3. PRIME POLYNOMIALS

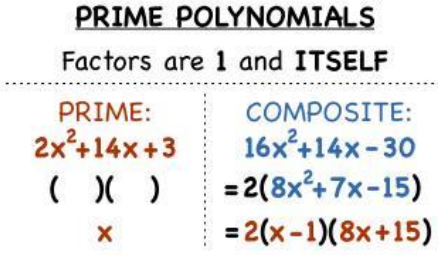
§3.1. Tests for Primeness

A polynomial $p(x) \in F[x]$ is **prime** (**irreducible**) over F if its degree is at least 1 and it cannot be factorised into polynomials of lower degree. Constant polynomials cannot be factorised into polynomials of lower degree, but for important technical reasons we exclude them, just as we don't allow the integer 1 to be called a prime number.

All other polynomials are called **composite** (or **reducible**) over F. Notice that we keep saying 'over F'. If we were to ask whether $x^2 - 2$ is prime, the correct answer would be "it depends on the field". Over $\mathbb{Q}$ it is prime, because we can't factorise it into two polynomials with rational coefficients. Over $\mathbb{R}$, of course, we can. We can write it as

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

A fundamental question that we'll consider is "how can you decide whether or not a given polynomial is prime over a given field".



Over $\mathbb{C}$, any polynomial of higher degree than 1 can be factorised completely into linear factors and so will be composite. This is because of the Fundamental Theorem of Algebra that states that every non-constant polynomial $f(x)$, over $\mathbb{C}$, has

a zero. A **zero** of a polynomial is an element θ of the field such that a(θ) = 0. By the Remainder Theorem $x - \theta$ will be a factor.

A linear polynomial is clearly prime no matter what the field is and a quadratic is prime if its discriminant has no square roots.

PRIMENESS TEST 1: Linear
Every polynomial in F[x] of degree 1 is prime over F.

PRIMENESS TEST 2: Quadratic
$ax^2 + bx + c \in$ F[x] is prime if and only if its discriminant, $b^2 - 4ac$ has no square roots in F.

Example 1: The quadratic $x^2 + x + 2$ is prime over $\mathbb{R}$ because its discriminant is –7, which is negative.

Example 2: The quadratic $x^2 + x - 3$ is prime over $\mathbb{Q}$ because its discriminant is 13 and $\sqrt{13}$ is irrational.

Example 3: The quadratic $x^2 + 2x - 5$ is prime over $\mathbb{Z}_7$ because its discriminant is 24 = 3 in $\mathbb{Z}_7$ and the squares mod 7 are 0, 1, 4 and 2 (9 = 2 mod 7), so 3 has no square root in $\mathbb{Z}_7$.

Testing for zeros is certainly one technique for showing that a polynomial is prime, but it only works up to degree 3.

PRIMENESS TEST 3: Cubics

Theorem 1: A cubic $a(x) \in F[x]$ is prime over F if and only if it has no zeros in F.

Proof: A prime cubic cannot have any zeros in F (otherwise, by the Remainder Theorem it would have a linear factor). Conversely if a polynomial of degree 2 or 3 has no zeros in F it must be prime because, if it could be factorised, one of the factors would have to be linear.

Example 4: $a(x) = x^3 + x + 1$ is prime over $\mathbb{Z}_2$ since $f(0) = f(1) = 1$. This test doesn't work if the degree exceeds 3.

PRIMENESS TEST 4: Quartics

Example 5: The quartic $(x^2 + 1)^2$ has no zeros in $\mathbb{R}$, yet it clearly isn't prime over $\mathbb{R}$.

Theorem 2: Suppose $a(x) \in \mathbb{Q}[x]$ is a quartic with irrational zeros $\alpha, \overline{\alpha}, \beta, \overline{\beta}$. If $|\alpha|^2 \notin \mathbb{Q}$ and $\alpha\beta \notin \mathbb{Q}$, then a(x) is prime over $\mathbb{Q}$.

Proof: Since a(x) has no rational zeros, it cannot factorise as a cubic times a quartic. Suppose it is the product of two rational polynomials. One of these will have α as a zero. If the other is α then $|\alpha|^2 \in \mathbb{Q}$. If the other is β or β then $\alpha\beta$ or $\alpha\beta$ $\mathbb{Q}$.

Theorem 2: A polynomial over $\mathbb{R}$ is prime if and only if it is linear or is quadratic with negative discriminant.

Proof: This follows from the fact that non-real zeros of real polynomials come in conjugate pairs.

If α and $\overline{\alpha}$ are non-real zeros then $(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\,\mathrm{Re}(\alpha)\,x + |\alpha|^2$ will be a quadratic factor with real coefficients.

Over $\mathbb{Q}$ there are prime polynomials of degree n for every positive degree.

If $n > 1$ the polynomial $a(x) = x^n - 2$ is prime. However this is not immediately obvious since, even if we know that the n'th roots of 2 are irrational, that merely shows that $a(x)$ has no linear factors. We'll be developing a test that *does* prove that $a(x)$ has no proper factors at all.

§3.2. Prime Polynomials over $\mathbb{Z}_p$

The fields of integers modulo a prime p are the most well known examples of fields with finitely many elements though, as we shall see later, other finite fields do exist.

In principle, testing for primeness over any finite field is perfectly straightforward. Since there are only finitely many polynomials of a given degree there are only finitely many possibilities to check.

PRIMENESS TEST 4: Brute Force (for Polynomials over a Finite Field)

If $a(x)$ has degree $n \geq 2$, list all the polynomials whose degree is m where $1 \leq m \leq n-1$. Now find all possible

products where the sum of the degrees of the factors is n. If one of these product is equal to a(x) then a(x) is composite. Otherwise it's prime.

Example 6: Find the prime polynomials over $\mathbb{Z}_2$ with degree at most 5.

Solution: Over $\mathbb{Z}_2$ the leading coefficient must be 1. For a polynomial of degree n there are n other coefficients which must be 0 or 1 and so there are 2^n possibilities. Altogether there are 2 linear polynomials, 4 quadratics, 8 cubics, 16 quartics and 32 quintics. From these we must eliminate the composite polynomials. Those that remain will be prime.

