17. Irreducible polynomials

Definition 17.1. *Let F be a field. We say that a non-constant polynomial $f(x)$ is* ***reducible over*** *F or a* ***reducible element of*** *$F[x]$, if we can factor $f(x)$ as the product of $g(x)$ and $h(x) \in F[x]$, where the degree of $g(x)$ and the degree of $h(x)$ are both less than the degree of $f(x)$,*

$$f(x) = g(x)h(x) \qquad \textit{and} \qquad d(g(x)) < d(f(x)), \quad d(h(x)) < d(f(x)).$$

We say that a non-constant polynomial $f(x)$ is ***irreducible*** *if it is not reducible.*

Example 17.2. *Consider the polynomial $x^2 - 2$.*

Note that $x^2 - 2$ has no zeroes over $\mathbb{Q}$. This is the same as saying that $\sqrt{2}$ is irrational, a result that goes all the way back to the time of Euclid.

If $x^2 - 2$ is reducible then we may write

$$x^2 - 2 = g(x)h(x),$$

where the degree of $g(x)$ and $h(x)$ is less than two. As the degree of the LHS is two, the only possibility is that both $g(x)$ and $h(x)$ have degree one. In this case $x^2 - 2$ has a zero in $\mathbb{Q}$, a contradiction.

Thus $x^2 - 2$ is irreducible over $\mathbb{Q}$.

On the other hand, $\sqrt{2} \in \mathbb{R}$ so that $x^2 - 2$ is reducible over $\mathbb{R}$,

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Example 17.3. *Consider $f(x) = x^3 + 3x + 2$ over the field $\mathbb{Z}_5$.*

Suppose that this is reducible. Then we can write

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

where both $g(x)$ and $h(x)$ have degree at most two. Possibly reordering we may assume that the degree of $g(x)$ is at most the degree of $h(x)$. It follows that $g(x)$ has degree one and $h(x)$ has degree two, since the sum of the degrees is three. Thus $f(x)$ has a zero, corresponding to the linear factor $g(x)$.

We check this by simply plugging in the elements of $\mathbb{Z}_5$.

$$\begin{aligned}
\phi_0(x^3 + 3x + 2) &= 0^3 + 3 \cdot 0 + 2 = 2 \\
\phi_1(x^3 + 3x + 2) &= 1^3 + 3 \cdot 1 + 2 = 1 \\
\phi_2(x^3 + 3x + 2) &= 2^3 + 3 \cdot 2 + 2 = 1 \\
\phi_3(x^3 + 3x + 2) &= 3^3 + 3 \cdot 3 + 2 = 3 \\
\phi_4(x^3 + 3x + 2) &= 4^3 + 3 \cdot 4 + 2 = 3.
\end{aligned}$$

Since we never get zero $f(x)$ must be irreducible.

Theorem 17.4. *Let $f(x) \in F[x]$ be a polynomial over a field F of degree two or three.*

Then $f(x)$ is irreducible if and only if it has no zeroes.

Proof. If $f(x)$ has zero α then we have already seen it can be factored as $(x-\alpha)h(x)$. If $f(x)$ has degree two then $g(x)$ has degree one and if $f(x)$ has degree three then $g(x)$ has degree two. Therefore $f(x)$ is reducible.

Now suppose that $f(x)$ is reducible. Then

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

where the degrees of $g(x)$ and $h(x)$ are less than the degree of $f(x)$. Possibly reordering we may assume that $g(x)$ has degree no more than the degree of $h(x)$.

It follows that $g(x)$ has degree one. If $g(x) = ax + b$ then $a \neq 0$. In this case

$$\alpha = -\frac{b}{a}.$$

is a zero of $g(x)$ and so it is a zero of $f(x)$. □

The most beautiful results in this area relate to irreducibility over the rationals. The first is due to Gauss:

Theorem 17.5. *If $f(x) \in \mathbb{Z}[x]$ then we can factor $f(x)$ into two polynomials of degrees r and s in $\mathbb{Z}[x]$ if and only if we can factor $f(x)$ into two polynomials of the same degrees r and s in $\mathbb{Q}[x]$.*

The point is that it is much easier to show that we cannot factor over $\mathbb{Z}[x]$.

Corollary 17.6. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, where $a_0 \neq 0$.*

If $f(x)$ has a zero in $\mathbb{Q}$ then it has a zero $m \in \mathbb{Z}$ and m divides a_0.

Proof. If α is a zero of $f(x)$ then $(x-\alpha)$ is a linear factor of $\mathbb{Q}[x]$.

