{B}$ *such that* $h : \mathbf{A} \to \mathbf{B}$ *is an elementary embedding, but* h *is not onto.*

Proof Since **A** is countable let $a_1, a_2, \ldots$ enumerate it's elements. Expand f_Ω to $\mathbf{f}_{\Omega^+}$ by adding new constant symbols $c_1, c_2, \ldots$ and let $\mathbf{A}^+$ be the structure **A** with now each element a_i of A interpreting c_i.
$Th(\mathbf{A}^+)$ now contains all the "facts" true of any element in A. $Th(\mathbf{A}^+$ is a countable consistent theory in L_{Ω^+}. Now enlarge f_{Ω^+} to $\mathbf{F}_{\Omega^1}$ by adding another new constant d. Let $\Gamma = Th(\mathbf{A}^+) \cup \{c_n \neq d | n \in \mathbb{N}\}$
Claim Every finite subset of Γ has a model.
Proof Since if $\Gamma_0 \subseteq \Gamma$ is finite, there is a largest $m-1$ so that c_{m-1} occurs in Γ_0. We claim

$$\mathbf{A} = \langle A, \langle R_{\mathbf{A}} \rangle_{R \in \mathrm{dom}\, \mathbf{r}}, \langle F_{\mathbf{A}} \rangle_{F \in \mathrm{dom}\, f}, a_1, a_2, \ldots, a_m \rangle \vDash \Gamma_0$$

All the sentences of $Th(\mathbf{A}^+)$ in Γ_0 are true in this structure, and by interpreting d as a_m we ensure all the "$c_n \neq d''$ formulae in Γ_0 are also true. QED Claim
By the Claim, and the Compactness Theorem, Γ has a model $\mathbf{B}'$. Let $\mathbf{B}'$ have domain B. Let $\mathbf{B}^+$ be the reduct of $\mathbf{B}'$ to $L_{\Omega+}$, let b_n interpret c_n.
Let h be given by sending a_n to $b_n \in B$

$$h(a_n) = b_n$$

Since $\mathbf{B}^+ \vDash Th(\mathbf{A}^+)$, for every sentence φ of $Th(\mathbf{A}^+)\mathbf{B}^+ \vDash \varphi$
φ mentions constants $c_1, \ldots, c_n$ say (which in $\mathbf{A}^+$ were interpreted as $a_1, \ldots, a_n$). Thus, everything that in **A** was true of $a_1, \ldots, a_n$ is true in **B** of $b_1, \ldots, b_n$; the ideas is that $\{b_i | i \in \mathbb{N}\}$ is a subset of **B** that is isomorphic to **A**. Formally we
Claim $h : A^+ \to B^+$ is an embedding.
Proof Check the clauses of the definitions 2.4 and 2.5, e.g. for $f \in \mathrm{dom} f_{\Omega^+}$

$$F_{A^+}(a_1,\ldots,a_{\mathbf{f}(F)}) = F_{B^+ +}(h(a_1),\ldots,h(a_{\mathbf{f}(F)})) = h(a) \qquad \text{et cetera}$$

Claim h is not onto.
This is because B contains a constant to interpret d and for all $n\mathbf{B}' \vDash c_n \neq d''$
Claim h is an elementary embedding of $\mathbf{A} \to \mathbf{B}$
Let $w \in W^A$ and let us suppose $\mathbf{A} \vDash \varphi[w]$. Suppose $w(i) = a_{j_i}(0 \leq i \leq n)$ then $\varphi(c_{j_0}/v_0),\ldots,(c_{j_n}/v_n)$ is a sentence of L_{Ω^+}, true in $\mathbf{A}^+$ and so true in $\mathbf{B}^+$. Since $h(a_{j_i}) = b_{j_i}$ we have $\mathbf{B} \vDash \varphi[h(w)]$ QED
What the impact of the theorem is, is that $h[\underline{A}]$ is a substructure of $\mathbf{B}$, isomorphic to A, but such that $\mathbf{B}$ nothing is true of elements of $h[A]$ that wasn't already true in $h[\underline{A}]$ itself. If as is usual we identify $\mathbf{A}$ with $h[A]$ we can think of $\mathbf{B}$ containing $\mathbf{A}$.
A particular example illustrates this technique.
Example 3 A non-standard model of arithmetic.
Let $\mathbb{N} = \langle \mathbb{N}, +_{\mathbb{N}}, 0_{\mathbb{N}}, ' \rangle$ be the standard natural numbers. We construct $\mathbb{N}^* \vDash Th(\mathbb{N})$ but $\mathbb{N}^* \ncong \mathbb{N}$.
Notice that in $\mathbb{N}$ by good luck every element of the domain happens to be definable by a term in the language, 3 for example is the interpretation of $0''$. Let $\Omega' \supseteq \Omega$ be given by adding one new constant symbol c to $\underline{\text{dom}f}_{\Omega}$.
φ_n be the sentence in $L_{\Omega'}$: $0 \underbrace{''\ldots'}_{\text{n times}} \neq c$
Let $\Gamma = Th(\mathbb{N}) \cup \{\varphi_n | n \in \mathbb{N}\}$
Claim Any finite subset $\Gamma_0 \subseteq \Gamma$ is consistent.
Proof Given Γ_0 pick m sufficiently large so that any $0\underbrace{''\ldots'}_{\text{n}}$ appearing in Γ_0 has $n < m$.
Then: $\mathbb{N}' = \langle \mathbb{N}, +_{\mathbb{N}}, \times_{\mathbb{N}}, 0_{\mathbb{N}}, '_{\mathbb{N}}, m \rangle \vDash \Gamma_0$ where now m interprets c : m is large enough so that any $\varphi_n \in \Gamma_0$ is satisfied with c interpreted as m. QED Claim.
By the Compactness Theorem Γ has a model $\mathbb{N}^*$ say.
Let $\mathbb{N}^* = \mathbb{N}^*|\Omega$ i.e. $\mathbb{N}^* = \langle \mathbb{N}^*, +_{\mathbb{N}^*}, \times_{\mathbb{N}^*}, 0_{\mathbb{N}^*}, '_{\mathbb{N}^*} \rangle$
Claim $\mathbb{N}^* \ncong \mathbb{N}$.
Proof This is because every element of $\mathbb{N}$ is of the form $0''\cdots'_{\mathbb{N}}$.
but this is false in $\mathbb{N}^*$: the element that interpreted c, $c_{\mathbb{N}^*}$, differs from all the
$0''\cdots'_{\mathbb{N}^*}$
but $\mathbb{N}^* \vDash Th(\mathbb{N})$. i.e. every statement of arithmetic is true in $\mathbb{N}^*$.

Definition 6.5 *For $n \in \mathbb{N}$, let* $\mathbf{n}$ *abbreviate* $0\underbrace{''\ldots'}_{n}$.

Notice that we can define $<$ by the formula $v_0 < v_1 \longleftrightarrow \exists v_2(v_1 = v_0 + v_2 \wedge v_2 \neq 0)$. Call an element of $\mathbb{N}^*$ *standard* if it is of the form $n_{\mathbb{N}^*}$. Otherwise call it *non-standard*.
The Compactness Theorem also tells us much about how the cardinalities of models can or cannot be characterised.

Theorem 6.6 *Let $\Gamma \subseteq L_\Omega$ be a theory with arbitrarily large finite models then Γ has an infinite model.*

Proof Find a sentence σ_n so that $\mathbf{A} \vDash \sigma_n iff |A| \geq n$
Let $\Delta = \{\sigma_n | n \in \mathbb{N}\} \cup \Gamma$.
Claim Every finite subset $\Delta_0 \subseteq \Delta$ has a model
Proof Δ_0 can only contain finitely many $\sigma_n's$. Let m be larger than any n so that $\sigma_n \in \Delta_0$.
Let A' be a model of Γ of size $\geq m$. Then $\mathbf{A}' \vDash \Delta_0$. QED Claim
by Compactness Δ has a model $\mathbf{B}$ say. Since for all $n\mathbf{B} \vDash \sigma_n|B|$ is infinite. QED
Thus *finiteness* alone cannot be characterised by any set of sentences. In particular there is no set of sentences Σ such that G is a finite group $iff \mathbf{G} \vDash \Sigma$.
Theorem 4 shows that finiteness cannot be characterised by a set of sentences, but the set $\{\sigma_n | n \in \mathbb{N}\}$ does show that an infinite set of sentences suffices to characterise being infinite.

Definition 6.7 *We say a property P of models is* finitely axiomatisable *if there is a finite set of sentences in a language, Σ, say so that*

$$\mathbf{A} \vDash \Sigma \textit{ iff } \mathbf{A} \textit{ has } P.$$

Remark This ties in with Definition 3.8b) of a theory being finitely axiomatisable; let T be a theory then suppose the property of being a model of T is axiomatisable by the finite T_0 say. Then the models of T_0 are precisely the models of T. Then T is also finitely axiomatisable by the same T_0 : since $T \vdash \delta \Leftrightarrow T \vDash T_0 \vDash \delta \Leftrightarrow T_0 \vdash \delta$, using Completeness and Soundness Theorems. Conversely if a theory T is finitely axiomatisable by some finite T_0 say, then the property of being a model of T is finitely axiomatisable by the same T_0 : since $T \vdash \sigma_0$ for all $\sigma_0 \in T_0$ and $T_0 \vdash \sigma$ for all $\sigma \in T$, we have just by Soundness, $\mathbf{A} \vDash T_0 \Leftrightarrow \mathbf{A} \vDash T$. Thus: The property of being a model of a theory T is finitely axiomatisable iff the theory is finitely axiomatisable. Thus the property of being a group, or a field of γ_p, or of being a strict partial order are all finitely axiomatisable [see Examples 3.5, 10, 7].

