

1. POLYNOMIALS

§1.1. Prime Polynomials

If F is a field then $F[x]$ represents all **polynomials** in x over F . These have the form:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

where each $a_i \in F$. The x is an “indeterminate”. We could dispense with the x ’s and write a polynomial in the form $(a_n, a_{n-1}, \dots, a_1, a_0)$ but the traditional way of writing it makes addition and multiplication seem very natural. While infinite power series such as $1 + x + x^2 + \dots$ can be quite useful in mathematics, they are not polynomials.

If $a_n \neq 0$ we say that the polynomial has **degree** n . The coefficient a_n is then called the **leading coefficient**. If it is 1 we say that $f(x)$ is **monic**.

The only polynomial for which we can’t define degree is the **zero polynomial**, 0. If this doesn’t look like a polynomial you could write it as $0x^2 + 0x + 0$ if you really want to!

Polynomials of degree 0 are the non-zero constant polynomials such as 2 or $\frac{1}{2}$. These are those polynomials that have inverses within $F[x]$. They are called the units of $F[x]$. Polynomials whose degree is positive do not have inverses, at least not within the set of polynomials. While it is true, in a certain sense, that

$\frac{1}{1-x} = 1 + x + x^2 + \dots$ the polynomial is not a unit because this inverse is not a polynomial.

Polynomials of degree 1 are the so-called linear polynomials, having the form $ax + b$ for $a \neq 0$. Clearly these cannot be factorised into polynomials of lower degree.

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 ”. If we were to ask whether $x^2 - 2$ is prime, the correct answer is “it depends on the field”. Over \mathbf{Q} , it is prime, because we cannot factorise it into two polynomials with rational coefficients. Over \mathbf{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”.

A linear polynomial is clearly prime no matter what the field is. Over \mathbf{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 \mathbf{C} , has a zero. A **zero** of a polynomial is an element θ of the field such that $f(\theta) = 0$. By the Remainder Theorem $x - \theta$ will be a factor.

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

PRIMENESS TEST 1: Low Degree

Theorem 1: A polynomial $f(x) \in F[x]$ with degree 2 or 3 is prime over F if and only if it has no zeros in F .

Proof: A prime polynomial of degree ≥ 2 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 1: $x^2 + x + 1$ is prime over \mathbf{Q} since neither of its zeros ω and ω^2 , is rational.

This test doesn’t work if the degree exceeds 3.

Example 2: The quartic $(x^2 + 1)^2$ has no zeros in \mathbf{R} , yet it clearly isn't prime over \mathbf{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 \mathbf{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 α and $\bar{\alpha}$ are non-real zeros then $(x - \alpha)(x - \bar{\alpha}) = x^2 - 2\operatorname{Re}(\alpha)x + |\alpha|^2$ 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 \mathbf{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.

Example 2: The polynomial $x^2 - 5x + 7$ is prime over \mathbf{R} . (If it factorised it would have linear factors and hence real zeros. But the discriminant is -3 and so the zeros are non-real.

§1.2. Prime Polynomials over \mathbf{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 in chapter 5, 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 \mathbf{Z}_p provided p and the degree of the polynomial are not too large.

PRIMENESS TEST 2: 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 3: Find the prime polynomials over \mathbf{Z}_2 with degree at most 5.

Solution: Over \mathbf{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 all always prime). For quadratics and cubics we need only eliminate those which have a zero in \mathbf{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 cubics: $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$.

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, 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 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.

$$\begin{array}{r}
 1101 \quad 1011 \\
 \underline{111 \times} \quad \underline{111 \times} \\
 1101 \quad 1011 \\
 1101 \quad 1011 \\
 \underline{1101} \quad \underline{1011} \\
 100011 \quad 110001
 \end{array}$$

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

§1.3. Integer Polynomials

An **integer polynomial** is one with integer coefficients, that is, an element of $\mathbf{Z}[x]$. 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 $f(x) \in \mathbf{Q}[x]$ then $f(x) = q g(x)$ for some $q \in \mathbf{Q}$ and primitive $g(x) \in \mathbf{Z}[x]$.

