# Chapter 1

## Introduction

Methods of solving quadratic equations have been known since ancient times. The technique of completing the square gives an explicit formula for the solutions in terms of *radicals*, i.e. expressions obtained from the coefficients by adding, subtracting, multiplying, dividing and taking roots.

It is natural to ask whether higher-degree polynomial equations can be solved in a similar way. Approximate solutions can be found graphically or by iterative methods. Computers can solve polynomial equations to any degree of accuracy that might be required for practical purposes, but the problem of finding exact expressions for the solutions is still of theoretical importance.

Algorithms for solving cubic and quartic equations were developed in the sixteenth century. A major obstacle was the fact that square roots of negative numbers occurred, even when solving equations which were known to have only real roots. Once complex numbers were understood, progress was more rapid, leading to algorithms for solving cubic and quartic equations. Gauss, Argand and others proved the *Fundamental Theorem of Algebra*: every polynomial with real or complex coefficients is a product of linear factors over $\mathbb{C}$, so no larger field is needed to solve polynomial equations over $\mathbb{C}$.

In 1824 Niels Abel proved that there is no general formula for solving a quintic (fifth degree) equation by radicals. However,

*some* quintics are solvable by radicals, so a criterion was required. Lagrange considered permutations of the roots but did not find a general result.

Évariste Galois (1811 - 1832) solved this problem shortly before he was killed in a duel. His work, which was not acknowledged in his lifetime, established the connection between symmetry groups and solvability of polynomial equations. This is the topic which we now call 'Galois Theory' in his honour.

In the twentieth century, Emmy Noether and others developed the structure theory of groups, rings and fields. Emil Artin generalised Galois's results in the language of field theory; this is the modern approach to the subject, in which Galois's 'symmetries' are redefined as mappings of the smallest field which contains the roots of the polynomial. Finite fields are often referred to as Galois fields, and a thorough understanding of fields is an essential starting point for Galois Theory.

For more details about the history of the subject, see Ian Stewart's book *Galois Theory* and St Andrews University's MacTutor History of Mathematics archive.

## 1.1 Rings, fields and polynomials

Recall that a **ring** $(R, +, \times)$ is a non-empty set $R$ with operations of addition and multiplication, such that $(R, +)$ is an abelian (i.e. commutative) group, $\times$ is associative on $R$, and $\times$ is distributive over $+$.

In this module, all rings will be commutative rings with unity. The **characteristic** $\chi(R)$ of such a ring $R$ is the smallest positive integer $n$ (if any) such that $n.1_R = 0_R$. If no such $n$ exists then $\chi(R) = 0$.

$a$ **divides** $c$ (written $a \mid c$) in a commutative ring $R$ if $ab = c$ for some $b \in R$.

An **integral domain** (ID) is a non-trivial commutative ring with unity which has no zero-divisors, i.e. if $ab = 0_R$ then at least one of $a$ and $b$ is $0_R$.

A **field** is a non-trivial commutative ring with unity in which every non-zero element has a multiplicative inverse.

Thus a field is an algebraic system in which it is possible to add, subtract, multiply and divide elements (except for division by 0) in such a way that all the 'usual' rules of arithmetic hold. We shall denote a general field by $K$ (from the German *körper*).

- Every ID or field has an additive and multiplicative identity, which are distinct. These will always be denoted by 0 and 1.
- The characteristic of an ID, and thus of a field, can only be zero or a prime.
- Every field is an ID. Every *finite* ID is a field. However, an infinite ID need not be a field. For example, $\mathbb{Z}$ is an ID but not a field.
- A **subfield** of a field $K$ is a subset $S \subset K$ which is itself a field under the operations in $K$. The test for this is that $S$ is non-trivial (check that $0 \in S$ and $1 \in S$), $a - b \in S$ for all $a, b \in S$, and $ab^{-1} \in S$ for all $a, b \in S$ with $b \neq 0$.
- Every field of characteristic 0 is infinite. $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are such fields.

  There are other fields between these, e.g. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$, which is clearly the smallest subfield of $\mathbb{R}$

containing the roots of $x^2 - 2 = 0$. Here, 'smallest' means that it has no proper subfield with the same property.

- The field of complex numbers $\mathbb{C}$ is **algebraically closed**. This means that every polynomial with coefficients in $\mathbb{C}$ factors linearly over $\mathbb{C}$.

- The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, with operations of addition and multiplication modulo $n$, is a ring with characteristic $n$. This is *not* a subring of $\mathbb{Z}$, since the operations are different: $+_n$ and $\times_n$ rather than the ordinary $+$ and $\times$.

  $(\mathbb{Z}_n, +_n, \times_n)$ is a field iff $n$ is prime. This field is then denoted by $\mathbb{F}_n$ or $GF(n)$.

- Every field $K$ has a smallest subfield, its **prime subfield**, which is isomorphic to $\mathbb{Q}$ if $\chi(K) = 0$ and to $\mathbb{F}_p$ if $\chi(K) = p$.

- Every finite field has order (i.e. number of elements) $q = p^n$, where $p$ is prime and $n \in \mathbb{N}$. The field $\mathbb{F}_q$ with $q$ elements is unique up to isomorphism. It has characteristic $p$ and contains $\mathbb{F}_p$. It is not a subfield of $\mathbb{C}$.

A **polynomial** over a ring $R$ is an expression of the form $a_0 + a_1 t + \cdots + a_n t^n$ where $a_0, \ldots, a_n \in R$. The symbol $t$ is called an **indeterminate**. A polynomial will be denoted by a single letter such as f or g. We can write f($t$) to make it clear that the indeterminate is called $t$, but in general $t$ should not be thought of as a number or a variable.

If $\mathrm{f} = \sum_{r=0}^{n} a_r t^r$ where $a_n \neq 0$ then $n$ is the **degree** of f, denoted by $\partial$f, and $a_n$ is the **leading coefficient** of f. If $a_n = 1$ then f is a **monic** polynomial.

The polynomials in $t$ over a ring $R$ themselves form a ring under the usual operations of adding and multiplying polynomials. This ring is denoted by $R[t]$.

A polynomial in $R[t]$ is necessarily a polynomial over any ring that contains $R$. Thus $t^2 - \sqrt{2}\,t + \dfrac{1}{2}$ is in $\mathbb{Q}(\sqrt{2})[t], \mathbb{R}[t]$ and $\mathbb{C}[t]$, but is not in $\mathbb{Z}[t]$ or $\mathbb{Q}[t]$.

A polynomial $\mathrm{f} \in \mathbb{Z}[t]$, i.e. one with integer coefficients, is also in $\mathbb{Q}[t], \mathbb{R}[t]$ and $\mathbb{C}[t]$. As $\mathbb{Q}$ is the smallest *field* containing the coefficients, we shall generally write $\mathrm{f} \in \mathbb{Q}[t]$. For example, writing $t^2 + t + 1 \in \mathbb{Q}[t]$ makes it clear that the integer coefficients lie in the field of rational numbers and not, say, the field of integers modulo 2, for which we would write $t^2+t+1 \in \mathbb{F}_2[t]$.

If $D$ is an integral domain (or field) then $D[t]$ is also an integral domain, but it is *not* a field since, in general, dividing polynomials does not give a polynomial. However we can divide polynomials in the 'usual' way in the following field:

**Definition 1.1** *Let $D$ be an integral domain. The field of* **rational expressions** *over $D$, denoted by $D(t)$, is*
$$\left\{ \frac{\mathrm{f}}{\mathrm{g}} \ : \ \mathrm{f}, \mathrm{g} \in D[t],\ \mathrm{g} \neq 0 \right\}.$$

Since g can be the constant polynomial 1, it is clear that $D[t] \subset D(t)$.

For example, $\mathbb{Z}[t]$ consists of expressions like $2t^5 - 4t^2 + 7t - 6$, while $\mathbb{Z}(t)$ includes expressions like $\dfrac{2t^2 + t - 3}{t^3 + 4}$. We have $\mathbb{Z}[t] \subset \mathbb{Z}(t)$.

A polynomial f is *not* defined to be a function, but it determines a function by $\mathrm{f}(x) = a_0 + a_1 x + \cdots + a_n x^n$. Note that we replace

$t$, which is just a symbol and does not take numerical values, by a variable $x$ which does. One reason for making this distinction is that over a finite field, different polynomials can correspond to the same function. For example, over $\mathbb{F}_2$, the map $x \mapsto x^n$ is the same function for all $n \in \mathbb{N}$, given by $0 \mapsto 0$, $1 \mapsto 1$. However, $t, t^2, t^3, \ldots$ are distinct elements of $\mathbb{F}_2[t]$.

The statement 'f = 0' means that f is the zero polynomial, so the function determined by f is identically zero. On the other hand, $\mathrm{f}(\alpha) = 0$ means that $\alpha$ is a **zero** of f, or a **root** of the equation $\mathrm{f}(x) = 0$.

