8. Polynomial rings

Let us now turn out attention to determining the prime elements of a polynomial ring, where the coefficient ring is a field. We already know that such a polynomial ring is a UFD. Therefore to determine the prime elements, it suffices to determine the irreducible elements.

We start with some basic facts about polynomial rings.

Lemma 8.1. *Let R be an integral domain.*

Then the invertible elements of $R[x]$ are precisely the invertible elements of R.

Proof. One direction is clear. An invertible element of R is an invertible element of $R[x]$.

Now suppose that $f(x)$ is a invertible elements of $R[x]$. Given a polynomial g, denote by $d(g)$ the degree of $g(x)$ (note that we are not claiming that $R[x]$ is a Euclidean domain). Now $f(x)g(x) = 1$. Thus

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

Thus both of f and g must have degree zero. It follows that $f(x) = f_0$ and that f_0 is an invertible element of R. □

Lemma 8.2. *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 universal property of polynomial rings is very useful.

Lemma 8.3. *Let*

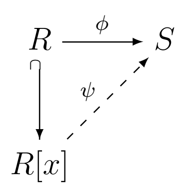
$$\phi \colon R \longrightarrow S$$

be any ring homomorphism and let $a \in S$ be any element of S.

Then there is a unique ring homomorphism

$$\psi \colon R[x] \longrightarrow S,$$

such that $\psi(x) = a$ and which makes the following diagram commute



Proof. Note that any ring homomorphism

$$\psi\colon R[x] \longrightarrow S$$

that sends x to a and acts as ϕ on the coefficients, must send

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

to

$$\phi(a_n)a^n + \phi(a_{n-1})a^{n-1} + \cdots + \phi(a_0).$$

Thus it suffices to check that the given map is a ring homomorphism, which is left as an exercise for the reader. □

Definition 8.4. *Let R be a ring and let α be an element of R. The natural ring homomorphism*

$$\phi\colon R[x] \longrightarrow R,$$

*which acts as the identity on R and which sends x to α, is called **evaluation at** α and is often denoted ev_α.*

*We say that α is a **root** of $f(x)$, if $f(x)$ is in the kernel of ev_α.*

Roots are also known as zeroes of $f(x)$.

Lemma 8.5. *Let K be a field and let α be an element of K.*

Then the kernel of ev_α is the ideal $\langle x - \alpha\rangle$.

Proof. Denote by I the kernel of ev_α

Clearly $x-\alpha$ is in I. On the other hand, $K[x]$ is a Euclidean domain, and so it is certainly a PID. Thus I is principal. Suppose it is generated by f, so that $I = \langle f\rangle$. Then f divides $x - \alpha$. If f has degree one, then $x - \alpha$ must be an associate of f and the result follows. If f has degree zero, then it must be a constant. As f has a root at α, in fact this constant must be zero, a contradiction. □

Lemma 8.6. *Let K be a field and let $f(x)$ be a polynomial in $K[x]$.*

Then we can write $f(x) = g(x)h(x)$ where $g(x)$ is a polynomial of degree one if and only if $f(x)$ has a root in K.

Proof. First note that a polynomial of degree one always has a root in K. Indeed any polynomial of degree one is of the form $ax + b$, where $a \neq 0$. Then it is easy to see that $\alpha = -\frac{b}{a}$ is a root of $ax + b$.

On the other hand, the kernel of the evaluation map is an ideal, so that if $g(x)$ has a root α, then in fact so does $f(x) = g(x)h(x)$. Thus if we can write $f(x) = g(x)h(x)$, where $g(x)$ has degree one, then it follows that $f(x)$ must have a root.

Now suppose that $f(x)$ has a root at α. Consider the polynomial $g(x) = x - \alpha$. Then the kernel of ev_α is equal to $\langle x - \alpha\rangle$. As f is in the kernel, $f(x) = g(x)h(x)$, for some $h(x) \in R[x]$. □

Lemma 8.7. *Let K be a field and let $f(x)$ be a polynomial of degree two or three.*

Then $f(x)$ is irreducible if and only if it has no roots in K.

Proof. If $f(x)$ has a root in K, then $f(x) = g(x)h(x)$, where $g(x)$ has degree one, by (8.6). As the degree of f is at least two, it follows that $h(x)$ has degree at least one. Thus $f(x)$ is not irreducible.

Now suppose that $f(x)$ is not irreducible. Then $f(x) = g(x)h(x)$, where neither g nor h is invertible. Thus both g and h have degree at least one. As the sum of the degrees of g and h is at most three, the degree of f, it follows that one of g and h has degree one. Now apply (8.6). □

Definition 8.8. *Let p be a prime.*

$\mathbb{F}_p$ denotes the unique field with p elements.

Of course, $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}_p$. However, as we will see later, it is useful to replace Z by F.

Example 8.9. *First consider the polynomial $x^2 + 1$.*

Over the real numbers this is irreducible. Indeed, if we replace x by any real number a, then a^2 is positive and so $a^2 + 1$ cannot equal zero.

On the other hand $\pm i$ is a root of $x^2 + 1$, as $i^2 + 1 = 0$. Thus $x^2 + 1$ is reducible over the complex numbers. Indeed $x^2 + 1 = (x + i)(x - i)$. Thus an irreducible polynomial might well become reducible over a larger field.

Example 8.10. *Consider the polynomial $x^2 + x + 1$.*

We consider this over various fields. As observed in (8.7) this is reducible if and only if it has a root in the given field.

Suppose we work over the field $\mathbb{F}_5$. We need to check if the five elements of $\mathbb{F}_5$ are roots or not. We have

$$1^2 + 1 + 1 = 3 \quad 2^2 + 2 + 1 = 2 \quad 3^2 + 3 + 1 = 3 \quad 4^2 + 4 + 1 = 1$$

Thus this is irreducible over $\mathbb{F}_5$. Now consider what happens over the field with three elements $\mathbb{F}_3$. Then 1 is a root of this polynomial. As neither 0 nor 2 are roots, we must have

$$x^2 + x + 1 = (x - 1)^2 = (x + 2)^2,$$

which is easy to check.

Example 8.11. *Now let us determine all irreducible polynomials of degree at most four over $\mathbb{F}_2$.*

Any linear polynomial is irreducible. There are two such x and $x+1$. A general quadratic has the form $f(x) = x^2 + ax + b$. $b \neq 0$, else x divides $f(x)$. Thus $b = 1$. If $a = 0$, then $f(x) = x^2 + 1$, which has 1 as a zero. Thus $f(x) = x^2 + x + 1$ is the only irreducible quadratic.

Now suppose that we have an irreducible cubic $f(x) = x^3+ax+bx+1$. This is irreducible if and only if $f(1) \neq 0$, which is the same as to say that there are an odd number of terms. Thus the irreducible cubics are $f(x) = x^3 + x^2 + 1$ and $x^3 + x + 1$.

Finally suppose that $f(x)$ is a quartic polynomial. The general irreducible is of the form $x^4 + ax^3 + bx^2 + cx + 1$. $f(1) \neq 0$ is the same as to say that either two of a, b and c are equal to zero or they are all equal to one. Suppose that

$$f(x) = g(x)h(x).$$

If $f(x)$ does not have a root, then both g and h must have degree two. If either g or h were reducible, then again f would have a linear factor, and therefore a root. Thus the only possibilty is that both g and h are the unique irreducible quadratic polynomials.

In this case

$$f(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1.$$

Thus $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, and $x^4 + x + 1$ are the three irreducible quartics.