8 The Important Number Sets

At this point, we have developed a basic understanding of arithmetic with natural numbers. We defined two basic operations on $\mathbb{N}$—namely addition and multiplication—and investigated enough properties for us to know that $\mathbb{N}$ is an *ordered semiring*. Let's briefly summarize these important properties.

8.1 The Natural Numbers

We summarize here the various important algebraic properties of the set of natural numbers $\mathbb{N}$ with the addition $+$ and multiplication $\cdot$ operations we have defined on it.

Theorem 8.1: The Natural Numbers with Addition are a Commutative Monoid.

- $(0 \in \mathbb{N}) \wedge (\forall n \in \mathbb{N})(0 + n = n + 0 = n)$. *existence of identity element*
- $(\forall x, y, z \in \mathbb{N})\big(x + (y + z) = (x + y) + z\big)$. *associativity*
- $(\forall x, y \in \mathbb{N})(x + y = y + x)$. *commutativity*

Theorem 8.2: The Natural Numbers with Multiplication are a Commutative Monoid.

- $(1 \in \mathbb{N}) \wedge (\forall n \in \mathbb{N})(1 \cdot n = n \cdot 1 = n)$. *existence of identity element*
- $(\forall x, y, z \in \mathbb{N})\big(x \cdot (y \cdot z) = (x \cdot y) \cdot z\big)$. *associativity*
- $(\forall x, y \in \mathbb{N})(x \cdot y = y \cdot x)$. *commutativity*

Theorem 8.3: The Natural Numbers are a Commutative Semiring.

- $(\forall x, y, z \in \mathbb{N})\big(x \cdot (y + z) = (x \cdot y) + (x \cdot z)\big)$. *distributivity*
- $(\forall x \in \mathbb{N})(0 \cdot x = x \cdot 0 = 0)$. *the additive identity is a multiplicative annihilator*

Theorem 8.4: The Natural Numbers are an Ordered Semiring.

- $(\forall x, y, z \in \mathbb{N})\big(x < y \iff x + z < y + z\big)$. *monotonicity of addition*
- $(\forall x, y, z \in \mathbb{N})\big(z \neq 0 \Rightarrow (x < y \iff x \cdot z < y \cdot z)\big)$. *monotonicity of multiplication*

Although we do not know how to *subtract* natural numbers from each other, we do know that we can *add* or *cancel* the same number from both sides of an equality.

Theorem 8.5: Addition on the Natural Numbers is Cancellative.
$(\forall x, y, z \in \mathbb{N})\big(x + z = y + z \iff x = y\big)$.

Similarly, even though we do not know what *division* means for natural numbers, we can still *multiply* or *cancel* the same *nonzero* number from both sides of an equality.

Theorem 8.6: Multiplication on the Natural Numbers is Cancellative.
$(\forall x, y, z \in \mathbb{N})\big(z \neq 0 \Rightarrow (x \cdot z = y \cdot z \iff x = y)\big)$.

Finally, there are no *nonzero zero-divisors* in the set of natural numbers.

Theorem 8.7: There are no Nonzero Zero-Divisors.
$(\forall x, y \in \mathbb{N})\Big(x \cdot y = 0 \Rightarrow \big((x = 0) \vee (y = 0)\big)\Big)$.

8.2 The Integral Numbers

It is clearly frustrating to not be able to subtract natural numbers from each other. In order to describe subtraction as an *operation* similar to addition and multiplication, we would expect to be able to subtract *any* two arbitrary natural numbers from each other, and we would also expect this subtraction to result in *another* natural number.

However, using our intuitive understanding of "subtraction" from grade school, we can not subtract 5 from 4 because $4 - 5$ would not be a natural number. But we ***want*** to.

