§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 do not 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 \( F \)”.

Over \( \mathbb{Q} \), it is prime, because we cannot factorise it into two polynomials with rational coefficients. Over \( \mathbb{R} \), of course we can write it as \((x - \sqrt{2})(x + \sqrt{2})\).

A fundamental question that we shall 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 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 \( \theta \) of the field such that \( f(\theta) = 0 \). By the Remainder Theorem \( x - \theta \) will be a factor.

A linear polynomial is clearly prime no matter what the field is and quadratics are prime if their discriminant has no square roots.

**PRIMENESS TEST 1: Linear**

Every polynomial \( f(x) \in F[x] \) of degree 1 is prime over \( F \).

**PRIMENESS TEST 2: Quadratic**

\( f(x) = ax^2 + bx + c \in F[x] \) 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 \(-7 < 0\).

**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 \( \mathbb{Z}_7 \).

The squares mod 7 are 0, 1, 4 and 2 (9 = 2 mod 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 \( f(x) \in F[x] \) 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:** \( f(x) = x^3 + x + 1 \) is prime over \( \mathbb{Z}_2 \) since \( f(0) = f(1) = 1 \).
This test doesn’t work if the degree exceeds 3.

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

Over the reals, some of the quadratics are prime — those with negative discriminant and hence no real zeros. But if a real polynomial has degree > 2 it must be composite.

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

**Proof:** The only part that isn’t immediately obvious is that real polynomials of degree > 2 are composite. This follows from the fact that non-real zeros of real polynomials come in conjugate pairs. If \(\alpha\) and \(\overline{\alpha}\) are non-real zeros then \((x - \alpha)(x - \overline{\alpha}) = x^2 - 2\text{Re}(\alpha)x + |\alpha|^2\) will be a quadratic factor with real coefficients.

Over the rational field there are prime polynomials of degree \(n\) for every \(n \geq 1\). For example for each such \(n\) the rational polynomial \(x^n - 2\) is prime over \(\mathbb{Q}\). This is not immediately obvious since even if one knows that the \(n\)’th roots of 2 are irrational for \(n \geq 2\), that merely shows that \(x^n - 2\) has no linear factors. We shall later find a test that does prove that all such polynomials are prime over \(\mathbb{Q}\).

### §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 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. Although there are more sophisticated techniques we shall rely on this simple-minded trial and error approach which works perfectly well for \(\mathbb{Z}_p\) provided \(p\) and the degree of the polynomial are not too large.

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

If \(p(x)\) has degree \(n \geq 2\), enumerate 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 \(p(x)\) then \(p(x)\) is composite. Otherwise it is 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. So 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. For a start both linear polynomials, \(x\) and \(x + 1\) are prime (linear polynomials of course 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: \(x^4 + x^3 + 1, x^4 + x^2 + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1\)

(We’ll leave the quintics till later.)
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.

Now 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 are working mod 2). This leaves three prime quartics: \( x^4 + x^3 + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1 \).

Before going onto the quintics let’s 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:

\[
10, 11, 111, 1011, 11001, 10011, 11111.
\]

Now the quintics with no zeros are:

\[
110001, 101001, 100101, 100011, 111101, 111011, 110111, 101111.
\]

We must eliminate the products of a prime quadratics with a prime cubic. But there is only one prime quadratic, \( 111 \), and there are 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.

\[
\begin{array}{cccc}
1101 & 1011 \\
111 & \times & 111 & \times \\
1101 & 1011 \\
1101 & 1011 \\
1101 & 1011 \\
100011 & 110001
\end{array}
\]

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:

\[
101001, 100101, 111101, 111011, 110111, 101111,
\]

that is, \( x^5 + x^3 + 1, x^5 + x^2 + 1, x^5 + x^4 + x^3 + x^2 + 1, x^5 + x^4 + x^2 + x + 1, x^5 + x^4 + x^2 + x + 1 \) 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 rational polynomial is one with rational coefficients. A primitive polynomial is an integer polynomial where the greatest common divisor of the coefficients is 1.

**Theorem 3:** If \( f(x) \in \mathbb{Q}[x] \) then \( f(x) = q \cdot g(x) \) for some \( q \in \mathbb{Q} \) and primitive \( g(x) \in \mathbb{Z}[x] \).

