6 The Inductive Nature of Arithmetic

Recall that we introduced a new, compact notation for expressing a common class of first-order sentences. We will now generalize this notation to any finite number of variables that are *all quantified the same way*.

Definition 6.1: Restricted Quantifier Notation.
Given a set X and a positive integer n, we make the following definitions.[1]

$$(\forall x_1, ..., x_n \in X)(\varphi(x)) \;:\Leftrightarrow\; \forall x_1 ... \forall x_n \big((x_1 \in X \wedge ... \wedge x_n \in X) \;\Rightarrow\; \varphi(x) \big)$$
$$(\exists x_1, ..., x_n \in X)(\varphi(x)) \;:\Leftrightarrow\; \exists x_1 ... \exists x_n \big((x_1 \in X \wedge ... \wedge x_n \in X) \wedge \varphi(x) \big)$$

[1] We are using the phrase "positive integer" here in an *intuitive* way to denote the number of variables being quantified. The numbers appearing in subscripts—such as x_1 and x_2—are just ways of distinguishing variables from each other.

6.1 The Least Element Principle

Definition 6.2: Order on $\mathbb{N}$.
Given $x, y \in \mathbb{N}$, we define what it means for x to be *(strictly) less than* y as follows.

$<$
$$x < y \;:\Leftrightarrow\; x \in y$$

Similarly, for any $x, y \in \mathbb{N}$, we define what it means for x to be *less than or equal to* y.[2]

$\leqslant$
$$x \leqslant y \;:\Leftrightarrow\; (x < y) \vee (x = y)$$

$> \geqslant$ We further define $x > y :\Leftrightarrow y < x$ and $x \geqslant y :\Leftrightarrow y \leqslant x$ for every $x \in \mathbb{N}$ and $y \in \mathbb{N}$ as you might expect. These definitions establish a *strict total order* $<$ on $\mathbb{N}$, along with a corresponding *weak total order* $\leqslant$, as we will see in the theorem below.

[2] Whenever we define a *strict* order $<$ on a set X, we can always define a *weak* version $\leqslant$ of that order by saying $x \leqslant y :\Leftrightarrow x < y \vee x = y$ for all $x, y \in X$.

Theorem 6.1: The Natural Numbers are Linearly Ordered by $\leqslant$.
The order $\leqslant$ defined on the set $\mathbb{N}$ has the following four properties.

1. $(\forall x \in \mathbb{N})(x \leqslant x)$. *Reflexivity*
2. $\big(\forall x, y \in \mathbb{N}\big)\big((x \leqslant y \wedge y \leqslant x) \;\Rightarrow\; x = y\big)$. *Antisymmetry*
3. $\big(\forall x, y, z \in \mathbb{N}\big)\big((x \leqslant y \wedge y \leqslant z) \;\Rightarrow\; x \leqslant z\big)$. *Transitivity*
4. $\big(\forall x, y \in \mathbb{N}\big)(x \leqslant y \vee y \leqslant x)$. *Totality*

The first three properties make $\mathbb{N}$ with $\leqslant$ a *partially ordered* set;[3] the inclusion of the last property makes $\mathbb{N}$ with $\leqslant$ a *linearly ordered* set.

[3] We say a relation $\leqslant$ on a set X is a *partial order* by definition *iff* the relation is *reflexive, antisymmetric,* and *transitive; i.e.,* the relation $\leqslant$ satisfies the first three properties listed in ***Theorem 6.1***.

In fact, the order $\leqslant$ we just defined has one more remarkable property: whenever we look at a nonempty set of natural numbers—call it M, where $M \subseteq \mathbb{N}$ and $M \neq \varnothing$—we can always find an element $m \in M$ that is *smallest* according to the order $\leqslant$ we defined. To say that m is the *smallest element of* M formally, we would say that m is *"smaller than anything else in M,"* which we could express as $(\forall n \in M)(m \leqslant n)$.