Proof: Let s be the least common multiple of the denominators of the coefficients of $f(x)$. Then $s.f(x) \in \mathbf{Z}[x]$. 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 3: Let $f(x) = \frac{9}{10}x^3 + \frac{15}{4}x^2 - \frac{24}{5}x + \frac{21}{2} \in \mathbf{Q}[x]$.

Then $20 f(x) = 18x^3 + 75x^2 - 96x + 210 \in \mathbf{Z}[x]$. 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 \mathbf{Q} ? The next theorem reduces the problem to that of deciding whether it's prime over \mathbf{Z} .

Theorem 4 (Gauss's Theorem):

If $a(x) \in \mathbf{Z}[x]$ is prime over \mathbf{Z} then it is prime over \mathbf{Q} .

Proof: Let $a(x)$ be a rational polynomial of degree n and suppose that $a(x) = b(x) c(x)$ where $b(x) = b_s x^s + \dots + b_1 x + b_0 \in \mathbf{Q}[x]$ with degree $s < n$ and $c(x) = c_t x^t + \dots + c_1 x + c_0 \in \mathbf{Q}[x]$ 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 $q, r \in \mathbf{Q}$ and primitive polynomials $d(x), e(x)$. Let $qr = u/v$ where u, v are coprime integers and where $v > 0$. Then $v a(x) = u d(x) e(x)$. Now 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 does not divide d_h and
 - p divides e_i for all $i < k$ but p does not 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:

$$v a_{h+k} = u(d_0 e_{h+k} + \dots + d_h e_k + \dots + d_{h+k} e_0).$$

Now p divides v and d_i for $i < h$ and p divides e_i for $i < k$, so p divides $u \cdot d_h \cdot e_k$. 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 4: 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 \mathbf{Z} and so by Gauss's Theorem it is prime over \mathbf{Q} .

§1.4. Tests for Primeness over \mathbf{Q}

Given a rational polynomial, how can we decide if it's prime over \mathbf{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 \mathbf{Z} implies primeness over \mathbf{Q} , so throughout this section all polynomials are assumed to have integer coefficients.

PRIMENESS TEST 3: Eisenstein's Test

Theorem 5 (Eisenstein's Theorem):

If $a(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbf{Z}[x]$ and p is a prime such that:

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

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

Proof: Let $a(x) = (b_r x^r + \dots + b_0)(c_s x^s + \dots + c_0)$ 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 $a_m = b_0 c_m + \dots + b_m c_0$. 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 \mathbf{Z} and so by Gauss's Theorem it is prime over \mathbf{Q} .

Example 5: The polynomial $x^{14} + 10x^{11} + 60x^{10} + 50x + 20$ is prime over \mathbf{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 \mathbf{Z}_p for some prime p .

PRIMENESS TEST 4: Mod p Test

Theorem 6: If an integer polynomial factorises over \mathbf{Z} then it factorises over any \mathbf{Z}_p .

Proof: If $f(x) = b(x)c(x)$ is a factorisation over \mathbf{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 \mathbf{Z}_p , for any prime p , it is prime over \mathbf{Q} .

Example 6: $(x^2 + 6x + 3)(5x + 7) = 5x^3 + 37x^2 + 57x + 21$ over \mathbf{Z} . Over \mathbf{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 \mathbf{Z}_p that doesn't mean that it has to be prime over \mathbf{Q} .

Example 7: $f(x) = x^4 + 6x^3 + 3x^2 + 3x + 3$ reduces to $x^4 + x^2 + x + 1$ over \mathbf{Z}_2 which factorises as $(x + 1)(x^3 + x^2 + 1)$. This might (mistakenly) lead us to believe that $f(x)$ factorises over \mathbf{Q} , but the original polynomial is prime over \mathbf{Q} by Eisenstein's Theorem.

Example 8: Prove that $3x^5 - x^4 + 12x^3 - 21x^2 + 81x + 243$ is prime over \mathbf{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 \mathbf{Z}_2 . Hence this polynomial is prime over \mathbf{Z} and hence, by Gauss's Theorem, it is prime over \mathbf{Q} .

PRIMENESS TEST 5: Too Many Primes Test

Theorem 7: An integer polynomial $f(x)$ of degree $n \geq 2$ which gives prime or ± 1 values for at least $2n + 1$ integer values of x is prime over \mathbf{Q} .