This might appear to require a considerable amount of effort, but in fact it is surprisingly easy if the degree is not too big. Both linear polynomials, x and $x + 1$ are prime (linear polynomials are always prime). For quadratics and cubics we need only eliminate those which have a zero in $\mathbb{Z}_2$. Now there are only two possible values, 0 and 1. A polynomial with 0 as a zero will clearly have zero constant term and a polynomial with 1 as a zero will have an even number of terms. Eliminating these we get the following list of polynomials with no zeros:

- quadratic: $x^2 + x + 1$
- cubic: $x^3 + x^2 + 1$ and $x^3 + x + 1$
- quartic: $x^4 + x^3 + 1$, $x^4 + x^2 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$

Now for quadratics and cubics, having no zeros is enough to ensure primeness so there is just one prime quadratic and there are two prime cubics.

How could a quartic with no zeros possibly factorise? Only by being the product of two prime quadratics. But $x^2 + x + 1$ is the only prime quadratic so the only extra one to be eliminated is

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

(remember we're working mod 2), leaving three prime quartics: $x^4 + x^3 + 1$, $x^4 + x + 1$ and $x^4 + x^3 + x^2 + x + 1$.

Before going onto the quintics let me introduce an abbreviated notation for these polynomials by simply listing the coefficients as a binary string, starting with the 1 for the leading coefficient. The prime polynomials up to degree 4 are thus:

10, 11, 111, 1101, 1011, 11001, 10011, 11111.

Now the quintics with no zeros are:

110001, 101001, 100101, 100011, 111101, 111011, 110111, 101111.

We must eliminate the products of a prime quadratic with a prime cubic. But there is only one prime quadratic, 111, and only two prime cubics, 1101 and 1011. So there are just two composite quintics to be eliminated from the above list.

To discover what they are we could revert to the usual notation, though it is possible to do the multiplication 'synthetically' with just the coefficients,

rather like long multiplication. The only difference is that there is no carrying'. In each position we reduce the column total mod 2.

```
 1101 1011
 111 × 111 ×
 1101 1011
 1101 1011
1101 1011
100011 110001
```

These are $x^5 + x + 1$ and $x^5 + x^4 + 1$ in normal notation. Eliminating these we are left with the following six prime quintics of degree 5, mod 2:

101001, 100101, 111101, 111011, 110111, 101111.

In normal notation these are:

$x^5 + x^3 + 1$, $x^5 + x^2 + 1$, $x^5 + x^4 + x^3 + x^2 + 1$,
$x^5 + x^4 + x^3 + x + 1$, $x^5 + x^4 + x^2 + x + 1$ and
$x^5 + x^3 + x^2 + x + 1$.

§3.3. Integer Polynomials

An **integer polynomial** is one with integer coefficients, that is, an element of $\mathbb{Z}[x]$.

A **primitive polynomial** is an integer polynomial where the GCD of the coefficients is 1.

Theorem 3: If $a(x) \in \mathbb{Q}[x]$ then $a(x) = q.b(x)$ for some $q \in \mathbb{Q}$ and primitive $b(x) \in \mathbb{Z}[x]$.

Proof: Let s be the least common multiple of the denominators of the coefficients of $a(x)$.
Then $s.a(x) \in \mathbb{Z}[x]$. Let r be the greatest common divisor of the coefficients of $s.a(x)$.
Then $g(x) = (s/r)f(x)$ is primitive. Putting $q = r/s$ we obtain the required result.

Example 7: Let $a(x) = \frac{9}{10}x^3 + \frac{15}{4}x^2 - \frac{24}{5}x + \frac{21}{2} \in \mathbb{Q}[x]$.
The LCM of the denominators is 20 and the GCD of the numerators is 3.
Multiplying $a(x)$ by 20/3 we get $6x^3 + 25x^2 - 32x + 70$, which is a primitive polynomial.

Given a polynomial with integer coefficients how can we decide if it's prime over $\mathbb{Q}$? The next theorem reduces the problem to that of deciding whether it's prime over $\mathbb{Z}$.

Theorem 4 (GAUSS'S THEOREM):
If $a(x) \in \mathbb{Z}[x]$ is prime over $\mathbb{Z}$ then it is prime over $\mathbb{Q}$.
Proof: Let $a(x)$ be a rational polynomial of degree n and suppose that:
$a(x) = b(x)\, c(x)$ where:
$b(x) = b_s x^s + ... + b_1 x + b_0 \in \mathbb{Q}[x]$ with degree $s < n$ and
$c(x) = c_t x^t + ... + c_1 x + c_0 \in \mathbb{Q}[x]$ with degree $t < n$.

Define $b_i = 0$ if $i > s$ and $c_i = 0$ if $i > t$.

By Theorem 3, $b(x) = q.d(x)$ and $c(x) = r.e(x)$ for some non-zero $q, r \in \mathbb{Q}$ and primitive polynomials $d(x)$, $e(x)$.

Let $qr = u/v$ where $GCD(u, v) = 1$ and $v > 0$.
Then $v.a(x) = u.d(x)\ e(x)$.
If $v = 1$ then we have a suitable integer factorisation.
Suppose $v > 1$ and let p be a prime divisor of v.
Since u and v are coprime, p doesn't divide u.

Since $d(x)$ is primitive, p doesn't divide all of its coefficients. Similarly for $e(x)$.

So for some $h \leq s$ and $k \leq t$:
- p divides d_i for all $i < h$ but p doesn't divide d_h and
- p divides e_i for all $i < k$ but p doesn't divide e_k.

(If p doesn't divide any of these coefficients then $h = k = 0$.)

Equating the coefficients of x^{h+k} in the equation
$v.a(x) = u.d(x)\ e(x)$ we get:

$$va_{h+k} = u(d_0e_{h+k} + ... + d_he_k + ... + d_{h+k}\ e_0).$$

Now p divides v and d_i for $i < h$ and p divides e_i for $i < k$, so p divides ud_he_k.

But p doesn't divide any of these three factors, a contradiction. That's why we must have $v = 1$ and hence an integer factorisation.

Example 8: Let $a(x) = x^3 - 3x - 1$. By examining the signs of $x^3 - 3x - 1$ at the endpoints we see that there are three real zeros, one in each of the open intervals $(-2, -1)$, $(-1, 0)$, $(1, 2)$ and so there are no integer roots. Hence $a(x)$ is prime over $\mathbb{Z}$ and so by Gauss's Theorem it's prime over $\mathbb{Q}$.

