CHAPTER I

The meaning of the finite and the infinite

1.1. Introduction.

We describe formal language, and use it to express the axioms of modified Zermelo-Fraenkel set theory with the axiom of choice (mZFC). These rules have been given in [Ad15] volume I, chapter III, section 2, and [Ad15] Volume II, chapter XIV, sections 2 and 5.

We extend the Peano axioms for standard arithmetic. Transfinite number theory is considered for the transnatural numbers $\mathbb{M}_t$. It is an extension of finite arithmetic, and is used to define other numbers in a similar way. We repeat a proof given in [Ad15] on the inconsistency of an uncountable number of combinations of the natural numbers compared with the countable rationals. We extend the ladder algebra of ordinal arithmetic given in [Ad15] to $\mathbb{M}_t$.

Our definition of the capital Ξ function to give a model of the real numbers will be used in volume III, chapter VI, to give a second proof of the general Riemann hypothesis.

1.2. Formal language. [5Co66]

In 1908, Zermelo presented a formal set of axioms for set theory which covered all reasoning in mathematics. The axiomatisation of set theory was in keeping with the spirit of the school of Formalism, led by David Hilbert. In the Formalist point of view, mathematics was seen as a purely formal game played with marks on paper, where the game must not lead to an inconsistent result.

The symbols used in a formal language, which are not the minimal set of symbols in the interpretation system we will give, we will designate as follows

NOT	&	OR	⇒	⇔
not	and	or	implies	if and only if
∀	∃	=	(,)	x, ′
for every	there exists	equals	parentheses	variable symbols

In principle, the names used under these symbols which give their meaning are independent of the formal language.

We may have met the symbols in the first row in [Ad15] chapter XII. They are connectives used in a logic called the *propositional calculus*. The symbols used in the combined first and second rows are the symbols of the *predicate calculus*. On the second row the symbol ∀, for every (or for all), is known as the universal quantifier, and the symbol ∃, there exists (or for some), is the existential quantifier. Parentheses are used in the language to ensure its precise evaluation. When this evaluation is obvious, they may be omitted. The variable symbols will be formed as x, x′, x″, etc., and we will often rewrite them as x_1, x_2, x_3, etc. if that is useful.

From this set of symbols we can create others. Variable symbols with a special defined use in a system, such as the identity element for a group, are called constants, and will be denoted by c, c′, etc. The variable symbols with the parenthesis symbol can be used to describe *relation symbols*, R_1, R_2, R_3, etc. Each R_k is provided with a natural number n_k which gives the number of variables in the parentheses which follow. To give examples of how these symbols could be used, for $n_0 = 2$ we can define a binary predicate $R_0(x_1, x_2)$, and this could represent $x_1 \leq x_2$, for $n_1 = 3$ we can define a predicate $R_1(x_1, x_2, x_3)$ in three variables, and this could represent $x_1 + x_2 = x_3$.

By these means symbols in the formal language can be used to express relations in arithmetic. For example if we wanted to express the uniqueness of addition in our language, this is

$$\forall x\ \forall y\ \forall z\ \forall u\ ((R_1(x, y, z)\ \&\ R_1(x, y, u)) \Rightarrow z = u.$$

Similarly, if $R_2(x, y, z)$ represents multiplication as $x.y = z$, then we can express associativity of multiplication in the formal language by

$$\forall x\ \forall y\ \forall z\ \exists t\ \exists u\ \exists v\ ((R_2(x, y, t)\ \&\ R_2(t, z, u)\ \&\ R_2(y, z, v)\ \&\ R_2(x, v, u)).$$

Although the existence of the additive identity zero can be expressed as $\exists x\ \forall y\ (R_1(x, y, y))$, rather than restate this every time we use it, we will introduce the axiom $\forall x\ (x + 0 = x)$. We can now see a way of, say, describing the axioms of a field given in chapter III, section 4, by using formal language.

We now give the rules for writing grammatically correct statements in a formal language. These statements are called *well-formed formulas* (*wff 's*).

(1) Let x and y be variables, c and c′ constants. Then $x = y$, $x = c$ and $c = c'$ are wff 's.
(2) If R is a relation symbol and $u_1, \ldots , u_n$ constants or variables, then $R(u_1, \ldots , u_n)$ is a wff.
(3) If A and B are wff 's then so are NOT (A), (A) & (B), (A) OR (B), (A) ⇒ (B) and (A) ⇔ (B).
(4) If A is a wff, so are ∃x A and ∀x A.

The set of *subformulas* of a wff A is defined as the smallest set which contains A and is closed under the following rules

(i) If NOT (B) is a subformula of A, so is B.
(ii) If (B) & (C), (B) OR (C) or (B) ⇒ (C) are subformulas of A, so are B and C.
(iii) If either ∃x B or ∀x B are subformulas of A, so is B(c) for a constant c.

In subsequent developments we will need to distinguish between the ideas of *free* and *bound* variables. An example is as follows. Suppose we had $\forall x\ y = z$, which by rule (4) is a wff. Now $y = z$ does not involve x, so the quantifier ∀x has no effect. A similar circumstance might be where variable and constant symbols occur in a wff without referencing anything.

Definition 1.2.1. A variable symbol in a wff is *free* or *bound* according as

(a) Every variable occurring in a formula for rules (1) and (2) above is free.
(b) Free and bound occurrences derived from rule (3) above are the same as those for A and B.
(c) Free and bound occurrences of variables in ∃x A and ∀x A are the same as those for A except free occurrences of x are now called bound.

We allow binding to occur more than once. If this does not occur, the wff is called *good*.

Definition 1.2.2. A *statement* is a formula with no free variables.

Let us recall the rules for the propositional calculus given in chapter XIII of [Ad15]. We introduced two variables, τ, which we will now identify with true, and υ, which we identify with false.

Then the truth tables for statements A and B map A(τ, υ), B(τ, υ) to NOT A, A & B, A OR B, A ⇒ B and A ⇔ B as follows

NOT A	A & B	A OR B	A ⇒ B	A ⇔ B	A	B
υ	τ	τ	τ	τ	τ	τ
υ	υ	τ	υ	υ	τ	υ
τ	υ	τ	τ	υ	υ	τ
τ	υ	υ	τ	τ	υ	υ

The number of possible truth table functions is four for a function of one variable, 16 for a function of two variables, and in general 2↑(2↑m) for a function of m variables.

In fact, we can reduce the number of tables required to just NOT A and, say, A & B, since

A OR B = NOT(NOT A & NOT B)
A ⇒ B = NOT(A & NOT B)
A ⇔ B = (A ⇒ B) & (B ⇒ A).

For the predicate calculus we can also introduce a simplification, since ∀ can be replaced by NOT ∃ NOT.

The rules of predicate logic allow true and false statements. We are usually interested in deriving from a collection of true, or *valid*, statements a collection of valid consequences by using *rules of deduction* or entailment. Since these rules only operate on valid statements, they do not reduce to predicate logic.

(A) *Rule of the propositional calculus*. If P is a propositional function in the variables $A_1, ..., A_n$ that is always true, then on replacing any A_k by a valid statement results in a valid statement.

(B) *Rule of inference*. This allows us to form new valid statements from old ones. If A and (A) ⇒ (B) are valid statements, so is B.

(C) *Rules of equality*. These allow us to manipulate equal signs. Let c, c′ and c′′ be constants.

  (i) c = c′, (c = c′) ⇒ (c′ = c) and ((c = c′) ⇒ (c′ = c′′)) ⇒ (c = c′′) are valid statements.

  (ii) If A is a statement, and if A′ represents A with every occurrence of c replaced by c′, then (c = c′) ⇒ ((A) ⇒ (A′)) is a valid statement.

(D) *Change of variables*. If A is a statement and A′ is obtained from A by replacing each occurrence of the symbol x by x′, then (A) ⇔ (A′) is a valid statement. This also applies to good statements, as we have defined them.

(E) *Rule of specialisation*. Let A(x) be a formula with one free variable x in which every occurrence of x is free, and A(c) be result from replacing every occurrence of x by the constant symbol c. Then (∀x A(x) ⇒ A(c)) is a valid statement.

(F) Let B represent a statement where c and x are absent. If A(c) ⇒ B is valid, so is ∃x A(x) ⇒ B. This allows us to argue about a statement using an 'arbitrary' constant c, and infer that ∀x A(x), since we have used no special properties of c.

(G) *Rearrangement of quantifiers to the beginning of a statement*. Let A(x) have x as its only free variable, where every occurrence of x is free, and B be a statement with x absent.

  (i) (NOT (∀x A(x))) ⇔ (∃x NOT (A(x))).

  (ii) ((∀x A(x)) & (B)) ⇔ (∀x ((A(x) & B))).

  (iii) ((∃x A(x)) & (B)) ⇔ (∃x (A(x)) & (B)).

1.3. Modified Zermelo-Fraenkel set theory (mZFC).

Sets are often used to describe mathematical systems; they include but are not restricted to collections of various types of number, for instance sequences or functions of numbers. The notion of a natural number itself can be expressed within this system. Further, we can introduce sets with an infinite number of members, or elements. We will not discuss in this section all aspects of generalisations of sets, confining ourselves to binary logic and locating truth. Toposes can be defined in category theory, and include the sets we study.

