6 *Repeating Ourselves*

Although we have not formally introduced the notion of a *"function,"* we have already encountered many examples of things that behave like *"functions."* In this section, we will continue to treat the concept of a *"function"* informally,[1] but we have already encountered many examples of things that *"behave like functions."* In particular, the operations $+$ and $\cdot$ that we have defined behave like *binary* functions, in that they take *two* natural number inputs and produce exactly one natural output.

[1] We will soon encounter this more formally, but the time is not yet ripe.

Definition 6.1: Exponentiation.
For every pair of natural numbers n and m, we define the following binary operation.

$$\begin{aligned} n^0 &:= 1 \\ n^{\mathfrak{suc}(m)} &:= n^m \cdot n \end{aligned}$$

x^y

We call this binary operation *exponentiation* and use the notation x^y to denote the exponential *"x raised to the power y"* when x and y are natural numbers. As we did with multiplication, we will take the convention that exponentition has *higher precedence* than both *multiplication* and *addition,* so expressions like $w + x^y \cdot z$ can be parsed unambiguously as $w + ((x^y) \cdot z)$ despite the lack of parentheses. ⌟

As a first matter, note $\forall x(x = x^1)$. The computation below should be convincing.

$$x^1 = x^{\mathfrak{suc}(0)} = x^0 \cdot x = 1 \cdot x = x$$

Now, this operation is of a different kind than the ones that we've encountered so far in several ways. Most obviously—as is heavily implied by the notation we introduced—exponentiation is ***not commutative!*** For example, $2^3 = 8 \neq 9 = 3^2$.

Exponentiation is also ***not associative!*** By convention, the notation for exponentiation is implicitly *"associative to the right,"* which means that an expression like a^{b^c} should be parsed as $a^{(b^c)}$. To make this clear, the following example writes the implied parentheses explicitly.

$$2^{\left(3^2\right)} = 2^9 = 512 \neq 64 = 8^2 = \left(2^3\right)^2$$

Instead, exponentials interact with multiplication in several ways that might seem unintuitive if we do not keep in mind that it really is just repeated multiplication.

Lemma 6.1.
Repeated (left-associated) powers can be simplified as products in the exponent.

$$\forall x \forall y \forall z \left((x^y)^z = x^{y \cdot z} \right)$$ ⌟

Lemma 6.2: Exponentiation is Homomorphic.
Exponentials split multiplicatively over sums.

$$\forall x \forall y \forall z \left(x^{y+z} = x^y \cdot x^z \right)$$ ⌟

Lemma 6.3: Distributivity of Exponentiation over Multiplication.
Raising a product of two natural numbers to a power is equivalent to taking the product of each of the factors individually raised to that power.

$$\forall x \forall y \forall z \left((x \cdot y)^z = x^z \cdot y^z \right)$$

It is important to note that, because *exponentiation is* ***not commutative****,* distributivity does not work from the *left;* it only works from the *right* as stated above. ⌟

Distributing exponentiation over multiplication *from the left* would look something like $x^{y \cdot z} = x^y \cdot x^z$, and this is clearly not *true* for all natural numbers x, y, and z. Look.

$$2^{2 \cdot 3} = 2^6 = 64 \neq 32 = 4 \cdot 8 = 2^2 \cdot 2^3$$

There is one more important way in which the exponential map is similar to addition and multiplication: it is an *increasing* function.[1] When we described this property for addition and multiplication, we called it *"monotonicity."* As a reminder, we expressed the monotonicity of addition as follows: for every pair of natural numbers x and y, if $x \leqslant y$, then $x + z \leqslant y + z$ for every natural number z. The thing to notice here is that adding the same quantity on both sides of an inequality *preserves the inequality.* This is precisely the property that exponentiation with a fixed natural base $b \geqslant 1$ has.