We know that $\mathrm{f}(\alpha) = 0$ if and only if $(t-\alpha)$ divides f over some field, i.e. $\mathrm{f} = (t-\alpha)\mathrm{g}$ where $\mathrm{g} \in L[t]$ and $L$ is some field that contains the coefficients in f. If f has degree $n$ then it has at most $n$ distinct zeros.

A zero $\alpha$ of f is **repeated** if $(t-\alpha)^m$ is a factor of f, for some integer $m \geq 2$. The highest power of $(t-\alpha)$ which divides f is called the **multiplicity** of $\alpha$ as a zero of f.

**Definition 1.2** *Let* $\mathrm{f} = k(t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_n)$ *where* $k, \alpha_1, \ldots, \alpha_n$ *are constants.*
*Let* $\delta(\mathrm{f}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$. *The* **discriminant** *of* f *is* $\delta(\mathrm{f})^2$, *denoted by* $\Delta(\mathrm{f})$.

Clearly $\Delta(c\mathrm{f}) = \Delta(\mathrm{f})$ for any constant $c \neq 0$, and $\Delta(\mathrm{f}) = 0$ if and only if f has any repeated zeros. Note that the labelling of the zeros of f as $\alpha_1, \alpha_2, \ldots$ is arbitrary and does not affect $\Delta(\mathrm{f})$, though a different ordering may change the sign of $\delta(\mathrm{f})$.

**Example** If $\mathrm{f} = 5(t-2)(t-3)(t-7) \in \mathbb{Q}[t]$ then $\delta(\mathrm{f}) = (2-3)(2-7)(3-7) = -20$ (or 20 if the zeros are ordered

differently) and $\Delta(\mathrm{f}) = 400$.

**Definition 1.3** *Let* $\mathrm{f} = \sum_{r=0}^{n} a_r t^r$. *The* **formal derivative** *of* f *is* $\mathrm{Df} = \sum_{r=1}^{n} r a_r t^{r-1}$.

The word 'formal' is used because this is a purely algebraic definition and no calculus is involved. However, the usual 'differentiation' rules can be shown to hold over any field: $\mathrm{D}(\mathrm{f} + \mathrm{g}) = \mathrm{Df} + \mathrm{Dg}$, $\mathrm{D}(\mathrm{fg}) = \mathrm{f\,Dg} + \mathrm{g\,Df}$, $\mathrm{D}(c\mathrm{f}) = c\mathrm{Df}$. The rule for finding the derivative of a composite function is also valid.

Over an arbitrary field, $ra_r$ is defined to mean $a_r + \cdots + a_r$ ($r$ times).

**Proposition 1.1** *Let* f *be a polynomial over a field* $K$. *Then* $\alpha$ *is a repeated zero of* f *if and only if* $\alpha$ *is a zero of both* f *and* Df.

**Proof** ($\Rightarrow$) Suppose $\alpha$ is a repeated zero of f.

Then there is a polynomial g (over some field) such that $\mathrm{f} = (t-\alpha)^2\mathrm{g}$.

Thus $\mathrm{Df} = (t-\alpha)^2\mathrm{Dg} + 2(t-\alpha)\mathrm{g} = (t-\alpha)((t-\alpha)\mathrm{Dg} + 2\mathrm{g})$.

Hence $(t-\alpha)$ is a factor of Df, so $\alpha$ is a zero of Df as well as of f. □

($\Leftarrow$): Exercise.

### 1.1.1 Examples

(i) Let $\mathrm{f} = t^4 - 4t^2 + 4 \in \mathbb{Q}[t]$, so $\mathrm{Df} = 4t^3 - 8t$.

$\sqrt{2}$ is a zero of both f and Df. This shows that $\sqrt{2}$ is a repeated zero of f.

(ii) Let $\mathrm{f} = mt^n + nmt + 1 \in \mathbb{Q}[t]$, where $m, n \in \mathbb{N}$ and $n > 2$ $\mathrm{Df} = nmt^{n-1} + nm$, so $\mathrm{Df}(x) = 0$ iff $x^{n-1} = -1$. Then $\mathrm{f}(x) = -mx + nmx + 1 =$
$(n-1)mx + 1$. If this is also 0, $x$ is real so $x = -1$. But if $\mathrm{f}(-1) = 0$ then $m = \dfrac{n}{n-1}$, which is not in $\mathbb{N}$ for any $n > 2$. We conclude that f has no repeated zeros.

Of the fields we have defined, only $\mathbb{C}$ is algebraically closed. A polynomial over the rational field $\mathbb{Q}$ may have all, some or none of its zeros in $\mathbb{Q}$. They certainly lie in $\mathbb{C}$; for example $t^2+3t+4$ has two complex zeros $\alpha$ and $\beta$, say, so over $\mathbb{C}$ we can write $t^2 + 3t + 4 = (t - \alpha)(t - \beta)$. We shall be interested in finding the 'smallest' field in which the zeros of a given polynomial lie.

Recall the following result, which was proved in Groups & Rings. It applies to polynomials with *integer* coefficients, but Example (ii) below shows how to adapt it to polynomials over $\mathbb{Q}$.

**Proposition 1.2 (The Rational Root theorem)** *Let* $\mathrm{f} = \sum_{r=0}^{n} a_r t^r \in \mathbb{Z}[t]$ *where* $a_0 \neq 0, a_n \neq 0$. *Suppose* f *has a rational zero* $\dfrac{p}{q}$, *where the integers* $p$ *and* $q$ *are coprime. Then* $p$ *divides* $a_0$ *and* $q$ *divides* $a_n$.

### 1.1.2 Examples

(i) Find a rational zero, if any exist, of $\mathrm{f} = 5t^4 - 2t^3 + 2t^2 - 7t - 6$.

By Proposition 1.2, any zero of f in $\mathbb{Q}$ has the form $\frac{p}{q}$ where $p \mid -6$, $q \mid 5$.

Thus the only possibilities are $\pm 1$, $\pm\frac{1}{5}$, $\pm 2$, $\pm\frac{2}{5}$, $\pm 3$, $\pm\frac{3}{5}$, $\pm 6$, $\pm\frac{6}{5}$.

By trying these, we find that $-\frac{3}{5}$ is the only rational zero of f.

(ii) Show that $t^4 + \frac{1}{2}t^3 - \frac{1}{2}t^2 + 1$ has no rational zeros.

Multiplying through by 2 gives $2t^4 + t^3 - t^2 + 2$. This is *not* the same polynomial but it has the same zeros, since $\mathrm{f}(x) = 0$ if and only if $k\mathrm{f}(x) = 0$ for any $k \neq 0$.

By the Rational Root theorem, the only possible rational zeros are $\pm 1$, $\pm 2$, $\pm\frac{1}{2}$. We can easily check that none of these is a zero, so the polynomial has no rational zeros.

(iii) If f is a *monic* polynomial in $\mathbb{Z}[t]$ then any rational zero of f is an integer which divides the constant term $a_0$. For instance, the only possible rational zeros of $t^5 - 3t^4 - t^3 + 3$ are $-3, -1, 1, 3$. We find that $-1$ and 1 are indeed zeros.

(iv) Let $\mathrm{f} = t^n + pt + p \in \mathbb{Q}[t]$, where $p$ is prime and $n \in \mathbb{N}$. The only possible rational zeros of f are integers which divide $p$, i.e. $\pm 1, \pm p$. Now $\mathrm{f}(-1) = (-1)^n \neq 0$, $\mathrm{f}(1) = 1 + 2p > 0$ and $\mathrm{f}(p) = p^n + p^2 + p > 0$.

If $n$ is odd, $\mathrm{f}(-p) = -p^n - p^2 + p < 0$. If $n$ is even, $\mathrm{f}(-p) = p^n - p^2 + p$, which is negative if $n = 1$ and positive otherwise.

We conclude that f has no rational zeros for any $n \in \mathbb{N}$.

The Rational Root theorem does not apply to polynomials over finite fields, since such fields are quite separate algebraic systems from $\mathbb{Q}$ and $\mathbb{Z}$. Unless there are obvious factors, we have to try all the possibilities:

### 1.1.3 Example

Let $\mathrm{f} = t^4 + 3t^2 + 2 \in \mathbb{F}_5[t]$. Find all the zeros of f in the field $\mathbb{F}_5$.

The elements of $\mathbb{F}_5$ are 0, 1, 2, 3 and 4, all calculations being carried out modulo 5. We find that $\mathrm{f}(0) = 2$, $\mathrm{f}(1) = 1$, $\mathrm{f}(2) = 0$, $\mathrm{f}(3) = 0$, $\mathrm{f}(4) = 1$. (Note that it can be easier to evaluate f(3) and f(4) as $\mathrm{f}(-2)$ and $\mathrm{f}(-1)$ respectively.)

Thus the only zeros of f in $\mathbb{F}_5$ are 2 and 3. Neither of these is a zero of $\mathrm{Df} = 4t^3 + t$, so f has no repeated zeros.

We can write $\mathrm{f} = (t-2)(t-3)\mathrm{g}$, or equivalently $(t+3)(t+2)\mathrm{g}$, where g is found to be $t^2 + 2$ (equivalently $t^2 - 3$, over $\mathbb{F}_5$) by the usual process of algebraic division.