A set of axioms for set theory was given for the first time by E. Zermelo in 1908, which was later developed by A. Fraenkel. This combined theory is often called Zermelo-Fraenkel (ZF) set theory and has been used to describe all of traditional mathematics. When the axiom of choice is appended, it is known as ZFC. We list the axioms of modified ZFC, or mZFC, and comment on them. The symbol m indicates we have modified an axiom.

(1) *Axiom of extensionality*.

$\forall x, y\ (\forall z\ (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$.

As for the system Z_2, this states that a set is determined by its members.

We can now define the *includes* symbols.

$x \subseteq y \Leftrightarrow \forall z\ (z \in x \Rightarrow z \in y)$ means x is included in y, and can equal it.

$x \subset y \Leftrightarrow x \subseteq y$ & NOT $x = y$ means x is properly included in y; it does not equal y.

(2) *Axiom of the empty set*.

$\exists x\ \forall y$ (NOT $y \in x$).

This empty set is denoted by ∅.

(m3) *Axiom of the void set*.

$\exists x\ \forall y$ (NOT $y \in x$) & $y \in x$).

This void set is denoted by ⨀, for which $\psi(x)$ defined later in ($m7_n$) is identically false.

(4) *Axiom of unordered pairs*.

$\forall x, y\ \exists z\ \forall w\ (w \in z \Leftrightarrow w = z$ OR $w = y)$.

The set z of unordered pairs is denoted by {x, y}. This means that {x} is {x, x}. For an ordered pair or *Cartesian product* <x, y>, we define this as the set {{x}, {x, y}}. It is possible to prove that <x, y> = <u, v> implies x = u and y = v.

A definition of a *function* can now be given.

A function is a set f of ordered pairs such that <x, y> and <x, z> in f ⇒ y = z. The set of x is called the *domain* of the function and the set y the *codomain*, *image* or *target*. Some authors define the range to be the codomain of a function and others the domain, so we do not use this. A *map* or *mapping* is the set corresponding to the function itself. This mapping is *one-to-one*, an *injection* or a *monomorphism* (the last of such triples are used particularly for groups) if every $x' \in x$ maps to a unique $y' \in y$. A map is *onto*, a *surjection* or an *epimorphism* if every $y' \in y$ is the codomain of the function f with domain x. The mapping is *one-to-one and onto*, a *bijection* or an *isomorphism* if it is both injective and surjective.

(5) Axiom of the *union* of sets.

$\forall x\ \exists y\ \forall z\ (z \in y \Leftrightarrow \exists u\ (z \in u\ \&\ u \in x))$.

We call the set y the union of all the sets in x. Using axiom (4) we can then show that given x and y, there exists a z satisfying $z = x \cup y$, that is, $u \in z \Leftrightarrow u \in x$ OR $u \in y$.

(6) Axiom of *infinity*.

$\exists x (\emptyset \in x \;\&\; \forall y (y \in x \Rightarrow y \cup \{y\} \in x)$.

We have already come across this in Z_2: if x is a natural number, the successor of x is defined as $x \cup \{x\}$.

($m7_n$) Axiom of *extended comprehension* (also called the modified axiom of *replacement*).

$\forall u_1, ..., u_k (\forall x \exists! y A_n(x, y, u_1, ..., u_k) \Rightarrow$

$\forall v \exists w \forall z (z \in w \Leftrightarrow \exists r ((r \in v \;\&\; A_n(r, z, u_1, ..., u_k))$ OR $r \in \odot))$.

This axiom scheme says that if for fixed $u_1, ..., u_k$ $A_n(x, y, u_1, ..., u_k)$ defines y uniquely as a function $\psi(x)$ of x, then for each v the codomain of v mapped to $\psi(v)$ creates a set, which may be void. Whenever we define a set by "S is a set such that ..." we are using this axiom. Here the property A_n which defines ψ may be very non-constructive or inconsistent, for instance to verify it we may need to answer a question about infinite sets.

(8) Axiom of the *power set*.

$\forall x \exists y \forall z (z \in y \Leftrightarrow z \subseteq x)$.

This states that for every x there exists a set y of all subsets of x. This y is defined by a property which is not covered by the axiom of restricted comprehension, because it is not defined as the codomain of any function.

(m9) Axiom of *consistent choice*.

If $n \Rightarrow A_n \neq \emptyset$ and $m \Rightarrow A_m \neq \emptyset$ are functions defined for all $n, m \in x$, then there exist other functions f(n), f(m), with $f(n) \in A_n$, $f(m) \in A_m$ & NOT $(n = m \Rightarrow f(n) \neq f(m))$.

This allows us to do an infinite amount of 'choosing' even without a property that would allow us to define the choice function which could otherwise be defined by axiom $m7_n$. The modification we have introduced is that this choice must not be void or multivalued. Thus we allow void states but not inconsistent rules of deduction.

(10) Axiom of *regularity* (or *well-founding*).

$\forall x \exists y (x = \emptyset$ OR $(y \in x \;\&\; \forall z (z \in x \Rightarrow$ NOT $z \in y)))$.

This axiom is somewhat artificial and we include it for technical reasons only. It is never used in conventional mathematics. It states that every set $x \neq \emptyset$ contains a minimal element with respect to the $\in$ relation (but not $\subseteq$), because we want our sets built up from $\emptyset$ where all descending chains with respect to $\in$ terminate with $\emptyset$. This axiom is similar to the well-ordering property, except that $\in$ is not an ordering because we could have $x \neq y$, NOT $x \in y$ and NOT $y \in x$.

Sets can be defined by modified Zermelo-Fraenkel set theory with the axiom of choice, mZFC, where the *axiom of extended comprehension* holds: For every set B and every well-formed formula $\psi(x)$, either there exists an $x \in X$ if and only if $\psi(x)$ holds and $x \in B$, or the set B is the void set, $\odot$, for which $\psi(x)$ is identically false.

So if P is a logical property and relation, called a predicate, there exists a set Y = {x: Px}, where we allow $X = \odot$, the void set, which satisfies a false predicate. For example, if a set is defined as the set of all barbers in town, B, and $b \in B$ is defined by b cuts hair for everyone in town, and b also satisfies the property that b does not cut b's hair, then this is a contradiction and $B = \odot$. We do not take this as an antimony in the axiomatics of sets.

$\odot$ can be expressed indirectly as the complement of $\mathbb{V}$. Nonvoid sets obey a predicate which is somewhere true. For instance, applied to the set $\{X: X \notin X\}$ (Russell's paradox),

$\odot = \{x: x \in \varnothing$ AND $x \notin \varnothing\}$

satisfies the paradox. A universal set (or universe) is then the set for a true predicate, say

$\mathbb{V} = \{x: x \in \mathbb{V} \text{ OR } x \notin \mathbb{V}\}$,

which is self-referential, in that $\mathbb{V}$ defines $\mathbb{V}$, or as a further example

$\mathbb{V} = \{x: x = x\}$.

The empty set satisfies $\varnothing \notin \varnothing$. In ZFC $\varnothing$ satisfies NOT $x \in \varnothing$, so the predicate y = NOT x allocates 'y ∈ ∅ is false' as a valid statement in ZFC, which has no rules of entailment from invalid to valid statements. In mZFC if a set is void, it is empty: $\odot \subseteq \varnothing$, since a void set satisfies more conditions than an empty one. But $\varnothing$ satisfies the condition that no $x \in \varnothing$, so $\odot \in \varnothing$ has a false $\psi(x)$, and $\odot = \varnothing$. Although we can form the set $\mathbb{V}'$ $\{x: \text{every } x \in \mathbb{V}'\}$, it is both the set complement of $\varnothing$ and $\odot$, so $\mathbb{V}' = \mathbb{V}$.

Thus mZFC allows the construction of the set of all sets without a contradiction arising from Russell's paradox, and we do not require a theory making the distinction between the set of all sets, which is normally called a *class*, outside ZFC true/false, and other types of set.

We now comment on what happens if some of these axioms are dropped. If the axiom of extensionality does not hold then the system may contain atoms, sets x with ∀y (NOT y ∈ x) but for which the sets x can be distinguished.

If the axiom of infinity does not hold, then we can take as a model of ZF the set of all finite sets which can be derived from ∅. Since the other axioms are also valid for finite sets, this axiom is independent of the other axioms of ZF, since axiom (6) becomes false for finite sets.

1.4. The Peano axioms for the transnatural numbers, $\mathbb{M}_t$.

The axioms for a set specify in the axiom of infinity that there exists a non-trivial set called the natural numbers. We will work with the set of natural numbers, $\mathbb{N}_{\neq 0} = \mathbb{N} = \{1, 2, 3, ... \}$, $\mathbb{N}_{\cup 0} = \mathbb{N} \cup \{0\}$ and the integers $\mathbb{Z}$ given by {..., -3, -2, -1, 0, 1, 2, 3, ...}.

Equality, =, satisfies the property of an *equivalence relation*, namely if m, n, p are members in a set then = is

reflexive: m = m (1)
symmetric: if m = n then n = m (2)
transitive: if m = n and n = p then m = p. (3)

If it is not the case that m = n, then we write $m \neq n$.