[1] In fact, it is ***strictly*** *increasing* as opposed to merely ***monotonically*** *increasing.* The difference between the two depends on whether we are asserting a *strict* or *weak* inequality. In general, a function f is *monotonically increasing iff* $x < y \Rightarrow f(x) \leqslant f(y)$ for every x and y. We say that f is *strictly increasing iff* $x < y \Rightarrow f(x) < f(y)$ for every x and y in its domain.

Lemma 6.4: Exponentiation is a Strictly Increasing Function.
Let b be a natural number such that $b \geqslant 2$. Then, using b as the base of an exponential on both sides of an inequality preserves that inequality.

$$\forall x \forall y (x < y \Rightarrow b^x < b^y)$$

⌟

Since $\forall x \forall y (x < y \Rightarrow x \leqslant y)$, the theorems we have discussed regarding monotonicity of addition, multiplication, and now exponentiation apply to both weak and strict inequalities. However, notice *Lemma 6.4* does not hold when $b = 0$.

One final important property the exponential map has—which it shares in common with the $\mathfrak{suc}(\circlearrowleft)$ functional—is that it can *never produce zero* as an output (except in the special case when the base of the exponential is zero). In fact, the exponential map with a nonzero base is *always positive.*

Lemma 6.5: Exponentials are Always Positive.
Let b be a natural number such that $b \neq 0$. The following then holds.

$$\forall n (b^n \neq 0)$$

This immediately implies $\forall n (b^n > 0)$ because $\forall n (n = 0 \vee \exists m (n = \mathfrak{suc}(m)))$. ⌟

6.1 *Inversion*

Theorem 6.1: Addition is Cancellative.
Eliminating the same summand from both sides of an equation preserves equality.

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

⌟

Definition 6.2: Differences.
Given two natural numbers x and y satisfying the relation $x \geqslant y$, we know that there exists a natural number k such that $x = y + k$. In such situations, we define the *difference between x and y* to be $x - y \coloneqq k$. ⌟

$x - y$

Lemma 6.6. For all n and m, if $n \geqslant m$, then $(n - m) + m = n$ and $(n + m) - m = n$. *Addition and subtraction cancel out.*

Lemma 6.7. For all x, y, and z, if $y \geqslant z$, then $x + (y - z) = (x + y) - z$. *Addition and subtraction associate.*

Lemma 6.8. For all x, y, and z, if $y \geqslant z$, then $x \cdot (y - z) = (x \cdot y) - (x \cdot z)$. *Products distribute over differences.*

Theorem 6.2: Multiplication is Cancellative.
Eliminating a *nonzero* factor from both sides of an equation preserves equality.

$$\forall x \forall y \forall z \Big(\big((x \cdot z = y \cdot z) \wedge (z \neq 0) \big) \Rightarrow x = y \Big)$$

⌟

Definition 6.3: Logarithms.
Let b be a natural number such that $b \geqslant 2$. Let x be a natural number and suppose that $x = b^y$ for some natural number y. In such situations, we define the *base-b logarithm* of x to be $\log_b(x) := y$. ⌟

$\log_b(x)$

It is important to note that $\log_b(x)$ is *only* defined when x is a power of b; in those situations, $\log_b(x)$ represents the natural number y that you would have to raise b to in order to obtain x. This means that $\log_b(x)$ for a fixed base $b \geqslant 2$ is ***not necessarily defined*** for every natural number x. The reason it makes sense to think of this as a *"function"* is actually because the exponential map with base $b \geqslant 2$ always maps *distinct inputs* to *distinct outputs:* $(x \neq y) \Rightarrow (b^x \neq b^y)$ for every x and y. This allows us to think about *"undoing"* the exponential—taking the *"inverse"* exponential.

Lemma 6.9: Logarithms are Inverse Exponentials.
Let b be a natural number satisfying $b \geqslant 2$. Base-b logarithms undo base-b powers.

$$\forall x \big(\log_b(b^x) = x \big)$$

Taking the base-b exponential of a base-b logarithm[1] is equivalent to doing nothing.

