

# Predicative Mathematics in Type Theory

Robin Adams

July 20, 2005

## 1 Introduction

We present a weak, logic-enriched type theory intended for the formalization of predicative mathematics in the style of Weyl's "Das Kontinuum". We show how the results stated and proved in "Das Kontinuum" would be formalized in such a system.

### 1. Differences between this system and Weyl:

- We allow (through  $E_{\mathbb{N}}$ ) the definition of functions by recursion. Weyl must define these as predicates in quite a complicated manner.
- We start the natural numbers at 0, rather than 1. We follow the order of progression

$$\mathbb{N} \rightarrow \mathbb{Z} \rightarrow \mathbb{Q}$$

rather than Weyl's

$$\mathbb{N} \rightarrow \mathbb{Q}^+ \rightarrow \mathbb{Q}$$

This requires quite a lot of change in the detail in the parts dealing with  $\mathbb{Z}$  and  $\mathbb{Q}$ .

- We use function types  $A \rightarrow B$  rather than functions as graphs or as predicates.

### 2. Differences between this system and ACA:

- We consider sets besides just sets of natural numbers.
- We allow the proof of large propositions by induction.
- We use Cartesian products  $A \times B$ , rather than coding pairs of natural numbers as natural numbers.
- We use function spaces to talk about "all functions", rather than functions as graphs.

In particular, " $X$  has at least  $n$  members" seems not to be definable in ACA.

## 2 The Basic System

### 2.1 Predicate Logic with Equality

$\perp$  : **Prop**,  
 $\perp E$  :  $(P : \mathbf{Prop}, \text{Prf}[\perp])\text{Prf}[P]$ ,

$\rightarrow$  :  $(\mathbf{Prop}, \mathbf{Prop})\mathbf{Prop}$ ,  
 $\rightarrow I$  :  $(P, Q : \mathbf{Prop}; (\text{Prf}[P])\text{Prf}[Q])\text{Prf}[\rightarrow [P, Q]]$ ,  
 $\rightarrow E$  :  $(P, Q : \mathbf{Prop}; \text{Prf}[\rightarrow [P, Q]]; \text{Prf}[P])\text{Prf}[Q]$ ,

Pearse :  $(P, Q : \mathbf{Prop}, ((\text{Prf}[P])\text{Prf}[Q])\text{Prf}[P])\text{Prf}[P]$ ,

$\forall$  :  $(A : \mathbf{Type}, (A)\mathbf{Prop})\mathbf{Prop}$ ,  
 $\forall I$  :  $(A : \mathbf{Type}, P : (A)\mathbf{Prop}, (x : A)\text{Prf}[P[x]])\text{Prf}[\forall[A, P]]$ ,  
 $\forall E$  :  $(A : \mathbf{Type}, P : (A)\mathbf{Prop}, \text{Prf}[\forall[A, P]], a : A)\text{Prf}[P[a]]$ ,

$=$  :  $(A : \mathbf{Type}, A, A)\mathbf{Prop}$ ,  
 $= I$  :  $(A : \mathbf{Type}, a : A)\text{Prf}[= [A, a, a]]$ ,  
 $= E$  :  $(A : \mathbf{Type}; P : (A)\mathbf{Prop}; a, b : A; \text{Prf}[= [A, a, b]]; \text{Prf}[P[a]])\text{Prf}[P[b]]$

We write

$$\begin{aligned} P \rightarrow Q & \text{ for } P \rightarrow Q, \\ \forall x : A. P[x] & \text{ for } \forall[A, [x]P[x]], \\ a =_A b & \text{ for } = [A, a, b] \end{aligned}$$

## 2.2 The Universe of Small Types

$$\begin{aligned}
U &: \mathbf{Type}, \\
T &: (U)\mathbf{Type}, \\
\mathbb{N} &: U, \\
0 &: T[\mathbb{N}], \\
s &: (T[\mathbb{N}])T[\mathbb{N}], \\
E_{\mathbb{N}} &: (C : (T[\mathbb{N}])U, T[C[0]]), \\
(n : \mathbb{N}, T[C[n]]) & T[C[s[n]]], \\
& n : \mathbb{N})T[C[n]], \\
E_{\mathbb{N}}[C, a, b, 0] &= a, \\
E_{\mathbb{N}}[C, a, b, s[n]] &= b[n, E_{\mathbb{N}}[C, a, b, n]], \\
\times &: (U, U)U, \\
\text{pair} &: (A, B : U; T[A]; T[B])T[\times[A, B]], \\
\pi_1 &: (A, B : U; T[\times[A, B]])T[A], \\
\pi_2 &: (A, B : U; T[\times[A, B]])T[B], \\
(A, B : U; a : T[A], b : T[B]) &(\pi_1[A, B, \text{pair}[A, B, a, b]] = a : T[A]), \\
(A, B : U; a : T[A], b : T[B]) &(\pi_2[A, B, \text{pair}[A, B, a, b]] = b : T[B]),
\end{aligned}$$

We write

$$\begin{aligned}
A &\text{ for } T[A], \\
A \times B &\text{ for } \times[A, B], \\
\langle a, b \rangle &\text{ for } \text{pair}[A, B, a, b] \quad (\text{where } A \text{ and } B \text{ are clear from the context})
\end{aligned}$$

### 2.3 The Universe of Small Propositions

$$\begin{aligned}
\text{prop} & : ? \\
V & : (\text{prop})\mathbf{Prop}, \\
\hat{\perp} & : \text{prop}, \\
() (V[\hat{\perp}]) & = \perp : \mathbf{Prop}, \\
\supset & : (\text{prop}, \text{prop})\text{prop}, \\
(P, Q : \mathbf{Prop}) (V[\supset [P, Q]]) & = \rightarrow [V[P], V[Q]] : \mathbf{Prop}, \\
\hat{\forall} & : (A : U, (T[A])\text{prop})\text{prop}, \\
(A : U, P : (T[A])\text{prop}) (V[\hat{\forall}[A, P]]) & = \forall [T[A], [x : T[A]] V[P[x]]] : \mathbf{Prop}, \\
\hat{=} & : (A : U, T[A], T[A])\text{prop}, \\
(A : U; a, b : T[A]) (V[\hat{=} [A, a, b]]) & = = [T[A], a, b] : \mathbf{Prop}, \\
\text{Ind} & : (P : (T[\mathbb{N}])\text{prop}, \text{Prf}[V[P[0]]], (n : T[\mathbb{N}], \text{Prf}[V[P[n]]]) \text{Prf}[V[P[s[n]]]])
\end{aligned}$$

We write

$$\begin{aligned}
P & \text{ for } V[P], \\
P \supset Q & \text{ for } \supset [P, Q], \\
\text{forall } x : A. P & \text{ for } \text{forall}[A, [x]P], \\
a \hat{=} b & \text{ for } \hat{=} [A, a, b]
\end{aligned}$$

### 2.4 Sets and Functions

$$\begin{aligned}
\mathbf{Set} & : (\mathbf{Type})\mathbf{Type}, \\
\text{set} & : (A : \mathbf{Type}, (A)\text{prop})\mathbf{Type}, \\
\in & : (A : \mathbf{Type}, A, \mathbf{Set}[A])\text{prop}, \\
(A : \mathbf{Type}, P : (A)\text{prop}, a : A) (\in [A, a, \text{set}[A, P]]) & = P[a] : \text{prop}, \\
\rightarrow & : (\mathbf{Type}, \mathbf{Type})\mathbf{Type}, \\
\lambda & : (A, B : \mathbf{Type}; (A)B) \rightarrow [A, B], \\
\text{app} & : (A, B : \mathbf{Type}; \rightarrow [A, B], A)B, \\
(A, B : \mathbf{Type}; b : (A)B, a : A) (\text{app}[A, B, \lambda[A, B, b], a]) & = b[a] : B
\end{aligned}$$

We write

$$\begin{aligned}
\{x : A \mid P[x]\} & \text{ for } \text{set}[A, [x]P[x]], \\
a \in_A S & \text{ for } \in [A, a, S] \quad (A \text{ may be tacet}) \\
A \rightarrow B & \text{ for } \rightarrow [A, B], \\
\lambda x : A. b[x] & \text{ for } \lambda[A, B, [x]b[x]] \quad (\text{where } B \text{ is clear from the context}), \\
f(a) & \text{ for } \text{app}[A, B, f, a] \quad (\text{where } A \text{ and } B \text{ are clear from the context})
\end{aligned}$$

## 2.5 Optional Extras

- Large elimination over  $\mathbb{N}$ :

$$\begin{aligned}
& (C : (T[\mathbb{N}])\mathbf{Type}, a : C[0], b : (n : T[\mathbb{N}], C[n])C[s[n]]) (LE_{\mathbb{N}}[C, \\
& (C : (T[\mathbb{N}])\mathbf{Type}, a : C[0], b : (n : T[\mathbb{N}], C[n])C[s[n]], n : \mathbb{N}) (LE_{\mathbb{N}}[C, a, b, s[n]] = b[n, LE_{\mathbb{N}}[C, a, b, n]] : C
\end{aligned}$$

- Huge elimination over  $\mathbb{N}$ :

$$\begin{aligned}
& HE_{\mathbb{N}} : (\mathbf{Type}, (n : T[\mathbb{N}], \mathbf{Type})\mathbf{Type}) \\
& (A : \mathbf{Type}, B : (n : T[\mathbb{N}], \mathbf{Type})\mathbf{Type}) (HE_{\mathbb{N}}[A, B, 0] = A : \mathbf{Type}), \\
& (A : \mathbf{Type}, B : (n : T[\mathbb{N}], \mathbf{Type})\mathbf{Type}, n : T[\mathbb{N}]) (HE_{\mathbb{N}}[A, B, s[n]] = B[n, HE_{\mathbb{N}}[A, B, n]] : \mathbf{Type})
\end{aligned}$$

- Definition of small propositions by recursion:

$$\begin{aligned}
& E_{\mathbb{N}}^{\text{PROP}} : (\text{prop}, (n : T[\mathbb{N}], \text{prop})\text{prop}, n : T[\mathbb{N}]) \\
& (P : \text{prop}, Q : (n : T[\mathbb{N}], \text{prop})\text{prop}) (E_{\mathbb{N}}^{\text{PROP}}[P, Q, 0] = P : \text{prop}), \\
& (P : \text{prop}, Q : (n : T[\mathbb{N}], \text{prop})\text{prop}, n : T[\mathbb{N}]) (E_{\mathbb{N}}^{\text{PROP}}[P, Q, s[n]] = Q[n, E_{\mathbb{N}}^{\text{PROP}}[P, Q, n]] : \text{prop})
\end{aligned}$$

- Definition of large propositions by recursion:

$$\begin{aligned}
& E_{\mathbb{N}}^{\text{PROP}} : (\mathbf{Prop}, (n : T[\mathbb{N}], \mathbf{Prop})\mathbf{Prop}) \\
& (P : \mathbf{Prop}, Q : (n : T[\mathbb{N}], \mathbf{Prop})\mathbf{Prop}) (E_{\mathbb{N}}^{\text{PROP}}[P, Q, 0] = P : \mathbf{Prop}), \\
& (P : \mathbf{Prop}, Q : (n : T[\mathbb{N}], \mathbf{Prop})\mathbf{Prop}, n : T[\mathbb{N}]) (E_{\mathbb{N}}^{\text{PROP}}[P, Q, s[n]] = Q[n, E_{\mathbb{N}}^{\text{PROP}}[P, Q, n]] : \mathbf{Prop})
\end{aligned}$$

- Proof of large propositions by induction:

$$\text{LInd} : (P : (T[\mathbb{N}])\mathbf{Prop}, \text{Prf}[P[0]], (n : T[\mathbb{N}], \text{Prf}[P[n]])\text{Prf}[P[s[n]]], n : T[\mathbb{N}])\text{Prf}[P[n]]$$

## 3 Sets

**Definition 3.1 (Equality of Sets)** For  $A, B : \mathbf{Set}[\tau]$ , we define  $A \simeq B$  to be the proposition

$$\forall x : \tau. x \in A \leftrightarrow x \in B$$

and  $A \not\simeq B$  to be its negation. These are small propositions iff  $\tau : U$ . In this case, we may write them as  $A \hat{=} B$  and  $A \hat{\neq} B$ .

**Definition 3.2 (Subset Relation)** For  $A, B : \mathbf{Set}[\tau]$ , we define  $A \subseteq B$  to be the proposition

$$\forall x : \tau. x \in A \rightarrow x \in B$$

and  $A \subset B$  to be

$$A \subseteq B \wedge A \neq B .$$

These are small propositions iff  $\tau : U$ , in which case we write them as  $A \hat{\subseteq} B$  and  $A \hat{\subset} B$ .

**Definition 3.3 (Disjoint)** For  $A, B : \mathbf{Set}[\tau]$ , the proposition “ $A$  and  $B$  are disjoint” is the proposition

$$\forall x : \tau. x \in A \rightarrow x \in B \rightarrow \perp .$$

This is a small proposition iff  $\tau : U$ .