No element of $\mathbb{F}_5$ is a zero of g, i.e. a square root of 3, so g has no zeros in $\mathbb{F}_5$. They exist in a larger field, but we cannot write them as $\pm\sqrt{3}$ as this would indicate *real* numbers. Recall from Groups & Rings that the required elements lie in the field $\mathbb{F}_{25}$, which can be constructed as $\mathbb{F}_5[t]/\langle \mathrm{h} \rangle$ where h is an irreducible quadratic over $\mathbb{F}_5$.

**Definition 1.4** *Let $\alpha_1, \ldots, \alpha_n$ be elements of a field.*

*The* **elementary symmetric functions** *of $\alpha_1, \ldots, \alpha_n$ are*

$$s_1(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} \alpha_i, \quad s_2(\alpha_1, \ldots, \alpha_n) = \sum_{1 \le i < j \le n} \alpha_i \alpha_j,$$

$$s_3(\alpha_1, \ldots, \alpha_n) = \sum_{1 \le i < j < k \le n} \alpha_i \alpha_j \alpha_k, \quad \ldots, \quad s_n(\alpha_1, \ldots, \alpha_n) = \alpha_1 \alpha_2 \cdots \alpha_n.$$

Let $\alpha$ and $\beta$ (not necessarily distinct) be the zeros of the monic quadratic $t^2 + bt + c$.

Then $t^2 + bt + c = (t - \alpha)(t - \beta) = t^2 - (\alpha + \beta)t + \alpha\beta$.
Hence $\alpha + \beta = -b$ and $\alpha\beta = c$.

The monic quadratic polynomial in $t$ with zeros $\alpha$ and $\beta$ is $t^2 - s_1(\alpha, \beta)t + s_2(\alpha, \beta)$.

Now let $\alpha, \beta$ and $\gamma$ be the zeros of the monic cubic $t^3 + bt^2 + ct + d$.

Then $t^3 + bt^2 + ct + d = (t - \alpha)(t - \beta)(t - \gamma)$. Expanding and comparing coefficients, $\alpha + \beta + \gamma = -b,\ \alpha\beta + \beta\gamma + \gamma\alpha = c,\ \alpha\beta\gamma = -d$.

The monic cubic polynomial in $t$ with zeros $\alpha, \beta$ and $\gamma$ is $t^3 - s_1(\alpha, \beta, \gamma)t^2 + s_2(\alpha, \beta, \gamma)t - s_3(\alpha, \beta, \gamma)$.

Similarly, by expanding $(t - \alpha_1) \cdots (t - \alpha_n)$ and comparing coefficients, we have:

**Proposition 1.3** *The monic polynomial in $t$ of degree $n$ with zeros $\alpha_1, \ldots \alpha_n$ is*
$t^n - s_1 t^{n-1} + s_2 t^{n-2} - \cdots + (-1)^n s_n$, *where $s_i$ denotes $s_i(\alpha_1, \ldots \alpha_n)$.*

### 1.1.4 Example

Let $\alpha, \beta$ and $\gamma$ be the zeros of $t^3 - 3t^2 + 5 \in \mathbb{Q}[t]$. Find a monic polynomial with zeros $\alpha^2, \beta^2$ and $\gamma^2$.

$s_1(\alpha, \beta, \gamma) = \alpha + \beta + \gamma = 3,\ \ s_2(\alpha, \beta, \gamma) = \alpha\beta + \beta\gamma + \gamma\alpha = 0,\ \ s_3(\alpha, \beta, \gamma) = \alpha\beta\gamma = -5$.

Thus $s_1(\alpha^2, \beta^2, \gamma^2) = \alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = 9$,

$s_2(\alpha^2, \beta^2, \gamma^2) = \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 = (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = 30$,

$s_3(\alpha^2, \beta^2, \gamma^2) = \alpha^2\beta^2\gamma^2 = (\alpha\beta\gamma)^2 = 25$.

The required polynomial is $t^3 - 9t^2 + 30t - 25$.

## Exercises 1.1

1. Decide, with reasons, whether each of the following is true or false.

   (a) $(\mathbb{N}, +, \times)$ is a ring.

   (b) $(\mathbb{Z}_6, +_6, \times_6)$ is an integral domain.

   (c) $\mathbb{R}[t]$ is an integral domain.

   (d) $\mathbb{C}[t]$ is a field.

   (e) $\mathrm{i}t^3 - 12\mathrm{i}t - \pi$ has three distinct zeros in $\mathbb{C}$.

   (f) Any symbol can be used for the indeterminate in a polynomial.

   (g) A polynomial is defined to be a type of function.

   (h) $\mathbb{Q}(t)$ is a field which contains both $\mathbb{Q}[t]$ and $\mathbb{Q}$.

   (i) The field $\mathbb{F}_4$ is the set $\{0, 1, 2, 3\}$ with operations $+_4$ and $\times_4$.

   (j) $t^2 + t + 1$ has no zeros in $\mathbb{F}_2$, but has two zeros in $\mathbb{F}_4$.

   (k) $\mathbb{F}_2$ is a subfield of both $\mathbb{F}_3$ and $\mathbb{F}_4$.

   (l) Every field of non-zero characteristic is finite.

2. Let $\mathrm{f} = t^4 - 3t^3 + 6t - 4 \in \mathbb{Q}[t]$. Find all the zeros of f in $\mathbb{C}$, and evaluate $\Delta(\mathrm{f})$.

3. Prove the "$\Leftarrow$" part of Proposition 1.1.

4. Suppose $c$ is a non-zero integer and $n$ is a positive integer. Show that the polynomial $t^n + t + c$ has no repeated rational zeros.

5. Use the Rational Root theorem to find all the rational zeros, if any exist, of

(a) $2t^3 + 5t^2 - 1$, (b) $t^4 + 2t^3 - t - 2$, (c) $t^4 - 3t^2 + 2t - \frac{1}{3}$.

6. (a) Show that $t^5 + 2t^3 + t + 3 \in \mathbb{F}_5[t]$ has no zeros in $\mathbb{F}_5$.

   (b) Show that $t^5 + 2t^3 + 4t + 3 \in \mathbb{F}_5[t]$ has a repeated zero, and find it.

7. Let $\mathrm{f} = t^5 + 6t^2 + t + 3 \in \mathbb{F}_7[t]$. Find all the zeros of f in $\mathbb{F}_7$. Hence express f as a product of linear factors and a non-linear factor in $\mathbb{F}_7[t]$.

8. Find (a) the monic quadratic in $\mathbb{Q}[t]$ whose zeros have sum 6 and product $-10$,

   (b) the monic cubic in $\mathbb{Q}[t]$ with zeros $\alpha, \beta$ and $\gamma$ such that $\alpha + \beta + \gamma = \alpha\beta + \beta\gamma + \gamma\alpha = \alpha\beta\gamma = -1$.

9. Let $\alpha$ and $\beta$ be the zeros of $t^2 - 5t - 4 \in \mathbb{Q}[t]$. Write down the values of $\alpha + \beta$ and $\alpha\beta$. Hence find the values of $\alpha^2 + \beta^2$ and $\alpha^2\beta^2$.

   Without finding $\alpha$ and $\beta$, obtain a quadratic in $\mathbb{Z}[t]$ whose zeros are $\alpha^2$ and $\beta^2$.

10. Expand $(\alpha+\beta+\gamma)^2$. Having done so, be confident that you can write down this expansion in its simplest form without needing to do any work!

    $\alpha, \beta$ and $\gamma$ are the zeros of $t^3+5t^2-10t-7 \in \mathbb{Q}[t]$. Without finding $\alpha, \beta$ and $\gamma$, find the value of $\alpha^2 + \beta^2 + \gamma^2$.

## 1.2 Solution of polynomial equations over $\mathbb{Q}$

The polynomial $t^n - 1$ has $n$ distinct zeros in the complex field $\mathbb{C}$. These are called the $n$th **roots of unity**. They are the

complex numbers $\mathrm{e}^{2k\pi\mathrm{i}/n}$, or equivalently $\cos\dfrac{2k\pi}{n}+\mathrm{i}\sin\dfrac{2k\pi}{n}$, for $k=0,1,\ldots,n-1$. In the complex plane, they are the vertices of a regular $n$-sided polygon with centre at 0 and one vertex at 1.

$t^n-1$ factorises as $(t-1)(t^{n-1}+t^{n-2}+\cdots+t+1)$, so the $n$th roots of unity other than 1 are the zeros of $t^{n-1}+t^{n-2}+\cdots+t+1$.

The square roots of 1 are 1 and $-1$. The fourth roots of 1 are 1, i, $-1$ and $-\mathrm{i}$.

The cube roots of 1 are $1,\omega,\omega^2$ where

$$\omega=\mathrm{e}^{2\pi\mathrm{i}/3}=\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}=-\frac{1}{2}+\mathrm{i}\frac{\sqrt{3}}{2}.$$

Note that $\omega^3=1$, $\dfrac{1}{\omega}=\omega^2=\overline{\omega}$, and $\omega^2+\omega+1=0$.