Proof: Suppose $a(x) = b(x).c(x)$ where $\deg a(x) = n$, $\deg b(x) = r \geq 1$ and $\deg c(x) = s \geq 1$. If $a(k)$ is prime for $k \in \mathbf{Z}$ then $b(k) = \pm 1$ or $c(k) = \pm 1$. Now there are at most r values of x for which $b(x) - 1 = 0$ and at most r values of x for which $b(x) + 1 = 0$. Hence there are at most $2r$ integer values of k for which $b(k) = \pm 1$. Similarly there are at most $2s$ integer values of k for which $c(k) = \pm 1$, giving at most $2r + 2s = 2n$ values for which $a(k)$ is prime or ± 1 .

We can improve on this by reducing, in most cases, the number of prime or ± 1 values we need to accumulate before we can conclude that the polynomial is prime.

Lemma: If $f(x) \in \mathbf{Z}[x]$ and $h, k \in \mathbf{Z}$ with $f(h) = 1$ and $f(k) = -1$ then $|h - k| \leq 2$.

Proof: As a polynomial in two variables $f(x) - f(y) = (x - y)q(x, y)$ for some polynomial in x, y with integer coefficients. Now $2 = f(h) - f(k) = (h - k)q(h, k)$ so $h - k = 1$ or 2 .

Theorem 8: Suppose $a(x) \in \mathbf{Z}[x]$ has degree $n \geq 6$.

If there are more than $n + 2$ values of k for which $a(k)$ is either prime or ± 1 , then $a(x)$ is prime over \mathbf{Q} .

Proof: Suppose $a(x) = b(x)c(x)$ is a proper factorisation over \mathbf{Z} where $r = \deg b(x) \leq s = \deg c(x)$. Let $u \leq 2r$ be the number of values of k for which $b(k) = \pm 1$ and let $v \leq 2s$ be the corresponding number for $c(x)$. If $a(k)$ is prime or ± 1 then $b(k) = \pm 1$ or $c(k) = \pm 1$ and the number of values of k for which this occurs is at most $u + v$.

Represent the values k for which $b(k) = \pm 1$ in order by a string of P's and N's of length m . (So, for example, the string PPNP represents four such values $k_1 < k_2 < k_3 < k_4$ where $b(k_1) = f(k_2) = f(k_4) = 1$ and $f(k_3) = -1$.)

There are 16 strings of length 4 but to satisfy the lemma they must start and finish with the same symbol. This gives:

PPPP, PPNP, PNPP, PNNP, NPPN, NPNN, NNPN, NNNN

A string of length 5 begin with one of these and end with the same symbol as the first. This gives the following possibilities:

PPPPP, PPNPP, PNPPP, PNNPP, NPPNN, NPNNN, NNPNN, NNNNN

but in view of the lemma we may eliminate

PNPPP, PNNPP, NPPNN, NPNNN leaving:

PPPPP, PPNPP, NNPNN, NNNNN.

Now suppose $b(x)$ has the string PPNPP. Then for some integers $k_1 < k_2 < k_3 < k_4 < k_5$, $b(k_1) = b(k_2) = b(k_4) = b(k_5) = 1$ and $f(k_3) = -1$. In view of the lemma k_1, \dots, k_5 must be 5 successive integers. So for some integer k , $b(x) - 1$ has zeros $\pm(k - 2)$ and $\pm(k - 1)$. Hence $b(x) - 1 = (x - k - 2)(x - k - 1)(x - k + 1)(x - k + 2)q(x)$ for some $q(x) \in \mathbf{Z}[x]$. Putting $x = k$ we get the contradiction $-2 = (-2)(-1) \cdot 1 \cdot 2 \cdot q(k) + 1$.

So the string PPNPP cannot arise. Nor can the string NNPNN. So the only valid strings of length 5 are PPPPP and NNNNN and hence if $u \geq 5$ then $u \leq r$. Similarly if $v \geq 5$ then $v \leq s$. Clearly if $u = 3$ or 4 $r \geq 2$. Similarly if $v = 3$ or 4 then $s \geq 2$.

