15. Polynomial rings

Definition-Lemma 15.1. *Let R be a ring and let x be an indeterminate.*

*The **polynomial ring** $R[x]$ is defined to be the set of all formal sums*

$$a_n x^n + a_{n-1}x^n + \dots a_1 x + a_0 = \sum a_i x^i$$

*where each $a_i \in R$ ($a_1, a_2, \dots$ are called the **coefficients** of the polynomial; a_i is the coefficient of x^i). Given two polynomials*

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum a_i x^i$$

$$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \sum b_i x^i$$

in $R[x]$ the sum of f and g, $f+g$, is defined as,

$$f+g = (a_n+b_n)x^n+(a_{n-1}+b_{n-1})x^{n-1}+\cdots+(a_1+b_1)x+(a_0+b_0) = \sum(a_i+b_i)x^i,$$

(where we have implicitly assumed that $m \leq n$ and we set $b_i = 0$, for $i > m$) and the product as

$$fg = c_{m+n}x^{m+n}+c_{m+n-1}x^{m+n-1}+\cdots+c_1x^1+c_0 = \sum_i c_i x^i = \sum_i(\sum_j a_j b_{i-j})x^i.$$

With this rule of addition and multiplication, $R[x]$ becomes a ring, with zero given as the polynomial with zero coefficients.

If R is commutative then $R[x]$ is commutative. If R has unity, $1 \neq 0$ then $R[x]$ has unity, $1 \neq 0$; 1 is the polynomial whose constant coefficient is one and whose other terms are zero.

Proof. A long and completely uninformative check. □

For example, if

$$f(x) = x^2 - 5x + 6 \in \mathbb{Z}[x] \qquad \text{and} \qquad g(x) = 2x^3 - 5 \in \mathbb{Z}[x],$$

then

$$\begin{aligned} f(x) + g(x) &= (x^2 - 5x + 6) + (2x^3 - 5) \\ &= 2x^3 + x^2 - 5x + 1, \end{aligned}$$

and

$$\begin{aligned} f(x)g(x) &= (x^2 - 5x + 6)(2x^3 - 5) \\ &= 2x^5 - 10x^4 + 12x^3 - 5x^2 - 25x - 30. \end{aligned}$$

Note that a polynomial determines a function $R \longrightarrow R$ in an obvious way. If one takes R to be the real numbers, then it is well known that a polynomial is determined by the corresponding function. In general,

however, this is far from true. For example take $R = \mathbb{Z}_2$ (one of the smallest possible rings). Then there are four functions from R to R and there are infinitely many polynomials. Thus two different polynomials will often determine the same function.

Definition 15.2. *Let R be a ring and let $f \in R[x]$ be a non-zero polynomial with coefficients in R. The **degree** of f is the largest n such that the coefficient of x^n is non-zero.*

Polynomial rings give interesting examples of infinite rings of finite characteristic. For example $\mathbb{Z}_2[x]$ has infinitely many polynomials—just let the degree go to infinity—but the characteristic is two. Indeed if you add a polynomials to itself you are just adding the coefficients to themselves, which are then all zero.

More generally $\mathbb{Z}_n[x]$ is an infinite ring of finite characteristic n.

Lemma 15.3. *Let R be an integral domain and let f and g be two non-zero elements of $R[x]$.*

Then the degree of fg is the sum of the degrees of f and g. In particular $R[x]$ is an integral domain.

Proof. Suppose that

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

where a_n and b_m are non-zero. Then $a_n b_m$ is non-zero and this is the largest non-zero coefficient of the product. So the degree of fg is $n+m$ which is the degree of f plus the degree of g. This is the first statement.

The second statement follows, by observing that a product fg can only equal zero if its degree is zero. In this case both f and g are constant polynomials and their product in $R[x]$ is equal to their product in R. As R is an integral domain this is zero only if one of f and g is zero. □

Lemma 15.4. *Let R be an integral domain.*

Then the units in $R[x]$ are precisely the units in R.

Proof. One direction is clear. A unit in R is a unit in $R[x]$.

Now suppose that $f(x)$ is a unit in $R[x]$. Given a polynomial g, denote by $d(g)$ the degree of $g(x)$. Now $f(x)g(x) = 1$. In particular neither $f(x)$ nor $g(x)$ is zero. Thus

$$\begin{aligned} 0 &= d(1) \\ &= d(fg) \\ &= d(f) + d(g). \end{aligned}$$

Thus both of f and g must have degree zero. It follows that $f(x) = f_0$ and that f_0 is a unit in $R[x]$. $\square$

It is interesting to consider what the field of fractions of a polynomial ring looks like. Suppose that F is a field and consider the polynomial ring $F[x]$. The field of fractions consists of all ratios of two polynomials with coefficients in F,

$$\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x] \}.$$

These are called rational functions and the field of rational functions is denoted $F(x)$. More generally if R is an integral domain with field of fractions F then $F(x)$ is the field of fractions of $R[x]$.

For example,

$$\frac{2x-3}{x^2-5x+6} \in \mathbb{Z}(x) = \mathbb{Q}(x).$$

We can also work with polynomial rings in one more than variable. We do the case of two variables but the general case is the same.