**Definition 3.4 (Empty Set)** For any type  $\tau : \mathbf{Type}$ , the empty set of  $\tau$ s,  $\emptyset_\tau$ , is defined to be

$$\{x : \tau \mid \hat{\perp}\} : \mathbf{Set}[\tau] .$$

**Lemma 3.5** For  $A : \mathbf{Set}[\tau]$ ,

$$\emptyset_\tau \subseteq A .$$

**Proof** This is the proposition

$$\forall x : \tau. \perp \rightarrow x \in A$$

which is easily proven using  $\perp E$ . **QED**

**Definition 3.6 (Universal Set)** For any type  $\tau : \mathbf{Type}$ , the universal set of  $\tau$ s,  $U_\tau$ , is defined to be

$$\{x : \tau \mid \hat{\top}\} : \mathbf{Set}[\tau] .$$

**Lemma 3.7** For  $A : \mathbf{Set}[\tau]$ ,

$$A \subseteq U_\tau .$$

**Proof** This is the proposition

$$\forall x : \tau. x \in A \rightarrow \top$$

which is easily proven using  $\top I$ . **QED**

**Definition 3.8** Let  $\tau : U$ . Given  $a_1, \dots, a_n : \tau$ , we write  $\{a_1, \dots, a_n\}$  for the set

$$\{x : \tau \mid x \hat{=} a_1 \hat{\vee} \dots \hat{\vee} x \hat{=} a_n\} : \mathbf{Set}[\tau] .$$

**Definition 3.9 (Complement)** For  $A : \mathbf{Set}[\tau]$ , the complement  $A^c$  is the set

$$\{x : \tau \mid x \notin A\} : \mathbf{Set}[\tau] .$$

**Definition 3.10 (Union)** For  $A, B : \mathbf{Set}[\tau]$ , the union  $A \cup B$  is the set

$$\{x : \tau \mid x \in A \vee x \in B\} : \mathbf{Set}[\tau] .$$

**Definition 3.11 (Intersection)** For  $A, B : \mathbf{Set}[\tau]$ , the intersection  $A \cap B$  is the set

$$\{x : \tau \mid x \in A \wedge x \in B\} : \mathbf{Set}[\tau] .$$

**Definition 3.12 (Relative Complement)** For  $A, B : \mathbf{Set}[\tau]$ , the relative complement  $A \setminus B$  is the set

$$A \cap B^c : \mathbf{Set}[\tau] .$$

## 4 Natural Numbers and Cardinalities

### 4.1 Natural Numbers

**Theorem 4.1 (Peano's Third Axiom)** If  $s[m] = s[n]$ , then  $m = n$ .

**Proof** Define the predecessor of  $n : \mathbb{N}$ ,  $\text{pred}[n]$ , to be

$$E_{\mathbb{N}}[[n]\mathbb{N}, 0, [x, y : \mathbb{N}]x]$$

Now, if  $s[m] = s[n]$ , then  $\text{pred}[s[m]] = \text{pred}[s[n]]$ , i.e.  $m = n$ . **QED**

**Theorem 4.2 (Peano's Fourth Axiom)** For  $n : \mathbb{N}$ ,

$$s[n] \neq 0$$

**Proof** This needs one of the following:

- HE with an empty type
- LE with an empty type in U
- $E_{\mathbb{N}}^{\text{PROP}}$
- $E_{\mathbb{N}}^{\text{PROP}}$

**QED**

**Theorem 4.3** For  $n : \mathbb{N}$ , either  $n = 0$  or there exists  $k : \mathbb{N}$  such that  $n = s[k]$ .

**Proof** We prove

$$n \hat{=}_{\mathbb{N}} 0 \vee \exists k : \mathbb{N}. n \hat{=}_{\mathbb{N}} s[k]$$

by induction on  $n$ .

The base case:  $0 = 0$ .

The induction step:  $s[n] = s[n]$ . **QED**

## 4.2 Addition

**Definition 4.4 (Addition)** For  $m, n : \mathbb{N}$ , we define  $m + n : \mathbb{N}$  to be

$$E_{\mathbb{N}}[[x]\mathbb{N}, m, [x, y]s[y], n]$$

Note that

$$\begin{aligned} m : T[\mathbb{N}] &\vdash m + 0 = m : T[\mathbb{N}], \\ m, n : T[\mathbb{N}] &\vdash m + s[n] = s[m + n] : T[\mathbb{N}] \end{aligned}$$

**Theorem 4.5 (Associative Law)** For  $m, n, p : \mathbb{N}$ ,

$$(p + m) + n = p + (m + n)$$

**Proof** Let  $m, p : \mathbb{N}$ . We prove

$$(p + m) + n \hat{=}_{\mathbb{N}} p + (m + n)$$

by induction on  $n$ .

By  $= I$  we have  $p + m = p + m$ , i.e.  $(p + m) + 0 = p + (m + 0)$ .

If  $(p + m) + n = p + (m + n)$ , then  $s[(p + m) + n] = s[p + (m + n)]$ , i.e.  $(p + m) + s[n] = p + (m + s[n])$ . **QED**

**Lemma 4.6** For  $n : \mathbb{N}$ ,

$$n = 0 + n$$

**Proof** We prove

$$n \hat{=}_{\mathbb{N}} 0 + n$$

by induction on  $n$ .

$0 = 0 + 0$  by  $= I$ . If  $m = 0 + m$ , then  $s[m] = s[0 + m]$ , i.e.  $s[m] = 0 + s[m]$ .

**QED**

**Lemma 4.7** For  $m, n : \mathbb{N}$ , the following is a theorem:

$$m + s[n] = s[m] + n$$

**Proof** Let  $m : \mathbb{N}$ . We prove

$$m + s[n] = s[m] + n$$

by induction on  $n$ .

$s[m] = s[m]$ , i.e.  $m + s[0] = s[m] + 0$ , by  $= I$ .

If  $m + s[n] = s[m] + n$ , then  $s[m + s[n]] = s[s[m] + n]$ , i.e.  $m + s[s[n]] = s[m] + s[n]$ . **QED**

**Theorem 4.8 (Commutative Law)** For  $m, n : \mathbb{N}$ , the following is a theorem:

$$m + n = n + m$$

**Proof** Let  $m : \mathbb{N}$ . We prove

$$m + n \hat{=}_{\mathbb{N}} n + m$$

by induction on  $n$ .

$m + 0 = 0 + m$  by Lemma 4.6.

If  $m + n = n + m$ , then  $s[m + n] = s[n + m] = s[n] + m$  by Lemma 4.7; i.e.  $m + s[n] = s[n] + m$ . **QED**

**Theorem 4.9 (Cancellation)** For  $m, n, p : \mathbb{N}$ , if  $m + p = n + p$ , then  $m = n$ .

**Proof** Let  $m, n : \mathbb{N}$ . We prove

$$m + p \hat{=}_{\mathbb{N}} n + p \supset m = n$$

by induction on  $p$ .

If  $m + 0 = n + 0$ , then  $m = n$  immediately.

Suppose the result holds for  $p$ . If  $m + s[p] = n + s[p]$ , i.e.  $s[m + p] = s[n + p]$ , then  $m + p = n + p$  by Peano's Third Axiom; hence  $m = n$  by induction hypothesis. **QED**

**Lemma 4.10 (Peano 4)** For  $m, n : \mathbb{N}$ , if  $m + n = 0$  then  $m = 0$  and  $n = 0$ .

**Proof** Suppose  $m + n = 0$ . If  $n \neq 0$ , then  $n = s[k]$  for some  $k : \mathbb{N}$  by Theorem 4.3. Hence  $m + n = s[m + k] = 0$ , contradicting Peano's Fourth Axiom.

Hence,  $n = 0$ . Therefore,  $m = m + 0 = m + n = 0$ . **QED**

### 4.3 Ordering Relations

**Definition 4.11 (Ordering Relation)** For  $m, n : \mathbb{N}$ , we define

$$\begin{aligned} m \leq n &\equiv \hat{\exists} p : \mathbb{N}. p + m \hat{=}_{\mathbb{N}} n : \text{prop} \\ m < n &\equiv \hat{\exists} p : \mathbb{N}. s[p] + m \hat{=}_{\mathbb{N}} n : \text{prop} \end{aligned}$$

**Lemma 4.12** For  $n : \mathbb{N}$ ,  $0 \leq n$ .

**Proof**  $n = n + 0$  by  $= I$ . **QED**

**Lemma 4.13** For  $m, n : \mathbb{N}$ , if  $m \leq n$  then  $s[m] \leq s[n]$ .

**Proof** If  $n = k + m$  then  $s[n] = k + s[m]$ . **QED**

**Theorem 4.14** For  $n : \mathbb{N}$ ,  $n \leq n$ .

**Proof**  $0 + n = n$  by Lemma 4.6. **QED**

**Theorem 4.15** For  $m, n, p : \mathbb{N}$ , if  $m \leq n$  and  $n \leq p$  then  $m \leq p$ .

**Proof** Let  $k, l : \mathbb{N}$  be such that  $n = k + m$  and  $p = l + n$ . Then

$$\begin{aligned} p &= l + (k + m) \\ &= (l + k) + m \quad (\text{Associativity}) \end{aligned}$$

**QED**

**Theorem 4.16 (Peano 4)** For  $m, n : \mathbb{N}$ , if  $m \leq n$  and  $n \leq m$  then  $m = n$ .

**Proof** Let  $k, l : \mathbb{N}$  be such that  $n = k + m$  and  $m = l + n$ . Then

$$\begin{aligned} 0 + n &= n \quad (\text{Lemma 4.6}) \\ &= k + (l + n) \\ &= (k + l) + n \quad (\text{Associativity}) \end{aligned}$$

Therefore,  $0 = k + l$  by the Cancellation Theorem. Hence  $l = 0$  by Lemma 4.10. Therefore,  $m = 0 + n = n$  (Lemma 4.6). **QED**

**Theorem 4.17** For  $m, n : \mathbb{N}$ , either  $m \leq n$  or  $s[n] \leq m$ .

**Proof** Let  $n : \mathbb{N}$ . We prove

$$m \leq n \hat{\vee} s[n] \leq m$$

by induction on  $m$ .

$0 \leq n$  by Lemma 4.12.

Suppose that  $m \leq n \vee s[n] \leq m$ . We must show  $s[m] \leq n \vee s[n] \leq s[m]$ .

**Case One** —  $m \leq n$  Let  $n = k + m$ . By Theorem 4.3,  $k = 0$  or  $k = s[l]$  for some  $l$ . If  $k = 0$ , then  $n = m$  (Lemma 4.6), so  $s[m] = 0 + s[n]$  (Lemma 4.6 again), and hence  $s[n] \leq s[m]$ . If  $k = s[l]$ , then  $n = s[l] + m = l + s[m]$  (Lemma 4.7) and so  $s[m] \leq n$ .

**Case Two** —  $s[n] \leq m$  Let  $m = k + s[n]$ . Then  $s[m] = s[k] + s[n]$  (Lemma 4.7), and so  $s[n] \leq s[m]$ .

**QED**

**Theorem 4.18** For  $m, n : \mathbb{N}$ , either  $m \leq n$  or  $n \leq m$ .

**Proof** From the previous theorem, if  $m \not\leq n$  then  $s[n] \leq m$ . Let  $m = k + s[n] = s[k] + n$  (Lemma 4.7). Then  $n \leq m$ . **QED**

**Lemma 4.19 (Peano 4)** For  $n : \mathbb{N}$ ,  $-n < 0$ .

**Proof** If  $0 = s[k] + n$ , then  $s[k] = 0$  by Lemma ??, contradicting Peano's Fourth Axiom. **QED**

**Lemma 4.20** For  $n : \mathbb{N}$ ,  $n < s[n]$ .

**Proof**  $s[n] = s[0] + n$  by Lemmas 4.6 and 4.7. **QED**

**Lemma 4.21** For  $m, n : \mathbb{N}$ ,  $m < n$  iff  $s[m] < s[n]$ .

**Proof**  $n = s[k] + m$  if and only if  $s[n] = s[k] + s[m]$ . **QED**

**Theorem 4.22 (Peano 4)** For  $n : \mathbb{N}$ ,  $\neg n < n$ .

**Proof** Suppose  $n < n$ . Let  $k : \mathbb{N}$  be such that  $n = s[k] + n$ . Then  $0 + n = s[k] + n$  by Lemma 4.6, hence  $0 = s[k]$  by Cancellation, contradicting Peano's Fourth Axiom. **QED**

**Theorem 4.23** For  $m, n, p : \mathbb{N}$ , if  $m < n$  and  $n < p$  then  $m < p$ .

**Proof** Let  $k, l : \mathbb{N}$  be such that

$$n = s[k] + m, \quad p = s[l] + n .$$

Then

$$\begin{aligned} p &= s[l] + (s[k] + m) \\ &= (s[l] + s[k]) + m \quad (\text{Associativity}) \\ &= s[s[l] + k] + m \end{aligned}$$

**QED**

**Theorem 4.24 (Trichotomy)** For  $m, n : \mathbb{N}$ , either  $m < n$ ,  $m = n$  or  $n < m$ .

**Proof** Let  $m : \mathbb{N}$ . We prove, by induction on  $n$ ,

$$m < n \vee m = n \vee n < m .$$

For the case  $n = 0$ : By Theorem 4.3,  $m$  is either 0 or  $s[k]$  for some  $k$ . If  $m = 0$ , then  $m = n$ . If  $m = s[k]$ , then  $m = s[k] + n$ , so  $n < m$ .

Now, suppose the result holds for  $n$ . We must show

$$m < s[n] \vee m = s[n] \vee s[n] < m$$

**Case One** —  $m < n$  or  $m = n$  If  $m < n$ , then  $n = s[k] + m$  for some  $k$ . If  $n = m$ , then  $n = 0 + m$  by Lemma 4.6. In either case  $n = l + m$  for some  $l$ . Therefore,  $s[n] = s[l] + m$  by Lemma 4.7, and so  $m < s[n]$ .

**Case Two** —  $n < m$  Let  $m = s[k] + n$ . By Theorem 4.3,  $k = 0$  or  $k = s[l]$  for some  $l$ .

If  $k = 0$ , then  $m = s[0] + n = s[n]$  (Lemmas 4.6 and 4.7). If  $k = s[l]$ , then  $m = s[s[l]] + n = s[l] + s[n]$  (Lemma 4.7), so  $s[n] < m$ .

**QED**

**Theorem 4.25** For  $m, n : \mathbb{N}$ ,  $m \leq n$  if and only if  $m < n$  or  $m = n$ .

**Proof**

$$\begin{aligned} m \leq n &\equiv \exists k : \mathbb{N}. n = k + m \\ &\Leftrightarrow n = 0 + m \vee \exists k : \mathbb{N}. n = s[k] + m && \text{(Theorem 4.3)} \\ &\Leftrightarrow m = n \vee m < n && \text{(Lemma 4.6)} \end{aligned}$$

**QED**

**Theorem 4.26 (Peano 4)** For  $m, n : \mathbb{N}$ ,  $m < n$  if and only if  $m \leq n$  and  $m \neq n$ .

**Proof** If  $m < n$ , then  $n = s[k] + m$  for some  $k$ , so  $m \leq n$ . Also,  $m \neq n$  by Theorem 4.22.

Conversely, suppose  $m \leq n$  and  $m \neq n$ . Then  $n = k + m$  for some  $k$ ; and  $k \neq 0$  lest  $m = n$  (Lemma 4.6). Therefore,  $k = s[l]$  for some  $l$  (Theorem ??). Hence  $n = s[l] + m$ , so  $m < n$ . **QED**

**Lemma 4.27** For  $m, n : \mathbb{N}$ ,  $m \leq n$  iff  $m < s[n]$ .

**Proof**  $n = k + m$  iff  $s[n] = s[k] + m$ , by Lemma 4.7 and Peano's Third Axiom. **QED**

**Lemma 4.28** For  $m, n : \mathbb{N}$ ,  $m < n$  iff  $s[m] \leq n$ .

**Proof**  $n = s[k] + m$  if and only if  $n = m + s[k]$  by Lemma 4.7. **QED**

**Lemma 4.29** For  $m, n, p : \mathbb{N}$ , if  $m < n$  and  $n \leq p$  then  $m < p$ .

**Proof** If  $n = s[k] + m$  and  $p = l + n$ , then  $p = l + (s[k] + m) = s[l + k] + m$  by the Associative Law. **QED**

**Lemma 4.30** For  $m, n : \mathbb{N}$ , either  $m < n$  or  $n \leq m$ .

**Proof** From Lemmas ?? and 4.27. **QED**

**Theorem 4.31** For  $m, n, p : \mathbb{N}$ , if  $m \leq n$  then  $m + p \leq n + p$ .

**Proof** Let  $k$  be such that  $n = k + m$ . Then

$$\begin{aligned} n + p &= (k + m) + p \\ &= k + (m + p) && \text{(Associativity)} \end{aligned}$$

Thus,  $m + p \leq n + p$ . **QED**

## 4.4 Multiplication

**Definition 4.32 (Multiplication)** For  $m, n : \mathbb{N}$ , define  $mn : \mathbb{N}$  to be

$$E_{\mathbb{N}}[[x]\mathbb{N}, 0, [x, y]y + m, n]$$

Thus,

$$\begin{aligned} m : \mathbb{N} &\vdash m0 = 0 : \mathbb{N} \\ m, n : \mathbb{N} &\vdash ms[n] = mn + m : \mathbb{N} \end{aligned}$$

**Theorem 4.33 (Distributive Law)** For  $m, n, p : \mathbb{N}$ ,

$$m(n + p) = mn + mp .$$

**Proof** Let  $m, n : \mathbb{N}$ . We prove, by induction on  $p$ ,

$$m(n + p) \hat{=}_{\mathbb{N}} mn + mp .$$

The base case,  $m(n + 0) = mn + m0$ , i.e.  $mn = mn$ , follows from  $= I$ .

