21. 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 21.1. *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 $g(x)$ (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 a unit in $R[x]$. $\qquad\square$

Lemma 21.2. *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. $\qquad\square$

The following universal property of polynomial rings, is very useful.
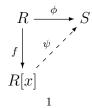
Lemma 21.3. *Let*

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

be any ring homomorphism and let $s \in S$ be any element of S.
Then there is a unique ring homomorphism

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

such that $\phi(x) = s$ and which makes the following diagram commute

$$
\begin{array}{ccc}
R & \xrightarrow{\ \phi\ } & S \\
{\scriptstyle f}\big\downarrow & {\scriptstyle \psi}\;\nearrow & \\
R[x] & &
\end{array}
$$

1

Proof. Note that any ring homomorphism

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

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

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

to

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

Thus it suffices to check that the given map is a ring homomorphism, which is left as an exercise to the reader. $\qquad\square$

Definition 21.4. *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 **zero** *(aka* **root***) of $f(x)$, if $f(x)$ is in the kernel of* ev_α.

Lemma 21.5. *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. $\qquad\square$

Lemma 21.6. *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 linear polynomial if and only if $f(x)$ has a root in K.

Proof. First note that a linear polynomial always has a root in K. Indeed any linear polynomial 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 $g(x)$ is linear, then it follows that $f(x)$ must have a root.
   Now suppose that $f(x)$ has a root at α. Consider the linear 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 $h(x) \in R[x]$. $\qquad\square$

Lemma 21.7. *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 (21.6). 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 a unit. 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 (21.6). $\qquad\qquad\square$

Definition 21.8. *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 21.9. *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 non-negative 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.

Consider the polynomial $x^2 + x + 1$. We consider this over various fields. As observed in (21.7) this is reducible iff 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

$$1^2 + 1 + 1 = 3 \quad 2^2 + 2 + 1 = 2 \quad 3^2 + 3 + 13 \quad 4^2 + 4 = 1$$

Thus $x^2 + x + 1$ 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.

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.

3

Now suppose that we have an irreducible cubic $f(x) = x^3 + ax + bx + 1$. This is irreducible iff $f(1) \neq 0$, 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 is 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.

Obviously it would be nice to have some more general methods of proving that a given polynomial is irreducible. The first is rather beautiful and due to Gauss. The basic idea is a follows. Suppose we are given a polynomial with integer coefficients. Then it is natural to also consider this polynomial over the rationals. Note that it is much easier to prove that this polynomial is irreducible over the integers than it is to prove that it is irreducible over the rationals. For example it is clear that

$$x^2 - 2$$

is irreducible over the integers. In fact it is irreducible over the rationals as well, that is, $\sqrt{2}$ is not a rational number.

First some definitions.

Definition 21.10. *Let R be a commutative ring and let $a_1, a_2, \ldots, a_k$ be a sequence of elements of R. The gcd of $a_1, a_2, \ldots, a_k$ is an element $d \in R$ such that*

(1) $d|a_i$, for all $1 \leq i \leq k$.
(2) If $d'|a_i$, for all $1 \leq i \leq k$, then $d'|d$.

Lemma 21.11. *Let R be a UFD.*

Then the gcd of any sequence $a_1, a_2, \ldots, a_k$ of non-zero elements of R exists.

4

Proof. There are two obvious ways to proceed.

The first is to take a common factorisation of each a_i into a product of powers of primes, as in the case $k = 2$.

The second is to recursively construct the gcd, by setting d_i to be the gcd of d_{i-1} and a_i and taking $d_1 = a_1$. In this case $d = d_k$ will be a gcd for the whole sequence $a_1, a_2, \ldots, a_k$. $\qquad\square$

Definition 21.12. *Let R be a UFD and let $f(x)$ be a polynomial with coefficients in R.*

The **content** *of $f(x)$, denoted $c(f)$, is the gcd of the coefficients of f.*

Example 21.13. *Let $f(x) = 24x^3 - 60x + 40$. Then the content of f is 4. Thus*

$$f(x) = 4(8x^3 - 15x + 10).$$

Lemma 21.14. *Let R be a UFD. Then every element of $R[x]$ has a factorisation of the form*

$$cf,$$

where $c \in R$ and the content of f is one.

Proof. Obvious. $\qquad\square$

Here is the key result.

Proposition 21.15. *Let R be a UFD. Suppose that g and $h \in R[x]$ and let $f(x) = g(x)h(x)$.*

Then the content of f is equal to the content of g times the content of h.