If elements of a set S satisfy an equivalence relation =, its application to elements belonging to S forms a *partition* of S:

if m ∈ S, then the intersection of all elements n ∈ S which equal m, with the set of all n′ ∈ S which do not equal m is the empty set:

for every $m \in S$, $\{n; n = m \in S\} \cap \{n'; n' \neq m \in S\} = \varnothing$,

where also

for every $m \in S$, $\{n; n = m \in S\} \cup \{n'; n' \neq m \in S\} = S$.

The natural numbers satisfy the Peano axioms describing an inductive procedure to generate them.

$1 \in \mathbb{N}$ (4)
for every $n \in \mathbb{N}$, there exists an s(n) interpreted as $(n + 1) \in \mathbb{N}$ (5)
there is no number $0 \in \mathbb{N}$ with s(0) = 1 (6)

for two numbers m, n ∈ $\mathbb{N}$, s(n) = s(m) implies n = m. (7)
(induction) a subset of $\mathbb{N}$ containing 1 and s(n) whenever n ∈ $\mathbb{N}$, is $\mathbb{N}$. (8)

We can express in an axiom system for sets for any property P that is not self-referentially true, that for the set {x: P; x ∈ X}, there exists a set {y: NOT P; y ∈ Y}. So we can introduce uncountable sets and establish uncountable induction.

Definition 1.4.1.The *transfinite natural numbers* $\mathbb{M}_t$, where t belongs to an index set which also satisfies the properties below, satisfy the axioms

$1 \in \mathbb{M}_t$ (9)
for every $m \in \mathbb{M}_t$ there exists an s(m) interpreted as $(m + 1) \in \mathbb{M}_t$ (10)
there is no number $0 \in \mathbb{M}_t$ with s(0) = 1 (11)
for two numbers m, n ∈ $\mathbb{M}_t$, s(m) = s(n) implies m = n (12)
$\mathbb{M}_t \subset \mathbb{M}_{s(t)}$ (13)
$\mathbb{M}_t$ is not bijective to $\mathbb{M}_{s(t)}$ (14)
there is no proper subset $\mathbb{M}'$ with the above properties satisfying $\mathbb{M}_t \subset \mathbb{M}' \subset \mathbb{M}_{s(t)}$ (15)
(induction) a subset of $\mathbb{M}_t$ containing 1 and s(m) whenever $m \in \mathbb{M}_t$ is $\mathbb{M}_t$. (16)

Notation 1.4.2. $\mathbb{M}_t$ with the number 0 appended to it is denoted by $\mathbb{M}_{t\cup 0}$.

Define < by the property, if m, n ∈ $\mathbb{M}_t$, then m < n if and only if there exists a $p \in \mathbb{M}_t$ so that m + p = n.

Definition 1.4.3. The *transrational numbers* $\mathbb{Q}_{Mt}$, t ≠ 1, are the set of numbers ±m/n where $m \in \mathbb{M}_{t\cup 0}$ and $n \in \mathbb{M}_t$.

Definition 1.4.4. A *transprime* number is a transnatural number which is only divisible without remainder by 1 and itself.

Definition 1.4.5. A *transinteger* is a transnatural number multiplied by 1, 0 or -1.

Definition 1.4.6. A *transcomposite* number is the product of either a transnatural number of transintegers or more restrictedly a product of a transnatural number of transnatural numbers.

Definition 1.4.7. The *transalgebraic* numbers $\mathbb{A}_t$ are combinations of the non-imaginary parts of transnatural numbers satisfying the field and the exponential or the suoperator axioms of chapter III, section 2.

1.5. A model for the real numbers.

The definition of a symbol as a universal object is given in chapter III, section 8, on category theory, definition 3.16.1. We now relax the previous rules, dropping axiom (15).

Definition 1.5.1.The *real transnatural* numbers represented by a symbol $\mathbb{S}_t$, where t belongs to a non-imaginary index set, satisfy the axioms for $\mathbb{M}_t$ except possibly axiom (15).

Definition 1.5.2. The *real transrational numbers* $\mathbb{Q}_{St}$, t ≠ 1, are the set of numbers ±m/n where $m \in \mathbb{S}_{t\cup 0}$ and $n \in \mathbb{S}_t$.

Definition 1.5.3. A *real transprime* number is a real transnatural number only divisible without remainder by 1 and itself.

Definition 1.5.4. The *real transalgebraic* numbers $\mathbb{A}_{St}$ are combinations of the non-imaginary parts of real transnatural numbers satisfying the field and the exponential or suoperator rules of chapter III, sections 6 and 7.

Now the jump in transcendence is not limited as t increases. Numbers in $\mathbb{A}_{St}$ are then discrete in $\mathbb{A}_{S(t+1)}$ and continuous in $\mathbb{A}_{S(t-1)}$. The question arises whether there is a model where $\mathbb{S}_t$ exists, but there are numbers with no imaginary components which do not belong to $\mathbb{A}_{St}$ for any t. In the general case the union of this set with $\mathbb{A}_{St}$ we call the *real numbers*, and we will find in the next section that we can form explicit calculations with models of them, which are representable when no such t exists.

1.6. The capital Ξ function.

The capital Ξ function will be used in Volume III, chapter VI to give a second proof of the general Riemann hypothesis. From the exponential operation we can form

$$a^1 = a,$$

but in a conventional real exponential algebra, for a ≠ 1 there is no

$$1^b = a.$$

What we do is introduce a function Ξ(a) so that

$$1^{\Xi(a)} = a.$$

Culturally this number has been introduced in an analogous way to our introduction of division by multizeros for the zero algebras in section 12 and *Superexponential algebra*, volume I, chapter III. The idea can be extended to suoperators.

An interesting feature of Ξ(a) is that it gives an ordering with a value which is greater than all transnatural ordinals, and thus gives a model for transcendence, and therefore in a proper sense, for real numbers.

Another observation is that Ξ(a) is directly computable with the algebra we already have to hand, since

$$1 = e^{i2n\pi},$$

and if we choose the classical complex algebra, this means

$$1^i = (e^{i2n\pi})^i = e^{-2n\pi}$$

and with

$$e^{\log_e a} = a,$$

this gives

$$a = 1^{\Xi(a)} = (e^{2\pi n})^i e^{2\pi n\left(\frac{\log_e a}{2\pi n}\right)},$$

$$\Xi(a) = 1 - \frac{i}{2\pi n}\log_e a. \ \square$$

1.7. The Euclidean algorithm.

Strictly speaking, before proving the division with remainder theorem, we need to prove that *any transnatural number* n *greater than* 1 *is either transprime or a product of transprimes*.

Proof. By the *method of induction*, if we wish to prove a statement for a positive transnatural number n, we can assume it has been proved for any number less than n. If n = 2, the theorem is proved. If n is transcomposite, it can be represented as ab, where both a and b are greater than 1 and less than n, but then we know by the induction method that a and b are either transprimes or the product of transprimes. ☐

The *fundamental theorem of arithmetic* states that *this factorisation is unique up to ordering*.

Proof. If n is transprime, the theorem is proved. Suppose n is transcomposite and there are two factorisations

$$n = pqr \ldots = p'q'r' \ldots$$

Let the transprimes be ordered in increasing size. By an induction hypothesis, no transprime p, q or r, ... can be the same as any of p', q', r', ... otherwise we could divide n by it and get two representations of a smaller number, where we would continue the proof with this smaller number. Since n is transcomposite it consists of at least two transprimes, so $n \geq p^2$ and $n \geq p'^2$ which implies $n > pp'$ with strict inequality, since p and p' are unequal. Now form $n - pp'$. This has pp' as a factor, so dividing pqr ... by p, p' must be a factor of qr ..., a contradiction. ☐

Suppose we represent the integer parts of the transrational numbers by notches along a line, for instance

|____|____|____|____|____|____|____|____|____|____|____|__

-1 0 1 2 3 4 5 6 7 8 9

then any transrational number may be represented uniquely by a transinteger plus a transrational number q equal to or greater than 0 and less than 1. This is the theorem given by Euclid, in book 7 of the Elements.

The algorithm may be restated as:
Every positive transnatural number n *can be written uniquely in terms of a positive transnatural number* w *less than* n *multiplied by another transnatural number* $k > 0$ *with a unique remainder* $0 \leq u < w$:

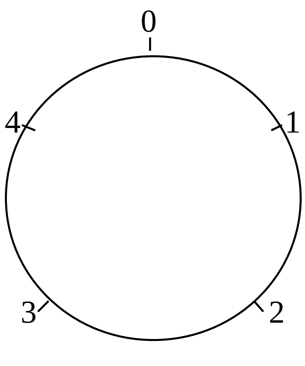
$$n = kw + u. \tag{1}$$

Proof. If w divides n, then u = 0 and we are done. Otherwise assume (1). If n comes between kw and $(k + 1)w$, then (1) holds with $0 < u < w$. ☐

Using the theorem, we develop an arithmetic for fixed w in which we only consider u above. This transfinite arithmetic is known as congruence, or clock arithmetic. The equation above is written in the notation

$$u = n \ (\text{mod } w),$$

where mod stands for the modulus, introduced by Gauss in his *Disquisitiones Arithmeticae*, which can be depicted in the example diagram for w = 5:



n (mod 5)

1.8. Fermat's little theorem.

Theorem 1.8.1. Fermat's little theorem extended to the transnatural numbers states that *for a transprime* p, verifiable directly for p = 2

$$x^p - x = bp. \qquad (1)$$

for some unique b *dependent on* x.

