5 *A Theory of Arithmetic*

Having developed a working understanding of the language of the first-order logic and what the rules for the *"equality"* predicate are, we are finally ready to study our first mathematical theory: the *first-order theory of arithmetic according to Peano.*[1][2] As discussed previously, this requires us to specify a few things up-front.

We will take a universe of discourse consisting of all and only those objects that provably exist. The members of our universe will be referred to as *natural numbers*.

0 We will use the constant symbol "0" to denote a particular natural number, who we call *"zero,"* and whose fundamental properties are given by the axioms of arithmetic.

We will not initially consider any predicate symbols other than the binary $=$ predicate for *"equality"* that we are familiar with from our study of the first-order logic.[3]

$\mathfrak{suc}(x)$ We will introduce one unary functional symbol "$\mathfrak{suc}$." Given an arbitrary natural number x, we denote by $\mathfrak{suc}(x)$ the *"next number after x."* We will not be more specific than that, but the precise meaning of what *"next"* means will be revealed, in part, by the axioms we write below and the properties that 0 is meant to embody.

[1] This is named after *Giuseppe Peano.*

[2] Actually, this is a lie. If we wanted this to actually be the first-order theory usually called *"Peano arithmetic,"* we would need to transform our definitions for addition and multiplication—which we will see below soon—from *definitions* into *axioms,* and include $+$ and $\cdot$ as binary functional symbols in the syntax of the theory. None of this is *actually* significant for us, and recursive definitions will play a large role in this course, so we instead choose to introduce $+$ and $\cdot$ as definitions rather than axioms.

[3] We will, of course, eventually want to study concepts such as *"less than or equal"* and *"being prime,"* but we will incorporate these ideas as *definitions within our theory* in terms of the primitive notions we are introducing now.

5.1 *Axiomatizing the Structure of a Discrete Line*

This theory is meant to describe the fundamental nature of the *"nonnegative whole numbers,"* along with their basic algebraic operations, and the consequences that follow. To that end, and for the sake of understanding the axioms that follow, we should try to have a *picture* in our heads because this *"fundamental nature"* is actually, secretly, about something much more important than *"numbers."* What we are trying to understand is the following ***structure***.

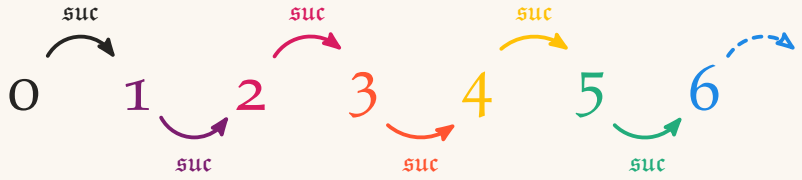

Figure 1. The abstract structure of the natural number line. Any point on this line can be reached by starting at zero and taking a finite number of discrete, consecutive steps in one direction.

Notice the *shape* of the natural number line. The important aspect of this structure is the *arrangement* of the numbers on this line with respect to one another. Crucially, the line ***begins at zero***, and ***proceeds in one direction*** from there on *forever* by taking ***discrete steps*** one-at-a-time. These properties are what fundamentally characterize *"the natural numbers"* and the *"arithmetic"* we perform with those *"numbers,"* so this structure is what we want to encode with our axioms for arithmetic.

The first axiom, then, asserts explicitly that 0 is a natural number by telling us that 0 is equal to something in our universe of discourse.

Axiom 0: Zero is a Natural Number.
$\exists x(x = 0)$. ⌟

Now, we would like to say that 0 is the *"first"* natural number. To express this idea, we must rely on the $\mathfrak{suc}(\cdot)$ functional symbol we introduced. There are several different, yet equivalent, ways we could now write *"zero is the first natural number,"*

but the simplest might be to say that *zero has no predecessors.* Instead of introducing a whole new symbol for the concept of a *"predecessor,"* we can use our successor functional symbol to say that *"no natural number has zero as its successor."*

Axiom 1: Zero is the First Natural Number.
$\forall x(\mathfrak{suc}(x) \neq 0)$. ⌟

These first two axioms establish that our natural number line starts at zero. Of course, we also need *the rest* of the numbers to exist. We can ensure this by asserting that, whenever we have a natural number x, the *successor* of x must exist.