The following table gives an upper bound for u in terms of r :

r	$u \leq$	
1	2	Always $u \leq 2r$
2	4	
3	4	If $u \geq 5$ then $u \leq r$
≥ 4	r	

The following table gives the upper bounds on u, v for varying cases of r, s :

n	r	s	$u \leq$	$v \leq$	$u + v \leq$
≥ 10	1	$n - 1$	2	$n - 1$	$n + 1$
	2	$n - 2$	4	$n - 2$	$n + 2$
	3	$n - 3$	4	$n - 3$	$n + 1$
	$r \geq 4$	$n - r$	r	$n - r$	n
9	1	8	2	8	10
	2	7	4	7	11
	3	6	4	6	10
	4	5	4	5	9
8	1	7	2	7	9
	2	6	4	6	10
	3	5	4	5	9
	4	4	4	4	8
7	1	6	2	6	8
	2	5	4	5	9
	3	4	4	4	8
6	1	5	2	5	7
	2	4	4	4	8
	3	3	4	4	8
5	1	4	2	4	6
	2	3	4	4	8
4	1	3	2	4	6
	2	2	4	4	8
3	1	2	2	4	6
2	1	1	2	2	4

For each value of n we can thus find an upper bound for the number of integer values of k for which $a(k)$ is prime or ± 1 . The target, in proving primeness, is 1 more than this value:

n	$u + v \leq$	target
≥ 10	$n + 2$	$n + 3$
9	11	12
8	10	11
7	9	10
6	8	9
5	8	9
4	8	9
3	6	7
2	4	5

Summarising this we obtain:

n	target
≥ 6	$n + 3$
4, 5, 6	9
3	7
2	5

Example 9: The polynomial $f(x) = x^3 - x^2 - 3x + 1$ is prime over \mathbf{Q} since it has at least 7 values which are prime or ± 1 :

k	-4	-3	-2	-1	0	1	2	3	4
f(k)	-67	-26	-5	2	1	-2	-1	10	37
	√		√	√	√	√	√		√

§1.5. 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 \mathbf{C} this may no longer be the case. For example if $\alpha = \sqrt{2}$ and the field is \mathbf{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 $x^4 - 2x^2 + 1$. If $\alpha = e^{2\pi i/9}$ then α is a zero of the rational polynomial $x^{13} - 1$.

For some values of α there is 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 \mathbf{C} we say that $\alpha \in \mathbf{C}$ is **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 α is **transcendental over F** .

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

But if $F = \mathbf{Q}$ 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 \mathbf{Q} .

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

Example 10: 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 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 is natural to insist on the polynomial to 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 quite different polynomials of the same degree and not be a zero of any non-zero polynomial of any lower degree. In fact this does never happens, as we shall prove shortly. But firstly let us return to the number $\alpha = e^{2\pi i/9}$.

Example 11: Find the minimum polynomial of $e^{2\pi i/9}$ over \mathbf{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 \mathbf{Q} ?

Notice that $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$. So α is a zero of one (or possibly both) 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 \mathbf{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? We need to develop a little theory before we can answer this question.

Theorem 9: The minimum polynomial of α over F :

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

Proof: Properties (2) and (4) 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* 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 12: The minimum polynomial of $\sqrt{2}$ over \mathbf{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 ≤ 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 \mathbf{Q} by Eisenstein's Theorem (Theorem 5) using $p = 2$.

(3) $x^2 - 2$ has no zeros over \mathbf{Z}_3 . Having degree ≤ 3 it is prime over \mathbf{Z}_3 and hence over \mathbf{Q} . (Theorem 6).

(4) The values of $x^2 - 2$ are prime or ± 1 for $x = 0, 1, 3, 5, 7$. (Theorem 8).

MINIMUM POLYNOMIAL

To find a minimum polynomial, $p(x)$, for α over F we must do *two* things:

- (A) Find $p(x) \in F[x]$ such that $p(\alpha) = 0$ and
- (B) Prove that $p(x)$ is prime.

(If we can't prove that our $p(x)$ is prime we look for a non-trivial factorisation. If we find one then α is a zero of one of the factors and we start all over again with that factor as our candidate.)