The fifth roots of 1 are $\mathrm{e}^{2k\pi\mathrm{i}/5}$ for $k=0,1,2,3,4$, i.e. $1,\eta,\eta^2,\eta^3,\eta^4$ where $\eta=\mathrm{e}^{2\pi\mathrm{i}/5}$.

$\alpha\in\mathbb{C}$ is called a **primitive** $n$th root of unity if $\alpha,\alpha^2,\ldots,\alpha^n$ are the $n$ distinct $n$th roots of unity. For example, both $\omega$ and $\omega^2$ are primitive cube roots of unity. Both i and $-\mathrm{i}$ are primitive fourth roots of unity, but 1 and $-1$ are not.

$\mathrm{e}^{2k\pi\mathrm{i}/n}$ is a primitive $n$th root of unity if and only if $k$ and $n$ are coprime. For example, the primitive 8th roots of unity are $\mathrm{e}^{\pi\mathrm{i}/4},\mathrm{e}^{3\pi\mathrm{i}/4},\mathrm{e}^{5\pi\mathrm{i}/4},\mathrm{e}^{7\pi\mathrm{i}/4}$ (taking $k=1,3,5,7$). The number of primitive $n$th roots of unity is given by the Euler totient function $\varphi(n)$.

When $p$ is prime, all the $p$th roots of unity except 1 are primitive.

The complex roots of a polynomial equation over $\mathbb{R}$ always occur in conjugate pairs.

The $n$th roots of a complex number $z$ can be found as follows. Express $z$ as $re^{\theta i}$ where $r \in \mathbb{R}^+$. Then $r^{1/n}e^{\theta i/n}$ is one $n$th root of $z$. Multiplying this by the $n$th roots of 1 gives all the $n$th roots of $z$. In the complex plane, these are represented by $n$ points equally spaced around a circle with centre 0 and radius $|z|^{1/n}$.

### 1.2.1 Example

Find the zeros in $\mathbb{C}$ of the polynomial $(t-1)^6 + 1 \in \mathbb{Q}[t]$.

The zeros are values of $x$ such that $(x-1)^6 = -1$, i.e. $x-1$ is a sixth root of $-1$.

Now $-1 = e^{\pi i}$, so $e^{\pi i/6}$ is one sixth root of $-1$. Multiplying this by each of the sixth roots of 1, namely $e^{2k\pi i/6}$ for $k = 0, \ldots, 5$, gives the six values of $x-1$ as $e^{\pi i/6}$, $e^{\pi i/2}$, $e^{5\pi i/6}$, $e^{7\pi i/6}$, $e^{3\pi i/2}$, $e^{11\pi i/6}$.

Using $e^{\pi i} = -1$, $e^{7\pi i/6} = -e^{\pi i/6}$ and $e^{11\pi i/6} = -e^{5\pi i/6}$, the required zeros can be written as $1 \pm e^{\pi i/6}$, $1 \pm i$, $1 \pm e^{5\pi i/6}$.

If $f \in \mathbb{Q}[t]$ has leading coefficient $a_n$ then $\frac{1}{a_n} f$ is in $\mathbb{Q}[t]$ and has the same zeros as f.

Thus we need only consider a monic polynomial $f = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$. The zeros of f are values of $x$ such that $f(x) = 0$.

Substituting $x = y - \frac{a_{n-1}}{n}$ in $f(x)$ (the **Tschirnhaus transformation**), the first two terms become $\left(y^n - n\frac{a_{n-1}}{n}y^{n-1} + \cdots\right) + a_{n-1}(y^{n-1} - \cdots)$, in which $y^{n-1}$ has coefficient 0. Thus a polynomial of degree $n$ can always be transformed into one which has no term of degree $n-1$.

## Quadratic equations

Let $\mathrm{f} = t^2+bt+c$. To find the zeros of f we solve $x^2+bx+c=0$ for $x$.

Put $x = y - \dfrac{b}{2}$ to get $y^2 - by + \dfrac{b^2}{4} + by - \dfrac{b^2}{2} + c = 0$, so

$y^2 = \dfrac{b^2}{4} - c = \dfrac{b^2-4c}{4}$.

Thus $y = \pm\dfrac{\sqrt{b^2-4c}}{2}$, so $x = \dfrac{-b \pm \sqrt{b^2-4c}}{2}$.

Let $\alpha$ and $\beta$ be these values of $x$. The discriminant of f is $\Delta(\mathrm{f}) = (\alpha-\beta)^2 = b^2-4c$.

**Proposition 1.4** *Let* $\mathrm{f} = t^2+bt+c \in \mathbb{Q}[t]$. *Then* $\Delta(\mathrm{f}) = b^2-4c$.

*If* $\Delta(\mathrm{f}) = 0$ *then* f *has a repeated real zero.*

*If* $\Delta(\mathrm{f}) > 0$ *then* f *has two distinct real zeros.*

*If* $\Delta(\mathrm{f}) < 0$ *then* f *has two distinct conjugate complex zeros.*

## Cubic equations

Let $\mathrm{f} = t^3+bt^2+ct+d$. The zeros of f are the roots of $x^3+bx^2+cx+d=0$.

Put $x = y - \dfrac{b}{3}$ (Tschirnhaus transformation) to get $y^3+py+q=0$, where $p$ and $q$ can be expressed in terms of $b, c$ and $d$ if desired (see exercises).

If $p=0$ then $y^3 = -q$ so $y = (-q)^{1/3}$, $(-q)^{1/3}\omega$, $(-q)^{1/3}\omega^2$ where $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$.

For example, $t^3-2$ has zeros $\alpha, \alpha\omega, \alpha\omega^2$ where $\alpha = 2^{1/3}$ is the real cube root of 2.

If $p \neq 0$ and there is no obvious factor we use the **Vieta substitution** $y = z - \dfrac{p}{3z}$

and get $z^6 + qz^3 - \dfrac{p^3}{27} = 0$, a quadratic in $z^3$, which gives

$z^3 = -\dfrac{q}{2} \pm \dfrac{1}{6}\sqrt{\dfrac{4p^3 + 27q^2}{3}}$.

Let $\varepsilon$ be a cube root of either value of $z^3$. Then $z = \varepsilon$, $\varepsilon\omega$ or $\varepsilon\omega^2$,

so $y = z - \dfrac{p}{3z}$, giving $y = \varepsilon - \dfrac{p}{3\varepsilon},\ \varepsilon\omega - \dfrac{p\omega^2}{3\varepsilon},\ \varepsilon\omega^2 - \dfrac{p\omega}{3\varepsilon}$. Subtracting $\dfrac{b}{3}$ gives the

three zeros of f. It is left as an exercise to show that each of the two values of $z^3$ yields the same solutions for $y$ and hence for $x$.

### 1.2.2 Example

Let $\mathrm{f} = t^3 + 6t^2 - 60t - 416$. The zeros of f are values of $x$ such that $\mathrm{f}(x) = 0$.

Let $x = y - 2$ (Tschirnhaus transformation), giving

$y^3 - 72y - 280 = 0$.

Now put $y = z + \dfrac{24}{z}$ (Vieta substitution) to get

$z^6 - 280z^3 + 13824 = 0$.

$z^3 = 140 \pm \sqrt{5776}$ so $z^3 = 64$ or $z^3 = 216$. Thus $z = 4, 4\omega, 4\omega^2, 6, 6\omega, 6\omega^2$.

$\dfrac{1}{\omega} = \omega^2$, so the distinct values of $z + \dfrac{24}{z}$ are $10$, $4\omega + 6\omega^2$, $4\omega^2 + 6\omega$, i.e. $y = 10, -5 \pm \sqrt{3}$ i.

$x = y - 2$, so the zeros of f are $8$, $-7 + \sqrt{3}$ i, $-7 - \sqrt{3}$ i.

If a cubic $\mathrm{f} \in \mathbb{Q}[t]$ has zeros $\alpha, \beta, \gamma$, then $\Delta(\mathrm{f}) = \delta(\mathrm{f})^2 = [(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)]^2$.

If f has a repeated zero then $\Delta(\mathrm{f}) = 0$.

If f has three distinct real zeros then $\delta(\mathrm{f}) \in \mathbb{R}$ so $\Delta(\mathrm{f}) > 0$.

If f has one real zero $\alpha$ and two complex zeros $\mu \pm \nu\mathrm{i}$ where $\mu, \nu \in \mathbb{R}$ and $\nu \neq 0$, then $\delta(\mathrm{f}) = (\alpha-\mu-\nu\mathrm{i})(\alpha-\mu+\nu\mathrm{i})(2\nu\mathrm{i}) = 2\nu((\alpha-\mu)^2+\nu^2)\mathrm{i}$, so $\Delta(\mathrm{f}) < 0$.

Let V be the **Vandermonde matrix** $\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{pmatrix}$. Then (see exercises) $\det(\mathrm{V}) = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$, so if $\alpha, \beta, \gamma$ are the zeros of f then $\Delta(\mathrm{f}) = \det(\mathrm{V})^2$.

