

1. THE NATURAL NUMBERS AND ARITHMETIC.

Theorem 1.1. Suppose, for each $i = 1, 2$, X_i is a nonempty set, $<_i$ well orders X_i , X_i has no $<_i$ -limit point and no $<_i$ -greatest element.

Then there is one and only one $f : X_1 \rightarrow X_2$ such that

$$x, y \in X_1 \text{ and } x <_1 y \Rightarrow f(x) <_2 f(y)$$

and $\text{rng } f = X_2$.

Proof. We give a sketch and leave the details to the reader.

By virtue of the preceding theory of well ordered sets exactly one of the following holds:

- (i) There is an order preserving map $f : X_1 \rightarrow X_2$ such that $\text{rng } f = X_2$.
- (ii) There is an order preserving map $f : X_1 \rightarrow X_2$ such that $\text{rng } f$ is an initial segment of X_2 not equal X_2 ;
- (iii) There is an order preserving map $f : X_2 \rightarrow X_1$ such that $\text{rng } f = X_1$ is an initial segment of X_1 not equal X_1 .

Exclude (ii) and (iii). □

1.1. The Peano postulates. Axiom. There is a nonempty well ordered set

$$\mathbb{N}$$

with no limit points and no greatest element.

We let

$$<, 0, S$$

be the well ordering on \mathbb{N} ; least element of \mathbb{N} ; and the successor function of \mathbb{N} , respectively. We let

$$\mathbb{N}^+ = \{n \in \mathbb{N} : n > 0\}.$$

The members of \mathbb{N} are called **natural numbers**. We let $1 = S(0), 2 = S(1), 3 = S(2)$, etc. (But what exactly does “etc.” mean here?) By virtue of the previous Theorem we are assured that there is, up to the natural notion of isomorphism, one such well ordered set.

Remark 1.1. Alternatively, we could have said that is a nonempty well ordered set \mathbb{N} with the property that the domain of the successor function is \mathbb{N} and that the range of the successor function is $\mathbb{N} \sim \{0\}$.

Theorem 1.2. Principle of induction. Suppose A is a subset of \mathbb{N} such that $0 \in A$ and

$$n \in A \Rightarrow S(n) \in A.$$

Then $A = \mathbb{N}$.

Proof. (Compare with the principle of transfinite induction.) Were it the case that $\mathbb{N} \sim A \neq \emptyset$, its least element, being nonzero, would be the successor of an element of A . This contradicts the hypothesis that the successor of an element of A is a member of A . □

Theorem 1.3. Defining a function by induction. Suppose

- (i) Y is a set;
- (ii) $\mathcal{G} = \{g : \text{for some } n, n \in \mathbb{N} \text{ and } g : \mathbb{I}(n) \rightarrow Y\}$;
- (iii) $G : \mathcal{G} \rightarrow Y$.

Then there is one and only one f such

$$f : \mathbb{N} \rightarrow Y$$

and such that

$$f(n) = G(f|I(n)) \quad \text{for each } n \text{ in } \mathbb{N}.$$

Proof. This is a special case of defining a function by transfinite induction. \square

Definition 1.1. A fundamental definition. Suppose X is a set.

X is **finite** if $X \approx I(n)$ for some $n \in \mathbb{N}$;

X is **countable** if X is finite or $X \approx \mathbb{N}$;

X is **infinite** if X is not finite;

X is **uncountable** if X is not countable.

2. BASIC THEORY OF FINITE SETS INCLUDING ARITHMETIC.

The following Theorem is basic to counting.

Theorem 2.1. Suppose m and n are natural numbers and $I(m) \approx I(n)$. Then $m=n$.

Proof. We prove this by induction. Let A be the set of natural numbers n such that if m is a natural number and $I(m) \approx I(n)$ then $m=n$.

It is evident that $0 \in A$.

Suppose $n \in A$. We will show that $S(n) \in A$. The present theorem will then follow by induction.

So suppose that m is a natural number and $I(S(n)) \approx I(m)$. Then, for some f ,

$$f : I(S(n)) \rightarrow I(m),$$

f is univalent and the range of f equals $I(m)$. Observe that $m \neq 0$ so $m = S(l)$ for some natural number l .

Suppose $f(n) = l$. Then $f|I(n)$ is univalent, has domain $I(n)$ and has range $I(l)$. Since $n \in A$ it follows that $n = l$ so $S(n) = m$.

If, on the other hand, $f(n) \neq l$ we define

$$g : I(n) \rightarrow I(l)$$

as follows. Let k be such that $f(k) = l$; note that $k \in I(n)$. We let

$$g = \{(k, f(n))\} \cup \{(j, f(j)) : j \in I(n) \sim \{k\}\}.$$

One verifies that g is univalent and has range $I(l)$. Since $n \in A$ we infer that $n = l$ so $S(n) = m$. \square

Definition 2.1. By virtue of the previous Theorem, for a finite set A we may set

$$|A| = n$$

where n is that natural number such that $A \approx I(n)$.

Theorem 2.2. Suppose $A \subset B$ and B is finite. Then $|A| \leq |B|$ with equality only if $A = B$.

Proof. Induct on $|B|$ using an argument similar to that used in the proof of the previous theorem. \square

Theorem 2.3. Suppose A and B are finite sets. Then $A \cup B$ is finite.

Proof. Induct on $|B|$ using the fact that if $b \in B$ then $A \cup B = (A \cup (B \sim \{b\})) \cup \{b\}$. \square

Theorem 2.4. Suppose A and B are finite sets. Then $A \times B$ is finite.