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

**Example 7:** Let \( f(x) = \frac{9}{10} x^3 + \frac{15}{4} x^2 - \frac{24}{5} x + \frac{21}{2} \in \mathbb{Q}[x] \).

Then \( 20 f(x) = 18x^3 + 75x^2 - 96x + 210 \in \mathbb{Z}[x] \). The GCD of its coefficients is 3 so \((20/3) f(x) = 6x^3 + 25x^2 - 32x + 70\) 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 \( a(x) = b(x) \cdot c(x) \) where \( b(x) = b_s x^s + \ldots + b_0 \in \mathbb{Q}[x] \) with degree \( s < n \) and \( c(x) = c_t x^t + \ldots + c_0 \in \mathbb{Q}[x] \) with degree \( t < n \). Define \( b_i = 0 \) if \( i > s \) and \( c_i = 0 \) if \( i > t \).

By Theorem 3, \( b(x) = q \cdot d(x) \) and \( c(x) = r \cdot e(x) \) for some non-zero \( q, r \in \mathbb{Q} \) and primitive polynomials \( d(x), e(x) \). Let \( qr = \frac{u}{v} \) where \( u, v \) are coprime integers and where \( v > 0 \).

Now \( v \cdot a(x) = u \cdot d(x) \cdot e(x) \). Suppose \( v = 1 \) then we have a suitable integer factorisation.

Since \( u \) and \( v \) are coprime \( p \) doesn’t divide \( u \).

Since \( d(x) \) is primitive \( p \) doesn’t divide any 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 \( p \) does not divide \( d_h \) and
- \( p \) divides \( e_i \) for all \( i < k \) but \( p \) does not divide \( e_k \).

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

\[
v \cdot d_{h+k} = u \cdot (d_0 e_{h+k} + \ldots + d_h e_k + \ldots + d_{h+k} e_0).\]

Now \( p \) divides \( v \) and \( d_i \) for \( i < h \) and \( p \) divides \( e_i \) for \( i < k \), so \( p \) divides \( u, d_h, e_k \). 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 \( f(x) = x^3 - 3x - 1 \). 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 \( f(x) \) is prime over \( \mathbb{Z} \) and so by Gauss’s Theorem it is 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**

**Theorem 5 (Eisenstein’s Theorem):**
If \( a(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \) and \( p \) is a prime such that:

- \( p \) divides \( a_0, a_1, \ldots, a_{n-1} \);
- \( p \) does not divide \( a_n \);  
- \( p^2 \) does not divide \( a_0 \)

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

**Proof:** Let \( a(x) = (b_r x^r + \ldots + b_0)(c_s x^s + \ldots + c_0) \) where \( r, s \geq 1 \).

Since \( p \) does not 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 \( a_n = b_0 c_n + \ldots + b_m c_0 \). Since \( p \) divides \( b_i \) for \( i < m \) and also \( a_n \) 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 \( x^{14} + 10x^{11} + 60x^7 + 50x + 20 \) is prime over \( \mathbb{Q} \) since it satisfies the Eisenstein criterion for \( p = 5 \). (Note that \( p = 2 \) won’t do.)

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 an integer polynomial factorises over \( \mathbb{Z} \) then it factorises over any \( \mathbb{Z}_p \).

**Proof:** If \( f(x) = b(x)c(x) \) is a factorisation over \( \mathbb{Z} \) into polynomials of lower degree then reducing each of these polynomials modulo \( p \) we get a non-trivial factorisation of \( f(x) \).

**Corollary:** If an integer polynomial is prime over \( \mathbb{Z}_p \), for any prime \( p \), it is prime over \( \mathbb{Q} \).

**Example 10:** \((x^2 + 6x + 3)(5x + 7) = 5x^3 + 37x^2 + 57x + 21 \) over \( \mathbb{Z} \). Over \( \mathbb{Z}_2 \) this reduces to the valid factorisation: \((x^2 + 1)(x + 1) = x^3 + x^2 + x + 1 \).

But beware. If an integer polynomial is composite over \( \mathbb{Z}_p \) that doesn’t mean that it has to be composite over \( \mathbb{Q} \).