The fundamental problem is that some natural numbers do not have *additive inverses.* Given $x \in \mathbb{N}$ and $y \in \mathbb{N}$, we say y is an *additive inverse for x iff* $x + y = 0 = y + x$. The solution, then, is to augment $\mathbb{N}$ with an additive inverse for each of its elements.[1] We will call this augmented set *the set of integers* and denote it with the symbol $\mathbb{Z}$. Informally, we usually say $\mathbb{Z} := \mathbb{N} \cup \{-x \mid x \in \mathbb{N}\}$. For example, the additive inverse of the integer 2 is the integer denoted by -2. If the motivation so far has made sense, it will feel natural to work under the presumption that $\mathbb{N} \subseteq \mathbb{Z}$.[2]

+ inverse

$\mathbb{Z}$

Unfortunately, we do not have time to describe *how* this augmentation process can be done, but rest assured that it *can* be done in a consistent way within the confines of Zermelo-Fraenkel set theory. For this reason, we will not *formally* define what an integer is, nor will we *formally* define addition, multiplication, or inequality on the integers. With this understanding, we will suppose that $\mathbb{Z}$ inherits all of the arithmetic and algebraic operations and theorems[3] that we discussed about the natural numbers —making $\mathbb{Z}$ an *ordered semiring* just like $\mathbb{N}$ is—along with one additional property.[4]

Theorem 8.8: The Integers with Addition are a Group.
$(\forall x \in \mathbb{Z})\big(\exists! y \in \mathbb{Z}\big)\big(x + y = 0\big)$.

It can be easily shown that $x \neq -x$ for all $x \in \mathbb{Z} \setminus \{0\}$, and that $-0 = 0$; so, the integers can be partitioned into the *positives,* the *negatives,* and *zero.* The positives and zero are all just natural numbers, and they obey all the same rules that we studied about natural numbers. We will now detail how the negative integers interact with the rest of the integers. First, the partial order $\leqslant$ from $\mathbb{N}$ extends to $\mathbb{Z}$ as follows.

Lemma 8.1.
$(\forall x \in \mathbb{Z})(0 < x \iff -x < 0)$.

positive
negative

For any arbitrary integer $x \in \mathbb{Z}$, we will say that x is *positive iff* $x > 0$, and we will define x to be *negative iff* $x < 0$. Notice that 0 is neither positive nor negative. Further, the interaction between negative numbers and multiplication is captured below.

Theorem 8.9.
For any $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$, the following equivalences hold.

- $(x \cdot y > 0) \iff \big((x > 0 \land y > 0) \lor (x < 0 \land y < 0)\big)$.
- $(x \cdot y < 0) \iff \big((x > 0 \land y < 0) \lor (x < 0 \land y > 0)\big)$.
- $(x \cdot y = 0) \iff (x = 0 \lor y = 0)$.

Theorem 8.10.
For all $x, y, z \in \mathbb{Z}$, we have the following.

- $(x < y \land 0 < z) \Rightarrow (x \cdot z < y \cdot z)$.
- $(x < y \land 0 > z) \Rightarrow (x \cdot z > y \cdot z)$.

Definition 8.1: Subtraction.
For every $x, y \in \mathbb{Z}$ we define *difference between x and y* by $x - y := x + (-y)$.

Lemma 8.2: Subtraction is not Associative.
$(\exists x, y, z \in \mathbb{Z})\big(x - (y - z) \neq (x - y) - z\big)$.

Lemma 8.3: Subtraction is not Commutative.
$(\exists x, y \in \mathbb{Z})(x - y \neq y - x)$.

[1] Since the notion of an "inverse" here is being considered with respect to *addition,* we usually denote the inverse of a number x by $-x$, calling it the "negative" of x.

[2] This is not ***technically*** *true* in ZF set theory, but it is *true* ***in spirit*** and will massively simplify our discussion during this section. We will make similar concessions for the rest of the number sets discussed here.

[3] … meaning that $+$ and $\cdot$ are both associative and commutative on $\mathbb{Z}$, and 0 and 1 are the respective identities corresponding to those operations, and $\cdot$ distributes over $+$, *et cetera*…