By Gauss $f(x)$ must have a linear factor in $\mathbb{Z}$,

$$f(x) = (ax + b)g(x).$$

Looking at the leading coefficients, we must have that a divides 1. So $a = \pm 1$. Possibly replacing $g(x)$ by $-g(x)$ we may assume that $a = 1$. If $m = -b$ then

$$f(x) = (x - m)g(x).$$

$m \in \mathbb{Z}$ is a zero of $f(x)$. Considering the constant coefficients m must divide a_0. □

Example 17.7. *Consider $x^2 - 2 \in \mathbb{Q}[x]$.*

Let's show that this is irreducible over $\mathbb{Q}$. If not then since $x^2 - 2$ is a quadratic polynomial then it would have a zero in $\mathbb{Z}$ and this zero would divide 2. The only possible choices are ±1 and ±2. It is easy to check that none of these are zeroes of $x^2 - 2$. Thus $x^2 - 2$ is irreducible over $\mathbb{Q}$. In other words, $\sqrt{2}$ is irrational.

Example 17.8. *Consider $f(x) = x^4 + 3x^2 - 7x + 1 \in \mathbb{Q}[x]$.*

Let's show that this is irreducible over $\mathbb{Q}$. We first check it does not have a linear factor. If it has a linear factor it has a zero in $\mathbb{Q}$ and so by (17.6) it must have a zero α in $\mathbb{Z}$ and this zero must divide 1. Thus $\alpha = \pm 1$. But

$$f(1) = 1 + 3 + 1 - 7 = -2 \qquad \text{and} \qquad f(-1) = 1 + 3 + 7 + 1 = 12.$$

Thus $f(x)$ has no linear factors. The only other possibility is that it factors as two quadratic polynomials. In this case we may write

$$x^4 + 3x^2 - 7x + 1 = (x^2 + ax + b)(x^2 + cx + d),$$

and by (17.6) we may assume that a, b, c and d are integers. Note that we may assume that both factors are monic, that is, their leading coefficients are 1, as the LHS is monic.

If we equate coefficients then we get the following equations:

$$bd = 1, \qquad ad + bc = -7, \qquad b + d + ac = 3, \qquad \text{and} \qquad a + c = 0.$$

Note that either $b = 1$ and $d = 1$ or $b = -1$ and $d = -1$. Either way we have $b = d$. The second equation then reads

$$(a + c)b = -7.$$

But the last equation says that $a + c = 0$, which is a contradiction. Thus $f(x) = x^4 + 3x^2 - 7x + 1$ is irreducible over $\mathbb{Q}$.

Theorem 17.9 (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 $\mathbb{Q}[x]$.

Proof. By Gauss' Lemma, we only have to rule out the possibility that $f(x)$ factors into polynomials of lower degree with integer coefficients.

Suppose that

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

is a factorisation of $f(x)$ over the integers. Suppose that

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 \\ g(x) &= b_d x^d + b_{d-1}x^{d-1} + \dots + b_0 \\ h(x) &= c_e x^e + c_{e-1}x^{e-1} + \dots + c_0. \end{aligned}$$

for some n, d and $e > 1$.

As $a_0 = b_0c_0$ is not divisible by p^2 either b_0 or c_0 is not divisible by p. Possibly switching $g(x)$ and $h(x)$ we may assume that b_0 is not divisible by p. As $a_n = b_dc_e$ and a_n is not divisible by p, then neither is b_d nor c_e.

Let m be the smallest integer such that c_m is not divisible by p. We have

$$a_m = b_0c_m + b_1c_{m-1} + b_2c_{m-2} + b_3c_{m-3} + \dots.$$

Every term on the RHS but the first is divisible by p. The first term is not divisible by p as neither b_0 nor c_m is divisible by p. Thus the RHS is not divisible by p. So the LHS is not divisible by p. The only coefficient of $f(x)$ not divisible by p is a_n. So we must have that $m = n$ and so $h(x)$ is a polynomial of degree n.

Thus $f(x)$ is irreducible. □

Note that we can apply Eisenstein to the polynomial $x^2 - 2$ with the prime $p = 2$ to conclude that $x^2 - 2$ is irreducible over $\mathbb{Q}$. Here is a more interesting example:

Example 17.10. *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 $9 = 3^2$.

Corollary 17.11. *Let p be a prime. Then*

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

is irreducible over $\mathbb{Q}$.

Proof. By Gauss, it suffices to consider factorisations of $f(x)$ over $\mathbb{Z}$.