**Example 11:** \( f(x) = x^4 + 6x^3 + 3x^2 + 3x + 3 \) reduces to \( x^4 + x^2 + x + 1 \) over \( \mathbb{Z}_2 \) which factorises as \( (x + 1)(x^3 + x^2 + 1) \). This might (mistakenly) lead us to believe that \( f(x) \) factorises over \( \mathbb{Q} \), but the original polynomial is prime over \( \mathbb{Q} \) by Eisenstein’s Theorem.

**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 is prime over \( \mathbb{Q} \).

### §3.5. Minimum Polynomials

Every complex number \( \alpha \) 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 case. 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 \( \alpha \) is a zero of the rational polynomial \( x^4 - 10x^2 + 1 \). If \( \alpha = e^{2\pi i/9} \) then \( \alpha \) is a zero of the rational polynomial \( x^9 - 1 \).

For some values of \( \alpha \) there is no rational polynomial at all that has \( \alpha \) 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 $C$ we say that $\alpha \in C$ is \textbf{algebraic} over $F$ if $f(\alpha) = 0$ for some non-zero $f(x) \in F[x]$. On the other hand if no such polynomial exists we say that $\alpha$ is \textbf{transcendental over} $F$.

If $F = C$ this classification is not very interesting. Every complex number is algebraic over $C$ since any $\alpha$ is the zero of the linear polynomial $x - \alpha$. Over $C$ there are no transcendental numbers at all.

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

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

\textbf{Example 13:} If $\alpha = e^{2\pi i/9}$ then $\alpha$ 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 to select from all polynomials having $\alpha$ 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 is natural to insist that the polynomial be monic.

The \textbf{minimum polynomial} of $\alpha$ over a field $F$ is the monic polynomial over $F$, of lowest degree, having $\alpha$ as a zero. The use of the word “the” suggests that it’s unique, but we don’t know that yet. Conceivably a certain $\alpha$ could be a zero of two quite different 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 shall prove shortly. But firstly let us return to the number $\alpha = e^{2\pi i/9}$.

\textbf{Example 14:} Find the minimum polynomial of $e^{2\pi i/9}$ over $Q$.

\textbf{Solution:} We know that $\alpha$ is a zero of the polynomial $x^9 - 1$ with rational coefficients. But is this the minimum polynomial over $Q$?

Notice that $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$. So $\alpha$ 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 $\alpha$ as a zero, meaning that $x^9 - 1$ could not be its minimum polynomial over $Q$.

Clearly $\alpha$ 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? We need to develop a little theory before we can answer this question.

\textbf{Theorem 7:} The minimum polynomial of $\alpha$ over $F$:

1. is unique;
2. has $\alpha$ as a zero;
3. divides any polynomial having $\alpha$ as a zero;
4. is monic;
5. is prime.

\textbf{Proof:} Properties (2) and (4) are incorporated into the definition. We prove (3) next. Let $p(x)$ be any minimum polynomial of $\alpha$ over $F$ (we can’t say the minimum polynomial yet). Let $f(x) \in F[x]$ with $f(\alpha) = 0$.

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

We can now prove uniqueness. For two minimum polynomials must divide each other and so be a non-zero constant multiple of one another. Being monic they must therefore be equal.

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 \( p(\alpha) = a(\alpha)b(\alpha) \) and since these belong to a field we must have \( a(\alpha) = 0 \) or \( b(\alpha) = 0 \). Either case would contradict the minimality of the degree of the minimum polynomial. Hence \( p(x) \) is prime.

We 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 cannot conclude that either \( a(M) \) or \( b(M) \) is zero.

**Example 15:** The minimum polynomial of \( \sqrt{2} \) over \( \mathbb{Q} \) 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 \( \leq 3 \) 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 \( \mathbb{Z}_3 \). Having degree \( \leq 3 \) it is prime over \( \mathbb{Z}_3 \) and hence over \( \mathbb{Q} \).
   (Theorem 6).

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 16:** 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 is 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
\[
c^3 - 3cs^2 = \frac{1}{2}.
\]
Putting \( s^2 = 1 - c^2 \) we get \( 4c^3 - 3c = \frac{1}{2} \) 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 shall consider all three.