Remark We have shown here that two theories T, T' axiomatise each other precisely when they have the same models.
Example 4 The property of being a strict total order, is finitely axiomatisable.
Let σ be the conjunction of the two sentences of Example 3.7 together with

$$\forall v_0 \forall v_1 [v_0 = v_1 \vee R(v_0, v_1) \vee R(v_1, v_0)]$$

Example 5 The property of being a strict total order, with a largest element, and such that each element with a "<-predecessor" has an immediate predecessor is finitely axiomatisable.
Let τ be σ of Example 4 together with

$$\forall v_0 [\exists v_1 R(v_1, v_0) \rightarrow \exists v_2 (R(v_2, v_0) \wedge \forall v_3 (\neg (R(v_2, v_3) \wedge R(v_3, v_0))))] \wedge$$

$$\wedge \exists v_0 \forall v_1 [v_0 \neq v_1 \rightarrow R(v_1, v_0)]$$

Lemma 6.8 *The property of being a well-ordered set is not characterised by any set of sentences.*

Proof The τ of Example 5 has arbitrarily large finite well ordered models but no infinite well ordered models. but τ must be true in any finite well ordered model. Suppose Σ were such that $\mathbf{A} \vDash \Sigma iff \mathbf{A}$ was well ordered by $R_{\underline{A}}$. Then $\Sigma \cup \{\tau\}$ has arbitrarily large finite models and hence by Theorem 4 an infinite one! Contradiction. [Since if $c \in A$ were the largest element c must have infinitely many $R_{\underline{A}}$ predecessors. but τ ensures that $R_{\underline{A}}$ an isomorphic copy of the negative integers.] QED

The remark after example 3.10 shows that the theory of fields of characteristic 0 has an inifinite set T of axioms. That doesn't settle the question of whether perhaps there is some *finite* set T_0 of axioms such that for all sentences φ in that language $T_0 \vdash \varphi \Leftrightarrow T \vdash \varphi$ (or equivalent φ is true in every such field $iff\varphi$ is true in every model of T_0 - note the use of Completeness and Soundness to state these equivalences). The following lemma essentially shows that this theory is *not* finitely axiomatisable.

Lemma 6.9 *Let φ be a sentence of the language of fields, and suppose T is as above. If $T \vDash \varphi$ then there is an n such that φ is true in every field of characteristic $\geq n$. Hence the theory of fields of characteristic* 0 *is not finitely axiomatisable.*

Proof before proving the first sentence let us see how this kills off any hope of finitely axiomatising fields of characteristic 0. Suppose T_0 is finite but is such that T and T_0 have the same consequences. Let φ be the conjunction of T_0. φ is true in fields with non-zero characteristic by Lemma 6! Let $\mathbf{F}$ be such a field. Since every $\psi \in T$ is such that $T \vdash \psi(T \quad \text{and} \quad T_0$ have the same consequences) $\mathbf{F} \vDash T$. So $\mathbf{F}$ has 0 characteristic! Contradiction. So let us turn to the first sentence.

(1st Proof) Let $T \vDash \varphi$ but suppose for no n is φ true in all fields of characteristic $\geq n$. Then let S be any finite subset of $T \cup \{\neg\varphi\}$ S only mentions finitely many of the formulae $\neg\gamma_p$. Let p_0 be greater than any of these $p's$. Then S is true in *some* field of characteristic $\geq p_0$. by the Compactness Theorem $T \cup \{\neg\varphi\}$ has a model. This contradicts $T \vDash \varphi$ (2nd Proof) [The first proof showed the *existence* only of such an n, this proof shows how to compute such an n].

Since $T \vDash \varphi$ by the Completeness Theorem $T \vdash \varphi$. Look at a proof of φ from T. This only uses a finite number of the formulae $\neg\gamma_p$. Let n be the least integer strictly greater than these $p's$. Then φ is true in any field of characteristic $\geq n$: Since $\sigma_F, \{\neg\gamma_p | p < n\} \vdash \varphi$ which implies $\sigma_F, \{\neg\gamma_p | p < n\} \vDash \varphi$ by the Soundness Theorem. QED

Example 4 Let T be the theory that contains the three axioms for groups plus the set $\{\wedge v_0 \neg[\mu_1 \vee \mu_2 \ldots \vee \mu_n] | n \in \mathbb{N}\}$, where μ_n is the formula that "says" v_0 has order $\leq n$. Models of this theory are the torsion-free groups (and so must be infinite (why?).) This theory is also not finitely axiomatisable: Suppose T_0 is finite and both T and T_0 have the same consequences, for a contradiction. By the remark after Example 3 this is equivalent to T and T_0 having the same models. However:

Claim If φ is a sentence in the language of group theory and $T \vDash \varphi$ then there is an $n \in \mathbb{N}$ so that φ is true in every group $\mathbf{G}$ whose elements all have order greater than or equal to n.

If the claim is true then T_0 cannot axiomatise T : let γ be the conjunction of the finitely many axioms of T_0, then $\vDash \gamma$ (since T and T_0 have the same consequences.) By the claim, for some $n\gamma$ is true in any group $\mathbf{G}$ all of whose elements have order $\geq n$ and such groups exist which are finite: for example, let p be a prime $\geq n$, then the cyclic group $\mathbb{Z}_p$ has every element of order precisely p. So $\mathbb{Z}_p \vDash \gamma$, but no

element of $\mathbb{Z}_p$ has infinite order. To prove the claim let $T \vDash \varphi$ be any finite subset of $T \cup \{\neg\varphi\}$; S only mentions finitely many of the formulae $\forall v_0 \neg[\mu_1 \vee \mu_2 \ldots \vee \mu_n]$. Let k be a number greater than any of the n's occurring here. By supposition there is a group **G** all of whose elements have order $\geq$ is false. Then S is true in **G**. by the Compactness Theorem $T \cup \{\neg\varphi\}$ has a model. This contradicts $T \vDash \varphi$.

Exercise 1 Think a bit more about what the ordered structure of $\mathbb{N}^*$ looks like: let $a \in \mathbb{N}^*$ be the interpretation of the named constant c. Clearly for every $n 0 \underbrace{''\ldots'}_{n} < c$ is true in $\mathbb{N}^*$.

(a) Prove that for any non-standard $d \in \mathbb{N}^*$ there exists a smaller non-standard $c < d$, . (The first part shows that, unlike $\mathbb{N}$, $\mathbb{N}^*$ will have an infinite <-descending chain of elements.)
b) Prove that the elements of $\mathbb{N}^*$ are linearly ordered.
Define an equivalence relation $\sim$ on $\mathbb{N}^*$ by $c - d \; iff \; c = d + e$ where e is a standard element, or $d = c + e$. Thus elements in the same equivalence class or "block" are only a "finite" distance from each other, and can be obtained one from the other by a finite number of applications of '. Thus the standard elements are all in one block,
c) Prove that the blocks are linearly ordered by $[c] \leq [d] \quad iff$ we define $[c] \leq [d]$ by $c + e = d$ for some element e. [To argue that this is a good definition you have to show that if $c' \in [c]$ and $d' \in [d]$ that $c' + e' = d'$ for some e', i.e. if one element of our block $[c]$, is less than one element of another block $[d]$, then the same is true for all elements in $[c]$ and in $[d]$.]
d) Show that there is no <-least non-standard block.
[Hint: Let d be non-standard and even. Then $d = c + c$. Show that c is non-standard and $[c] < [d]$.]
e)* Show that if $[c]$ and $[d]$ are two different blocks, then there is a block $[e]$ with $[c] < [e] < [d]$.
[Hint: Either $c + d$ or $c + d + 1$ is even; suppose $c + d$ is and consider $(c + d)/2$]
$\mathbb{N}^*$ thus consists of the standard block, order isomorphic to $\mathbb{N}$, followed by countably many blocks, $[c]$ above, such that each block is order-isomorphic to $\mathbb{Z}$, but such that the blocks are linearly ordered, without least (Part d)) or greatest (similar to d)) element, and such that the ordering is dense (part e); i.e. the ordering of blocks looks like the rationals $\mathbb{Q}$.
Remark The existence of such an $\mathbb{N}^*$ was shown by Skolem (1934). Much studied in contemporary logic are similar nonstandard models of the Peano Axioms.

Exercise 2 Let σ be a sentence true in all infinite models of a theory Γ. Show that there exists $k \in \mathbb{N}$ so that for any model **A**, if $|A| \geq k$ *and* $\mathbf{A} \vDash \Gamma$ then $A \vDash \sigma$.
Exercise 3 Find a language, and a sentence σ in that language so that if $\mathbf{A} \vDash \sigma$ then $|A|$ is infinite.
Exercise 4 Show that the property of having an infinite domain is not finitely axiomatisable. [Note this doesn't contradict Ex.3.]
Exercise 5 Show that the theory of torsion groups is not axiomatisable. [Hint: Suppose Γ axiomatised this theory and show $\Gamma \cup T$ (where T is as in Example 4 p.89) has a model.
Exercise 6* Show that the theory of algebraically closed fields of characteristic 0 is not finitely axiomatisable.
Exercise 7* Show that the theory of algebraically closed fields of characteristic $p > 0$ is not finitely axiomatisable.
[**Hint** (Exercises 6 and 7) A field is algebraically closed if every polynomial in one indeterminate x, say with coefficients in the field, has a root. We thus need to have solutions to $a_n x^n + \ldots + a_1 x + a_0 = 0$. So consider, for Ex.6, in addition to $\sigma_F \cup \{\neg\gamma_p | p \in \mathbb{N}\}$, all sentences of the form

$$\forall v_0 \forall v_1 \ldots \forall v_n \exists v_{n+1} [v_n . v^{n_{n+1}} + v_{n-1} v^{n-1_{n+1}} + \ldots v_1 . v_{n+1} + v_0 = 0]$$

where as always v^{n_i} abbreviates $v_i . v_i . v_{i\ldots} . v_i$ (n times). Then give the fact (which you shouldn't prove) that for a given characteristic p, for any n there is a non-algebraically closed field of characteristic p in which all polynomials of degree $\leq n$ have a root. 7 follows in the same way as 6.]