Axiom 2: The Successor of a Natural Number is a Natural Number.
$\forall x \exists y(y = \mathfrak{suc}(x))$. ⌟

Up until this point we know, at a minimum, the natural number line looks as follows.

Figure 2. The first natural number 0 along with its first two successors.

Being required to continue to use "$\mathfrak{suc}$" to refer to the things on this line will get incredibly tedious remarkably quickly, so we introduce the following definitions.

$$\begin{aligned} 1 &:= \mathfrak{suc}(0) \\ 2 &:= \mathfrak{suc}(1) \\ 3 &:= \mathfrak{suc}(2) \\ 4 &:= \mathfrak{suc}(3) \\ &\vdots \end{aligned}$$

We proceed from this point forward with the understanding that these definitions go on *forever,* assigning to each position on the natural number line the symbol the we would *normally* think of as representing *"the number"* that belongs at that position.

Immediately, one might begin to wonder: do any of these symbols 1, 2, 3, …, actually refer to *anything real?* Are these *natural numbers?* Let's verify that 1 actually exists.

Lemma 5.1: One is a Natural Number.
$\exists x(x = 1)$.

Proof. Recall that $\exists x(x = 0)$ from *Axiom 0*. In otherwords, there exists some natural number x such that $x = 0$. Now, remembering *Axiom 2*, we can infer that there exists a natural number y such that $y = \mathfrak{suc}(x)$. Since $x = 0$, this obviously implies $y = \mathfrak{suc}(0)$. Again, relying on our eiditic memory, we remember that $\mathfrak{suc}(0) = 1$ by definition. This then means $y = 1$. We thus conclude that $\exists z(z = 1)$.

QED

Axiom 3: Natural Numbers with Equal Successors are Equal.
$\forall x \forall y(\mathfrak{suc}(x) = \mathfrak{suc}(y) \Rightarrow x = y)$. ⌟

Axiom 4: Schema of Weak Induction.
For any well-formed formula φ with at most one free variable, the following holds.

$$\Big(\varphi(0) \wedge \forall k\big(\varphi(k) \Rightarrow \varphi\big(\mathfrak{suc}(k)\big)\big)\Big) \Rightarrow \forall x\big(\varphi(x)\big)$$

⌟

5.2 *The Fundamental Algebraic Structure*

Addition

Definition 5.1: Addition.
For every pair of natural numbers n and m, we define the following binary *operation*.

$$\begin{aligned} n + 0 &:= n \\ n + \mathfrak{suc}(m) &:= \mathfrak{suc}(n + m) \end{aligned}$$

We call this binary operation *"addition"* and use the notation $n + m$ to denote *"the sum of n with m"* when n and m are natural numbers. ⌟

Lemma 5.2.
$1 + 1 = 2$.

Proof. Recall that $1 = \mathfrak{suc}(0)$ by definition, and that $2 = \mathfrak{suc}(1)$ by definition. We can leisurely observe the following deduction.

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

Therefore, we can conclude that $1 + 1 = 2$.

QED

Lemma 5.3.
$\forall x(x + 1 = \mathfrak{suc}(x))$.

Proof. Let n be an arbitrary natural number. We must observe the following.

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

This shows us that $n + 1 = \mathfrak{suc}(n)$. We therefore conclude $\forall x(x + 1 = \mathfrak{suc}(x))$.

QED

Lemma 5.4.
$\forall x(\mathfrak{suc}(x) = 1 + x)$.

Proof. We will prove $\forall x(1 + x = \mathfrak{suc}(x))$ by weak induction.

Basis Step:
The definition of the symbol "1" tells us that $\mathfrak{suc}(0) = 1$, and the definition of addition implies $1 = 1 + 0$. Therefore, we know $\mathfrak{suc}(0) = 1 + 0$.

Inductive Step:
Let k be an arbitrary natural number. Assume $1 + k = \mathfrak{suc}(k)$.[1] Now, observe.

