5. NATURAL NUMBERS

§5.1. The Peano Axioms

We begin by defining the natural numbers:

0, 1, 2, 3, 4, ...

If you can think back far enough to when you first learnt to count you won't remember ever having been given a formal definition of number. Moreover many of the basic properties of these numbers will have been 'proved' by assertion, or at best by observing them in a few examples.

It's possible to set up axioms for the natural numbers independently of the axioms of set theory, using the so-called Peano Axioms, but here we're taking the view that every object in mathematics is a set, so we'll define the set of natural numbers using set-theoretical constructions, and then we'll define a natural number to be any element of that set. We'll then be able to *prove* the Peano axioms rather than assume them.

DEFINITION OF NATURAL NUMBERS

$0 = \varnothing$, the empty set;

$1 = 0^+ = 0 \cup \{0\} = \{0\}$,

$2 = 1^+ = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$,

$3 = 2^+ = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$,

……………………………………………..

$n = \{0, 1, 2, …, n - 1\}$.

……………………………………………..

NOTE:

(1) Every one of the above can be justified as being a set by the ZF axioms.

(2) The natural number *n* is defined as a set with *n* elements.

(3) Each of these is a complicated construction using just the empty set as building blocks.

So, for example, $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

Thank goodness we don't have to write the date in terms of the empty set!

But can we be sure that n^+ is always a set? Just because we write something to look like a set doesn't mean that it *is* a set. After all $\{x \mid x \notin x\}$ looks like it should be a set, but it isn't. Let's settle this question now.

Theorem 1: If S is a set then so is S^+.

Proof: Suppose S is a set.

Then {S} = {S, S} is a set by the Axiom of Pairing.

Hence {S, {S}} is a set, also by the Axiom of Pairing.

Hence $\cup\{S, \{S\}\} = S \cup \{S\}$ is a set by the Axiom of Unions. ✋☺

Now we defined

$$S^* = \cap\{x \mid (S \in x) \wedge (y \in x \to y^+ \in x)\}.$$

But is it a set? We will prove later that if S is a set then S* is a set. We only need 0* to be a set and this is what the Axiom of Infinity asserts. We write 0* as ℕ and we call it the set of **natural numbers**. So ℕ = {0, 1, 2, ... } and it is a set.

Now we prove the Peano axioms. Of course this means that they are no longer axioms.

Theorem 2 (Peano Axioms):

(P1) $0 \in \mathbb{N}$.

(P2) $\forall n[n \in \mathbb{N} \to n^+ \in \mathbb{N}]$.

(P3) $\forall n[n^+ \neq 0]$.

(P4) $\forall m \forall n[m^+ = n^+ \to m = n]$.

(P5) If $S \subseteq \mathbb{N}$ and $0 \in S$ and $n^+ \in S$ for all $n \in S$, then $S = \mathbb{N}$.

Proof: (P1) and (P2) follow from the fact that $\mathbb{N} = 0^*$.

(P3) Let $n \in \mathbb{N}$ and suppose $n^+ = 0$. Then $n \cup \{n\} = 0$, and so $n \in 0$, a contradiction.

(P4) We shall postpone the proof of (P4).

(P5) Suppose that $S \subseteq \mathbb{N}$, $0 \in S$ and $n \in S$ implies that $n^+ \in S$.

Let $T = \{x \mid 0 \in x \wedge \forall y[y \in x \to n^+ \in x]\}$.

Then $S \in T$ and so $\mathbb{N} = \cap T \subseteq S$. Hence $S = \mathbb{N}$. ✋☺

NOTE: (P5) is the foundation for the Principal of Induction.

When we have defined addition we'll see that:

$$n^+ = n + 1,$$

and so these five 'axioms' will look more familiar if we write them in such terms:

(P1) 0 is a natural number.
(P2) For all n, $n + 1$ is a natural number.
(P3) $n + 1$ is never zero.
(P4) If $m + 1 = n + 1$ then $m = n$.
(P5) If $0 \in S \subseteq \mathbb{N}$, and $n + 1 \in S$ whenever $n \in S$,

then $S = \mathbb{N}$.

If you say that these are obvious, you're relying too much on your intuition. Of course that's not such a bad thing, but in keeping with the spirit of Axiomatic Set Theory, everything has to either be assumed as an axiom, or proved from the axioms. Just to say "it's obvious" is not good enough. Even to say, as a proof of (P4) "just subtract 1 from both sides" requires subtraction to be defined.