Exercise 8 Let L_Ω be the language of fields, but with an extra binary predicate R added to $domr_\Omega$. The theory of *ordered fields* is the deductive closure of σ_F together with

(i) $\forall v_0 \forall v_1 [R(v_0, v_1) \vee R(v_1, v_0) \vee v_0 = v_1]$

(ii) $\forall v_0 \forall v_1 \forall v_2 [R(v_0, v_1) \wedge R(v_1, v_2) \to R(v_0, v_2 0]$

(iii) $\forall v_0 \neg R(v_0, v_0$

(iv) $\forall v_0 \forall v_1 \forall v_2 [R(v_0, v_1) \to R(v_0 + v_2, v_1 + v_2)]$

R is thus intended to be a strict linear order with an additivity property (iv). Show that there are non-Archimedean models of this theory: i.e. there are models with elements c, d such that for no natural number n is $d < c + c + \ldots + c$ (n times), writing $<$ for R.

Exercise 9* The theory of *ordered abelian groups* is the deductive closure of axioms for abelian groups plus (i)-(iv) of Exercise 8. One can show that every such group is torsion free. [Suppose $c \neq 0$ in the group, then $c < 0$ or $c > 0$. Suppose $c > 0$ then $c + c > c + 0 = c > 0$ similarly $c + C + c > c + c > 0$ etc. Likewise if $c < 0$ then $n.c. < 0$].
Show that if a countable abelian group is torsion free then it can be ordered. i.e. we can find a relation $<$ to add to the group structure so that $<$ obeys (i)-(iv) above.
[Hint: First show a finitely generated torsion free abelian group can be so ordered. Such groups, if they have n generators, look like $\mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$ (n times) i.e. every element is of the form
$x = m_1 g_1 + m_2 g_2 + \ldots + m_n g_n \quad (m_i \in \mathbb{Z})$ where $\{g_1, \ldots g_n\}$ is the set of generators for the group. If
$y = m'_1 g_1 + \ldots \quad + m'_n g_n$ put $x < y$ if $\langle m_1, \ldots m_n \rangle < \langle m'_1, \ldots, m'_n \rangle$
lexicographically (i.e. the least $i \leq n$ so that $m_i \neq m'_i$ has $m_I < m'_i$). Check that this works. Now let $\mathbf{A}$ be any countable torsion free abelian group.
Let Ω be a similarity type for the language of ordered groups together with an infinite set of constants $c_1, c_2, \ldots, c_n \ldots (n \in \mathbb{N})$ to name all the elements $a_1, a_2, \ldots, a_n, \ldots$ of A (as A is countable). Then

$$\mathbf{A}^+ = (A, +_\mathbf{A}, -_\mathbf{A}, 0_\mathbf{A}, \langle a_i \rangle i \in \mathbb{N}\rangle \quad \text{interprets} \quad L_\Omega$$

Let $T = \{\sigma \in Th(\mathbf{A}^+) | \sigma \text{ atomic } \}$ in this language and let Γ be T together with (i)-(iv) above and the group axioms. Then every finite subset of Γ has a model.]

Exercise 10* (This involves some topological concepts) Let $\mathcal{M}$ be the class of all interpretations of L_Ω for some fixed Ω. For each sentence φ in L_Ω. Let $U_\phi = \{\mathbf{A} \in \mathcal{M} | \mathbf{A} \vDash \varphi\}$. Let $\mathcal{M}$ generated by the basis $\{U_\phi | \varphi$ a sentence of $L_\Omega\}$. Show that $\langle \mathcal{M}, \mathcal{U} \rangle$ being a compact space is equivalent to the Compactness Theorem for L_Ω.

The Incompleteness of Number Theory

This chapter deals with two particular theories, arithmetic and the formal number theory Q. Arithmetic is defined as the set of all sentences true in the structure $\mathbb{N} = \langle \mathbb{N}, +_{\mathbb{N}}, \times_{\mathbb{N}}, 0_{\mathbb{N}}, '_{\mathbb{N}} \rangle$ ($Th(\mathbb{N})$ in our earlier notation). We shall see that there is no formula which defines in $\mathbb{N}$ the set of code numbers of arithmetic. This is Tarski's theorem on the undefinability of truth. We shall prove something much stronger by showing that arithmetic is "essentially unaxiomatisable", that is there is no finite or even effectively decidable set of axioms T so that every statement of arithmetic is provable from T. We shall do this by showing that the theory Q is "essentially incomplete". It is incomplete in the sense that here is a sentence in the language of number theory φ say so that neither $Q \vdash \varphi$ nor $Q \vdash \neg\varphi$. This is quite easy to show. What is remarkable is the result of Gödel that says for any finite set of axioms $T \supseteq Q$ if T is consistent, there will always be some φ (depending on T) so that T neither proves φ nor $\neg\varphi$. But Q is essentially incomplete in the sense that there is no effectively decidable, consistent set of axioms $T \supseteq Q$ such that for every ψ, $T \vdash \psi$ or $T \vdash \neg\psi$. Thus for every such set of axioms $T \supseteq Q$ there will be sentences of arithmetic which are not provable from T. To phrase it more loosely: no effectively given axiom system constaining Q is sufficient to deduce all the truths about $\mathbb{N}$.

As spinoff from this result we obtain that there can be no computable "algorithm" for deciding which statements of number theory are true.

In the first section we discuss the notions of computability and recursiveness, essentially to continue our argument that all the notions of our formal deductive system could be carried out on a computer, (or, more explicitly using *recursive functions*). We also look at the "diagonalisation" of a formula, this will be used to build a self referential statement rather like Epimenides' Liar Paradox "This statement is false".

In §7.2 we look against at Q, show that it too has very concrete non-standard models, and argue that every recursive function is "representable in Q". §7.3 gives the heart of Gödel's arguement, the diagonal lemma that will yield Incompleteness.

7.1 Arithmetisation of Syntax : Gödel's numbers, Diagonalisation

We have made a number of remarks concerning the possibility of "making effective" various of the syntactic notions we've discussed. The purpose of first part of this section is to tie some of these remarks together. For the particular language of the formal number theory Q (this is the language of Example 2.5 which we shall call L for the rest of this chapter) we give a set of code numbers for the syntax of the language, and in this context they are known as Gödel numbers (or gn).

Definition 7.1 (Gödel numbers of symbols)

Symbol	(	)	→	¬	∀	0	′	+	×	=
gn	1	2	3	4	49	6	68	688	6888	7
Symbol		x	y	z	v_3	v_4	....			
gn		5	59	599	5999	59999	...			

Given this system formulae may be coded as numbers, and a number may be decoded into a formula. Notice that if we wanted to consider countable languages with additional relation or function symbols we can use the 78 and 68 series to code these up. For readability we use x, y, and z as shorthand for v_0, v_1, and v_2.

Example 1 $\exists x\, y = (x + x)$ is officially

$$(\neg\forall x(\neg y = (x + x)))$$

and so has code 1449514597156885222.

Example 2 4951449591414597568886222 codes $\forall x(\neg\forall y(\neg(\neg(y = (x\times)))$.

Now the terms t in our language L are built up from our constant symbols, variables and function symbols, namely, $0, v_i, +, \times, '$. We claim there would be no problem to write a programme to test whether a number was the gn of a *term*. We simply test that it is built up in the correct way from the correct components, has the right number of left and right brackets etc., etc. For examplke 166868886682688 doesn't code a term, whilst the same string with another 1 at the front and 668682 appended to the rear does. We say that being a term of L is *effectively decidable*, because we we have effective (=computerisable) algorithm for testing whether its gn codes a term or not.
As we have noted in earlier chapters all of our syntactic concepts of our formal system are also effectively decidable. From testing numbers to see whether they are gn's of terms it's a short step to testing numbers to see if they're gn's of formulae L, sentences of L, to see whether "the gn of φ' comes from the gn of φ by replacing some (possibly none) occurrences of ψ in φ by χ". i.e. to test whether $\mathrm{Rep}(\psi, \chi, \varphi, \varphi')$. So

Proposition 7.2 *Being a term/formulae/sentence of L is effectively decidable as is* $\mathrm{Rep}(\psi, \chi, \varphi, \varphi')$.

The following is somewhat more sophisticated but the ideas are essentially no different: we can test whether a formula is one of the axioms A1-A7. For A1-A3, A6, A7 this isn't so hard: first test whether the components are formulae (or in the case of A7 atomic formulae). For A4 we have to write a programme to test whether a term is substitutable in a formula, but given the recursive nature of Definition 2.6 this isn't problematic. We then test our putative instance of A4 to see if it's right shape, test that t has been properly substituted etc. A5 is no different, even easier.
Given that we can test a formula for being an axiom of PC, and given also that we can test whether a formula is one of Q1-Q7 (this is easy: there are finitely many axioms of Q) we now have the possibility of testing whether a *string* of formulae, $\varphi_1, \ldots, \varphi_n$ is a properly constituted *proof* of φ_n from Q; we test first if φ_1 is a formula, then if it's one of A1-A7 or Q1-Q7; do the same for φ_2, or see if φ_2 arose by applying R2 to φ_1; then test $\varphi_3, \ldots$ at each stage testing for formulahood, axiomhood, or being derived from an earlier formula on the list. And so on right through to φ_n. Thus *given* a purported proof of φ_n we can

indeed check effectively whether φ_n is a theorem of Q. Note this is *not* the same as being given φ_n out of the blue and being asked "is φ_n" a theorem of Q?" (or in other words "is $Q \vdash \varphi_n$ true?"). This latter situation lies at the heart of our problem, we shall be able to see that there's no effective way in general to test whether an arbitrary φ is a theorem of Q or not. We can only check a "proof's" correctness when given one. All in all, by working with gn's:

Proposition 7.3 *We can effectively decide whether a given formula is an axiom of Q or is one of A1-A7. We can effectively decide given a list of strings of symbols, if it constitutes a properly constructed proof from Q of the last string in the list.*

Actually we can be far more precise about this idea of effectively decidable through the notion of "recursive function"

Definition 7.4 (Recursive functions) *The* basis functions *are:* $(1) S(n) = n+1; (2) z(n) = 0$ *(all* n*)* (3) *for each* i, $jU^{i_j}(n_1, n_2, \ldots n_i) = n_j \quad 0 < j \leq i$.
The basis functions *are recursive functions. The recursive functions are built up as follows:*
If $g : \mathbb{N}^{K+2} \to \mathbb{N}$, *for some* $k \geq 0$, *and* g *is recursive* then *so is*
$f : \mathbb{N}^{k+1} \to \mathbb{N}$, *where we define:*

$$f(0, y_1, \ldots, y_k) = p \quad some \quad p \quad in \quad \mathbb{N}$$

$$f(x+1, y_1, \ldots, y_k) = g(f(x, y_1, \ldots, y_k) \qquad \text{(Recursion)}$$

If $g : \mathbb{N}^{k+1} \to \mathbb{N}$, *and* g *is recursive then so is* $f : \mathbb{N}^{k+1} \to \mathbb{N}$ *where we define*
$f(x, y_1, \ldots, y_k)$ = *least* z *such that* $g(z, y_1, \ldots, y_k) = 0$ *if such exists*
= *undefined if there's no such* z. (Minimalisation)
If $g : \mathbb{N}^k \to \mathbb{N}$, *and* $g, f_1, \ldots, f_k$ *are recursive then so is* $g(f_1, \ldots, f_k)$ (Composition).