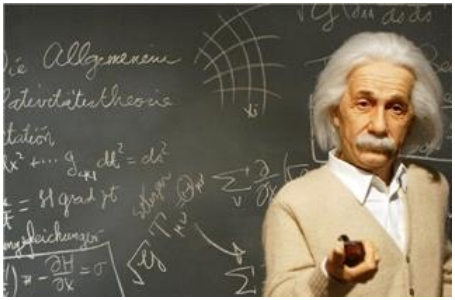
§3.4. Tests for Primeness over $\mathbb{Q}$

Given a rational polynomial, how can we decide if it's prime over $\mathbb{Q}$? There's no simple systematic procedure that can be applied in every case. Instead we present a number of techniques that can be used in specific situations.

We can multiply any rational polynomial by a suitable integer to produce an integer polynomial and, by Gauss's Theorem, primeness over $\mathbb{Z}$ implies primeness over $\mathbb{Q}$, so throughout this section all polynomials are assumed to have integer coefficients.

PRIMENESS TEST 5: Eisenstein's Test

Do not confuse Gotthold Eisenstein (1823–1852) with Albert Einstein (1879–1955). Eisenstein was a mathematician, while Einstein was a theoretical physicist.



Theorem 5 (EISENSTEIN'S THEOREM):
If a(x) = $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ and p is a prime such that:

- p divides $a_0, a_1, ... , a_{n-1}$,
- p does not divide a_n,
- p^2 does not divide a_0

then a(x) is prime over $\mathbb{Q}$.

Proof:
Let a(x) = $(b_r x^r + ... + b_0)(c_s x^s + ... + c_0)$ where $r, s \geq 1$.
Since p doesn't divide $a_n = b_r c_s$, it doesn't divide either of b_r or c_s.
Let m be the smallest value of i such that p doesn't divide b_i.
Then p divides b_i for any $i < m$ and $m \leq r < n$.
Now $a_m = b_0 c_m + ... + b_m c_0$.

Since p divides b_i for $i < m$ and also a_m then it must divide $b_m c_0$. But it doesn't divide b_m, so it must divide c_0.

Similarly p divides b_0 and so p^2 must divide a_0 (which equals $b_0 c_0$), a contradiction. So in fact such an $a(x)$ cannot factorise into polynomials of lower degree over $\mathbb{Z}$ and so by Gauss's Theorem it is prime over $\mathbb{Q}$.

Example 9: The polynomial

$$x^{14} + 10x^{11} + 60x^{10} + 50x + 20$$

is prime over $\mathbb{Q}$ since it satisfies the Eisenstein criterion for $p = 5$. [Note that $p = 2$ won't do because 2^2 divides 20.]

Of course if an integer polynomial fails one or more of the Eisenstein criteria that doesn't mean that it is composite. There are plenty of prime polynomials which don't conform to the above conditions. While Eisenstein's Theorem is useful for generating prime polynomials of a given degree it's not particularly useful for testing a random polynomial. In such cases a more useful technique is to consider the corresponding polynomial over $\mathbb{Z}_p$ for some prime p.

PRIMENESS TEST 6: Mod *p* Test

Theorem 6: If $a(x) \in \mathbb{Z}[x]$ is prime over $\mathbb{Z}_p$, for any prime p, then it is prime over $\mathbb{Z}$.

Proof: If $a(x) = b(x)c(x)$ was a factorisation over $\mathbb{Z}$ then reducing each of these factors modulo p we'd get a non-trivial factorisation of $a(x)$.

Example 10: Consider $a(x) = 5x^3 + 37x^2 + 57x + 21$. Over $\mathbb{Z}_2$ this reduces to $x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1)$. Does this mean that $a(x)$ is composite over $\mathbb{Z}$?

In fact $a(x) = (x^2 + 6x + 3)(5x + 7)$ and so does happen to be composite over $\mathbb{Z}$.

But beware. If an integer polynomial is *composite* over $\mathbb{Z}_p$ that doesn't mean that it has to be composite over $\mathbb{Z}$.

Example 11: $a(x) = x^4 + 6x^3 + 3x^2 + 3x + 3$ reduces to $x^4 + x^2 + x + 1$ over $\mathbb{Z}_2$.
This factorises over $\mathbb{Z}_2$ as $(x + 1)(x^3 + x^2 + 1)$.
This might (mistakenly) lead us to believe that $f(x)$ is composite over $\mathbb{Z}$, it is clearly prime over $\mathbb{Q}$ by Eisenstein's Theorem.

So the mod p test is a one-way test. If it's prime over $\mathbb{Z}_p$ then it's prime over $\mathbb{Z}$, and hence over $\mathbb{Q}$, but not conversely.

Example 12: Prove that

$$3x^5 - x^4 + 12x^3 - 21x^2 + 81x + 243$$

is prime over $\mathbb{Q}$.
Solution: Modulo 2 the polynomial becomes $x^5 + x^4 + x^2 + x + 1$ which, as we saw in Example 3, is prime over $\mathbb{Z}_2$. Hence this polynomial is prime over $\mathbb{Z}$ and hence, by Gauss's Theorem, it's prime over $\mathbb{Q}$.

§3.5. Conjugate Polynomials

If $a(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, where a_0 and a_n are non-zero, we define its **conjugate** to be

$$a^*(x) = a_0 x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n.$$

This is not to be confused with taking the complex conjugate of the coefficients.

Theorem 7: Suppose a(x) has degree n and a(0) $\neq 0$.
Then a*(x) = $x^n a(x^{-1})$.
Proof: Suppose a(x) = $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$.
Then a(x^{-1}) = $a_n x^{-n} + a_{n-1}x^{-(n-1)} + ... + a_1 x^{-1} + a_0$

$$= \frac{a_n + a_{n-1}x + ... + a_1 x^{n-1} + a_0 x^n}{x^n} = \frac{a^*(x)}{x^n}.$$

Corollary: The zeros of a*(x) are precisely the inverses of the zeros of a(x).

Example 13: a(x) = $x^2 - 5x + 6$ has zeros 2, 3.
Hence a*(x) = $6x^2 - 5x + 1$ has zeros $\frac{1}{2}$ and $\frac{1}{3}$.

Theorem 8: Suppose a(x) = b(x)c(x) where a(0) $\neq 0$.
Then a*(x) = b*(x)c*(x).
Proof: Suppose that a(x) = $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ where a_0 and a_n are non-zero and suppose that b(x), c(x) have degrees r, s respectively.

$$a^*(x) = x^n a(x^{-1}) = x^r b(x^{-1}).x^s c(x^{-1}) = b^*(x)c^*(x).$$

Corollary: If a(0) $\neq 0$ then a(x) is prime if and only if $a^*(x)$ is prime.