Suppose  $m(n + p) = mn + mp$ . We must show  $m(n + s[p]) = mn + ms[p]$ , i.e.  $m(n + p) + m = mn + (mp + m)$ .

$$\begin{aligned} m(n + p) + m &= (mn + mp) + m && \text{(i.h.)} \\ &= mn + (mp + m) && \text{(Associative Law)} \end{aligned}$$

**QED**

**Theorem 4.34 (Associative Law)** For  $m, n, p : \mathbb{N}$ ,

$$(mn)p = m(np)$$

**Proof** Let  $m, n : \mathbb{N}$ . We prove, by induction on  $p$ ,

$$(mn)p \hat{=}_{\mathbb{N}} m(np) .$$

The base case,  $(mn)0 = m(n0)$ , i.e.  $0 = 0$ , follows from  $= I$ .

Suppose  $(mn)p = m(np)$ . We must show  $(mn)s[p] = m(ns[p])$ , i.e.  $(mn)p + mn = m(np + n)$ .

$$\begin{aligned} (mn)p + mn &= m(np) + mn && \text{(i.h.)} \\ &= m(np + n) && \text{(Distributive Law)} \end{aligned}$$

**QED**

**Lemma 4.35** For  $n : \mathbb{N}$ ,

$$0n = 0 .$$

**Proof** We prove

$$0n \hat{=}_{\mathbb{N}} 0$$

by induction on  $n$ .

The base case,  $0 \times 0 = 0$ , i.e.  $0 = 0$ , follows from  $= I$ .

Suppose  $0n = 0$ . We must show  $0s[n] = 0$ , i.e.  $0n = 0$ . This is simply the induction hypothesis. **QED**

**Lemma 4.36** For  $m, n : \mathbb{N}$ ,

$$s[m]n = mn + n .$$

**Proof** Let  $m : \mathbb{N}$ . We prove, by induction on  $n$ ,

$$s[m]n \hat{=}_{\mathbb{N}} mn + n .$$

The base case,  $s[m]0 = m0 + 0$ , i.e.  $0 = 0$ , follows from  $= I$ .

Suppose  $s[m]n = mn + n$ . We must show  $s[m]s[n] = ms[n] + s[n]$ , i.e.  $s[s[m]n + m] = s[(mn + m) + n]$ .

$$\begin{aligned} s[s[m]n + m] &= s[(mn + n) + m] && \text{(i.h.)} \\ &= s[(mn + m) + n] && \text{(Associative and Distributive Laws)} \end{aligned}$$

**QED**

**Theorem 4.37 (Commutative Law)** For  $m, n : \mathbb{N}$ ,

$$mn = nm .$$

**Proof** Let  $m : \mathbb{N}$ . We prove, by induction on  $n$ ,

$$mn \hat{=}_{\mathbb{N}} nm .$$

The base case,  $m0 = 0m$ , i.e.  $0 = 0m$ , follows from Lemma 4.35.

Suppose  $mn = nm$ . We must show  $ms[n] = s[n]m$ , i.e.  $mn + m = s[n]m$ .

$$\begin{aligned} mn + m &= nm + m && \text{(i.h.)} \\ &= s[n]m && \text{(Lemma 4.36)} \end{aligned}$$

**QED**

**Theorem 4.38** For  $m, n, p : \mathbb{N}$ , if  $m \leq n$  then  $pm \leq pn$ .

**Proof** Let  $n = k + m$ . Then

$$\begin{aligned} pn &= p(k + m) \\ &= pk + pm && \text{(Distributive Law)} \end{aligned}$$

**QED**

**Theorem 4.39** For  $m, n, p : \mathbb{N}$ , if  $m < n$  and  $p \neq 0$  then  $mp < np$ .

**Proof** Let  $n = s[k] + m$ . Let  $p = s[q]$ , using Theorem 4.3. Then, making free use of previous results,

$$\begin{aligned} np &= s[k]p + mp \\ &= kp + p + mp \\ &= s[kp + q] + mp \end{aligned}$$

**QED**

**Theorem 4.40 (Cancellation Law)** For  $m, n, p : \mathbb{N}$ , if  $mp = np$  and  $p \neq 0$  then  $m = n$ .

**Proof** By trichotomy, either  $m < n$ ,  $m = n$  or  $n < m$ . If  $m < n$ , then  $mp < np$ , by the previous theorem. Similarly, if  $n < m$ , then  $np < mp$ . Either of these would contradict the irreflexivity of  $<$ . Therefore,  $m = n$ . **QED**

## 4.5 Cardinality

This section requires very little change from Weyl's work, but seems to be impossible to formalise in ACA.

Throughout this section, let  $\tau : U$ .

**Definition 4.41 (LE)** Define the set  $K_n : \mathbf{Set}[\mathbf{Set}[\tau]]$  of sets with at least  $n$  elements as follows:

$$\begin{aligned} K_0 &= U_{\mathbf{Set}[\tau]} \\ K_{s[n]} &= \{A : \mathbf{Set}[\tau] \mid \hat{\exists} a : \tau.a \in A \wedge A \setminus \{a\} \in K_n\} \end{aligned}$$

We then define "A has at least  $n$  elements" to be the proposition

$$A \in K_n .$$

**Lemma 4.42 (LE, LI)** If  $A$  has at least  $n$  elements and  $A \simeq B$ , then  $B$  has at least  $n$  elements.

**Proof** We prove, by induction on  $n$ :

$$\forall A, B. A \text{ has at least } n \text{ elements} \rightarrow A \simeq B \rightarrow B \text{ has at least } n \text{ elements} .$$

For  $n = 0$ , the proposition is

$$\forall A, B. \top \rightarrow A \simeq B \rightarrow \top .$$

Suppose the result holds for  $n$ . Suppose  $A$  has at least  $s[n]$  elements. Then there exists  $a \in A$  such that  $A \setminus \{a\}$  has at least  $n$  elements. As  $A \simeq B$ , we have  $a \in B$  and  $A \setminus \{a\} \simeq B \setminus \{a\}$ . Therefore, by i.h.,  $B \setminus \{a\}$  has at least  $n$  elements. Thus,  $B$  has at least  $s[n]$  elements. **QED**

**Lemma 4.43 (LE)** For  $A : \mathbf{Set}[\tau]$ ,  $A$  has at least  $s[0]$  elements iff

$$\exists x : \tau.x \in A .$$

**Proof** “ $A$  has at least  $s[0]$  elements” is the proposition

$$\exists a \in A. \top$$

which is equivalent to the condition given. **QED**

**Theorem 4.44 (LE, LI)** For  $\tau : U$  and  $X : \mathbf{Set}[\tau]$ , if  $X$  has at least  $s[n]$  elements, then  $X$  has at least  $n$  elements.

**Proof** We prove

$$\forall X : \mathbf{Set}[\tau]. X \in K_{s[n]} \rightarrow X \in K_n$$

by induction on  $n$ .

For  $n = 0$ , let  $X \in K_{s[0]}$ . We must show  $X \in K_0$ ; but this is the proposition  $\top$ .

Now, suppose the result holds for  $n$ . Let  $X \in K_{s[s[n]]}$ . Then there exists  $x \in X$  such that  $X' \in K_{s[n]}$ , where

$$X' = \{y : \tau \mid y \in X \wedge x \neq y\} .$$

By the induction hypothesis,  $X' \in K_n$ , and so  $X \in K_{s[n]}$ . **QED**

**Theorem 4.45 (LE, LI)** For  $m, n : \mathbb{N}$  and  $X : \mathbf{Set}[\tau]$ , if  $m \leq n$  and  $X$  has at least  $n$  elements, then  $X$  has at least  $m$  elements.

**Proof** We shall prove

$$X \in K_{k+m} \rightarrow X \in K_m$$

by induction on  $k$ .

If  $X \in K_{0+m}$ , then  $X \in K_m$  by Lemma 4.6.

Assume the result holds for  $k$ . Suppose  $X \in K_{s[k]+m}$ . Then  $X \in K_{s[k+m]}$  by Lemma 4.7. Therefore, by the previous theorem,  $X \in K_{k+m}$ . The result follows by the induction hypothesis. **QED**

**Theorem 4.46 (LE, LI)** For  $A, B : \mathbf{Set}[\tau]$  and  $n : \mathbb{N}$ , if  $A \subseteq B$  and  $A$  has at least  $n$  elements, then  $B$  has at least  $n$  elements.

**Proof** We prove

$$\forall A, B : \mathbf{Set}[\tau]. A \subseteq B \rightarrow A \text{ has at least } n \text{ elements} \rightarrow A \text{ has at least } n \text{ elements}$$

by induction on  $n$ .

For  $n = 0$ , the proposition is

$$\top \rightarrow \top$$

which is a tautology.

Suppose the result holds for  $n$ . Suppose  $A$  has at least  $s[n]$  elements. Then there exists  $a \in A$  such that  $A \setminus \{a\}$  has at least  $n$  elements. Now,  $a \in B$  and  $A \setminus \{a\} \subseteq B \setminus \{a\}$ . By the induction hypothesis,  $B \setminus \{a\}$  has at least  $n$  elements; therefore,  $B$  has at least  $s[n]$  elements. **QED**

**Theorem 4.47 (LE)** For  $A : \mathbf{Set}[\tau]$ ,  $n : \mathbb{N}$  and  $a : \tau$ , if  $A$  has at least  $n$  elements and  $a \notin A$ , then  $A \cup \{a\}$  has at least  $s[n]$  members.

**Proof**  $a \in A \cup \{a\}$  and  $(A \cup \{a\}) \setminus \{a\} = A$  has at least  $n$  members. **QED**

**Lemma 4.48 (Substitution of Elements (LE, LI))** Let  $X : \mathbf{Set}[\tau]$ ;  $a, b : \tau$ ; and  $n : \mathbb{N}$ . If  $X$  has at least  $n$  elements,  $a \in X$ , and  $b \notin X$ , then  $(X \setminus \{a\}) \cup \{b\}$  has at least  $n$  elements.

**Proof** Let  $a, b : \tau$ . We shall prove by induction on  $n$ :

$\forall X : \mathbf{Set}[\tau]. X$  has at least  $n$  elements  $\rightarrow a \in X \rightarrow b \notin X \rightarrow (X \setminus \{a\}) \cup \{b\}$  has at least  $n$  elements.

For  $n = 0$ , the proposition is

$$\forall X. \top \rightarrow a \in X \rightarrow b \notin X \rightarrow \top$$

which is a tautology.

Suppose the result holds for  $n$ . Suppose  $X$  has at least  $s[n]$  elements,  $a \in X$ , and  $b \notin X$ . Then there exists  $c \in X$  such that  $X \setminus \{c\}$  has at least  $n$  elements.

**Case One** —  $a = c$  In this case, we are given that  $X \setminus \{a\}$  has at least  $n$  elements. It follows from the previous theorem that  $(X \setminus \{a\}) \cup \{b\}$  has at least  $s[n]$  elements.

**Case Two** —  $a \neq c$  Then  $c \in X \setminus \{a\}$ . Therefore, by the induction hypothesis,

$$X' = ((X \setminus \{a\}) \setminus \{c\}) \cup \{b\}$$

has at least  $n$  elements. Therefore, by the previous theorem

$$(X \setminus \{a\}) \cup \{b\} = X' \cup \{c\}$$

has at least  $s[n]$  elements.

**QED**

**Theorem 4.49 (Theorem R (LE, LI))** Let  $X : \mathbf{Set}[\tau]$ ,  $x : \tau$ ,  $n : \mathbb{N}$ . If  $X$  has at least  $s[n]$  elements and  $x \in X$ , then  $X \setminus \{x\}$  has at least  $n$  elements.

**Proof** We are given that there exists  $x_0 \in X$  such that  $X_0 = X \setminus \{x_0\}$  has at least  $n$  elements. If  $x = x_0$ , there is nothing to prove. Otherwise, by Substitution of Elements,

$$X \setminus \{x\} = ((X \setminus \{x_0\}) \setminus \{x\}) \cup \{x_0\}$$

has at least  $n$  elements. **QED**

**Definition 4.50 (Cardinal Numbers)** For  $n : \mathbb{N}$ , the cardinal number  $n, \bar{n}$ , is

$$\{x : \mathbb{N} \mid x < n\} : \mathbf{Set}[\mathbb{N}] .$$

The cardinal number  $\infty$  is  $U_{\mathbb{N}}$ .

For  $A : \mathbf{Set}[\mathbb{N}]$ , the proposition “ $A$  is a cardinal number” is the proposition

$$A \simeq U_{\mathbb{N}} \hat{\vee} \exists n : \mathbb{N}. A \simeq \bar{n} : \text{prop} .$$

**Definition 4.51 (Cut)** “ $A : \mathbf{Set}[\mathbb{N}]$  is a cut” is the following proposition:

$$\hat{\forall} m, n : \mathbb{N}. n \in A \supset m \leq n \supset m \in A : \text{prop} .$$

**Lemma 4.52**  $\emptyset_{\mathbb{N}}$  and  $U_{\mathbb{N}}$  are cuts.

**Proof** The proposition “ $\emptyset_{\mathbb{N}}$  is a cut” is

$$\forall m, n : \mathbb{N}. \perp \rightarrow m \leq n \rightarrow \perp$$

which is a tautology.