A function is *recursive* then, only if it can be built up from the basis functions by finitely many application of "recursion" and "minimalisation", and composition.
Note Because of the minimalisation operation a recursive function $f : \mathbb{N}^k \to \mathbb{N}$ need not be *total*, i.e. $\mathrm{dom} f \subseteq \mathbb{N}^k$, not necessarily $\mathrm{dom} f = \mathbb{N}^k$.
It turns out that any function on $\mathbb{N}$ (or $\mathbb{N}^k$) to $\mathbb{N}$ in everyday computational use is recursive. One can also prove

Proposition 7.5 *Any recursive function is "computable" i.e. there is a program which will calculate the function.*

More relevant to us, is that all of the effectively decidable concepts such as "formula", "axiom of PC" and "proof" can be formulated using recursive functions. That is: there are recursive functions
$F_{form} : \mathbb{N} \to \mathbb{N}$ so that

$F_{form}(x)$	$= 1$	if x is gn of a formula
	$= 0$	if not.
$F_{Ax}(x)$	$= 1$	if x is gn of an axiom A1-A7 or of Q1-Q7
	$= 0$	if not.

Similarly if $n_1, n_2, \ldots, n_k$ is a list of gn's of strings of symbols, there is a recursive F_{pf}, so that if $x = 2^{n_1}3^{n_2}5^{n_3}\ldots p_k^{n_k}$ ($p_k = k'th$ prime number)

$F_{Pf}(x)$ = 1 if x codes a list of strings in the above manner, and the list is a proof of the last formula in the list

= 0 if not

[The point of coding lists of strings of symbols in the above fashion is that given x, we can decode its prime factors, look at the powers of the primes and decode what the individual formulae in the list are.]

Definition 7.6 *If $X \subseteq \mathbb{N}$, X is* decidable *if there's a recursive function*

$f : \mathbb{N} \to \mathbb{N}$ so that $f(n)$ = 1 if $n \in X$

= 0 if $n \notin X$.

The impact of the above discussion concerning decidability of testing for formulae/terms/proofs/etc., is that the set of gn's of formulae/terms/proofs/etc., are decidable sets of natural numbers. Thus

Proposition 7.7 *The sets of gn numbers of the following sets are decidable (also known as recursive): formulae, terms, axioms of PC + Q, codes of proofs in PC + Q (coded using prime powers).*

It's not too important whether you have in mind the notion of *recursive function* as the basic concept (and hence *decidable* sets of numbers or the rather more informal idea of computable/programmable functions and being able to *effectively decide* a question through a program. [In fact nobody has thought of any definition of "computable" that doesn't produce precisely the recursive functions.] What is important is the realisation that the concepts of formula, axiom, proof etc., are "codable using simple functions". We shall later quote a theorem that all of these functions are definable in, and their properties that we need, provable in, the system Q.

Notation To make reading easier we introduce abbreviations for some of the terms of Q : we write

1 instead of $0'$ 2 instead of $0''$.

These are not new terms of L, merely abbreviations for terms. We write $x \neq y$ rather than $\neg(x = y)$ (although we revert to the latter for the purpose of our official Gödel number coding). Thus $\mathbf{n}$ is to be considered the numeral which will denote the number n when interpreted in $\mathbb{N}$. The recursive functions are indeed about the numbers of $\mathbb{N}$ and are indeed "true in $\mathbb{N}$" in the following sense:

Proposition 7.8 *If F is a k-place recursive function then there is a formula φ_F with $FV(\varphi) = \{v_0, v_1, \ldots, v_k\}$ so that $F(n_1, \ldots, n_k) = m$ iff $\mathbb{N} \vDash \varphi_F(\mathbf{n_1}, \ldots, n_k, \mathbf{m})$.*

The formula φ_F is built up in an analogous way to how the recursive function F is constructed; I don't wish to go into this construction, but it is not unreasonable to suppose that from the very concrete way recursive functions are built that such a formula could be found.

We should thus have for example that n is the prime power code of a list of formulae that codes a proof from the axioms of Q of the last formula in the list, i.e. $F_{Pf}(n) = 1, iff \mathbb{N} \vDash \varphi_{F_{Pf}}(1, \mathbf{n})$. This is indeed just what we should want.

The Diagonalisation of a formula

Consider the formula $\exists y x = ((10.y)+2)$ of L. Interpreted in $\mathbb{N}$, this says "(the valuation of) $x \equiv 2 mod 10$." In other words the last digit of the number assigned to x, as a decimal number, is 2. But notice that if we consider x as a gn of a symbol string we could reinterpret this as saying the string with gnx ends with the symbol).

Definition 7.9 *If ψ is any formula of L, that is* 0 *with n_o many " " after it.*

Definition 7.10 *If $\psi \in L$ the* diagonalisation *of ψ is the formula in L*

$$\exists x(x = \lceil \psi \rceil \wedge \psi)$$

[or officially $(\neg \forall x(x = \lceil \psi \rceil \rightarrow (\neg \psi)))$].

Example 3

φ	$gn(\varphi)$	diagonalisation of φ	T
$y = 0$	676	$\exists x(x = \mathbf{676} \wedge y = 0)$	F
$x = 0$	576	$\exists x(x = \mathbf{576} \wedge x = 0)$	F
$x \neq 0$	145762	$\exists x(x = \mathbf{145762} \wedge x \neq 0)$	T
$\exists y(x = ((\mathbf{10} \times y) + \mathbf{2})$	suppose this has gnn_0		
	$\exists x(x = \mathbf{n_0} \wedge \exists y(x = ((\mathbf{10} \times y) + \mathbf{2}))$	T since $gn(\varphi)$ ends with a 2, or, φ ends with a).	

Lemma 7.11 *There is a recursive function [computable function] diag, so that if n is the gn of a formula φ, diag(n) is the gn of the diagonalisation of φ. Thus by Proposition 5 there is a formula Ψ_{diag} so that $\mathbb{N} \vDash \Psi_{diag}(\mathbf{n}, \mathbf{m})$ iff $m = diag(n)$.*

Proof Let lh (for length) be the function $lh(n) =$ least $m(0 < m \wedge n < 10^m$.
Then lh is a recursive [computable] function: $lh(n)$ is just the number of digits in the usual decimal arabic numeral for n. So $lh(1879) = 4; lh(0) = 1$ etc.
Define * by $m^* n = m.10^{lh(n)+n}$ - also recursive [computable]
If $m \neq 0, m * n$ is the number whose decimal numeral is formed by writing the decimal numeral for m before the decimal numeral for n So $23 * 14$ is 2314
Define num (n) as the gn of **n** i.e. $\overbrace{6686868\ldots68}^{ntimes}$
num(n) is defined by recursion as

$$\text{num(o)} = 6$$
$$\text{num(n+1)} = \text{num(n)} * 68$$

So num is recursive [computable].
Define diag by diag(n) = 144951414157* (num(n)*(34*(n*2222)))
diag is then recursive [computable]. QED

Lemma 7.12 *If φ is a formula of L and $FV(\varphi) = \{x\}$ and ψ is the diagonalisation of φ then*

$$\mathbb{N} \vDash \psi \text{ iff } \mathbb{N} \vDash \varphi(\lceil \varphi \rceil)$$

Proof $\varphi(\lceil\varphi\rceil)$ is precisely what the diagonalisation says. QED

THEOREM 7.13 (TARSKI'S THEOREM ON THE UNDEFINABILITY OF TRUTH) *There is no formula φ so that for any sentence σ, $\mathbb{N} \vDash \sigma$ iff $\mathbb{N} \vDash \Psi(\lceil\sigma\rceil)$*

Proof Suppose there were such a formula Ψ with $FV(\Psi) = \{y\}$ say. Then let $\varphi(x)$ be $\exists y(\varphi_{diag}(x, y) \wedge \neg\psi(y))$. Now let χ be the diagonalisation of φ. χ is then a sentence. We get a contradiction. By Lemma 7 $\mathbb{N} \vDash \chi iff \mathbb{N} \vDash \varphi(\lceil\varphi\rceil)$, but writing this out we get this happens iff $\mathbb{N} \vDash \exists y(\Psi_{diag}(\lceil\varphi\rceil, y) \wedge \neg\psi(y))$. But χ *is* the diagonalisation of φ! So $gn(\chi) = diag(gn(\varphi))$ so $\mathbb{N} \vDash \Psi_{diag}(\lceil\varphi\rceil, \lceil\chi\rceil) \wedge) \neg\psi(\lceil\chi\rceil)$. Putting this together we have $\mathbb{N} \vDash \chi iff \mathbb{N} \vDash \neg\psi(\lceil\chi\rceil)$. But by our supposition on ψ this happens iff $\mathbb{N} \vDash \neg\chi$! So there can be no such ψ. QED

What Tarski's Theorem shows is that there is no short-cut to finding out the truths of arithemetic: there is no conceivable formula which is only true in $\mathbb{N}$ at those integers that are themselves codes of statements that are true in $\mathbb{N}$.