[1] *This is only possible for powers of b!*

$$\forall x \Big(\exists y (x = b^y) \Rightarrow \big(b^{\log_b(x)} = x \big) \Big)$$

⌟

Because $\log_b(\circlearrowleft)$ behaves like an *"inverse"* for $b^{\circlearrowleft}$, it has a relationship with addition and multiplication similar to that of exponentiation, but in the *"reverse"* direction.

Lemma 6.10.
Let b be a natural number such that $b \geqslant 2$, and suppose x is a natural number satisfying the condition $\exists y (x = b^y)$. Then, raising x to a power within a logarithm is equivalent to linearly scaling that logarithm by the power.

$$\forall n \big(\log_b(x^n) = n \cdot \log_b(x) \big)$$

⌟

Lemma 6.11: Logarithms are Homomorphic.
Let b be a natural number such that $b \geqslant 2$. Suppose x and y are arbitrary natural numbers satisfying $\exists z (x = b^z)$ and $\exists z (y = b^z)$. The following equality then holds.

$$\log_b(x \cdot y) = \log_b(x) + \log_b(y)$$

This tells us that logarithms split additively over products when possible. ⌟

Theorem 6.3: Change of Base.
Let k and ℓ be natural numbers such that $k \geqslant 2$ and $\ell \geqslant 2$ satisfying the condition $\exists j (\ell = k^j)$. Then, for any natural number x satisfying $\exists y (x = k^y)$ and $\exists y (x = \ell^y)$, the following identity holds.

$$\log_k(\ell) \cdot \log_\ell(x) = \log_k(x)$$

⌟

These theorems about logarithms all have various preconditions requiring certain numbers to be powers of other numbers, which is unfortunately necessary because

our universe of discourse contains *only* natural numbers. However, as it turns out, these theorems are all still *true* in *any* algebraic structure that implements *"addition"* $\bigcirc + \bigcirc$, *"multiplication"* $\bigcirc \cdot \bigcirc$, and *"exponentiation"* $\bigcirc^{\bigcirc}$ consistent with the operations we have studied for natural numbers. This means that, in the future, if we were to consider an algebraic structure like the *real numbers,* for example, these theorems would become much more powerful (because the preconditions to all of these theorems would be satisfied *almost always* in a structure like the *reals.*)

6.2 *Iteration*

Definition 6.4: Iterated Sums.
Given an arbitrary sequence of natural numbers a_0, a_1, a_2, …, and any two natural numbers n and m, we recursively define below what it means to iterate the addition operation $+$ over a contiguous finite segment of this sequence using the Σ symbol.

$$\begin{aligned}
\sum_{i=n+\mathfrak{suc}(m)}^{n} a_i &:= 0 \\
\sum_{i=n}^{n+0} a_i &:= a_n \\
\sum_{i=n}^{n+\mathfrak{suc}(m)} a_i &:= \left(\sum_{i=n}^{n+m} a_i\right) + a_{n+\mathfrak{suc}(m)}
\end{aligned}$$

Let's briefly explain the notation above by looking at the *second* and *third* lines first; we will return to the *first* line afterwards. The Σ represents the fact that we are iterating the $+$ operation; above and below Σ are the *"limits"* of this summation. The *"lower limits of summation"* for the second and third line look something like $i = n$, indicating that the variable i within the *"body"* of the summation begins at n. We then iterate through the values in the sequence a_n, a_{n+1}, a_{n+2}, … until the reach the *"upper limit of summation,"* applying the $+$ operation as we go.

The *base case* of our recursion is on the second line. Here, the upper limit is $n + 0$, which is just n; this means we begin at a_n and stop at a_n, so our result is just the n^{th} term in the sequence a_n.