We know that $\det(\mathrm{V}) = \det(\mathrm{V}^\mathsf{T})$, so $\Delta(\mathrm{f}) = \det(\mathrm{V})\det(\mathrm{V}^\mathsf{T}) = \det(\mathrm{V}\mathrm{V}^\mathsf{T})$.

Now $\mathrm{V}\mathrm{V}^\mathsf{T} = \begin{pmatrix} 3 & \alpha+\beta+\gamma & \alpha^2+\beta^2+\gamma^2 \\ \alpha+\beta+\gamma & \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 \\ \alpha^2+\beta^2+\gamma^2 & \alpha^3+\beta^3+\gamma^3 & \alpha^4+\beta^4+\gamma^4 \end{pmatrix}$.

If $\mathrm{f} = t^3 + pt + q \in \mathbb{Q}[t]$ then $\alpha+\beta+\gamma = 0$ (the coefficient of $t^2$) and using the elementary symmetric functions we get $\alpha^2+\beta^2+\gamma^2 = -2p, \alpha^3+\beta^3+\gamma^3 = -3q, \alpha^4+\beta^4+\gamma^4 = 2p^2$, giving $\Delta(\mathrm{f}) = -4p^3 - 27q^2$. If $p > 0$ then clearly $\Delta(\mathrm{f}) < 0$.

Note: the values of $z^3$ that we found when solving this cubic are $-\dfrac{q}{2} \pm \dfrac{1}{6}\sqrt{\dfrac{-\Delta(\mathrm{f})}{3}}$.

**Proposition 1.5** *Let* $\mathrm{f} = t^3 + pt + q \in \mathbb{Q}[t]$. *Then the discriminant of* f *is* $-4p^3 - 27q^2$.

*If* $\Delta(\mathrm{f}) = 0$ *then* f *has real zeros, including a repeated zero.*

*If* $\Delta(\mathrm{f}) > 0$ *then* f *has three distinct real zeros.*

*If* $\Delta(\mathrm{f}) < 0$ *then* f *has one real zero and two distinct conjugate complex zeros.*

### 1.2.3 Examples

(i) Let $\mathrm{f} = t^3 + 3t + 1$. As $\mathrm{f}(1) \neq 0$ and $\mathrm{f}(-1) \neq 0$, f has no rational zeros.

$\Delta(\mathrm{f}) = -135 < 0$ so f has one real zero and two conjugate complex zeros.

To solve $\mathrm{f}(x) = 0$ put $x = z - \dfrac{1}{z}$ (Vieta), so $z^6 + z^3 - 1 = 0$.

Hence $z^3 = \dfrac{-1 \pm \sqrt{5}}{2}$.

Let $\varepsilon$ be the real cube root of $\dfrac{-1+\sqrt{5}}{2}$. Then $z = \varepsilon, \varepsilon\omega, \varepsilon\omega^2$.

The zeros of f are $\varepsilon - \dfrac{1}{\varepsilon}$ (real but not rational), $\varepsilon\omega - \dfrac{\omega^2}{\varepsilon}$ and $\varepsilon\omega^2 - \dfrac{\omega}{\varepsilon}$.

(ii) Let $\mathrm{f} = t^3 - 3t + 1$. As in the previous example, f has no rational zeros.

$\Delta(\mathrm{f}) = 81 > 0$ so f has three distinct real zeros. To solve $\mathrm{f}(x) = 0$ put $x = z + \dfrac{1}{z}$.

Then $z^6 + z^3 + 1 = 0$, so $z^3 = \dfrac{-1 \pm \mathrm{i}\sqrt{3}}{2}$, i.e. $z^3 = \omega$ or $z^3 = \omega^2$.

Let $\eta = \mathrm{e}^{2\pi\mathrm{i}/9}$, so $\eta^3 = \omega$. Then $z = \eta, \eta\omega, \eta\omega^2$, i.e. $z = \eta, \eta^4, \eta^7$. $\eta^9 = 1$, so $\dfrac{1}{\eta} = \eta^8$.

The three zeros of f are $\alpha = \eta + \eta^8$, $\beta = \eta^2 + \eta^7$, $\gamma = \eta^4 + \eta^5$.
Each of $\alpha, \beta, \gamma$ is a sum of conjugate complex numbers, so is real (but not rational). In fact, $\alpha = 2\cos\frac{2\pi}{9}, \beta = 2\cos\frac{4\pi}{9}, \gamma = 2\cos\frac{8\pi}{9}$.
As $\cos 2\theta = 2\cos^2\theta - 1$ we have $\alpha^2 = \beta + 2$, $\beta^2 = \gamma + 2$, $\gamma^2 = \alpha + 2$, so the zeros of f are $\alpha$, $\alpha^2 - 2$, $2 - \alpha - \alpha^2$. Their sum is 0, as expected since f has no $t^2$ term.

(iii) Let $\mathrm{f} = t^3 - 2t^2 - t + 1$. To solve $\mathrm{f}(x) = 0$ put $x = y + \frac{2}{3}$ to get $y^3 - \frac{7}{3}y - \frac{7}{27} = 0$.
$\Delta(\mathrm{f}) = 49 > 0$ so f has three distinct real zeros.
In general $z^3$ will not have a 'nice' cube root. An alternative method when $\Delta(\mathrm{f}) > 0$ is to substitute $y = r\cos\theta$ and use the identity $\cos 3\theta \equiv 4\cos^3\theta - 3\cos\theta$.
Let $y = r\cos\theta$, so the equation is $r^3\cos^3\theta - \frac{7}{3}r\cos\theta - \frac{7}{27} = 0$.
Thus $\frac{r^3}{4}\cos 3\theta + \frac{3r^3}{4}\cos\theta - \frac{7r}{3}\cos\theta - \frac{7}{27} = 0$.
Now find $r > 0$ and $\theta$ such that $\frac{3r^3}{4} - \frac{7r}{3} = 0$ and $\frac{r^3}{4}\cos 3\theta - \frac{7}{27} = 0$.
$9r^2 = 28$ so $r = \frac{2}{3}\sqrt{7} \approx 1.764$. Also $\cos 3\theta = \frac{28}{27r^3} = \frac{1}{2\sqrt{7}} \approx 0.189$ so $3\theta \approx 1.38 + 2n\pi$.
Thus $\cos\theta \approx 0.895, -0.033, -0.832$, giving $y \approx 1.58, -0.11, -1.47$.
$x = y + \frac{2}{3}$ so f has zeros $2.25, 0.56, -0.80$ (correct to two decimal places).

## Quartic equations

A monic quartic polynomial over $\mathbb{Q}$ has the form $t^4 + bt^3 +$

$ct^2 + dt + e$. The $t^3$ term can be eliminated by a Tschirnhaus transformation, so we can assume that $b = 0$.

If also $d = 0$ we have $t^4 + ct^2 + e$, a quadratic in $t^2$. If $e = 0$ we can take out a factor of $t$ and get a cubic. In other cases we proceed as follows:

$t^4 + ct^2 + dt + e$ must factorise over $\mathbb{C}$ in the form $(t^2 + kt + \ell)(t^2 - kt + m)$, otherwise there would be a non-zero $t^3$ term. Expanding and comparing coefficients gives:

$\ell + m - k^2 = c$, $k(m - \ell) = d$, $\ell m = e$.

For $k \neq 0$, the first two of these yield $\ell = \frac{1}{2}\left(k^2 + c - \frac{d}{k}\right)$ and $m = \frac{1}{2}\left(k^2 + c + \frac{d}{k}\right)$.

Then $\ell m = e$ gives $k^6 + 2ck^4 + (c^2 - 4e)k^2 - d^2 = 0$,

so $(-k^2)^3 - 2c(-k^2)^2 + (c^2 - 4e)(-k^2) + d^2 = 0$.

It follows that $-k^2$ is a zero of the cubic $t^3 - 2ct^2 + (c^2 - 4e)t + d^2$.

**Definition 1.5** *The* **cubic resolvent** *of the quartic* $t^4 + ct^2 + dt + e \in \mathbb{Q}[t]$ *is the polynomial* $\rho = t^3 - 2ct^2 + (c^2 - 4e)t + d^2$.

As we can (in theory) solve a cubic, we can find the zeros of the cubic resolvent. Let $-k^2$ be a zero of $\rho$. From this we can find values of $k, \ell, m$ and then solve two quadratics to get the zeros of the quartic.

The formulae for the cubic resolvent and the quantities $\ell$ and $m$ will be given if they are needed in a test or examination question.

Suppose $d \neq 0$. Then $d^2 > 0$ and a graph shows that $\rho$ has at least one negative real zero, which can be taken as $-k^2$.

### 1.2.4 Example

Let $\mathrm{f} = t^4+2t^2+t+2$, so $\rho = t^3-4t^2-4t+1 = (t+1)(t^2-5t+1)$ which has a negative real zero $-1$. To make $-k^2 = -1$, take $k = 1$ (or $-1$).

Then $\ell + m = c + k^2 = 3$ and $m - \ell = \dfrac{d}{k} = 1$ so $\ell = 1, m = 2$.

