9 *Setting the Foundation*

9.1 *What Does Elementhood Really Mean?*

Axiom 6: Regularity.
Every nonempty set x contains an $\in$-minimal element—an element of x that doesn't contain any of the other elements of x as an element.

$$\forall x\Big(x \neq \varnothing \Rightarrow \exists y\big(y \in x \wedge \forall z(z \in x \Rightarrow z \notin y)\big)\Big)$$

Since this element, referred to as y in the sentence above, doesn't contain any of the other elements of x within itself, it cannot share any elements with x. This realization allows us to rewrite this sentence a little more compactly as follows.

$$\forall x\big(x \neq \varnothing \Rightarrow \exists y(y \in x \wedge x \cap y = \varnothing)\big)$$

Both of these sentences are equivalent, and they establish that sets are *"well-founded"* with respect to the elementhood $\in$ relation in Zermelo-Fraenkel set theory. ⌟

Theorem 9.1: Sets Do Not Contain Themselves.
$\forall x(x \notin x)$.

Proof. Let x be a set, and suppose towards a contradiction that $x \in x$. We know $\{x\}$ exists by the *Axiom of Pairing*, and we can clearly see $x \in \{x\}$, showing us $\{x\} \neq \varnothing$. By the *Axiom of Regularity*, we then know there exists $t \in \{x\}$ such that $t \cap \{x\} = \varnothing$. Notice that $t \in \{x\}$ implies $t = x$, so we now have $x \cap \{x\} = \varnothing$. However, recalling our assumption $x \in x$ and observation $x \in \{x\}$ from earlier, we realize $x \in x \cap \{x\}$ by definition, so that $x \cap \{x\} \neq \varnothing$, contradicting what we just said! ↯
Therefore, $x \notin x$, and we conclude that sets cannot contain themselves as elements.
QED

Theorem 9.2: Two Sets Cannot Both Contain Each Other.
$\forall x \forall y(x \notin y \vee y \notin x)$

Proof. Let x and y be sets, and suppose towards a contradiction $x \in y$ and $y \in x$. Consider the set $\{x, y\}$, which we know exists by the *Axiom of Pairing,* and observe that $x \in \{x, y\}$ and $y \in \{x, y\}$. This implies $\{x, y\} \neq \varnothing$, so that applying the *Axiom of Regularity* induces the existence of some $t \in \{x, y\}$ such that $t \cap \{x, y\} = \varnothing$. Because $t \in \{x, y\}$, we know either $t = x$ or $t = y$; we now take two cases.

Case 1:
Suppose $t = x$. Since $y \in x$, this implies $y \in x \cap \{x, y\}$, so that $x \cap \{x, y\} \neq \varnothing$.

Case 2:
Suppose $t = y$. Since $x \in y$, this implies $x \in y \cap \{x, y\}$, so that $y \cap \{x, y\} \neq \varnothing$.

In either case, we see that $t \cap \{x, y\} \neq \varnothing$, contradicting $t \cap \{x, y\} = \varnothing$ from earlier. ↯
Therefore, we conclude that $x \notin y$ or $y \notin x$ must hold.
QED

9.2 *Is This All There Is?*

The time has finally come for us to analyze *Axiom 0* in detail. The point of this axiom is to formally assert the existence of a set that contains all and only the *"natural numbers"* so that we can recover all of the information we gained about natural numbers in the *theory of arithmetic* within set theory.

Fundamentally, we learned in the theory of arithmetic that there are two kinds of natural numbers: *the first natural number zero*, and *the (iterated) successors of zero.* These were represented using the *constant symbol* "0" and the *functional symbol* "$\mathfrak{suc}(\circlearrowleft)$," which were introduced without definition during the preamble to the theory. In order to understand what arithmetic means in set theory, we need to define what "0" and "$\mathfrak{suc}(\circlearrowleft)$" mean *in terms of sets.*

0 We define *the natural number zero* to be $0 \coloneqq \varnothing$. Further, given an arbitrary set x, we
$\mathfrak{suc}(x)$ define *the successor of* x to be $\mathfrak{suc}(x) \coloneqq x \cup \{x\}$.