Theorem 6.2: Least Element Property of $\mathbb{N}$.
$\forall M\big((M \subseteq \mathbb{N} \wedge M \neq \varnothing) \;\Rightarrow\; (\exists m \in M)(\forall n \in M)(m \leqslant n)\big)$.

This theorem is written with our new notation. To be clear, this theorem is equivalent to the following sentence: $\forall x\Big((x \subseteq \mathbb{N} \wedge x \neq \varnothing) \;\Rightarrow\; \exists y\big(y \in x \wedge \forall z(z \in x \;\Rightarrow\; y \leqslant z)\big)\Big)$. This immensely important theorem tells us that $\mathbb{N}$ is *well-ordered* by $\leqslant$, and that makes it possible for us to prove properties of natural numbers in an *interesting* way.

Theorem 6.3: Weak Induction.
For any *wff* φ with at most one free variable, the following equivalence holds.

$$(\forall n \in \mathbb{N})(\varphi(n)) \;\Leftrightarrow\; \varphi(0) \wedge (\forall k \in \mathbb{N})\Big(\varphi(k) \;\Rightarrow\; \varphi\big(\mathfrak{suc}(k)\big)\Big)$$

Proof. Let φ be a *wff*. We will prove the equivalence by showing both directions.

Fragment 1: Forwards.
Assume $(\forall n \in \mathbb{N})(\varphi(n))$. This immediately implies $\varphi(0)$ since $0 \in \mathbb{N}$. For the rest of the proof, let $k \in \mathbb{N}$ and assume $\varphi(k)$. Observe that $\varphi\big(\mathfrak{suc}(k)\big)$ because we assumed $(\forall n \in \mathbb{N})(\varphi(n))$. Therefore, $\varphi(k) \;\Rightarrow\; \varphi\big(\mathfrak{suc}(k)\big)$, and we can thus conclude $(\forall n \in \mathbb{N})\Big(\varphi(n) \;\Rightarrow\; \varphi\big(\mathfrak{suc}(n)\big)\Big)$ as desired.

Fragment 2: Backwards.
Assume $\varphi(0)$ and $(\forall k \in \mathbb{N})\Big(\varphi(k) \;\Rightarrow\; \varphi\big(\mathfrak{suc}(k)\big)\Big)$. Towards a contradiction, suppose there exists $n \in \mathbb{N}$ such that $\neg\varphi(n)$. Consider $M \coloneqq \{x \mid x \in \mathbb{N} \wedge \neg\varphi(x)\}$, the set of all counterexamples to φ. Because we assumed $\neg\varphi(n)$ and $n \in \mathbb{N}$, we know that $n \in M$ by definition, so $M \neq \varnothing$. Further, $M \subseteq \mathbb{N}$ because every element of M must be a natural number. Thus, we know that there exists some $m \in M$ such that $(\forall x \in M)(m \leqslant x)$ by ***Theorem 6.1***. Since $m \in M$, we know $m \in \mathbb{N}$[4] and $\neg\varphi(m)$.

[4] Recall there are two kinds of natural numbers: *zero* and the ones that are *successors*.

Case 1:
Suppose $m = 0$ and recall that $\neg\varphi(m)$ because $m \in M$. We know $\varphi(0)$ by assumption, which means we know $\varphi(m)$, contradicting $\neg\varphi(m)$. ↯

Case 2:
Suppose that there exists $\ell \in \mathbb{N}$ such that $m = \mathfrak{suc}(\ell)$. We now take two cases.