PRIME POLYNOMIAL

To prove that a given polynomial $p(x)$ is prime over \mathbf{Q} we have four techniques to try:

- (1) **(LOW DEGREE)** If its degree is at most 3 we need only show that it has no zeros in \mathbf{Q} (Theorem 1).
- (2) **(EISENSTEIN)** We can try Eisenstein's Theorem (Theorem 5). That is if for some suitable prime p which divides every coefficient *except* the leading coefficient and if p^2 doesn't divide the constant term, then $p(x)$ is prime over \mathbf{Q} . (If $p(x)$ doesn't satisfy the Eisenstein criterion itself it might after a suitable linear substitution such as $x \rightarrow x+1$. If the new polynomial can be shown to be prime then the original one must have been also.
- (3) **(MOD p)** We can try proving that the corresponding polynomial is prime over \mathbf{Z}_p for some prime p (Theorem 6).
- (4) **(TOO MANY PRIMES)** We can try showing that $p(x)$ takes prime or ± 1 values for too many integer values of x . "Too many" means:

- 5 values for quadratics,
- 7 for cubics,
- 9 for degree 4, 5 or 6
- 10 for degree 7;
- 11 for degree 8 and so on.

Note that these are all one way tests. If any or all these tests fail that is **NO GUARANTEE** that $p(x)$ isn't prime. Only by actually obtaining a factorisation can we show that.

We conclude this chapter with another example of minimum polynomial, one that will play an important part in the proof of the impossibility of trisecting any angle by ruler and compass.

Example 13: Find the minimum polynomial of $2\cos(\pi/9)$ over \mathbf{Q} .

Solution: Remember that there are two things 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 $c^3 - 3cs^2 = 1/2$. Putting $s^2 = 1 - c^2$ we get $4c^3 - 3c = 1/2$ and if $x = 2c$ we get $x^3 - 3x - 1 = 0$.

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

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

(4) **(TOO MANY PRIMES)** $x^3 - 3x - 1$ takes values which are prime or ± 1 for the 7 values $x = -3, -2, -1, 0, 1, 2, 3$. This too many for a composite cubic.

§1.6. Numbers of Real Zeros

Primeness of a polynomial is one very important ingredient in Galois Theory. Counting the number of real zeros of a polynomial with real coefficients is complicated by the uncertainty about multiple zeros. Do we count a double zero once or twice? Fortunately for the sort of polynomials we shall be interested in — minimum polynomials — this question doesn't arise. Minimum polynomials are prime and prime polynomials don't have repeated zeros.

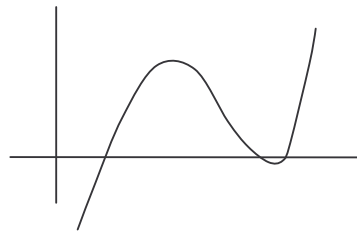
Theorem 10: Prime polynomials have distinct zeros.

Proof: Suppose $f(x) \in F[x]$ and $f(x) = (x - \alpha)^2 g(x)$ where α belongs to some field K containing F and $g(x) \in K[x]$. Then α is a zero of the derivative and hence of the greatest common divisor of $f(x)$ and its derivative. It follows that $f(x)$ and its derivative are not coprime and so $f(x)$ is not prime.

Since non-real zeros of real polynomials come in conjugate pairs a prime polynomial of odd degree must have an odd number of real zeros (so at least one). A prime polynomial of even degree has an even number of real zeros. But how many?

We could draw the graph of the polynomial and observe the number of times the curve crosses the axis. This would give us a pretty good idea. But when we draw a graph, even with the aid of a computer, we are only plotting finitely many points and make assumptions as to what is happening in between. If the points are very close together we might be very confident that we know what happens between them. But can we be certain? The Intermediate Value Theorem and Rolle's Theorem can help to remove any lingering uncertainty.

Since polynomials (considered as functions) are continuous everywhere we can guarantee that if two points on the graph lie on opposite sides of the x -axis then there is a real zero between them. At least one, that is. But it's conceivable that the curve might cross the x -axis, then ducks back briefly onto the other side, before crossing the axis a third time and continuing on its way. It could be that instead of one real zero in this vicinity there are three of them, very close together. They could be so close that all three zeros occur between two successive plotted points. And no matter how fine the resolution of our graph there remains the doubt as to whether it crosses the x -axis cleanly or whether it hesitates — whether there is just a single zero as the graph appears to suggest or rather three (or even five or more) zeros, extremely close together.