(1) **(LOW DEGREE)** It is not difficult to see, from what we have 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 are rational we would 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) \textsc{(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 irrational.)

(3) \textsc{(MOD }p\text{)} 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 roots in \(\mathbb{Z}_5\) and so is prime over \(\mathbb{Z}_5\) and hence \(x^3 - 3x - 1\) is prime over \(\mathbb{Q}\).

§3.6. Numbers of Real Zeros

In order to find insoluble polynomials we need to be able to determine the number of non-real zeros of a real polynomial. This may seem easy – just draw the graph and count how many times the curve cuts the x-axis.

This is all very well, but if we want an absolutely rigorous proof that a polynomial is insoluble we need to consider two important difficulties. Drawing a graph means plotting a finite number of points and guessing what happens in between. Even if we obtain exact values of the ordinates of these points we are making assumptions about the intermediate values. We can always decide to plot many more points, but at the end of the day we will have only finitely many points.

Suppose we have the following points plotted.

Since polynomials are continuous we know, by the Intermediate Value Theorem, that there is at least one real zero in this interval. Here it would be very reasonable to suppose that there is just one real zero.

But it could be that there are three (or even more) real zeros, very close together.

In order to be absolutely sure we would need to find the number of real zeros of the derivative of this polynomial in this interval. That in turn would lead to the same problems and we would have to investigate higher and higher derivatives until we reach a quadratic.
A second problem is the following. Suppose we have plotted (exactly) the following four points.

It would be reasonable to guess that there are no real zeros in this interval.

But there could be two (or even more).

To settle the question we would have to look at tangents. If indeed there were no zeros we would be able to find points close enough so that the tangents intersect above the x-axis. (Of course we would have to ensure that the curves did not intersect these tangents further.)

To carry out this careful analysis on a quintic would be quite a deal of work, and as we are interested here in the algebra, and not calculus, we will be content to simply plot the graph and hope that we have used enough points to see what is going on.

**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 rational zeros it is 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 \( \mathbb{Q} \).

1. \( x^7 + 6x^4 - 18x^3 + 42x + 12 \)
2. \( x^5 + 10x^3 - 2x^2 + 7x + 91 \)
3. \( x^4 + x^2 - 1 \)
4. \( x^6 + x^5 - x^4 + 5x^3 + 4x^2 + 4x + 5 \)
**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, e.g. 102021 represents \( x^3 + 2x^2 + 2x + 1 \). 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 \( \pi + i \) over \( \mathbb{C} \) and over \( \mathbb{R} \).

**Exercise 6:** Find the minimum polynomials over \( \mathbb{Q} \) of the following:

(i) \( 1 + \sqrt{7} \)
(ii) \( \sqrt{2} + i \)
(iii) \( i + \omega \)
(iv) \( e^{2\pi i/5} \)
(v) \( \sqrt{11 + 6\sqrt{2}} \)
(vi) \( \tan(\pi/5) \)
(vii) \( \frac{1}{2} + \sqrt{3} \)

