Chapter III Set Theory as a Theory of First Order Predicate Logic.

Here is an appealing and apparently clear picture of the "universe of all sets": Suppose that a set A of "individuals" or "Urelements" is given. Then we can form sets from those individuals; these will be subsets of A. We can then form sets of which these subsets of A are in turn members;. In fact, it seems reasonable to hold that we can form not only such sets, but also sets which consist partly of subsets of A and partly of members of A; the sets which have only individuals as members and those which have only sets of individuals as members are special cases of this more general category. Having formed this second tier of sets we can then proceed to form a third tier, a collection of sets the members of which may be individuals, sets of individuals and sets which themselves count sets of individuals among their members. Carrying on in this manner ad infinitum we run through the so-called "cumulative hierarchy (of sets)". The structure which results in this way is the subject of the *theory of sets*. It is this structure that any axiomatic set theory should try to capture.

It isn't quite right to speak of *the* structure of set theory. For what the iterative process of forming sets produces evidently depends on the set A with which we start. But among the many different hierarchies which are generated by different sets of Urelements there is one that is special. This is the hierachy which results when we start with nothing, so to speak, i.e. when we begin with the empty set. It may not be immediately obvious that this will get us anything at all, but only a little reflection shows that it does. All that needs to be acknowledged is that the empty set is fit to act as a member of other sets. Once we accept this, we see that there is at least one other set besides the empty set, viz. the set whose only member is the empty set. (Clearly this set is different from the empty set, for it does have a member, whereas the empty set itself has none.) As soon as we have these two sets, it is possible to form more sets, e.g. the set which has both these two sets as members, etc. In fact, even if we start with the empty set of individuals, iterated set formation leads eventually to an unimaginably huge universe, and one that is certainly big enough to model any abstract structure - such as that of the real numbers, or of all functions from real numbers to real numbers, etc., etc. - that pure mathematics and the sciences which use mathematics as a tool ever made a topic of investigation. Because it gives us enough for these purposes, while on the other hand it apparently does without "extra-logical" assumptions (it does not involve the assumption of any "Urelements", which are themselves not sets), the hierarchy which starts from the empty set has become the preferred object of study within mathematical logic. It is this structure that is usually referred to as *the cumulative hierarchy*.

The cumulative hierarchy, then, is that structure which we get when, starting from the empty set, we generate sets by the iterative procedure just sketched and carrying on "ad infinitum", as we just put it. But what is "ad infinitum"? It may be that what is meant by this appwars reasonably clear at first. But upon reflection the illusion of clarity quickly evaporates. The infinite, in all its different manifestations, is one of the trickiest abstract concepts there are, and this applies to the phrase "ad infinitum", as it figures in our informal description of the cumulative hierarchy, no less than to any other manifestation of it.

Set Theory was invented in large part to analyse the concept of infinity, and to develop systematic means of studying and describing its different manifestations in different contexts. Because of this it is in the curious situation that what it has to say about infinity is constitutive of the very structure of which it is meant to provide an accurate description. As a result there is, from the perspective we adopted in Ch. 2 a certain kind of circularity here, which is unlike anything we have found in connection with other theories discussed there that aim at the description of a single structure, such as the theory of the order of the rationals, or Peano Arithmetic, or the Theory of Real Closed Fields. In all those cases there was a well-defined, and independently definable, structure against which the axioms of the theory could be checked, so that various well-defined questions can be raised about the relation beteen structure and theory, e.g. whether the theory gives a complete, or a categorical characterisation of the structure. (And as we saw it is often possible, if rarely simple to answer such questions.)

Set Theory is different in this respect. The very question what the structure is like that it is its purpose to describe cannot be detached from the description that the theory itself provides; for part of what the theory asserts is what iteration of a given operation or set of operations *ad infinitum* comes to, and thus what the structure is that is the result of such an iteration ad infinitum.

One of the striking discoveries about infinity - which stood, one might say, at the cradle of Set Theory as we know it today - was that it comes in different 'degrees', or 'sizes'. As we noted in Ch. 1, Cantor. the founder of modern set Theory, showed that the power set P(X) of a set X is of higher cardinality than X itself. This is true for any set X whatever, and so in particular when X is infinite. Consequently each infinite set X is the starting point of an unbounded sequence X, P(X), P(P(X)),.. of sets of ever larger infinite cardinality. But havin established that there is a multiplicity of different infinities, the set theorist sees himself confronted with further questions, concerning (a) the extent and (b) the structure of this multiplicity. Two such questions have dominated Set Theory for most of its history: (i) How many different sizes of infinity - how many 'cardinalites' - are there altogether? and (ii) are there any sets X whose cardinality |X| is between that of the set N of the natural numbers and that of its power set P(N)? (This second question is known as the issue of the *Continuum Hypothesis*. The Continuum Hypothesis (CH) is the statement that there are no such sets X: $\neg (\exists X)(|N| < |X| < |P(N)|)$.)

The investigations concerning the CH can be divided into three phases. At first, the goal was simply to decide whether or not the Continuum Hypothesis is true. This is the way Cantor, the one who introduced the issue of of the CH into Set Theory, understood it. (Cantor seems to have worked on this problem relentlessnly and the strain caused by his failure to settle the matter is said to have contributed to his eventual mental breakdown.) The second phase set in after, in the early parts of the 20-th Century, Set Theory had been formalised and characterised as a formal theory, given by a certain set of axioms. At that point the problem of the CH took on a correspondingly formal complexion: Can the CH be either proved or refuted from the axioms of formal Set Theory[1]? This question was settled in two stages. First Gödel proved in 1940 that CH is consistent with formal Set Theory, and thus that the axioms do not refute it. Then, in 1963, Cohen proved that CH is independent of this system, i.e. that it cannot be proved from its axioms either.

Cohen's result was not only the conclusion of the second phase, but also the point of departure for the third. This phase (which continues to the present day and will quite possibly never be concluded) is characterised by the search for new set-theoretical principles which settle the CH one way or the other, and which at the same time can be argued to be true on independent, intuitively persuasive grounds.

[1] The formalisation of Set Theory didn't lead to just one set of axioms. However, it became clear fairly soon that the major proposals do not differ from each other as far as CH is concerned. So we can, without serious distortion to what actually happened, describe this phase in the history of Chas the question whether CH can be either proved or refuted from one of these axiomatic theories, viz from the theory ZF, or 'Zermelo-Fraenkel',which will be presented in this Chapter.

Though a number of formal results were achieved in the aftermath of Cohen's result, involving new axioms which settle the CH one way or thev other, none of the new axioms that were proposed seem to qualify as unequivocally true. So, from a conceptual point of view the CH is na open question to this day

For our present purposes the first question - What is the total range of infinite cardinalities? - is of more immediate importance. Work on this question has taken on a flavour much like that connected with CH: Various axioms have been proposed, each of which tells us something about the range of infinite cardinalities. Most of these axioms are 'Large Cardinal Axioms', which when added to ZF guarantee the existence of cardinalities larger then any that can be proved to exist without them. But the conceptual difficulty connected with these results is much like the one we just mentioned in connection with CH: In general it is difficult to persuade oneself that the proposed axioms must be true.

Connected with the question how large infinities can get is the question what should be understood by the phrase 'ad infinitum'. Even the multiplicity of cardinalites that is guaranteed by ZF by itself (i.e. without the addition of any further axioms) implies that many different answers are possible in principle here. One possible interpretation of *ad infinitum* is that "iteration ad infinitum" should be understood as iteration going up to the first, or 'lowest', degree of infinity, viz. that of denumerably infinity. The structure which is obtained by iterating, starting from the empty set, the set-forming operations up to this first level of infinity is known as the *Hierarchy of Hereditarily Finite Sets*. It goes by this name because all its elements are sets that are *hereditarily finite* in the sense that (a) they are finite themselves, and (b) their members are also finite sets, and likewise for the members of those members, and so on all the way down. It is clear, however, that this is *not* the structure that the axioms of Set Theory should try to capture. It is of the essence of the "real" structure of sets that some of the sets in it are inifinite. Since the Hierarchy of Hereditarily Finite Sets doesn't contain any such sets, not even the set of natural numbers, it cannot be the the one we are after.

Even apart from this consideration, the Hierarchy of Hereditarily Finite Sets should not qualify as the structure that Set Theory should describe on the grounds that what we intuitively want is the structure which results from iterating the set-forming operations through *all* infinite cardinalities; teh itereation shouldn't be stopped at any earier stage, and stopping at the very first opportunity that offers itself is about as far removed from this general desideratum as possible

As we already noted, there is no way to determine the properties of the full structure of sets completely independently of what Set Theory says, for it is the theory which asserts how large and complex sets can become. In the light of all the work that has been donme on the question of large c ardinals there has been a growing impression that what can be said about this must to some extent remain a matter of stipulation. The upshot of this is that there may be no one 'true' structure of sets and therefore possibly also no one correct axiomatic set theory. The second question is complicated, however, by the c ircumstance that axiomatic set theories like the Theory of Zermelo-Fraenkel, or 'ZF', which we will present below, admit of so-called 'inner models' - structures which satisfy all the axioms of the theory but which are obtained be iterating the set formation operations only up to the cardinality of some set whose existence the axioms enable us to prove.[2] For this reason the quest for th right axiomatisation of Set Theory does not stand or fall with the quest for the true 'set-theoretical universe'.

Not only are first order axiomatic set theories like ZF exceptional from the perspective adopted in Ch. 2, they also hold a unique position within the landscape of logic, mathematics and the exact sciences in a different sense. As we noted in the Interlude on Set Theory in Ch.1, Set Theory is indispensible in the formalisation of mathematics. As we also noted there, the insight that it is needed for this purpose is certainly not self-evident; and as things actually happened, it was something that was learned the hard way: The insight emerged when Russell detected the error which had slipped into Frege's attempt to reduce arithmetic to 'pure logic' and which Russell exposed in the form of what has come to be known as 'Russell's Paradox'.

[2] This sounds paradoxical, for how can a structure which verifies all the axioms of the theory fail to contain sets that the theory claims to exist? The answer is that an inner model will in general not only lack the sets which would be reached only by carrying the iteration beyond the point where th inner model is reached, but also many of the functions which establish 1-1 correspondences between sets that are part of the inner model. This makes it possible for sets in the inner model to appear from a perspective internal to the inner model as if they had a larger cardinality than they can do from the external perspective of 'reality', - the functions that would establish them as being of the same cardinality as certain other sets of the internal model (and thus as having no larger cardinality than these), simply are not around.

The need for set-theoretical principles arises in the formalisation of any part of mathematics or science. It arises in particular in the formalisation of parts of *metamathematics*, i.e. of the discipline which deals with the general properties (such as completeness , consistency, soundness, compactness, etc.) of logical systems like the predicate calculus. And it is especially in such formalisations that the conceptual implications of its use are most important. For the point of such formalisations is to make certain that the general framework of mathematics and science does indeed have the general poperties of soundness and consistency which we attribute to it. [3]

When Set Theory is used as metatheory in formalisation, and especially in its role as metatheory in the formalisation of parts of metamathematics, it is of the outmost importance that its principles be ascertainable as true. For this reason formalisations in metamathematics should try to make as parsimonious a use of set-theoretic principles as possible, and to employ only those whose

[3] To give an idea of what formalisations of parts of metamathematics come to, here is an outline of the formalisation of the very first results we proved in Ch. 1, the soundness and completeness of first order logic. The formalisation of these results will involve, first, formal definitions within the language of ZF of the syntax, model theory and proof theory of first order predicate logic. This means that the languages of predicate logic, their symbols, formulas, and derivations as well as the models for those languages and the sequencs of formulas that constiotute correct derivations, are represented as set-theoretic objects, and that soundness and completeness are formulated as statements - pertaining to those objects - in the language of set-theory. Second, the proofs of soundness and completeness can then be turned into formal axiomatic derivations - in the sense defined in CH.1, Sn 1 - from the axioms of set theory together with the mentioned definitions.

Note that such attemtps at providing additional support for the soundness of our general logical framework are affected by an ineliminable element of ciruclarity. For the fact that the soundness theorem can be demonstrated in the form of a formal derivation provides support for its being true only to the extent that the formal method of derivationthat is used in the demonstration can be trusted. But that is precisely the issue that the soundness proof is trying to establish. It sould be noted that this circularity will be there independently of whether the formalisation of axioms of set-theory. These only add a further element of uncertainty insofar as there can be any doubt about *their* truth.

Of special significance is the fact that Set Theory is needed in the formalisation of the metamathematics of Set Theory itself. Here Set Theory plays the double role of object of investigation on the one hand and formalism within which the formalisation is being carried out on the other. This double role has given rise to forms of argumentation in which systermatic switches are made back-and-forth between the system as object- and as metaformalism.

validity is beyond controversy. As we will see, the axioms of ZF enjoy a coniderable degree of intuitive plausibility, though even among them it is possible to make out some differences in the kind or degree of self-evidence that attaches to them.

As a matter of fact the set-theoretical principles that are needed to formalise the more elementary parts of metamathematics (including all the results that were presented in Chs. 1 and 2) seem to be self-evident to a remarkable extent. Even if the combination of these principles with those of pure logic does go beyond what we now consider to be within the scope of pure logic, this does not seem to seriously affect the central purpose of the formalisation of metamathematics - to provide a proper foundation of scientific thought and reasoning.

