Math From Scratch Lesson 35: Polynomials

W. Blaine Dowler

August 31, 2013

Contents

1 Defining Polynomials **1**

2 Working with Polynomials **2**
2.1 Addition . . . 2
2.1.1 Closure . . . 3
2.1.2 Commutativity . . . 4
2.1.3 Associativity . . . 4
2.1.4 Existence of Identity . . . 4
2.1.5 Existence of Inverses . . . 5
2.2 Distributive Property . . . 5
2.3 Multiplication . . . 6
2.3.1 Closure . . . 6
2.3.2 Commutativity . . . 7
2.3.3 Associativity . . . 7
2.3.4 Existence of Identity . . . 8
2.3.5 Existence of Inverses . . . 8

3 Conclusion **9**

4 Next Lesson **9**

1 Defining Polynomials

Exponents were first introduced in lesson 6, and they will come heavily into play now. We will find it convenient to define *polynomials* for our future work. These are combinations of parameters and variables which can be either finite or

infinite, and which often represent physical quantities. Polynomials in a single variable can be expressed in the form:

$$P(x) = \sum_{n=0}^{N} a_n x^n = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_N x^N$$

where $P(x)$ is our polynomial, the various $a_n \in \mathbb{Z}$ are parameters, $x \in \mathbb{R}$ is our variable and N is the highest exponent of x, also known as the *order* of the polynomial. Note that N need not be a finite number, although it does need to be a whole number. This is true in the formal sense: $N \in \mathbb{W}$.

2 Working with Polynomials

It is worth nothing that polynomials form an algebra. One might instinctively assume that, since each polynomial is constructed of real numbers (which form an algebraic field) that polynomials would also form an algebraic field. They do not. To study them in detail, we must find logical ways to define the addition and multiplication of polynomials.

Let us begin with three polynomials, denoted

$$P(x) = \sum_{n=0}^{N} a_n x^n = a_0 x^0 + a_1 x^1 + a_2 x^2 + \ldots + a_N x^N$$

and

$$Q(x) = \sum_{n=0}^{M} b_n x^n = b_0 x^0 + b_1 x^1 + b^2 x^2 + \ldots + b_M x^M$$

and finally

$$R(x) = \sum_{n=0}^{L} c_n x^n = c_0 x^0 + c_1 x^1 + c^2 x^2 + \ldots + c_L x^L$$

Note that the parameters differ between the two, which is how we distinguish the polynomials, but the variables are indistinguishable. When comparing two polynomials, we need to have matching variables throughout for sensible comparisons. We will use these to define and test the rules of addition and multiplication for polynomials.

2.1 Addition

The goal is to find some meaning for "+" in the context of polynomials which is instinctive for the mathematician, meaningful and useful. To do so, we need

to define the functions $\max(i,j)$ and $\min(i,j)$ for $i,j \in \mathbb{W}$:

$$\max(i,j) = \begin{cases} i, i \geq j \\ j, i < j \end{cases}$$

and

$$\min(i,j) = \begin{cases} j, i \geq j \\ i, i < j \end{cases}$$

We may now develop a definition of addition for $P(x) + Q(x)$. We start by extending the definitions of both polynomials as follows: if $\max(M,N) = M$ (i.e. if the order of $Q(x)$ is greater than the order of $P(x)$, and therefore has more terms) then we extend $P(x)$ as follows: for all $N < n \leq M$, $a_n = 0$. Conversely, if $\min(M,N) = N$, then we set $b_n = 0$ for all $M < n \leq N$. With these extensions, we have ensured that both $P(x)$ and $Q(x)$ have the same order, without changing the actual value of either polynomial. With this extension, we can define the addition of polynomials $P(x)$ and $Q(x)$ as

$$P(x) + Q(x) = \sum_{n=0}^{\max(N,M)} (a_n + b_n) x^n$$

Let's look at an example: let $P(x) = 3x^2 + 5x + 2$ and $Q(x) = x^3 - 4x^2 + 7x + 1$. Then $P(x) + Q(x) = x^3 - x^2 + 12x + 3$.

The extension of the polynomials was required to make sure every sum $a_n + b_n$ is defined. We need to confirm that this is consistent with our known addition properties. The properties to check are closure, commutativity, associativity, existence of identity, and existence of inverses.

2.1.1 Closure

For each $a_n + b_n$, we can define d_n such that $a_n + b_n = d_n$. Thus,

$$P(x) + Q(x) = \sum_{n=0}^{\max(N,M)} d_n x^n$$

which is consistent with the definition of a polynomial. Thus, polynomials are closed under addition.