Exercise 1a) Determine which formulae, *if any* have the following as Gödel numbers
(i) 11459978862359976682 (ii) 491595975357668682 (iii) 495575
b) Code up the following formulae
(i) $z = ((y \times 0'') + x) \quad \wedge x(x' = 0 \longleftrightarrow x = 0)$
Exercise 2 If $n_1 = 495144568762 n_2 = 495145687623146687 62, n_3 = 14668762$ and $x = 2^{n_1}3^{n_2}5^{n_3}$ would $F_{Pf}(x) =$ 1 or 0?

7.2 Q REVISITED

Gödel's First Incompleteness Theorem formalised this argument, not about sentences that are true in $\mathbb{N}$, but about what things are provable from the axiom system Q, or any set of axioms extending Q. (The argument in Tarski's theorem above is based on an idea of Gödel's.) An important point in the last section was Proposition 5 asserting that all recursive functions and defining formulae in $\mathbb{N}$; we shall also need to assert at some point that all such functions are representable in some sense in the theory Q too. We need to prove a few things about what we can prove using the axiom of Q first.
Proofs in Q follow our usual format
Example 4a) $Q \vdash \quad 1 \neq 2$

1	$\forall x \forall y(x' = y' \rightarrow x = y)$	$Q1$
2	$\forall x(x' \neq 0)$	$Q2$
3	$1 \neq 0$	Partic.2
4	$0 \neq 1$	Standard using $s = t \rightarrow t = s, R1$, and 3
5	$1 = 2 \rightarrow 0 = 1$	Partic. on 1
6	$1 = 2$	Hyp
7	$0 = 1$	$r1, 56$

So $Q, 1 = 2 \vdash 0 = 1$ and $0 \neq 1$ so by Lemma 36e) $q \vdash 1 \neq 2$
Example 4b $Q \vdash 2 + 2 = 4$

1	$\forall x \forall y (x + y') = (x + y)'$	Q5
2	$2 + 1' = (2 + 1)'$	Partic. on 1
3	$2 + 0' = (2 + 0)'$	Partic on 1
4	$\forall x (x + 0) = x$	$Q4$
5	$2 + 0 = 2$	Partic. on $4x = 2$
6	$2 + 0' = 2' (= 3)$	
7	$2 + 1' = 3'$	Similarly using 2, 6
8	$(2 + 2) = 4$	Rewriting 7

The axioms of Q look natural enough (they are) and fairly innocuous theorems as above can be proved from them. But that doesn't mean that every sentence we normally think true in $\mathbb{N} = \langle \mathbb{N}, =, +, \times, ', 0 \rangle$ is provable in Q. We illustrate by means of some non-standard models of Q that this isn't the case. $\mathbb{N}$ we can think of as the *standard* interpretations of the axioms Q. But there are others.

Example 5 $\mathbb{N}^* = \langle \mathbb{N} \cup \{\infty\}. +_{\mathbb{N}^*}, \times_{\mathbb{N}^*}, '_{\mathbb{N}^*}, 0_{\mathbb{N}^*} \rangle$, i.e. $\mathbb{N}$ with an extra element ∞ added to the domain. We have to specify how to extend $+, \times, '$ to this new domain. We do this so that, appropriately, ∞ is "bigger" than all the n of $\mathbb{N}$.

Thus: $\infty' = \infty \quad ; \quad n + \infty = \infty = \infty + n \quad$ for any $n \in \mathbb{N} \cup \{\infty\}$.

$n \times \infty = \infty = \infty \times n$ but $0 \times \infty \times 0 = 0$

Claim All the axioms of Q are true in $\mathbb{N}^*$

The only difficulty is in verifying the axioms when ∞ is used to substitute for $v_0 \in \mathbb{N}$, and also if $v_0 = \infty$ itself.

Lemma 7.14 $Q \nvdash \forall x (x' \neq x)$.

Proof By the Soundness Theorem it's enough to show there's a model of Q in which $\forall x (x' = x)$ is false. $\mathbb{N}^*$ is such a model, as $\infty' = \infty$ in $\mathbb{N}^*$ QED

Example 6 $\mathbb{N}^{**} =< \mathbb{N} \cup \{\ ,\ \}, +_{\mathbb{N}^{**}}, \times_{\mathbb{N}^{**}}, '_{\mathbb{N}^{**}}, 0_{\mathbb{N}^{**}} >$ where we now add two elements $\ ,\ $. We specify that $'=\ ,\ '=\ $ and $+$ and $\times$ are given by

$x +_{\mathbb{N}^{**}} y$	0	1	n	
0	0	1	$\ldots n$	...
1	1	2	$\ldots 1 + n$	...
m	m	$m + 1$	$\ldots m + n$	...
			...	...
			...	

$x \times_{\mathbb{N}^{**}} y$	0	1	2	n	
0	0	0	0	... 0	...
1	0	1	2	... n	...
2	0	2	4	... $2n$ ...	...
m	0	m	$m2$	... mn	...
	0			...	...
	0			...	...

Lemma 7.15 *None of the following are theorems of Q (*although they are true in the standard interpretation*)*

$$\forall x 0 + x = x \quad \forall x \forall y x + y = y + x$$

$$\forall x 0 x x = 0 \quad \forall x \forall y x \times y = y \times x$$

Proof Exercise. QED

You might at this point think that the system Q is useless for any practical purpose. But the contrary is true. The Representability Theorem below corrects this impression. As a prelude to explaining its contents we look at some examples of what we *can* do in Q.

LEMMA 7.16 *For all natural numbers m, n*

a) If $m = n$ then $Q \vdash$ m = n *b)* If $m \neq n$ then $Q \vdash$ m ≠ n

Proof

a) If $m = m$ we can use simply

1 $\forall x\ x = x$	A6
2 $\forall x(x = x) \rightarrow$ m = m	A4 $m = t$
3 m = m	R1 on 2,3

b) We already showed $Q \vdash$ **1** ≠ 2 and $Q \vdash$ **2** ≠ 3 (as an exercise). This can be generalised to any $m \neq n$. The details are uninteresting. QED

LEMMA 7.17 *If $i + j = k$* then $Q \vdash$ i + j = k

Proof By induction on j : $j = 0$ $Q \vdash$ i + 0 = k is essentially Q4 $j = m + 1$: so for some $n, k = n + 1$ and $i + m = n$. So by Inductive Hypothesis $Q \vdash$ i + m = n and this $Q \vdash$ $(\text{i} + m)' = \text{n}'$ (using A7 and *some more*). But $Q \vdash$ $(\text{i} + m')$ by Q5. So, $Q \vdash$ i + j = k. QED

COROLLARY 7.18 *If $i + j \neq k$* then $Q \vdash$ i + j ≠ k

Proof Let $i + j = n \neq k$. By the last lemma $Q \vdash$ i + j = n and lemma 3 gives $Q \vdash$ n ≠ k

LEMMA 7.19 *If $ij = k$* then $Q \vdash$ i × j = k and $ij \neq k$ implies $Q \vdash$ i × j ≠ k

Proof Similar to the above, exercise.
Since we have that $i + j = k \Leftrightarrow Q \vdash$ i + j = k we can say that the formula $v_1 + v_2 = v_3$ of L represents addition [meaning the common addition on $\mathbb{N}$]. In general we have the following more general definition.

DEFINITION 7.20 *Let $f : \mathbb{N}^k \rightarrow \mathbb{N}$. f is* representable in Q *if there is a formula $\varphi(v_1, \ldots, v_k, v_{k+1})$ [*with free variables precisely as shown*] such that if $p_1, \ldots, p_k, j \in \mathbb{N}$* and *$f(p_1, \ldots, p_k) = j$ then*

(1) $Q \vdash \varphi(p_1, \ldots, p_k, j)$

(2) $Q \vdash \forall v_{k+1}[\varphi(\text{p}_1, \ldots, \text{p}_k, v_{k+1}) \rightarrow v_{k+1} = j]$

Example 6 The projection function U^i_j is represented by the formula

$$v_1 = v_1 \ \wedge .. \qquad \ldots \wedge\ v_i = v_i \wedge\ v_{i+1} = v_j$$

Proof This works because of any $k_1, \ldots, k_i$

$$\vdash (k_1 = k_1 \wedge \ldots \wedge\ k_i = k_i \wedge v_{i+1} = k_j) \leftrightarrow v_{i+1} = k_j$$

Example 7 We have shown (Lemmas 12-14) that addition and multiplication are represented in Q by the formulae $v_1 + v_2 = v_3$ and $v_1 \times v_2 = v_3$

Theorem 7.21 *Every recursive function is representable in Q.*

[Every computable function needed to settle whether strings of symbols are formulae/axioms/proofs/etc are representable in Q'
Proof Omitted: see Boolos & Jeffrey: Computability and Logic Ch.14. The details of the formal proofs are rather tedious, and anyway going into recursive functions is not a part of this course.
Remark The converse of Theorem 7 is also true. The recursive functions are precisely those representable in Q. Since Q seems so weak it might be thought that adding extra axioms to Q would increase the number of representable functions. But if $Q' \supseteq Q$, $Q' \backslash Q$ is finite and every new axiom of $Q' \backslash Q$ is true in $\mathbb{N}$, one may show that the functions representable in Q' are still those that are recursive.
Conclusion diag is representable in Q.

Lemma 7.22 *For any formula $\varphi(x) \in L$,* any $n \in \mathbb{N}$ $Q \vdash \exists x(x = \mathrm{n} \wedge \varphi) \leftrightarrow \varphi(\mathrm{n}/x)$

Proof This is just Exercise 3.11e)

Corollary 7.23 *$\varphi \in L$* and *ψ be the diagonalisation of φ. Then*

$$Q \vdash \psi \leftrightarrow \varphi(\ulcorner \varphi \urcorner)$$

Proof Use Lemma 7.22 $\exists x(x = \mathrm{n} \wedge \varphi)$ is ψ, if n is the gn of φ; $\varphi(n/x)$ is then $\varphi(\lceil \varphi \rceil)$
Notice that this is analogous to Lemma 7.