Set Theory, then, can be seen as occupying a position halfway between logic and mathematics. On the one hand it seems to be about some particular matehamatical structure or structures, and as such it is on a par with other branches of mathematics. But on the other hand its central concepts, and the analyses of them that it has provided, come as close to what we would consider 'pure logic' as anything that doesn't actually lie squarely within it.

2. The Axioms of Set Theory.

In order to state the axioms of ZF we must first decide on a first order language in which they are to be expressed. We start with the assumption that this language has only one non-logical constant, the 2-place predicate ε, which designates the relation that holds between x and y when x is a member, or element, of the set y. As we go along, we will extend this language with new vocabulary, but always giving explicit definitions for the new notions in terms of the original ε. Thus each time a new predicate or function symbol is added to the language, the theory we are building is extended through the addition of a corresponding definition. As we have seen in Section 2.3, these additions always yield conservative extensions, which do not increase the set of theorems expressible in the original vocabulary $\{\varepsilon\}$.

The first principle that an axiomatic theory of sets should make explicit is the one which states what makes for the identity of a set. The principle we adopt, and which is in a sense definitory of the concept of set, is the *principle of extensionality*, according to which two sets are identical if and only if they have the same members:

SA 1. $(\forall x)(\forall y)\ (x = y \leftrightarrow (\forall z)(z\ \varepsilon\ x \leftrightarrow z\ \varepsilon\ y))$

The next three axioms tell us something about how to make new sets out of given sets. They testify to the possibility of forming *pairs*, *unions* and *power sets*, respectively

SA 2. $(\forall x)(\forall y)(\exists z)(\forall u)(u\ \varepsilon\ z \leftrightarrow (u = x\ \ v\ \ u = y))$
SA 3. $(\forall x)(\exists z)(\forall u)(u\ \varepsilon\ z \leftrightarrow (\exists v)(v\ \varepsilon\ x\ \ \&\ \ u\ \varepsilon\ v))$
SA 4. $(\forall x)(\exists z)(\forall u)(u\ \varepsilon\ z \leftrightarrow (\forall v)(v\ \varepsilon\ u \rightarrow v\ \varepsilon\ x))$

It is customary to denote the sets whose existence is asserted in SA2-SA4 as {x,y}, $\cup$(x) and *P* (x). Instead of '$\cup$(x)' and '*P* (x)' we also write '$\cup$x' and '*P* x'. {x} is short for {x,x},

N.B. these 'notational conventions' are our first examples of the mentioned practice in Set Theory to extend the language of set theory with new non-logical constants and the theory of set theory with axioms that have the form of explicit definitions for those constants. For instance, SA2 garantees the existence of an unordered pair for any two entities x and y, and it is easy to see that this pair is also unique. (This follows from the Extensionality Axiom SA1.) In other words the axioms so far adopted entail the following theorem:

(1) $(\forall x)(\forall y)(\exists z)((\forall u)(u\ \varepsilon\ z \leftrightarrow (u = x\ \ v\ \ u = y))\ \&$
$(\forall z')((\forall u)(u\ \varepsilon\ z' \leftrightarrow (u = x\ \ v\ \ u = y)) \rightarrow z' = z)))$

As we saw in Ch.2, (1) is the necessary and sufficient condition in order that adding the following definition (2) of the function constant {-,-} to any theory containing the axioms SA1 - SA2 yields a conservative extension.

(2) $(\forall x)(\forall y)(\forall z)(z = \{x,y\} \leftrightarrow (\forall u)(u\ \varepsilon\ z \leftrightarrow (u = x\ \ v\ \ u = y)))$

The same comment applies to the introduction of $\cup$ and *P*.

The next addition to our axiomatic theory is meant to capture the Comprehension Principle, the principle that for every property there exists a set which consists of just those entities which have the property (cf. Sn. 1.3.1). Here we encounter two difficulties. One of them is the problem that in this categorical form the Comprehension Principle cannot be true. (This is what Russell discovered when reading the ms.

of Frege's *Grundgesetze der Arithmetik* and explained in terms of 'Russell Paradox'.) So the best we can hope for is to adopt the principle in some weaker form.

In fact, there are two weakened versions of the Comprehension Principle which play a part in modern set theory. The first of these is due to Zermelo and the second to Fraenkel. Although the first version is logically entailed by the second, and thus the second sufficient by itself, we follow tradition in presenting both.

The first version is known as the *Aussonderungsaxiom.* This principle says that for any property P and any set x we can form the set *of those members of* x which have P. (That this is indeed a (weak) version of the Comprehension Principle follows if we assume that for each set there is the corresponding property of being a member of that set. For in that case we can form the complex property of (i) satisfying p and (ii) being a member of x; the set of all things satisfying this complex property is then the set which the Aussonderungsaxiom postulates for P and x.)

In trying to state the Aussonderungsaxiom within our language {ε} we encounter the second problem. Since we are working within first order logic, we do not have the means of quantifying over properties, and so wwe must make do with those properties which can be expressed within our language. So, just as for the Principle of Mathematical Induction in our formulation or Peano Arithmetic in Ch. 2, the best we can do is to specify the Aussonderungs-principle in the form of an axiom schema, i.e. as an infinite set of axioms, one for each formula A(u) of the language. As in the case of the Induction Schema PA7, we allow additional free variables $y_1,.., y_n$ in A. Thus the Aussonderungsaxiom takes the form given in SA5.[4]

SA 5. $(\forall x)(\forall y_1)...(\forall y_n)(\exists z)(\forall u)(u \; \varepsilon \; z \leftrightarrow (u \; \varepsilon \; x \; \& \; A(y_1,..,y_n,u)))$

[4] One might have thought that in the case of Set Theory there is no need to opt for an axiom schema: Instead of adopting an axiom for each formula A could we not quantify over sets, since sets are after all what Set Theory is about? Unfortunately this will not do. The claim - which would correspond to the categorical form of the Comprehension Principle - that for any set p there is a set z consisting of the members of p is a tautology; and the principle - corresponding to the Aussonderungsprinzip - that for any sets x and p there is a set z consisting of the members of x which are also members of p, while not actually tautologous, only asserts that the intersecion of two sets exists. This proves to be much weaker than the claim made by SA5 that every describable subset of a given set x exists.

Note that SA5. entails the existence of the intersection $x \cap y$ of two sets x and y. We obtain $x \cap y$ by applying SA5. to the formula '$u \, \varepsilon \, y$'. It is easily seen, moreover, that (4) satisfies the conditions for a definition of a 2-place function constant, and thus that we can extend our theory conservatively by adopting this defintion. (From now on we will adopt new vocabulary without making an explicit note that doing so is correct when this is obvious and/or the notation is familiar from informal treatments of Set Theory.)

(4) $(\forall x)(\forall y)(\forall z)(\forall u)(u \, \varepsilon \, z \leftrightarrow (u \, \varepsilon \, x \,\&\, u \, \varepsilon \, y)))$

The restriction which SA5 imposes on the Comprehension Principle is too severe and a set theory powerful enough to serve as framework for the formalization of mathematics and other areas of knowledge and reasoning needs something stronger. More specifically, we need a principle with the power to yield sets which are not subsets of sets that have already been constructed. The principle that has been adopted to this end, known as the "Replacement Principle"[5], is that the range of a function whose domain is a set is a set too. The Replacement principle too is a weakened version of the Comprehension Principle and one that (for all we know) is consistent.

In the formalisation of the Replacement Principle we have to deal with the same difficulty that we encountered in connection with the Aussonderungsaxiom. To state the principle we must speak about functions. But what is a function? Within set theory it is common to identify a function with its "course of values", i.e. with the set of all ordered pairs <a,b>, where a is an argument of the function and b is the corresponding value. Thus functions are sets, and if we make the usual identification of the ordered pair <a,b> with the unordered pair construct {{a}, {a,b}}, then functions are sets which are built out of their arguments and values by means that are entirely within the set formation repertoire we have already accepted in that it is entailed by the axioms SA1-SA5 already adopted.

If we were to formulate the Replacement Principle as involving functions in this sense, then we wouldn't get any sets whose existence cannot be proved from SA1-SA5. For suppose f is any function in this sense, i.e. a function-representing set of ordered pairs. Then the existence of a set consisting of the range of f is secured in any case by

[5] The replacement Axiom is the axiom of ZF that is due to Fraenkel. It is also sometimes referred to as"Fraenkel's Axiom".

SA5, viz as the set of all u such that u ε x and A, where x is the set $\cup\cup$f and A(v) is the formula $(\exists z)(\exists v)(z\ \varepsilon\ f\ \&\ z = \langle v,u\rangle)$. The existence of x is guranteed by SA3.

In order to get a version that enables to infer the existence of something whose existence isn't ascertainable in any case, we must once more make use of what can be described in our language of axiomatic set theory. This time what we want are descriptions of functions. That is, we need formulas A(u,v) with two free variables u and v, u for the argument of the function and v for the corresponding value. As in the case of SA5 we allow additional free variables $y_1,.., y_n$ in A.

This time we must be careful to make sure that our axiom schema does not overgenerate. If we allow aribitrary formulas A(u,v), then we are back at the contradiction that comes with the Comprehension Principle (e.g. by using for A(u,v) the formula '$(u = u\ \&\ \neg\ v\ \varepsilon\ v)$'. In order to avoid this we must restrict the A's that are permissible in the schema, to those which are 'functional for arguments which belong to the given set x':

(3) $(\forall u)(\forall v_1)(\forall v_2)(u\ \varepsilon\ x\ \&\ A(y_1,,y_n,u,v_1)\ \&\ A(y_1,,y_n,u,v_2) \rightarrow v_1 = v_2))$

Restricting the instances of A in the sense of (3) we obtain SA6 as formulation of the Replacement Schema

SA 6. $$(\forall x)(\forall y_1)..(\forall y_n)((\forall u)(\forall v_1)(\forall v_2)(u\ \varepsilon\ x\ \&\ A(y_1,,y_n,u,v_1)\ \& \\ A(y_1,,y_n,u,v_2) \rightarrow v_1 = v_2)) \rightarrow \\ (\exists z)(\forall v)(\ v\ \varepsilon\ z \leftrightarrow (\exists u)\ (u\ \varepsilon\ x\ \&\ A(y_1,,y_n,u,v))))$$

The axioms we have formulated so far represent a powerful set of principles to generate new sets from old ones. However, most of this power becomes relevant only when the sets involved are infinite. Generation of finite sets (more precsiely: the hereditarily finite sets) can be accomplished just with the axioms of pair formation and union, SA2 and SA3. However, there is nothing in the axioms we have so far adopted which entails the existence of any infinite set. One way in which this can be shown is to note that one the models for these axioms is the one we get when we iterate the operation $O(x) \equiv x \cup P\, x$ an infinite number of times, but stop at the first opportunity. As we observed earlier, the elements of this model are the hereditarily finite sets and it is straightforward to show that this is a model of SA1-SA6

So we need a further axiom - an "Axiom of Infinity" - to guarantee the existence of infinite sets. Interestingly, we need to postulate the existence of only one infinite set, for once such a set has been given, the axioms we have adopted generate a large (in fact, dazzlingly large) multitude of such sets.[6] There is a large number if different ways in which this requirement could be fulfilled. The form in which the axiom is usually giv en is as the claim that there is a set which (i) contains the empty set $\varnothing$ and (ii) contains for each of its members w also the 'successor' of w, i.e. the set $w \cup \{w\}$.

SA 7 $(\exists y)(\varnothing \,\varepsilon\, y \;\&\; (\forall w)\, (w \,\varepsilon\, y \rightarrow (w \cup \{w\}) \,\varepsilon\, y))$

It should be intuitively clear that any set y which (i) contains $\varnothing$ and (ii) contains $w \cup \{w\}$ whenever it contains w must be infinite. In fact, we can prove that the sets $\varnothing, \varnothing \cup \{\varnothing\}, \varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}$, ... are all members of such a y and also that they are all distinct from each other. In this way we can show that y has more elements than any finite number n.

It is easy to show that among the sets y which satisfy conditions (i) and (ii) there must be a minimal one. Let y_1 be any set satisfying (i) and (ii). If there is any other set y_2 which also satisfies these conditions, then the intersection $y_1 \cap y_2$ satisfies the conditions as well. So the smallest subset of y_1 which satisfies the conditions will necessarily be the smallest such set in absolute terms. Let S be the set of all subsets y of y_1 such that (i) $\varnothing \,\varepsilon\, y$ and (ii) $(\forall w)\, (w \,\varepsilon\, y \rightarrow (w \cup \{w\}) \,\varepsilon\, y)$ and let y_o be the set defined by

$(\forall v)(v \,\varepsilon\, y_o \leftrightarrow (v \,\varepsilon\, y_1 \;\&\; (\forall y)\, (y \,\varepsilon\, S \rightarrow v \,\varepsilon\, y)))$

Then clearly y_o satisfies (i) and (ii) and furthermore $y_o \subseteq y$ for every subset y of y_1 satisfying (i) and (ii).[7] So y_o is indeed the smallest set with these properties. An informal argument shows that y_o consists just of the sets $\varnothing$ (= "0"), $\varnothing \cup \{\varnothing\}$ (= "1"), $\varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}$ (= "2"),.. .