2.1.2 Commutativity

For each $a_n + b_n$, we can define d_n such that $a_n + b_n = d_n$. Thus,

$$P(x) + Q(x) = \sum_{n=0}^{\max(N,M)} (a_n + b_n) x^n = \sum_{n=0}^{\max(N,M)} d_n x^n$$

which is a polynomial. We can now compare this to

$$Q(x) + P(x) = \sum_{n=0}^{\max(N,M)} (b_n + a_n) x^n = \sum_{n=0}^{\max(N,M)} (a_n + b_n) x^n = \sum_{n=0}^{\max(M,N)} d_n x^n$$

Since each sum $a_n + b_n$ is commutative as a_n and b_n are real numbers, the polynomial as a whole is commutative. Thus, this addition property is also true for polynomials.

2.1.3 Associativity

This is remarkably similar in style to the commutativity proof. We instead define $a_n + b_n + c_n = d_n$ and associativity is a side effect of the associativity of the sums, as $(a_n + b_n) + c_n = a_n + (b_n + c_n)$. Thus, our definition of polynomial addition is associative.

2.1.4 Existence of Identity

This is also straightforward with the groundwork above. Since all previous definitions have worked by using the existing definitions, we can try the same technique here. Let us define the zero polynomial of order N as

$$0(x) = \sum_{n=0}^{N} 0 x^n$$

Thus,

$$P(x) + 0(x) = \sum_{n=0}^{\max(N,M)} a_n x^n = P(x)$$

and an identity exists.

2.1.5 Existence of Inverses

We continue with the current trend, starting with the existing $P(x)$ and defining

$$-P(x) = \sum_{n=0}^{N} -a_n x^n$$

Thus,

$$P(x) + (-P(x)) = \sum_{n=0}^{N} (a_n + (-a_n)) x^n = \sum_{n=0}^{N} 0x^n = 0(x)$$

and we see that all polynomials have inverses. To ensure that this definition of addition cannot, in fact, be a definition of multiplication, we ensure that $0(x)$ has an inverse. (Keep in mind, the multiplicative identity has no inverse.)

$$0(x) + 0(x) = \sum_{n=0}^{\max(N,M)} (0+0) x^n = 0(x)$$

Thus, $0(x)$ is self inverse, meaning $0(x) = -0(x)$.

We have a complete definition of addition for polynomials.

2.2 Distributive Property

In order to define multiplication for polynomials, we must first impose a property which includes multiplication in its definition. We must demand that the distributive property hold in order to define multiplication, such that:

$$P(x) \cdot (Q(x) + R(x)) = P(x) \cdot Q(x) + P(x) \cdot R(x)$$

Note that this is logically tenuous. We cannot prove the distributive property in isolation. We must instead assume it, define multiplication in some way, and then show that the definition of multiplication is consistent and valid in our definition. While this may seem illogical, the distributive property is an axiom, not an inherent result of an algebra. If we cannot produce a consistent definition of multiplication after assuming the distributive property, then we cannot have an algebra with multiplication and the distributive property, so we will be limited to groups, monoids, or other algebraic structures which have only one operation.

2.3 Multiplication

We now need to define multiplication to determine what kind of an algebra we are dealing with by defining multiplication. If we had only two terms to multiply, namely ax^N and bx^M, the product of these two real numbers would be abx^{N+M}. If we had only bx^M and $P(x)$, then the product would be given by the distributive property, such that

$$bx^M \cdot P(x) = \sum_{n=0}^{N} ba_n x^{n+M}$$

We can extend this notion by applying the distributive property in a termwise sense.

$$P(x) \cdot Q(x) = \sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j x^{i+j}$$

In the case of addition, the order of the sum was the maximum of the orders of the polynomials in the addition. In multiplication, the order becomes the sum of the orders of the polynomials factors. Let's look at an example: let $P(x) = 3x^2 + 5x + 2$ and $Q(x) = x^3 - 4x^2 + 7x + 1$. Then,

$$\begin{aligned} P(x) \cdot Q(x) &= \left(3x^2 + 5x + 2\right) \cdot \left(x^3 - 4x^2 + 7x + 1\right) \\ &= 2 + 14x - 8x^2 + 2x^3 + 5x + 35x^2 - 20x^3 + 5x^4 + 3x^2 + 21x^3 - 12x^4 + 3x^5 \\ &= 3x^5 - 7x^4 + 3x^3 + 30x^2 + 19x + 2 \end{aligned}$$

2.3.1 Closure

To demonstrate closure, we must show that the product of polynomial multiplication is, in every case, a polynomial itself. We can see by the example above that this is true in at least one case, but that does not necessarily prove that this is true in every case. Let us define terms d_n such that

$$d_n = \sum_{i=0}^{N+M} a_i \cdot b_{n-i}$$

With this definition in place, we can now see that

$$P(x) \cdot Q(x) = \sum_{j=0}^{N+M} d_j x^j$$

which is just another polynomial.