[1] This is our *inductive hypothesis.*

$$\begin{aligned} 1 + \mathfrak{suc}(k) &= \mathfrak{suc}(1 + k) && \text{by definition of addition} \\ &= \mathfrak{suc}\big(\mathfrak{suc}(k)\big) && \text{by the } \textit{inductive hypothesis} \end{aligned}$$

This shows us that $1 + \mathfrak{suc}(k) = \mathfrak{suc}(\mathfrak{suc}(k))$ as required.

Therefore, by *Axiom 4*, we conclude that $\forall n(1 + n = \mathfrak{suc}(n))$ as desired.

QED

Theorem 5.1: Zero is the Additive Identity.
The natural number 0 is an *identity element* with respect to *addition.* This means that adding 0 to any natural number leaves that number unchanged.

$$\forall x(x + 0 = x) \land \forall x(0 + x = x)$$

In fact, zero is the *only* natural number with this property important property.

$$\forall x\Big(\big(\forall y(x + y = y) \land \forall y(y + x = y)\big) \Rightarrow x = 0\Big)$$

⌟

Theorem 5.2: Associativity of Addition.
The order in which we carry out a sequence of repeated additions does not impact the final result. This makes $+$ an example of what's called an *associative* operation.

$$\forall x \forall y \forall z\big(x + (y + z) = (x + y) + z\big)$$

⌟

Theorem 5.3: Commutativity of Addition.
The order in which we provide the inputs to addition does not affect the output.

$$\forall x \forall y(x + y = y + x)$$

⌟

Multiplication

Definition 5.2: Multiplication.
For every pair of natural numbers n and m, we define the following binary operation.

$$\begin{aligned} n \cdot 0 &:= 0 \\ n \cdot \mathfrak{suc}(m) &:= (n \cdot m) + n \end{aligned}$$

We call this binary operation *"multiplication"* and use the notation $n \cdot m$ to denote *"the product of n with m."* If the context is clear, it is common to simplify the notation by writing nm to mean $n \cdot m$, though this should be done with care to avoid confusion. To simplify notation for mixed expressions involving both $\cdot$ and $+$, we adopt the convention that multiplication takes precedence over addition. This means we will consider $(x \cdot y) + z = x \cdot y + z$ to be *true* for all natural numbers x, y, and z. ⌟

Multiplication was defined recursively in terms of addition. If we closely analyze the above definition, we might actually realize that this definition encodes the idea that *multiplication is nothing more than repeated addition.* We can describe the relationship between multiplication and addition as follows.

Theorem 5.4: Distributivity of Multiplication over Addition.
Multiplication on the right by a sum of two numbers is equivalent to adding together two products by *"distributing"* the multiplication operation over the sum.

$$\forall x \forall y \forall z\big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$$

⌟

There are some even more surprising relationship between multiplication and addition. For example, if we multiply using the *additive identity,* then the result gets *"annihilated"* and we just get the additive identity back. We also cannot multiply

nonzero numbers together to produce 0—the only way to produce the additive identity as a product of two numbers is by annihilating one of them using zero.

Theorem 5.5.
Multiplying by the zero, additive identity, annihilates the other number. The result then is zero, the additive identity, again.

$$\forall x(x \cdot 0 = 0) \land \forall x(0 \cdot x = 0)$$

Further, if a product of two numbers results in zero, then one of the two *factors* of the product must have been zero. This is usually expressed by saying *"there are no nonzero zero-divisors."*

$$\forall x \forall y\Big(x \cdot y = 0 \Rightarrow \big((x = 0) \lor (y = 0)\big)\Big)$$ ⌟

If we squint our eyes and consider multiplication as an operation in its own right, *"forgetting"* that multiplication is just iterated addition, we will notice that multiplication actually has many of the same properties that we discovered about addition.