[6] The need to postulate the existence of an infinite set was one of the disappointments of the so-called 'logicist programme', of which both Frege and Russell were advocates, to reduce mathematics to logic. It is hard too accept the existence of infinite sets as a principle that is valied for logical reasons.

[7] Here of course "$y_o \subseteq y$" is short for "$(\forall z)\, (z \,\varepsilon\, y_o \rightarrow z \,\varepsilon\, y)$".

It should be clear that the set y_0 is uniquely determined by the conditions we have used to define it. y_0 is usually referred to as "ω". The set ω plays a pivotal role in Set Theory. We will soon meet it again when we will develop the concept of an ordinal. ω will be the *first transfinite ordinal.*

We are now in a position to give an impression of the importance of SA6. Given the existence of ω we can of course prove, using SA2 and SA3, that the sets $\omega \cup \{\omega\}$ (= "ω + 1"), $(\omega \cup \{\omega\}) \cup \{\omega \cup \{\omega\}\}$ (= "ω + 2"), ω +3, etc. exist as well. These sets form another infinite sequence, and it seesm reasonable to assume that this sequence too has a 'limit', just as the sequence 0, 1, 2, ... has the limit ω . But it is only with the help of SA6. that can show that this limiting set actually exists.

The argument goes as follows. Let A(x,y) be the formula:

$(x = \varnothing \ \& \ y = \omega) \vee ((\exists u)(x = u \cup \{u\} \ \& \ (\forall w)\ (A(u,w) \rightarrow \ y = w \cup \{w\}))$

It is easy to show that for all $n \ \varepsilon \ \omega$, (i) $(\exists v)\ A(n,v)$ and (ii) $(\forall v)\ (\forall w)(A(n,v) \ \& \ (A(n,w) \rightarrow \ v = w)$. To see this it is enough to observe that (a) $\varnothing$ is a set n satisfying (i) and (ii) and (b) if any set n satisfies (i) and (ii), then so does $n \cup \{n\}$. Since ω is by definition the smallest set S with the properties that $\varnothing \ \varepsilon$ S and that whenever $n \ \varepsilon$ S then $n \cup \{n\} \ \varepsilon$ S, it follows that all members of ω satisfy (i) and (ii). To show (a) and (b) we proceed as follows. First, it is clear that there is exactly one set v such that $A(\varnothing,v)$, viz. ω. for when $n = \varnothing$ only the first disjunct of A is relevant. So (a) holds. Second, suppose that n satisfies (i) and (ii). Let y be the unique v such that A(n,v). To see that $n \cup \{n\}$ also satisfies (i) and (ii), note that now only the second disjunct of A is relevant. But from the second disjunct of A it is obvious that there is exactly one z such that $A(n \cup \{n\}, z)$, viz. the set $y \cup \{y\}$.

This shows that for all $n \ \varepsilon \ \omega$ there is exactly one w such that A(n,w). So we can apply SA6. with ω for x and the given formula A. The resulting instance of SA6. allows us to conclude that there is a set S which contains the sets "ω+ n" for all $n \ \varepsilon \ \omega$.

The Axioms SA1-SA7 make up what is often identified as "Zermelo-Fraenkel Set Theory" or ZF, after Ernst zermelo and Abraham Fraenkel, the two mathematicians who were responsible for its formulation.[8] Often one adds to this system two additional axioms. The first seems to be evidently true of the structure of all sets as we intuit it, and so should, from our perspective, be included. This axiom expresses the idea that all sets are "built up from below". The idea is that when you take any set and try to make your way down to its "foundation" - by taking a member of the set, then a member of this member, then a member of that member, etc. - you must come to an end after a finite number of steps: There are no inifinite descending 'ε-sequences'.

That the following axiom expresses this intuition is not immediately obvious.:

SA 8. $(\forall x)\ (x \neq \emptyset \rightarrow (\exists y)(y\ \varepsilon\ x\ \&\ y \cap x = \emptyset))$

In fact, that SA8 does indeed prevent the existence of any infinite chain of sets s_n such that for all n $s_{n+1}\ \varepsilon\ s_n$, is quite involved and exploits deduction strategies that are specific to formal set theory and that it would carry us too far at this point to explain in sufficient detail. Sometimes one distinguishes explicitly between the theory axiomatised by SA1-SA7 ("ZF without Foundation“) and the one axiomatised by SA1-SA8 ("ZF with Foundation"). We will assume that SA8 is part of what we call ZF.

The last axiom - the *Axiom of Choice* (AC) - is generally regarded as more difficult to justify on intuitive grounds than those we have already considered. For this reason it is usually not considered as an integral part of ZF as such. But it has a reasonable degree of plausibility nonetheless, and it entails a large number of important set-theoretic results which cannot be proved without it. For this reason it has become standard practice to distinguish between ZF with and without AC. (The combination wird usually denoted as ZF+AC.)

The Axiom of Choice can be formulated in an astoundingly large number of different ways, some of which are very different from each other. But all of them can be shown equivalent on the basis of the axioms SA1 - SA7, so which formulation one chooses doesn't really matter in the end. In its perhaps most familiar form the axiom says that for any set x whose members are non-empty sets there exists a

[8] Fraenkel's only contribution to ZF is the Replacemernt Schema. We have just had a glimpse of the importance of this axiom, and we will soon have plenty of additional evidence. In fact the role of SA6 within ZF is so crucial, that it fully justifies the inclusion of Fraenkel's name in the designation of the theory.

function f with domain x which selects for each y in x a value f(y) that is an element of x. Note well that in this case the function which the AC asserts to exist is a function in the sense of set-theoretic object, i.e. a set of ordered pairs.

SA 9. $(\forall x)\ ((\forall y)\ (y\ \varepsilon\ x \rightarrow y \neq \varnothing) \rightarrow (\exists f)(\mathrm{function}(f)\ \&\ \mathrm{Dom}(f) = x\ \&\ (\forall y)\ (y\ \varepsilon\ x \rightarrow f(y)\ \varepsilon\ y))$[9]

Experience with the theory ZF has shown that essentially all the theorems of set theory that have been proved by methods accepterd within mathematics can be formulated and formally derived within it. As an example, consider Cantor's Theorem, according to which there exists no injection of the power set $P(x)$ of a given set x into x.

Cantor's Theorem asserts that there exists no function of a certain kind. This involves quantification over functions. Since in ZF we can quantify only over sets we must once again make use of the set-theoretical concept of a function according to which it is a set of ordered pairs. Thus we come to the following formal statement (4) of the theorem.

(4) $(\forall x) \neg (\exists f)(\mathrm{Dom}(f) = P(x)\ \&\ \mathrm{Ran}(f) \subseteq x)$

(Here "$\mathrm{Dom}(f) = P(x)$" is to be understood as in the explanation of SA9. and "$\mathrm{Ran}(f) \subseteq x$" is short for $(\forall v)(\exists u)\ \langle u,v\rangle\ \varepsilon\ f \rightarrow v\ \varepsilon\ x)$).

Within ZF the proof of Cantor's Theorem goes roughly as follows. Suppose that f were an injection of $P(x)$ into x, for some set x. Let S be the set of all u ε $P(x)$ such that $\neg(f(u)\ \varepsilon\ u)$ - formally:

(5) $(\forall u)(\ u\ \varepsilon\ S \leftrightarrow u\ \varepsilon\ P(x)\ \&\ \neg(f(u)\ \varepsilon\ u)$.

That this set exists follows from SA5, taking $P(x)$ as x and $\neg(f(u)\ \varepsilon\ u)$ as A(u). But now we can prove: $f(S)\ \varepsilon\ S \leftrightarrow \neg(f(S)\ \varepsilon\ S)$. Since this is a contradiction, the assumption that there exist x and f as hypothesized has been refuted; thus Cantor's Theorem has been proved.

[9] The part beginning with "$(\exists f)$" would, in basic notation, be: $(\exists f)((\forall u)(u\ \varepsilon\ f \leftrightarrow (\exists v)(\exists w)(v\ \varepsilon\ x\ \&\ u = \langle v,w\rangle\ )\ \&$ $(\forall y)\ (y\ \varepsilon\ x \rightarrow (\exists w)(\langle v,w\rangle\ \varepsilon\ f\ \&\ w\ \varepsilon\ y)))$

This 'proof' of Cantor's Theorem looks superficially very much like the proof that was presented in Ch. 1. But there is a difference of purport. The argument we have just presented is to be seen as an outline of what can be turned into a formal (i.e. axiomatic) derivation of the formal statement of Cantor's Theorem from the Axioms of ZF.
It should be emphasised that all proofs offered in this chapter should be understood in this way; they are all sketches of proofs that can be implemented as axiomatic derivations from ZF. In practice it hardly ever makes sense to carry out such derivations in full detail. Such derivations tend to conceal the ideas on which the proof is based behind a welter of formally necessary but intuitively trivial inference steps with which the intuitive ideas have next to nothing to do.

##

Since ZF is a first order theory, it is subject to all the general results that apply to such theories. In particular, it is subject to the downward Skolem-Löwenheim Theorem. In the case of set theory this seems particularly puzzling. For suppose that ZF is consistent. (This is something we cannot prove. But now, after many decades of intimate experience with the theory which should have given much opportunit which should have given much opportunity to discover an inconsistency if indeed there was one, it seems very unlikely that the theory would be inconsistent after all.) Then ZF has a model (which, as can easily be shown, must be infinite) and so by Skolem-Löwenheim it must have a denumerable model - M, say. Clearly M is not the intended model of ZF. For the "real" structure of all sets is surely non-denumerable. For one thing, any model of ZF must, in view of the axiom of infinity, have a set "ω" and this set will be infinite, since it contains each of the sets $\varnothing, \varnothing \cup \{\varnothing\}, \varnothing \cup \{\varnothing\} \cup \{\varnothing \cup \{\varnothing\}\}$, ... and such sets will also be elements of the model and will all be distinct. But when ω belongs to the model, then so does $P(\omega)$ and this set is, by Cantor's Theorem, non-denumerable. In other words, there should be non-denumerably many elements in the model which all stand in the ε–relation to $P(\omega)$. But how can that be if M is only denumerable?

The paradox dissolves when we reflect on the exact meaning of Cantor's Theorem in the ZF formulation given above. In this formulation the theorem says that there is no "functional" set of ordered pairs which maps $P(\omega)$1-to-1 into ω. But does this really mean that $P(\omega)$ is non-denumerable? Well, it wouldn't if there weren't all that many functions within the model M, so that even if $P(\omega)$ is denumerable from an external point of view, this fact could not be established within M for lack of the right function.

The existence of such models as M is thus no contradiction after all. It isn't a contradiction, because the axioms of ZF, while truly asserting the existence of such infinite sets as ω, do not succeed in truly asserting the existence of non-denumerably infinite powersets, such as $P(\omega)$. A denumerable set may behave, from the internal perspective of a given model, as non-denumerable simply because there are too few functions to expose it as a "fake non-denumerable" set, even though from an external perspective that is what it is, since an injection of it into ω does in fact exist.

Ordinals and Cardinals

We now proceed to develop the basics of an important part of set theory, the theory of ordinals and cardinals. We follow the now generally adopted approach originally due to Von Neumann.

Both the notion of an ordinal and that of a cardinal were invented by Cantor, as part of his attempts to develop a general consistent theory of infinite sets. Cantor was interested in particular in distinguishing between different kinds of infinity, something for which Cantor's Theorem provides the basis: The power set of any infinite set is x of a different, "higher" degree of infinity than is x itself. This distinction gives rise to the notion of *cardinality* and of *cardinal number*. Two sets have the same cardinality iff they can be injected into each other. Thus a set and its power set are always of distinct cardinality. Cantor then tried to develop a notion of cardinal number such that two sets have the same cardinal number iff they have the same cardinality.

Cantor also developed a more fine-grained method of counting infinite sets, which applies directly only to sets whose members are given in some order. The members of such sets would then be each assigned an ordinal number, and the set as a whole would be assigned the first ordinal number after all those assigned to members in it. Thus ordinal numbers were meant to be used as means of "counting" infinite sets in much the same ways as the natural numbers are used to count finite sets. This role that ordinal numbers were meant to play led to the idea that the class of all ordinals can be generated by the same kind of iterative procedure that is also assumed to generate the stucture of all sets: Each ordinal x gives rise to a next ordinal, the *successor* of x; and whenever a certain unbounded family of ordinals has been constructed, the limit of this family will once again be an ordinal, the first ordinal after all the members of the family. The problem with such an inductive characterization of the generation process is that it is not quite clear how far it goes. For it is clear that not every unbounded family of ordinals will have an ordinal as limit. In particular the family of all ordinals - which is unbounded, as for each ordinal there is also its successor - cannot have such a limit. For if Ω were this ordinal, then Ω would be a member of the family of all ordninals and so would its successor. But then Ω would not come after all ordinals in the family: contradiction.