Proof. Induct on $|B|$ using the previous theorem in conjunction with the fact that if $b \in B$ then $A \times B = (A \times (B \sim \{b\})) \cup (A \times \{b\})$. \square

Theorem 2.5. Suppose $n \in \mathbb{N}$, $f : \mathbb{I}(n) \rightarrow A$, and $\text{rng } f = A$. Then A is finite.

Proof. Let B be the set of those m in $\mathbb{I}(n)$ which, for some a in A , are the least members of $f^{-1}[\{a\}]$. Then $f|_B$ is univalent and has range A . Thus $A \approx B$ and is therefore finite because $B \subset \mathbb{I}(n)$. \square

Definition 2.2. Definition of addition and subtraction. Suppose $m, n \in \mathbb{N}$. Let

$$m + n = |(\{0\} \times \mathbb{I}(m)) \cup (\{1\} \times \mathbb{I}(n))|$$

and let

$$mn = |\mathbb{I}(m) \times \mathbb{I}(n)|.$$

We call these binary operations on \mathbb{N} **addition** and **multiplication**, respectively.

Theorem 2.6. Addition and multiplication are associative and commutative.

Proof. This follows directly from the facts that $\{0\} \times A \cup (\{1\} \times B \approx \{0\} \times B) \cup (\{1\} \times A$ and $A \times (B \times C) \approx (A \times B) \times C$ whenever A, B, C are sets. \square

Now all you have to do is remember your number facts and you'll be promoted to the third grade!

The following three Theorems follow directly from the definitions.

Theorem 2.7. $n + 0 = n$ for $n \in \mathbb{N}$.

Theorem 2.8. $S(n) = n + 1$ for $n \in \mathbb{N}$.

Theorem 2.9. Suppose $m, n \in \mathbb{N}$. Then

$$mn = 0 \Leftrightarrow 0 \in \{m, n\}.$$

Theorem 2.10. Suppose m and n are natural numbers. Then

$$m < n \Leftrightarrow m + p = n \text{ for some positive natural number } p.$$

Proof. Suppose $m < n$. Then $P = \{l \in \mathbb{N} : m \leq l < n\}$ is finite and nonempty so $p = |P| > 0$. Now

$$(\{0\} \times \mathbb{I}(m)) \cup (\{1\} \times \mathbb{I}(p)) \approx \mathbb{I}(m) \cup P = \mathbb{I}(n).$$

Thus $m + p = n$.

On the other hand, suppose $m + p = n$ for some $p > 0$. Then

$$A = \{0\} \times \mathbb{I}(m) \subset (\{0\} \times \mathbb{I}(m)) \cup (\{1\} \times \mathbb{I}(p)) = B$$

so $m = |A| \leq |B| = m + p = n$. Since $B \sim A$ is nonempty as $p > 0$, we infer from Theorem 2.2 that $m \neq n$. Thus $m < n$. \square

Theorem 2.11. Suppose m, n and p are natural numbers. Then

$$m + n = m + p \Rightarrow n = p.$$

Proof. Were it the case that $n < p$, we would have $n + q = p$ for some $q > 0$ so that

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

Similarly, one excludes $n > p$. \square

Theorem 2.12. Suppose m, n and p are natural numbers and $p > 0$. Then

$$mn = mp \Rightarrow n = p.$$

Proof. Were it the case that $n < p$, we would have $n + q = p$ for some $q > 0$ so that

$$mn = m(p + q) = mp + mq < mp$$

because $mq > 0$. Similarly, one excludes $n > p$. \square

Theorem 2.13. The division algorithm. Suppose $a \in \mathbb{N}$ and $b \in \mathbb{N} \sim \{0\}$. There is a unique member (q, r) of $\mathbb{N} \times \mathbb{N}$ such that

$$a = qb + r \quad \text{and} \quad r < b.$$

Proof. For existence we induct on a . Indeed, if $a, q, r \in \mathbb{N}$ and $a = qb + r$ and $r < b$ then $r + 1 \leq b$ so

$$a + 1 = \begin{cases} qb + (r + 1) & \text{if } r + 1 < b, \\ (q + 1)b & \text{if } r + 1 = b. \end{cases}$$

For uniqueness, suppose $q_i, r_i \in \mathbb{N}$ and $r_i < b$, $i = 1, 2$ and $q_1b + r_1 = q_2b + r_2$. If $q_1 = q_2$ then $r_1 = r_2$ by cancellation. If $q_1 < q_2$ then $q_2 = q_1 + s$ for some member s of $\mathbb{N} \sim \{0\}$ so $sb + r_1 = r_2$ by cancellation; this is impossible since that would imply $r_2 = sb + r_1 \geq sb \geq b$. One treats the case $q_2 < q_1$ similarly. \square

Definition 2.3. For $m, n \in \mathbb{N}$ let

$$m^n = \left| \mathbb{I}(m)^{\mathbb{I}(n)} \right|.$$

Exercise 2.1. Define $\mathbf{e}, \mathbf{o} : \mathbb{N} \rightarrow \mathbb{N}$ by setting

$$\mathbf{e}(n) = 2n, \quad \mathbf{o}(n) = 2n + 1, \quad n \in \mathbb{N}.$$

Show that \mathbf{e} and \mathbf{o} are univalent and that \mathbb{N} is the disjoint union of their ranges.

Show that

$$\mathbb{N} \times \mathbb{N} \ni (m, n) \mapsto 2^m \mathbf{o}(n) \in \mathbb{N}$$

is univalent with range $\mathbb{N} \sim \{0\}$.

Use the foregoing to show that there is no natural number whose square is 2.