Theorem 3 (Principle of Induction):
If P is a predicate and both P0 and $\forall n \in \mathbb{N}[Pn \rightarrow Pn^+]$. Then $\forall n \in \mathbb{N}[Pn]$.
Proof: Suppose $P0 \wedge \forall n \in \mathbb{N}[Pn \rightarrow Pn^+]$.
Let $S = \{n \in \mathbb{N} \mid Pn\}$. Then $0 \in S$ and

$$\forall n \in \mathbb{N}[Pn \rightarrow Pn^+]$$

By (P5) $S = \mathbb{N}$, that is $\forall n \in \mathbb{N}[Pn]$. ✋☺

Sets that are elements of themselves seem counter-intuitive yet nothing in the ZF axioms rules out the possibility of $x \in x$ occurring. Indeed, as we'll see later, it *is* possible to have a ZF model in which this can occur. But if $x \in x$ then $x^+ = x \cup \{x\} = x$. This had better not happen with any natural number because, if so, our counting would get stuck at some point.

For example, suppose that $0 \notin 0$ (pretty obvious since the empty set has no elements) and suppose that
$1 \notin 1$and $2 \notin 2$ and $3 \notin 3$ but $4 \in 4$. Then we'd have to count as follows: 0, 1, 2, 3, 4, 4, 4, 4, …..

There's a story (though anthropologists deny that it's true) that a certain tribe of aborigines counted 1, 2, 3, many. This is what the above situation would lead to. We had better show that n^+ is never the same as n, or in other words that $n \notin n$ for any natural number n.

Theorem 4: No natural number is a subset of any of its elements.
Proof: Let S be the set of natural numbers that are not a subset of any of their elements. Clearly $0 \in$ S.
Suppose $n \in$ S. Suppose $n^+ \subseteq m \in n^+$.
If $m \in n$, $n \subseteq n^+ \subseteq m \in n$, a contradiction.
If $m = n$ then $n^+ \in n$ so $n \in n$ and hence $n \subseteq n \in n$, a contradiction. ✋☺
Corollary: No natural number is an element of itself.

So, $x \in x$ can't happen for natural numbers. But what's to stop it happening for other sets? The answer is "nothing". It all depends on what flavour of Set Theory you want to build!

We define a set to be **transitive** if $\cup S \subseteq S$. Clearly 0 is transitive, since $\cup 0 = 0$. Since $1 = \{0\}$, $\cup 1 = 0$ and so 1 is transitive. Since $2 = 1^+ = \{0\} \cup \{1\} = \{0, 1\}$, $\cup 2 = \{0\} = 1 = \{0\} \subseteq 2$. Hence 2 is transitive.

Theorem 5: All natural numbers are transitive.
Proof: 0 is transitive since $\cup 0 = 0$.
Suppose n is transitive.
Then $\cup n \subseteq n$. Now $n^+ = n \cup \{n\}$ so

$$\cup n^+ = \cup n \cup n \subseteq n \subseteq n^+.$$

Hence n^+ is transitive. By induction all natural numbers are transitive. ✋☺

Theorem 6 (P4): If $m^+ = n^+$ then $m = n$.
Proof: If $m^+ = n^+$ and $m \neq n$ then $m \in n$ and $n \in m$ and so $m \in \cup m \subseteq m$, whence $m \in m$, contradicting the Corollary to Theorem 4. Hence $m = n$. ✋☺

§5.2. The Ordering of the Natural Numbers

To construct a working model of the natural numbers within set theory we need to define the arithmetic operations. But before we do that we'll define the ordering of the natural numbers. We define $m < n$ to simply mean that $m \in n$. This is consistent with the ordering we've grown up with. For example $2 < 4$ because $4 = \{0, 1, 2, 3\}$ and so $2 \in 4$. We must now show that this ordering has the familiar properties.

Theorem 7 (Transitive Law):
If $m < n$ and $n < r$ then $m < r$.
Proof: Suppose $m \in n$ and $n \in r$. Then $m \in \cup r \subseteq r$ and so $m \in r$. ✋☺

What is a little harder to show is that any two natural numbers are comparable. That is, given any two natural numbers m, n either $m = n$ or $m < n$ or $m > n$ (by which we mean that $n < m$). According to our definition of 'less than' this means that given any two natural numbers m, n either $m = n$ or $m \in n$ or $n \in m$.

This property doesn't hold for sets in general. For example if $S = \{1, 2\}$ and $T = \{2, 3\}$ none of the relationships $S = T$, $S \in T$ and $T \in S$ hold.

We say that natural numbers m, n are **comparable** if $m \in n$, $m = n$ or $n \in m$. Comparability is clearly an equivalence relation.