So, for which unbounded families of ordinals may it be assumed that limits exist? There seems no easy answer to this question. However, Von Neumann came up with a very ingenious solution, which consists in giving an explicit definition of a concept of "ordinal number", which apparently satisfies all the intuitive requirements that Cantor and the set theorists coming after him demanded of it. In this definition the successor of an ordinal x is defined by the operation we have already encountered a number of times, viz. as $x \cup \{x\}$. Von Neumann's explicit definition of the property of being an ordinal identifies the ordinals with those sets which are (i) linearly ordered by ε and (ii) are transitive - a transitive set being one which has the property that the members of its members are also members of it. Here is the formal definition:

Definition. A set x is an *ordinal* iff

(i) x is linearly ordered by ε, i.e. we have for all members u, v, w of x:

(a) $(u \varepsilon v \ \& \ v \varepsilon w) \rightarrow u \varepsilon w$

(b) $u \varepsilon v \ \ v \ \ u = yv \ v \ \ v \varepsilon u$

(ii) x is *transitive*, i.e. for any y and z such that $y \varepsilon x$ and $z \varepsilon y$, we have $z \varepsilon x$.[10]

[10] In the version of ZF we have presented here, in which the well-foundedness axiom SA8 is one of the axioms, this definition is adequate in the sense that oit supports all the theorems about ordinaly which follow. There also developments of set theory in which well-foundedness is not taken for granted - that is, SA8 is not adopted aas an axiom, or at least not from the outset. Withn such a weaker set-theory it is still possible to develop the theory of the ordinals on the basis of an explicit defintion, but now this definition must include the clause that an ordinal x is a set of sets which is well-ordered by ε - that is: if x is not empty, then there is a member of x which contains no member of x. (Exercise: Check that with this extra clause in the definition of 'ordinal' all the proofs which follow can be carried out without the use of SA8)

We write "Ord(x)" to express that x is an ordinal.

We can prove, in the order in which they are listed, the following theorems about ordinals:

<u>Theorem O1</u>. Ord($\varnothing$); Ord($\{\varnothing\}$); Ord($\{\varnothing,\{\varnothing\}\}$); etc.

<u>Theorem O2</u>. $(\forall x)(\mathrm{Ord}(x) \rightarrow \mathrm{Ord}(x \cup \{x\}))$

<u>Proof.</u> Suppose that Ord(x). So x is transitive and linearly ordered by ε. We must show (i) that $x \cup \{x\}$ is linearly ordered by ε and (ii) that x U {x} is transitive. (ia). Let u, v, $w \,\varepsilon\, x \cup \{x\}$ such that $u \,\varepsilon\, v \,\varepsilon\, w$. When u, v, $w \,\varepsilon\, x$, then $u \,\varepsilon\, w$, since Ord(x). If $u = x$ or $v = x$ then we have a violation of axiom SA 8. So the only remaining possibility is that where u, $v \,\varepsilon\, x$ and $w = x$. But then again $u \,\varepsilon\, w$. (ib) Suppose that u, $w \,\varepsilon\, x \cup \{x\}$. We want to show that $u \,\varepsilon\, w \vee u = w \vee w \,\varepsilon\, u$. If u, $w \,\varepsilon\, x$, this follows from the fact that Ord(x). If $u = x$ & $w = x$ then $u = w$; if $u \,\varepsilon\, x$ & $w = x$, then $u \,\varepsilon\, w$; if $w \,\varepsilon\, x$ & $u = x$, then $w \,\varepsilon\, u$. (ii) Let $u \,\varepsilon\, w \,\varepsilon\, x \cup \{x\}$. We want to show that $u \,\varepsilon\, x \cup \{x\}$. If $w \,\varepsilon\, x$, then $u \,\varepsilon\, x$ because x is transitive, so $u \,\varepsilon\, x \cup \{x\}$. If $w = x$, then again $u \,\varepsilon\, x$ and so $u \,\varepsilon\, x \cup \{x\}$.

<u>Theorem O3.</u> $(\forall x)(\mathrm{Ord}(x) \rightarrow (\forall y)(y \,\varepsilon\, x \rightarrow \mathrm{Ord}(y))$

<u>Proof</u>: Exercise

<u>Theorem O4.</u>

$$(\forall x)(\forall y)((\mathrm{Ord}(x) \;\&\; \mathrm{Ord}(y)) \rightarrow (x \,\varepsilon\, y \vee x = y \vee y \,\varepsilon\, x)) \qquad (1)$$

<u>Proof.</u> Suppose the theorem does not hold. Then there is a counterexample to (1), i.e. there are x, y such that

(2) $(\mathrm{Ord}(x) \;\&\; \mathrm{Ord}(y)) \;\&\; \neg(x \,\varepsilon\, y) \;\&\; x \neq y \;\&\; \neg(y \,\varepsilon\, x)$.

With regard to x there are two possibilities: (a) there is no $x' \,\varepsilon\, x$ such that (2) holds with x' for x and some y' or other for y. (b) there exists such an x'. In this second case we can form the set of all those $x' \,\varepsilon\, x$ for which there is a y' so that x' and y' satisfy (2). Since this set is by assumption non-empty, it has by SA8, a member x_o whose intersection with the set is empty. For this x_o we are then in case (a). Having thus obtained a minimal x_o we can now also find a minimal y_o among the y which jointly with x_o provide a counterexample to (1). Now let u be any member of x_o. Then, since Ord(x_o), Ord(u). Since also Ord(y_o) and x_o, y_o form a minimal counterexample to (1), we have: $u \varepsilon y_o \vee u = y_o \vee y_o \varepsilon u$. When $u = y_o \vee y_o \varepsilon u$, then $y_o \varepsilon x_o$, contrary to assumption. So $u \varepsilon y_o$. Since this holds for arbitrary $u \varepsilon x_o$, we have

(3) $(\forall u)(u \varepsilon x_o \rightarrow u \varepsilon y_o)$

Now let w be any member of y_o. Then as above we infer from minimality of y_o that $w \varepsilon x_o \vee w = x_o \vee x_o \varepsilon w$, and, again as above, that of these three possibilities only $w \varepsilon x_o$ is a live option. So we get

(4) $(\forall w)(w \varepsilon x_o \rightarrow w \varepsilon y_o)$

From (3) and (4) we get by extensionality: $x_o = y_o$, which contradicts the assumption that x_o, y_o satisfy (2). So (1) holds without exception.

<u>Theorem O5</u>. $(\forall x)((\forall y)((y \varepsilon x \rightarrow \text{Ord}(y)) \rightarrow \text{Ord}(\cup x))$

<u>Proof</u>: Exercise.

<u>Theorem O6.</u> Ord(ω)

<u>Proof</u>. The strategy we will follow is to show that (a) all members of ω are ordinals and (b) that $\omega = \bigcup\omega$. Since by Theorem O5 and (a) Ord($\bigcup\omega$), (b) completes the proof.

(a) Let S be the set of all $x \varepsilon \omega$ such that Ord(x). (This set exists in virtue of SA5.) It is easy to show that S satisfies the conditions (i) $\varnothing \varepsilon S$ and (ii) $(\forall w)(w \varepsilon S \rightarrow w \cup \{w\} \varepsilon S)$. So, since ω is the smallest set satisfying these conditions, $\omega \subseteq S$. This concludes the proof of (a).

(b) First suppose that $u \varepsilon \omega$. Then $u \cup \{u\} \varepsilon \omega$. so there is a y such that $u \varepsilon y \varepsilon \omega$. So $u \varepsilon \cup\omega$. To show that $\cup\omega \subseteq \omega$ we proceed as under (a): Let S' be the set of all x in ω such that $(\forall w)(w \varepsilon x \rightarrow w \varepsilon \omega)$. Again we can show that S' satisfies the two conditions (i) and (ii) mentioned under (a). So $\omega \subseteq S'$. So if $u \varepsilon y \varepsilon \omega$, then $u \varepsilon \omega$. Now suppose that

$u \ \varepsilon \cup \omega$. Then for some y, $u \ \varepsilon \ y \ \varepsilon \ \omega$. So $u \ \varepsilon \ \omega$.

ω is our first example of an ordinal which is unbounded, in the set that for each $x \ \varepsilon \ \omega$ there is a $y \ \varepsilon \ \omega$ such that $x \ \varepsilon \ y$. Such ordinals are also called *limit ordinals.* If an ordinal is not a limit ordinal. it is, according to Thm O7 below, always of the form $w \cup \{w\}$. Such ordinals are called *successor ordinals*:

Definition. *LimOrd(*x) iff Ord(x) & $x \neq \varnothing$ & $(\forall w)(w \ \varepsilon \ x \rightarrow (\exists v)(w \ \varepsilon \ v \ \& \ v \ \varepsilon \ x))$

SuccOrd(x) iff Ord(x) & $(\exists v)(x = v \cup \{v\})$

Theorem O7. If Ord(x), then either (i) x = or (ii) SuccOrd(x) or (iii) LimOrd(x).

Proof: Exercise.

We already showed that with the help of SA7 we can prove the existence of the limit of the ordinals ω , $\omega + 1$, $\omega + 2$, ... (This is the ordinal we denoted as $\omega + \omega$.) In fact, SA7 makes it possible to prove the existence of a huge, barely surveyable, spectrum of limit ordinals beyond ω. Nevertheless, all ordinals that can be obtained by such methods are denumerable, i.e. stand in one-one correspondence with ω. To prove the existence of non-denumerable ordinals we have to appeal to a principle of a very different sort, which is implicit in the Axiom of Choice SA9. To establish this principle, the so-called Well-ordering Theorem, we need another, equally fundamental result, known as the Recursion Theorem.

The Recursion Theorem says, roughly, that recursive definitions along the ordinals constitute a valid means of defining functions. The theorem can be stated in a variety of ways. The one chosen here is inspired partly by the specific use to which we will put the theorem below.

In order to facilitate the statement of the theorem and the formulation of its proof, we introduce two notatonal devices. The first is a matter of strightforward definition. It will be conventient to have a compact notaton for the restriction of a function f to a certain set X. This restriction is the function whose domain is the intersection of X with the domain of f and which assigns to the arguments in its domain the same values as f. To indicate restriction we use the symbol "$\restriction$". Thus "$f\restriction X$" stands for the set of all pairs <x, y> such that <x, y> ε f and x ε X.

The second bit of notation is a little more involved and needs to be handled with more care. One of the most common devices in natural language is the definite dscriptive term, such as "the King of France" or "the smallest perfect number" or "the empty set". The semantics of such terms is apparently that they denote the unique thing satisfying their descriptive content (i.e. the property expressed by their common noun phrase), provided there is just one such thing; but when there is no such thing, or if there is more than one, then there seems to be something wrong with the description - it is no longer clear what the description denotes; arguably it doesn't denote anything. Because of the danger of denotation failure, the device of definite description isoften excluded from the notational repertoire of formal logic, a policy which we have been following here too. But sometimes the device is handy and allows for more perspicuous formulas than would be availableotherwise. And since that will be the case in the Recursion Theorem to be stated presently, we introduce the device now.

For any variable x and formula A (typically, with free occurrences of the variable x, though strictly speaking we do not need to make this restriction) let "(Tx)A" stand for the unique x such that A(x). We will use this expression as a term, i.e. as occupying argument positions of predicates. Thus we will write for instance "P(c, (Tx)A)" to express the proposition that c stands in the relation P to the unique x such that A. However, we will only do so in contexts in which the unique existence of such an x is guaranteed, i.e. where the formula

(*) $(\exists x)\ (A(x)\ \&\ (\exists y)\ (A(y) \rightarrow x = y))$

holds. Note that where this conditon is fulfilled we can eliminate every occurrence of (Tx)A using notaton we already have. For instance, "

$$P(c,\ (Tx)A)$$

can then be rewritten as

$$(\exists x)\ (A(x)\ \&\ (\exists y)\ (A(y) \rightarrow x = y)\ \&\ P(c,\ x)).$$

When the formula in which the term "(Tx) A" occurs is complex, there are usually a numer of different ways in which its elimination might be carried out. For instance, we might get rid of the term from the sentence $\neg P(c, (Tx)A)$ either by placing the quantificational complex inside the scope of or outside it, getting, respectively, (a) and (b):

(a) $(\exists x)\ (A(x)\ \&\ (\exists y)\ (A(y) \rightarrow\ x = y)\ \&\ \neg P(c,\ x)).$

(b) $\neg(\exists x)\ (A(x)\ \&\ (\exists y)\ (A(y) \rightarrow\ x = y)\ \&\ P(c,\ x)).$

But under the required conditions (i.e. that (*) holds) such alternative eliminations are provably equivalent.

<u>Exercise.</u> Show that

$$\vdash (*) \rightarrow ((a) \leftrightarrow (b))$$

Equipped with these additrional means of notation we return to the Recursion Theorem. Suppose we want to define a function $f(\alpha, x_1,..., x_n)$, where α ranges over an ordinal γ and the x_i over some set X, and that we want to do this by (i) specifying, for arbitrary $x_1,..., x_n \varepsilon X$, the values of $f(0, x_1,..., x_n)$; (ii) specifying for arbitrary $x_1,..., x_n \varepsilon X$ and successor ordinal $\alpha + 1 \varepsilon \gamma$, the values of $f(\alpha + 1, x_1,..., x_n)$ on the basis of those of $f(\alpha, x_1,..., x_n)$; and (iii) specifying for arbitrary $x_1,..., x_n \varepsilon X$ and limit ordinals $\lambda \varepsilon \gamma$, the values of $f(\lambda, x_1,..., x_n)$ on the basis of the set of all $f(\beta, x_1,..., x_n)$ with $\beta < \lambda$, λ and $x_1,..., x_n$. Then a function f satisfying just those stipulations will indeed exist. (In fact, the proof of the theorem indicates a method for constructing an explicit definition of this function and prove of this definition that it is a proper defnition in the sense that it is satisfied by exactly one object, which satisdfies the imposed criteria. But this is an further aspect of the Recursion Theorem that we will notgo into here.)