Thus $\mathrm{f} = (t^2 + t + 1)(t^2 - t + 2)$, whose zeros are:
$\frac{1}{2}(-1 + \mathrm{i}\sqrt{3})$, $\frac{1}{2}(-1 - \mathrm{i}\sqrt{3})$, $\frac{1}{2}(1 + \mathrm{i}\sqrt{7})$, $\frac{1}{2}(1 - \mathrm{i}\sqrt{7})$.

Returning to $\mathrm{f} = t^4 + ct^2 + dt + e = (t^2 + kt + \ell)(t^2 - kt + m)$, let $\alpha_1, \alpha_2$ be the zeros of $t^2 + kt + \ell$ and let $\alpha_3, \alpha_4$ be the zeros of $t^2 - kt + m$.

Then $\alpha_1 + \alpha_2 = -k$ and $\alpha_3 + \alpha_4 = k$.

Let $u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$, so $u = -k^2$ and we know that $\rho(-k^2) = 0$, i.e. $\rho(u) = 0$.

Now also $\mathrm{f} = [(t - \alpha_1)(t - \alpha_3)][(t - \alpha_2)(t - \alpha_4)] = (t^2 + k't + \ell')(t^2 - k't + m')$, say.

By the same reasoning as before, $-k'^2$ is a zero of the cubic resolvent $\rho$.

Let $v = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$. Then $v = (-k')(k') = -k'^2$, so $\rho(v) = 0$.

Similarly if $w = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$ then $\rho(w) = 0$.

Thus $u, v, w$ are zeros of $\rho$. Clearly if they are distinct, they are all the zeros of $\rho$. By verifying that $u + v + w = 2c, uv + vw + uw = c^2 - 4e$ and $uvw = -d^2$, it can be shown that $\rho = (t - u)(t - v)(t - w)$ even if $u, v, w$ are not distinct.

**Proposition 1.6** *If* $\mathrm{f} = t^4 + ct^2 + dt + e \in \mathbb{Q}[t]$ *has zeros*

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$ *then* $\rho$*, the cubic resolvent of* f*, has zeros* $u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), v = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$ *and* $w = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$.

## Exercises 1.2

1. Find, in exponential form, all the primitive fifth, sixth, tenth and twelfth roots of unity.

2. Find the zeros in $\mathbb{C}$ of: (a) $t^{10} - 1$, (b) $t^4 + 1$, (c) $(t-2)^5 - 32$.

3. Find the zeros of the following cubics in $\mathbb{Q}[t]$. Where appropriate, give solutions in terms of $\varepsilon = 2^{1/3}$ and $\omega = \mathrm{e}^{2\pi \mathrm{i}/3}$. In each case, also find the discriminant.

   (a) $t^3 - 16$, (b) $t^3 + 1$, (c) $t^3 - 3t - 2$, (d) $t^3 + 6t + 2$,

   (e) $t^3 - 9t - 9$ (for (e), try the methods of both Examples 1.2.3 (ii) and (iii)).

4. Let $\alpha, \beta, \gamma$ be the zeros of $\mathrm{f} = t^3 + pt + q \in \mathbb{Q}[t]$, where $q \neq 0$.

   (a) Show that $\beta + \gamma = -\alpha$ and $\beta\gamma = \alpha^2 + p$.

   (b) Deduce that $\beta$ and $\gamma$ are given by $\dfrac{-\alpha \pm \sqrt{-3\alpha^2 - 4p}}{2}$.

   (c) Show that $\Delta(\mathrm{f}) = -(3\alpha^2 + 4p)(3\alpha^2 + p)^2$. Deduce that if $\delta(\mathrm{f}) \in \mathbb{Q}$ then all three zeros of f are *rational functions* of $\alpha$, i.e. they have the form $\dfrac{\mathrm{g}(\alpha)}{\mathrm{h}(\alpha)}$ where g and h are polynomials.

   (d) Given that one zero of $t^3 - 6t + 6$ is $-2^{1/3} - 2^{2/3}$, use part (b) to find the other zeros in surd form.

5. If the Tschirnhaus transformation $x = y - \dfrac{b}{3}$ transforms $x^3 + bx^2 + cx + d$ to $y^3 + py + q$, find expressions for $p$ and $q$ in terms of $b, c$ and $d$.

   Show that the cubic in $x$ and the cubic in $y$ have the same discriminant.

6. Prove the statement on Page 9 that each of the two values of $z^3$ in the solution of the cubic yields the same values of $x$.

7. (a) Let V be the Vandermonde matrix on page 10. Show that the determinant of V is $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$. (Hint: first carry out some column operations.)

   (b) Using the fact that $\alpha^3 + p\alpha + q = \beta^3 + p\beta + q = \gamma^3 + p\gamma + q = 0$, show that

   (i) $\alpha^3 + \beta^3 + \gamma^3 + p(\alpha + \beta + \gamma) + 3q = 0$,

   (ii) $\alpha^4 + \beta^4 + \gamma^4 + p(\alpha^2 + \beta^2 + \gamma^2) + q(\alpha + \beta + \gamma) = 0$.

   Hence derive the expression for $\Delta(\mathrm{f})$ in Proposition 1.5.

8. Let f be a cubic polynomial in $\mathbb{Q}[t]$ which has an irrational real zero $r$ and complex zeros $p - q\mathrm{i}$, $p + q\mathrm{i}$ where $q \neq 0$. Show that $|p + q\mathrm{i}|^2 \notin \mathbb{Q}$.

9. Find the zeros of the following quartics in $\mathbb{Q}[t]$:

   (a) $4t^4 - 4t^2 - 16t + 5$, (b) $4t^4 + 8t - 3$.

10. Show that the quartic $t^4 + ct^2 + dt + e \in \mathbb{Q}[t]$ has the same discriminant as its cubic resolvent. (Use Proposition 1.6.)

## 1.3 Tests for irreducibility

Let $D$ be an integral domain. Recall that a **unit** in $D$ is an element which has a multiplicative inverse in $D$. Thus $-1$ and

1 are the only units of $\mathbb{Z}$. They are also the only units of the integral domain $\mathbb{Z}[t]$. In a field, every non-zero element is a unit.

A non-zero, non-unit element is said to be **reducible** in $D$ if it is the product of two non-unit elements of $D$, and **irreducible** in $D$ otherwise.

If a polynomial is (ir)reducible in $D[t]$, we can say that it is (ir)reducible **over** $D$.

To avoid being concerned about units, we introduce the following terminology:

**Definition 1.6** *Let $D$ be an integral domain. A polynomial $\mathrm{f} \in D[t]$, of degree $\geq 1$, is* **properly reducible** *over $D$ if $\mathrm{f} = \mathrm{gh}$ where $\mathrm{g}, \mathrm{h} \in D[t], \partial\mathrm{g} < \partial\mathrm{f}$ and $\partial\mathrm{h} < \partial\mathrm{f}$.*

Over a *field*, 'properly reducible' means the same as 'reducible'.

If a polynomial in $\mathbb{Z}[t]$ is properly reducible over $\mathbb{Z}$ then clearly it is reducible over $\mathbb{Q}$. We shall show in due course that the converse is also true.

Recall the following from Groups & Rings:

**Proposition 1.7** *Let $K$ be a field. Every polynomial in $K[t]$ of degree 1 is irreducible over $K$. A polynomial in $K[t]$ of degree 2 or 3 is reducible over $K$ if and only if it has a zero in $K$.*

It can be shown that the expression of a polynomial as a product of irreducible factors over a field is unique (up to constant factors and the order of the factors). Thus a polynomial of degree $n$ over a field $K$ has at most $n$ distinct zeros.

### 1.3.1 Examples

(i) Let $\mathrm{f} = 3t^2 + 12 \in \mathbb{Q}[t]$. f is reducible over $\mathbb{Z}$, as $\mathrm{f} = 3(t^2+4)$. It is *not* properly reducible over $\mathbb{Z}$ since it is not a product of two polynomials in $\mathbb{Z}[t]$, both of degree $< 2$. f is not reducible over $\mathbb{Q}$, since 3 is a unit in $\mathbb{Q}[t]$ (but not in $\mathbb{Z}[t]$).

(ii) Let $\mathrm{f} = t^3 - 3t + 1 \in \mathbb{Q}[t]$. We saw in Example 1.2.3 (ii) that f has no rational zeros. As $\partial \mathrm{f} \leq 3$, this is enough to show that f is irreducible over $\mathbb{Q}$. We found its three real zeros $\alpha, \beta$ and $\gamma$. Over $\mathbb{R}$, f is reducible as $(t-\alpha)(t-\beta)(t-\gamma)$.

(iii) Let $\mathrm{f} = t^3 + t^2 + 3 \in \mathbb{F}_7[t]$. We find that none of $0, 1, \ldots, 6$ is a zero of f in $\mathbb{F}_7$. As $\partial \mathrm{f} \leq 3$, this is enough to show that f is irreducible over $\mathbb{F}_7$.