The *recursive case* of our definition is on the third line. There, the upper limit is $n + \mathfrak{suc}(m)$, indicating we start from the n^{th} term in the sequence and continue until the $(n + \mathfrak{suc}(m))^{\text{th}}$ term, computing the following.

$$\begin{aligned}
a_n + a_{n+1} + ... + a_{n+m} + a_{n+\mathfrak{suc}(m)} &= \left(a_n + a_{n+1} + ... + a_{n+m}\right) + a_{n+\mathfrak{suc}(m)} \\
&= \left(\sum_{i=n}^{n+m} a_i\right) + a_{n+\mathfrak{suc}(m)}
\end{aligned}$$

Now, returning to the first line: this represents a *degenerate case*—corresponding to what's typically called an *"empty sum"*—in which the lower limit of summation is *strictly greater* than the upper limit of summation. In this situation, we want to define this in such a way that the *"empty sum"* captures the idea of *"doing nothing."* Since zero—the additive identity—is the number that corresponds with *"doing nothing*

with respect to addition," it should feel perfectly reasonable to define the output of an empty sum to be 0, a number that does nothing with respect to the iterated operation.

Lemma 6.12: Gauss' Little Formula.
For every natural number n, we have $2 \cdot \sum_{i=0}^{n} i = n \cdot (n+1)$. ⌟

Proof. We will show $2 \cdot \sum_{i=0}^{n} i = n \cdot (n+1)$ by induction.

Basis Step:
We need to show $2 \cdot \sum_{i=0}^{0} i = 0 \cdot (0+1)$. Witness now the following argument.

$$\begin{aligned}
2 \cdot \sum_{i=0}^{0} i &= 2 \cdot 0 && \text{by definition of } \Sigma \\
&= 0 && \text{since } \forall x(x \cdot 0 = 0) \\
&= 0 \cdot 1 && \text{since } \forall x(0 \cdot x = 0) \\
&= 0 \cdot (0+1) && \text{because } \forall x(0 + x = x)
\end{aligned}$$

It should now be clear that $2 \cdot \sum_{i=0}^{0} i = 0 \cdot (0+1)$ as desired.

Inductive Step:
Let k be a natural number. Assume that $2 \cdot \sum_{i=0}^{k} i = k \cdot (k+1)$. We now need to show that $2 \cdot \sum_{i=0}^{k+1} i = (k+1) \cdot ((k+1)+1)$. We begin on the left and observe.

$$\begin{aligned}
2 \cdot \sum_{i=0}^{k+1} i &= 2 \cdot \left(\left(\sum_{i=0}^{k} i \right) + (k+1) \right) && \text{by definition of } \Sigma \\
&= 2 \cdot \left(\sum_{i=0}^{k} i \right) + 2 \cdot (k+1) && \text{by distributivity of } \cdot \text{ over } + \\
&= k \cdot (k+1) + 2 \cdot (k+1) && \text{by the } \textit{inductive hypothesis} \\
&= (k+1) \cdot k + (k+1) \cdot 2 && \text{by commutativity of } \cdot \\
&= (k+1) \cdot (k+2) && \text{by distributivity of } \cdot \text{ over } + \\
&= (k+1) \cdot \big(k + (1+1)\big) && \text{because } 1+1 = 2 \\
&= (k+1) \cdot \big((k+1)+1\big) && \text{by associativity of } +
\end{aligned}$$

As a result, we have $2 \cdot \sum_{i=0}^{k+1} i = (k+1) \cdot ((k+1)+1)$ as desired.

We therefore conclude $2 \cdot \sum_{i=0}^{n} i = n \cdot (n+1)$ for every natural number n by *Axiom 4.*
QED

Theorem 6.4: Geometric Sums Formula.
Let x be an arbitrary natural number x such that $x > 0$. Then, for every natural number n, the following equality holds.

$$(x-1) \cdot \sum_{i=0}^{n} x^i = x^{n+1} - 1$$ ⌟

Proof. Fix an arbitrary natural number x such that $x > 0$. We proceed by induction.