Case 2.1:
Suppose $\varphi(\ell)$. Recall $(\forall k \in \mathbb{N})\Big(\varphi(k) \;\Rightarrow\; \varphi\big(\mathfrak{suc}(k)\big)\Big)$, so that we have $\varphi(\ell) \;\Rightarrow\; \varphi\big(\mathfrak{suc}(\ell)\big)$, which implies $\varphi(\ell) \;\Rightarrow\; \varphi(m)$. By *modus ponens*, we obtain $\varphi(m)$. This contradicts $\neg\varphi(m)$, which we know because $m \in M$. ↯

Case 2.2:
Suppose $\neg\varphi(\ell)$, telling us that $\ell \in M$ by definition. Since m is the *least element* of M, we know $m \leqslant \ell$, implying $(m \in \ell) \vee (m = \ell)$ by definition. Now, recall that $m = \mathfrak{suc}(\ell)$, meaning $m = \ell \cup \{\ell\}$ by definition. Because $\ell \in \{\ell\}$, we know $\ell \in \ell \cup \{\ell\}$, and thus $\ell \in m$. Since we know $\forall x(x \notin x)$, we can say $\ell \neq m$. Combining all of these facts together, we realize that $m \in \ell$ and $\ell \in m$, contradicting the theorem $\forall x \forall y\big(x \in y \;\Rightarrow\; y \notin x\big)$. ↯

We have contradictions in both cases, so we instead conclude $\varphi(n)$ as desired.

Having proven both directions, we are now burdened with the weight of knowing that $(\forall n \in \mathbb{N})(\varphi(n)) \;\Leftrightarrow\; \varphi(0) \wedge (\forall k \in \mathbb{N})\Big(\varphi(k) \;\Rightarrow\; \varphi\big(\mathfrak{suc}(k)\big)\Big)$.

QED

Lemma 6.1.
$(\forall x \in \mathbb{N})\big(\mathfrak{suc}(x) \neq 0\big)$.

Proof. Let $x \in \mathbb{N}$. Notice that $x \in \{x\}$, so that $x \in x \cup \{x\}$, so that $x \in \mathfrak{suc}(x)$ by definition. Therefore, $\mathfrak{suc}(x) \neq \varnothing$, which means $\mathfrak{suc}(x) \neq 0$ by definition.

QED

6.2 Addition

Definition 6.3: Addition on the Natural Numbers.
We define how to *add* a natural number $n \in \mathbb{N}$ with another one as follows.

$$\begin{aligned} n + 0 &:= n \\ n + \mathfrak{suc}(m) &:= \mathfrak{suc}(n + m) \quad \text{if } m \in \mathbb{N} \end{aligned}$$

Lemma 6.2.
$1 + 1 = 2$.

Proof. Observe the following sequence of equalities.

$$\begin{aligned} 1 + 1 &= 1 + \mathfrak{suc}(0) && \text{by definition of 1} \\ &= \mathfrak{suc}(1 + 0) && \text{by definition of } + \\ &= \mathfrak{suc}(1) && \text{by definition of } + \\ &= 2 && \text{by definition of 2} \end{aligned}$$

Therefore, $1 + 1 = 2$. Rejoice.

QED

Lemma 6.3.
$(\forall x \in \mathbb{N})(x + 0 = x)$.

Proof. Let $x \in \mathbb{N}$ and observe that $x + 0 = x$ by definition of addition on $\mathbb{N}$.

QED

Lemma 6.4.
$(\forall x \in \mathbb{N})(0 + x = x)$.

Proof. We will show $(\forall n \in \mathbb{N})(0 + n = n)$ by *weak induction.*

Basis Step:
Observe that $0 + 0 = 0$ by definition of addition on $\mathbb{N}$.

Inductive Step:
Let $k \in \mathbb{N}$, and assume that $0 + k = k$. We will show $0 + \mathfrak{suc}(k) = \mathfrak{suc}(k)$. Observe.

$$\begin{aligned} 0 + \mathfrak{suc}(k) &= \mathfrak{suc}(0 + k) && \text{by definition of } + \\ &= \mathfrak{suc}(k) && \text{by the } \textit{inductive hypothesis} \end{aligned}$$

Therefore, we can conclude $(\forall n \in \mathbb{N})(0 + n = n)$ as desired.

QED

Lemma 6.5.
$(\forall x \in \mathbb{N})\big(x + 1 = \mathfrak{suc}(x)\big)$.