Likewise, the proposition “ $U_{\mathbb{N}}$  is a cut” is

$$\forall m, n : \mathbb{N}. \top \rightarrow m \leq n \rightarrow \top$$

which is a tautology.

**QED**

**Theorem 4.53** For  $A : \mathbf{Set}[\mathbb{N}]$ , if  $A$  is a cut,  $A \not\simeq \emptyset_{\mathbb{N}}$ , and  $A \not\simeq U_{\mathbb{N}}$ , then there exists  $n : \mathbb{N}$  such that

$$A \simeq \{x : \mathbb{N} \mid x \leq n\} .$$

**Proof** We shall show that there exists  $n$  such that  $n \in A$  and  $s[n] \notin A$ . The result then follows, for:

$$x \leq n \Rightarrow x \in A$$

since  $A$  is a cut, and

$$\begin{aligned} x \in A &\Rightarrow s[n] \not\leq x && (A \text{ is a cut}) \\ &\Rightarrow x \leq n && (\text{Theorem 4.17}) \end{aligned}$$

Thus,  $A \simeq \{x : \mathbb{N} \mid x \leq n\}$ .

So, suppose there is no  $n$  such that  $n \in A$  and  $s[n] \notin A$ ; i.e. that

$$\forall n : \mathbb{N}. n \in A \rightarrow s[n] \in A \tag{1}$$

There exists  $x$  such that  $x \in A$  (lest  $A \simeq \emptyset_{\mathbb{N}}$ ), so  $0 \in A$  (because  $0 \leq x$  by Lemma 4.12). From this and (1), it follows by induction that

$$\forall n : \mathbb{N}. n \in A .$$

Hence,  $A \simeq U_{\mathbb{N}}$ , which is a contradiction. **QED**

**Theorem 4.54** For  $A : \mathbf{Set}[\mathbb{N}]$ ,  $A$  is a cut iff  $A$  is a cardinal number.

**Proof** Suppose  $A$  is a cut. By the previous theorem, either  $A \simeq \emptyset_{\mathbb{N}}$ ,  $A \simeq U_{\mathbb{N}}$ , or  $A \simeq \{x : \mathbb{N} \mid x \leq n\}$  for some  $n : \mathbb{N}$ .

If  $A \simeq \emptyset_{\mathbb{N}}$ , then  $A \simeq \bar{0}$  (Lemma ??). If  $A \simeq U_{\mathbb{N}}$ ,  $A$  is a cardinal number immediately. If  $A \simeq \{x : \mathbb{N} \mid x \leq n\}$ , then  $A \simeq \overline{s[n]}$  (Lemma 4.27).

Conversely, suppose  $A$  is a cardinal number, i.e.  $A \simeq U_{\mathbb{N}} \vee \exists n : \mathbb{N}. A \simeq \bar{n}$ .

If  $A \simeq U_{\mathbb{N}}$ , then  $\forall x : \mathbb{N}. x \in A$ , and it follows easily that  $A$  is a cut.

Suppose  $A \simeq \bar{n}$ . Suppose  $y \in A$  and  $x \leq y$ . Then  $y < n$ , so  $x < n$ , and hence  $x \in A$ . Thus,  $A$  is a cut. **QED**

**Theorem 4.55** For cuts  $A$  and  $B$ ,  $A \subseteq B$  or  $B \subseteq A$ .

**Proof** Let  $A$  and  $B$  be cuts. Suppose  $A \not\subseteq B$ . Then there is some  $m \in A$  such that  $m \notin B$ . Now, let  $x \in B$ . Then  $m \not\leq x$  lest  $m \in B$ , so  $x \leq m$  (Theorem 4.18). Therefore,  $x \in A$ . Thus,  $B \subseteq A$ . **QED**

**Theorem 4.56** For  $m, n : \mathbb{N}$ , if  $m \leq n$  then  $\bar{m} \subseteq \bar{n}$ .

**Proof** This is immediate from Theorem ??. **QED**

**Theorem 4.57 (LE,LI)** For  $\tau : U$  and  $A : \mathbf{Set}[\tau]$ ,

$$\{x : \mathbb{N} \mid A \text{ has at least } s[x] \text{ elements}\}$$

is a cut.

**Proof** If  $A$  has at least  $s[n]$  elements, and  $m \leq n$ , then  $s[m] \leq s[n]$  by Lemma 4.13, hence  $A$  has at least  $s[m]$  elements by Theorem 4.45. **QED**

**Definition 4.58 (Cardinality (LE))** For  $\tau : U$  and  $A : \mathbf{Set}[\tau]$ , the cardinality of  $A$ ,  $|A|$ , is

$$\{n : \mathbb{N} \mid A \text{ has at least } s[n] \text{ elements}\} : \mathbf{Set}[\mathbb{N}] .$$

**Lemma 4.59** If  $A \simeq B$  then  $|A| \simeq |B|$ .

**Proof** By Lemma 4.42,  $A$  has at least  $s[n]$  elements iff  $B$  has at least  $s[n]$  elements. **QED**

**Definition 4.60 (LE)** For  $A : \mathbf{Set}[\tau]$  and  $n : \mathbb{N}$ ,  $A$  has exactly  $n$  elements iff

$$|A| \simeq \bar{n} .$$

**Lemma 4.61** If  $A \simeq B$  and  $A$  has exactly  $n$  elements, then  $B$  has exactly  $n$  elements.

**Proof** By Lemma 4.59,  $|A| \simeq |B|$ . Therefore, if  $|A| \simeq \bar{n}$  then  $|B| \simeq \bar{n}$ .  
**QED**

**Lemma 4.62 (LE)** For  $A : \mathbf{Set}[\tau]$ ,  $n : \mathbb{N}$ ,  $A$  has exactly  $n$  elements iff

$$\forall m : \mathbb{N}. A \text{ has at least } m \text{ elements} \leftrightarrow m \leq n .$$

**Proof**  $A$  has at least 0 elements trivially, and  $0 \leq n$  by Lemma 4.12.  
Therefore, the following conditions are equivalent:

- $\forall m : \mathbb{N}. A$  has at least  $m$  elements  $\leftrightarrow m \leq n$
- $\forall x : \mathbb{N}. A$  has at least  $s[x]$  elements  $\leftrightarrow s[x] \leq n$  (using Theorem 4.3).
- $\forall x : \mathbb{N}. A$  has at least  $s[x]$  elements  $\leftrightarrow x < n$  (Lemma ??)

and this last condition is  $|A| \simeq \bar{n}$ . **QED**

**Theorem 4.63 (LE, LI)** A set  $A : \mathbf{Set}[\tau]$  has exactly  $n$  elements if and only if  $A$  has at least  $n$  elements, and  $A$  does not have at least  $s[n]$  elements.

**Proof** By the lemma, the proposition “ $A$  has at exactly  $n$  elements” is equivalent to

$$\forall x : \mathbb{N}. A \text{ has at least } n \text{ elements} \leftrightarrow x \leq n \tag{2}$$

We must show that this is equivalent to “ $A$  has at least  $n$  elements, and  $A$  does not have at least  $s[n]$  elements”.

Suppose (2) holds. Then as  $n \leq n$  (Theorem ??),  $A$  has at least  $n$  elements. And, as  $s[n] \not\leq n$  (lest, by Lemma ??,  $n < n$ , which is impossible by Theorem 4.22),  $A$  does not have at least  $s[n]$  elements.

Conversely, suppose  $A$  has at least  $n$  elements, but not at least  $s[n]$ . If  $A$  has at least  $x$  elements, then  $s[n] \not\leq x$  by Theorem 4.45, so  $x \leq n$  by Lemma ?? . Conversely, if  $x \leq n$ , then  $A$  has at least  $x$  elements by Theorem 4.45.

**QED**

**Corollary 4.64** For  $A : \mathbf{Set}[\tau]$ ,  $A$  has exactly 0 elements iff

$$\forall x. x \notin A .$$

**Proof** Every set has at least 0 elements. Therefore, by the theorem,  $A$  has exactly 0 elements iff  $A$  does not have at least  $s[0]$  elements; which, by Lemma 4.43, is equivalent to

$$\neg \exists x. x \in A ;$$

which in turn is equivalent to the condition given. **QED**

**Theorem 4.65 (LE, LI)** For  $A : \mathbf{Set}[\tau]$ ,  $a : \tau$  and  $n : \mathbb{N}$ , if  $A$  has exactly  $n$  elements and  $a \notin A$ , then  $A \cup \{a\}$  has exactly  $s[n]$  elements.

**Proof** Suppose  $A$  has exactly  $n$  elements, so (by Lemma 4.62)

$$\forall x. A \text{ has at least } x \text{ elements} \leftrightarrow x \leq n .$$

We must show that

$$\forall x. A \cup \{a\} \text{ has at least } s[x] \text{ elements} \leftrightarrow x < s[n] .$$

We have

$$\begin{aligned} A \cup \{a\} \text{ has at least } s[x] \text{ elements} &\Leftrightarrow A \text{ has at least } x \text{ elements} && \text{(Theorems R and 4.47)} \\ &\Leftrightarrow x \leq n \\ &\Leftrightarrow x < s[n] && \text{(Lemma 4.27)} \end{aligned}$$

**QED**

**Theorem 4.66 (LE, LI)** For  $A : \mathbf{Set}[\tau]$ ,  $a : \tau$  and  $n : \mathbb{N}$ , if  $A$  has exactly  $s[n]$  elements and  $a \in A$ , then  $A \setminus \{a\}$  has exactly  $n$  elements.

**Proof** Suppose  $A$  has exactly  $s[n]$  elements, so

$$\forall x. A \text{ has at least } s[x] \text{ elements} \leftrightarrow x < s[n] .$$

By Lemma 4.62, we must show

$$\forall x. A \setminus \{a\} \text{ has at least } x \text{ elements} \leftrightarrow x \leq n .$$

We have

$$\begin{aligned} A \setminus \{a\} \text{ has at least } x \text{ elements} &\Leftrightarrow A \text{ has at least } s[x] \text{ elements} && \text{(Theorems R and 4.47)} \\ &\Leftrightarrow x < s[n] \\ &\Leftrightarrow x \leq n && \text{(Lemma 4.27)} \end{aligned}$$

**QED**

**Theorem 4.67 (LE, LI)** For  $A : \mathbf{Set}[\tau]$ ;  $a, b : \tau$ ; and  $n : \mathbb{N}$ ; if  $A$  has exactly  $n$  elements,  $a \in A$  and  $b \notin A$ , then  $(A \setminus \{a\}) \cup \{b\}$  has exactly  $n$  elements.

**Proof** Suppose  $A$  has exactly  $n$  elements, so (by Lemma 4.62)

$$\forall x. A \text{ has at least } x \text{ elements} \leftrightarrow x \leq n .$$

By Lemma 4.62, we must show

$$\forall x. (A \setminus \{a\}) \cup \{b\} \text{ has at least } x \text{ elements} \leftrightarrow x \leq n .$$

We have

$$\begin{aligned} (A \setminus \{a\}) \cup \{b\} \text{ has at least } x \text{ elements} &\Leftrightarrow A \text{ has at least } x \text{ elements} && \text{(Substitution of Elements)} \\ &\Leftrightarrow x \leq n \end{aligned}$$

**QED**

**Theorem 4.68 (LE, LI)** For  $A, B : \mathbf{Set}[\tau]$  and  $m, n : \mathbb{N}$ , if  $A$  has exactly  $m$  elements,  $B$  has exactly  $n$  elements, and  $A$  and  $B$  are disjoint, then  $A \cup B$  has exactly  $m + n$  elements.

**Proof** Let  $A : \mathbf{Set}[\tau]$ ,  $m : \mathbb{N}$ , and suppose  $A$  has exactly  $m$  elements. We prove, by induction on  $n$ ,

$\forall B. B$  has exactly  $n$  elements  $\rightarrow A$  and  $B$  are disjoint  $\rightarrow A \cup B$  has exactly  $m+n$  elements

For the case  $n = 0$ , suppose  $B$  has exactly 0 elements. Then, by Corollary 4.64, there is no  $x$  such that  $x \in B$ . It follows that  $A \simeq A \cup B$ , and so  $A \cup B$  has exactly  $m$  (that is,  $m + 0$ ) elements by Lemma 4.61.

Suppose the result holds for  $n$ . Suppose  $B$  has exactly  $s[n]$  elements, and  $A$  and  $B$  are disjoint. Then there exists  $b \in B$  such that  $B \setminus \{b\}$  has exactly  $n$  elements, and  $A$  and  $B \setminus \{b\}$  are disjoint. By i.h.,

$$A \cup (B \setminus \{b\})$$

has exactly  $m+n$  elements. Hence,  $A \cup B$  has exactly  $s[m+n]$  (that is,  $m+s[n]$ ) elements by Theorem 4.65. **QED**

**Theorem 4.69 (LE, LI)** For  $n : \mathbb{N}$ ,  $\bar{n}$  has exactly  $n$  elements.

**Proof** We prove

$\bar{n}$  has exactly  $n$  elements

by induction on  $n$ .

There is no  $x : \mathbb{N}$  such that  $x < 0$  by Lemma 4.19; hence, by Corollary 4.64,  $\bar{0}$  has exactly 0 elements.