More precisely, let $A(x_1,..., x_n, y)$ be a formula which is "functional in y" provided the $x_1,..., x_n$ are taken from $X_1,..., X_n$, i.e.

(1) $(\forall x_1)(\forall x_2)..(\forall x_n)(\forall y)(\forall z)(x_1 \varepsilon X_1\ \&\ ...\&\ x_n \varepsilon X_n \rightarrow$
$(A(x_1,..., x_n, y)\ \&\ A(x_1,..., x_n, z) \rightarrow\ y = z)\ )$

Similarly, let $B(x_1,..., x_n, u, v, y)$ and $C(x_1,..., x_n, u, v, y)$ be formulas which express a functional dependency of y on any $x_1,..., x_n \varepsilon X_1,..., X_n$, arbitrary u and $\alpha \varepsilon \gamma$:

(2) $(\forall x_1)(\forall x_2)..(\forall x_n)(\forall u)(\forall \alpha)(\forall y)(\forall z)(x_1 \varepsilon X_1\ \&..\&\ x_n \varepsilon X_n\ \&$

$\alpha + 1 \,\varepsilon\, \gamma \rightarrow (B(x_1,\ldots,x_n,u, \alpha + 1, y) \;\&\; B(x_1,\ldots,x_n,u,\alpha + 1, z) \rightarrow y = z))$

(3) $(\forall x_1)(\forall x_2)..(\forall x_n)(\forall u)(\forall \lambda)(\forall y)(\forall z)(x_1 \,\varepsilon\, X_1 \;\&..\&\; x_n \,\varepsilon\, X_n \;\&\; \lambda \,\varepsilon\, \gamma$
$\&\; \mathrm{limord}(\lambda) \rightarrow (C(x_1,\ldots,x_n, u, \lambda, y) \;\&\; C(x_1,\ldots, x_n, u, \lambda, z) \rightarrow y = z))$

Then there is a unique function f which is defined on the $X_1,\ldots, X_n$ and and which, for arbitrary $x_1 \,\varepsilon\, X_1,. .., x_n \,\varepsilon\, X_n$, and $\beta + 1, \lambda \,\varepsilon\, \gamma$ satisfies the following three conditions:

(i) $f(0, x_1,\ldots, x_n) = \mathrm{Ty}\; A(x_1,\ldots, x_n, y)$
(ii) $f(\beta + 1, x_1,\ldots, x_n) = \mathrm{Ty}\; B(x_1,\ldots,x_n, f\lceil(\beta+1), \beta, y)$
(iii) $f(\lambda, x_1,\ldots, x_n) = \mathrm{Ty}\; C(x_1,\ldots,x_n,f\lceil\lambda, \lambda\square, y)$

<u>Proof of the Recursion Theorem:</u>

We begin by proving that

(*) For fixed $x_1 \,\varepsilon\, X_1,. .., x_n \,\varepsilon\, X_n$ there exists a function $f_{\{x_1,\ldots, x_n\}}$ defined on γ such that the clauses (i), (ii) and (iii) hold for the given $x_1,\ldots, x_n$ and arbitrary $\beta + 1, \lambda \,\varepsilon\, \gamma$.
(We omit the subscript $\{x_1,\ldots, x_n\}$ for ease of notation).

We prove by induction on ordinals $\beta < \gamma$ the following statement:

(4) (1) There exists exactly one function f^β with domain equal to $\beta + 1$ and which, for ordinals belonging to $\beta + 1$ satisfies the clauses (i), (ii), (iii); and
(2) whenever $\delta < \beta$, then $f^\delta \subseteq f^\beta$.

We consider the three cases (a) $\beta = 0$; (b) $\beta = \alpha + 1$; and (c) $\beta = \lambda$, where $\mathrm{limord}(\lambda)$

(a) Let

(5) $f^0 = \{<0, \mathrm{Ty}\; A(x_1,\ldots, x_n, y)>\}$.

It is easy to verify that (4.1) and (4.2) are both satisfied.

(b) Assume (4) for ordinals $< \alpha + 1$. Let

(6) $f^{\alpha+1} = f^\alpha \cup \{< \alpha + 1, \mathrm{Ty}\; B(x_1,\ldots, x_n, f^\alpha, \alpha + 1, y) >\}$.

It is easy to see that $f^{\alpha+1}$ satisfies the conditions (i)-(iii). To see that it is the only such function, suppose there are two such functions, g and g'. Then for some β, $g(\beta) \neq g'(\beta)$. Let δ be the smallest such β. If $\delta < \alpha +1$ then $g\lceil(\delta +1) \neq g'\lceil(\delta +1)$. But it is easy to verify that both $g\lceil(\delta +1)$ and $g'\lceil(\delta +1)$ are functions with domain $\delta +1$ which satisfy conditions (i)-(iii). So by induction hypothesis they are both identical to f^{δ}, and so must be identical to each other: contradiction. The remaining possibility is that $\delta = \alpha +1$. But then $g\lceil(\delta +1) = g'\lceil(\delta +1) = f^{\alpha}$. Since g and g' also satisfy clause (ii) for the case where $\beta = \alpha$, it is easily verified that they are both equal to $f^{\alpha+1}$ as defined in (6).
Finally, let δ be any ordinal $< \alpha +1$. Since $f\lceil(\delta +1)$ has domain $\delta +1$ and evidently satisfies (i)-(iii), it follows by induction that

(7) $f^{\delta} = f\lceil(\delta +1) \subseteq f^{\alpha+1}$.

(c) Let λ be a limit ordinal $< \gamma$ and assume (4) for all ordinals $< \lambda$. We put

(8) $f^{\lambda} = \cup_{\beta<\lambda} f^{\beta} \cup \{< \lambda, \text{Ty } C(x_1,..., x_n, \cup_{\beta<\lambda} f^{\beta}, \lambda, y) >\}$.

Note that since for all $\delta < \beta < \lambda$, $f^{\delta} \subseteq f^{\beta}$, $\cup_{\beta<\lambda} f^{\beta}$ is a function. So f^{λ} is a function too. Again it is easy to verify that this function satisfies (i)-(iii), that its domain is $\lambda +1$. To show that it is the only function with these properties and that for $\beta < \lambda$, $f^{\beta} \subseteq f^{\lambda}$, one proceeds as under (b).

To obtain the existence of a function f defined on $X_1 \times ... \times X_n \times \gamma$ which satisfies (i) - (iii) for arbitrary $x_1 \varepsilon X_1,..., x_n \varepsilon X_n$, and arbitrary $\alpha \varepsilon \gamma$, we observe that we could have proceeded just as well in the proof just given by adding at each stage pairs of the forms (5), (6) and (8), resepctively for all possible combinations of $x_1 \varepsilon X_1,..., x_n \varepsilon X_n$. It is easily seen that the above proof goes through essentially unchanged.

The recursion Theorem enables us to assert the existence of, among many other things, certain "arithmetical" operations on ordinals, in particular ordinal addition and multiplication. That is, for any ordinal γ there are 2-place functions $+_{\gamma}$ and $._{\gamma}$ defined on $\gamma \times \gamma$ such that the following holds for ordinals $\alpha, \beta < \gamma$:

(i_+) $\alpha +_{\gamma} 0 = \alpha$

(ii+) $\alpha +_{\gamma} (\beta+1) = (\alpha+_{\gamma} \beta) +1$

(iii+) $\alpha +_{\gamma} (\lambda) = \bigcup_{\beta \, \varepsilon \, \lambda} (\alpha+_{\gamma} \beta)$

(i.) $\alpha \cdot_{\gamma} 0 = 0$

(ii.) $\alpha \cdot_{\gamma} (\beta+1) = (\alpha \cdot_{\gamma} \beta) + \alpha$

(iii.) $\alpha \cdot_{\gamma} (\lambda) = \bigcup_{\beta \, \varepsilon \, \lambda} (\alpha \cdot_{\gamma} \beta)$

For finite ordinals these operations are just the addition and multiplication familiar from ordinary artihmetic. To be precise, $+_{\gamma}$ is the set of all triples <<n,m>, n + m>, where n and m are finite ordinals and "+" is the operation of ordinary arithmetical addition on the natural numbers (which according to the set-theoretical perspective just are the finite ordinals); and similarly for $\cdot_{\gamma}$. However, for infinite ordinals the operations behave in a way which is quite surprising for someone used to the "plus" and "times" on the natural numbers. For instance, neither additoion nor multiplication are in general commutative. This is a consequence of a kind of absorption that happens when the left argument the operation is much smaller than its right argument. Thus we have in particular:

(OA.1) If n is finite and α is infinite, then
(i) $n + \alpha = \alpha$
(ii) $n \cdot \alpha = \alpha$

So we have for instance: $1 + \omega = \omega$ and $2 \cdot \omega = \omega$; and since $\omega \neq \omega + 1$ and $\omega \neq \omega \cdot 2$, the commutative laws "$\alpha + \beta = \beta + \alpha$" and "$\alpha \cdot \beta = \beta \cdot \alpha$" and are not generally valid.

Exercise: prove (OA.1) and the inequalities following it.

On the other hand the associative laws hold without exception:

(OA.2) (i) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
(ii) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

Exercise: Of the following two putative laws one is generally valid while the other is not. Prove the validity of the valid one and give a counter-example to the other one:

(OA.3) (i) $(\alpha + \beta) \cdot \gamma = (\alpha \cdot \gamma) + (\beta \cdot \gamma)$
(ii) $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$

Well-Foundedness and the Well-Ordering Theorem.

The next important theorem we need to establish is the so-called Well-ordering Theorem, which asserts that every set can be put into a 1-1 correspondence with some ordinal. We can also express this using the term *equipollent*.

Def. Let X and Y be sets. X and Y are *equipollent* iff there exists a bijection from X to Y.

So we can also express the Well-ordering Theorem by saying that every set is equipollent with some ordinal.

The Well-ordering Theorem implies - and this is what has given it its name - that every set X can be well-ordered, i.e. that there exists for X a binary relation (i.e. a set of ordered pairs) R which (i) is transitive, (ii) asymmetric and (iii) has the property that for every non-empty subset Y of X there is a y ε Y such that for all z ε Y, if z ≠ y then yRz. (N.B a relation R with these three properties is in particular linear, i.e. for each x, y in the field of R, we have xRy v x = y v yRx. Show this.) For evidently the correspondence between X and some ordinal entails the existence of such a well-ordering. (Exercise: Show this.)

Well-ordering Theorem.

Every set X is equipollent to some ordinal.

Proof. Let X be any set. If X is the empty set there is nothing to prove. So we assume that X is non-empty. We proceed as follows. We consider the set $\mathbb{R}$ of all well-orderings of subsets of X. (That this set exists is easily seen. For each well-ordering of a subset of X is a set of ordered pairs of members of X. Since the ordered pairs of members of X form a definable subset Z of *P*(*P*(X)), the set of all well-orderings of subsets of X is a subset of *P*(Z).) Moreover, this subset is definable (by the three properties (i), (ii), (iii) mentoned in the definition of well-ordering above). So $\mathbb{R}$ is a set.)

We first show that each such well-ordering R determines a unique order preserving map from R onto some ordinal α_R, i.e. a unique 1-1 function f_R onto α_R such that for all x, y in the field of R, xRy iff $f_R(x) \varepsilon f_R(y)$. We argue as follows. Let Y be the field of R. For each y ε Y understand by *the R-initial segment of* Y determined by y that subset Z of Y which consists of y and all $z \varepsilon Y$ such that $z R y$. It is enough to show that for each $y \varepsilon Y$ there exists a unique order-preserving map f_y from the R-initial segment determined by y onto some ordinal α_y and that moreover the f_y are nested, i.e. that if $z R y$, then $f_z \subseteq f_y$. (For either there is an R-last element u in Y, in which case Y is identical with the R-initial segment of Y determined by u; or else there is no last element, but then the union of all the functions f_y for $y \varepsilon Y$ will be, since the f_y are nested, an order-preserving map from Y onto the union of the α_y.) Suppose there is a y for which there is no f_y as described. Then, since R is a well-ordering, there is a R-first such y. Either this y has an immediate R-predecessor z in Y. But then there is a unique order-preserving map f_z from the segment determined by z onto some ordinal α_z. So if $f_y = f_z \cup \{<y, \alpha_z>\}$, then f_y is a unique order-preserving map from the segment determined by y onto $\alpha_z +1$. If y does not have an immediate R-predecessor, then we put $f_y = \bigcup_{zRy} f_z \cup \{<y, \bigcup_{zRy} \alpha_z>\}$. Again we conclude, now also using the nestedness of the f_z, that f_y is a unique order-preserving map from the segment determined by y to some ordinal. So in both cases we get a contradiction.