Lemma 7.24 *For any formulae ρ, ψ, χ of L*

$$(\chi \leftrightarrow \exists y(\rho(\mathrm{n}, y) \wedge \psi(y))),\ \forall y(\rho(\mathrm{n}, y) \leftrightarrow y = \mathrm{k}) \vdash \chi \leftrightarrow \exists y(y = \mathrm{k} \wedge \psi(y)))$$

Proof Uninteresting and omitted.
This is the meat:

Lemma 7.25 (The Diagonal Lemma (Gödel)) *Let T* be a theory (in any language $L' \supseteq L$) in which *diag* is representable (e.g. Q). Given any formula $\psi(y)$ with $FV(\psi) = \{y\}$, there is a sentence χ in L' with $T \vdash \chi \leftrightarrow \psi(\ulcorner \chi \urcorner)$
Thus χ is *equivalent to the expression resulting from inserting the numeral for its own gödel number into ψ.*

Proof *Informally*: (1) Define $\varphi(x)$ to be $\exists y(y = \mathrm{diag}(x) \wedge \psi(y))$

(2) Define χ to be the diagonalisation of φ, i.e. χ is $\exists x(x = \ulcorner \varphi \urcorner \wedge \varphi)$

(3) By Corollary 7.23 $Q \vdash \chi \leftrightarrow \varphi(\ulcorner\varphi\urcorner)$

But from the definition of $\varphi(x)$ this then gives

$$Q \vdash \chi \leftrightarrow \exists y(y = \mathrm{diag}(\ulcorner\varphi\urcorner) \wedge \psi(y))$$

But χ *is* the diagonalisation of φ, so that the y above can be replaced by $\ulcorner\chi\urcorner$. So Lemma 7.22 allows us to conclude

$$Q \vdash \chi \leftrightarrow \psi(\ulcorner\chi\urcorner)$$

Formally: Let $\rho(x,y)$ represent "y = diag(x)" in T. Then for any $n, k \in \mathbb{N}$ if diag$((n) = k$ $T \vdash \forall y(\rho(n,y) \leftrightarrow y = \mathrm{k})$. Let $\varphi(x)$ be $\exists y(\rho(x,y) \wedge \psi(y))$ and let n be the gn of φ. Let χ be $\exists x(x = \mathrm{m} \wedge \exists y(\rho(x,y) \wedge \psi(y)))$. Since n = $\ulcorner\varphi\urcorner$, χ is the diagonalisation of φ. By Lemma 7.22 we get

$$T \vdash \chi \leftrightarrow \exists y(\rho(\mathrm{n}, y) \wedge \psi(y))$$

Let k be the gn of χ. Then diag(n) = k and $k = \lceil\chi\rceil$.

So as $T \vdash \forall y(\rho(n,y) \leftrightarrow y = \mathrm{k})$
$T \vdash \chi \leftrightarrow \exists y(y = \mathrm{k} \wedge \psi(y))$ By Lemma 7.24.

So $T \vdash \chi \leftrightarrow \psi(\mathrm{k})$ i.e. $T \vdash \chi \leftrightarrow \psi(\ulcorner\chi\urcorner)$ QED

The diagonal lemma allows to build self-referential statements just as in Tarski's theorem. This we do now. First (as always) a definition.

DEFINITION 7.26 *A set $X \subseteq \mathbb{N}$ is* definable in a theory T *in L' if there's a formula $B(y) \in L'$ so that for any $k \in \mathbb{N}$*

$$k \in X \Rightarrow T \vdash B(k) \qquad\qquad k \notin X \Rightarrow T \vdash \rceil B(k)$$

$X \subseteq \mathbb{N}^2$ is definable if there's $B(y,z) \in L'$ so that for any

$$k, l \in \mathbb{N}\langle k,1\rangle \in X^2 \Rightarrow T \vdash B(\mathrm{k},1)\langle k,1\rangle \notin X^2 \Rightarrow T \vdash \neg B(k,1)$$

Example 7 (in Q)

Formula	defines
$x = 0 \wedge x = 1$	$\{0,1\}$
$\exists y(y + y = x)$	Evens
$\exists z(z + x = y)$	Set of pairs $\langle x, y\rangle$ so that $x \leq y$.

LEMMA 7.27 *If $T \supseteq Q$ and is consistant then the set of gn's of theorems of T is not definable in T.*

Proof diag is representable in Q and so in T. Suppose $\theta(y)$ is a formula in language of T so that θ defines those integers that are gn's of theorems of T. By the Diagonal Lemma, there is a sentence χ so that.

$$T \vdash \chi \leftrightarrow \neg\theta(\ulcorner\chi\urcorner) \qquad\qquad (\text{putting } \neg\theta \text{ for } \psi)$$

Let $k = gn(\chi)$ then

$$(*) \qquad\qquad T \vdash \chi \leftrightarrow \neg\theta(k)$$

We get a contradiction: suppose $T \nvdash \chi$, then k isn't the gn of a theorem of T and so

$T \vdash \neg\theta(\mathrm{k})$ (because θ defines the set of gn's of theorems of T)

Using the equivalence $(*)$ we get $T \vdash \chi$; supposing in turn k *is* the gn of a theorem of T, θ defines the set of such k so $T \vdash \theta(k)$. But by $(*)$ then $T \vdash \neg\chi$!! Contradiction; so there's no such formula $\theta(y)$. QED
We can now prove Tarski's Theorem as a corollary of the above.

Corollary 7.28 (Tarski's indefinability theorem) *The set of gn's of sentences true in* $\mathbb{N}$ *is not definable in arithmetic.*

Proof The $(\mathbb{N})$ is a consistent extension of Q. Apply the last lemma. QED
This is already a profound result. But Gödel's Theorem (of which Tarski's Theorem above was just a corollary) shows much more: it shows that arithmetic is essentially *unaxiomatisable*.

Definition 7.29 *A theory* T is *axiomatisable* if there's an [effectively] decidable subset T_0 so that the deductive consequences of T_0 are precisely those of T. i.e. for any sentence, $T \vdash \sigma \iff T_0 \vdash \sigma$.

This is thus a generalisation of the idea of finitely axiomatisable. If we can't have a finite aximoatisation of a theory, perhaps we can have an infinite one, but one in which we can effectively decide whether a given formula is an axiom. PC already has infinitely many axioms, but we argued in §3.1 tht it was axiomatisable in the above sense.
Example 7 The theory of algebraically closed fields, or torsion free groups, *is* axiomatisable. We can write a computer programme that would give us (potentially) all the axioms of fields and the axioms that say "every polynomial of degree n has a root", etc. The theory of algebraically closed fields is then the set of sentences derivable from these axioms. This shows that the theory can be axiomatised by an "effectively decidable" set of axioms. One can further show that the set of gn's of such axioms form a decidable set using recursive functions.
Example 8 Q is axiomatisable since it only has 7 axioms, and it's trivial to write a program that tests whether a number is then a gn of one of $Q1 - Q7$.
The importance of axiomatisable theories is:

Proposition 7.30 *Let* T be an axiomatisable theory in L. *Then there is a computable algorithm for generating the theorems deducible from* T. *i.e. there is a computer programme tha outputs gn's of sentences* σ so that $T \vdash \sigma$.

Proof Informally: we are told that there's a computer program, P, that defines a T_0 so that for any sentence σ $T \vdash \sigma$ iff $T_0 \vdash \sigma$, i.e. the programme outputs 1 if given a number which is a gn of a member of T_0, and outputs 0 otherwise. As in Prop 4 where we argued that we could effectively decide whether a number was a code of a proof Q, we can now reason in the same way to say we can effectively decide whether we have the code number of a proof from T_0 (that ends in a sentence), *where we have to make use* of our programme P as a "subroutine" to check for uses of axioms of T_0. The algorithm is then simple: we go through all numbers n and check whether n codes a proof in T_0 of a sentence, if so, we output the gn of that sentence. QED
[Again: this does *not* say there is a programme P such that given the gn of sentence σ, P will output 1 if $T_0 \vdash \sigma$ and 0 otherwise; indeed we shall see *there can be no such programme.*]

LEMMA 7.31 *If the set, S* of sentences deducible from a consistent and axiomatisable set of axioms T is *complete*, then it is decidable [effectively decidable].

Proof: We show effective decidability: By the last lemma let R be the programme that when fed in n, outputs the gn of the sentence at the end of the proof in T_0 which n codes, [where T_0 is the decidable set, which axiomatises T], and outputs 0 if n *doesn't* code such a proof. Now, S is *complete* so for *any* sentence σ of L, either $T \vdash \sigma$ or $T \vdash \sigma$ or $T \vdash \neg\sigma$ (or equivalently $T_0 \vdash \sigma$ or $T_0 \vdash \neg\sigma$). *Thus* as we run the program R, after a finite number of steps in the program either R outputs the gn of σ or that of $\neg\sigma$ (but not both as T is consistent). So, our algorithm is essentially that of Proposition 21; that, together with completeness of S gives an algorithm for testing 'theoremhood' from T. QED

THEOREM 7.32 (GÖDEL'S FIRST INCOMPLETENESS THEOREM) *There is no* $T \supseteq Q$, such that T is consistent and completely axiomatisable.