Suppose  $\bar{n}$  has exactly  $n$  elements.  $x < s[n]$  iff  $x \leq n$  (Lemma 4.27), iff  $x < n$  or  $x = n$  (Theorem 4.25). Thus,

$$\overline{s[n]} \simeq \bar{n} \cup \{n\} .$$

By Theorem 4.65,  $\bar{n} \cup \{n\}$  has exactly  $s[n]$  elements. By Lemma ??, it follows that  $\overline{s[n]}$  has exactly  $s[n]$  elements. **QED**

## 5 Integers

**Definition 5.1 (Integer)** For  $m, n : \mathbb{N}$ , the integer  $m - n$  is

$$\{\langle x, y \rangle \mid m + y \hat{=}_{\mathbb{N}} n + x\} : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$$

For  $A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , “ $A$  is an integer” is the proposition

$$\hat{\exists} m, n : \mathbb{N}. A \simeq m - n .$$

**Lemma 5.2** For  $m, n : \mathbb{N}$ , and  $A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  is an integer, then

$$A \simeq m - n \leftrightarrow \langle m, n \rangle \in A .$$

**Proof** Suppose  $A \simeq m - n$ . As  $\langle m, n \rangle \in m - n$  (since  $m + n = n + m$ ), we have

$$\langle m, n \rangle \in A .$$

Conversely, suppose  $\langle m, n \rangle \in A$ . We are given that there exist  $m', n' : \mathbb{N}$  such that  $A \simeq m' - n'$ , and hence  $m + n' = n + m'$ . Therefore, for  $x, y : \mathbb{N}$ ,

$$\begin{aligned} \langle x, y \rangle \in A &\leftrightarrow x + n' = y + m' \\ &\leftrightarrow x + m + n' = y + m + m' \\ &\leftrightarrow x + n + m' = y + m + m' \\ &\leftrightarrow x + n = y + m \\ &\leftrightarrow \langle x, y \rangle \in m - n \end{aligned}$$

Thus,  $A \simeq m - n$ . **QED**

**Theorem 5.3** For  $m, m', n, n' : \mathbb{N}$ ,

$$m - n \simeq m' - n' \leftrightarrow m + n' = m' + n .$$

**Proof**

$$\begin{aligned} m - n \simeq m' - n' &\leftrightarrow \langle m', n' \rangle \in m - n \quad (\text{previous lemma}) \\ &\leftrightarrow m' + n = n' + m \end{aligned}$$

**QED**

**Definition 5.4 (Set of Integers)**  $\mathbb{Z}$ , the set of integers, is defined to be

$$\{A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}] \mid A \text{ is an integer}\} : \mathbf{Set}[\mathbf{Set}[\mathbb{N} \times \mathbb{N}]] .$$

**Definition 5.5 (Coercion of  $\mathbb{N}$  into  $\mathbb{Z}$ )** For  $n : \mathbb{N}$ , define  $n^* : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$  by

$$n^* = n - 0 .$$

**Lemma 5.6** For  $n : \mathbb{N}$ ,  $n^*$  is an integer.

**Lemma 5.7** For  $m, n : \mathbb{N}$ ,  $m = n$  iff  $m^* \simeq n^*$ .

**Definition 5.8 (Addition of Integers)** For  $A, B : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , we define  $A + B$  to be

$$\{\langle x, y \rangle \mid \hat{\exists} m, m', n, n' : \mathbb{N}. \langle m, n \rangle \in A \hat{\wedge} \langle m', n' \rangle \in B \hat{\wedge} m + m' + y \hat{=} n + n' + x\} : \mathbf{Set}[\mathbb{N} \times \mathbb{N}] .$$

**Lemma 5.9** If  $A \simeq A'$  and  $B \simeq B'$ , then  $A + B \simeq A' + B'$ .

**Proof** Trivial. **QED**

**Lemma 5.10** For  $A, B : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  and  $B$  are integers then  $A + B$  is an integer. In fact, if  $A \simeq m - n$  and  $B \simeq m' - n'$ , then

$$A + B \simeq (m + m') - (n + n') .$$

**Proof** Let  $\langle x, y \rangle \in A + B$ . Then there exist  $a, b, c, d \in \mathbb{N}$  such that

$$\begin{aligned} m + b &= n + a \\ m' + d &= n' + c \\ a + c + y &= b + d + x \\ \therefore m + m' + y + b + d &= n + n' + y + a + c \\ &= n + n' + b + d + x \\ \therefore m + m' + y &= n + n' + x \end{aligned}$$

Conversely, suppose  $m + m' + y = n + n' + x$ . Then, as  $\langle m, n \rangle \in A$  and  $\langle m', n' \rangle \in B$ , we have

$$\langle x, y \rangle \in A + B .$$

**QED**

**Lemma 5.11** For  $m, n \in \mathbb{N}$ ,  $m^* + n^* \simeq (m + n)^*$ .

**Theorem 5.12 (Associative Law)** For  $A, B, C \in \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A, B$  and  $C$  are integers, then

$$A + (B + C) \simeq (A + B) + C .$$

**Proof** Let  $A \simeq m - n$ ,  $B \simeq p - q$ , and  $C \simeq r - s$ . By the previous lemma, we must show that

$$(m + (p + r)) - (n + (q + s)) \simeq ((m + p) + r) - ((n + q) + s) .$$

By Theorem 5.3, we must show

$$(m + (p + r)) + ((n + q) + s) = ((m + p) + r) + (n + (q + s)) .$$

This follows from the Associative Law for addition of natural numbers. **QED**

**Theorem 5.13 (Commutative Law)** For  $A, B \in \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  and  $B$  are integers, then

$$A + B \simeq B + A .$$

**Proof** Let  $A \simeq m - n$ ,  $B \simeq p - q$ . By Lemma 5.10, we must show that

$$(m + p) - (n + q) \simeq (p + m) - (q + n) .$$

By Theorem 5.3, we must show

$$(m + p) + (q + n) = (p + m) + (n + q) .$$

This follows from the Associative and Commutative Laws for addition of natural numbers. **QED**

**Theorem 5.14** For  $A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  is an integer then

$$A + 0^* \simeq A .$$

**Definition 5.15** For  $A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , define  $-A$  to be

$$\{\langle m, n \rangle \mid \langle n, m \rangle \in A\} : \mathbf{Set}[\mathbb{N} \times \mathbb{N}] .$$

**Lemma 5.16** For  $A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  is an integer then  $-A$  is an integer.

**Lemma 5.17** For  $A, A' : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A \simeq A'$  then  $-A \simeq -A'$ .

**Theorem 5.18** For  $A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  is an integer then

$$A + (-A) \simeq 0^* .$$

**Definition 5.19 (Multiplication of Integers)** For  $A, B : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , define  $AB : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$  to be

$$\{\langle m, n \rangle \mid \exists p, q, r, s : \mathbb{N}. \langle p, q \rangle \in A \wedge \langle r, s \rangle \in B \wedge m = pr + qs \wedge n = ps + qr\}$$

**Lemma 5.20** For  $A, B : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  and  $B$  are integers then  $AB$  is an integer. In fact, if  $A \simeq m - n$  and  $B \simeq p - q$ , then  $AB \simeq (mp + nq) - (mq + np)$ .

**Lemma 5.21** For  $A, A', B, B' : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A \simeq A'$  and  $B \simeq B'$  then  $AB \simeq A'B'$ .

**Lemma 5.22** For  $m, n : \mathbb{N}$ ,  $m^*n^* \simeq (mn)^*$ .

**Theorem 5.23** For  $A, B, C : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A, B$  and  $C$  are integers, then

$$A(BC) \simeq (AB)C .$$

**Theorem 5.24** For  $A, B : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  and  $B$  are integers, then

$$AB \simeq BA .$$

**Theorem 5.25** For  $A : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  is an integer, then

$$A1^* \simeq A .$$

**Definition 5.26 (Ordering on Integers)** For  $A, B : \mathbf{Set}[\mathbb{N}]$ , “ $A \leq B$ ” is the proposition

$$\hat{\exists} m, m', n, n' : \mathbb{N}. \langle m, n \rangle \in A \wedge \langle m', n' \rangle \in B \wedge m + n' \leq m' + n .$$

“ $A < B$ ” is the proposition

$$\hat{\exists} m, m', n, n' : \mathbb{N}. \langle m, n \rangle \in A \wedge \langle m', n' \rangle \in B \wedge m + n' < m' + n .$$

**Lemma 5.27** For  $A, A', B, B' : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A \simeq A'$  and  $B \simeq B'$ , then  $A < B$  iff  $A' < B'$ .

**Lemma 5.28** For  $m, n : \mathbb{N}$ ,  $m^* < n^*$  iff  $m < n$ .

**Theorem 5.29** For  $A, B, C : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A, B$  and  $C$  are integers,  $A < B$  and  $B < C$  then  $A < C$ .

**Theorem 5.30** For  $A, B : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A$  and  $B$  are integers then exactly one of

$$A < B, A \simeq B, B < A$$

holds.

**Theorem 5.31** For  $A, B, C : \mathbf{Set}[\mathbb{N}^2]$ , if  $A, B$  and  $C$  are integers and  $A < B$  then

$$A + C < B + C .$$

**Theorem 5.32** For  $A, B, C : \mathbf{Set}[\mathbb{N}^2]$ , if  $A, B$  and  $C$  are integers,  $A < B$  and  $0^* < C$  then

$$AC < BC .$$

**Definition 5.33 (Domain of integers)** For  $M : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , the proposition “ $M$  is a domain of integers” is the proposition

$$\forall m, m', n, n' : \mathbb{N}. \langle m, n \rangle \in M \rightarrow m + n' = n + m' \rightarrow \langle m', n' \rangle \in M .$$

For  $A, M : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , “ $A$  belongs to  $M$ ” is the proposition

$$\exists m, n : \mathbb{N}. \langle m, n \rangle \in A \wedge \langle m, n \rangle \in M .$$

**Lemma 5.34** For  $M, M' : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $M \simeq M'$ , then  $M$  is a domain of integers iff  $M'$  is a domain of integers.

**Lemma 5.35** For  $A, A', M, M' : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $A \simeq A'$  and  $M \simeq M'$ , then  $A$  belongs to  $M$  iff  $A'$  belongs to  $M'$ .

**Lemma 5.36** For  $M, N : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , if  $M$  and  $N$  are domains of integers, then  $M \simeq N$  if and only if, for every integer  $A$ ,  $A$  belongs to  $M$  iff  $A$  belongs to  $N$ .

**Definition 5.37 (Binary Domain of Integers)** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , the proposition “ $M$  is a binary domain of integers” is the proposition

$$\forall m, m', n, n', p, p', q, q' : \mathbb{N}. \langle m, n, p, q \rangle \in M \rightarrow m + n' = m' + n \rightarrow p + q' = p' + q \rightarrow \langle m', n', p', q' \rangle \in M .$$

For  $A, B : \mathbf{Set}[\mathbb{N}^2]$  and  $M : \mathbf{Set}[\mathbb{N}^4]$ , the proposition “ $\langle A, B \rangle$  is in  $M$ ” is the proposition

$$\exists m, n, p, q : \mathbb{N}. \langle m, n \rangle \in A \wedge \langle p, q \rangle \in B \wedge \langle m, n, p, q \rangle \in M .$$

**Lemma 5.38** For  $M, M' : \mathbf{Set}[\mathbb{N}^4]$ , if  $M \simeq M'$ , then  $M$  is a binary domain of integers iff  $M'$  is a binary domain of integers.

**Lemma 5.39** For  $A, A', B, B' : \mathbf{Set}[\mathbb{N}^2]$  and  $M, M' : \mathbf{Set}[\mathbb{N}^4]$ , if  $A \simeq A'$ ,  $B \simeq B'$  and  $M \simeq M'$ , then  $\langle A, B \rangle$  is in  $M$  if and only if  $\langle A', B' \rangle$  is in  $M'$ .

**Lemma 5.40** For  $M, M' : \mathbf{Set}[\mathbb{N}^4]$ , if  $M$  and  $M'$  are binary domains of integers, then  $M \simeq M'$  if and only if, for any integers  $A$  and  $B$ ,  $\langle A, B \rangle$  is in  $M$  iff  $\langle A, B \rangle$  is in  $M'$ .

## 6 Rationals

**Definition 6.1** For  $A, B : \mathbf{Set}[\mathbb{N} \times \mathbb{N}]$ , we define  $\frac{A}{B}$  to be

$$\{\langle m, n, p, q \rangle \mid A(p - q) \simeq B(m - n)\} : \mathbf{Set}[\mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}] .$$

**Lemma 6.2** For  $A, A', B, B' : \mathbf{Set}[\mathbb{N}^2]$ , if  $A \simeq A'$  and  $B \simeq B'$  then  $\frac{A}{B} \simeq \frac{A'}{B'}$ .

**Lemma 6.3** For  $A, A', B, B' : \mathbf{Set}[\mathbb{N}^2]$ , if  $A, A', B$  and  $B'$  are integers, then

$$\frac{A}{B} \simeq \frac{A'}{B'} \leftrightarrow AB' \simeq A'B .$$

**Lemma 6.4** For integers  $A, B : \mathbf{Set}[\mathbb{N}^2]$ ,  $\frac{A}{B}$  is a binary domain of integers, and, for integers  $C, D$ ,  $\langle C, D \rangle$  is in  $\frac{A}{B}$  iff  $AD \simeq BC$ .

**Definition 6.5 (Rational)** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , “ $Q$  is a rational” is the proposition

$$\exists m, n, p, q : \mathbb{N}. p \neq q \wedge Q \simeq \frac{m - n}{p - q} .$$

**Lemma 6.6** For  $Q, Q' : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q \simeq Q'$ , then  $Q$  is a rational iff  $Q'$  is a rational.

**Lemma 6.7** Every rational is a binary domain of integers.

**Definition 6.8 (Set of Rationals)**  $\mathbb{Q}$  is

$$\{Q : \mathbf{Set}[\mathbb{N}^4] \mid Q \text{ is a rational}\} : \mathbf{Set}[\mathbf{Set}[\mathbb{N}^4]] .$$

**Definition 6.9 (Coercion from  $\mathbb{Z}$  into  $\mathbb{Q}$ )** For  $A : \mathbf{Set}[\mathbb{N}^2]$ , define  $A^\dagger$  to be

$$\frac{A}{1^*} .$$

**Lemma 6.10** For  $A, A' : \mathbf{Set}[\mathbb{N}^2]$ , if  $A \simeq A'$  then  $A^\dagger \simeq A'^\dagger$ .

**Lemma 6.11** For  $A : \mathbf{Set}[\mathbb{N}^2]$ , if  $A$  is an integer then  $A^\dagger$  is a rational.

**Definition 6.12 (Addition of Rationals)** For  $A, B : \mathbf{Set}[\mathbb{N}^4]$ , define  $A + B$  to be

$$\{\langle m, n, p, q \rangle \mid p \neq q \wedge \exists a, b, c, d, x, y, z, w : \mathbb{N} \mid \langle a, b, c, d \rangle \in A \wedge \langle x, y, z, w \rangle \in B \wedge (m-n)(c-d)(z-w) \simeq (a-b)(p-q)\}$$

**Lemma 6.13** For  $A, A', B, B' : \mathbf{Set}[\mathbb{N}^4]$ , if  $A \simeq A'$  and  $B \simeq B'$  then  $A + B \simeq A' + B'$ .