Let $\gamma = \bigcup_{R \varepsilon \mathbb{R}} \alpha_R$. We now make use of the Axiom of Choice, assuming that there exists a function g defined on the set of non-empty subsets of X such that for any such subset Z, $g(Z) \varepsilon Z$. We also use the Recursion Theorem. This allows us to assert that there exists a function f defined on $\gamma + 1$ which satisfies the following clauses:

(i) $f(0) = g(X)$

(ii) $f(\alpha+1) = g(X - Ran(f\upharpoonright(\alpha+1)),$ if $X - Ran(f\upharpoonright(\alpha+1) \neq \emptyset;$
X otherwise;

(iii) $f(\lambda) = g(X - Ran(\bigcup_{\beta<\lambda} f\upharpoonright\beta)),$ if $Y - Ran(\bigcup_{\beta<\lambda} f\upharpoonright\beta) \neq \emptyset;$
X otherwise.

Note that once $f(\alpha) = X$ then this will remain so for $\beta > \alpha$ - i.e. we also have $f(\beta) = X$. For "$f(\alpha) = X$" means that all of X has been exhausted by the time we reach α (i.e. $X \subseteq f\upharpoonright\alpha$). Moreover, for each α such that $f(\alpha) \neq X$ the relation R_α defined by:

$<u,v> \varepsilon R_\alpha$ iff there are δ, β such that $\delta < \beta$, $f(\delta) = u$ and $f(\beta) = v$

is a well-ordering and α is the ordinal $\alpha(R_\alpha)$ corresponding to this well-ordering in the sense of the first part of the proof. Therefore $\alpha \varepsilon \gamma$. So $f(\gamma) = X$ and consequently the first ordinal β such that $f(\beta) = X$ belongs to $\gamma + 1$. But this means that $X - \mathrm{Ran}(f\lceil\beta)$ is empty. So $f\lceil\beta$ is a 1-1 map from β onto X. q.e.d.

The Well-ordering Theorem makes it possible to compare all sets according to size, in the following sense. For each set X let $|X|$ denote the smallest ordinal α such that α is equipollent with X. Since any two ordinals α, β are comparable as to size - we have either $\alpha \varepsilon \beta$ or $\alpha = \beta$ or $\beta \varepsilon \alpha$ - the relation "$X < Y$" defined by

$$X < Y \text{ iff } |X| \ \varepsilon \ |Y|$$

is a strict linear order on the totality of all sets. $|X|$ is also called *the cardinality of* X, or *the cardinal of* X. And by a *cardinal*, or*cardinal number*, we understand any ordinal that is equal to its own cardinality, i.e. any ordinal α such that $\alpha = |\alpha|$. Note that every finite ordinal is also a cardinal, but that among the infinite ordinals cardinals are extremely rare. For instance, ω is a cardinal, but $\omega + 1$, $\omega + 2$,..., $\omega + \omega$, $\omega.3$, ... $\omega.\omega$, ... are all of the same cardinality as ω and thus are not cardinals. Nevertheless we do know that there are also larger cardinals than ω. For according to Cantor's Theorem no set is equipollent with its power set. So in particular the cardinal number of $P(\omega)$ - it is often referred to as "beth$_1$" - is different from, and thus is larger than, ω; and the cardinal of the power set of the power set of ω is bigger than and so forth. But how much bigger is beth$_1$ than ω? In particular, is it the next cardinal after or are there other cardinals in between? This question, which was already raised by Cantor, can be said to have been the single most important question in set theory since Cantor, Dedekind and others first laid its foundations in the second half of the nineteenth century. (Cantor himself is said to have worked on this question with such desperation that it led, or at any rate significantly contributed, to a condition of clinical depression) The hypothesis that beth$_1$ is the first cardinal after ω is known as the *Continuum Hypothesis*. (It is called this because, as can be shown without too much difficulty, is also the cardinality of the "mathematical continuum", i.e. of the set of all real numbers.) After many fruitless attempts to prove the Continuum Hypothesis (from the Axioms of ZF, or from other, intuitively plausible axioms), Gödel succeeded in 1940 to prove at least that the Hypothesis was consistent with ZF (in fact, with a somewhat stronger theory known after its architects as "Gödel-Bernays") It was not until 1961 that Paul Cohen showed that the Continuum Hypothesis is *independent from* ZF, i.e. that its negation is consistent with ZF. Since then various attempts have been made to think of intuitively valid principles which would settle the question, even if the search for such principles has produced many intreresting results about ZF and its possible models.

With the cardinal numbers comes a "cardinal arithmetic" which must be sharply distinguished form the ordinal artithmetic mentioned earlier. We give just two operations here, cardinal addition, **+**, and cardinal multiplication, $\odot$:

For any cardinals κ, μ

(1) $\kappa + \mu = |X \cup Y|$, where X and Y are any sets such that $|X\{ = \kappa$,
$|Y| = \mu$ and $X \cap Y = \varnothing$.

(2) $\kappa \odot \mu = |X \times. Y|$, where X and Y are any sets such that $|X\{ = \kappa$
and $|Y| = \mu$

Some results about cardinal arithmetic:

(3) For arbitrary cardinals κ and μ

(i) $\kappa + \mu = \mu + \kappa$
(ii) $\kappa \odot \mu = \mu \odot \kappa$

(4) For all infinite cardinals μ and arbitrary cardinals κ

(i) if $\kappa \leq \mu$ then $\kappa + \mu = \mu$
(ii) if X is a set of cardinality $\leq \mu$ and for each $x \varepsilon X$, x is of cardinality $\leq \mu$, then $\cup_{x \varepsilon X}$ x has cardinality $\leq \mu$.

(5) if $\kappa \leq \mu$, then $\kappa \odot \mu = \mu$

Of these only (3), (4) and (5) deserve careful attention. The other properties are left as exercises. We begin with the comparatively simple (3).

Our proof of (3) is based on the following three observations. The first is:

(6) Every cardinal is a limit ordinal.

(Exercise: Prove this.)

The second observation is closely related to the second:

(7) Every infinite ordinal α can be written in exactly one way as the ordinal sum $\lambda + n$ of a limit ordinal λ and a finite ordinal n.

(7) is proved by an easy induction on ordinals. For $\alpha = 0$ the assertion is trivial. Suppose that $\alpha = \beta +1$ and (6) holds for β. Then there are unique λ and n such that $\beta = \lambda + n$. Then clearly $\alpha = \lambda + (n+1)$. Moreover, if $\alpha = \beta +1$ for some other pair of a limit ordinal μ and a finite ordinal m, then (i), as α is a successor ordinal, $m = k + 1$ for some finite ordinal k. But then $\beta = \mu +k$. Since by assumption the decomposition of is unique, $\mu = \lambda$ and $k = n$. Finally assume that α is a limit ordinal. Then obviously
$\alpha = \alpha +0$. Moreover, if for any λ and n, $\alpha = \lambda + n$, then $n = 0$; for otherwise α would be a successor ordinal. So $\alpha = \lambda + 0 = \lambda$.

The third observation requires the following definition. For any limit ordinal λ let *the* ω*-sequence generated by* λ be the set $\{\lambda + n\}_{n \in \omega}$. We denote this set as $\Omega(\lambda)$. Note that if λ, μ are distinct limit ordinals, then $\Omega(\lambda) \cap \Omega(\mu) = 0$. Using this notion, we claim:

(8) For every limit ordinal λ,

(i) $\lambda = \omega \cup \bigcup_{\beta \in Z} \Omega(\beta)$,
where Z is the set of limit ordinals $< \lambda$.

(8) is fairly obvious: The members of a limit ordinal are either limit ordinals or successor ordinals. Clearly every limit ordinal is the only limit ordinal in its ω-sequence, all the other members of the sequence being successor ordinals. The limit of the sequence is again a limit ordinal. The successor ordinals, moreover, are, according to (7), all of the form $\mu + n$, where μ is a limit ordinal and n is some finite ordinal > 0. So it should be evident that the right hand side of (i) exhausts λ.

Now let X and Y be a pair of disjoint sets of cardinal λ and let f and g be bijections from X and Y to λ, respectively. These functions assign edach member x of X and each member y of Y unique ordinals α_x and α_y belonging to λ. By (7) these ordinals have unique representations α_x

$= \mu_x + n_x$ and $\alpha_y = \mu_y + n_y$. We must construct a bijection of $X \cup Y$ to λ. The trick is to map X onto the "even" members of λ and Y onto the "odd" members. That is, we let h be the function which maps each $x \in X$ to the ordinal $\mu_x + 2.n_x$ and each $y \in Y$ to the ordinal $\mu_y + (2.n_y + 1)$. It should be obvious (i) (using (7)) that h is a 1-1 and (ii) (using (8)) that h is onto λ.

(4) and (5) are proved together. In the proof we make use of the fairly obvious inequality:

(9) if X is a set of cardinality $\leq \kappa$ and for each $x \in X$, x is of cardinality $\leq \mu$, then $|\cup_{x \in X} x|$ has cardinality $\leq |\kappa \times. \mu|$.

(Exercise: Prove this)

We prove by induction on infinite cardinals μ that whenever κ is a cardinal $\leq \mu$, then $\kappa \ominus \mu = \mu$. We distinguish between three cases; (a) $\mu = \omega$; (b) $\mu = \kappa^{+}$, where κ^{+} is the first cardinal after κ; (c) μ is a limit cardinal, i.e. for each cardinal $\kappa < \mu$ we also have $\kappa^{+} < \mu$. Case (a) is left as an exercise. We consider case (b). Let X be the set of all limit ordinals between κ and κ^{+}. X is well-ordered by ε and so there is a (unique) ordinal β and 1-1 ε-preserving map f_X from β onto X. Using the Axiom of Choice (henceforth: AC) we assume that h is a function defined on all subsets Y of μ such that $|\mu - Y| = \kappa$ which assigns to each such Y a subset h(Y) of $\mu - Y$ of cardinality κ. Similarly, using AC together with the Induction Hypothesis, we assume that bi is a function which assigns to any pair <Y,Z> of subsets of μ both of which are of cardinality κ a bijection bi(Y,Z) from Y to Z. For any ordinals δ, γ such that $\delta < \gamma$ let $[\delta, \gamma)$ be the set of all ordinals α such that $\delta \leq \alpha < \gamma$. We define the function g by recursion on β as follows:

(i) $g(0) = \text{bi}(f_X(0) \times. f_X(0),\ f_X(0))$

(ii) $g(\alpha+1) = g(\alpha) \cup \text{bi}(((f_X(\alpha+1) \times. [f_X(\alpha), f_X(\alpha+1)) \cup$
$([f_X(\alpha), f_X(\alpha+1)) \times. f_X(\alpha+1))) ,\ h(\text{Ran}(g(\alpha)))$

(iii) $g(\lambda) = \cup_{\delta<\lambda}\, g(\delta)$

With regard to (ii) it is important to note that the two arguments of bi are indeed both of cardinality κ and that if $g(\alpha)$ is a bijection between $f_X(\alpha) \times f_X(\alpha)$ and some subset of μ, then $g(\alpha+1)$ is a bijection between

$f_X(\alpha+1) \times f_X(\alpha+1)$ and some subset of μ. With regard to (iii) we may note that $g(\lambda)$ is a bijection from $f_X(\lambda) \times f_X(\lambda)$ to some subset of μ of cardinality κ. The conclusion that the range of $g(\lambda)$ is of cardinality κ we use the Induction Hypothesis together with (9).
It is easily seen that, as $\cup_{\alpha<\beta} f_X(\alpha) = \mu$, g is a bijection from $\mu \times \mu$ to some subset of μ. It follows that $\mu \times \mu$ and μ are equipollent.

The proof for case (c) is similar to that for case (b). This time let X be the set of all infinite cardinals $< \mu$. Let f_X and β be defined as before. It is easily verified that $\beta \leq \mu$. Let h be a function which asigns to pair consisting of a subset Y of μ with $|Y| < \mu$ and an infinite cardinal $\alpha < \mu$ a subset of μ - Y of cardinality α, and let bi be a function which assigns to each pair of sets Y, Z of the same cardinality $\alpha < \mu$ a 1-1 map bi(Y, Z) from Y onto Z. (Again the existence of such a function is entailed by the Induction Hypothesis.) This time let g be the function with domain β defined by the clauses (i) and (iii) above together with the clause

$$\text{(ii')} \quad g(\alpha+1) = \quad g(\alpha) \cup \text{bi}(((f_X(\alpha+1) \times. [f_X(\alpha), f_X(\alpha+1)) \cup ([f_X(\alpha), f_X(\alpha+1)) \times. f_X(\alpha+1))) \ , \ h(\text{Ran}(g(\alpha)), f_X(\alpha+1))$$

It is easy to verify that in (ii') both arguments of bi are of cardinality $f_X(\alpha+1)$ and thus that if $g(\alpha)$ is a 1-1 function from $f_X(\alpha) \times f_X(\alpha)$ to some subset of μ (of cardinality $f_X(\alpha)$), then $g(\alpha+1)$ is a 1-1 function from $f_X(\alpha+1) \times f_X(\alpha+1)$ to some subset of μ (of cardinality $f_X(\alpha+1)$). With regard to (iii) note that since $\lambda < \beta \leq \mu$, $|\lambda| < \mu$. So, using (9) we can once again conclude that the range of $\cup_{\delta<\lambda} g(\delta)$ has a cardinality not greater than the maximum of $|\lambda|$ and $f_X(\lambda)$ and thus of cardinality $< \mu$.

