1. Motivation

Perhaps you have seen a definition of a polynomial as a function of the form

$$P(x) = c_0 + c_1 x + \cdots + c_n x^n$$

where each c_i is a constant (called a coefficient) and where n is a nonnegative integer.

One problem with this definition is the vagueness of the term "constant." Are the coefficients presumed to be integers? Real numbers? Complex numbers?

This matters when we are considering whether or not a polynomial factors. For example, does $x^2 - 2$ factor or not? If we are only considering integers as valid coefficients, then the answer is no. But if we allow real numbers, then $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ is a perfectly valid factorization. What about $x^2 + 1$? If we only allow real coefficients, then this polynomial does not factor, but if we allow complex coefficients, it factors as $x^2 + 1 = (x - i)(x + i)$.

Could the coefficients be elements of $\mathbb{Z}_m$? Sure, why not?

Another issue is how to define equality of polynomials. Consider $f(x) = x^7 + 2x - 1$ and $g(x) = 3x + 6$, where the coefficients are in $\mathbb{Z}_7$. Are they the same or not? On one hand, we usually say that two polynomials are the same only if they have the same coefficients, and these polynomials do not have the same coefficients. However, if we consider them as *functions* $\mathbb{Z}_7 \to \mathbb{Z}_7$, they are the same. (RQ #1 asks you to check this: plug in $x = 0, 1, 2, \ldots 6$, reduce modulo 7, and see that f and g agree.) So, if we want to say that f and g are *different polynomials*, we cannot define polynomials as functions, because, as functions, f and g are the same.

If polynomials are not defined as functions, what are they? What does the "x" mean, if it's not an input?

2. Formal Polynomials

In an effort to resolve these questions, we adopt a more formal viewpoint. It will take some effort, but we will have a precise, unambiguous definition of "polynomial" as distinct from "polynomial function."

Given a commutative ring R, we will define the ring of polynomials with coefficients in R as a subring of the ring of formal power series with coefficients in R.

Formal Power Series

We define the **ring of formal power series over** R, denoted $R[[x]]$ to be the set of all infinite sequences of ring elements:

$$R[[x]] \quad = \quad \{(s_0, s_1, s_2, \ldots) : s_i \in R\}$$

The elements s_i of the sequence are called the **coefficients** of the power series. (See the top of page 197.) Two power series $(s_0, s_1, s_2, \ldots)$ and $(t_0, t_1, t_2, \ldots)$ are **equal** if and only if their corresponding coefficients are equal, i.e. $s_i = t_i$ for all i. (Proposition 5.6)

Note. You can think of the s_i as coefficients of x in $\displaystyle\sum_{i=0}^{\infty} s_i x^i$.

We define **addition and multiplication of formal power series** (see the bottom of page 198) and prove that $R[[x]]$ with these two binary operations is a commutative ring (Proposition 5.7). Note that the **additive identity** is $(0, 0, 0, \ldots)$ and the **multiplicative identity** is $(1, 0, 0, \ldots)$.

RQ #2 and 3 ask you to practice adding and multiplying formal power series. Here's an example of multiplying power series.

Example. Multiply $\sigma = (1, 4, 5, 0, 0, 0, \dots)$ by $\tau = (3, 2, 0, 0 \dots)$. Using the notation in the textbook:

$$s_0 = 1,\ \ s_1 = 4,\ \ s_2 = 5,\ \ s_i = 0 \text{ for } i > 2 \quad \text{and} \quad t_0 = 3,\ \ t_1 = 2, \quad \text{and } t_i = 0 \text{ for all } i > 1$$