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

**Exercise 8:** Prove that if \( \alpha \) 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 does not prove that it is 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) If \( f(x) = x^4 + x^2 - 1 \) then \( f(0) = -1, f(\pm 1) = 1, f(\pm 2) = 19, f(\pm 3) = 89, f(\pm 4) = 271 \).
(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 \( \mathbb{Q} \) are \(-4\sqrt[3]{1/3}, -4\sqrt[3]{1/3} \omega, -4\sqrt[3]{1/3} \omega^2\). 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** Putting \( x = y + 1 \) the polynomial becomes \((y + 1)^4 + (y + 1)^3 + (y + 1)^2 + (y + 1) = y^4 + 5y^3 + 10y^2 + 10y + 5\) 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 with non-zero constant terms are:
\[
\begin{array}{cccccccccccc}
10001, & 10002, & 10011, & 10012, & 10021, & 10022, & 10101, & 10102, & 10111, & 10112, & 10121, & 10122, \\
10201, & 10202, & 10211, & 10212, & 10221, & 10222, & 11001, & 11002, & 11011, & 11012, & 11021, & 11022, \\
11101, & 11102, & 11111, & 11112, & 11121, & 11122, & 11201, & 11202, & 11211, & 11212, & 11221, & 11222, \\
12001, & 12002, & 12011, & 12012, & 12021, & 12022, & 12101, & 12102, & 12111, & 12112, & 12121, & 12122, \\
12201, & 12202, & 12211, & 12212, & 12221, & 12222. \\
\end{array}
\]
Eliminating those with \( x = \pm 1 \) as a zero we get:
\[
\begin{array}{cccccccccccc}
10001, & 10012, & 10022, & 10102, & 10111, & 10121, & 10201, & 10202, & 11002, & 11012, & 11021, & 11101, \\
11111, & 11122, & 11212, & 12002, & 12011, & 12022, & 12102, & 12111, & 12112, & 12121, & 12122, \\
122001, & 12202, & 12211, & 12212, & 12221, & 12222. \\
\end{array}
\]
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:
\[
\begin{array}{ccc}
101 & 10201 & 11012 & 12022 \\
112 & 12211 & 10001 & \\
122 & & 11221 & \\
\end{array}
\]
Eliminating these we have the monic prime quartics:
Exercise 5: Over \( \mathbb{C} \) it is clearly \( x - (\pi + i) \). Let \( \alpha = \pi + i \). Then \((\alpha - \pi)^2 + 1 = 0\) so \( \alpha \) is a zero of \( f(x) = x^2 - 2\pi x + (1 + \pi^2) \). The zeros of \( f(x) \) are \( \pi \pm i \) so \( f(x) \) has no real zeros and, being quadratic, it is prime over \( \mathbb{R} \).

Exercise 6:
(i) Let \( \alpha = i + \omega \). Then \( 1 + (\alpha - i) + (\alpha - i)^2 = 0 \) and so \( i(2\alpha + 1) = \alpha^2 + \alpha \). Squaring we get: \((2\alpha + 1)^2 + (\alpha^2 + \alpha)^2 = 0\), so \( \alpha \) is a zero of \( f(x) = x^4 + 2x^3 + 5x^2 + 4x + 1 \).

Now \( f(0) = f(-1) = 1 \), \( f(1) = f(-2) = 13 \), \( f(2) = f(-3) = 61 \), \( f(3) = f(-4) = 193 \) and \( f(5) = f(-6) = 1021 \) giving 10 values for which \( f(x) \) is \pm 1 or prime. Hence \( f(x) \) is prime over \( \mathbb{Q} \) and so is the minimum polynomial of \( i + \omega \) over \( \mathbb{Q} \).

(ii) 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 \( \alpha \neq 1 \), \( \alpha \) is a zero of \( f(x) = x^4 + x^3 + x^2 + x + 1 \).

By Exercise 3 this is prime over \( \mathbb{Z} \), and hence over \( \mathbb{Q} \) and so it is the minimum polynomial of \( \alpha \) over \( \mathbb{Q} \).

(iii) Let \( \alpha = \sqrt{11 + 6\sqrt{2}} \). Then \( \alpha^2 = 11 + 6\sqrt{2} \) and hence \((\alpha^2 - 11)^2 = 72\). Thus \( \alpha \) is a zero of \( f(x) = x^4 - 22x^2 + 49 \). But \( f(x) \) factorizes as \((x^2 - 6x + 7)(x^2 + 6x + 7)\) and in fact \( \alpha \) is a zero of \( x^2 - 6x + 7 \). This certainly prime over \( \mathbb{Q} \) since its roots, \( 3 \pm \sqrt{2} \), 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!

(iv) 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.

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

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 \( \alpha \) is a zero of \( x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23 \).

Now our usual methods don’t seem very promising. Once we introduce field extensions in the next chapter we will have a very simple way of establishing the primeness over \( \mathbb{Q} \) of this 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 \( c^n - \left(\begin{array}{c} n \\ 2 \end{array}\right) c^{n-2} s^2 + \left(\begin{array}{c} n \\ 4 \end{array}\right) c^{n-4} s^4 - \ldots = 1 \).

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 $\alpha_i$ with $\alpha_n \neq 0$.

Let $\beta = \sqrt[n]{\alpha}$. 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 $\sqrt[n]{\alpha}$ 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.