2.3.2 Commutativity

To show that polynomials commute under this form of multiplication, we need to show that $P(x) \cdot Q(x) = Q(x) \cdot P(x)$

$$\begin{aligned} P(x) \cdot Q(x) &= \sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j x^{i+j} \\ &= \sum_{j=0}^{N} \sum_{i=0}^{M} b_j a_i x^{j+i} \\ &= Q(x) \cdot P(x) \end{aligned}$$

2.3.3 Associativity

This is the challenge. We need to show that $(P(x) \cdot Q(x)) \cdot R(x) = P(x) \cdot (Q(x) \cdot R(x))$.

Now,

$$\begin{aligned} (P(x) \cdot Q(x)) \cdot R(x) &= \left(\sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j x^{i+j} \right) \cdot R(x) \\ &= \left(\sum_{i=0}^{N} \sum_{j=0}^{M} a_i b_j x^{i+j} \right) \cdot \left(\sum_{k=0}^{L} c_k x^k \right) \\ &= \sum_{i=0}^{N} \sum_{j=0}^{M} \sum_{k=0}^{L} (a_i b_j) c_k x^{i+j+k} \\ &= \sum_{i=0}^{N} \sum_{j=0}^{M} \sum_{k=0}^{L} a_i (b_j c_k) x^{i+j+k} \\ &= P(x) \cdot \left(\sum_{j=0}^{M} \sum_{k=0}^{L} b_j c_k x^{j+k} \right) \\ &= P(x) \cdot (Q(x) \cdot R(x)) \end{aligned}$$

Thus, polynomial multiplication is associative.

2.3.4 Existence of Identity

The identity is fairly straightforward. The identity polynomial is defined by $1(x) = \sum_{n=0}^{N} a_n x^n$ where $a_0 = 1$ and $a_n = 0 \forall n \in \mathbb{N}$. In other words,

$$1(x) = 1$$

This, combined with our definition of multiplication, satisfies the condition that

$$P(x)\,1 \cdot (x) = 1(x) \cdot P(x) = P(x)$$

Thus, the multiplicative identity exists.

2.3.5 Existence of Inverses

If inverses exist (for all but the zero polynomial) then we would need to find their general structure. Alternatively, we can find even a single example of a polynomial which cannot have an inverse, and therefore demonstrate that we cannot have inverses in general.

It is trivial to show that any zero order polynomial (except for the zero polynomial) has an inverse. The entire polynomial is thus nothing more than the real number a_0, so the inverse polynomial is ${a_0}^{-1}$, the inverse of the real number. We now look at first order polynomials to see if we can find an inverse to those.

We start with the polynomials $P(x) = a_0 + a_1 x$ and $Q(x) = \sum_{n=0}^{M} b_n x^n$. We need to find conditions on the various b_n, depending only upon a_0, a_1 and the order of $P(x)$, such that $P(x) \cdot Q(x) = 1$.

We begin with the constant term, or the zero order term: $a_0 \cdot b_0 = 1$. All other terms have x^m where $m \geq 1$. Thus, we have the condition that $b_0 = \frac{1}{a_0}$. Right here, we can see that there are polynomials without inverses: this condition alone ensures that any polynomial with a constant term of zero, such as $P(x) = x$, cannot have an inverse. This is because the order of the polynomial must be a whole number. If the order of a polynomial were permitted to be an integer, we'd have a chance, since we could have zero constant terms with non-zero terms elsewhere. Even then, we do have problems coming up with generic inverses. (We need to have the inverses of polynomial factors: to develop an inverse to $P(x) = a_0 + a_1 x$, we need $P^{-1}(x) = \frac{1}{a_0 + a_1 x}$, not $P^{-1}(x) = \frac{1}{a_0} + \frac{1}{a_1 x}$ or anything similar. To prove this in depth requires techniques we haven't discovered yet, so we won't deal with polynomials having integer exponents for a while.)

3 Conclusion

Polynomials fit the definition of a commutative or Abelian algebraic ring, but not a field.

4 Next Lesson

In our next lesson, we examine the means to find the roots of some simple polynomials.