Polynomials

We've been working with polynomials since taking algebra in middle school. But what is a polynomial, exactly? In this section, we will extend some of our ideas about rings to sets of polynomials. First, though, we need to have a better idea of what makes a polynomial a polynomial.

It is easy enough to come up with some examples of polynomials as we'd see them in College Algebra.

$$x^2 + x - 1 \qquad x^3 - 1 \qquad 7 \qquad \frac{1}{2}x^7 - \frac{2}{3}x^2 + 1 \qquad \pi x^3 + ex + \sqrt{2}$$

Just as important, we can come up with examples of things that sort of look like polynomials but aren't.

$$x^{1/2} + 2x \qquad x^{-1} + x^{\sqrt{2}} \qquad x^2 + x = 7x^3 \qquad 1 + x + x^2 + \cdots$$

From here, let's try to generalize. A polynomial in the **variable** x is an **expression** which can be written as a **finite sum** of things of the form cx^k, where c is **some kind of number** and k is a **natural number exponent**. The cs are called the coefficients of the polynomial.

We can add polynomials by "combining like terms", such as

$$\begin{aligned} (x^2 + 2x + 1) + (3x^2 - 4x + 27) &= (1+3)x^2 + (2-4)x + (1+27) \\ &= 4x^2 - 2x + 28. \end{aligned}$$

And if a particular polynomial is "missing" a term, we can pretend it is there with coefficient zero.

$$\begin{aligned} (x^2 + 1) + (x + 1) &= (x^2 + 0x + 1) + (0x^2 + x + 1) \\ &= (1+0)x^2 + (0+1)x + (1+1) \\ &= x^2 + x + 2 \end{aligned}$$

We can even multiply polynomials by using the "distributive property" over and over again.

$$\begin{array}{ccccc} & & +2x^2 & +3x & +1 \\ & \cdot & +1x^2 & -2x & +2 \\ \hline & & +4x^2 & +6x & +2 \\ & +3x^3 & -6x^2 & -2x & \\ 2x^4 & +3x^3 & +1x^2 & & \\ \hline 2x^4 & +6x^3 & -1x^2 & +4x & +2 \end{array}$$

As mathematicians, we might start to suspect that the "variable", x, is not so special, and really just serves as a placeholder to keep the coefficients separate. We may as well think of a polynomial as a list of coefficients, and really only need the variables to keep track of what position each coefficient takes in the list. This role could be played by a mapping from the natural numbers, say $f : \mathbb{N} \to \mathbb{Q}$ (if the coefficients are rational numbers), where $f(i)$ is the coefficient of x^i. Now the arithmetic of polynomials corresponds to a funny arithmetic on functions $\mathbb{N} \to \mathbb{Q}$. Note that to make the arithmetic on *polynomials* work, we just need to have an arithmetic on *coefficients* – which is provided by a ring.

Definition 1. *Let R be a ring. A mapping $a : \mathbb{N} \to R$ is called a* polynomial *with* coefficients in R *if there is a natural number M such that $a_i = 0$ whenever $i > M$.*

If x is a symbol not belonging to R (called an indeterminate*), we can write a as a formal polynomial* in *x:*

$$\begin{aligned} a(x) &= a_0 + a_1 x + a_2 x^2 + \cdots \\ &= \sum_i a_i x^i \end{aligned}$$

It is important to remember that the $+$ and $\sum$ in these expressions are not *interpreted in the arithmetic in R, but are* formal symbols*.*

The set of all polynomials in x with coefficients in R is denoted $R[x]$.

Proposition 1. *Let R be a ring and x an indeterminate. We define operations $+$ and $\cdot$ on $R[x]$ as follows: if $a, b \in R[x]$, then*

$$\begin{aligned} (a+b)(k) &= a(k) + b(k) \\ (a \cdot b)(k) &= \sum_{i+j=k} a(i) b(j) \end{aligned}$$

where the arithmetic on the right hand sides takes place in R.

1. *These operations make $R[x]$ into a ring.*

2. *$R[x]$ is commutative if and only if R is commutative.*

3. *$R[x]$ is unital if and only if R is unital. In this case $1_{R[x]}$ is the polynomial whose 0th coefficient is 1_R and whose every other coefficient is 0_R.*

To be clear: This is the usual polynomial arithmetic we know and love, but with coefficients coming from any fixed ring rather than from a ring of numbers.

Examples

- In $(\mathbb{Z}/(3))[x]$, let $p(x) = [1] + [2]x$ and $q(x) = [2] + x$. Find $p + q$ and pq.
- In $(\mathbb{Z}/(6))[x]$, let $p(x) = [1] + [2]x$ and $q(x) = [1] + x + [3]x^2$. Compute pq.
- In $\mathsf{Mat}_2(\mathbb{Z})[x]$, let
$$p(x) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} x.$$
Find p^2.

Degree and the Leading Term

Let a be a polynomial. Note that if $a \neq 0$, then there is a *largest* natural number d such that $a_d \neq 0$. This d is called the *degree* of a and denoted $\deg a$. (The degree of the zero polynomial is undefined.) We call a_d the *leading coefficient* of a, and $a_d x^d$ is called the *leading term*. If R is unital and the leading coefficient of $a(x)$ is 1, we say that a is *monic*.

Proposition 2. *Let R be a domain.*

1. *$R[x]$ is a domain.*
2. *$\deg ab = \deg a + \deg b$ for all nonzero $a, b \in R$.*
3. *$a \in R[x]$ is a unit if and only if $\deg a = 0$ and a_0 is a unit in R.*

Corollary 3. *Let F be a field. Then $N : F[x] \to \mathbb{N}$ given by $N(a) = \deg a$ is a multiplicative norm.*

We will be concerned mostly with $R[x]$ when R is a field or a domain. In this situation we will consider two basic questions:

Let R be a domain.

1. How is the structure of R reflected in the structure of $R[x]$? (Quite a bit, it turns out.)
2. Given a polynomial $p(x) \in R[x]$, can we detect whether or not $p(x)$ is irreducible? (Sometimes.)

Exercises

1. (Formal power series: $R[[x]]$)