The set-theoretical results we have mentoned here are only a small excerpt from the vast stock of theorems of this theory (some of them extremely difficult) that are known. Our selection has been governed primarily by the need to provide a certain impression of the two principal ways of "counting the infinite" which set theory has made precise and which are associated with the concepts of *ordinal* and *cardinal*, respectively. More specifically - and this is true in partiuclar for the last few results - we have aimed at providing the set-theoretical underpinnings for the following "converse" of the Downward Skolem-Löwenheim Theorem, which was preeented on p. . This converse, the

"Upward Skolem-Löwenheim Theorem", says that if a set of sentences Δ has a denumerably infinite model, then for every infinite cardinal κ, Δ has a model whose universe is of cardinality κ.

Theorem. (Upward Skolem-Löwenheim Theorem.)
Let Δ be a set of sentence of some language L, let M be a model for L such that $|U_M| = \omega$ and $M \models \Delta$. Let k be any infinite cardinal $> \omega$. Then there exists a model M' such that $M \models \Delta$ and $|U_M| = \kappa$.

Proof. The proof is similar to that of the Completeness Theorem. Let Δ, M and κ be as in the statement of the theorem. To show that Δ has a model M' of cardinality κ we extend L to the language L' by adding to it a set of cardinality κ of new individual constants. We shall show presently that the sentences of L' can be enumerated in a sequence the length of which is exactly κ. (To be precise, that there exists a 1-1 function from κ to the set of sentences of L'.) But before we do this, a remark is in order about "languages" with a non-denumerably infinite vocabulary. So far we have considered only languages whose voacabulary was at most denumerable. Even a denumerably infinite, as opposed to a finite, vocabulary may perhaps seem a little counterintuitive from the perspective of our experience with actual languages. For the vocabularies of those languages, as normally understood, do appear to be finite. However, it is clear how a denumerbly inifinite vocabulary can be "simulated" with the help of a finite number of signs. As an eaxmple we may consider the vocabulary consisting of all *numerals*, i.e. all canonical names of natural numbers. Our standard decimal notation provides such names as combinations of the ten signs "0", "1", ... , "9". Alternatively, we can use, as numeral for the number n, the complex sign consisting of a "0" followed by n "1"s.

But a non-denumerable vocabulary cannot be simulated in this way, for the set of all finite sequences over some finite "aphabet" of signs will always be denumerable. (Exercise: Show this.) So the concept of a language with a non-denumerable vocabulary is an abstraction, or extrapolation, from our intuitive concpet of a language in a way that languages with denumeranbly infinite vocabularies are not. So what should we understand by such a non-denumerable language?

To focus on this question, we should be clear of the kind of abstraction involved in the notion of a non-denumerable set - such as. for instance, the cardinal κ. The existence of such sets follows from our axioms of set theory; and set theory offers various constructs to form non-denumerable sets out of others (as well, of course, as out of denumerable sets). But obviously we are never in a position to actually display or enumerate such a set explicitly - that is precisely what the term "non-denumerable" conveys. In the light of these considerations it is reasonable to see non-denumerable languages also as set-theoretical constructs, or, more accurately, to see the sentences and other well-formed expressons of such languages as constructs from finite subsets of their non-denumerable vocabularies. But in what sense can a well-formed expression of a language L - i.e. a sequence of "words" of L, i.e. of items from L's vocabulary - be a set-theoretic object? The natural answer to this question would seem to be: To the extent that sequences are, or can be considered, set-theoretical objects.

So what is a sequence in the set-theoretical sense? Set Theory suggests two possible asnwers to this question. According to the first answer a sequence of two elements will be an ordered pair- thus <a,b> is the sequence consistingof the elements a and b. Similarly a sequence consisting of three elements, a, b and c, say, will be a triple, e.g. the pair consisting of <a,b> and c: <<a,b>,c>, etc. The second answ<er is that a sequence is a functon the domain of which is an ordinal, and whose values are the members of the sequence. Thus the sequence consisting of a and b is the function {<0,a>,<{0},b>}, or {<0,a>,<1,b>} - a function the domain of which is the ordinal 2 (i.e. the set {0,{0}}). Similarly the sequence consisting of a,b and c is the function {<0,a>,<1,b>, <2,c>}, etc. This second notion of sequence has the advantages that it can be defined once and for all by a single, simple, explicit definition and (ii) that it generalizes straightforwardly to the infinite: a sequence in this sense can be finite or infinite according as the ordinal that is its domain is finite or infinite.

Adopting this second notion of sequence, we come to the following characterization of non-denumerable languages. As before a language L is a function from symbols to signatures (see p. 1), where the possibility that the domain of L is non-denumerable is explicitly included. The terms and sentences of L are then finite sequences of members of the domain of L, where "sequence" is to be understood in the set-theoretical sense just indicated, which satisfy the clauses (i) and (ii) of the definition of *term* and the clauses (i)-(v) of the definition of *formula* on p.1.

Now that we have made precise what should be understood by the language L' and its terms and sentences, we return to the proof of our theorem. We first divide the set C of new constants into two sets C_1 and C_2 , each of cardinality k. Let $\Delta' = \Delta \cup \{\neg(c = c')$: c and c' are distinct constants in C_1}. It is easily seen that Δ' is consistent. For let A be a finite subset of Δ'. A will consist of some finite subset of Δ together with finitely many sentences of the form "$\neg(c = c')$". In the model M the former are true by assumption. Moreover, since U_M is infinite, it is possible to chose distinct denotations in U_M for each of the finitely many new constants that occur in sentences in Δ' of the second kind.

We now come to the point where we need some of the cardinal arithmetic we have presented here and all that was required to get that far. It is clear that the cardinality of the sentences of L' is at least κ, for even the sentences which have the form "$c = c_o$", where c_o is some particular new constant and c is any new constant, already has cardinality κ. But is the set of sentences of L' *exactly* of cardinality κ? To see that this is so, we first observe that the set of symbols of L' has cardinality κ. This follows directly from (3) on p.44. Our second observation is that for each n the set of n-place sequences of members of L' has cardinality κ. For n = 1 this is obvious. Suppose the claim is true for n = m. To see that it is then also true for n = m + 1, note that every m+1-place sequence of members of L' is decomposable, in a unique way, into (i) an m-place sequence of members of L' and (ii) a member of L'. Thus the set of all m+1-place sequences is equipollent with the cardinal product of the cardinal of the set of m-place sequences and the cardinality of L'. By induction hypothesis this is equal to $\kappa \cdot \kappa$, which according to (4) on p. 44 is equal to κ. Our last observation is that the set of all finite sequences of members of L' has cardinality κ. This follows from the fact that this set can be written as $\cup_{n \; \varepsilon \; \omega} X_n$, where for n = 1,2,... X_n is the set of all n-place sequences of members of L'. It follows from (5) on p. 44 that this set is again of cardinality κ. Since teh set of sentences of L' is a subset of this set, its cardinaltity is at most κ. We already know that its cardinality is at least κ. So it is exactly κ.

From here on the proof closely follows the completeness proof we gave earlier. Let $\{A_\beta\}_{\beta \; \varepsilon \; \kappa}$ be an enumeration of length κ of all the sentences of L'. We use this enumeration to construct a sequence $\{\Delta_\beta\}_{\beta \; \varepsilon \; \kappa}$ of extensions of Δ'. As in the completeness proof, the union Δ_κ of this sequence will determine a model M' of Δ' and this M' will be the model we are looking for. We define by means of the clauses:

(i) $\Delta_0 = \Delta'$

(a) $\Delta_\beta \cup \{A_\beta\}$, provided $\Delta_\beta \cup \{A_\beta\}$ is consistent and A_β is not of the form $(\exists v_j)B$

(ii) $\Delta_{\beta+1} =$ (b) $\Delta_\beta \cup \{A_\beta, B(c/v_j\}$, provided $\Delta_\beta \cup \{A_\beta\}$ is consistent, A_β is of the form $(\exists v_j)B$ and c is a constant from C_2 which occurs neither in Δ_β nor in A_β.

(c) Δ_β, provided Δ_β U $\{A_\beta\}$ is inconsistent.

(iii) $\Delta_\lambda = \cup_{\beta\, \varepsilon\, \lambda}\, \Delta_\beta$

Note (i) that for all $\beta \;\varepsilon\; \kappa$ there is a c not occurring in Δ_β or A_β. For only $|\beta|$ new constants can have been introduced into Δ_β and only finitely many such constants can occur in A_β. Since there are κ new constants in all and $|\beta| < \kappa$, it follows that there are still κ constants left. Note (ii) that by the Recursion Theorem the clauses (i)-(iii) define a function defined on κ. The range of this function is a set and so is its union. Call this union Δ_κ.

As in the completeness proof one shows that Δ_κ is consistent and complete in L'. Also, defining once more the relation $\sim$ between individual constants of L' by:

c $\sim$ c' iff$_{def}$ the sentence c = c' belongs to Δ_κ

we show as before that $\sim$ is an equivalence relation and that whenever c $\sim$ c' and $P(t_1,.., c,..,t_n) \;\varepsilon\; \Delta_\kappa$, then $P(t_1,.., c',..,t_n) \;\varepsilon\; \Delta_\kappa$.
Moreover, since for any pair c, c' of distinct new constants the sentence $\neg(c = c')$ belongs to , all new constants belong to distinct equivalence classes under $\sim$. So, if we define the model M' in the same way as in the completeness proof, then $|U_{M'}| = \kappa$. As before one shows that for every sentence A in Δ_κ, M $\models$ A.

The Interpretation of Number Theory in Set Theory.

It is common to think of the members of the set ω as the "natural numbers". ω has a number of properties that suggest such an identification. For instance, as we have seen, ω is linearly ordered by ε and this order has the same structure as the set on natural numbers: (i) it begins with the empty set (which it is therefore natural to identify with the number 0), (ii) has the property that each "number" n has an immediate successor $n \cup \{n\}$, as well as, if it is different from $\varnothing$, an immediate predecessor, and (iii) it runs on forever. However, a proper identification of ω with the natural numbers requires that we interpret all operations and relations of number theory as operations and relations on ω, and in such way that number-theoretic laws turn into theorems of set theory.

In this section we formulate such an interpretation of number theory within set theory. It will have the property that for any theorem of our axiom system of Peano arithmetic the interpretation of that theorem (a sentence in the language of set theory) will be a theorem of the set-theoretical axioms SA1 - SA7.

Before we do this, we will define in more general terms the notion of an interpretation of a theory T1, formulated in a first order language L1, within a second theory T2, formulated within a first order language L2. Any such interpretation will be based on interpretations of all the non-logical constants of L1 by formulae of L2. For instance, if R is a 2-place relation of L1, then an interpretation of R in L2 will take the form of an L2 formula $A_R(v_1, v_2)$ in which v_1 and v_2 are the only free variables. An example which we have encountered already in a somewhat different context is the interpretation of the relation $\leq$ of the theory of Boolean lattices in terms of the operation U of Boolean Algebras. We can interpret the theory of Boolean lattices within the theory of Boolean Algebras by interpreting $\leq$ by means of the formula $v_1 \cup v_2 = v_2$.

For function constants of L1 the matter is a little more complicated. Since function constants form terms, and not formulas, interpreting an L1 function by means of an L2 formula makes no direct sense; rather the interpreting formula should be thought of as interpreting certain atomic formulae in which the function constant occurs. For instance, an interpretation of the theory of Boolean Algebras within the theory of Boolean lattices must be based on, among other things, an interpretation of the2-place function constant U. This interpretation is to be understood as the interpretation of the atomic formula $v_1 \cup v_2 = v_3$. A natural choice (also encountered earlier) would be the formula

(1) $v_1 \leq v_3$ & $v_2 \leq v_3$ & $(\forall v_4)(v_1 \leq v_4$ & $v_2 \leq v_4 \rightarrow v_3 \leq v_4)$

In general, to interpret an n-place function constant we need an n+1-place formula $A_C(v_1, \ldots ,v_n,v_{n+1})$. Note well that in order that for $A_C(v_1, \ldots ,v_n,v_{n+1})$ to be suitable as the intepration of an n-place function constant, the last argument most be functional in the first n arguments, that is, we must have that for all relevant values of the ariables the following open formula is satisfied:

(2) $A_C(v_1, \ldots ,v_n,y)$ & $A_C(v_1, \ldots ,v_n,z) \rightarrow y = z$

In general, interpretation of T1 within T2 involves yet another L2 formula, viz one which demarcates the universe of T1 within the universe of T2. The case before us, the interpretation of number theory within set theory, is an example. It is only the members of ω that are to be the "natural numbers" in our interpretation, not the entire universe - consisting of all sets - that our set theory talks about. The interpretation of the "universe of T1" is a formula $A_U(v_1)$ with only v_1 free. In the interpretation of Peano Arithmetic within ZF this formula should of course say that v_1 belongs to ω. We will give this formula as "$v_1 \varepsilon \omega$"; but of course, if the target language of our interpretation is our original, "minimal" language of set theory whose only non-logical constant is ε, then this formula must be seen as abbreviation of a much more complicated formula from which the "ω" has been eliminated, using the defintions by means of which it was introduced.