We could settle this if we knew enough about the zeros of the derivative. For to cross backwards and forwards there would need to be turning points. And if there are no real zeros for the derivative in the vicinity then there can only be only one real zero for the polynomial itself.

Theorem 11: If $f(a) < 0 < f(b)$ and if $f'(x)$ has at most one real zero in the interval $[a,b]$ then $f(x)$ has exactly one real zero in $[a,b]$.

Proof: By the Intermediate Value Theorem $f(x)$ has at least one real zero in $[a,b]$. If there was more than one there would have to be at least three and between each successive pair there would have to be a real zero for the derivative.

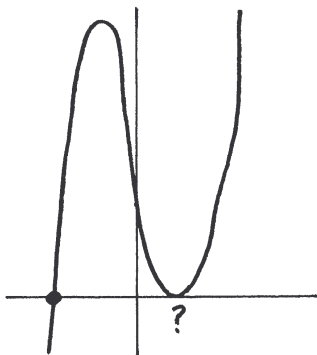
Theorem 12: If $f(a)$, $f(b)$ and $f'(a)$ all have the same sign and there is at most one real zero for $f'(x)$ in $[a, b]$ then there are no real zero for $f(x)$ in $[a, b]$.

Proof: Without loss of generality suppose that $f(a)$, $f(b)$ and $f'(a)$ are all positive. In order for $f(x)$ to have a real zero in $[a, b]$ it must have a local maximum followed by a local minimum and so $f'(x)$ would have at least two real zeros in $[a, b]$.

Let's illustrate this with an example.

Example 14: Find the number of real zeros of $f(x) = x^5 - x^4 + 5x^3 + 2x^2 - 6x + 2$.

Solution: A rough graph indicates that there is one zero near -1.2 and possibly two close together near 0.5 .



A more accurate graph suggests that although the curve comes down close to the x-axis near $x = 0.5$ it has a local minimum just above the x-axis. So the probable answer is that there is exactly one zero. But can we be quite sure?

It could be that near $x = -1.2$ the curve cuts the x-axis three times in quick succession, so close together that it all happens between two of our plotted points. Likewise our graph may suggest that the minimum near $x = 0.5$ is positive but we don't have the exact value of x at this minimum. So how can we be sure?

Let's establish a table of values, being careful that our arithmetic is absolutely exact.

$$f(x) = x^5 - x^4 + 5x^3 + 2x^2 - 6x + 2$$

$$f'(x) = 5x^4 - 4x^3 + 15x^2 + 4x - 6$$

$$f''(x) = 20x^3 - 12x^2 + 30x + 4$$

$$f'''(x) = 60x^2 - 24x + 30$$

Since the discriminant of $f'''(x)$ is negative we know for certain that every value of $f'''(x)$ is positive. It has no real zeros. Since our graph suggests that all the activity is occurring between -2 and $+2$ we restrict our attention to that range. And at this stage we confine ourselves to integer values to simplify the arithmetic. If necessary we can put the magnifying glass on any section.

x	f(x)	f'(x)	f''(x)
-2	-66	158	-264
-1	3	14	-58
0	2	-6	4
1	3	14	42
2	54	110	176

What do these values reveal with certainty? Since $f'''(x)$ has no real zeros there are no turning points for $f''(x)$ and so clearly we can be certain that there are no real zeros on the intervals $(-\infty, -1]$ and on $[0, \infty)$. On $[-1, 0]$ there is at least one real zero by the Intermediate Value Theorem and no more than one by Rolle's Theorem. (More than one would require two turning points here and there are none.) So we can say with certainty that $f''(x)$ has exactly one real zero and that this is in the interval $[-1, 0]$.

Now we move up one level to consider $f'(x)$. There can be no real zeros for $f'(x)$ on $(-\infty, -1]$ because that would require at least two real zeros of $f''(x)$ on this interval and we know there are none. In $(-1, 0)$ there must be at least one by the Intermediate Value Theorem and exactly one by Rolle's Theorem. More than one would require at least two real zeros for $f''(x)$ on this interval and we are sure there is exactly one. Similarly there is exactly one real zero for $f'(x)$ on $(0, 1)$ and none on $(1, \infty)$. So $f'(x)$ has exactly two real zeros, one in $(-1, 0)$ and one in $(0, 1)$.