Basis Step:
We will first prove that $(x-1) \cdot \sum_{i=0}^{0} x^i = x^{0+1} - 1$. Let us observe.

$$\begin{aligned}
(x-1)\cdot\sum_{i=0}^{0}x^i &= (x-1)\cdot\left(x^0\right) && \text{by definition of } \Sigma\\
&= (x-1)\cdot 1 && \text{by definition of exponentiation}\\
&= x-1 && \text{since } \forall n(n\cdot 1=n)\\
&= x^1-1 && \text{since } \forall n\left(n=n^1\right)\\
&= x^{0+1}-1 && \text{because } 0+1=1
\end{aligned}$$

This then shows us that $(x-1)\cdot\sum_{i=0}^{0}x^i = x^{0+1}-1$, which is what we needed.

Inductive Step:
Let k be a natural number. Assume $(x-1)\cdot\sum_{i=0}^{k}x^i = x^{k+1}-1$. Check this out.

$$\begin{aligned}
(x-1)\cdot\sum_{i=0}^{k+1}x^i &= (x-1)\cdot\left(\sum_{i=0}^{k}x^i + x^{k+1}\right) && \text{by definition of } \Sigma\\
&= (x-1)\cdot\sum_{i=0}^{k}x^i + (x-1)\cdot x^{k+1} && \text{by distributing } \cdot \text{ over } +\\
&= \left(x^{k+1}-1\right) + (x-1)\cdot x^{k+1} && \text{by the } \textit{inductive hypothesis}
\end{aligned}$$

The rest is just simplification. We show those details below.

$$\begin{aligned}
\left(x^{k+1}-1\right) + (x-1)\cdot x^{k+1} &= \left(x^{k+1}-1\right) + x^{k+1}\cdot(x-1) && \text{by commutativity of } \cdot\\
&= \left(x^{k+1}-1\right) + \left(x^{k+1}\cdot x - x^{k+1}\cdot 1\right) && \text{by distributing } \cdot \text{ over } -\\
&= \left(x^{k+1}-1\right) + \left(x^{(k+1)+1} - x^{k+1}\cdot 1\right) && \text{by definition of exponentiation}\\
&= \left(x^{k+1}-1\right) + \left(x^{(k+1)+1} - x^{k+1}\right) && \text{since } \forall n(n\cdot 1=n)\\
&= \left(x^{(k+1)+1} - x^{k+1}\right) + \left(x^{k+1}-1\right) && \text{by commutativity of } +\\
&= \left(\left(x^{(k+1)+1} - x^{k+1}\right) + x^{k+1}\right) - 1 && \text{by associativity of } + \text{ with } -\\
&= x^{(k+1)+1} - 1 && \text{by } \forall n\forall m\left(m\leqslant n \Rightarrow (n-m)+m=n\right)
\end{aligned}$$

Finally, this shows $(x-1)\cdot\sum_{i=0}^{k+1}x^i = x^{(k+1)+1}-1$, finishing our inductive step.

We therefore conclude $(x-1)\cdot\sum_{i=0}^{n}x^i = x^{n+1}-1$ for every n by *Axiom 4*.

QED

Definition 6.5: Iterated Products.
Given an arbitrary sequence of natural numbers a_0, a_1, a_2, …, and any two natural numbers n and m, we recursively define below what it means to iterate multiplication $\cdot$ over a contiguous finite segment of this sequence using the Π symbol.

Π

$$\begin{aligned}
\prod_{i=n+\mathfrak{suc}(m)}^{n} a_i &:= 1\\
\prod_{i=n}^{n+0} a_i &:= a_n\\
\prod_{i=n}^{n+\mathfrak{suc}(m)} a_i &:= \left(\prod_{i=n}^{n+m} a_i\right)\cdot a_{n+\mathfrak{suc}(m)}
\end{aligned}$$

⌟