**Lemma 6.14** For  $A, B : \mathbf{Set}[\mathbb{N}^4]$ , if  $A$  and  $B$  are rationals then  $A + B$  is a rational.

**Lemma 6.15** For  $A, B, C, D : \mathbf{Set}[\mathbb{N}^2]$ , if  $A, B, C$  and  $D$  are integers and  $B \neq 0^* \neq D$  then

$$\frac{A}{B} + \frac{C}{D} \simeq \frac{AD + BC}{BD} .$$

**Lemma 6.16** For  $A, B : \mathbf{Set}[\mathbb{N}^2]$ , if  $A$  and  $B$  are integers then

$$(A + B)^\dagger \simeq A^\dagger + B^\dagger .$$

**Theorem 6.17** For  $A, B : \mathbf{Set}[\mathbb{N}^4]$ , if  $A$  and  $B$  are rationals then

$$A + B \simeq B + A .$$

**Theorem 6.18** For  $A, B, C : \mathbf{Set}[\mathbb{N}^4]$ , if  $A, B$  and  $C$  are rationals then

$$A + (B + C) \simeq (A + B) + C .$$

**Theorem 6.19** For  $A : \mathbf{Set}[\mathbb{N}^4]$ , if  $A$  is a rational then

$$A + 0^{*\dagger} \simeq A .$$

**Definition 6.20** For  $A : \mathbf{Set}[\mathbb{N}^4]$ , we define  $-A$  to be

$$\{\langle m, n, p, q \rangle \mid \langle n, m, p, q \rangle \in A\} : \mathbf{Set}[\mathbb{N}^4] .$$

**Lemma 6.21** For  $A, A' : \mathbf{Set}[\mathbb{N}^4]$ , if  $A \simeq A'$  then  $-A \simeq -A'$ .

**Lemma 6.22** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q$  is a rational then  $-Q$  is a rational.

**Lemma 6.23** For  $A, B : \mathbf{Set}[\mathbb{N}^2]$ , if  $A$  and  $B$  are integers and  $B \neq 0$ , then

$$-\frac{A}{B} \simeq \frac{-A}{B} .$$

**Lemma 6.24** For  $A : \mathbf{Set}[\mathbb{N}^2]$ , if  $A$  is an integer then

$$-(A^\dagger) \simeq (-A)^\dagger .$$

**Theorem 6.25** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q$  is a rational then

$$Q + (-Q) \simeq 0^{*\dagger} .$$

**Definition 6.26 (Multiplication of Rationals)** For  $A, B : \mathbf{Set}[\mathbb{N}^4]$ , we define  $AB : \mathbf{Set}[\mathbb{N}^4]$  to be

$$\{\langle m, n, p, q \rangle \mid p \neq q \wedge \exists a, b, c, d, x, y, z, w : \mathbb{N}. \langle a, b, c, d \rangle \in A \wedge \langle x, y, z, w \rangle \in B \wedge (m-n)(c-d)(z-w) \simeq (p-q)(a-b)\}$$

**Lemma 6.27** For  $A, A', B, B' : \mathbf{Set}[\mathbb{N}^4]$ , if  $A \simeq A'$  and  $B \simeq B'$  then  $AB \simeq A'B'$ .

**Lemma 6.28** For  $A, B : \mathbf{Set}[\mathbb{N}^4]$ , if  $A$  and  $B$  are rationals then  $AB$  is a rational.

**Lemma 6.29** For  $A, B, C, D : \mathbf{Set}[\mathbb{N}^2]$ , if  $A, B, C$  and  $D$  are integers and  $B \neq 0^* \neq D$  then

$$\frac{A C}{B D} \simeq \frac{AC}{BD} .$$

**Lemma 6.30** For  $A, B : \mathbf{Set}[\mathbb{N}^2]$ , if  $A$  and  $B$  are integers then

$$(AB)^\dagger \simeq A^\dagger B^\dagger .$$

**Theorem 6.31** For  $A, B : \mathbf{Set}[\mathbb{N}^4]$ , if  $A$  and  $B$  are rationals then

$$AB \simeq BA .$$

**Theorem 6.32** For  $A, B, C : \mathbf{Set}[\mathbb{N}^4]$ , if  $A, B$  and  $C$  are rationals then

$$A(BC) \simeq (AB)C .$$

**Theorem 6.33** For  $A : \mathbf{Set}[\mathbb{N}^4]$ , if  $A$  is a rational then

$$A1^{*\dagger} \simeq A .$$

**Definition 6.34 (Reciprocal)** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , we define  $Q^{-1}$  to be

$$\{\langle m, n, p, q \rangle \mid \langle p, q, m, n \rangle \in Q\} .$$

**Lemma 6.35** For  $Q, Q' : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q \simeq Q'$  then  $Q^{-1} \simeq Q'^{-1}$ .

**Lemma 6.36** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q$  is a rational then  $Q^{-1}$  is a rational.

**Lemma 6.37** For  $A, B : \mathbf{Set}[\mathbb{N}^2]$ , if  $A$  and  $B$  are integers and  $A \neq 0^* \neq B$ , then

$$\left(\frac{A}{B}\right)^{-1} \simeq \frac{B}{A} .$$

**Theorem 6.38** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q$  is a rational and  $Q \neq 0^{*\dagger}$ , then

$$QQ^{-1} \simeq 1^{*\dagger} .$$

**Definition 6.39 (Ordering on the Rationals)** For  $Q, Q' : \mathbf{Set}[\mathbb{N}^4]$ , the proposition  $Q < Q'$  is the proposition

$$\exists a, b, c, d, m, n, p, q : \mathbb{N}. \langle a, b, c, d \rangle \in Q \wedge \langle m, n, p, q \rangle \in Q' \wedge d < c \wedge q < p \wedge (a-b)(p-q) < (c-d)(m-n) .$$

**Lemma 6.40** For  $Q, Q', R, R' : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q \simeq Q'$  and  $R \simeq R'$ , then  $Q < R$  iff  $Q' < R'$ .

**Theorem 6.41** For  $Q, R, S : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q, R$  and  $S$  are rationals,  $Q < R$  and  $R < S$  then  $Q < S$ .

**Theorem 6.42** For  $Q, R : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q$  and  $R$  are rationals, then exactly one of

$$Q < R, Q \simeq R, R < Q$$

holds.

**Theorem 6.43** For  $Q, R, S : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q, R$  and  $S$  are rationals and  $Q < R$ , then

$$Q + S < R + S .$$

**Theorem 6.44** For  $Q, R, S : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q, R$  and  $S$  are rationals,  $Q < R$  and  $0^{*\dagger} < S$ , then

$$QS < RS .$$

**Definition 6.45 (Domain of Rationals)** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , "M is a domain of rationals" is the proposition

$$\forall m, m', n, n', p, p', q, q' : \mathbb{N}. p \neq q \rightarrow p' \neq q' \rightarrow \langle m, n, p, q \rangle \in M \rightarrow \frac{m-n}{p-q} \simeq \frac{m'-n'}{p'-q'} \rightarrow \langle m', n', p', q' \rangle \in M .$$

For  $A, M : \mathbf{Set}[\mathbb{N}^4]$ , "A belongs to M" is the proposition

$$\exists m, n, p, q : \mathbb{N}. \langle m, n, p, q \rangle \in A \wedge \langle m, n, p, q \rangle \in M .$$

**Lemma 6.46** For  $M, M' : \mathbf{Set}[\mathbb{N}^4]$ , if  $M \simeq M'$  then M is a domain of rationals iff  $M'$  is a domain of rationals.

**Lemma 6.47** For  $A, A', M, M' : \mathbf{Set}[\mathbb{N}^4]$ , if  $A \simeq A'$  and  $M \simeq M'$ , then A belongs to M if and only if  $A'$  belongs to  $M'$ .

**Lemma 6.48** For  $m, n, p, q : \mathbb{N}$  and  $M : \mathbf{Set}[\mathbb{N}^4]$ , if M is a domain of rationals, then  $\frac{m-n}{p-q}$  belongs to M iff  $\langle m, n, p, q \rangle \in M$ .

**Definition 6.49** For  $M, M' : \mathbf{Set}[\mathbb{N}^4]$ , the proposition  $M \approx M'$  (M and  $M'$  are equal as domains of rationals) is the proposition

$$\forall m, n, p, q : \mathbb{N}. p \neq q \rightarrow (\langle m, n, p, q \rangle \in M \leftrightarrow \langle m, n, p, q \rangle \in M') .$$

**Lemma 6.50** If M, N and P are domains of rationals:

1.  $M \approx M$
2.  $M \approx N \rightarrow N \approx M$
3.  $M \approx N \rightarrow N \approx P \rightarrow M \approx P$

## 7 Real Numbers

**Definition 7.1 (Cut)** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , "M is a cut" is the proposition

$M$  is a domain of rationals  $\wedge \forall a, b, c, d, m, n, p, q : \mathbb{N}. c \neq d \rightarrow p \neq q \rightarrow \frac{a-b}{c-d} < \frac{m-n}{p-q} \rightarrow \langle m, n, p, q \rangle \in M$

**Lemma 7.2** For  $M, M' : \mathbf{Set}[\mathbb{N}^4]$ , if  $M \approx M'$  then  $M$  is a cut iff  $M'$  is a cut.

**Lemma 7.3** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , if  $M$  is a domain of rationals, then  $M$  is a cut iff, for all rationals  $Q, R$ , if  $Q < R$  and  $R$  belongs to  $M$  then  $Q$  belongs to  $M$ .

**Definition 7.4 (Open Cut)** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , "M is an open cut" is the proposition

$M$  is a cut  $\wedge \forall a, b, c, d : \mathbb{N}. c \neq d \rightarrow \langle a, b, c, d \rangle \in M \rightarrow \exists m, n, p, q : \mathbb{N}. p \neq q \wedge \frac{a-b}{c-d} < \frac{m-n}{p-q} \wedge \langle m, n, p, q \rangle \in M$

**Lemma 7.5** For  $M, M' : \mathbf{Set}[\mathbb{N}^4]$ , if  $M \approx M'$ , then  $M$  is an open cut iff  $M'$  is an open cut.

**Lemma 7.6** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , if  $M$  is a domain of rationals, then  $M$  is an open cut iff  $M$  is a cut and, for every rational  $Q$  that belongs to  $M$ , there is a rational  $R$  that belongs to  $M$  such that  $Q < R$ .

**Definition 7.7 (Real Number)** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , the proposition "R is a real number" is the proposition

$R$  is an open cut  $\wedge (\exists m, n, p, q : \mathbb{N}. p \neq q \wedge \langle m, n, p, q \rangle \in R) \wedge \exists m, n, p, q : \mathbb{N}. p \neq q \wedge \langle m, n, p, q \rangle \notin R$  .

**Lemma 7.8** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , if  $R$  is a domain of rationals, then  $R$  is a real number iff  $R$  is an open cut, there exists a rational  $Q$  such that  $Q$  is a member of  $R$ , and there exists a rational  $Q$  such that  $Q$  is not a member of  $R$ .

**Lemma 7.9** For  $R, R' : \mathbf{Set}[\mathbb{N}^4]$  domains of rationals, if  $R \approx R'$  then  $R$  is a real number iff  $R'$  is a real number.

**Definition 7.10 (Set of Real Numbers)** The set of real numbers  $\mathbb{R}$  is

$$\{R : \mathbf{Set}[\mathbb{N}^4] \mid R \text{ is a real number}\} : \mathbf{Set}[\mathbf{Set}[\mathbb{N}^4]] .$$

**Definition 7.11 (Coercion from  $\mathbb{Q}$  to  $\mathbb{R}$ )** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , define  $Q^\ddagger$  to be

$$\{\langle m, n, p, q \rangle \mid p \neq q \wedge \exists a, b, c, d : \mathbb{N}. c \neq d \wedge \langle a, b, c, d \rangle \in Q \wedge \frac{m-n}{p-q} < \frac{a-b}{c-d}\} : \mathbf{Set}[\mathbb{N}^4] .$$

**Lemma 7.12** For  $Q, Q' : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q \simeq Q'$  then  $Q^\ddagger \approx Q'^\ddagger$ .

**Lemma 7.13** For  $Q : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q$  is a rational then  $Q^\ddagger$  is a real number.

## 7.1 Addition

**Definition 7.14 (Addition of Real Numbers)** For  $R, S : \mathbf{Set}[\mathbb{N}^4]$ , define  $R \oplus S$  to be

$$\{\langle m, n, p, q \rangle \mid p \neq q \wedge \exists a, b, c, d, x, y, z, w : \mathbb{N}. c \neq d \wedge z \neq w \wedge \langle a, b, c, d \rangle \in R \wedge \langle x, y, z, w \rangle \in S \wedge \frac{m-n}{p-q} \simeq \frac{a-b}{c-d} + \frac{x-y}{z-w}\}$$

**Lemma 7.15** For  $R, S : \mathbf{Set}[\mathbb{N}^4]$ , if  $R$  and  $S$  are real numbers then  $R \oplus S$  is a real number.

**Lemma 7.16** For  $R, R', S, S' : \mathbf{Set}[\mathbb{N}^4]$  real numbers, if  $R \approx R'$  and  $S \approx S'$  then  $R \oplus S \simeq R' \oplus S'$ .

**Lemma 7.17** For  $Q, R : \mathbf{Set}[\mathbb{N}^4]$ , if  $Q$  and  $R$  are rationals then

$$(Q + R)^\ddagger \simeq Q^\ddagger \oplus R^\ddagger .$$

**Theorem 7.18** For  $R, S : \mathbf{Set}[\mathbb{N}^4]$ , if  $R$  and  $S$  are real numbers, then

$$R \oplus S \approx S \oplus R .$$

**Theorem 7.19** For  $R, S, T : \mathbf{Set}[\mathbb{N}^4]$ , if  $R, S$  and  $T$  are real numbers, then

$$R \oplus (S \oplus T) \approx (R \oplus S) \oplus T .$$

**Theorem 7.20** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , if  $R$  is a real number then

$$R \oplus 0^{*\ddagger} \approx R .$$

**Definition 7.21** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , we define  $\ominus R$  to be

$$\{\langle m, n, p, q \rangle \mid p \neq q \wedge \exists a, b, c, d : \mathbb{N}. c \neq d \wedge \frac{a-b}{c-d} < \frac{m-n}{p-q} \wedge \langle a, b, c, d \rangle \notin R\} : \mathbf{Set}[\mathbb{N}^4] .$$

In Weyl, this is just "This form of addition admits a unique inverse operation, i.e., subtraction."

**Lemma 7.22** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , if  $R$  is a real number then  $\ominus R$  is a real number.

**Lemma 7.23** For  $R, R' : \mathbf{Set}[\mathbb{N}^4]$  real numbers, if  $R \approx R'$  then  $\ominus R \approx \ominus R'$ .