Now we consider $f(x)$ itself. Using the above techniques we easily see that indeed there are no real zeros in $(-\infty, -2)$, exactly one in $(-2, -1)$ and none in $(1, \infty)$. On $(-1, 0)$ we know that there is exactly one stationary point. Since $f(-1)$ and $f(0)$ are both positive and the derivative at $x = -1$ is also positive it is clear that this stationary point must be a local maximum. Thus $f(x)$ must remain positive over this interval. So there are no real zeros for $f(x)$ in $(-1, 0)$.

There remains the interval $(0, 1)$. There is exactly one stationary point here and since $f'(0) < 0$ and $f(1) > 0$ it must be a local minimum. The question is, does this local minimum lie above or below the x -axis? We don't appear to be able to solve the quartic exactly. If we could then things would be a lot simpler. An approximation, no matter how good, will not deliver 100% certainty.

The fact that there are no real zeros for $f''(x)$ in $(0, 1)$ means that $f(x)$ has no points of inflection in this interval and so the curve cannot cross the tangents at the two endpoints. If the tangents at $x = 0$ and at $x = 1$ each cut the x -axis outside the interval then the curve must remain away from the x -axis and so there would be no real zeros in the interval.

Now recall that such tangents are used in Newton's Method. The Newton's Method Formula: $x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$ gives the point where the tangent at $x = x_0$ cuts the x -axis. If $x = x_0$ is our first guess generally $x = x_1$ is a better approximation and we use this as our new x_0 , successively getting better and better approximations. Here we are not interested in approximations, but if x_0 is one of the endpoints this formula gives the point where the tangent at that point cuts the x -axis. If it lies outside the interval we are in business. (If it doesn't we have to consider points closer together. We may then be able to prove that the local minimum is positive, or we may actually locate negative values showing that it does not.)

If $x_0 = 0$ then $x_1 = 1/3$ and if $x_0 = 1$ then $x_1 = 11/14$. Since neither of these lies outside the interval $(0, 1)$ we need to move in more closely to the local minimum and so we add two further rows to our table.

x	$f(x)$	$f'(x)$
0.5	0.09375	-0.4375
0.6	0.14816	1.584

If $x_0 = 0.5$ then $x_1 = 0.7142857...$ Although this is only a very good approximation we can be quite sure that it exceeds 0.6 and so the tangent at $x = 0.5$ cuts the x -axis outside the interval $(0.5, 0.6)$. Thus we are guaranteed that the local minimum (which is clearly very close to $x = 0.5$, but we haven't found its exact value) is definitely positive. Hence there are no real zeros for $f(x)$ in $(0, 1)$. This means that $f(x)$ has only one real zero and this is in the interval $(-2, -1)$.

Theorem 13: Suppose f is a differentiable function such that:

- (1) $f(a) > 0$;
- (2) $f(b) > 0$;
- (3) $f'(a) < 0$;
- (4) $f'(x) > 0$ for $x \in [a, b]$;
- (5) for some $c \in [a, b]$, $c - \frac{f(c)}{f'(c)} \notin [a, b]$

then $f(x) > 0$ for $x \in [a, b]$.

Proof: The curve is concave upwards along the entire interval and so lies above the tangents at each endpoint. Condition (5) implies that one or other of these tangents cuts the x -axis outside the interval.

EXERCISES FOR CHAPTER 1

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

- (1) Every polynomial is composite over \mathbf{C} .
- (2) There are no prime cubics over \mathbf{R} .
- (3) There is a prime polynomial of degree 24 over \mathbf{Q} .
- (4) If a polynomial has no rational zeros it is prime over \mathbf{Q} .
- (5) Every polynomial is either prime or composite.
- (6) There are only finitely many prime quartics over \mathbf{Z}_5 .
- (7) A polynomial of the form $x^3 + px^2 + p^2x + p^3$ is prime over \mathbf{Q} by Eisenstein.
- (8) If $f(x) \in \mathbf{Z}[x]$ is prime for infinitely many integers x then it is prime over \mathbf{Q} .
- (9) If $f(0) > 0$ and $f(1) > 0$ and $1 - \frac{f(1)}{f'(1)} \notin [0, 1]$ then $f(x)$ has no real zeros in $[0, 1]$.
- (10) If $f(0) < 0$ and $f(1) > 0$ and $f'(x)$ has exactly one real zero in $[0, 1]$ then $f(x)$ also has exactly one real zeros in $[0, 1]$.