A polynomial a(x) is **symmetric** if a*(x) = a(x). The following theorem mirrors the theorem about zeros of a real polynomial coming in conjugate pairs.

Theorem 9:
(1) The zeros of a symmetric polynomial a(x) come in inverse pairs.
(2) If deg a(x) is odd then –1 is a zero.
Proof: The first part is now obvious. If a(x) has odd degree then one of the zeros must be its own inverse and so must be ±1. But if
$a(x) = a_0x^{2n+1} + a_1x^{2n} + ... + a_nx^{n+1} + a_nx^n + ... + a_1x + a_0$
then clearly $x = -1$ is a zero.
Depending on the coefficients it's also possible for $x = 1$ to be a zero.

Example 14: $a(x) = x^5 + x^4 - 6x^3 - 6x^2 + x + 1$ is a symmetric polynomial, Solve $a(x) = 0$.
Solution:
$a(-1) = 0$ so $x + 1$ is a factor, and
$a(x) = (x + 1)(x^4 - 6x^2 + 1)$.
Solving $x^4 - 6x^2 + 1 = 0$ as a quadratic in x^2 we get
$$x^2 = \frac{6 \pm \sqrt{36 - 4}}{2} = 3 \pm 2\sqrt{2}.$$
Hence $x = \pm\sqrt{3 \pm 2\sqrt{2}} = \pm(1 \pm \sqrt{2})$.
So the zeros of $a(x)$ are -1, $1 + \sqrt{2}$, $1 - \sqrt{2}$, $-1 + \sqrt{2}$ and $-1 - \sqrt{2}$.
Note that these come in inverse pairs since
$$\frac{1}{\sqrt{2} + 1} = \frac{\sqrt{2} - 1}{2 - 1} = \sqrt{2} - 1.$$

§3.6. Minimum Polynomials

Every complex *number* α is a zero of some polynomial, namely $x - \alpha$. However if we insist that the coefficients come from some proper subfield of $\mathbb{C}$ this may no longer be the acceptable. For example if $\alpha = \sqrt{2}$ and the field is $\mathbb{Q}$, the polynomial $x - \sqrt{2}$ no longer qualifies. However $x^2 - 2$ does.

If $\alpha = \sqrt{2} + \sqrt{3}$ then $\alpha^2 = 5 + 2\sqrt{6}$ and so

$$(\alpha^2 - 5)^2 = 24.$$

Hence α is a zero of the rational polynomial

$$x^4 - 10x^2 + 1.$$

If $\alpha = e^{2\pi i/9}$ then α is a zero of the rational polynomial

$$x^9 - 1.$$

For some values of α there's no rational polynomial at all that has α as a zero. Well, that is excepting the zero polynomial which has every complex number as a zero! This leads us to the concept of algebraic and transcendental numbers.

If F is a subfield of $\mathbb{C}$ we say that $\alpha \in \mathbb{C}$ is **algebraic over F** if $a(\alpha) = 0$ for some non-zero $a(x) \in F[x]$. On the other hand if no such polynomial exists we say that α is **transcendental over F**.

Over $\mathbb{C}$ this classification isn't very interesting. Every complex number is algebraic over $\mathbb{C}$ since any α is

the zero of the linear polynomial $x - \alpha$. Over $\mathbb{C}$ there are no transcendental numbers at all.

Over $\mathbb{R}$ the classification is no more interesting. Again, there are no transcendental numbers over $\mathbb{R}$, for if $a + b\mathrm{i} \in \mathbb{C}$ it is a zero of the real polynomial

$$x^2 - 2ax + (a^2 + b^2).$$

But over $\mathbb{Q}$ the classification is extremely interesting. In fact in this classical case we drop all reference to the field and simply say that α is **algebraic** or **transcendental**. In the absence of any field when these terms are used it is understood that we mean algebraic or transcendental over $\mathbb{Q}$.

As we saw earlier $\sqrt{2} + \sqrt{3}$ and $e^{2\pi i/9}$ are algebraic (over $\mathbb{Q}$). But it's possible to demonstrate that the special constants π and e are transcendental.

The set of algebraic numbers over a field F can be shown to be a subfield of $\mathbb{C}$. This is proved in Chapter 5. Over $\mathbb{Q}$ the field of algebraic numbers is a proper subfield. This can be shown by a counting argument, using the theory of transfinite numbers. Although $\mathbb{Q}$ and $\mathbb{R}$ are both infinite it can be shown that they can't be put into 1-1 correspondence. There are, in fact, different sizes of infinity and the size of $\mathbb{Q}$ is the smallest infinite number, while the size of $\mathbb{R}$ is bigger. If you want to find out more about the many different infinite numbers you can find them discussed in my notes on *Set Theory*.

Example 15: If $\alpha = e^{2\pi i/9}$ then α is algebraic being a zero of the polynomial $x^9 - 1$. But this is not the only non-zero rational polynomial which could have been used. We could have used any multiple of the polynomial $x^9 - 1$ such as $(x^9 - 1)(x^7 + 5) = x^{16} + 5x^9 - x^7 - 5$.

What we clearly want is to select from all polynomials having α as a zero one of *lowest* degree. This doesn't lead us to a unique candidate since $2x^9 - 2$ has the same degree as $x^9 - 1$. So it's natural to insist that the polynomial be *monic*.

The **minimum polynomial** of α over a field F is the monic polynomial over F, of lowest degree, having α as a zero. The use of the word 'the' suggests that it's unique, but we don't know that yet. Conceivably a certain α could be a zero of two different monic polynomials of the same degree and not be a zero of any non-zero polynomial of any lower degree. In fact this never happens, as we'll prove shortly. But firstly let's return to the number $\alpha = e^{2\pi i/9}$.

Example 16:
Find the minimum polynomial of $e^{2\pi/9}$ over $\mathbb{Q}$.
Solution: We know that α is a zero of the polynomial $x^9 - 1$ with rational coefficients.
But is this the *minimum* polynomial over $\mathbb{Q}$?
Notice that $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$.
So α is a zero of one (or possibly both) of these factors.

Either way there would be a rational polynomial of degree less than 9 which has α as a zero, meaning that $x^9 - 1$ could not be its minimum polynomial over $\mathbb{Q}$.

Clearly α is not a zero of the first factor. So it must be a zero of $x^6 + x^3 + 1$. Is this now the required minimum polynomial? If we can show that this is a prime polynomial then the answer is "yes".