Theorem 5.6: One is the Multiplicative Identity.
The natural number 1 is an *identity element* with respect to *multiplication.* This means that multiplying any natural number by 1 leaves that number unchanged.

$$\forall x(x \cdot 1 = x) \land \forall x(1 \cdot x = x)$$ ⌟

Theorem 5.7: Associativity of Multiplication.
The order in which we carry out a sequence of repeated multiplications does not impact the final result. This makes $\cdot$ yet another example of an *associative* operation.

$$\forall x \forall y \forall z\big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$$ ⌟

Theorem 5.8: Commutativity of Multiplication.
The order in which inputs are provided to multiplication does not affect the result.

$$\forall x \forall y(x \cdot y = y \cdot x)$$ ⌟

Note that, thanks to commutativity, there is no meaningful distinction between *"distributivity on the* ***right****"* and *"distributivity on the* ***left****"* for multiplication over addition. More precisely, for any natural numbers a, b, and c, not only do we know that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ thanks to *Theorem 5.4*, but we also know that it works the other way: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Putting Things in Order

Definition 5.3: Inequality.
For every pair of natural numbers n and m, we define the following *relation.*

$$n \leqslant m \;\; :\Leftrightarrow \;\; \exists p(n + p = m)$$

We call this a *"weak inequality,"* implying the idea of a *strict inequality,* defined below.

$$n < m \;\; :\Leftrightarrow \;\; n \leqslant m \land n \neq m$$ ⌟

:⇔

Note the use of a new symbol :⇔ in the above definition.[1] In the same way that we use := and = to distinguish between *defining* and *comparing* ***objects,*** we use the symbols :⇔ and ⇔ to distinguish between *defining* and *comparing* ***expressions.***

[1] This symbol is usually verbalized as *"[…] if and only if, by definition, […]."*

Lemma 5.5.
For every pair of natural numbers n and m, the following inequalities are equivalent.

$$\begin{aligned} n < m &\Leftrightarrow \exists p(n + p = m \wedge p \neq 0) \\ &\Leftrightarrow \exists p\big((n + p) + 1 = m\big) \end{aligned}$$

⌟

Corollary 5.1.
For any natural number n such that $0 < n$, we have $\exists m(m + 1 = n)$. ⌟

These orders have some very important properties.

Theorem 5.9: The Weak Inequality of Natural Numbers is a Linear Order.
Because $x + 0 = x$ for every natural number x, the $\leqslant$ order on the natural numbers has a property we call *reflexivity*, similar to our first axiom for equality.

$$\forall x(x \leqslant x)$$

However, unlike equality, the $\leqslant$ order is *not symmetric:* we have $2 \leqslant 3$, but $3 \not\leqslant 2$. Instead, the $\leqslant$ order has a different property called *antisymmetry.*

$$\forall x \forall y\big((x \leqslant y \wedge y \leqslant x) \Rightarrow x = y\big)$$

Finally, this order has a property we call *transitivity.*

$$\forall x \forall y \forall z\big((x \leqslant y \wedge y \leqslant z) \Rightarrow x \leqslant z\big)$$

These three properties make $\leqslant$ an example of a *partial order* on the natural numbers. There is one more property—often taken for granted—that ensures any two natural numbers can always be compared. This is called *totality.*

$$\forall x \forall y(x \leqslant y \vee y \leqslant x)$$

An equivalent way to express this property, using the *strict* version of inequality, is sometimes called *trichotomy.*

$$\forall x \forall y\big((x = y) \vee (x < y) \vee (y < x)\big)$$

With all these properties, we call $\leqslant$ an example of a *linear order* on the naturals. ⌟

Theorem 5.10: Monotonicity of Addition.
Adding the same number on both sides of an inequality *"preserves"* the inequality.

$$\forall x \forall y \forall z(x \leqslant y \Rightarrow x + z \leqslant y + z)$$

⌟

Theorem 5.11: Monotonicity of Multiplication.
Multiplying the same *natural* number[2] on both sides of an inequality *"preserves"* the inequality, just as we saw before with addition.

$$\forall x \forall y \forall z(x \leqslant y \Rightarrow x \cdot z \leqslant y \cdot z)$$

⌟

[2] Note the importance of our universe of discourse for this discussion. If we had taken a universe of discourse that contained *"negative numbers,"* whatever those are, then this theorem would no longer be *true* as written.