Proof Theorem 7 stated that every recursive [computable] function is representable in Q; that is if for example $f : \mathbb{N} \to \mathbb{N}$ is recursive [computable] there is a formual $\rho(x, y)$ so that if $f(n) = m$

$$Q \vdash \rho(\mathrm{n}, \mathrm{m})$$

If $T \supseteq Q$ then also $T \vdash \rho(\mathrm{n}, \mathrm{m})$. Since ρ represents f we have too that if $f(n) \neq k$ $T \vdash \neg\rho(\mathrm{n}, \mathrm{k})$. Thus ρ defines the function f. Lemma 22 says that the set of consequences of T is a decidable, [effectively decidable] set of gn's. i.e. there's a recursive function [computable function] f so that

$$\begin{aligned} f(m) &= 1 \quad \text{if } m \text{ is the } gn \text{ of a sentence provable from } T \\ &= 0 \quad \text{if not.} \end{aligned}$$

But then if $\rho(x, y)$ is the formula that defines f as above then the formula $\theta(x) \equiv \rho(x, 1)$ defines in T the set of theorems of T. Since

$$\begin{aligned} &\text{if} \quad T \vdash \varphi \; f(gn(\varphi)) = 1 \qquad \Rightarrow T \vdash \theta(\ulcorner\varphi\urcorner) \\ &\text{if} \quad T \nvdash \varphi \; f(gn(\varphi)) = 0 \qquad \Rightarrow T \vdash \neg\theta(\ulcorner\varphi\urcorner) \end{aligned}$$

This contradicts Lemma 19. So if $T \supseteq Q$ is axiomatisable, it is either incomplete or inconsistent. QED

Remark 1) Since Q is a very weak theory the theorem is a very strong one: it includes all consistent theories extending Q

2) This is one of the most significant theorems in logic; one can paraphrase it as saying that no matter how we effectively extend the axiom system Q there will be truths of arithmetic that are not provable from it.

COROLLARY 7.33 *Arithmetic (=* $Th(\mathbb{N})$*) is not axiomatisable.*

Proof $Th(\mathbb{N})$ is itself complete and consistent. But $Th(\mathbb{N}) \supseteq Q$. So there's no effective set of axioms for it. QED

Remark 3) Gödel's Second Incompleteness theorem says something about consistency in systems extending Peano arithmetic (*PA* - a stronger theory than Q). In *PA* (or any consistent extension T of *PA*) we can

find a formula $\pi(v_0, v_1)$ which represents the relation $Pf(y, n)$: "y is the prime power code of a proof of the formula φ with $gn\ n$". If PA were inconsistent we would have $PA \vdash 0 = 1$. $gn(0 - \mathbf{1}) = 67668$. So, if PA is consistent we cannot have $\exists y Pf(y, 67668)$. The theorem says $PA \nvdash \neg\exists y \pi(y, \mathbf{67668})$. To paraphrase this, PA cannot prove that it itself is consistent. And similarly for any system T containing PA. This is sometimes stated rather loosely as arithmetic cannot use arithmetical means to establish its own consistency.

Exercise 3 Show	$Q \vdash 2 \neq 3$	Hint: follow the format of Example 4
	$Q \vdash 0 \neq 3$	Hint: this is easier, only use Q2
	$Q \vdash 2 + 1 = 3$	Hint: copy Example 4
	$Q \vdash 1.1 = 1$	Hint: don't do it. Examples involving muliplication rapidly become awkward.

However $Q \vdash \forall x \exists y(x \times y = y)$ and $Q \vdash \forall x \exists y(x + y = x)$ are not so hard.

Exercise 4 Convince yourself that the other axioms of Q are true in $\mathbb{N}^*$.

Exercise 5 Show that Q6 is not provable from the other axioms of Q [Hint: Make a small modification to the interpretation of $\times$ in $\mathbb{N}^*$.]

Exercise 6 Let T be as in Lemma 19; check the following sets for definability in such a T

(i)	$\{gn(\varphi) \mid T \nvdash \neg\varphi\}$
(ii)	$\{gn(\varphi) \mid T \nvdash \neg\varphi\}$
(iii)	$\{gn(\varphi) \mid T \vdash \varphi \text{ or } T \nvdash \varphi\}$

Exercise 7 Let $T \supseteq Q$ be consistent as above. Show that there is no $R \subseteq \mathbb{N}$, definable in T, so that if $T \vdash \varphi$ then $gn(\varphi) \in R$, but if $T \vdash \neg\varphi$ then $gn(\varphi) \notin R$.

7.3 The Second Incompleteness Theorem

The First Incompleteness Theorem was proven by contradiction. In it we showed that any $T \supseteq Q$ if consistent and axiomatisable was incomplete. The proof by contradiction hides the fact that given T one can explicitly find a sentence ρ such that $T \nvdash \rho$ and $T \nvdash \neg\rho$. We proceed now to construct such a sentence and show that it has the right properties. Assume from now on $T \supseteq Q$ is axiomatisable.

Remark 3 asserted the existence of a formula $\pi(v_0, v_1)$ which represents in T $Pf(y, n)$ "y is the prime power coce of a proof of the formula φ with $gn(\varphi) = n$". Thus

if	$Pf(y, n)$ then	$T \vdash \pi(y, \mathrm{n})$ and
if not	$Pf(y, n)$ then	$T \vdash \neg(y, \mathrm{n})$.

Further, the function $f(n) = 14^* n^* 2$ is computable and so there is a formula $\nu(v_0, v_1)$ so that

if $f(n) = m$	$T \vdash \nu(\mathrm{n}, \mathrm{m})$
if $f(n) \neq m$	$T \vdash \neg\nu(\mathrm{n}, \mathrm{m})$

$f(n)$ is $gn(\neg\varphi)$ if $n = gn(\varphi)$. Thus ν represents the function which returns the gn of the negation of the formula whose gn is n.
Consider now the formula with free variable v_0

$$\varepsilon(v_0): \ \forall v_1[\pi(v_1, v_0) \to \forall v_3(\neq (v_0, v_3) \to \exists v_4(v_4 \leq v_1 \wedge \pi(v_4, v_3)))]$$

"if there's a proof of (the formula with gn) v_0 then there's a proof with smaller code number of the negation of (the formula with gn) v_0". Now apply the Diagonal Lemma. There's a sentence ρ so that

$$T \vdash \rho \leftrightarrow \varepsilon(\ulcorner \rho \urcorner)$$

Intuitively now, $\varepsilon(v_0)$ asserst that if $gn(\varphi)$ is v_o, then φ is not provable. [Since we're assuming T consistent, because if $T \vdash \varphi$, $\varepsilon(v_0)$ says there's a proof of $\neg\varphi$ with a smaller code number which is a contradiction; so $T \nvdash \varphi$.] But $\rho \leftrightarrow \varepsilon(\ulcorner \rho \urcorner)$ by R1. So, as in the last sentence ρ is not provable. Contradiction. But $T \vdash \neg\rho$ implies by R1 $T \vdash \neg\varepsilon(\ulcorner \rho \urcorner)$. Btu notice that assuming T consistent $T \nvdash \rho$. I.e. there's no proof of ρ i.e. "for all y not $Pf(y, r)$" (where $r = gn(\rho)$) so the antecedent of $\varepsilon(v_0)$ is *always* false. So $T \vdash \varepsilon(\ulcorner \rho \urcorner)$. Contradiction! So neither $T \vdash \rho$ nor $T \vdash \neg\rho$. So, we've provided a ρ that illustrates T's incompleteness. ρ depends on π of course, and π in turn depends on our formula that represents the gn's of axioms of T, but apart from that the procedure for obtaining ρ is uniform.
Actually the argument under the "converse" assumption $T \vdash \neg\rho$ had a large hole in it: I went from assuming $T \nvdash \rho$ to saying "for all natural numbers y not $Pf(y, r)$" and *therefore* $T \vdash \forall v_0 \neg\pi(v_0, \mathbf{r})$. Then I used the latter to say therefore $T \vdash \varepsilon(\ulcorner \varphi \urcorner)$. But just because $T \vdash \neg\pi(\mathrm{y}, \mathbf{r})$ for any $y \in \mathbb{N}$, doesn't mean $T \vdash \forall v_0 \neg\pi(v_0, \mathbf{r})$. π only *represents* Pf. We put this right below.

Theorem 7.34 (Gödel-Rosser 1936) *With T, ε, ρ as above neither $R \vdash \rho$ nor $T \vdash \neg\rho$.*

Proof Let $r = gn(\rho)$. Let $q = gn(\neg\rho)$. Let ν represent the "negation" function as above. We first give an informal proof and then a formal one.
(Informal proof). Suppose $T \vdash \rho$. Since $T \vdash \rho \leftrightarrow \varepsilon(\ulcorner \rho \urcorner)$ we have

(1) $T \vdash \varepsilon(\ulcorner \rho \urcorner)$.

Let k be the code number of proof of ρ from T. So $Pf(k, r)$ and thus

(2) $T \vdash \pi(\mathrm{k}, \mathbf{r})$.

As $q = gn(\neg\rho)$ we have

(3) $T \vdash \nu(\mathbf{r}, \mathrm{q})$.

By using Particularisation and R1 a couple of times (1) - (3) give

(4) $T \vdash \exists v_4(v_4 \leq \mathbf{r} \ \wedge \ \pi(v_4, \mathrm{q}))$.

But we're assuming T consistent; so $T \nvdash \neg\rho$, i.e. for all $n \in \mathbb{N}$

(5) $T \vdash \neg\pi(\mathrm{n}, \mathrm{q})$ (as π represents Pf)

which contradicts (4)!

Conversely suppose $T \vdash \neg\rho$. Let m be a code of a proof of $\neg\rho$ from T so $Pf(m, q)$ and

(6) $T \vdash \pi(\mathrm{m}, \mathrm{q})$

Now $T \vdash \neg\varepsilon(\ulcorner\rho\urcorner)$ i.e. $T \vdash \neg\varepsilon(\mathbf{r})$. That is

(7) $T \vdash \exists\nu_1[\pi(\nu_1, \mathbf{r}) \wedge \exists\nu_3[\nu(\mathbf{r}, \nu_3) \wedge \neg\exists\nu_4(\nu_4 \leq \nu_1 \wedge \pi(\nu_4, \nu_3)))]]$.