Proof. We prove this by induction. For x = 0

$$0^p - 0 = 0p.$$

Assume (1) holds. Then for $x \to x + 1$, by the binomial theorem and the transnatural primality of p, so p does not divide any denominator

$$(x + 1)^p - (x + 1) = x^p - x + px^{p-1} + [p(p - 1)/2]x^{p-2} + ... + 1^p - 1 = bp + cp$$

for some unique c. ☐ (2)

1.9. Euler's totient theorem.

Let u be any positive transinteger, and let the totient φ(u) denote the number of positive transintegers, 1 included, which are coprime to u and not greater than u. Since primality makes sense for transnatural numbers, it also makes sense for relative primality.

By definition φ(1) = 1. Also if p is a transprime number

$$\varphi(p) = p - 1.$$

Next suppose u transcomposite, and let p, q, r, s, ... be the different transprimes dividing u.

Consider the series of transintegers, 1, 2, 3, ... u. Of these the following are multiples of p:

p, 2p, 3p, ... (t/p).p,

(u/p in all).

Write these down with the sign +. Similarly, write down all the multiples of q, r, s, ... each with the sign +.

In the same series there are u/(pq) multiples of pq. Write these down with the sign –, and do the same with all the multiples of pr, ps, qr, ... (taking all the products of p, q, r, s, ... two at a time). Next write down all the multiples of the triple products pqr, pqs, ... each with the sign +, and so on, until at last we come to the multiples of pqrs... with sign $(-1)^{k-1}$, k being the number of different primes.

Now take any number θ which is not greater than t and not coprime to it. It will involve in its composition a certain number (λ say) of the different transprimes p, q, r, ... How many times will it occur among the multiples already written down?

By the binomial theorem, the number of combinations of λ things taken v at a time is

$$\lambda!/[u!(\lambda - v)!].$$

Taking its appearances in the order of the sets of multiples, θ will occur for λ times, the binomial coefficient, for v = 1 with the sign +, then for λ(λ – 1)/2 times for v = 2 with the sign –, then λ(λ – 1)(λ – 3)/3! times for v = 3 with the sign +, and so on.

If then we take the algebraic sum of all the sets, we have θ occurring with a coefficient

$$\lambda - \lambda(\lambda - 1)/2! + \lambda(\lambda - 1)(\lambda - 3)/3! - ... = 1 - (1 - 1)^{\lambda} = 1.$$

Thus the algebraic sum in question is the sum of all positive transintegers not greater than u and not coprime to it. Now the *number* of these integers is equal to the excess of the number of positive terms in the whole sum, as originally written, above the number of negative terms:

$$u\{(1/p + 1/q + 1/r + ...) - (1/(pq) + 1/(pr) + 1/(qr) + ...) + (1/(pqr) + 1/(pqs) + ...) - ... + (-1)^{k-1}.1/(pqrs\ ...)\}.$$

Subtracting this from u, we have finally

$$\varphi(u) = u(1 - 1/p)(1 - 1/q)(1 - 1/r) \ ... \ \square \qquad (1)$$

Corollary 1.9.1. *If* u *is odd,* φ(u) *is even.* □

We now prove Euler's totient theorem.

Theorem 1.9.2. *Let* t *be transprime or transcomposite*, *then*

$$\varphi(t)[x^{\varphi(t) + 1} - x] \equiv 0 \ (\text{mod } t). \qquad (2)$$

Proof. Consider first the case when x is coprime to t′. If α, β, γ, ... λ are the φ(t′) numbers which are transprime to t′ and less than it, the products xα, xβ, xγ, ... xλ are all coprime to t′; moreover we have seen no two of them are congruent (mod t′). Hence the products xα, xβ, xγ, ... xλ are congruent to α, β, γ, ... λ in a different order, and therefore

$$x\alpha.x\beta.x\gamma \ ... \ x\lambda = \alpha.\beta.\gamma \ ... \ \lambda.$$

Dividing by α.β.γ ... λ, which is coprime to t′, we obtain

$$x^{\varphi(t')} - 1 \equiv 0 \ (\text{mod } t'),$$

when x is coprime to t′. In the case when x is not coprime to t″, derived from equation (1), with t = t′t″ and only t′ coprime to x, φ(t″)x ≡ 0 (mod t″). Then on using φ(t) = φ(t′)φ(t″) and (mod t) = (mod t′)(mod t″), theorem 1.9.2 is obtained from

$$(x^{\varphi(t)} - 1) = (x^{\varphi(t')} - 1)(x^{\varphi(t) - \varphi(t')} + x^{\varphi(t) - 2\varphi(t')} + ... + 1). \ \square$$

Further developments are given in *Innovation in mathematics* [Ad14], in the chapter 'Some simple proofs on general reciprocity'.

1.10. Transp-adic numbers.

The p-adic number system for any transprime number p extends the ordinary arithmetic of the rational numbers in a different way from the extension of the rational number system to the real and complex number systems. The extension uses an alternative interpretation of the concept of *closeness* or *absolute value*. In particular, trans p-adic numbers have the property that they are considered closer the more their differences are divisible by higher powers of p. These numbers exist also for transprimes. A trans p-adic number b is represented for $j \geq k \in \mathbb{Z}_t$ and $0 \leq a_i < p \in \mathbb{M}_t$ by

$$b = \sum_{i=j}^{k} \frac{a_i}{p^i}. \qquad (1)$$

Congruence arithmetic can then be encoded if

$$(j - k) = 0 \ (\text{mod } q) \qquad (2)$$

usually for some transprime q, but now an ordering is not naturally defined.

1.11. The inconsistency of the uncountability hypothesis for $\mathbb{N}^{\mathbb{N}}$.

We repeat a small part of [Ad14] on countable and uncountable sets and ordinal infinities, and extend it, but first we find the conditions under which the principle of induction is valid for sets.

Doly García remarks that if a property holds for a set indexed by 1, n and n + 1, one cannot argue that it holds for the entire set, an instance being given by the set $A_1 = \{1\}$, with the property that $2 \notin A_1$, and in general for $A_n = \{1, 2, ... n\}$, where $n + 1 \notin A_n$, so that each complement exists for finite n, but not the entire set $\mathbb{N}$. This is part of the reason for us introducing ladder numbers, but we need to view this where nonstandard analysis is not used.

To respond to this criticism, if we look at the definition of the empty set, we see that mZFC deals with predicates in a nonstandard way – the same sentence may range over true and false in the definition of a set, and false defines the void set in mZFC, and not otherwise. Then if we look at the complement of A_1, this is $\mathbb{N}\backslash\{1\}$, and the complement of A_n is $\mathbb{N}\backslash\{1, 2, ... , n\}$, so applying the principle of induction, over the set $A_{\mathbb{N}}$ we are dealing with $\mathbb{N}\backslash\mathbb{N}$, which is the empty or void set, and thus the same property ranges over true and false in agreement with its principle of induction for sets. However, as we will put in more technical detail after theorem 1.11.2

Proposition 1.11.1. *If the property for a set does not range over the void set, it does not become false*.

In mZFC, if a predicate holds for all finite $n \in \mathbb{N}$, either the predicate does not hold for all n, which could be the case for standard set theory, where the set of all n not including all finite n is empty, which satisfies a false predicate, or the predicate holds for all n, which is the case for nonstandard set theory, since now the set of all n not including all finite n has elements.

When mapping properties, for instance a bijection $\{\mathbb{V}, \emptyset\} \leftrightarrow \{\mathbb{V}, \emptyset\}$ restricted to $\mathbb{V} \to \mathbb{N}$, for standard set theory possible mappings are $\mathbb{V} \leftrightarrow \mathbb{V}$, $\mathbb{V} \leftrightarrow \emptyset$, $\emptyset \leftrightarrow \mathbb{V}$ and $\emptyset \leftrightarrow \emptyset$. Since $\mathbb{V}$ maps to true and $\emptyset$ to false, we define that $\leftrightarrow$ satisfies the truth table for IF and only IF, written as $\Leftrightarrow$, with $A \leftrightarrow B \leftrightarrow C$ satisfying $(A \Leftrightarrow B)$ & $(B \Leftrightarrow C)$.

$A \Leftrightarrow B$	A	B
T	T	T
F	T	F
F	F	T
T	F	F

This allows that the principle of induction applies to bijective properties in standard set theory. □

If there exists at least one bijection between the elements of two sets S and T, then this is an equivalence relation and we say S and T have the same *cardinality*.

If $\mathbb{N}$ is countable, so is its power set $2^{\mathbb{N}}$, in general there is a bijection between $\mathbb{M}_t$ and $2^{\mathbb{M}t}$, $\mathbb{S}_t$ and $2^{\mathbb{S}t}$, and $\mathbb{R}_t$ to $2^{\mathbb{R}t}$, as an extension of the theorem proved here.

Theorem 1.11.2. *There exists a bijection between the set of rationals,* $\mathbb{Q}$, *and what we define as* $\mathbb{N}^{\mathbb{N}}$.