(iv) Let $\mathrm{f} = t^4 - t^3 + 5t - 3$. By the Rational Root theorem, f has no rational zeros. This does *not* show that it is irreducible over $\mathbb{Q}$. In fact, it is reducible as $\mathrm{f} = (t^2+t-1)(t^2-2t+3)$, a product of two irreducible quadratic factors over $\mathbb{Q}$.

**Definition 1.7** *Let $R, S, R', S'$ be sets with $R \subset R', S \subset S'$. Let $\phi, \phi'$ be mappings from $R$ to $S$ and $R'$ to $S'$. If $\phi'(a) = \phi(a)$ for all $a \in R$ then $\phi'$* **extends** *$\phi$, and $\phi$ is the* **restriction** *of $\phi'$ to $R$.*

Recall that a ring (or field) **homomorphism** is a map between rings (or fields) $R$ and $S$ such that $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ for all $r_1, r_2 \in R$.

A homomorphism also has the property that $\phi(0_R) = 0_S$. When $R$ and $S$ are integral domains or fields then $\phi(1_R) = 1_S$. If $\phi$ is bijective, it is a ring (or field) **isomorphism**.

We may often omit the word 'ring' or 'field', except where there is any danger of confusion with group homomorphisms.

**Proposition 1.8** *Let $\phi : R \to S$ be a ring homomorphism and define $\bar{\phi} : R[t] \to S[t]$ by $\bar{\phi}\left(\sum_{r=0}^{n} a_r t^r\right) = \sum_{r=0}^{n} \phi(a_r)t^r$. Then $\bar{\phi}$ is a ring homomorphism which extends $\phi$. If $\phi$ is an isomorphism then so is $\bar{\phi}$.*

**Proof**

Let $\mathrm{f} = \sum_{r=0}^{n} a_r t^r$ and $\mathrm{g} = \sum_{r=0}^{m} b_r t^r \in R[t]$. Assume, without loss of generality, that $m \leq n$. If $m < n$, take $b_r$ to be 0 for $r = m+1, \ldots, n$.

Then $\bar{\phi}(\mathrm{f} + \mathrm{g}) = \bar{\phi}\left(\sum_{r=0}^{n}(a_r + b_r)t^r\right) = \sum_{r=0}^{n} \phi(a_r + b_r)t^r =$

$\sum_{r=0}^{n}(\phi(a_r) + \phi(b_r))t^r$

$= \sum_{r=0}^{n} \phi(a_r)t^r + \sum_{r=0}^{m} \phi(b_r)t^r = \bar{\phi}(\mathrm{f}) + \bar{\phi}(\mathrm{g})$.

Also $\bar{\phi}(\mathrm{fg}) = \bar{\phi}\left(\sum_{s=0}^{n+m}\sum_{r=0}^{s} a_r b_{s-r} t^s\right) = \sum_{s=0}^{n+m}\sum_{r=0}^{s} \phi(a_r)\phi(b_{s-r})t^s =$ $\bar{\phi}(\mathrm{f})\bar{\phi}(\mathrm{g})$. Thus $\bar{\phi}$ is a ring homomorphism.

$\bar{\phi}$ acts on elements of $R$ by $\bar{\phi}(a) = \bar{\phi}(at^0) = \phi(a)t^0 = \phi(a)$, so it extends $\phi$.

If $\phi$ is an isomorphism then it has an inverse $\phi^{-1} : S \to R$. Define $\bar{\phi}^{-1} : S[t] \to R[t]$ by $\bar{\phi}^{-1}\left(\sum_{r=0}^{n} a_r t^r\right) = \sum_{r=0}^{n} \phi^{-1}(a_r)t^r$. By the same reasoning as for $\phi$ above, $\bar{\phi}^{-1}$ is also a ring homomorphism and is clearly the inverse of $\bar{\phi}$. Thus $\bar{\phi}$ is an isomorphism.

□

We shall usually omit the bar and denote the extended homomorphism by $\phi$ also.

Recall that the **natural homomorphism** from $\mathbb{Z}$ into $\mathbb{Z}_n$ is the map $\nu_n$ defined by $\nu_n(a) = a \bmod n$. For example, $\nu_3(8) = 8 \bmod 3 = 2$.

$\nu_n$ is a ring homomorphism, so by Proposition 1.8 it can be extended to a ring homomorphism $\nu_n : \mathbb{Z}[t] \to \mathbb{Z}_n[t]$ which has the effect of reducing each coefficient modulo $n$. If $p$ is prime, $\mathbb{Z}_p$ is the finite field $\mathbb{F}_p$.

For example, $\nu_5(2t^6+8t^5-5t^3-6t+10) = 2t^6+3t^5+4t \in \mathbb{F}_5[t]$.

**Definition 1.8** *Let* f *be a non-zero polynomial in* $\mathbb{Z}[t]$*. The* **content** *of* f*, denoted by* $c_{\mathrm{f}}$*, is the largest positive integer which divides all the coefficients in* f*.*

f *is a* **primitive** *polynomial if* $c_{\mathrm{f}} = 1$*.*

*If* $\mathrm{f} \in \mathbb{Q}[t]$*, let* $k$ *be the smallest positive integer such that* $k\mathrm{f} \in \mathbb{Z}[t]$*. The* **content** *of* f *is then* $c_{\mathrm{f}} = \dfrac{1}{k} c_{k\mathrm{f}}$*.*

### 1.3.2 Example

Let $\mathrm{f} = \dfrac{3}{5}t^2 - \dfrac{3}{4}t + \dfrac{9}{10}$. Then $k = 20$ in the above definition, and

$\mathrm{f} = \dfrac{1}{20}(12t^2 - 15t + 18) = \dfrac{3}{20}(4t^2 - 5t + 6)$. $4t^2 - 5t + 6$ is primitive, and $c_{\mathrm{f}} = \dfrac{3}{20}$.

Every non-zero polynomial $\mathrm{f} \in \mathbb{Q}[t]$ has a unique expression as $c_{\mathrm{f}}\hat{\mathrm{f}}$ where $\hat{\mathrm{f}}$ is primitive.

**Proposition 1.9** *Let* f *and* g *be primitive polynomials in* $\mathbb{Z}[t]$. *Then* fg *is primitive.*

## Proof

Suppose fg is not primitive, so there is a prime $p$ which divides all its coefficients. Apply $\nu_p : \mathbb{Z}[t] \to \mathbb{F}_p[t]$ to get $\nu_p(\mathrm{fg}) = 0$. As $\nu_p$ is a homomorphism, $\nu_p(\mathrm{f})\nu_p(\mathrm{g}) = 0$.

But $\mathbb{F}_p[t]$ is an integral domain so this implies either $\nu_p(\mathrm{f}) = 0$ or $\nu_p(\mathrm{g}) = 0$. Thus $p$ divides all the coefficients in either f or g, so at least one of f and g is not primitive.

Thus if f and g are both primitive, fg is also primitive. □

**Proposition 1.10 (Gauss's lemma)** *Let* $\mathrm{f} \in \mathbb{Z}[t]$. *Then* f *is reducible over* $\mathbb{Q}$ *if and only if* f *is properly reducible over* $\mathbb{Z}$.

## Proof

The 'if' direction is obvious. For 'only if', suppose that $\mathrm{f} \in \mathbb{Z}[t]$ is reducible over $\mathbb{Q}$, so $\mathrm{f} = \mathrm{gh}$ where $\mathrm{g}, \mathrm{h} \in \mathbb{Q}[t]$ both have degree less than $\partial\mathrm{f}$. Then $\mathrm{f} = c_\mathrm{g}\hat{\mathrm{g}}c_\mathrm{h}\hat{\mathrm{h}}$ where $\hat{\mathrm{g}}, \hat{\mathrm{h}} \in \mathbb{Z}[t]$ are primitive.

Thus $\mathrm{f} = c_\mathrm{g}c_\mathrm{h}\hat{\mathrm{g}}\hat{\mathrm{h}}$. By Proposition 1.9 $\hat{\mathrm{g}}\hat{\mathrm{h}}$ is primitive, so $c_\mathrm{f} = c_\mathrm{g}c_\mathrm{h}$.

But $\mathrm{f} \in \mathbb{Z}[t]$, so $c_\mathrm{f} \in \mathbb{Z}$. Thus $\mathrm{f} = (c_\mathrm{f}\hat{\mathrm{g}})(\hat{\mathrm{h}})$ where each of $c_\mathrm{f}\hat{\mathrm{g}}$ and $\hat{\mathrm{h}}$ is in $\mathbb{Z}[t]$ and has degree less than $\partial\mathrm{f}$. Hence f is properly reducible over $\mathbb{Z}$. □

### 1.3.3 Examples

(i) From Examples 1.1.2 (i), $\mathrm{f} = 5t^4 - 2t^3 + 2t^2 - 7t - 6$ has a zero $-\frac{3}{5}$, so $\mathrm{f} = \left(t + \frac{3}{5}\right)\mathrm{g}$ for some $\mathrm{g} \in \mathbb{Q}[t]$. Thus f =

$(5t+3)\frac{\mathrm{g}}{5}$, and Gauss's lemma guarantees that $\frac{\mathrm{g}}{5} \in \mathbb{Z}[t]$. That is, $\mathrm{f} = (5t+3)(t^3+at^2+bt-2)$ where $a, b \in \mathbb{Z}$.