Proof. Let $x \in \mathbb{N}$. Observe the following.

$$\begin{aligned} x + 1 &= x + \mathfrak{suc}(0) && \text{by definition of 1} \\ &= \mathfrak{suc}(x + 0) && \text{by definition of } + \\ &= \mathfrak{suc}(x) && \text{by definition of } + \end{aligned}$$

Therefore, $x + 1 = \mathfrak{suc}(x)$ as desired.

QED

Theorem 6.4: Associativity of Addition.
$(\forall x, y, z \in \mathbb{N})\big(x + (y + z) = (x + y) + z\big)$.

Proof. Let $x, y \in \mathbb{N}$. We prove $(\forall z \in \mathbb{N})\big(x + (y + z) = (x + y) + z\big)$ by *weak induction.*

Basis Step:
Notice that $x + (y + 0) = x + y = (x + y) + 0$ by definition of addition on $\mathbb{N}$.

Inductive Step:
Let $k \in \mathbb{N}$ and assume that $x + (y + k) = (x + y) + k$. Observe now the following.

$$\begin{aligned} x + \big(y + \mathfrak{suc}(k)\big) &= x + \mathfrak{suc}(y + k) && \text{by definition of } + \\ &= \mathfrak{suc}\big(x + (y + k)\big) && \text{by definition of } + \\ &= \mathfrak{suc}\big((x + y) + k\big) && \text{by the } \textit{inductive hypothesis} \\ &= (x + y) + \mathfrak{suc}(k) && \text{by definition of } + \end{aligned}$$

We thus have $x + \big(y + \mathfrak{suc}(k)\big) = (x + y) + \mathfrak{suc}(k)$.

We can therefore conclude that $(\forall z \in \mathbb{N})\big(x + (y + z) = (x + y) + z\big)$ as desired.

QED

Theorem 6.5: Commutativity of Addition.
$(\forall x, y \in \mathbb{N})(x + y = y + x)$.

Proof. This proof is left as an exercise to the reader. □

6.3 Multiplication

Definition 6.4: Multiplication on the Natural Numbers.
We define how to *multiply* a natural number $n \in \mathbb{N}$ with another one as follows.

$$\begin{aligned} n \cdot 0 &:= 0 \\ n \cdot \mathfrak{suc}(m) &:= (n \cdot m) + n \quad \text{if } m \in \mathbb{N} \end{aligned}$$

Lemma 6.6: One is the Multiplicative Identity.
$(\forall x \in \mathbb{N})\big((x \cdot 1 = x) \wedge (1 \cdot x = x)\big)$.

Proof. First, let $n \in \mathbb{N}$ and observe that $n \cdot 1 = n \cdot \mathfrak{suc}(0) = (n \cdot 0) + n = 0 + n$ by the definition of multiplication. Recalling that addition is commutative, we can then see $0 + n = n + 0 = n$ by the definition of addition. Thus, $(\forall x \in \mathbb{N})(1 \cdot x = x)$.
Next, we will prove $(\forall x \in \mathbb{N})(1 \cdot x = x)$ by *weak induction.*

Basis Step:
Observe that $1 \cdot 0 = 0$ by the definition of multiplication.

Inductive Step:
Let $k \in \mathbb{N}$ and assume $1 \cdot k = k$. We will now show $1 \cdot \mathfrak{suc}(k) = \mathfrak{suc}(k)$. Observe.

$$\begin{aligned} 1 \cdot \mathfrak{suc}(k) &= (1 \cdot k) + 1 && \text{by definition of multiplication} \\ &= k + 1 && \text{by the } \textit{inductive hypothesis} \\ &= \mathfrak{suc}(k) && \text{because } (\forall x \in \mathbb{N})(\mathfrak{suc}(x) = x + 1) \end{aligned}$$

Therefore, we can conclude that $(\forall x \in \mathbb{N})(1 \cdot x = x)$.

QED

Lemma 6.7: Zero is the Multiplicative Annihilator.
$(\forall x \in \mathbb{N})\big((x \cdot 0 = 0) \wedge (0 \cdot x = 0)\big)$.