Example 17:
Show that $a(x) = x^6 + x^3 + 1$ is prime over $\mathbb{Q}$.
Solution: The easiest test to use is Eisenstein's, but unfortunately this polynomial doesn't qualify. However it is often possible to make a linear substitution so that it does.

In this case, if $d(x) = a(x + 1)$ then
$d(x) = a(x + 1) = (x + 1)^6 + (x + 1)^3 + 1$
$= x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 3.$
So $d(x)$ is clearly prime by Eisenstein's test.

Now if $a(x) = b(x)c(x)$ was a non-trivial factorisation then $d(x) = a(x + 1) = b(x + 1)c(x + 1)$, a contradiction. Hence $x^6 + x^3 + 1$ is prime, and so it is the minimum polynomial of $e^{2\pi/9}$.

Theorem 10: If $a(x) \in \mathbb{Z}[x]$ and $a(ax + b)$ is prime over $\mathbb{Z}$ then so is $a(x)$.
Proof: The argument is as in Example 17. Of course we would need $a \neq 0$ but we didn't have to say that because

if $a = 0$ then $a(ax + b) = a(b)$ is a constant and constant polynomials are not prime.

Theorem 11: The minimum polynomial of α over F:

(1) has α as a zero;
(2) is monic;
(3) divides any polynomial having α as a zero;
(4) is unique;
(5) is prime.

Proof: Properties (1) and (2) are incorporated into the definition. We prove (3) next.

Let $p(x)$ be *any* minimum polynomial of α over F (we can't say "the" yet).

Let $a(x) \in F[x]$ with $a(\alpha) = 0$.

Now by the Division Algorithm $a(x) = p(x)q(x) + r(x)$ for some $q(x), r(x) \in F[x]$ with $r(x) = 0$ or $\deg r(x) < \deg p(x)$.

Now $r(\alpha) = a(\alpha) - p(\alpha)q(\alpha) = 0$ since $p(\alpha) = a(\alpha) = 0$.

If $r(x)$ is not the zero polynomial this contradicts the minimality of the degree of the minimum polynomial. Hence $r(x) = 0$ and so $a(x) = p(x)q(x)$.

We can now prove (4). By (3), two minimum polynomials must divide each other and so must be a non-zero constant multiple of one another. Being monic they must therefore be equal.

Finally we come to (5). Clearly p(x) cannot be a constant polynomial, so it remains to show that it has no proper factorisation (into factors of lower degree). Suppose, to the contrary, that p(x) = a(x)b(x) is a non-trivial factorisation. Then p(α) = a(α)b(α) and since these belong to a field we must have a(α) = 0 or b(α) = 0. Either case would contradict the minimality of the degree of the minimum polynomial. Hence p(x) is prime.

We can define minimum polynomials of matrices in a similar way. These matrix minimum polynomials satisfy properties (1) to (4) but not necessarily (5). The difference is that if we have p(M) = a(M)b(M) for matrices we can't conclude that either a(M) or b(M) is zero. So minimum polynomials of matrices need not be prime.

Example 18: The minimum polynomial of $\sqrt{2}$ over Q is $x^2 - 2$. There are two parts to this. It is not enough to observe that $\sqrt{2}$ is a zero of $x^2 - 2$. We must also verify that $x^2 - 2$ is prime. We can do this in many ways.

(1) $x^2 - 2$ has no rational zeros and has degree at most 3 and so is prime (Theorem 1).
(Remember that 'no zeros in the field' only guarantees primeness for quadratics and cubics.)

(2) $x^2 - 2$ is prime over $\mathbb{Q}$ by Eisenstein's Theorem (Theorem 5) using p = 2.

(3) $x^2 - 2$ has no zeros over $\mathbb{Z}_3$. So it is prime over $\mathbb{Z}_3$ and hence over $\mathbb{Q}$.

We now apply these primality tests to find another example of a minimum polynomial, one that will play an important part in the proof of the impossibility of trisecting any angle by ruler and compass.

Example 19: Find the minimum polynomial of $2\cos(\pi/9)$ over $\mathbb{Q}$.
Solution: Remember that there are two thing to do:
(A) find a suitable candidate and
(B) prove that it's prime.

(A) Let $c = \cos(\pi/9)$ and $s = \sin(\pi/9)$.
By De Moivre's Theorem:
$(c + is)^3 = \cos(\pi/3) + i \sin(\pi/3)$.
Expanding $(c + is)^3$ and equating real parts we get

$$c^3 - 3cs^2 = ½.$$

Putting $s^2 = 1 - c^2$ we get $4c^3 - 3c = ½$ and if $x = 2c$ we get $x^3 - 3x - 1 = 0$.

(B) We have three possible techniques we can choose from. We only need one of them to show that $x^3 - 3x - 1$ is prime over $\mathbb{Q}$. However, to provide practice with the techniques we'll consider all three.

(1) **(LOW DEGREE)** It's not difficult to see, from what we've done above, that the zeros of $x^3 - 3x - 1$ are $2\cos(\pi/9)$, $2\cos(5\pi/9)$ and $2\cos(7\pi/9)$. If we could guarantee that none of these is rational we'd know that $x^3 - 3x - 1$ is prime (cubic with no rational zeros). But although they 'look' irrational it might be quite messy to show directly that they are.

(2) **(EISENSTEIN)** $x^3 - 3x - 1$ doesn't satisfy the Eisenstein criterion for any prime. But if we replace x by $x + 1$ we get $x^3 + 3x^2 + 3$ which does. So $x^3 - 3x - 1$ is prime. (Incidentally this now settles the fact that the above three values of $2\cos x$ are all irrational.)

(3) **(MOD *p*)** Mod 3, $x^3 - 3x - 1$ becomes $x^3 + 2$. Unfortunately this isn't prime over $\mathbb{Z}_3$ so this tells us nothing about $x^3 - 3x - 1$ over $\mathbb{Q}$.
Mod 5 it becomes $x^3 + 2x + 4$ which is a cubic with no zeros in $\mathbb{Z}_5$ and so is prime over $\mathbb{Z}_5$ and hence $x^3 - 3x - 1$ is prime over $\mathbb{Q}$.

EXERCISES FOR CHAPTER 3

Exercise 1: For each of the following determine whether it is true or false. Give reasons.