Axiom 0: Infinity.
We say that a set I is *inductive* when $\varnothing \in I$ and $\forall x(x \in I \Rightarrow x \cup \{x\} \in I)$.

$$\exists N\Big(\varnothing \in N \wedge \forall n\big(n \in N \Rightarrow n \cup \{n\} \in N\big) \wedge$$
$$\forall M\Big(\big(\varnothing \in M \wedge \forall m\big(m \in M \Rightarrow m \cup \{m\} \in M\big)\big) \Rightarrow N \subseteq M\Big)\Big)$$

We can state this more compactly using the definition of *"inductive set"* given earlier.

$$\exists N\big(N \text{ is inductive} \wedge \forall M(M \text{ is inductive} \Rightarrow N \subseteq M)\big)$$

It can be shown[1] that there can only be one set N that makes the inside of that existential statement *true*—in other words, the set the axiom above asserts exists is
$\mathbb{N}$ *unique.* We call that *the set of natural numbers* and use the symbol $\mathbb{N}$ to denote it. ⌟

[1] Using the *Axiom of Extensionality.*

Lemma 9.1.
The following statements, which adapt the axioms of arithmetic to be statements about $\mathbb{N}$ and its elements, all hold within set theory.

0. $(\exists x \in \mathbb{N})(x = 0)$.
1. $(\forall x \in \mathbb{N})(\mathfrak{suc}(x) \neq 0)$.
2. $(\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(y = \mathfrak{suc}(x))$.
3. $(\forall x \in \mathbb{N})(\forall y \in \mathbb{N})(\mathfrak{suc}(x) = \mathfrak{suc}(y) \Rightarrow x = y)$. ⌟

Theorem 9.3: Characterization of the Natural Numbers.
For every $n \in \mathbb{N}$, either $n = 0$ or $(\exists m \in \mathbb{N})(n = \mathfrak{suc}(m))$.

Proof. Towards a contradiction, suppose there exists some $x \in \mathbb{N}$ such that $x \neq 0$ and $(\forall m \in \mathbb{N})(x \neq \mathfrak{suc}(m))$. Consider $M \coloneqq \{m \mid m \in \mathbb{N} \wedge m \neq x\} = \mathbb{N} \setminus \{x\}$.[2] Note that $x \notin M$ by definition. We will show that M is an inductive set.

[2] We can easily see M exists by the *Axiom Schema of Separation.*

First, we know $0 \in \mathbb{N}$ and $x \neq 0$, so we know $0 \in \mathbb{N} \setminus \{x\}$ by definition. Thus, $0 \in M$.

Second, let $y \in M$, and recall this means $y \in \mathbb{N} \wedge y \neq x$ by definition. Since $y \in \mathbb{N}$, we know $\mathfrak{suc}(y) \in \mathbb{N}$. Since we assumed $(\forall m)(x \neq \mathfrak{suc}(m))$, we know $x \neq \mathfrak{suc}(y)$, and therefore $\mathfrak{suc}(y) \in M$ by definition. Thus, $\forall m(m \in M \Rightarrow \mathfrak{suc}(m) \in M)$.

These two facts combined tell us that M is an inductive set, and therefore $\mathbb{N} \subseteq M$ by the *Axiom of Infinity*. But, if we remember that $x \in \mathbb{N}$, this now implies $x \in M$, contradicting the fact that $x \notin M$. ↯ Therefore, either $x = 0$ or $(\exists m \in \mathbb{N})(x = \mathfrak{suc}(m))$.

QED

Theorem 9.4: Weak Induction.
The schema of weak induction from the theory of arithmetic is *true* when adapted to be a statement about $\mathbb{N}$ and its elements in set theory. For any well-formed formula φ with at most one free variable, the following equivalence holds.

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

Proof. Let φ be a well-formed formula with at most one free variable, and assume that $\varphi(0)$ and also $(\forall k \in \mathbb{N})(\varphi(k) \Rightarrow \varphi(\mathfrak{suc}(k)))$. Towards a contradiction, suppose there exists some $\dot{n} \in \mathbb{N}$ such that $\neg\varphi(\dot{n})$. Consider the set of all counterexamples $M \coloneqq \{m \mid m \in \mathbb{N} \wedge \neg\varphi(m)\}$,[1] and notice that $M \neq \varnothing$ because $\dot{n} \in M$ by definition. This means we can apply the *Axiom of Regularity* to M and deduce that there exists some $\dot{m} \in M$ such that $\dot{m} \cap M = \varnothing$.