**Theorem 7.24** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , if  $R$  is a real number then

$$R \oplus (\ominus R) \approx 0^{*\ddagger} .$$

## 7.2 Ordering

**Definition 7.25 (Ordering on Reals)** For  $R, S : \mathbf{Set}[\mathbb{N}^4]$ , the proposition  $R \ll S$  is the proposition

$$R \subseteq S \wedge R \neq S .$$

**Lemma 7.26** For  $R, R', S, S' : \mathbf{Set}[\mathbb{N}^4]$  real numbers, if  $R \approx R'$  and  $S \approx S'$  then  $R \ll S$  iff  $R' \ll S'$ .

**Theorem 7.27** For  $R, S, T : \mathbf{Set}[\mathbb{N}^4]$ , if  $R, S$  and  $T$  are real numbers,  $R \ll S$  and  $S \ll T$ , then  $R \ll T$ .

**Theorem 7.28** For  $R, S : \mathbf{Set}[\mathbb{N}^4]$ , if  $R$  and  $S$  are real numbers, then exactly one of

$$R \ll S, R \simeq S, S \ll R$$

holds.

**Definition 7.29 (Positive)** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , the proposition "R is positive" is the proposition

$$0^{*\dagger} \ll R .$$

For  $R : \mathbf{Set}[\mathbb{N}^4]$ , the proposition "R is negative" is the proposition

$$R \ll 0^{*\dagger} .$$

**Lemma 7.30** For  $R, R' : \mathbf{Set}[\mathbb{N}^4]$  real numbers, if  $R \approx R'$ , then  $R$  is positive iff  $R'$  is positive, and  $R$  is negative iff  $R'$  is negative.

## 7.3 Open Remainders

**Definition 7.31 (Open Remainder)** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , the proposition "M is an open remainder" is the proposition

$M$  is a domain of rationals  $\wedge (\forall a, b, c, d, m, n, p, q : \mathbb{N}. \langle a, b, c, d \rangle \in M \rightarrow \frac{a-b}{c-d} < \frac{m-n}{p-q} \rightarrow \langle m, n, p, q \rangle \in M)$ .

**Definition 7.32 (Complement)** For  $M : \mathbf{Set}[\mathbb{N}^4]$ , the upper complement  $M^c$  is defined to be

$$\{\langle m, n, p, q \rangle \mid \exists a, b, c, d : \mathbb{N}. \frac{a-b}{c-d} < \frac{m-n}{p-q} \wedge \langle a, b, c, d \rangle \notin M\} : \mathbf{Set}[\mathbb{N}^4] .$$

The lower complement  $M_c$  is defined to be

$$\{\langle m, n, p, q \rangle \mid \exists a, b, c, d : \mathbb{N}. \frac{m-n}{p-q} < \frac{a-b}{c-d} \wedge \langle a, b, c, d \rangle \notin M\} : \mathbf{Set}[\mathbb{N}^4] .$$

**Lemma 7.33** 1. If  $M$  is an open cut, then  $M^c$  is an open remainder.

2. If  $M$  is an open remainder, then  $M_c$  is an open cut.

3. If  $M$  is an open cut, then  $(M^c)_c \approx M$ .

4. If  $M$  is an open remainder, then  $(M_c)^c \approx M$ .

## 7.4 Multiplication

**Definition 7.34 (Multiplication of a Real by a Positive Rational)** For  $Q, R : \mathbf{Set}[\mathbb{N}^4]$ , define  $Q \cdot R$  to be

$$\{\langle m, n, p, q \rangle \mid p \neq q \wedge \exists a, b, c, d : \mathbb{N}. c \neq d \wedge \langle a, b, c, d \rangle \in R \wedge \frac{m-n}{p-q} \simeq Q \frac{a-b}{c-d}\} : \mathbf{Set}[\mathbb{N}^4] .$$

**Lemma 7.35** If  $Q \simeq Q'$  and  $R \simeq R'$  then  $Q \cdot R \simeq Q' \cdot R'$ .

**Lemma 7.36** If  $Q$  is a rational,  $R$  a real number, and  $0^{*\dagger} < Q$ , then  $Q \cdot R$  is a real number.

**Lemma 7.37** If  $Q$  and  $Q'$  are rationals and  $0^{*\dagger} < Q$ , then  $Q \cdot Q'^{\ddagger} \simeq (QQ')^{\ddagger}$ .

**Definition 7.38 (Multiplication of a Real by a Rational)** For  $Q, R : \mathbf{Set}[\mathbb{N}^4]$ , define  $Q \times R$  to be

$$\begin{aligned} \{\langle m, n, p, q \rangle \mid & (Q \simeq 0^{*\dagger} \wedge \langle m, n, p, q \rangle \in 0^{*\ddagger\dagger}) \\ & \vee (0^{*\dagger} < Q \wedge \langle m, n, p, q \rangle \in Q \cdot R) \\ & \vee (Q < 0^{*\dagger} \wedge \langle m, n, p, q \rangle \in \ominus(-Q \cdot R))\} : \mathbf{Set}[\mathbb{N}^4] . \end{aligned}$$

**Lemma 7.39** If  $Q \simeq Q'$  and  $R \simeq R'$  then  $Q \times R \simeq Q' \times R'$ .

**Lemma 7.40** If  $Q$  is a rational and  $R$  a real number, then  $Q \times R$  is a real number.

**Definition 7.41 (Multiplication of Reals)** For  $R, S : \mathbf{Set}[\mathbb{N}^4]$ , define  $R \otimes S$  to be

$$\begin{aligned} \{\langle m, n, p, q \rangle \mid & (S \simeq 0^{*\ddagger\dagger} \wedge \langle m, n, p, q \rangle \in 0^{*\ddagger\dagger}) \\ & \vee (0^{*\ddagger\dagger} \ll S \wedge \exists a, b, c, d : \mathbb{N}. c \neq d \wedge \langle a, b, c, d \rangle \in R \wedge \langle m, n, p, q \rangle \in \frac{a-b}{c-d} \odot S) \\ & \vee (S \ll 0^{*\ddagger\dagger} \wedge \exists a, b, c, d : \mathbb{N}. c \neq d \wedge \langle a, b, c, d \rangle \in R^c \wedge \langle m, n, p, q \rangle \in \frac{a-b}{c-d} \odot S)\} : \mathbf{Set}[\mathbb{N}^4] . \end{aligned}$$

**Lemma 7.42** If  $R$  and  $S$  are real numbers, then  $R \otimes S$  is a real number.

**Lemma 7.43** If  $R, R', S$  and  $S'$  are real numbers,  $R \approx R'$  and  $S \approx S'$ , then  $R \otimes S \approx R' \otimes S'$ .

**Definition 7.44 (Reciprocal)** For  $R : \mathbf{Set}[\mathbb{N}^4]$ , define  $R^b$  to be

$$\begin{aligned} \{\langle m, n, p, q \rangle \mid & p \neq q \wedge \\ & ((0^{*\ddagger\dagger} \ll R \wedge \frac{m-n}{p-q} \odot R \ll 1^{*\ddagger\dagger}) \vee \\ & (R \ll 0^{*\ddagger\dagger} \wedge 1^{*\ddagger\dagger} \ll \frac{m-n}{p-q} \odot R))\} . \end{aligned}$$

## 7.5 Miscellany

**Definition 7.45 (Natural Number Exponentiation (LE))** For  $R : \mathbf{Set}[\mathbb{N}^4]$  and  $n : \mathbb{N}$ , we define  $R^n$  to be

$$E_{\mathbb{N}}[[x]\mathbf{Set}[\mathbb{N}^4], 1^{*\dagger\dagger}, [n, X]R \otimes X, n]$$

Thus

$$\begin{aligned} R^0 &= 1^{*\dagger\dagger} \\ R^{s[n]} &= R \otimes R^n \end{aligned}$$

**Definition 7.46 (Algebraic Numbers (LE))** For  $n : \mathbb{N}$  and  $R : \mathbf{Set}[\mathbb{N}^4]$ , define the proposition " $R$  is algebraic of degree at most  $n$ " to be

$$\langle R, 1^{*\dagger\dagger} \rangle \in E_{\mathbb{N}}[[x]\mathbf{Set}[\mathbf{Set}[\mathbb{N}^4]^2], \{ \langle A, B \rangle \mid A \text{ is a real number} \wedge B \simeq 0^{*\dagger\dagger} \}, [m, X] \{ \langle A, B \rangle \mid \exists a, b, c, d : \mathbb{N}. \langle A, A \otimes B \ominus \frac{a-b^\dagger}{c-d} \rangle \in X \}] .$$

For  $R : \mathbf{Set}[\mathbb{N}^4]$ , define " $R$  is algebraic" to be

$$\exists n : \mathbb{N}. R \text{ is algebraic of degree at most } n .$$

Explanation: Let us write  $\Delta^n(L)$  for

$$E_{\mathbb{N}}[[x]\mathbf{Set}[\mathbf{Set}[\mathbb{N}^4]^2], L, [m, X] \{ \langle A, B \rangle \mid \exists a, b, c, d : \mathbb{N}. \langle A, A \otimes B \ominus \frac{a-b^\dagger}{c-d} \rangle \in X \}] .$$

We have thus defined " $R$  is algebraic of degree at most  $n$ " to be

$$\langle R, 1 \rangle \in \Delta^n(\mathbb{R} \times \{0\}) .$$

We have

$$\begin{aligned} \Delta^0(L) &= L \\ \Delta^{n+1}(L) &= \{ \langle A, B \rangle \mid (\exists q \in \mathbb{Q}) \langle A, AB - q \rangle \in \Delta^n(L) \} \end{aligned}$$

and hence that

$$\begin{aligned} \Delta^n(L) &= \{ \langle A, B \rangle \mid (\exists a_1, \dots, a_n \in \mathbb{Q}) \langle A, A^n B - a_1 A^{n-1} - a_2 A^{n-2} - \dots - a_n \rangle \in L \} \\ \therefore \Delta^n(\mathbb{R} \times \{0\}) &= \{ \langle A, B \rangle \mid A \text{ is a real number} \wedge (\exists a_1, \dots, a_n \in \mathbb{Q}) A^n B - a_1 A^{n-1} - a_2 A^{n-2} - \dots - a_n \in L \} \\ \therefore \langle R, 1 \rangle \in \Delta^n(\mathbb{R} \times \{0\}) &\leftrightarrow A \text{ is a real number} \wedge (\exists a_1, \dots, a_n \in \mathbb{Q}) A^n - a_1 A^{n-1} - a_2 A^{n-2} - \dots - a_n \in L \end{aligned}$$

## 8 Complex Numbers

Weyl defines complex numbers as sets of octuples of natural numbers: roughly, a complex number is a set of the form  $A \times B$ , where  $A$  and  $B$  are real numbers. ( $\times$  here denotes Cartesian product, not the preliminary form of multiplication defined above.) As we have product types in our system, we can simply define:

**Definition 8.1 (Complex Number)** For  $Z : \mathbf{Set}[\mathbb{N}^4]^2$ , the proposition " $Z$  is a complex number" is the proposition

$$\pi_1(Z) \text{ is a real number} \wedge \pi_2(Z) \text{ is a real number} .$$

## 9 Sequences and the Convergence Principle

**Definition 9.1 (Positive and Negative Infinity)** We define  $+\infty$  to be

$$\{\langle m, n, p, q \rangle \mid p \neq q\}$$

and  $-\infty$  to be

$$\emptyset_{\mathbb{N}^4} .$$

**Lemma 9.2** For  $M : \mathbf{Set}[\mathbb{N}^4]$  a domain of rationals,  $M$  is an open cut iff  $M$  is either a real number,  $+\infty$  or  $-\infty$ .

**Definition 9.3 (Limit Inferior)** For  $t[n]$  a term of type  $\mathbf{Set}[\mathbb{N}^4]$  involving a free variable  $n : \mathbb{N}$ , the limit inferior  $\liminf_{n \rightarrow \infty} t[n]$  is defined to be

$$\{\langle m, n, p, q \rangle \mid p \neq q \wedge \exists a, b, c, d, k : \mathbb{N}. c \neq d \wedge \frac{m-n}{p-q} < \frac{a-b}{c-d} \wedge \forall l : \mathbb{N}. k < l \rightarrow \langle a, b, c, d \rangle \in t[l]\} .$$

**Lemma 9.4** If

$$\forall n : \mathbb{N}. t[n] \text{ is a real number}$$

then  $\liminf_{n \rightarrow \infty} t[n]$  is an open cut.

**Definition 9.5 (Convergent sequence)** For  $f : \mathbb{N} \rightarrow \mathbf{Set}[\mathbb{N}^4]$ , the proposition "f is a convergent sequence of real numbers" is the proposition

$$(\forall n : \mathbb{N}. f[n] \text{ is a real number}) \wedge$$

$$\forall a, b, c, d : \mathbb{N}. c \neq d \rightarrow 0^{*\dagger} < \frac{a-b}{c-d} \rightarrow \exists n : \mathbb{N}. \forall p, q : \mathbb{N}. n < p \rightarrow n < q \rightarrow -\frac{a-b}{c-d} \text{ belongs to } f[p] \ominus f[q] \wedge \frac{a-b}{c-d}$$

**Definition 9.6 (Convergence)** For  $f : \mathbb{N} \rightarrow \mathbf{Set}[\mathbb{N}^4]$  and  $C : \mathbf{Set}[\mathbb{N}^4]$ , the proposition "f is a sequence of real numbers that converges to C" is the proposition

$$(\forall n : \mathbb{N}. f[n] \text{ is a real number}) \wedge C \text{ is a real number} \wedge$$

$$\forall a, b, c, d : \mathbb{N}. c \neq d \rightarrow 0^{*\ddagger} < \frac{a-b}{c-d} \rightarrow \exists n : \mathbb{N}. \forall p : \mathbb{N}. n < p \rightarrow -\frac{a-b}{c-d} \text{ belongs to } f[p] \ominus C \wedge \frac{a-b}{c-d} \text{ does not belong to } C$$

**Theorem 9.7 (Cauchy's Convergence Principle)** For  $f : \mathbb{N} \rightarrow \mathbf{Set}[\mathbb{N}^4]$ , f is a convergent sequence of real numbers if and only if there exists  $C : \mathbf{Set}[\mathbb{N}^4]$  such that f is a sequence of real numbers that converges to C.

The C required in this theorem is  $\liminf_{n \rightarrow \infty} f(n)$ .

**Theorem 9.8** "Exactly one number belongs to the intersection of a sequence of nested intervals whose lengths pass below every positive number."