(1) Every polynomial is composite over $\mathbb{C}$.
(2) There are no prime cubics over $\mathbb{R}$.
(3) There is a prime polynomial of degree 24 over $\mathbb{Q}$.
(4) If a polynomial has no zeros in $\mathbb{Q}$ it's prime over $\mathbb{Q}$.
(5) Every polynomial is either prime or composite.
(6) There are only finitely many prime quartics over $\mathbb{Z}_5$.
(7) A polynomial of the form $x^3 + px^2 + p^2x + p^3$ is prime over $\mathbb{Q}$ by Eisenstein.

Exercise 2: Prove that the following polynomials are prime over $\mathbb{Q}$.

(i) $x^7 + 6x^4 - 18x^3 + 42x + 12$
(ii) $x^4 + 10x^3 - 2x^2 + 7x + 91$
(iii) $x^4 + x^2 - 1$
(iv) $x^6 + x^5 - x^4 + 5x^3 + 4x^2 + 4x + 5$

Exercise 3: Which of the following polynomials are prime over the field indicated?
For those that are composite you must exhibit a factorisation over the appropriate field.
For those that are prime you must give valid reasons.

(i) $x + \pi$ over $\mathbb{C}$;
(ii) $x^2 + 4x + 3$ over $\mathbb{R}$;
(iii) $x^2 + 4x + 6$ over $\mathbb{R}$;

(iv) $x^4 + 1$ over $\mathbb{R}$;
(v) $x^3 - 1$ over $\mathbb{Q}$;
(vi) $x^3 + 2$ over $\mathbb{Q}$;
(vii) $x^5 + x^2 - x + 1$ over $\mathbb{Q}$;
(viii) $x^4 + x + 1$ over $\mathbb{Z}_3$;
(ix) $x^4 + 1$ over $\mathbb{Z}_3$;
(x) $x^{13} - 50x^9 + 60x^7 - 300x + 60$ over $\mathbb{Q}$;
(xi) $15x^4 + 117x - 9$ over $\mathbb{Q}$;
(xii) $x^4 + x^3 + x^2 + x + 1$ over $\mathbb{Q}$.

Exercise 4: Find all the monic prime quartics over $\mathbb{Z}_3$. (To save writing, represent the quartics by their sequence of coefficients, eg 102021 represents $x^5 + 2x^3 + 2x + 1$. List your polynomials, in this compact way and in some lexicographic order, and then provide details of your working.)

Exercise 5: Find the minimum polynomials of $\pi + i$:
(i) over $\mathbb{C}$,
(ii) over $\mathbb{R}$,
(iii) over $\mathbb{Q}$.

Exercise 6: Find the minimum polynomials over $\mathbb{Q}$ of the following:
(i) $1 + \sqrt{7}$
(ii) $\sqrt{2} + i$
(iii) $\sqrt{11 + 6\sqrt{2}}$;
(iv) $e^{2\pi i/5}$;

(v) $\tan(\pi/5)$;
(vi) $i + \omega$;
(vii) $\sqrt[3]{2} + \sqrt{3}$.

Exercise 7: Prove that if $k \in \mathbb{Q}$ then $\cos(2k\pi)$ is an algebraic number.

Exercise 8: Prove that if α is a non-zero algebraic number then so are $\sqrt{\alpha}$ and $\frac{1}{\alpha}$.

SOLUTIONS FOR CHAPTER 3

Exercise 1:
(1) **FALSE** The linear ones are prime.
(2) **TRUE** Every real cubic has a real zero.
(3) **TRUE** $x^{24} - 2$ is prime by Eisenstein's Theorem.
(4) **FALSE** It could be the product of two prime quadratics.
(5) **FALSE** The constant polynomials are neither.
(6) **TRUE** There are only 2500 quartics altogether, over $\mathbb{Z}_5$.
(7) **FALSE** Eisenstein's Theorem fails to prove primeness since the constant term is divisible by p^2. But this doesn't prove that it's composite. However $x = -p$ is a zero so the polynomial has the linear factor $x + p$.

Exercise 2:
(i) Eisenstein with $p = 3$ [Note: $p = 2$ doesn't work.]

(ii) mod 2 it is $x^4 + x + 1$ which is prime over $\mathbb{Z}_2$.
(iii) Let $a(x) = x^4 + x^2 + 2$. This is a quadratic in x^2 and so the zeros of $a(x)$ are:

$$\sqrt{\frac{-1+\sqrt{5}}{2}}, -\sqrt{\frac{-1+\sqrt{5}}{2}}, \sqrt{\frac{-1-\sqrt{5}}{2}}, -\sqrt{\frac{-1-\sqrt{5}}{2}}$$

Since $\sqrt{5}$ is irrational, none of these are rational. Hence if a(x) factorises over $\mathbb{Q}$ it must be as a product of two rational quadratics, say $b(x)$ and $c(x)$.
Without loss of generality $\alpha = \sqrt{\frac{-1+\sqrt{5}}{2}}$ is a zero of $b(x)$. The other zero of $b(x)$ must be $-\sqrt{\frac{-1+\sqrt{5}}{2}}$, since the other two are non-real. But the product of these is $-\frac{-1+\sqrt{5}}{4}$ which is not rational.
(iv) Mod 2 the polynomial becomes $x^6 + x^5 + x^4 + x^3 + 1$ which factorizes into primes as
$(x^2 + x + 1)(x^4 + x + 1)$.
Mod 3 it is $x^6 + x^5 + 2x^4 + 2x^3 + x^2 + x + 2$ which factorizes into primes as $(x^3 + x^2 + 2)(x^3 + 2x + 1)$.
Thus no factorization over $\mathbb{Z}$ can give rise to consistent prime factorizations over both $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

Exercise 3:
(i) **PRIME** A linear polynomial over any field is prime.
(ii) **COMPOSITE** It is $(x + 1)(x + 3)$
(iii) **PRIME** The discriminant is –8 and so the polynomial has no real zeros. Being a quadratic it must be prime over $\mathbb{R}$.