[1] We know that M exists by the *Axiom Schema of Separation.*

Now, we know from our *previous result* that either $\dot{m} = 0$ or $(\exists m \in \mathbb{N})(\mathfrak{suc}(m) = \dot{m})$. Since $\dot{m} \in M$ implies $\neg\varphi(\dot{m})$, we know that $\dot{m} \neq 0$ because that would contradict one of our initial assumptions $\varphi(0)$. Thus, there must exist some $\ddot{m} \in \mathbb{N}$ such that $\mathfrak{suc}(\ddot{m}) = \ddot{m} \cup \{\ddot{m}\} = \dot{m}$. As it turns out, we can prove that $\ddot{m} \notin M$. First, observe.

$$\ddot{m} \in \{\ddot{m}\} \quad \Rightarrow \quad \ddot{m} \in \ddot{m} \cup \{\ddot{m}\} \quad \Rightarrow \quad \ddot{m} \in \mathfrak{suc}(\ddot{m}) \quad \Rightarrow \quad \ddot{m} \in \dot{m}$$

Since $\ddot{m} \in \dot{m}$ and $\dot{m} \cap M = \varnothing$, we can deduce $\ddot{m} \notin M$.[2] Then, by the definition of M, this lets us say $\varphi(\ddot{m})$. The time has now come for us to recall that we initially assumed $(\forall k \in \mathbb{N})(\varphi(k) \Rightarrow \varphi(\mathfrak{suc}(k)))$; if we apply this assumption to $\varphi(\ddot{m})$, then we can infer $\varphi(\mathfrak{suc}(\ddot{m}))$, which means $\varphi(\dot{m})$. However, this contradicts $\neg\varphi(\dot{m})$! ↯
Therefore, we must conclude $(\forall n \in \mathbb{N})(\varphi(n))$ instead.

[2] Otherwise, we would have $\ddot{m} \in \dot{m} \cap M$, implying $\ddot{m} \in \varnothing$, contradicting the fact that $\varnothing$ is empty.

QED

Corollary 9.1: Strong Induction.
For any well-formed formula φ with at most one free variable, the following holds.

$$(\forall k \in \mathbb{N})\Big(\big(\forall j \in \mathbb{N}\big)\big(j < k \Rightarrow \varphi(j)\big) \Rightarrow \varphi(k)\Big) \Leftrightarrow (\forall n \in \mathbb{N})\big(\varphi(n)\big)$$ ⌟

Theorem 9.5.
$(\forall n \in \mathbb{N})(n = \{m \mid m \in \mathbb{N} \wedge m < n\})$. ⌟

9.3 *A Number of Important Things*

Now that we have proven each of the axioms of arithmetic as theorems about $\mathbb{N}$ in set theory, we recover *every* theorem of arithmetic inside set theory for free. We will take the time now to summarize the most important properties of $\mathbb{N}$ here, and along the way we will introduce various other sets of numbers that should seem familiar.

As we survey these number sets, we will describe them as *"algebraic structures"* by detailing their algebraic properties. The point of doing this is to understand that these are concrete examples of *abstract algebraic structures.* You are bound to come across other examples of these (and other) algebraic structures in the future.

The Natural Numbers

The set of natural numbers $\mathbb{N}$ is equipped with two binary operations—*addition* and *multiplication,* denoted by $+$ and $\cdot$ respectively—and a *linear order* denoted by the $\leqslant$ symbol. This structure is an *"ordered semiring,"* a term that we will describe by listing its various constituent properties below.

Theorem 9.6: The Natural Numbers Form an Ordered Semiring.
The natural number 0 is the *identity element* with respect to addition, and addition is an *associative* operation on the set of natural numbers. These two facts make $\mathbb{N}$ with addition an example of a *monoid.*

monoid

1. $0 \in \mathbb{N}$ and $(\forall x \in \mathbb{N})(0 + x = x + 0 = x)$ — *existence of additive identity*
2. $(\forall x, y, z \in \mathbb{N})(x + (y + z) = (x + y) + z)$ — *associativity of addition*

Addition also happens to be *commutative,* so $\mathbb{N}$ with addition is a *commutative monoid.*

3. $(\forall x, y \in \mathbb{N})(x + y = y + x)$ — *commutativity of addition*

The natural number 1 is the *identity element* with respect to multiplication, and multiplication is an *associative* operation, making $\mathbb{N}$ with multiplication also a *monoid.*

4. $1 \in \mathbb{N}$ and $(\forall x \in \mathbb{N})(1 \cdot x = x \cdot 1 = x)$ — *existence of multiplicative identity*
5. $(\forall x, y, z \in \mathbb{N})(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$ — *multiplication is associative*

We also know that multiplication *distributes* over addition, though the converse does not hold in the naturals with these operations. The additive identity, which is 0 in this case, also acts as an *annihilator* with respect to multiplication.