Proof. Nowhere does the induction we will carry out range over the predicate for a void set, since its function of functions $\mathbb{N} \to \mathbb{N} \to ...$ mapped in sequence to $\mathbb{N} \to \mathbb{N} \times \mathbb{N} \to ...$ has a fixed and not exhausted function as its domain. This assertion is proved in chapter XIV section 6 of [Ad15], where cardinals defined by bijections are shown to be lowest ordinals, ordinals are countable if there is a bijection to ℕ, and it is proved that because a union of countably many countable sets is countable, that suoperators on countable ordinals are countable.

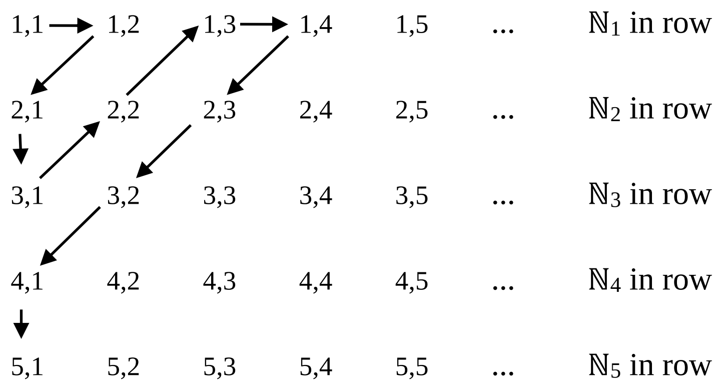
For finite or countably infinite sets S, T or U we define ≡ by the existence of at least one bijection within the natural numbers ℕ. This is an equivalence relation, in that $S \equiv S$, if $S \equiv T$ then $T \equiv S$, and if $S \equiv T$ and $T \equiv U$, then $S \equiv U$, so this forms a partition between those sets belonging to the equivalence class, and those outside it. Then for sets S_n, T_n, $n \in \mathbb{N}$, if for each n $S_n \equiv T_n$, then for the set of all S_n, $\{S_{nn}\} \equiv \{T_{nn}\}$, where this means if $S_n \equiv T_n$, then the bijection is maintained for $S_{n+1} \equiv T_{n+1}$, and the second subscript indicates a distinguished copy for $S_n \neq \varnothing$, defined inductively: $S_{n1} = \{S_n\}$, $S_{n2} = \{\{S_n\}\}$, $S_{n\,p+1} = \{S_{np}\}$.☐

We will adopt the argument of Cantor that *the set* ℚ *of rationals is countable*.

Define the Cartesian product of all natural number pairs $\mathbb{N} \times \mathbb{N}$ as $\mathbb{N}^2$. Consider the rational numbers not in lowest terms given by the set $\mathbb{Q} \equiv \{\{1/n\}, \{2/n\}, \{3/n\}, . . .\}$ ≡ the unordered distinguished copies$\{\mathbb{N}_1, \mathbb{N}_2, \mathbb{N}_3, . . .\} \equiv \mathbb{N} \times \mathbb{N}$ (a set of ordered pairs) which by the Cantor argument given next is ≡ ℕ.

The mapping from ℕ to ℚ is given in the following diagram.

$(m, n) \to m/n \in \mathbb{Q}_{\neq 0}$.



What is meant by the symbols . . . in the sets just given? This indicates that if the pth position is occupied, then a similar item exists at position p + 1, although we can remove . . . from the language and use the properties of ℕ itself given in section 1.2. Then by induction defined through the properties of ℕ, we have $\mathbb{N} \equiv \mathbb{N}^p$ for p a natural number, so that the set

$$\{\mathbb{N}_1, \mathbb{N}_2{}^2, . . , \mathbb{N}_p{}^p, . . .\}$$
$$\equiv \{\mathbb{N}_1, \mathbb{N}_2 \times \mathbb{N}_2, . . , \mathbb{N}_p \times \mathbb{N}_p \times . . \text{(p terms)}, . . .\} \equiv \mathbb{N}, \quad (1)$$

contains by definition $\mathbb{N}^{\mathbb{N}} \equiv \{\mathbb{N} \times \mathbb{N} \times . . .\}$. This is in violation of the assumptions of the uncountable continuum hypothesis (UCH) in set theory, that $\{0, 1\}^{\mathbb{N}}$ is uncountable. ☐

Repeated proof. By the definition of a union of sets and induction

$$\bigcup_{\mathbb{N}} n \equiv \mathbb{N},$$

the union of all $n \in \mathbb{N}$ is ℕ.

When we go over to countably infinite sets, a property exists which does not hold for finite sets, that for distinct copies $\mathbb{N}_n$

$$\bigcup \mathbb{N}_n \equiv \mathbb{N}.$$

This is extended and is inherent in the Cantor argument for the countability of $\mathbb{Q}$, that there exists a constructible bijective mapping

$$\mathbb{N} \equiv \bigcup_{\mathbb{N}} \mathbb{N}_n \equiv (\bigcup_{\mathbb{N}} n) \times \mathbb{N} \equiv \mathbb{N} \times \mathbb{N}. \quad (2)$$

If the size of the nth diagonal, up or down, in the previous diagram is n, and the sum of the diagonals is given by the arithmetic series

$$1 + 2 + 3 + ... + n = n(n + 1)/2,$$

then for each $m \in \mathbb{N}$ there is an $n(n + 1)/2$ and $t \in \mathbb{N}$ with the last diagonal of size n, $0 \leq t < n < n(n + 1)/2$, and by the Euclidean algorithm of section 1.3, a bijection

$$m \leftrightarrow n(n + 1)/2 + t.$$

This is a bijection

$$\mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N},$$

or as we have written

$$\mathbb{N} \times \mathbb{N} \equiv \mathbb{N}.$$

Let $\mathbb{N}^1$ be $\mathbb{N}$, and $\mathbb{N}^{p-1} \times \mathbb{N}$ be $\mathbb{N}^p$. By the definition of the natural numbers in section 2 the principle of induction states that because $\mathbb{N}^1$ is a subset of $\mathbb{N}$ containing 1 and $(n + 1)$ whenever $n \in \mathbb{N}$, and if $\mathbb{N}^{p-1} \leftrightarrow \mathbb{N}$ holds for 1 and $(p - 1) + 1$, then $\mathbb{N}^p \leftrightarrow \mathbb{N}$, so we have shown by the definition of $\mathbb{N}^p$,

$$\mathbb{N} \equiv \mathbb{N} \times \mathbb{N} \equiv \mathbb{N}^{p-1} \times \mathbb{N} \equiv \mathbb{N}^p.$$

There is a bijection

$$\mathbb{N}_n \leftrightarrow \mathbb{N}$$

obtained by stripping out all containing parentheses. Thus

$$\mathbb{N}_n \equiv \mathbb{N}, \quad (3)$$

and we have proved the equivalence (2), where we can add the comment for any n,

$$n \times \mathbb{N} \equiv \mathbb{N}.$$

From the equivalence (3) we get

$$\mathbb{N}_p{}^p \equiv \mathbb{N}. \quad (4)$$

Thus we have shown directly that equation (1) holds, where

$\mathbb{N}^p \rightarrow \mathbb{N}$ is injective implies $\mathbb{N}^{p+1} \rightarrow \mathbb{N}$ is injective,

so, because there is no void set in the mappings, by induction we obtain its consequence

$\mathbb{N}^{\mathbb{N}} \rightarrow \mathbb{N}$ is injective,

and since for the constant $\{1\}^{\mathbb{N}}$

$\mathbb{N} \leftrightarrow \{1\}^{\mathbb{N}} \times \mathbb{N} \rightarrow \mathbb{N}^{\mathbb{N}}$ is injective

we derive the result

$$\mathbb{N}^{\mathbb{N}} \equiv \mathbb{N}. \ \square \quad (5)$$

Another way of stating this is that an uncountable continuum cannot be represented by $\mathbb{N}^{\mathbb{N}}$ which is dependent on the countability of $\mathbb{Q}$ and our induction rule, and the countability of $\mathbb{Q}$ takes precedence over the uncountability of the continuum.

Thus in a version of the second order logic developed here, all suoperators constructing sets build countable sets from countable sets. So we must compare this new conclusion with an uncountable continuum assumption when proving consistent results. ☐

To deal with objections to the above proof, it has been stated that the arguments we have given in [Ad14] are dependent on representable infinitesimals. But the proof we have given here is not dependent on representable infinitesimals, and if representable infinitesimals are inconsistent then so are the axioms for a field, since their existence is contingent on either the axioms for a field, or on the existence of infinitesimals themselves.

Secondly, it might be claimed that there is no technical basis for applying induction to sets. As we have seen in section 2 on formal language and the axioms for mZFC in section 3, this is not so. Further, the discussion in [Ad15], chapter XIV, connects set theory with arithmetic, covered in the Peano axioms of section 4 defining induction. This [Ad15] discussion extends these considerations to arithmetic with suoperators, with similar results.

The technical basis we have just discussed may be expressed in category theory, presented in chapter III of this volume. An idea is that of a symbol representing a universal object, which could be a set. But because exponentiation is not directly representable in category theory, since exponentiation is nonassociative, we use section 9 of that chapter also, which represents nonassociative operations in a standard invariant form.