(iv) **COMPOSITE** The only prime polynomials over $\mathbb{R}$ are the linear ones and the prime quadratics.
This one is $(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$.
(v) **COMPOSITE** $x - 1$ is a factor.
(vi) **PRIME** The zeros of $x^3 + 4$ over $\mathbb{C}$ are:

$$-4^{1/3}, -4^{1/3}\omega, -4^{1/3}\omega^2.$$

None of these is rational and so the polynomial, being a cubic, must be prime.
(vii) **COMPOSITE** It is $(x^2 + 1)(x^3 - x + 1)$.
(viii) **COMPOSITE** $x = 1$ is a zero.
(ix) **PRIME** $x^4 + 1$ has no zeros so if composite it would have to be the product of two prime quadratics (including the case of a prime quadratic squared).
These prime quadratics over $\mathbb{Z}_3$ are $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$.
No product of two of these is equal to $x^4 + 1$.
(x) **PRIME** By Eisenstein for p = 5.
(xi) **PRIME** Mod 2 it becomes $x^4 + x + 1$ which is prime over $\mathbb{Z}_2$. Note that Eisenstein fails.
(xii) **PRIME** Replacing x by $x + 1$ we get:
$(x + 1)^4 + (x + 1)^3 + (x + 1)^2 + (x + 1)$
$= x^4 + 5x^3 + 10x^2 + 10x + 5$ which is prime over $\mathbb{Q}$ by Eisenstein for $p = 5$. Hence the given polynomial must be prime over $\mathbb{Q}$.

Exercise 4: The monic quartics over $\mathbb{Z}_3$ with non-zero constant terms are:
10001, 10002, 10011, 10012, 10021, 10022, 10101, 10102, 10111, 10112, 10121, 10122, 10201, 10202,

10211, 10212, 10221, 10222, 11001, 11002, 11011, 11012, 11021, 11022, 11101, 11102, 11111, 11112, 11121, 11122, 11201, 11202, 11211, 11212, 11221, 11222, 12001, 12002, 12011, 12012, 12021, 12022, 12101, 12102, 12111, 12112, 12121, 12122, 12201, 12202, 12211, 12212, 12221, 12222.

Eliminating those with $x = \pm 1$ as a zero we get:
10001, 10012, 10022, 10102, 10111, 10121, 10201, 10202, 11002, 11012, 11021, 11101, 11111, 11122, 11221, 11222, 12002, 12011, 12022, 12101, 12112, 12121, 12211, 12212.

These are either prime or the product of two monic prime quadratics. By a similar process we find that the monic prime quadratics are: 101, 112, 122.
Their products (including their squares) are:

	101	112	122
101	10201	11012	12022
112		12211	10001
122			11221

Eliminating these we have the monic prime quartics:

10012, 10022, 10102, 10111, 10121, 10202, 11002, 11021, 11101, 11111, 11122, 11222, 12002, 12011, 12101, 12112, 12121, 12212.

Exercise 5:
(i) Over $\mathbb{C}$ it is clearly $x - (\pi + i)$.
(ii) Let $\alpha = \pi + i$.
Then $(\alpha - \pi)^2 + 1 = 0$ so α is a zero of
$a(x) = x^2 - 2\pi x + (1 + \pi^2)$. The zeros of $a(x)$ are $\pi \pm i$ so $a(x)$ has no real zeros and, being quadratic, it is prime over $\mathbb{R}$. Hence the minimum polynomial of $\pi + I$ over $\mathbb{R}$ is $x^2 - 2\pi x + (1 + \pi^2)$.
(iii) There's no minimum polynomial of $\pi + i$ over $\mathbb{Q}$ since $\pi + i$ is not algebraic over $\mathbb{Q}$. The reason for this is that if $\pi + i$ was algebraic then $\pi = (\pi + i) - i$ would be in the field of algebraic numbers, a contradiction. [We are assuming two things about algebraic numbers that haven't been proved here: (1) π is transcendental; (2) the algebraic numbers form a field.]

Exercise 6:
(i) Let $\alpha = 1 + \sqrt{7}$.
Then $(\alpha - 1)^2 = 7$ and hence $\alpha^2 - 2\alpha - 6 = 0$.
Is $m(x) = x^2 - 2x - 6$ prime over $\mathbb{Q}$?
The discriminant is $\Delta = 24$ and since $\sqrt{24} \notin \mathbb{Q}$, $m(x)$ has no rational zeros, and being quadratic, it is prime.
Hence the minimum polynomial of $1 + \sqrt{7}$ over $\mathbb{Q}$ is

$$x^2 - 2x - 6.$$

(ii) Let $\alpha = \sqrt{2} + i$.
Then $(\alpha - i)^2 = 2$ and so $\alpha^2 - 2\alpha i - 3 = 0$.
Hence $\alpha^2 - 3 = 2\alpha i$ and so

$(\alpha^2 - 3)^2 = -4\alpha^2$, which simplifies to $\alpha^4 - 2\alpha^2 + 9 = 0$.
So α is a zero of $m(x) = x^4 - 2x^2 + 9$.
Is it prime over $\mathbb{Q}$?

The mod p technique clearly fails for $p = 2$ and 3 and trying it for any larger primes would be daunting. Is there another way?

Clearly the four zeros of $m(x)$ are:

$$\sqrt{2} + i,\ \sqrt{2} - i,\ -\sqrt{2} + i \text{ and } -\sqrt{2} - i.$$

All four are irrational (in fact none of them is even real) so $m(x)$ has no rational zeros.

The only chance of it being composite is for it to be the product of two prime quadratics. Now these prime quadratic would have to have two of the above four zeros. The sum and product of these would have to be rational. A quick check reveals that this is not possible.
Hence the minimum polynomial of $\sqrt{2} + i$ over $\mathbb{Q}$ is

$$x^4 - 2x^2 + 9.$$

(iv) Let $\alpha = e^{2\pi i/5}$. Then $\alpha^5 - 1 = 0$. However this factorizes as $(\alpha - 1)(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = 0$ and since $\alpha \neq 1$, α is a zero of $f(x) = x^4 + x^3 + x^2 + x + 1$.
By Exercise 3 this is prime over $\mathbb{Z}_3$, and hence over $\mathbb{Q}$ and so it is the minimum polynomial of α over $\mathbb{Q}$.

(v) Let $c = \cos(\pi/5)$ and $s = \sin(\pi/5)$. Then $(c + is)^5 = 1$. Expanding, and equating the imaginary parts we get:

$$5c^4s - 10c^2s^3 + s^5 = 0.$$

Clearly $s \neq 0$ and so $5c^4 - 10c^2s^2 + s^4 = 0$.

Hence $\tan(\pi/5) = s/c$ is a zero of $f(x) = x^4 - 10x^2 + 5$. This is prime over $\mathbb{Q}$ by Eisenstein's Theorem with $p = 5$ and so is the required minimum polynomial.