6. $\big(\forall x, y, z \in \mathbb{N}\big)\big(x \cdot (y + z) = (x \cdot y) + (x \cdot z) \ \wedge \ (x + y) \cdot z = (x \cdot z) + (y \cdot z)\big)$ — *distributivity of multiplication / addition*
7. $(\forall x \in \mathbb{N})(0 \cdot x = x \cdot 0 = 0)$ — *zero is the multiplicative annihilator*

All these facts, taken together up until this point, make $\mathbb{N}$ with addition and multiplication an example of a *semiring.* Additionally, multiplication is also *commutative.*

semiring

8. $(\forall x, y \in \mathbb{N})(x \cdot y = y \cdot x)$ — *commutativity of multiplication*

Finally, when we define $\leqslant$ as we did in the theory of arithmetic,[1] we know that $\leqslant$ is a *partial order* on $\mathbb{N}$,[2] and addition and multiplication interact *monotonically* with respect to this order. Said another way: addition and multiplication *preserve inequalities.*

[1] Recall that $a \leqslant b$ was defined to mean $(\exists c \in \mathbb{N})(a + c = b)$ for every $a, b \in \mathbb{N}$.

[2] In fact, $\leqslant$ is a *linear* order on $\mathbb{N}$.

9. $(\forall x, y, z \in \mathbb{N})(x \leqslant y \ \Rightarrow \ x + z \leqslant y + z)$ — *monotonicity of addition*
10. $(x, y, z \in \mathbb{N})\Big(\big((x \leqslant y) \wedge (0 \leqslant z)\big) \ \Rightarrow \ \big((x \cdot z \leqslant y \cdot z) \wedge (z \cdot x \leqslant z \cdot y)\big)\Big)$ — *monotonicity of multiplication*

A set with two binary operations and a partial order satisfying each of these properties (with the possible exception of 8.) is called an *ordered (commutative) semiring.* ⌟

ordered semiring

Theorem 9.7: Addition and Multiplication Are Cancellative.
Although subtraction is not defined as an operation on natural numbers, we can emulate subtraction by speaking about addition instead. When the same quantity is being *added* to both sides of an (in)equality, *cancelling* it out preserves (in)equality.[3]

[3] Although *"cancellativity"* is generally written as a statement about equations, it is also *true* about inequalities in each of the *ordered* algebraic structures we are discussing here.

› $(\forall x, y, z \in \mathbb{N})(x + z = y + z \Rightarrow x = y)$ — *additive cancellativity*

Something similar holds about multiplication: when the same *nonzero* quantity is multiplied on both sides of an (in)equality, *cancelling* it out preserves (in)equality.

› $(\forall x, y, z \in \mathbb{N})((x \cdot z = y \cdot z \wedge z \neq 0) \Rightarrow x = y)$ ⌟ — *multiplicative cancellativity*

Theorem 9.8: The Natural Numbers Form a Semidomain.
The set of natural numbers has what we call the *"domain property,"* which means that there do not exist *"nonzero zero-divisors."* The only divisor of the annihilator is itself.

› $(\forall x, y \in \mathbb{N})\big((x \cdot y = 0) \Rightarrow (x = 0 \vee y = 0)\big)$ ⌟ *no nonzero zero-divisors*

The Integral Numbers

The natural numbers might feel *"incomplete"* in the sense that it does not contain *negative* numbers. An intuitive description of who the negative numbers are might be: numbers x with the property $x < 0$. In fact, if we were to define what it meant for a number x to be *"negative,"* we might say precisely that it means $x < 0$, and a corresponding definition for x being *"positive"* might be $0 < x$.

negative
positive

However, that's not really *why* we miss the negative numbers when we're working within $\mathbb{N}$. What we really miss is the ability to *subtract.* The thing we are in search of is *additive inverses* for each natural number.