Thirdly, the previous proof raises issues of the status of the Cantor diagonal argument on the uncountability of the real numbers. Before dealing with this, we address its counterpart for finite sets, where the Cantor argument does not work. We extend this idea to infinite but countable sets.

The Cantor diagonal argument is deconstructed as follows. First note the example of a finite set consisting of elements ordered as (a, b), where a and b $\in$ {0, 1}, can be described as two finite sets E, F where E = {(0, 0), (0, 1)} and F = {(1, 0), (1, 1)}. In this example we define *diagonal* E to be found from

$(\underline{0}, 0)$
$(0, \underline{1})$,

that is, (0, 1) as underlined, so NOT *diagonal* E = NOT (0, 1) = (1, 0). So E is finite, and the fact that NOT *diagonal* E $\notin$ E (but $\in$ F) does not show that {E, F} is not a finite set. We have proved that *for a finite set, the diagonalisable elements form a subset of the finite set under an ordering*.

In the finite case the Cantor theorem holds that the power set (the set of subsets) of any set is larger than the set, but the NOT *diagonal* relation for finite sets does not give the correct interpretation for infinity. The correct definition of a set S_m being finite is that it is empty or has all elements $(s_1, s_2, ... s_m)$ with fixed m $\in \mathbb{N}$, and an infinite set is not finite. ☐

Definition 1.11.3. A *Eudoxus number*, u $\in \mathbb{U}$, is a number bounded within [m, n] $\in \mathbb{N}_{\neq 0}$ for some n > m, so that there exists some other natural number m which when multiplied by u lies within [m, n]. By bounded, we mean it has an absolute value, possibly represented by a norm, and this absolute value is positive, even if u is not.

Proposition 1.11.4. *A Cauchy sequence, which is normally held to represent real numbers representable at most by a convergent sum of a countably infinite set of rational numbers, satisfies the Eudoxus property.*

Theorem 1.11.5. *In the standard representation of real numbers as Cauchy sequences, the real numbers are countable.*

Proof. For the diagonal argument for infinite sets, consider the list of Eudoxus numbers denoted in binary and indexed by $2n_i$

$2\mathbb{N}$	The set of all diagonalisable Eudoxus numbers with respect to an ordering
$2n_i$	u_i

Firstly, we will consider a specific ordering of $\mathbb{U}$. By a similar argument to the finite case *diagonal* $\{u_i\}$ = {the Eudoxus number with the ith digit taken from u_i}, so NOT *diagonal* $\{u_i\} \notin \{u_i\}$ is consistent, since $\mathbb{N} \equiv 2\mathbb{N} \equiv (2\mathbb{N} + 1) \equiv 2\mathbb{N} \cup (2\mathbb{N} + 1)$, and all Eudoxus numbers are indexed by $n_i \in \mathbb{N} \equiv \mathbb{N}_{diagonal} \cup \{n_i\}_{nondiagonal}$. In this ordering $\{n_i\}_{nondiagonal}$ is one element appearing after the diagonal terms, or can be inserted in first to show the bijection with $\mathbb{N}$. Thus the utility of the diagonal argument disappears under a specific ordering.

We will now consider a generic ordering covering all possible orderings of $\mathbb{U}$. Then the larger set of $\{n_i\}_{nondiagonal}$ now corresponds to the set of possible $\mathbb{U}$, so each instance of this diagonal can appear, say, as the first element of $\mathbb{U}$ in a different ordering. Thus the utility of the diagonal argument now disappears under a generic ordering, and we are back to proving $\mathbb{N}^{\mathbb{N}} \equiv \mathbb{N}$, which we have already done, and so the Eudoxus numbers are countable. ☐

This theorem is in conflict with the assertion that $\{0, 1\}^{\mathbb{N}}$ is uncountable, which in turn uses the unacceptable definition that the NOT *diagonal* relation for countably infinite sets acts as a criterion for uncountability. However as mentioned by P. J. Cohen in [1Co63], [1Co64] ‘one can construct models in which the set of constructible reals is countable’. ☐

1.12. Fields and zero algebras.

The axioms for a *field* $\mathbb{F}$, +, ×, which we will denote simply by $\mathbb{F}$, satisfy for a, b, c ∈ $\mathbb{F}$, with a × b being written as ab

additive closure: $a + b \in \mathbb{F}$ (1)
associativity: $a + (b + c) = (a + b) + c$ (2)
abelian addition: $a + b = b + a$ (3)
existence of a zero: there exists a $0 \in \mathbb{F}$ satisfying
$a + 0 = a$ (4)
existence of negative elements: there exists a $(-a) \in \mathbb{F}$ with
$a + (-a) = 0,$ (5)
which we write introducing subtraction as
$a - a = 0$
multiplicative closure: $ab \in \mathbb{F}$ (6)
associativity: $a(bc) = (ab)c$ (7)
commutativity: $ab = ba$ (8)
existence of a 1: there exists a $1 \in \mathbb{F}$ satisfying
$a1 = a$ (9)
existence of inverse elements: there exists an $a^{-1} \in \mathbb{F}$ for $a \neq 0$ with
$a(a^{-1}) = 1,$ (10)
which we write introducing division as
$a/a = 1$
distributive law: $a(b + c) = (ab) + (ac).$ (11)

The motivation for introducing zero algebras is that multizeros which exist in them are consistent under division, whereas division by zero is inconsistent for a field. We give the axioms for a zero algebra, which like the axioms for a set do not define uniquely its chosen elements, followed by a discussion of its properties and their models.

The axioms for a *zero algebra* 𝕐, under + and ×, which we will denote simply by 𝕐, satisfy conditions (1), (2), (3), (6), (7), (8), (9), (10) and (11) for a field with the axioms for zero excluded (so this means axiom (10) always holds in a zero algebra, since zero does not belong to it), and there exist multizeros a0 ∊ 𝕐 satisfying

ordered elements:	there exists an ordering on elements so that one of a = b, a > b or b > a holds, where a $\geq$ b and b $\geq$ c implies a $\geq$ c	
additive cancellation:	a = b if and only if a + c = b + c	(12)
negative pairing:	every a is paired with a (-a)	
multizeros:	if a > (-a) an a0 ∊ 𝕐 exists with a + (-a) = a0,	(13)
which we write introducing subtraction in the case a > (-a)		
	a – a = a0	(14)
negative multiplication:	(-a)b = -(ab)	(15)
associativity:	a(b0) = (ab)0	(16)
existence of inverse elements	for multizeros; division by multizeros satisfies: (a0)/(b0) = a/b	(17)
existence of ultrainfinity:	a/(b0) = (a/b)Ч	(18)
ultrainfinity multiplication:	(a0)(bЧ) = ab	(19)
extension:	any property holding for, say, a above holds for the substitution a0 and aЧ.	(20)

For 𝕐 it may be convenient to represent a0 by a(0) when a is a specific decimal number.

How do we form concrete models of zero algebras? We look for a standard model for them. Like complex numbers which are defined by their rules, being outside other number systems otherwise, we find zero algebras have no implementations in fields, but mappings from zero algebras to fields can be defined where fields are consistent. We will also investigate whether nonstandard zero algebras exist.

The elements of a zero algebra denoted by ..., aЧЧ, aЧ, a, a0, a00, ... etc., may or may not be mapped to a field. There are two sorts of mappings from the operations on a zero algebra to the operations on a field: mappings for addition, and mappings for multiplication.

For the standard model of zero algebras, positive numbers in a zero algebra are mapped in sequence to the same positive numbers belonging to a field.

For additive operations in such a zero algebra using multizeros, the mapping to operations in a field is given by

a + (-a) = a0 → a + (-a) = 0,

in the case when a > (-a). This is the only such additive axiom.

For multiplicative operations in a standard zero algebra, the mapping to operations in a field are more varied:

a(b0) = (ab)0 → a(b0) = (ab)0 = 0,

multiplication and division is closed under multizeros, and rules (12) and (15) operate in both a zero algebra and a field. n0 = m0 does not hold for a zero algebra when n ≠ m, but does hold in a field, where division by zero is inconsistent for a field, because 0.n = 0.m, so 0/0 = m/n for any m, n. This means

$$(n0)/(m0) = (n/m) \rightarrow 0/0,$$ which is not defined in a field.

Thus a zero algebra is consistent when its operations are constrained to operations consistent for a field, but it is also consistent for operations which are inconsistent for a field. ☐

We also have (-1)(-1) = 1 – 2(0), since

$$-1(1(0)) = -1(0)$$
$$(-1)(-1 + 1) = 1(0) - 2(0)$$
$$(-1)(-1) + (-1) = 1 - 1 - 2(0),$$

which proves the statement using the cancellation rule. Since (–1)(–1) ≠ 1, we say negative numbers in a zero algebra branch or have colours. This branching may be evaluated (mod n), but congruence arithmetic here goes from 1 to n, since there is no 0. Then compared with equation (13)

$$(-a) + (-a)(-1) = (-a) + a - 2a(0) = a(0) - 2a(0) = -a(0). \quad (21)$$

Since axiom (10) for a field without a zero holds, we have

$$(-1)(-1)^{-1} = 1,$$

giving

$$(-1)(-1)^{-1} - 2(0) = 1 - 2(0),$$
$$= (-1)(-1), \quad (22)$$

and 𝕐 is consistent under subtraction, with a0 ≠ -a0, and we can say 0 ∉ 𝕐. ☐

There are degrees of freedom available to zero algebras, so a0 may be replaced by ay0, aЧ by aЧ/y where y ∈ 𝕐 with (ay0)/(by0) = a/b, etc. ☐

We can define a mapping between zero algebras, say in which for constant d

$$a' = a, \ (-a') = d + (-a),$$

where now under this transformation

$$a' + (-a') = d + a(0) = a'(0) \quad (23)$$

for some number d ∈ 𝕐. This is a nonstandard model for a zero algebra. ☐

The complex numbers, ℂ, can be given a partial order as follows. Let $a + ib = re^{i\theta} \in \mathbb{C}$. Define an order on ℂ by

(1) c = a + ib > c′ = a′ + ib′ if the norm of c > the norm of c′. The norm is defined as the positive value of $\sqrt{a^2 + b^2}$ or alternatively and equivalently as the positive value of r.