(vi) Let $\alpha = i + \omega$.

Then $(\alpha - i)^3 = 1$.

Hence $\alpha^3 - 3i\alpha^2 + 3i^2\alpha + i = 1$.

$\therefore \alpha^3 - 3\alpha - 1 = i(3\alpha^2 - 1)$.

Hence $(\alpha^3 - 3\alpha - 1)^2 = -(3\alpha^2 - 1)^2$.

$\therefore \alpha$ is a zero of

$m(x) = x^6 + 9x^2 + 1 - 6x^4 - 2x^3 + 6x + 9x^4 - 6x^2 + 1$

$= x^6 + 3x^4 - 2x^3 + 3x^2 + 6x + 2$

Now it's a bit daunting to show that this is prime by the techniques we've developed so far. What if we proceed differently?

$(\alpha - \omega)^2 + 1 = 0$ so this gives $\alpha^2 - 2\alpha\omega + \omega^2 + 1 = 0$.

Now $1 + \omega^2 = -\omega$ so we get $\alpha^2 - 2\alpha\omega - \omega = 0$.

This looks promising. So $\alpha^2 = \omega(2\alpha + 1)$.

Cubing we get $\alpha^6 = 8\alpha^3 + 12\alpha^2 + 6\alpha + 1$.

Hence $\alpha^6 - 8\alpha^3 - 12\alpha^2 - 6\alpha - 1 = 0$.

Now this is to different to $m(x)$.

No, I haven't made a mistake. The fact that we have two different polynomials that α satisfies means that the minimum polynomial must divide both and hence the minimum polynomial of α over $\mathbb{Q}$ must have lower degree than $m(x)$. In fact it must divide the greatest

common divisor of m(x) and this new polynomial. It was a good thing we didn't waste time trying to prove that m(x) is prime, because it isn't!

So let's work out the GCD of

$$x^6 + 3x^4 - 2x^3 + 3x^2 + 6x + 2 \text{ and}$$
$$x^6 - 8x^3 - 12x^2 - 6x - 1.$$

Dividing the latter into the former we get a quotient of 1 and a remainder of the difference, namely:

$$3x^4 + 6x^3 + 15x^2 + 12x + 3.$$

Making this monic we get $x^4 + 2x^3 + 5x^2 + 4x + 1$.

It seems likely that this is our minimum polynomial, but we went the long way about it. Remember that the minimum polynomial of ω is not $x^3 - 1$ but $x^2 + x + 1$, so we could have obtained this quartic much mor quickly.
The quickest way to obtain this polynomial is to note that

$$(\alpha - i)^2 + (\alpha - i) + = 0.$$

But now we must prove that $x^4 + 2x^3 + 5x^2 + 4x + 1$ is prime over $\mathbb{Q}$.

We would have got this same quartic if we had let α be any one of $i + \omega$, $-i + \omega$, $i + \omega^2$ and $-i + \omega^2$. So these must be the four zeros of our quartic.
All are irrational (indeed none is even real), so the only way the quartic could factorise over $\mathbb{Q}$ is for it to be the product of two prime quadratics. These will each have two of the above four as zeros, and if they are to have

rational coefficients the sum and product of their two zeros must be rational. A quick check shows that this is not possible. Hence the quartic is prime and so is the minimum polynomial of $i + \omega$.

(v) Let $\alpha = \sqrt{11 + 6\sqrt{2}}$. Then $\alpha^2 = 11 + 6\sqrt{2}$ and hence $(\alpha^2 - 11)^2 = 72$.
Thus α is a zero of $f(x) = x^4 - 22x^2 + 49$.
But a(x) factorizes as $(x^2 - 6x + 7)(x^2 + 6x + 7)$ and in fact α is a zero of $x^2 - 6x + 7$. This certainly prime over $\mathbb{Q}$ since its zeros, $3 \pm \sqrt{2}$, are not rational. Hence the minimum polynomial is $x^2 - 6x + 7$.
Note: if we had observed at the outset that $\sqrt{11 + 6\sqrt{2}}$ is simply $3 + \sqrt{2}$ we would have reached this much more quickly!

(vii) Let $\alpha = \sqrt[3]{2} + \sqrt{3}$.

Then $\alpha - \sqrt{3} = \sqrt[3]{2}$ and so $(\alpha - \sqrt{3})^3 = 2$ and so $\alpha^3 - 3\sqrt{3}\alpha^2 + 9\alpha - 3\sqrt{3} = 2$. This isn't yet a polynomial with rational coefficients. But we can write this equation as $\alpha^3 + 9\alpha - 2 = 3\sqrt{3}(1 + \alpha^2)$.

Squaring both sides gives:
$(\alpha^3 + 9\alpha - 2)^2 = 27(1 + \alpha^2)^2$ and so simplifying we get:
$\alpha^6 - 9\alpha^4 - 4\alpha^3 + 27\alpha^2 - 36\alpha - 23 = 0$.
So α is a zero of $x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$.

Our usual methods are hard to apply when the degree is this large, so we give up. Once we introduce

field extensions in the next chapter we'll have a very simple way of establishing the primeness over $\mathbb{Q}$ of this polynomial. We will also be able to compute the degree of the minimum polynomial. In this example it will be 6 and so it will then be clear that we have indeed got the minimum polynomial.

Exercise 7: Let $k = \frac{m}{n}$, $c = \cos(2\pi k)$ and $s = \sin(2\pi k)$.

Then $(c + is)^n = 1$. Expanding the LHS by the Binomial Theorem and equating real parts we get

$$c^n - \binom{n}{2} c^{n-2}s^2 + \binom{n}{4} c^{n-4}s^4 - \ldots = 1.$$

Putting $s^2 = 1 - c^2$ we can write this as an integer polynomial in c.
Hence c is an algebraic number.

Exercise 8: Suppose that

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$$

for some n and some rational α_i with $\alpha_n \neq 0$.

Let $\beta = \sqrt{\alpha}$.

Then $\alpha = \beta^2$ and so

$$a_n\beta^{2n} + a_{n-1}\beta^{2n-2} + \ldots + a_1\beta^2 + a_0 = 0.$$

Hence $\sqrt{\alpha}$ is algebraic.

Let $\gamma = \frac{1}{\alpha}$. Then $a_0\gamma^n + a_1\gamma^{n-1} + \ldots + a_{n-1}\gamma + a_n = 0$.

Hence $\frac{1}{\alpha}$ is algebraic.