Proof. It is clear that the content of g divides the content of f. Therefore we may assume that the content of g and h is one, and we only have to prove that the same is true for f.

Suppose not. As R is a UFD, it follows that there is a prime p that divides the content of f. We may write

$$g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \quad \text{and} \quad h(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0.$$

As the content of g is one, at least one coefficient of g is not divisible by p. Let i be the first such, so that p divides a_k, for $k < i$ whilst p does not divide a_i. Similarly pick j so that p divides b_k, for $k < j$, whilst p does not divide b_j.

Consider the coefficient of x^{i+j} in f. This is equal to

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1} + a_i b_j + a_{i+1} b_{j+1} + \cdots + a_{i+j} b_0.$$

Note that p divides every term of this sum, except the middle one $a_i b_j$. Thus p does not divide the coefficient of x^{i+j}. But this contradicts the definition of the content. $\qquad\square$

Theorem 21.16. *(Gauss' Lemma) Let R be a UFD and let $f(x) \in R[x]$. Let F be the field of fractions of R. Suppose that the content of f is one and that we may write $f(x) = u_1(x)v_1(x)$, where $u_1(x)$ and $v_1(x)$ are in $F[x]$.*

Then we may find $u(x)$ and $v(x)$ in $R[x]$, such that
$$f(x) = u(x)v(x)$$
where the degree of u is the same as the degree of u_1 and the degree of v is the same as the degree of v.

In particular if f is irreducible in $R[x]$ then it is irreducible in $F[x]$.

Proof. We have
$$f(x) = u_1(x)v_1(x).$$
Now clear denominators. That is, multiply through by the product c of all the denominators in $u_1(x)$ and $v_1(x)$. In this way we get an expression of the form
$$cf(x) = u_2(x)v_2(x),$$
where now u_2 and v_2 belong to $R[x]$. Now write
$$u_2(x) = au(x) \qquad \text{and} \qquad v_2(x) = bv(x).$$
We get
$$cf(x) = abu(x)v(x).$$
By (21.15) we can c divides ab, $ab = c\alpha$, where $\alpha \in R$. Therefore, replacing $u(x)$ by $\alpha u(x)$, we have
$$f(x) = u(x)v(x). \qquad \square$$

Corollary 21.17. *Let R be a UFD.*
Then $R[x]$ is a UFD.

Proof. It is clear that the Factorisation algorithm terminates, by induction on the degree. Therefore it suffices to prove that irreducible implies prime.

Suppose that $f(x) \in R[x]$ is irreducible. If f has degree zero, then it is an irreducible element of R and hence a prime element of R and there is nothing to prove.

Otherwise we may assume that the content of f is one. By Gauss' Lemma, f is not only irreducible in $R[x]$ but also in $F[x]$. But then f is a prime element of $F[x]$ as $F[x]$ is a UFD.

Now suppose that f divides gh, where g and $h \in R[x]$. As f is prime in $F[x]$, f divides g or h in $F[x]$. Suppose it divides g. Then we may write
$$g = fk,$$

6

some $k \in F[x]$. As in the proof of Gauss' Lemma, this means we may write
$$g = fk',$$
some $k' \in R[x]$. But then $f(x)$ divides g in $R[x]$. $\qquad\square$

Corollary 21.18. $\mathbb{Z}[x]$ *is a UFD.*

Definition 21.19. *Let R be a commutative ring and let $x_1, x_2, \ldots, x_n$ be indeterminates.*

A monomial in $x_1, x_2, \ldots, x_n$ is a product of powers of $x_1, x_2, \ldots, x_n$. If $I = (d_1, d_2, \ldots, d_n)$, then let
$$x^I = \prod x_i^{d_i}.$$

*The **degree** d of a monomial is the sum of the degrees of the individual terms, $\sum d_i$.*

The polynomial ring $R[x_1, x_2, \ldots, x_n]$ is equal to the set of all finite formal sums
$$\sum_I a_I x^I,$$

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 21.20. *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.

Lemma 21.21. *Let R be a commutative ring and let $x_1, x_2, \ldots, x_n$ be indeterminates. Let $S = R[x_1, x_2, \ldots, x_{n-1}]$. Then there is a natural isomorphism*
$$R[x_1, x_2, \ldots, x_n] \simeq S[x_n].$$

Proof. Clear. $\qquad\square$

To illustrate how this proceeds, it will probably help to give an example. Consider the polynomial
$$\frac{2}{3}x^3 - 7xy + y^5.$$

7

Consider this as a polynomial in y, whose coefficients lie in the ring $R[x]$. That is

$$y^5 + (-7x)y + 2/3x^3 \in R[x][y].$$

Corollary 21.22. *Let R be a UFD. Then $R[x_1, x_2, \ldots, x_n]$ is a UFD.*

Proof. By induction on n. The case $n = 1$ is (21.17).