[4] This property elevates $\mathbb{Z}$ from a *semiring* into a *ring.*

8.3 The Rational Numbers

Now that we have added *additive* inverses to $\mathbb{N}$, producing $\mathbb{Z}$, we can ask the same question about the other important operation we have been discussing: *multiplication.*[5] Ideally, we would want to define, for each integer x, a *multiplicative inverse* x^{-1} so that $x \cdot x^{-1} = 1$. However, unlike with addition, we must be a little more careful with multiplication because of the fact that zero is a *multiplicative annihilator:* if 0 had a multiplicative inverse 0^{-1}, then $0 \cdot 0^{-1} = 1$ by definition, but also $0 \cdot 0^{-1} = 0$ because we are multiplying by zero, which would imply $0 = 1$. ↯ Thankfully, this is the only problematic element—we can go ahead and define multiplicative inverses for every *nonzero* integer,[6] and the resulting set of numbers we call the set of *rational numbers*, which we denote by the symbol $\mathbb{Q}$. Traditionally, we define consider a rational number to be a *quotient* $\frac{x}{y}$, where $x \in \mathbb{Z}$ and $y \in \mathbb{N} \setminus \{0\}$, leading us to the informal definition $\mathbb{Q} := \left\{ \frac{x}{y} \,\middle|\, x \in \mathbb{Z} \wedge y \in \mathbb{N} \setminus \{0\} \right\}$. Here, we call x the *numerator* and y the *denominator.*

· *inverse*

$\mathbb{Q}$

$\frac{x}{y}$

[5]In contrast to the notation we used with addition, we usually denote the *multiplicative* inverse of a number x by x^{-1}. In general, this is the notation used for inverses with respect to arbitrary operations.

[6]This property elevates $\mathbb{Q}$ from a *ring* into a *field.*

Again, we will proceed under the presumption that $\mathbb{Z} \subseteq \mathbb{Q}$ by identifying the integer $x \in \mathbb{Z}$ with the rational number $\frac{x}{1} \in \mathbb{Q}$. With this idea in mind, given two rational numbers $\frac{x_1}{y_1} \in \mathbb{Q}$ and $\frac{x_2}{y_2} \in \mathbb{Q}$, we will define their sum and product as follows.

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} := \frac{x_1 y_2 + x_2 y_1}{y_1 \cdot y_2}$$
$$\frac{x_1}{y_1} \cdot \frac{x_2}{y_2} := \frac{x_1 \cdot x_2}{y_1 \cdot y_2}$$

Also, given a rational number $\frac{x \cdot z}{y \cdot z} \in \mathbb{Q}$, we will identify $\frac{x \cdot z}{y \cdot z} = \frac{x}{y}$. With this understanding, we can see $\frac{0}{1}$ and $\frac{1}{1}$ are the additive and multiplicative *identities* respectively.

Theorem 8.11: The Rationals with Multiplication are a Group.
$(\forall p \in \mathbb{Q})(\exists! q \in \mathbb{Q})\left(p \cdot q = \frac{1}{1}\right)$.

To compare two rationals $\frac{x_1}{y_1}, \frac{x_2}{y_2} \in \mathbb{Q}$ to each other—extending the partial order $\leqslant$ from $\mathbb{Z}$ to $\mathbb{Q}$—we compare their numerators after ensuring they have the same denominator.

$$\frac{x_1}{y_1} < \frac{x_2}{y_2} \quad :\Leftrightarrow \quad x_1 \cdot y_2 < x_2 \cdot y_1$$

8.4 The Real Numbers

$\mathbb{R}$

There are two common ways to construct the set of *real numbers* $\mathbb{R}$ out of the rationals by *"completing"* them in one of two ways. In the first way, we want to ensure that every bounded set of rationals has a *least upper bound;* this leads to the construction of the reals using *Dedekind cuts.* In the second way, we want to ensure that every *Cauchy convergent* sequence of rational numbers *actually* converges; this leads what is known as the *Cauchy sequences* construction. In order to not distract from our focus in this course, we won't detail these approaches here. The point is that the set of real numbers $\mathbb{R}$ contains every *"non-imaginary"* number you've probably ever heard of throughout grade school, and $\mathbb{R}$ has all of the algebraic properties you would expect it to have. This is the last number set we are interested in covering; we summarize the *"spiritual"* relationship between these sets as follows.