For  $f, g : \mathbb{N} \rightarrow \mathbf{Set}[\mathbb{N}^4]$ , if

$\forall n : \mathbb{N}. f(n)$  is a real number,

$\forall n : \mathbb{N}. g(n)$  is a real number,

$\forall n : \mathbb{N}. f(n) \ll f(s[n])$ ,

$\forall n : \mathbb{N}. g(s[n]) \ll g(n)$ ,

$\forall n : \mathbb{N}. f(n) \ll g(n), \forall a, b, c, d : \mathbb{N}. c \neq d \rightarrow \exists n : \mathbb{N}. g(n) \ominus f(n) \ll \frac{a-b^\dagger}{c-d}$

then there exists a unique  $C : \mathbf{Set}[\mathbb{N}^4]$  such that  $C$  is a real number and

$\forall n : \mathbb{N}. f(n) \ll C \ll g(n)$  .

**Theorem 9.9** "Given a monotone increasing sequence of real numbers whose members remain below a definite bound, there is a number to which the sequence converges."

For  $f : \mathbb{N} \rightarrow \mathbf{Set}[\mathbb{N}^4]$  and  $U : \mathbf{Set}[\mathbb{N}^4]$ , if

$\forall n : \mathbb{N}. f(n)$  is a real number,

$U$  is a real number,

$\forall n : \mathbb{N}. f(n) \ll f(s[n])$ ,

$\forall n : \mathbb{N}. f(n) \ll U$

then there exists  $L : \mathbf{Set}[\mathbb{N}^4]$  such that  $L$  is a real number and  $f$  is a sequence of real numbers that converges to  $L$ .

**Theorem 9.10 (Dedekind's Cut Principle)** If  $A$  and  $B$  are two domains of rationals such that every rational that belongs to  $A$  is smaller than every one belonging to  $B$ , and if, for every positive rational  $a$ , there exists a rational  $x$  belonging to  $A$  and a rational  $y$  belonging to  $B$  such that  $y - x \leq a$ , then there exists a unique real number  $C$  such that

$(\forall Q \text{ belonging to } A) \neg (C \ll Q^\ddagger)$

and

$(\forall Q \text{ belonging to } B) \neg (Q^\ddagger \ll C)$  .

Classically, the principle holds for sets of real numbers:

"For  $A, B : \mathbf{Set}[\mathbf{Set}[\mathbb{N}^4]]$ , if

$\forall X, Y : \mathbf{Set}[\mathbb{N}^4]. X$  is a real number  $\rightarrow Y$  is a real number  $\rightarrow X \in A \rightarrow Y \in B \rightarrow X \ll Y$

and if

$\forall a, b, c, d : \mathbb{N}. c \neq d \rightarrow 0^{*\dagger} < \frac{a-b}{c-d} \rightarrow \exists X, Y : \mathbf{Set}[\mathbb{N}^4]. X$  is a real number  $\wedge X \in A \wedge Y$  is a real number  $\wedge Y \in B$

then there exists a unique real number  $C$  such that

$$\forall X : \mathbf{Set}[\mathbb{N}^4]. X \text{ is a real number} \rightarrow X \in A \rightarrow \neg(C \ll X)$$

and

$$\forall Y : \mathbf{Set}[\mathbb{N}^4]. Y \text{ is a real number} \rightarrow Y \in B \rightarrow \neg(Y \ll C) ."$$

However (Weyl claims) this cannot be proven predicatively.

**Theorem 9.11** "Every bounded set of rationals has a unique least upper bound and a unique greatest lower bound."

For  $A$  a domain of rationals and  $Q, Q'$  rationals, if  $Q' < R < Q$  for every rational  $R$  that belongs to  $A$ , then there exists unique real numbers  $S, I$  such that

$$\forall Q \text{ belonging to } A. (Q^\ddagger \ll S \vee Q^\ddagger \approx S)$$

$$\forall Q \text{ belonging to } A. (I \ll Q^\ddagger \vee I \approx Q^\ddagger)$$

and, for any real numbers  $U, L$ :

- If

$$\forall Q \text{ belonging to } A. (Q^\ddagger \ll U \vee Q^\ddagger \approx U)$$

then  $S \ll U$  or  $S \approx U$ .

- If

$$\forall Q \text{ belonging to } A. (I \ll Q^\ddagger \vee I \approx Q^\ddagger)$$

then  $L \ll I$  or  $L \approx I$ .

Classically, this result holds for bounded sets of real numbers:

"Every bounded set of real numbers has a unique least upper bound and a unique greatest lower bound."

However, this result is not provable predicatively.

**Theorem 9.12** "Every bounded infinite set of rational numbers has an accumulation point."

For  $M$  a domain of rationals and  $Q, Q'$  rationals, if

$$\forall R \text{ belonging to } M. Q < M < Q'$$

and, for every  $f : \mathbb{N} \rightarrow \mathbf{Set}[\mathbb{N}^4]$ , if

$$\forall n : \mathbb{N}. f(n) \text{ is a rational belonging to } M$$

then

$$\exists m, n : \mathbb{N}. m \neq n \wedge f(m) \simeq f(n) ,$$

then there exists a unique real number  $C$  such that

$$\forall \text{rationals } \epsilon. 0^{*\dagger} < \epsilon \rightarrow (\exists R \text{ belonging to } M). C \ominus \epsilon^\ddagger \ll R^\ddagger \ll C \oplus \epsilon^\ddagger .$$

Classically, the result holds for sets of real numbers:  
 "Every bounded infinite set of real numbers has an accumulation point."  
 However, this result cannot be proven predicatively.

**Definition 9.13 (The Unit Interval)** For  $X : \mathbf{Set}[\mathbb{N}^4]$ , the proposition " $X$  is in the unit interval" is the proposition

$$X \text{ is a real number} \wedge (0^{*\dagger} \ll X \vee 0^{*\dagger} \approx X) \wedge (X \ll 1^{*\dagger} \vee 1^{*\dagger} \approx X) .$$

**Theorem 9.14 (Heine-Borel Theorem)** "Consider a sequence of intervals  $\Delta_n$ . Let every real number in the unit interval  $0 \leq x \leq 1$  lie in the interior of one of the intervals of this sequence. Then there is a natural number  $n$  such that every one of these real numbers already lies in the interior of one of the finitely many intervals  $\Delta_1, \Delta_2, \dots, \Delta_n$ ."

Let  $f, g : \mathbb{N} \rightarrow \mathbf{Set}[\mathbb{N}^4]$ . Suppose

$$\forall n : \mathbb{N}. f(n) \text{ is a real number}$$

$$\forall n : \mathbb{N}. g(n) \text{ is a real number}$$

$$\forall n : \mathbb{N}. f(n) \ll g(n) \forall X : \mathbf{Set}[\mathbb{N}^4]. X \text{ is in the unit interval} \rightarrow \exists n : \mathbb{N}. f(n) \ll X \ll g(n)$$

Then there exists  $n : \mathbb{N}$  such that

$$\forall X : \mathbf{Set}[\mathbb{N}^4]. X \text{ is in the unit interval} \rightarrow \exists k : \mathbb{N}. k < n \wedge f(k) \ll X \ll g(k)$$

**Proof** Suppose the conclusion were false. Let  $R$  be the domain of rationals such that

$$l \in R \leftrightarrow (\forall l' \leq l)(l' < 0^{*\dagger} \vee \exists n : \mathbb{N}. f(n) \ll l' \ll g(n))$$

(This can be written out formally as a term in  $\mathbf{Set}[\mathbb{N}^4]$ . Then  $R$  is an open cut to which all negative rational numbers, but not  $1^{*\dagger}$ , belong. Therefore,  $R$  is a real number in the unit interval. Hence, by hypothesis, there exists  $n$  such that  $f(n) < R < g(n)$ . From this, a contradiction can be generated. **QED**

Classically, the Heine-Borel Theorem holds in the following form:

"Let  $A$  be a set of intervals such that every real number of the unit interval belongs to the interior of some member of  $A$ . Then there exist finitely many members  $\Delta_1, \dots, \Delta_n \in A$  such that every real number in the unit interval belongs to the interior of one of  $\Delta_1, \dots, \Delta_n$ ."

However, this cannot be proven predicatively.

## 9.1 Infinite Series

**Definition 9.15 (Sequence of Partial Sums (LE))** Let  $t[i]$  be a term of type  $\mathbf{Set}[\mathbb{N}^4]$  involving a free variable  $i : \mathbb{N}$ . For  $n : \mathbb{N}$ , we define  $\sum_{i=0}^n t[i]$  to be

$$E_{\mathbb{N}}[[x]\mathbf{Set}[\mathbb{N}^4], t[0], [n, X]X \oplus t[s[n]]] : \mathbf{Set}[\mathbb{N}^4] .$$

**Definition 9.16** For  $t[i]$  a term of type  $\mathbf{Set}[\mathbb{N}^4]$  involving a free variable  $i : \mathbb{N}$ , define  $\sum_{i=0}^{\infty} t[i]$  to be

$$\lim_{n \rightarrow \infty} \inf \sum_{i=0}^n t[i] .$$

## 10 Continuous Functions

**Definition 10.1** For  $X, Q : \mathbf{Set}[\mathbb{N}^4]$ , the proposition  $|X| \leq Q$  is defined to be

$X$  is a real number  $\wedge Q$  is a rational  $\wedge Q$  does not belong to  $X \wedge \forall m, n, p, q : \mathbb{N}. p \neq q \rightarrow \frac{m-n}{p-q} < Q \rightarrow \langle m, n, \dots \rangle$

**Definition 10.2 (Real Function)** For  $f : \mathbf{Set}[\mathbb{N}^4] \rightarrow \mathbf{Set}[\mathbb{N}^4]$ , the large proposition "f is a real function" is defined to be

$$\forall X : \mathbf{Set}[\mathbb{N}^4]. X \text{ is a real number} \rightarrow f(X) \text{ is a real number} .$$

**Definition 10.3 (Continuous)** For  $f : \mathbf{Set}[\mathbb{N}^4] \rightarrow \mathbf{Set}[\mathbb{N}^4]$ , and  $A : \mathbf{Set}[\mathbb{N}^4]$ , the large proposition "f is a function on the unit interval continuous at A" is defined to be

For every positive rational  $Q$ , there exists a positive rational  $R$  such that, whenever  $X$  is in the unit interval and  $|X \ominus A| \leq R$ , then  $|f(X) \ominus f(A)| \leq Q$ .

For  $f : \mathbf{Set}[\mathbb{N}^4]$ , the large proposition "f is continuous on the unit interval" is defined to be

For every real  $A$ , if  $A$  is in the unit interval then  $f$  is continuous at  $A$ .

For  $f : \mathbf{Set}[\mathbb{N}^4]$ , the large proposition "f is uniformly continuous on the unit interval" is defined to be

For every positive rational  $Q$ , there exists a positive rational  $R$  such that, whenever  $X$  and  $Y$  are in the unit interval and  $|X \ominus Y| \leq R$ , then

$$|f(X) \ominus f(Y)| \ll Q .$$

**Theorem 10.4 (Intermediate Value Theorem)** Let  $f : \mathbf{Set}[\mathbb{N}^4] \rightarrow \mathbf{Set}[\mathbb{N}^4]$  and  $A, B, V : \mathbf{Set}[\mathbb{N}^4]$ . Suppose  $f$  is continuous on the unit interval,  $A, B$  and  $V$  are real numbers,

$$0^{*\dagger\dagger} \ll A, B \ll 1^{*\dagger\dagger}$$

and

$$f(A) \ll V \ll f(B)$$

Then there exists a real number  $C$  such that  $A \ll C \ll B$  and  $f(C) \approx V$ .

**Proof** Let  $C$  be the domain of rationals such that  $L$  belongs to  $C$  if and only if

There exists a rational  $L'$  such that  $L < L'$  and  $f(L'^{\ddagger}) < V$ .

Then  $C$  is a real number and in the unit interval. From the fact that  $f$  is continuous at  $C$ , we can rule out the possibilities  $f(C) \ll V$  and  $V \ll f(C)$ ; hence  $f(C) \approx V$ . **QED**

This theorem can be extended to functions of more than one argument.

**Theorem 10.5** "A continuous function on a closed interval is bounded, and attains its bounds."

Let  $f : \mathbf{Set}[\mathbb{N}^4] \rightarrow \mathbf{Set}[\mathbb{N}^4]$ . If  $f$  is continuous on the unit interval, then there exist real numbers  $A$  and  $B$  in the unit interval such that, for all  $X$  in the unit interval,

$$(f(A) \ll f(X) \vee f(A) \approx f(X)) \wedge (f(X) \ll f(B) \wedge f(X) \approx f(B)) .$$

**Proof** Define  $M$ , the least upper bound of the range of  $f$ , to be the domain of rationals to which  $m$  belongs if and only if there exists a rational  $l$  in the unit interval such that  $m < f(l^{\ddagger})$ .

For  $X : \mathbf{Set}[\mathbb{N}^4]$ , let  $M(X)$  be the domain of rationals to which  $m$  belongs if and only if there exists a non-negative rational  $l$  that belongs to  $X$  such that  $m < f(l^{\ddagger})$ . Then, for  $X \in (0, 1]$ ,  $M(X)$  is the least upper bound of  $f[(0, 1]]$ .

There are two cases:

**Case One** For every positive rational  $l \leq 1^{*\ddagger}$ , we have

$$M(l^{\ddagger}) \approx M$$

In this case, we may take  $B$  to be  $0^{*\ddagger}$ .

**Case Two** There exists a positive rational  $l \leq 1^{*\ddagger}$  such that

$$M(l^{\ddagger}) \approx M$$

In this case, define  $B$  to be the domain of rationals to which  $l$  belongs iff there exists a rational  $l'$  such that  $l < l' \leq 1$  and  $M(l'^{\ddagger}) \ll M$ . Then  $B$  is a real number.

In either case, from the continuity of  $f$  at  $B$ , it cannot be that  $f(B) \ll M$ , so it must be that  $f(B) \approx M$ . This also shows that  $M$  is a real number (and not  $+\infty$ ).

$A$  can be found similarly. **QED**

**Theorem 10.6** For  $f : \mathbf{Set}[\mathbb{N}^4] \rightarrow \mathbf{Set}[\mathbb{N}^4]$ , if  $f$  is continuous on the unit interval, then  $f$  is uniformly continuous on the unit interval.

**Proof** See Weyl, pp. 83–85. No details need changing. **QED**

Weyl also mentions the following:

- The Fundamental Theorem of Algebra can be proven predicatively.
- We cannot prove predicatively that every injective function has an inverse. However, it still holds that every continuous, monotone function  $f$  has an inverse. The value of  $f^{-1}(Y)$  is defined to be the domain of rationals  $q$  such that

$$q < 0 \vee (q < 1 \wedge f(q) < Y)$$

(This is the case where  $f$  is a function on the unit interval.)