Definition 15.5. *Let R be a commutative ring and let x and y be indeterminates.*

*A **monomial** in x and y is a product of powers of x and y,*

$$x^i y^j.$$

*The **degree** d of a monomial is the sum of the degrees of the individual terms, $i + j$.*

*The **polynomial ring** $R[x, y]$ is equal to the set of all finite formal sums*

$$\sum_{i,j} a_{ij} x^i y^j$$

*with the obvious addition and multiplication. The **degree of a polynomial** is the maximum degree of a monomial term that appears with non-zero coefficient.*

Example 15.6. *Let x and y be indeterminates. A typical element of $\mathbb{Q}[x, y]$ might be*

$$x^2 + y^2 - 1.$$

This has degree 2. Note that xy also has degree two. A more complicated example might be

$$\frac{2}{3}x^3 - 7xy + y^5,$$

a polynomial of degree 5.

The nice thing about polynomial rings in one more than one variable is that one can construct them iteratively as polynomial rings in one variable. Again, we just do the case of two variables:

Lemma 15.7. *Let R be a commutative ring and let x and y be indeterminates. Let $S = R[x]$. Then there is a natural isomorphism*

$$R[x, y] \simeq S[y].$$

We will skip the proof which is not hard but we will try to illustrate how the proof proceeds by giving an example. Consider the polynomial

$$\frac{2}{3}x^3 - 7xy + y^5 \in \mathbb{Q}[x, y].$$

Consider this as a polynomial in y, whose coefficients lie in the ring $\mathbb{Q}[x]$, so that

$$y^5 + (-7x)y + 2/3x^3 \in \mathbb{Q}[x][y].$$

Note that by symmetry we may also consider the as a polynomial in x with coefficients in the ring $\mathbb{Q}[y]$,

$$\frac{2}{3}x^3 + (-7y)x + y^5 \in \mathbb{Q}[y][x].$$

Lemma 15.8. *If R is an integral domain then so is $R[x_1, x_2, \ldots, x_n]$.*

Proof. We just do the case of two variables x and y; the general case is by induction on the number of variables.

As R is an integral domain (15.3) implies that $R[x]$ is an integral domain. As $R[x]$ is an integral domain (15.3) implies that $R[x][y]$ is an integral domain. As $R[x, y]$ is isomorphic to $R[x][y]$ it follows that $R[x, y]$ is an integral domain. □

In particular if R is an integral domain then there is a field of fractions $R(x, y)$ of $R[x, y]$. As in the case of one variable the elements of $R(x, y)$ are rational functions, the quotients of polynomials with coefficients in R.

It is interesting to understand the various ring homomorphisms attached to a polynomial ring. We start with a really obvious one.

Lemma 15.9. *Let R be a ring. The natural inclusion*

$$R \longrightarrow R[x]$$

which just sends an element $r \in R$ to the constant polynomial r, is a ring homomorphism.

Proof. Easy. □

The following is a little bit more complicated but very useful:

Definition 15.10. *Suppose that $R \subset S$ is a subring of the ring S. Let α be an element of S.*

Then the map

$$\phi_\alpha \colon R[x] \longrightarrow S,$$

which sends

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longrightarrow a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1 \alpha + a_0$$

is a ring homomorphism.

It is characterised by the property that it sends x to α and has no effect on the coefficients.

This map is called ***evaluation at*** *α.*

Proof. An exercise for the reader. □

We will be mostly interested in the case when R and S are fields.

Example 15.11. *Consider the ring homomorphism evaluation at zero*

$$\phi_0 \colon \mathbb{Q}[x] \longrightarrow \mathbb{R}.$$

This sends the polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longrightarrow a_n 0^n + a_{n-1}0^{n-1} + \cdots + a_1 0 + a_0 = a_0.$$

Thus a polynomial is sent to its constant term.

Example 15.12. *Consider the ring homomorphism evaluation at three*

$$\phi_3 \colon \mathbb{Q}[x] \longrightarrow \mathbb{R}.$$

This sends the polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longrightarrow a_n 3^n + a_{n-1}3^{n-1} + \cdots + a_1 3 + a_0.$$

Note that

$$\phi_3(x^2 - 5x + 6) = 3^2 - 5 \cdot 3 + 6 = 0.$$

Thus $x^2 = 5x + 6$ is in the kernel N of ϕ_3.

Of course $x^2 - 5x + 6 = (x - 2)(x - 3)$ and $x - 3$ is in the kernel N of ϕ_3.

Example 15.13. *Consider the ring homomorphism evaluation at i*

$$\phi_i \colon \mathbb{Q}[x] \longrightarrow \mathbb{C}.$$

This sends the polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longrightarrow a_n i^n + a_{n-1}i^{n-1} + \cdots + a_1 i + a_0.$$

Note that

$$\phi_i(x^2 + 1) = i^2 + 1 = 0$$

Thus $x^2 + 1$ is in the kernel N of ϕ_i.

Example 15.14. *Consider the ring homomorphism evaluation at* π

$$\phi_\pi \colon \mathbb{Q}[x] \longrightarrow \mathbb{C}.$$

This sends the polynomial

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \longrightarrow a_n \pi^n + a_{n-1}\pi^{n-1} + \cdots + a_1 \pi + a_0.$$

It turns out that the kernel N of ϕ_π is trivial, so that ϕ_π is one to one. It follows that $\mathbb{Q}[\pi]$ is isomorphic to $\mathbb{Q}[x]$.

Definition 15.15. *Suppose that* $E \subset F$ *is a subfield of the field* F*. Let* α *be an element of* F*.*

We say that α *is a* ***zero*** *of* $f(x) \in E[x]$*, if* $f(x)$ *is in the kernel* N *of* ϕ_α*.*

Of course $f(x)$ is in the kernel if and only if $\phi_\alpha(f(x)) = 0$.