We let c_i be the coefficients of the product: $\sigma\tau = (c_0, c_1, c_2, \dots)$. We compute the coefficients one by one:

$$\begin{aligned}
c_0 &= \sum_{i=0}^{0} s_i\, t_{0-i} \;=\; s_0 t_0 \;=\; 1 \cdot 3 = 3 \\
c_1 &= \sum_{i=0}^{1} s_i\, t_{1-i} \;=\; s_0 t_1 \,+\, s_1 t_0 \;=\; 1 \cdot 2 \,+\, 4 \cdot 3 \;=\; 2 + 12 \;=\; 14 \\
c_2 &= \sum_{i=0}^{2} s_i\, t_{2-i} \;=\; s_0 t_2 \,+\, s_1 t_1 \,+\, s_2 t_0 \;=\; 1 \cdot 0 \,+\, 4 \cdot 2 \,+\, 5 \cdot 3 \;=\; 0 + 8 + 15 \;=\; 23 \\
c_3 &= \sum_{i=0}^{3} s_i\, t_{3-i} \;=\; s_0 t_3 \,+\, s_1 t_2 \,+\, s_2 t_1 \,+\, s_3 t_0 \;=\; 1 \cdot 0 \,+\, 4 \cdot 0 \,+ 5 \,\cdot 2 \,+\, 0 \cdot 3 \;=\; 0 + 0 + 10 + 0 = 10 \\
c_4 &= \sum_{i=0}^{4} s_i t_{4-i} \;=\; s_0 t_4 \,+\, s_1 t_3 \,+\, s_2 t_2 \,+\, s_3 t_1 \,+\, s_4 t_0 \;=\; 1 \cdot 0 \,+\, 4 \cdot 0 \,+\, 5 \cdot 0 \,+\, 0 \cdot 2 \,+\, 0 \cdot 3 \;=\; 0
\end{aligned}$$

Consider $c_n \;=\; \sum_{i=0}^{n} s_i t_{n-i}$, for $n \geq 4$. If $i > 2$ then $s_i = 0$, so $s_i t_{n-i} = 0$. On the other hand, if $i \leq 2$, then $n - i \geq 2 > 1$, so $t_{n-i} = 0$ and $s_i t_{n-i} = 0$. Thus $c_n = 0$ for $n \geq 4$.

Thus $\sigma\tau = (3, 14, 23, 10, 0, 0, 0, \dots)$.

Formal Polynomials

We define a **polynomial** to be a formal power series whose coefficients are eventually all zero. (See the bottom of page 197.) The subset of $R[[x]]$ consisting of polynomials is a subring of $R[[x]]$ (Corollary 5.9), called the **ring of polynomials over** R and denoted $R[x]$.

Note that this means that two polynomials are equal if and only if their corresponding coefficients are equal (because that it what it means for two formal power series to be equal.)

We consider R as a subring of $R[x]$ and $R[[x]]$ by identifying $r \in R$ with $(r, 0, 0, \dots) \in R[x] \subset R[[x]]$. Thus "constants" are considered polynomials.

We define the **indeterminate element**, denoted x, of $R[x]$ to be the polynomial $(0, 1, 0, 0, \dots)$.

Using the definition of multiplication of formal power series, we compute x^2, x^3, x^4, etc. We have:

$$\begin{aligned}
1 &= (\mathbf{1}, 0, 0, 0, 0, 0, 0, \dots) \\
x &= (0, \mathbf{1}, 0, 0, 0, 0, 0, \dots) \\
x^2 &= (0, 0, \mathbf{1}, 0, 0, 0, 0, \dots) \\
x^3 &= (0, 0, 0, \mathbf{1}, 0, 0, 0, \dots) \\
x^4 &= (0, 0, 0, 0, \mathbf{1}, 0, 0, \dots) \\
&\ \ \vdots
\end{aligned}$$

We show that every polynomial can be expressed as a sum of products of constants with powers of x, recovering the familiar notation for polynomials. (See Lemma 5.10 and Proposition 5.11.) For example,

$$\begin{aligned}
(3, 2, 6, 0, 0, \dots) &= (3, 0, 0, \dots) \,+\, (0, 2, 0, 0, \dots) \,+\, (0, 0, 6, 0, 0, \dots) \\
&= (3, 0, 0, \dots) \,+\, (2, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots) \,+\, (6, 0, 0, \dots) \cdot (0, 1, 0, \dots) \cdot (0, 1, 0, \dots) \\
&= 3 \,+\, 2x \,+\, 6x^2
\end{aligned}$$

This is great, because we have a lot of good algebraic reflexes that allow us to manipulate polynomials when they are written in familiar notation.