First note that

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

as can be easily checked. Consider the map

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}[x] \qquad \text{given by} \qquad f(x) \longrightarrow f(x+1).$$

This is an example of an evaluation homomorphism; in this case we evaluate $f(x)$ at $x+1$. Thus we get a ring homomorphism. This map is an isomorphism, since the inverse map sends $f(x)$ to $f(x-1)$ (evaluation at $x-1$).

Note that

$$\begin{aligned} g(x) &= f(x+1) \\ &= \frac{(x+1)^p - 1}{x} \\ &= x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-1} \\ &= x^{p-1} + px^{p-2} + \cdots + p. \end{aligned}$$

Observe that $\binom{p}{i}$ is divisible by p, for all $1 \leq i < p$, so that we can apply Eisenstein to the polynomial $g(x)$, using the prime p, to conclude that $g(x)$ is irreducible.

Suppose that $f(x) = h(x)k(x)$ is a factorisation of $f(x)$ over the integers. Then

$$g(x) = f(x+1) = h(x+1)k(x+1),$$

is a factorisation of $g(x)$ over the integers. Here we use the fact that the map $f(x) \longrightarrow f(x+1)$ is a ring homomorphism. As we already decided we cannot factor $g(x)$ into polynomials of lower degree, it follows that we cannot factor $f(x)$ either.

Thus $f(x)$ is irreducible. □

It seems worth pointing out a rather nice fact about factorisation of polynomials over a field F.

Theorem 17.12. *Let $p(x)$ be an irreducible polynomial over a field F.*

If $p(x)$ divides the product $f(x)g(x)$ of two polynomials over F then $p(x)$ must divide one of the factors $f(x)$ or $g(x)$.

Corollary 17.13. *Let $p(x)$ be an irreducible polynomial over a field F.*

If $p(x)$ divides the product $f_1(x)f_2(x)\dots f_k(x)$ of the polynomials over the field F then $p(x)$ must divide one of the factors $f_i(x)$, for some index $1 \leq i \leq k$.

Proof. Follows by induction on k, using (17.12). □

Theorem 17.14. *If F is a field then every nonconstant polynomial $f(x)$ can be factored into irreducible polynomials. Morever this factorisation is unique up to order and units.*

Proof. We first show that $f(x)$ can be factored into irreducibles.

If $f(x)$ is irreducible then we are done. If not, then $f(x) = g(x)h(x)$, where both $g(x)$ and $h(x)$ have smaller degree than $f(x)$. If $g(x)$ and $h(x)$ are irreducible then we are done. Otherwise one of $g(x)$ or $h(x)$ factors and we keep going. Eventually this process must stop, since at every stage we have a reducible polynomial the degree of the factors goes down.

Now suppose that we can find two factorisations,

$$p_1(x)p_2(x)p_3(x)\dots p_m(x) = q_1(x)q_2(x)q_3(x)\dots q_n(x).$$

of $f(x)$ into irreducibles. As $p_1(x)$ divides the LHS it must also divide the RHS. But then $p_1(x)$ must divide one of the factors. Re-ordering the factors on the RHS we may assume that $p_1(x)$ divides $q_1(x)$. As $q_1(x)$ is irreducible it follows that

$$q_1(x) = u_1p_1(x)$$

where u_1 is a constant polynomial. As u_1 is non-zero, u_1 is a unit. Replacing $q_1(x)$ with $u_1q(x)$ and cancelling $q_1(x)$ from both sides we obtain an equality of the form

$$p_2(x)p_3(x)\dots p_m(x) = u_1q_2(x)q_3(x)\dots q_n(x).$$

Now we repeat the same argument with $p_2(x)$. It must divide one of the factors, which we may assume is $q_2(x)$, so that $q_2(x) = u_2p_2(x)$. Cancelling $p_2(x)$ from both sides we obtain an equality of the form

$$p_3(x)p_4(x)\dots p_m(x) = u_1u_2q_3(x)q_4(x)\dots q_n(x).$$

Continuing in this way we eventually arrive at

$$1 = u_1u_2\dots u_mq_{m+1}(x)q_{m+2}(x)\dots q_n(x).$$

The only way this is possible is if $m = n$ so that we get

$$1 = u_1u_2\dots u_m.$$

It follows that $p_1, p_2, \dots, p_m$ and $q_1, q_2, \dots, q_n$ are the same, up reordering and unit factors. □

Example 17.15. *It is not hard to see that*

$$x^4 + 3x^3 + 2x + 4 = (x-1)^3(x+1) \in \mathbb{Z}_5[x].$$

We may also rewrite this factorisation as

$$x^4 + 3x^3 + 2x + 4 = (x-1)^2(2x-2)(3x+3) \in \mathbb{Z}_5[x].$$

Here we didn't change the order, but we messed around a little bit with the units.