Theorem 8: Any two natural numbers are comparable.
Proof: Let $C(n) = \{m \in \mathbb{N} \mid m \text{ is comparable with } n\}$.
$C(0) = \mathbb{N}$: Just use induction on the set $\{n \in \mathbb{N} \mid n \in C(0)\}$. Clearly $0 \in C(0)$.

Suppose $n \in C(0)$. Then $n \in 0$ or $n = 0$ or $0 \in n$.
The first of these alternatives is a contradiction.
Each of the remaining two possibilities implies that
$0 \in n^+$ so $n^+ \in C(0)$.

If $\mathbf{C}(n) = \mathbb{N}$ then $\mathbf{C}(n^+) = \mathbb{N}$:
Suppose $C(\mathbb{N}) = \mathbb{N}$. We show by induction that for all natural numbers m, $m \in C(n^+)$.
$0 \in C(n^+)$ since $n^+ \in C(0)$. Suppose $m \in C(n^+)$.
Then $m \in n^+$ or $m = n^+$ or $n^+ \in m$.
Case 1 $m \in n^+$: Then $m = n$ or $m \in n$.
Case 1A $m = n$: Then $m^+ = n^+$.
Case 1B $m \in n$:
Since $C(n) = \mathbb{N}$, m^+ is comparable with n.
Case 1B(i) $n \in m^+$:
Then $n \in m$ or $n = m$, both contradicting $m \in n$.
Case 1B(ii) $n = m^+$ or $m^+ \in n$: Then $m^+ \in n^+$.
Case 2 $m = n^+$ or $n^+ \in m$: Then $n^+ \in m^+$.
Hence m^+ is comparable with n^+ and so $C(n^+) = \mathbb{N}$.
By induction $C(n) = \mathbb{N}$ for all natural numbers n. ✋☺

Theorem 9: $m \in n$ if and only if $m \subset n$.
Proof: Suppose $m \in n$.
If $x \in m$ then $x \in \cup n \subseteq n$. Hence $m \subseteq n$.
But $m \neq n$ by the corollary to Theorem 4. Hence $m \subset n$.

Conversely suppose that $m \subset n$.

By Theorem 6, $m \in n$ or $n \in m$ ($m = n$ is ruled out by the fact that m is a *proper* subset). If $n \in m$ then $n \in n$, contradicting the corollary to Theorem 3. Hence $m \in n$. 🖐☺

Theorem 10: S^* is a set for all sets S.
Proof: I'll just give an outline of the proof. The details of the two inductions are left as exercises.
(1) We prove by induction on n that there exists a function F_n with domain n^+ such that for all $m \le n$, $F_n(m^+) = F_n(m)^+$ and $F_n(0) = S$.
(2) We prove by induction on n that if $m < n$ then for all $x \le m$, $F_m(x) = F_n(x)$.
(3) Define the generalized relation F by $xFy \leftrightarrow y = F_n(x)$ for some n.
(4) By (2) F is a generalized function.
(5) $\mathbb{N}$ is a set so, by the Axiom of Substitution, $S^* = F[\mathbb{N}]$ is a set. 🖐☺

§5.3. The Arithmetic of the Natural Numbers

It's heavy going proving rigorously what seems so obvious intuitively. We haven't even got to the stage of proving that 2 + 2 = 4. We now define addition of natural numbers. If you think this is unnecessarily complicated, ask yourself how you would go about defining addition, without resorting to such vague notions of taking heaps of things and combining them.

We shall define addition inductively. The next theorem justifies this approach.

Theorem 11 (Definition by Induction): If X is a set and $a \in X$ and $F:X \to X$ is a function then there exists a unique function $u: \mathbb{N} \to X$ such that:

(1) $u(0) = a$;

(2) $u(n^+) = F(u(n))$ for all $n \in \mathbb{N}$.

Proof: Let $C = \{A \subseteq \mathbb{N} \times X \mid (0, a) \in A \wedge (n^+, F(x)) \in A$ whenever $(n, x) \in A\}$.

Since $\omega \times X \in C$, $C \neq 0$. Let $U = \cap C$.

Then $U \in C$ and so U is the smallest element of C.

We prove that U is a function.

Let $S = \{n \in \mathbb{N} \mid (n, x) \in U$ and (n, y) implies that $x = y\}$.

$0 \in S$: If not then $(0, b) \in U$ for some $b \neq a$.

Then $u - \{(0, b)\} \in S$, contradicting the fact that U is the smallest element of C.

$n \in S \to n^+ \in S$: Suppose $n \in S$ and $n^+ \notin S$.

Since $n \in S$ there exists a unique x with $(n, x) \in U$.

Hence $(n^+, F(x)) \in U$.