Proof. First, let $n \in \mathbb{N}$ and observe that $n \cdot 0 = 0$ by the definition of multiplication. Thus, $(\forall x \in \mathbb{N})(x \cdot 0 = 0)$. Next, we will show $(\forall x \in \mathbb{N})(0 \cdot x = 0)$ by *weak induction.*

Basis Step:
Observe that $0 \cdot 0 = 0$ by the definition of multiplication.

Inductive Step:
Let $k \in \mathbb{N}$ and assume $0 \cdot k = 0$. We will now show $0 \cdot \mathfrak{suc}(k) = 0$. Observe.

$$\begin{aligned} 0 \cdot \mathfrak{suc}(k) &= (0 \cdot k) + 0 && \text{by definition of multiplication} \\ &= 0 + 0 && \text{by the } \textit{inductive hypothesis} \\ &= 0 && \text{by definition of addition} \end{aligned}$$

Thus, we have that $0 \cdot \mathfrak{suc}(k) = 0$ as desired.

Therefore, we can conclude that $(\forall x \in \mathbb{N})(0 \cdot x = 0)$.

QED

Theorem 6.6: Distributivity of Multiplication over Addition.
$(\forall x, y, z \in \mathbb{N})\big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$.

Proof. Left as an exercise for the reader. □

Theorem 6.7: Associativity of Multiplication.
$(\forall x, y, z \in \mathbb{N})\big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$.

Proof. Let $x, y \in \mathbb{N}$. We will prove $(\forall z \in \mathbb{N})\big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$ by *weak induction.*

Basis Step:
Notice that $x \cdot (y \cdot 0) = x \cdot 0 = 0$ by the definition of multiplication on $\mathbb{N}$. Similarly, we can see that $(x \cdot y) \cdot 0 = 0$ by the same definition. Thus, $x \cdot (y \cdot 0) = (x \cdot y) \cdot 0$.

Inductive Step:
Let $k \in \mathbb{N}$, and assume $x \cdot (y \cdot k) = (x \cdot y) \cdot k$. We now observe with our eyeballs.

$$\begin{aligned} x \cdot \big(y \cdot \mathfrak{suc}(k)\big) &= x \cdot \big((y \cdot k) + y\big) && \text{by definition of } \cdot \\ &= x \cdot (y \cdot k) + x \cdot y && \text{by } \textit{distributivity} \text{ of } \cdot \text{ over } + \\ &= (x \cdot y) \cdot k + x \cdot y && \text{by the } \textit{inductive hypothesis} \\ &= (x \cdot y) \cdot \mathfrak{suc}(k) && \text{by definition of } \cdot \end{aligned}$$

As a result, we have that $x \cdot \big(y \cdot \mathfrak{suc}(k)\big) = (x \cdot y) \cdot \mathfrak{suc}(k)$.

Therefore, we can conclude $(\forall z \in \mathbb{N})\big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$ as desired.

QED

Theorem 6.8: Commutativity of Multiplication.
$(\forall x, y \in \mathbb{N})(x \cdot y = y \cdot x)$.

Proof. This proof is left as an exercise to the reader.

QED

6.4 Higher-Order Operations

Definition 6.5: Exponentiation.
↑ We define how to *exponentiate* any $n \in \mathbb{N}$ with a natural number exponent as follows.

$$\begin{aligned} n^0 &:= 1 \\ n^{\mathfrak{suc}(m)} &:= n^m \cdot n \quad \text{if } m \in \mathbb{N} \end{aligned}$$

Theorem 6.9.
$(\forall x, y, z \in \mathbb{N})(x^y \cdot x^z = x^{y+z})$.

Definition 6.6: Tetration.
↑↑ We define how to raise any $n \in \mathbb{N}$ to a natural number exponent recursively below.

$$\begin{aligned} n \uparrow\uparrow 0 &:= 1 \\ n \uparrow\uparrow \mathfrak{suc}(m) &:= n^{n \uparrow\uparrow m} \quad \text{if } m \in \mathbb{N} \end{aligned}$$