Definition 9.1: Additive Inverses.
Given a natural number $x \in \mathbb{N}$, we say that $y \in \mathbb{N}$ is an *additive inverse for* x if and only if $x + y = 0$, meaning that adding x with y produces the additive identity. ⌟

additive inverse

This is an example of a notion that can be generalized to any situation in which we have a set of *things* that are related by a *binary operation* with respect to which an *"identity element"* exists.[1]

We obtain $\mathbb{Z}$, the set of *integers,* by (recursively) insisting that every natural number has an additive inverse. Of course, in the theory of sets, in order for us to really *know* what $\mathbb{Z}$ is, we should know precisely what its elements are *as sets.* Will not describe those details here. Instead, we will believe the following noble lie.[2]

$\mathbb{Z}$

Noble Lie 9.1. Every natural number is an integer. More formally, $\mathbb{N} \subseteq \mathbb{Z}$.

Theorem 9.9: The Integers Are an Ordered Ring.
The set of integers $\mathbb{Z}$ inherits from $\mathbb{N}$ all of the properties of an *ordered semiring,* but when considering $\mathbb{Z}$ with addition, we can see that $\mathbb{Z}$ has one additional property that elevates it from a *monoid* in to a *group.*

group

› $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y = 0)$ *existence of all additive inverses*

Since $\mathbb{Z}$ with addition is a monoid *with additive inverses for every element*, and $\mathbb{Z}$ with multiplication is a monoid, and multiplication still distributes over addition, and the additive identity is still the multiplicative annihilator, we now officially promote $\mathbb{Z}$ from a *semiring* to a *ring.* Addition and multiplication are still monotonic with respect to the standard $\leqslant$ order, so we call $\mathbb{Z}$ an *ordered ring.* ⌟

ring
ordered ring

Some more detail about the consequences of including additive inverses for all elements will be added at a later point. For now, if there is some *"gradeschool"* fact about integers that you think you know, it is *probably* a theorem about $\mathbb{Z}$.

henlo[3]

[1] We will see more interesting, and complicated, examples of this later.

[2] This is technically a *lie* in the sense that it is not actually *true* about $\mathbb{N}$ and $\mathbb{Z}$ as they are traditionally constructed in Zermelo-Fraenkel set theory, and I am therefore intentionally telling you something *false.* However, this is ***true in spirit*** we would like this to be *true,* and the only reason it isn't is because of implementation details about the particular way in which $\mathbb{Z}$ is traditionally constructed. In fact, what *is true* is that a copy of the *algebraic structure* $\mathbb{N}$ that we described earlier appears within the *algebraic structure* $\mathbb{Z}$. This much deeper fact—the thing that makes this lie *"noble"*—is the more important thing; it would be instructive to understand precisely what this means. If only we had the time…

[3] …this section will be expanded later…

The Rational Numbers

We arrived at $\mathbb{Z}$ by *"completing"* $\mathbb{N}$ in a sense: there were some natural numbers (*i.e.,* every natural number except for 0) that did not have inverses with respect to *addition.* While this makes $\mathbb{Z}$ a little nicer to work in than $\mathbb{N}$, it may leave you unsatisfied if you ever find yourself *multiplying* integers together. Ideally, it would be nice to have the ability to *divide* just like we now have the ability to *subtract.* This corresponds to the demand for *"multiplicative inverses,"* though we now have to be more careful than we were when we made this demand about addition because of the fact that *we cannot divide by zero!*[1]

[1] This is not an arbitrary restriction: it would be a serious problem to introduce a multiplicative inverse for the additive identity in any *ring,* and you are encouraged to think about why that might be the case.

Definition 9.2: Multiplicative Inverses.
mult. inverse
Given an integer $x \in \mathbb{Z}$, we say that $y \in \mathbb{Z}$ is a *multiplicative inverse for* x if and only if $x \cdot y = 1$, meaning that multiplying x by y produces the multiplicative identity. ⌟

Noble Lie 9.2. Every integer is a rational number. More formally, $\mathbb{Z} \subseteq \mathbb{Q}$.

Theorem 9.10: The Rationals Are an Ordered Field.
henlo ⌟

henlo[2]

[2] …this section will be expanded later…

The Real Numbers

Noble Lie 9.3. Every rational number is a real number. More formally, $\mathbb{Q} \subseteq \mathbb{R}$.

henlo[3]

[3] …this section will be expanded later…