Since $n^+ \notin S$ there exists y such that $(n^+, y) \in U$ for some $y \neq F(x)$.

Then $U - \{(n^+, y)\} \in U$, contradicting the fact that U is the smallest element of C.

Uniqueness follows from the fact that U is the smallest element of C. ✋☺

We now define the basic arithmetic operations for the natural numbers inductively.

Addition

(A0) $x + 0 = x$

(A1) $x + y^+ = (x + y)^+$

Multiplication

(M0) $x0 = 0$

(M1) $xy^+ = xy + x$

Exponentiation

(E0) $x^0 = 1$

(E1) $x^{y^+} = x^y\, x$

Theorem 12: $0 + x = x$ for all natural numbers x.
Proof: We prove this by induction on x.
$0 + 0 = 0$ by (A0).
Suppose that $0 + x = x$.
Then $0 + x^+ = (0 + x)^+$ by (A1)
$= x^+$ by the induction hypothesis. ✋☺

Theorem 13: $x + y^+ = x^+ + y$ for all natural numbers x, y.
Proof: Induction on y.
$x + 0^+ = (x + 0)^+$ by (A1)
$= x^+$ by (A0)
$= x^+ + 0$ by (A0).
Suppose that $x + y^+ = x^+ + y$.
Then $x + y^{++} = (x + y^+)^+$ by (A1)
$= (x^+ + y)^+$ by the induction hypothesis
$= x^+ + y^+$ by (A1). ✋☺

Theorem 14: $x + y = y + x$ for all natural numbers x, y.
Proof: Induction on y.
$x + 0 = 0$ by (A0)
$= 0 + x$ by Theorem 10.
Suppose that $x + y = y + x$.
Then $x + y^+ = (x + y)^+$ by (A1)
$= (y + x)^+$ by the induction hypothesis
$= y + x^+$ by (A1)
$= y^+ + x$ by Theorem 11. ✋☺

Theorem 15: If $x + u = x + v$ then $u = v$.
Proof: We prove this by induction on x.
Suppose $x = 0$. The result follows from Theorem 12.
Now suppose that it is true for x and suppose that

$$x^+ + u = x^+ + v.$$

Then $x + u^+ = x + v^+$ by Theorem 13.
Hence $u^+ = v^+$ by the induction hypothesis.
Finally, this implies that $u = v$ by the Peano Axiom 4 (Theorem 6). Hence it's true for x^+ and so, by induction, it is true for all x. ✋☺

Theorem 16: If $x \leq y$ then there is a unique z such that $x + z = y$.
Proof: The uniqueness was proved in Theorem 15.
We now prove the existence of z by induction on y.
If $y = 0$ then $0 + 0 = 0$ proves that it is true in this case.
Suppose it is true for y and suppose that $x \leq y^+$.
Thus $x \subseteq y^+ = y \cup \{y\}$.
Hence $x = y$ or $x \subseteq y$.

Case 1: $x = y$. Then take $z = 1$.
$x + 1 = x^+ = y^+$ and so it is true for y^+.
Case 2: $x \subseteq y$. This is the same as $x \leq y$ and by our induction hypothesis there exists z such that $x + z = y$.
Then $x + z^+ = (x + z)^+ = y^+$ and so it is true for y^+.
So, by induction it is true for all y. ✋☺

We define the unique z as the difference between x and y and denote it by $y - x$. We call the process **subtraction**.

Theorem 17: For all natural numbers x, y, z the following hold:

- $(x + y) + z = x + (y + z)$.
- $x(y + z) = xy + xz$.
- $0x = 0$
- $y^+x = yx + x$
- $xy = yx$
- $1x = x$
- $(xy)^z = x^z y^z$
- $x^y x^z = x^{y+z}$
- $(x^y)^z = x^{yz}$
- If $x + y = 0$ then $x = y = 0$
- If $xy = 0$ then $x = 0$ or $y = 0$
- $x \leq y$ if and only if $y = x + z$ for some z.
- $0 \leq x$.
- If $xz = yz$ and $z \neq 0$ then $x = y$.
- If $x \leq y$ then $x + z \leq y + z$ and $xz \leq yz$.

- If $x \leq y$ and $y \leq z$ then $x \leq z$.
- If $x \leq y$ and $y \leq x$ then $x = y$.

Proof: The proofs are left as exercises. They are all proved by induction, and the list is carefully ordered so that results that are needed in any induction precede it in the list.

There's a lot more that can be proved about the arithmetic of natural numbers, but it's all pretty well plain sailing now, so we'll now turn our attention to extending our number system to rational numbers, real numbers and complex numbers.