Intuitively, $A_U(v_1)$ should define a non-empty universe, i.e. the sentence $(\exists v_1)A_U(v_1)$ ought to be true. As for the unique condition on interpretations for function constants, we will impose this condition when we wil need it.

These preliminaries should suffice to make sense of the following definition:

Def. 1 Let L1 and L2 be first order languages. A *translation base for interpreting* L1 *in* L2 is a pair consisting of (i) a formula $A_U(v_1)$ of L2 with only v_1 free and (ii) a function which maps each non-logical constant C of L1 onto a formula $A_C(v_1, \ldots ,v_k)$ of L2 in which $v_1, \ldots ,v_k$

are the only free variables and where (a) if C is an n-ary predicate constant, then k = n and (b) if C is an n-ary function constant, then k = n+1.

Each translation base for interpreting L1 in L2 induces a function which maps arbitrary formulas of L1 onto formulas of L2, so that in particular sentences form L1 turn into sentences of L2. In case L2 has only predicate, but no function constants, the translation is quite straightforward: Basically all one needs to do to translate any formula B of L1 is to replace each atomic subformula $P(x_1, \ldots ,x_k)$ by $A_P(v_1, \ldots ,v_k)$ (making sure to rename bound variables where necessary). But when L1 contains function constants the matter is more complicated. For how are we to translate an atomic formula $P(t_1, \ldots ,t_k)$ where all or some of the t_i are terms other than variables. To see what the problem is, consider once more the above interpretation of the union operation of the language of Boolean Algebras given in (1). Suppose we want to translate the formula

(3) $(x \cup y) \cup z = x \cup (y \cup z)$.

Here we have a predication involving the special predicate symbol = and two complex terms. Since (1) applies directly only to atomic formulas of the form $x \cup y = z$, there is no direct way in which it can be applied to (3). One way in which we can make it apply is to rewrite (3) into an equivalent formula in which all atomic subformulas are of the form to which (1) can be applied directly:

(4) (3) $\Rightarrow$

$(\exists u)(u = x \cup y \;\&\; u \cup z = x \cup (y \cup z)) \Rightarrow$

$(\exists u)(\exists v)(u = x \cup y \;\&\; v = y \cup z \;\&\; u \cup z = x \cup v) \Rightarrow$

$(\exists u)(\exists v)(\exists w)(u = x \cup y \;\&\; v = y \cup z \;\&\; w = x \cup v \;\&\; u \cup z = w)$

The last formula of (4) can now be translated by replacing its atomic formulas with suitable variants of (1).

An alternative way of dealing with this problem is to associate with each term t a formula $A_t(v_1)$ of L2 which represents t in the sense that, intuitively speaking, it is satisfied uniquely by the "value of the intrerpretation of t"; thus $A_t(v_1)$ serves as the translation of the formula $t = v_1$. As can be seen from Definition 2 below, the definition of $A_t(v_1)$ has teh reduction illustrated in (4) built into it.

Def. 2 Let T1 be a theory of the first order language L1 and T2 a theory of the first order language L2. Let $< A_U, I>$ be a translation base for interpreting L1 in L2.

1. $< A_U, I>$ is *suitable according to* T2 iff

   (i) $T2 \models (\exists v_1)A_U(v_1)$

   (ii) For each n-place function constant F of L1

(5) $$T2 \models (\forall v_1) .. (\forall v_n)(\forall y)(\forall z)(A_C(v_1, \ldots ,v_n,y) \;\&\; A_C(v_1, \ldots ,v_n,z) \rightarrow y = z)$$

2. Suppose that $< A_U, I>$ is suitable for T2. The *interpretations* of terms and formulas of L1 in L2 *based on* $< A_U, I>$ are defined as follows:

   1. Terms. For each term t the interpretation of t based on $< A_U, I>$ is the formula $A_t(v_1)$ defined as follows

   i. If t is the variable x, then $A_t(v_1)$ is $v_1 = x$

   ii. If t is the term $F((t_1, \ldots ,t_n)$, then $A_t(v_1)$ is the formula $(\exists x_1).. (\exists x_n)(A_{t_1}(x_1) \;\&\; .. \;\&\; A_{t_n}(x_n) \;\&\; A_F(x_1, \ldots ,x_n,v_1))$

   2. Formulas. For each formula B the interpretation of B based on $< A_U, I>$, $I^*(B)$, is defined by:

   i. $I^*(P(t_1, \ldots ,t_n)) =$
   $(\exists x_1)..(\exists x_n)(A_{t_1}(x_1) \;\&\; .. \;\&\; A_{t_n}(x_n) \;\&\; A_P(x_1, \ldots ,x_n))$

   ii. $I^*(\neg B) = I^*(\neg B)$; $I^*(B \;\&\; C) = I^*(B) \;\&\; I^*(C)$; $I^*(B \vee C) = I(B)$ ` $\vee\, I^*(C)$; $I^*(B \rightarrow C) = I^*(B) \rightarrow I^*(C)$; $I^*(B \leftrightarrow C) = I^*(B) \leftrightarrow I^*(C)$;

   (iii) $I^*((\forall v_i)B) = (\forall v_i)(A_U(v_i) \rightarrow I^*(B))$;
   $I^*((\exists v_i)B) = (\exists v_i)(A_U(v_i) \;\&\; I^*(B))$

3. The translation base $<A_U, I>$ is an *interpretation of* T1 *within* T2 iff (i) $<A_U, I>$ is suitable according to T2; and

   (ii) For any sentence B of L1, if $T1 \models B$, then $T2 \models I^*(B)$.

N.B. If T1 is given by a set of axioms, then to check that 3.ii. is satisfied it suffices that each of these axioms translates into a theorem of T2.

We now turn to the interpretation of Peano Arithmetic in ZF Set Theory. After the general foundations we have just discussed, this is now quite straightforward. All we need to do is define a translation base for interpreting the language L_{PA} into the language of set theory $\{\varepsilon\}$, and then check that it satisfies the conditions (i) and (ii) of Def. 3.2.

In defining the translation base, we will continue with the convenient device of specifying the interpretations of the non-logical constants of Peano Arithmetic in the definitionally extended language of set theory we have been using. As with the formula
$v_1 \varepsilon \omega$, an interpretation in the language $\{\varepsilon\}$ can be obtained from the fomula thus specified by elimination of the defined function constants and predicates.

The interpretation of the constants = and S is straightforward. But those of + and · require some thought. What needs to be done is to mimick the recursive defintions of + and · given by the Peano axioms PA3- PA6. We accomplish this by using the familiar trick of quantifying over finite functions which encode initial segments of the relevant recursion. Thus the interpretation of + has the following form.

(6) $(\exists f)(Fn(f) \;\&\; Dom(f) = v_2 \cup \{v_2\} \;\&\; f(\varnothing) = v_1 \;\&\; (\forall n)(n \;\varepsilon\; v_2 \rightarrow f(n\cup \{n\}) = f(n) \cup \{f(n)\}) \;\&\; f(v_2) = v_3)$

The function f defined in the quantifier-free part of (6) is intuitively the function which assigns to each of the numbers n from 0 to v_2 as values the numbers $v_1 + n$. This has the effect that in particular v_3 is the number $v_1 + v_2$. The interpretation of · is constructed along the same lines; the formula looks a little more complicated because the recursive clause for · makes use of +.

<u>Def. 3</u> Translation Base for interpreting Peano Arithmetic in ZF:

(i) $A_U(v_1)$:= $v_1 \;\varepsilon\; \omega$

(ii) $I(0)$:= $v_1 = \varnothing$

(iii) $I(S)$:= $v_2 = v_1 \cup \{v_1\}$

(iv) $I(+)$:= $(\exists f)(Fn(f) \;\&\; Dom(f) = v_2 \cup \{v_2\} \;\&\; f(\varnothing) = v_1 \;\&\; (\forall n)(n \;\varepsilon\; v_2 \rightarrow f(n\cup \{n\}) = f(n) \cup \{f(n)\}) \;\&\; f(v_2) = v_3)$

(iv) $I(\cdot)$:= $(\exists f)(Fn(f)\ \&\ Dom(f) = v_2 \cup \{v_2\}\ \&\ f(\varnothing) = \varnothing\ \&$
$(\forall n)(n\ \varepsilon\ v_2 \rightarrow I(+)(\ f(n),\ n,\ f(n \cup \{n\}))\ \&$
$f(v_2) = v_3)$

Theorem. The translation base of Def. 3 is an interpretation of Peano Arithmetic within ZF, in the sense of Def. 2.3.

##

Let us call an interpretation of T1 within T2 *absolute* iff the first member of its translation base (i.e. the formula $A_U(v_1)$) is true of all things in the "universe of T2", that is, if T2 $\models$ $(\forall v_1)A_U(v_1)$. The situation where there is an absolute interpretation of T1 in T2 can also be described as follows: For each non-logical constant C of T1 there is an explicit definition B_C of C in T2, such that, if T2 is the theory in the language L2 $\cup$ L1 which we obtain by adding all these definitions to T2, then T2' $\models$ T1.

An important relationship between theories T1 and T2 is when each is absolutely interpretable within the other. In such a situation T1 and T2 can be regarded as different formalizations of the same "conceptual structure" - whether one starts from the notions that are primitive in T1 (i.e. the non-logical constants of L1) or from those that are primitive in T2, the other notions can always be obtained from these by explicit definition so that the axioms of the other theory become theorems of the first. A very simple (and quite uninteresting) example is provided by the theory of partial order, which can be formulated either in the language {<} with the axioms PO1 and PO2 above - let this theory be TPO1 - or in the language {$\leq$}, with the axioms (PO1') $(\forall x)(\forall y)\forall z)(x \leq y\ \&\ y \leq z \rightarrow x \leq z)$ and (PO2') $(\forall x)(\forall y)(x \leq y\ \&\ y \leq x\rightarrow x= y)$ - let this theory be TPO2. Then TPO1 is absolutely interpretable wihin TPO2 and TPO2 is absolutely interpretable within TPO1.

Exercise. Prove this by formulating definitions of $\leq$ in TPO1 and < in TPO2 and then showing that each definition turns the axioms of one theory into theorems of the other.

A more interesting example is provided by the theory of groups. The formalization that we gave here, with $\cdot$ and $^{-1}$ as primitives, constitutes only one of many possibilities. Another version one often encounters in the literature starts with $\cdot$ and e as primitives and takes as axioms (for instance) (i) $(\forall x)(x \cdot e = x)$; (ii) $(\forall x)(e \cdot x = x)$. (iii) $(\forall x)(\forall y)(\forall z)((x \cdot y) \cdot z = x \cdot (y \cdot z))$; (iv) $(\forall x)(\exists y)(x \cdot y = e)$.

It is not hard to show that (i) - (iv) entail that the y of (iv) is unique. (Argument: Suppose that $x \cdot y = e$ and that $y \cdot u = e$. Then $x = x \cdot e = x \cdot (y \cdot u) = (x \cdot y) \cdot u = e \cdot u = u$. So $y \cdot x = y \cdot u = e$. Now suppose that y and z are both such that $x \cdot y = e$ and $x \cdot z = e$. Then $y = y \cdot e = y \cdot (x \cdot z) = (y \cdot x) \cdot z = e \cdot z = z$.) So we may define $(\forall x)(\forall y) (x^{-1} = y \leftrightarrow x \cdot y = e)$. it is eaasy to check that with this definiton all axioms of the version of group theory given in the text follow from (i) - (iv) above.

Exercise. It is also possible to formulate the theory of groups with just one 2-place operation / as primitive. Intuitively x/y means the same as $x \cdot y^{-1}$.

(i) Show that if we add to our original formulation of the theory of groups (8) as additional axiom, then the sentences (9) - (12) are derivable as theorems

(8) $(\forall x)(\forall y)(\forall z)(x / y = z \leftrightarrow z = x \cdot y^{-1})$

(9) $(\forall x)(\forall y)(x/x = y/y)$

(10) $(\forall x)(\forall y)(x = x/(y/y))$

(11) $(\forall x)(\forall y)((x/x)/(x/y) = y/x)$

(12) $(\forall x)(\forall y)(\forall z)((x/y)/z = x/(z/((y/y)/y)))$

(ii) Let TG' be the theory given by (9) - (12). Show that the formulas (13) - (15) are definitions in TG' (i.e. show that the relevant existence and uniqueness conditions for the definientia of (13) - (15) are theorems of TG')

(13) $(\forall z)(e = z \leftrightarrow (\forall y)(z = y/y))$

(14) $(\forall x)(\forall y)(x^{-1} = y \leftrightarrow y = e/x))$

(15) $(\forall x)(\forall y)(\forall z)(x \cdot y = z \leftrightarrow z = x/y^{-1}))$

(iii) Show that all axioms of our original formulations of the theory of groups are derivable from (9) - (15).