Example. The power series σ in the example above is the polynomial $1 + 4x + 5x^2$ and τ is the polynomial $3 + 2x$. Their product $\sigma\tau$ is $3 + 14x + 23x^2 + 10x^3$, just as we expect.

Some other important terms: **degree** of a polynomial (page 198, see also Lemma 5.8, page 199), the **zero polynomial** (the degree of which is undefined, see top of page 198), the **constant term** and **leading coefficient** of a polynomial (bottom of page 201), a **monic** polynomial (bottom of page 201).

When k is a field, $k[x]$ is a domain (Corollary 5.9(ii)), and we can construct the fraction field of $k[x]$, denoted $k(x)$, and called the **field of rational functions over** k. (See top of page 205.)

3. Polynomial Functions

A polynomial $f \in R[x]$ gives rise to a **polynomial function**, denoted $f^{\#} : R \to R$, as follows:

$$\text{If } f = (s_0, \dots, s_n, 0, 0, \dots), \text{ then } f^{\#}(a) \;=\; s_0 + s_1 a + s_2 a^2 + \,\dots\, + s_n a^n$$

This is exactly what we would get if we were to write f in the usual notation and "plug in" a for x.

Now that we have carefully defined polynomials and distinguished them from polynomial functions, we can return to the confusing example given above: $f(x) = x^7 + 2x - 1$ and $g(x) = 3x + 6$. Considered as *polynomials* in $\mathbb{Z}_7[x]$, they are different, because their coefficients do not match. Considered as *functions* $\mathbb{Z}_7 \to \mathbb{Z}_7$ they are the same, since they always have the same outputs, given the same inputs.

The distinction between polynomials and polynomial functions also becomes apparent by counting. Suppose we want to count the number of polynomials in $\mathbb{Z}_2[x]$. We have:

$$0,\;\; 1,\;\; x,\;\; 1+x,\;\; x^2,\;\; 1+x^2,\;\; 1+x+x^2,\;\; \dots$$

There are infinitely many. (See Corollary 5.12 for a proof.) On the other hand, how many functions are there from $\mathbb{Z}_2$ to $\mathbb{Z}_2$? Well, the only possible inputs are 0 and 1, and the only possible outputs are 0 and 1. There are only four ways to assign outputs, so there are only four functions from $\mathbb{Z}_2$ to $\mathbb{Z}_2$. (RQ #4 asks you to check this.)

In particular, in $\mathbb{Z}_p[x]$, $f(x) = x^p - x$ is a nonzero polynomial, but since Fermat's Little Theorem implies that $a^p = a$ in for all $a \in \mathbb{Z}_p$, the associated function $f^{\#}$ is identically zero.

Reading Questions

Exercise 1. By plugging in all possible values of x in $\mathbb{Z}_7$, check that the two functions $f(x) = x^7 + 2x - 1$ and $g(x) = 3x + 6$, when considered as functions $\mathbb{Z}_7 \to \mathbb{Z}_7$, are actually the same function.

Exercise 2. Use the definition of addition of formal power series to compute the following sums.

(a) $(1, 1, 1, 1, 1, 1, \dots) + (2, 0, 2, 0, 2, 0, \dots)$

(b) $(2, 0, 0, 0, \dots) + (0, 1, 0, 0, \dots) + (0, 0, 3, 0, 0, \dots)$

Exercise 3. Use the definition of multiplication of formal power series to compute the following products.

(a) $(0, 0, 0, \dots) \cdot (1, 2, 3, 4, \dots)$

(b) $(1, 0, 0, 0, \dots) \cdot (1, 2, 3, 4, \dots)$

(c) $(5, 0, 0, 0, \dots) \cdot (1, 2, 3, 4, \dots)$

(d) $(0, 1, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots)$

(e) $(0, 1, 0, 0, \dots) \cdot (0, 0, 1, 0, \dots)$

Exercise 4. Check that there are only four functions $\mathbb{Z}_2 \to \mathbb{Z}_2$. Write input-output tables for each one.