Exercise 2: Prove that the following polynomials are prime over \mathbf{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 \mathbf{C} ;
- (ii) $x^2 + 4x + 3$ over \mathbf{R} ;
- (iii) $x^2 + 4x + 6$ over \mathbf{R} ;
- (iv) $x^4 + 1$ over \mathbf{R} ;
- (v) $x^3 - 1$ over \mathbf{Q} ;
- (vi) $x^3 + 2$ over \mathbf{Q} ;
- (vii) $x^5 + x^2 - x + 1$ over \mathbf{Q} ;
- (viii) $x^4 + x + 1$ over \mathbf{Z}_3 ;
- (ix) $x^4 + 1$ over \mathbf{Z}_3 ;
- (x) $x^{13} - 50x^9 + 60x^7 - 300x + 60$ over \mathbf{Q} ;
- (xi) $15x^4 + 117x - 9$ over \mathbf{Q} ;
- (xii) $x^4 + x^3 + x^2 + x + 1$ over \mathbf{Q} .

Exercise 4: Find all the monic prime quartics over \mathbf{Z}_3 .

(To save writing, represent the quartics by their sequence of coefficients, eg 10221 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 $\pi + i$ over \mathbf{C} and over \mathbf{R} .

Exercise 6: Find the minimum polynomials over \mathbf{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) $\sqrt[3]{2} + \sqrt{3}$?

Exercise 7: Prove that if $k \in \mathbf{Q}$ 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 1

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 \mathbf{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 $x + p$.
- (8) **TRUE** Infinitely many prime values exceeds the finite limit needed by Theorem 8.
- (9) **FALSE** Theorem 13 requires that $f'(x)$ has no real zeros in the interval. If $f(x) = 400x^3 - 200x^4 - 190x^2 - 4x + 11$ then $f'(x) = 1200x^2 - 800x^3 - 380x - 4$ and $f(1) = 17$, $f'(1) = 16$ and so $1 - f(1)/f'(1) < 0$ which, if the statement was true would mean that $f(x) > 0$ for all $x \in [0, 1]$. However $f(0.5) = -1$ and so there are two real zeros for $f(x)$ in the interval.
- (10) **TRUE** by Theorem 11.

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 \mathbf{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 \mathbf{Z} can give rise to consistent prime factorizations over both \mathbf{Z}_2 and \mathbf{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 **R**.
- (iv) **COMPOSITE** The only prime polynomials over **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 **Q** 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 **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 **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 **Q** by Eisenstein for $p = 5$. Hence the given polynomial must be prime over **Q**.

Exercise 4: The monic quartics 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: Over **C** it is clearly $x - (\pi + i)$. Let $\alpha = \pi + i$. Then $(\alpha - \pi)^2 + 1 = 0$ so α 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 **R**.

Exercise 6:

- (i) $x^4 + 2x^3 + 5x^2 + 4x + 1$
(ii) $x^4 + x^3 + x^2 + x + 1$
(iii) $x^2 - 6x + 7$
(iv) $x^4 - 10x^2 + 5$
(v) $x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$

(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 α 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 ± 1 or prime. Hence $f(x)$ is prime over \mathbf{Q} and so is the minimum polynomial of $i + \omega$ over \mathbf{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 $\alpha \neq 1$, α is a zero of $f(x) = x^4 + x^3 + x^2 + x + 1$. By Exercise 3 this is prime over \mathbf{Z}_3 , and hence over \mathbf{Q} and so it is the minimum polynomial of α over \mathbf{Q} .

(iii) 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 $f(x)$ 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 \mathbf{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 \mathbf{Q} by Eisenstein's Theorem with $p = 5$ and so is the required minimum polynomial.

(v) 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 $x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23$.

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

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 $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$ for some n and some rational α_i with $\alpha_n \neq 0$.

Let $\beta = \sqrt{\alpha}$. Then $\alpha = \beta^2$ and so $a_n\beta^{2n} + a_{n-1}\beta^{2n-2} + \dots + a_1\beta^2 + a_0 = 0$.

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

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

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