(2) If the norms of c and c′ are equal, define c > c′ for those values for which a > a′.

(3) If the methods (1) and (2) give the same result, define c > c′ for those values where b > b′.

It follows that otherwise the two complex numbers are equal.

Hence this order relation can be used to define a standard complex zero algebra. To define a complex zero algebra where the real part or the imaginary part are absent but not both, define these cases separately for the zero algebra. ☐

1.13. Ordinal (ladder) arithmetic in $\mathbb{M}_t$ and $\mathbb{R}_t$.

Definition 1.13.1. We adopt the *standard protocol* for ladder algebra:

$$\boldsymbol{\Omega}_{\mathbb{M}t} = \sum_{\text{all } \mathbb{M}t} 1. \quad (1)$$

For any n $\in \mathbb{M}_t$, n < $\mathbf{\Omega}_{\mathbb{M}t}$, so $\mathbf{\Omega}_{\mathbb{M}t} \notin \mathbb{M}_t$. In other words, the size of $\mathbf{\Omega}_{\mathbb{M}t}$ is not bijective to any element belonging to $\mathbb{M}_t$, because if it were bijective to m $\in \mathbb{M}_t$, from the Peano axioms it would also be bijective to m + 1, and m $\neq$ m + 1. We will treat $\mathbf{\Omega}_{\mathbb{M}t}$ as being irreducible. This means we do not split $\mathbf{\Omega}_{\mathbb{M}t}$ into noncontiguous components, or truncate or extend it. Because $\mathbf{\Omega}_{\mathbb{M}t}$ is irreducible, we do not allow ourselves for example the statement $\mathbf{\Omega}_{\mathbb{M}t} = \mathbf{\Omega}_{\mathbb{M}t} + 1$. We will usually treat $\mathbf{\Omega}_{\mathbb{M}t}$ as being an element of a field.

Definition 1.13.2. We adopt the <u>*strict transfer principle*</u> for ladder algebra:
the axioms for a field or zero algebra hold with respectively a$\mathbf{\Omega}_{\mathbb{M}t}$, b$\mathbf{\Omega}_{\mathbb{M}t}$ *and* c$\mathbf{\Omega}_{\mathbb{M}t}$ *replacing some or all of* a, b *and* c *in these axioms*. ☐

An example is $1\mathbf{\Omega}_{\mathbb{M}t} = \mathbf{\Omega}_{\mathbb{M}t}$.

This model has implications for our theory of infinite groups, and it allows the construction of a model of unfinished sets derived from the finished infinity $\mathbf{\Omega}_{\mathbb{R}}$, where the unfinished set for $\mathbb{R}$ the set of real numbers is defined as $\mathbf{\Omega}_{\mathbb{R}} - 1$.

We adopt for $\mathbf{\Omega}_{\mathbb{M}t}$ the negation shown below of a property attributed by Archimedes to Eudoxus of Cnidus for finite natural numbers: the ordinal infinity $\mathbf{\Omega}_{\mathbb{M}t}$ is inaccessible with respect to n and obeys the rule

for every m $\in \mathbb{M}_t$ *and for* $\mathbf{\Omega}_{\mathbb{M}t}$ *there does not exist an* n $\in \mathbb{M}_t$: $\mathbf{\Omega}_{\mathbb{M}t} <$ mn. ☐ (2)

Definition 1.13.3. *Ladder transnatural numbers* $\mathbf{L}_{\mathbb{M}t\cup 0}$ are defined by

$\mathbf{L}_{\mathbb{M}t\cup 0} = \bigcup_m[\mathbb{M}_{t\cup 0}(\mathbf{\Omega}_{\mathbb{M}t})^m]$, m $\in \mathbb{M}_{t\cup 0}$.

The algorithmic proof of a proposition by induction: choose a start value, assume for n and then prove for n + 1, now extends to n $\in \mathbf{L}_{\mathbb{M}t\cup 0}$ under the strict transfer principle. However, the Peano axiom of induction states that the natural numbers are unique, so we must augment it for $\mathbb{N}_{\cup 0}$ by saying it contains no elements $(\mathbf{\Omega}_{\mathbb{M}t})^m$. In ladder algebra the complement of all $\mathbb{M}_t$ is not empty, so an induction predicate can always be true, even in mZFC.

We know that any number k $\in \mathbb{M}_t$ is even or odd. We have seen this is part of a more general result that for any n $\in \mathbb{M}_t$ a transfinite number is representable as k (mod n). The question arises, what is the evaluation of $\mathbf{\Omega}_{\mathbb{M}t}$ (mod n)? An option is that $\mathbf{\Omega}_{\mathbb{M}t}$ is representable in terms of colour logics to be introduced in chapter II, as a different colour than that of finite numbers. This is consistent with its allocation in a transnatural ladder number satisfying the axioms of a field.

An alternative is to distinguish between finite and infinite proofs, and allocate within an infinite system a value of variables (mod n). These two definitions are similar, one applying colours to states (the numbers of the algebra), the other applying them to transformations (the finite or infinite proofs that can be obtained).

What is the status of finite proofs in this situation? We have seen by the axiom of the strict transfer principle above, that proofs by countable induction over $\mathbb{N}$ reduce to finite proofs. Thus there exist some finite proofs over countably infinite sets.

We argue in terms of states and not processes. For infinite processes, obtained values may oscillate infinitely. There are at least two approaches that we can take to enable consistency.

The first looks at logical deduction. Valid reasoning based on the evaluation of finitely determined states by processes which terminate finitely are retained. Otherwise valid infinite reasoning is restricted, so that we may be able to obtain consistent results previously unavailable. We can find *preferred evaluations* of these infinitely determined states or those with infinite processes so that the induction procedure is restricted for these types. We adopt the following method employing arguments under the strict transfer principle. For reasoning using all $\mathbb{M}_t$, start with the first element of $\mathbb{M}_t$, which is 1, and employ *linear induction* by allocating either $\mathbb{M}_t$, or an ordered block of n elements which belong to $\mathbb{M}_t$, so that the same proof is valid in each block. *Nonlinear induction* can be defined for other partitions.

The second approach extends Boolean logic. General multivalued logics are discussed in volume II, chapter V. Thus, for example, for the infinite type of systems we have been considering, we could have multivalued logic operating on three states, 'true', 'false' and 'oscillates'. A particular type of multivalued logic discussed in chapter XIII of [Ad15] is *probability logic*. A Boolean type logic with two states τ and υ can be extended so that its values are linear combinations of τ and υ, in particular retaining the boundary condition that both τ and υ exist within the logic. A linear probability logic contains the states $c\tau + (1 - c)\upsilon$ where c is, say, a real variable. It is a theorem that oscillating values may be allocated as the value $\frac{1}{2}\tau + \frac{1}{2}\upsilon$ in a linear probability logic.

The model used to interpret this logic is not here the statistical correlation approach given in chapter XIII of [Ad15], although its evaluation may be found as a limit process acting on its correlation with oscillating values.

In Greek antiquity, the paradox of the liar states that 'All Cretans are liars' and that this statement was made by a Cretan. It should be intuitively clear that a consideration of this paradox should reveal nothing about Cretans or liars, yet a famous mathematician spent a considerable effort on a project which in effect states the contrary. Such considerations are known as diagonal arguments. A theorem that the consistency of the real number system cannot be proved uses diagonal arguments.

In the 'paradox of the liar' the value of " 'A is valid' and 'A is invalid'" is false, and is not the same as " 'A is valid' and 'A is invalid' is false" (which is true) on keeping track of the level of nesting of the quotes and their implicit parentheses, so the paradox vanishes.

A further theorem that there exist undecidable statements uses general recursive functions. As is mentioned in chapter XIV of [Ad15], a function f(x) = 1 is general recursive, a function f(x) = 0 is general recursive, but their union is inconsistent since $1 \neq 0$, but the theorem ignores this fact. Thus we are left with the result that inconsistent statements are undecidable. I think we should have known that to begin with.

Since for us, logic also includes parentheses in its syntax, validity or invalidity of a formula may depend on the presence or absence of such parentheses, and this includes inductive statements, which must have them.

X is invalid	means	X is invalid
(X is invalid) is valid	means	X is invalid,

where similar and further nestings are possible. For example there is a possible chain

(((X is invalid) is invalid) is invalid).