Set $S = R[x_1, x_2, \ldots, x_{n-1}]$. By induction S is a UFD. But then $S[x]$ $R[x_1, x_2, \ldots, x_n]$ is a UFD. $\qquad\square$

Now we give a way to prove that polynomials with integer coefficients are irreducible.

Lemma 21.23. *Let*

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

be a ring homomorphism.

Then there is a unique ring homomorphism

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

which makes the following diagram commute

$$
\begin{array}{ccc}
R & \xrightarrow{\ \phi\ } & S \\
\big| & & \big| \\
R[x] & \xrightarrow{\ \psi\ } & S[x]
\end{array}
$$

and which sends x to x.

Proof. Let

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

be the composition of ϕ with the natural inclusion of S into $S[x]$. By the universal property of $R[x]$, there is a unique ring homomorphism

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

The rest is clear. $\qquad\square$

Theorem 21.24. *(Eisenstein's Criteria) Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

be a polynomial with integer coefficients. Suppose that there is a prime p such that p divides a_i, $i \leq n - 1$, p does not divide a_n and p^2 does not divide a_0.

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

8

Proof. There is no harm in assuming that the content of f is one, so that by Gauss' Lemma, it suffices to prove that f is irreducible over $\mathbb{Z}$.

Suppose not. Then we may find two polynomials $g(x)$ and $h(x)$, of positive degree, with integral coefficients, such that

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

Suppose that

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$
$$g(x) = b_d x^d + b_{d-1} x^{d-1} + \cdots + b_0$$
$$h(x) = c_e x^e + c_{e-1} x^{e-1} + \cdots + c_0,$$

for some n, d and $e > 1$. As $a_n = b_d c_e$ and a_n is not divisible by p, then neither is b_d nor c_e.

Consider the natural ring homomorphism

$$\mathbb{Z} \longrightarrow \mathbb{F}_p.$$

This induces a ring homomorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x].$$

It is convenient to denote the image of a polynomial $g(x)$ as $\bar{g}(x)$. As we have a ring homomorphism,

$$\bar{f}(x) = \bar{g}(x)\bar{h}(x).$$

Since the leading coefficient of f is not divisible by p, $\bar{f}(x)$ has the same degree as $f(x)$, and the same holds for $g(x)$ and $h(x)$. On the other hand, every other coefficient of $f(x)$ is divisible by p, and so

$$\bar{f}(x) = \bar{a}_n x^n.$$

Since $\mathbb{F}_p$ is a field, $\mathbb{F}_p$ is a UFD and so $\bar{g} = \bar{b}_d x^d$ and $\bar{g}(x) = \bar{c}_e x^e$. It follows that every other coefficient of $g(x)$ and $h(x)$ is divisible by p. In particular b_0 and c_0 are both divisible by p, and so, as $a_0 = b_0 c_0$, a_0 must be divisible by p^2, a contradiction. $\qquad\square$

Example 21.25. *Let*

$$f(x) = 2x^7 - 15x^6 + 60x^5 - 18x^4 - 9x^3 + 45x^2 - 3x + 6.$$

Then $f(x)$ is irreducible over $\mathbb{Q}$. We apply Eisenstein with $p = 3$. Then the top coefficient is not divisible by 3, the others are, and the smallest coefficient is not divisible by $9 = 3^2$.

Lemma 21.26. *Let p be a prime. Then*

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

is irreducible over $\mathbb{Q}$.

9

Prof. James McKernan

Proof. By Gauss' Lemma, it suffices to prove that $f(x)$ is irreducible over $\mathbb{Z}$.

First note that

$$f(x) = \frac{x^p - 1}{x - 1},$$

as can be easily checked. Consider the change of variable

$$y = x - 1.$$

As this induces an automorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$$

by sending x to $x - 1$, this will not alter whether or not f is irreducible. In this case

$$f(y) = \frac{(y + 1)^p - 1}{y}$$

$$= y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots \binom{p}{p-1}$$

$$= y^{p-1} + p y^{p-2} + \cdots + p.$$

Note that $\binom{p}{i}$ is divisible by p, for all $1 \le i < p$, so that we can apply Eisenstein to $f(y)$, using the prime p. $\qquad\square$