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

8.5 Some Notable Functions

For convenience, we make the following definitions as abbreviations for the various sets of numbers we've introduced.

$$\begin{aligned}
\mathbb{N}_{\geqslant 0} &:= \{n \in \mathbb{N} \mid 0 \leqslant n\} = \mathbb{N} & \mathbb{Q}_{\geqslant 0} &:= \{q \in \mathbb{Q} \mid 0 \leqslant q\} \\
\mathbb{N}_{+} &:= \{n \in \mathbb{N} \mid 0 < n\} = \mathbb{N} \setminus \{0\} & \mathbb{Q}_{+} &:= \{q \in \mathbb{Q} \mid 0 < q\} \\
\mathbb{N}_{-} &:= \{n \in \mathbb{N} \mid n < 0\} = \varnothing & \mathbb{Q}_{-} &:= \{q \in \mathbb{Q} \mid q < 0\} \\
\mathbb{Z}_{\geqslant 0} &:= \{z \in \mathbb{Z} \mid 0 \leqslant z\} = \mathbb{N} & \mathbb{R}_{\geqslant 0} &:= \{r \in \mathbb{R} \mid 0 \leqslant r\} \\
\mathbb{Z}_{+} &:= \{z \in \mathbb{Z} \mid 0 < z\} = \mathbb{N}_{+} & \mathbb{R}_{+} &:= \{r \in \mathbb{R} \mid 0 < r\} \\
\mathbb{Z}_{-} &:= \{z \in \mathbb{Z} \mid z < 0\} = \mathbb{N}_{-} & \mathbb{R}_{-} &:= \{r \in \mathbb{R} \mid r < 0\}
\end{aligned}$$

Definition 8.2: Absolute Value Function.
The *absolute value* function $|\square| : \mathfrak{A} \to \mathfrak{A}_{\geqslant 0}$ is given, for every $x \in \mathfrak{A}$, as follows below.

$|\square|$

$$|x| := \begin{cases} x & \text{if } 0 \leqslant x \\ -x & \text{if } x < 0 \end{cases}$$

Definition 8.3: Max & Min Functions.
Let $\mathfrak{A} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$, and let $A \subseteq \mathfrak{A}$ such that $A \neq \varnothing$. We say that A is *bounded above iff* $(\exists b \in \mathfrak{A})(\forall a \in A)(a \leqslant b)$, and A has a *maximal element iff* $(\exists b \in A)(\forall a \in A)(a \leqslant b)$.

maximal

`max` When A contains a maximal element $M \in A$, we define $\mathtt{max}(A) := M$. Because $\leqslant$ is *antisymmetric,* this maximal element is unique, making `max` a well-defined function.

Similarly, we say that A is *bounded below iff* $(\exists b \in \mathfrak{A})(\forall a \in A)(b \leqslant a)$, and we say that A contains a *minimal element iff* $(\exists b \in A)(\forall a \in A)(b \leqslant a)$.

minimal

`min` When A contains a minimal element $m \in A$, we define $\mathtt{min}(A) := m$. Because $\leqslant$ is *antisymmetric,* this minimal element is unique, making this a well-defined function.

Definition 8.4: Floor & Ceiling Functions.
Let $\mathfrak{A} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$.
The *floor* function $\lfloor\square\rfloor : \mathfrak{A} \to \mathbb{Z}$ is given by the following mapping for every $x \in \mathfrak{A}$.

$\lfloor\square\rfloor$

$$\lfloor x \rfloor := \mathtt{max}\big(\{z \in \mathbb{Z} \mid z \leqslant x\}\big)$$

The *ceiling* function $\lceil\square\rceil : \mathfrak{A} \to \mathbb{Z}$ is given by the following mapping for every $x \in \mathfrak{A}$.

$\lceil\square\rceil$

$$\lceil x \rceil := \mathtt{min}\big(\{z \in \mathbb{Z} \mid x \leqslant z\}\big)$$

Definition 8.5: Square Root Function.
Let $\mathfrak{A} \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$. The *square root* function $\sqrt{\square} : \left\{a^2 \,\middle|\, a \in \mathfrak{A}\right\} \to \mathfrak{A}$ is given by the following mapping for each $x \in \left\{a^2 \,\middle|\, a \in \mathfrak{A}\right\}$.

$\sqrt{\square}$

$$\sqrt{x} := y \quad \text{where } y \in \mathfrak{A} \text{ such that } x = y^2$$

Definition 8.6: Logarithm Function.
Let $b \in \mathbb{R}_{\geqslant 0}$ such that $b \neq 0$ and $b \neq 1$.
The *base b logarithm* is the function $\log_b(\square) : \mathbb{R}_+ \to \mathbb{R}$ defined for each $x \in \mathbb{R}_+$ below.

$\log_b(\square)$

$$\log_b(x) := y \quad \text{where } y \in \mathbb{R} \text{ such that } b^y = x$$