Thus there are an infinite number of states and their infinite countable evaluation

(((X is invalid) is invalid) is invalid) ...

is equivalent to the evaluation

$$\mathrm{Y} = \prod_{\text{all natural numbers } \mathbb{N}} -1.$$

For example, using the strict transfer principle to evaluate

$$Y = \prod_{\text{all } \mathbb{N}} -1, \quad (3)$$

partition ℕ into blocks of pairs starting from 1, then for each pair evaluate as a member of

$W = (-1)_{\text{odd } \mathbb{N}} \times (-1)_{\text{even } \mathbb{N}}$,

and the product is always 1. Thus under the linear induction principle,

$Y = 1$,

and consequently the infinite countable evaluation equivalent to finding Y

(((X is invalid) is invalid) is invalid) ...

evaluates to X which is valid. Its linear probability logic evaluation is $\frac{1}{2}\tau + \frac{1}{2}\upsilon$. ☐

There exist ideals of these blocks, in which proofs of the above type live, for the example above 1.W and -1.W, and say cosets of the ideal 1.W

0 + W, and -2 + W,

where only the 0 coset is the preferred evaluation. It follows that the preferred evaluation of $\mathbf{\Omega}_{\mathbb{M}t}$ obtained additively is even and not odd, and its linear probability evaluates to

$\frac{1}{2}(\text{even} = \tau)\tau + \frac{1}{2}(\text{odd} = \tau)\upsilon$. ☐

The application of ideas of colour states and colour logics to algebraic numbers is dealt with in volume III, chapter II. We can treat $\alpha\sqrt{2}$ as a number with α neither even nor odd and $\alpha^2 = 1$, whilst forbidding the real number $\sqrt{2}$. We consider issues of transcendence involving the exponential constant e and the number derived from geometry π, and the connection with colour logics involving the capital Ξ function of section 6 also in volume III.

The successor function of adding 1 creates an order relation in ℕ. The set $\mathbb{N}_{\neq 0}$ has a least element but no maximum element. The set of negative numbers $-\mathbb{N}_{\neq 0}$ has a highest element but no minimum element. The set of integers $\mathbb{Z} = -\mathbb{N}_{\neq 0} \cup \{0\} \cup \mathbb{N}_{\neq 0}$ has neither a maximum nor a minimum element.

We have generated from $\mathbb{M}_t$ using the NOT relation for bijections, the set $\mathbb{M}_{t+1}$ as a successor of $\mathbb{M}_t$. If we treat $_{(t)}$ as a colour obtained from the set $\mathbb{M}_t$ then $\mathbf{\Omega}_{\mathbb{M}(t+1)}$ is a successor colour to $\mathbf{\Omega}_{\mathbb{M}(t)}$.

Sometimes we will treat successor functions as generating numbers or colours in a finite, or congruence, arithmetic. For a set $\{0, 1, \ldots, n - 1\} \in \mathbb{N}_{\cup 0}$ we can map an arbitrary number $k \in \mathbb{N}_{\cup 0}$ to k (mod n) in this set.

We saw that for $1^{\Xi(a)} = a \in \mathbb{N}_{\cup 0}$. By the strict transfer principle Ξ(a) can be deemed as being larger than any $\mathbf{\Omega}_{\mathbb{M}t}$, which we denote by $\mathbf{\Omega}_{\mathbb{R}}$.

We can further introduce a sequence

$\mathbf{\Omega}_{\mathbb{N}} < \mathbf{\Omega}_{\mathbb{R}t} < \mathbf{\Omega}_{\mathbb{R}u} < \ldots$

in which there are no bijections of the type $\mathbb{R}_t \to \mathbb{R}_u$. It can now occur that, say, an algorithm halts in $\mathbb{R}_u$ but not in $\mathbb{R}_t$, so $\mathbb{R}_u$ is inaccessible with respect to $\mathbb{R}_t$. ☐

The allocation of two values, True and False, to logical evaluation may be extended to an n-fold set of values. There is a relation and a difference between these values and recursive procedures. In recursion, if we apply the NOT operator to say the property of being countable for a set, then we have seen we can substitute the ordinal infinity $\mathbf{\Omega}_{\mathbb{M}t}$ describing ladder numbers in the countably infinite set $\mathbb{M}_t$ by the uncountable ordinal infinity $\mathbf{\Omega}_{\mathbb{R}t}$ of $\mathbb{R}_t$ described by the standard protocol

$$\mathbf{\Omega}_{\mathbb{R}t} = \sum_{\text{all } \mathbb{R}t} 1. \quad (4)$$

If we now apply inductively this procedure to $\boldsymbol{\Omega}_{\mathbb{R}t}$, we get a higher order uncountability of a set $\mathbb{R}_u$ with ordinal infinity $\boldsymbol{\Omega}_{\mathbb{R}u}$. There is then a countable or uncountable sequence

$$\boldsymbol{\Omega}_{\mathbb{N}} \to \boldsymbol{\Omega}_{\mathbb{R}t} \to \boldsymbol{\Omega}_{\mathbb{R}u} \to \ldots$$

corresponding to sets with successively higher cardinality.

$$\mathbb{N} \to \mathbb{R}_t \to \mathbb{R}_u \to \ldots$$

For the allocation of NOT to the value True or False, we merely switch their values. Nevertheless, we can consider this mapping as a recursion (mod 2). For an n-valued logic this may be considered as recursive (mod n).

This comparison we have been making has up to now been restricted to algebras which are abelian and associative. It is our thesis that these ideas can be extended to nonabelian and nonassociative n-fold logics. ☐

An uncountable set $\mathbb{R}$ is not generated recursively by any means from $\mathbb{N}$, even when it has a countably infinite set embedded within it. We say $\boldsymbol{\Omega}_{\mathbb{R}}$ with uncountable $\mathbb{R}$ is strictly less than ultrainfinity nЧ, $n \in \mathbb{N}$, generated in the zero algebras of section 12, whereas there exist a hierarchy of ultrainfinities $n\text{Ч}^m$, $m \in \mathbb{N}$, including superexponential types of this sort of expression, all of which are greater than $\boldsymbol{\Omega}_{\mathbb{R}}$. This arises because $(\boldsymbol{\Omega}_{\mathbb{R}})^{-1} = \boldsymbol{\varepsilon}_{\mathbb{R}}$ is not a multizero; no $a - a = \boldsymbol{\varepsilon}_{\mathbb{R}}$. ☐

The axioms for exponentiation are given as a case of those for suoperators in chapter XVII of [Ad15], and in chapter III of this volume. We extend the strict transfer principle to these axioms too. It follows that we may employ $(\boldsymbol{\Omega}_{\mathbb{M}t})^2$ and $(\boldsymbol{\Omega}_{\mathbb{M}t})^v$ for v an exponent $\in \mathbb{F}$ or $\mathbb{Y}$. For v a positive number, $(\boldsymbol{\Omega}_{\mathbb{M}t})^v$ becomes an example of a hyperinfinity.

We will denote $(\boldsymbol{\Omega}_{\mathbb{M}t})^{-1}$ by $\boldsymbol{\varepsilon}_{\mathbb{M}t}$. From the property of $\boldsymbol{\Omega}_{\mathbb{M}t}$ the ordinal infinitesimal $\boldsymbol{\varepsilon}_{\mathbb{M}t}$ satisfies

for every $m \in \mathbb{M}_t$ *and for* $\boldsymbol{\varepsilon}_{\mathbb{M}t}$ *there does not exist an* $n \in \mathbb{M}_t$: $n\boldsymbol{\varepsilon}_{\mathbb{M}t} > m$. (5)

Similarly $(\boldsymbol{\Omega}_{\mathbb{M}t})^{-u} = (\boldsymbol{\varepsilon}_{\mathbb{M}t})^u$ is a hyperinfinitesimal. ☐

If we define $\boldsymbol{\Omega}_{\mathbb{Z}t} = \sum_{\text{all } \mathbb{Z}t} 1$, then

$$\boldsymbol{\Omega}_{\mathbb{Z}t} = 1 + 2\boldsymbol{\Omega}_{\mathbb{M}t}. \quad ☐ \qquad (6)$$

The set $\mathbb{Q}$ of zero or positive rational numbers where $q = m/n \in \mathbb{Q}$, $m \in \{\mathbb{M}_t \cup 0\}$, $n \in \mathbb{M}_t$, ignoring the equivalence relation where m/n is in lowest terms, may be mapped bijectively to the set of pairs {m, n}. Then under the axiom system we are adopting, derived from the strict transfer principle acting on all pairs bounded by m and n, the number of elements of $\mathbb{Q}$ in not necessarily lowest terms is $\boldsymbol{\Omega}_{\mathbb{M}t} (\boldsymbol{\Omega}_{\mathbb{M}t} + 1)$. ☐

Using the strict transfer principle we obtain the Euler formula

$$e^{i\theta\boldsymbol{\Omega}} = \cos(\theta\boldsymbol{\Omega}) + i\sin(\theta\boldsymbol{\Omega}). \quad ☐$$

We may obtain integrals using this principle:

$$\int_0^{\Omega} x^2 \, dx = \frac{1}{3}\boldsymbol{\Omega}^3. \quad ☐$$