Now from this we can certainly deduce $T \vdash \exists\nu_1\pi(\nu_1, \mathbf{r})$. Why are we not finished? Because we *can't* deduce from this alone that there's some natural number n with $T \vdash \pi(n, \mathbf{r})$ [and so $Pf(n, r)$ and so $T \vdash \rho$ - a contradiction.] This is the point alluded to above. But $T \vdash \nu(\mathbf{r}, \mathrm{q})$ and as ν represents a function we can show

$T \vdash \nu(\mathbf{r}, \mathrm{q}) \wedge \nu(\mathbf{r}, \nu_3) \rightarrow \nu_3 = q$, so we may use substitutability of equals and some R1 to get

(8) $T \vdash \exists\nu_1[\pi(\nu_1, \mathbf{r}) \wedge \forall\nu_4(\nu_4 \nleq \nu_1 \wedge \neg\pi(\nu_4, \mathrm{q}))]$

Using Particularistion with $\nu_4 = m$ we get

(9) $T \vdash \exists\nu_1[\pi(\nu_1, \mathbf{r}) \wedge (\mathrm{m} \nleq \nu_1 \wedge \neg\pi(\mathrm{m}, \mathrm{q}))]$

But (6) implies then

(10) $T \vdash \exists\nu_1[\pi(\nu_1, \mathbf{r}) \wedge \mathrm{m} \nleq \nu_1]$

So not from T we can deduce the existence of an $n \leq m$ so that $T \vdash \pi(n, \mathbf{r})$. If not $Pf(n, r)$ then $T \vdash \neg\pi(\mathrm{n}, \mathbf{r})$; so assuming T consistent $Pf(n, r)$ holds. That is, $T \vdash \rho$. Thus T is inconsistent!

Actually some rather annoying details have again been swept under the carpet in both parts of the above proof. What I should have used is the following proofs: for any natural number m

$$(*) \qquad \begin{array}{l} Q \vdash \nu_1 \leq m \wedge m \leq \nu_1 \\ \\ Q \vdash \nu_1 \leq m \rightarrow \nu_1 = 0 \wedge \nu_1 = 1 \wedge \ldots \wedge \nu_1 = m \end{array}$$

I needed these facts especially just after (10) above - but in fact also implicitly used them in the first half too.

(Formal proof). Suppose $T \vdash \rho$. Actually everything in the informal proof is good enough as it stands apart from the very last claim that (5) contradicts (4). Since $T \supseteq Q$ we can use $(*)$ above and prove $T \vdash \nu_4 \leq \mathbf{r} \rightarrow \nu_4 = 0 \wedge \nu_4 = 1 \wedge \ldots \wedge \nu_4 = r$.

Since we can also prove according to (5)

$$T \vdash \neg\pi(0, q) \wedge \neg\pi(1, \mathrm{q}) \wedge \ldots \wedge \neg\pi(\mathbf{r}, \mathrm{q})$$

we can with help of a suitable tautology get

$$T \vdash \forall\nu_4\neg(\nu_4 \leq r \wedge \pi(\nu_4, \mathrm{q}))$$

which contradicts (4).

The converse, supposing $T \vdash \neg\rho$, requires some more work. We simply rewrite the whole proof. So assume $T \vdash \neg\rho$ and $Pf(m, q)$. Thus

$T \vdash \pi(\mathrm{m}, \mathrm{q})$.But

$T \vdash \pi(\mathrm{m}, \mathrm{q}) \to \forall v_1(\mathrm{m} \le v_1 \to \exists v_2(v_2 \le v_1 \wedge \pi(v_2, q)))$ or

$T \vdash \forall v_1[\pi(m, \mathrm{q}) \to (\mathrm{m} \le v_1 \to \exists v_2(v_2 \le v_1 \wedge \pi(v_2, \mathrm{q})))]$

and by Particularisation

$T \vdash \pi(\mathrm{m}, \mathrm{q}) \to (\mathrm{m} \le v_1 \to \exists v_2(v_2 \le v_1 \wedge \pi(v_2, \mathrm{q})))$.

By R1 we then get

(11) $T \vdash \pi(\mathrm{q}))$.

Since T is consistent $T \nvdash \rho$ so $T \vdash \neg\pi(n, \mathbf{r})$ for any $n \in \mathbb{N}$. Since $T \supseteq Q$, by (*) above

$$T \vdash v_3 \le m \to v_3 = 0 \wedge v_3 = \mathbf{1} \wedge \ldots \wedge v_3 = m.$$

By use of a suitable tautology this gives

(12) $T \vdash v_3 \le \mathrm{m} \to \neg\pi(v_3, r)$.

Now construct a formal proof from $T \cup \{\pi(v_1, \mathbf{r}), \nu(\mathbf{r}, v_4)\}$

1	$\pi(v_1, \mathbf{r})$	Hyp
2	$\nu(\mathbf{r}, v_4)$	Hyp
3	$v_1 \le m \wedge \mathrm{m} \le v_1$	(*) Theorem
4	$\mathrm{m} \le v_1 \to \exists v_2(v_2 \le v_1 \wedge \pi(v_2, \mathrm{q}))$	(11) above
5	$v_1 \le \neg\pi(v_1, \mathbf{r})$	(12) above (replacing v_3 by v_1)
6	$\neg\pi(v_1, \mathbf{r}) \wedge \exists v_2(v_2 \le v_1 \wedge \pi(v_2, \mathrm{q}))$	3, 4, 5 using R1 and tautology $P \wedge Q \to [((P \to R) \to (Q \to S)) \to R \wedge S]$
7	$\exists v_2(v_2 \le v_1 \wedge \pi(v_2, \mathrm{q}))$	1,6 using R1 and tautology $P \to ((\neg P \wedge Q) \to Q)$
8	$\nu(r, \mathrm{q})$	As ν represents negation
9	$\nu(r, \mathrm{q}) \wedge \nu(\mathbf{r}, v_4) \to v_4 = \mathrm{q}$	Likewise
10	$v_4 = \mathrm{q}$	2, 8, 9 using R1 and a tautology
11	$\exists v_2(v_2 \le v_1 \wedge \pi(v_2, v_4))$	Using 7, 10 and an Equality Axiom.

Thus $T, \pi(v_1, \mathbf{r}), \nu(\mathbf{r}, v_4) \vdash \exists v_2(v_2 \le v_1 \wedge \pi(v_2, v_4))$
or $T, \pi(v_1, \mathbf{r}) \vdash \forall v_4(\nu(\mathbf{r}, v_4) \to \exists v_2(v_2 \le v_1 \wedge \pi(v_2, v_4)))$
using the Deduction Theorem and R2; and doing the same again

$$T \vdash \forall v_1(\pi(v_1, \mathbf{r}) \to \forall v_4(\nu(\mathbf{r}, v_4) \to \exists v_2(v_2 \le v_1 \wedge \pi(v_2, v_4))))$$

i.e. $T \vdash \rho$. Contradiction. QED

We have thus seen that the sentence ρ above (known appropriately enough as a Rosser sentence) whilst true, is neither provable nor disprovable from T (although $\rho \leftrightarrow \varepsilon(\ulcorner \rho \urcorner)$ is provable.) ρ is rather complicated and depends on notions of coding, gn's, provability and so on. It is thus somewhat "metamathematical" in content, whereas Q, for example, is a simple mathematical theory. It is possible to find "undecided" strictly mathematical statements, although it wasn't until 1976 that one was found.
We describe below what the statement is. The statement is true in so far that it is provable from set theory, ZF, but it is not provable in Peano Arithmetic, PA. Recall that although PA has an infinite set of axioms, the gn's of the axioms form an effectively decidable set and every axiom of Q is provable from PA. Thus $PA \supseteq Q$. The theory $ZF \supseteq PA$, and so since the statement is provable from ZF, it's negation can't be proven from PA (unless ZF is inconsistent.) It is thus neither provable nor disprovable from PA. Actually the statement is provable from Ramsey's Theorem which is in turn provable from ZF. In the following

$$[X]^e = \{Y \subseteq X | Y \text{ contains } e \text{ elements}\}\}.$$

A *partition* into n disjoint pieces of $[X]^3$ is a set, $X_i (1 \leq i \leq n)$, of n subsets of $[X]^e$, so that $X_i \cap X_j = \varnothing$ is $i \neq j$, and whose union is all of $[X]^e$.

Theorem 7.35 (Ramsey's Theorem) *Let X be an infinite set and let $e, n \in \mathbb{N}$. If $[X]^e$ is partitioned into n disjoint pieces then one of the X_i is infinite.*

The unprovable statement in PA is a finite-version of this theorem. [Recall a natural number m is the set of its predecessors.]
A *homogeneous subset* of m for a given partition is a subset $H \subseteq m$ so that all of $[H]^e$ ends up in precisely one of the X_i. Let $(+)$ be the following statement.
$(+)$ For every $e, n, k \in \mathbb{N}$ there is $m \in \mathbb{N}$, so that for every partition of $[m]^e$ into n pieces, there's a homogeneous subset of m for the partition of size at least k.
One can show that $PA \vdash (+)$. But now if we add the further simple requirement that the homogeneous subset H must satisfy $\text{size}(H) \geq \min(H)$ and call this statement $(++)$ then we have the following

Theorem 7.36 (Paris-Harrington Theorem; 1976) $(++)$ can be proved from Ramsey's Theorem thus $ZF \vdash (++)$ but $PA \nvdash (++)$.

The significance of the fact that $(++)$ can't be proved from PA but can from a slightly stronger theory resides in the fact that (1) PA is a rich theory in which many theorems of number theory can be proven and that (2) $(++)$ is a simple statement about finite sets of natural numbers. Much simpler than the Rosser sentence ρ above. The existence of "undecided" statements in PA was known since the Gödel-Rosser result of 1936. But it took 40 years to find a purely *mathematical* sentence which was not provable nor disprovable from PA.

Exercise 8 Let $T \supseteq PA$, then is the following set definable in T?

$$\{gn(\varphi) \mid T \vdash \varphi \text{ or } T \vdash \neg\varphi,\ \varphi \text{ a sentence } \}$$

[Hint: Suppose this is definable by $\theta(y)$ and take the conjunction of θ with $\delta(y)$ where the latter is $\forall z[\nu(y,z) \rightarrow (\exists x \pi(x,z) \rightarrow \exists v_4 \leq x\ \pi(v_3, y))$[; show that this defines $\{gn(\varphi) \mid T \vdash \varphi,\ \varphi \text{ a sentence}\}$.

Exercise 9 $\mathbb{N} \vDash PA$ so does $\mathbb{N} \vDash \rho$ or $\mathbb{N} \vDash\ \neg\rho$?