(ii) Let $\mathrm{f} = t^4+2t^3+3t+2 \in \mathbb{Z}[t]$. Then $\mathrm{f}(-2) = -4$, $\mathrm{f}(-1) = -2$, $\mathrm{f}(1) = 8$, $\mathrm{f}(2) = 40$. Hence by the Rational Root theorem f has no zeros in $\mathbb{Q}$, so it has no factors of degree 1 in $\mathbb{Q}[t]$. However, it might have two quadratic factors. By Gauss's lemma we can assume the coefficients are integers, so the factors would have the form $(t^2+at+1)(t^2+bt+2)$ or $(t^2+at-1)(t^2+bt-2)$ where $a, b \in \mathbb{Z}$.

In the first case, $\mathrm{f} = t^4+(a+b)t^3+(ab+3)t^2+(2a+b)t+2$ so $a+b=2, ab+3=0, 2a+b=3$. These equations are inconsistent. The same is true in the second case. Hence f is irreducible over $\mathbb{Q}$.

**Proposition 1.11 (The localization principle)** *Let* $\mathrm{f} \in \mathbb{Z}[t]$ *and let* $p$ *be a prime which does not divide the leading coefficient of* f*.*

*If* $\nu_p(\mathrm{f})$ *is irreducible over* $\mathbb{F}_p$*, then* f *is irreducible over* $\mathbb{Q}$*.*

## Proof

If f is reducible over $\mathbb{Q}$ then by Gauss's lemma $\mathrm{f} = \mathrm{gh}$ where $\mathrm{g}, \mathrm{h} \in \mathbb{Z}[t]$ with $\partial\mathrm{g} < \partial\mathrm{f}$, $\partial\mathrm{h} < \partial\mathrm{f}$. Thus $\nu_p(\mathrm{f}) = \nu_p(\mathrm{gh}) = \nu_p(\mathrm{g})\nu_p(\mathrm{h})$, as $\nu_p$ is a homomorphism.

As $p$ does not divide the leading coefficient, $\nu_p(\mathrm{f})$ has the same degree as f while the degrees of $\nu_p(\mathrm{g})$ and $\nu_p(\mathrm{h})$ are both less than $\partial\mathrm{f}$. Hence $\nu_p(\mathrm{f})$ is reducible over $\mathbb{F}_p$.

It follows that if $\nu_p(\mathrm{f})$ is irreducible over $\mathbb{F}_p$ then f is irreducible over $\mathbb{Q}$. □

Note that if $\nu_p(\mathrm{f})$ is *reducible* over $\mathbb{F}_p$, this does *not* imply that f is reducible over $\mathbb{Q}$.

### 1.3.4 Examples

(i) Let $\mathrm{f} = t^3 + 5t + 16 \in \mathbb{Z}[t]$. Then $\nu_3(\mathrm{f}) = t^3 + 2t + 1 = \bar{\mathrm{f}}$, say. As this is cubic, it is reducible over $\mathbb{F}_3$ if and only if it has a zero in $\mathbb{F}_3$. Now $\bar{\mathrm{f}}(0) = 1$, $\bar{\mathrm{f}}(1) = 1$, $\bar{\mathrm{f}}(2) = 1$, so $\bar{\mathrm{f}}$ has no zeros in $\mathbb{F}_3$. Hence $\bar{\mathrm{f}}$ is irreducible over $\mathbb{F}_3$, so by the localization principle f is irreducible over $\mathbb{Q}$.

(ii) The only irreducible quadratic over $\mathbb{F}_2$ is $t^2+t+1$ so the only product of two irreducible quadratics over $\mathbb{F}_2$ is $(t^2+t+1)^2$, which equals $t^4 + t^2 + 1$ in $\mathbb{F}_2[t]$.

Let $\mathrm{f} = at^4 + bt^3 + ct^2 + dt + e \in \mathbb{Z}[t]$ where $a, b, c, d, e$ are *odd* integers.

$\nu_2(\mathrm{f}) = t^4 + t^3 + t^2 + t + 1$ has no zero in $\mathbb{F}_2$, so no factor of degree 1 in $\mathbb{F}_2[t]$.

Also $\nu_2(\mathrm{f}) \neq (t^2+t+1)^2$, so it has no irreducible quadratic factor in $\mathbb{F}_2[t]$. Thus $\nu_2(\mathrm{f})$ is irreducible over $\mathbb{F}_2$. Since $2 \not| \ a$, it follows by the localization principle that f is irreducible over $\mathbb{Q}$.

(iii) Let $\mathrm{f} = t^4 + 20t^3 - 15t^2 + 10t - 5 \in \mathbb{Z}[t]$.

$\nu_2(\mathrm{f}) = t^4 + t^2 + 1$, which is reducible over $\mathbb{F}_2$ as $(t^2 + t + 1)(t^2 + t + 1)$.

This gives no information about whether or not f is reducible over $\mathbb{Q}$. The next result will enable us to show that f is in fact irreducible over $\mathbb{Q}$.

**Proposition 1.12 (Eisenstein's irreducibility criterion)** *Let* $\mathrm{f} = \sum_{r=0}^{n} a_r t^r \in \mathbb{Z}[t]$. *If there exists a prime* $p$ *which di-*

*vides each of* $a_0, \ldots, a_{n-1}$ *but* not $a_n$*, and* $p^2$ *does not divide* $a_0$*, then* f *is irreducible over* $\mathbb{Q}$*.*

## Proof

Suppose, for a contradiction, that f and $p$ satisfy the given conditions and that f is reducible over $\mathbb{Q}$.

Then by Gauss's lemma f is properly reducible over $\mathbb{Z}$, i.e. f = gh where $\mathrm{g} = b_\ell t^\ell + \cdots + b_0 \in \mathbb{Z}[t]$, $\mathrm{h} = c_m t^m + \cdots + c_0 \in \mathbb{Z}[t]$ and $0 < \ell < n,\ 0 < m < n$.

$\nu_p(\mathrm{f}) = \nu_p(a_n)t^n$, as all other terms are congruent to 0 modulo $p$.

As $\nu_p$ is a homomorphism, $\nu_p(\mathrm{f}) = \nu_p(\mathrm{g})\nu_p(\mathrm{h})$. Now $t^n$ factors uniquely (up to unit multiples) into irreducibles over the field $\mathbb{F}_p$ as $t \times t \times \cdots \times t$, so we must have $\nu_p(\mathrm{g}) = \nu_p(b_\ell)t^\ell$ and $\nu_p(\mathrm{h}) = \nu_p(c_m)t^m$ for some integers $\ell, m$ as above.

Thus $p$ divides all except the leading coefficient in each of g and h. In particular $p \mid b_0, p \mid c_0$ and so $p^2 \mid b_0 c_0$. But $b_0 c_0 = a_0$ and, by assumption, $p^2 \nmid a_0$.

We have a contradiction, so f is irreducible over $\mathbb{Q}$. □

**Proposition 1.13** $a_0 + a_1 t + \cdots + a_n t^n$ *is reducible over* $\mathbb{Q}$ *if and only if*
$a_0 t^n + a_1 t^{n-1} + \cdots + a_n$ *is reducible over* $\mathbb{Q}$*.*

## Proof

Let $\mathrm{f} = \sum_{r=0}^{n} a_r t^r$ and let $\mathrm{g} = \sum_{r=0}^{n} a_r t^{n-r}$. In $\mathbb{Q}(t)$, $\dfrac{\mathrm{f}}{t^n} = \sum_{r=0}^{n} a_r t^{r-n}$ $= \mathrm{g}(u)$ where $u = \dfrac{1}{t}$.

Suppose g is reducible over $\mathbb{Q}$ as hk where $\partial \mathrm{h} = \ell > 0, \partial \mathrm{k} = m > 0$, $\ell + m = n$.

Then $\mathrm{f}(t) = t^n \mathrm{g}(u) = t^n \mathrm{h}(u)\mathrm{k}(u) = t^\ell \mathrm{h}(u) t^m \mathrm{k}(u)$. But each of $t^\ell \mathrm{h}(u)$ and $t^m \mathrm{k}(u)$ is a polynomial over $\mathbb{Q}$ of degree less than $n$ in $t$, so $\mathrm{f}(t)$ is reducible over $\mathbb{Q}$.

Swapping the rôles of f and g shows that if f is reducible over $\mathbb{Q}$ then so is g. □

**Proposition 1.14** *For any $a \in \mathbb{Q}$,* f *is reducible over $\mathbb{Q}$ if and only if* $\mathrm{f}(t+a)$ *is reducible over $\mathbb{Q}$.*

**Proof** Suppose $\mathrm{f}(t+a)$ is reducible over $\mathbb{Q}$ in the form $\mathrm{f}(t+a) = \mathrm{g}(t)\mathrm{h}(t)$.
Then $\mathrm{f}(t) = \mathrm{g}(t-a)\mathrm{h}(t-a)$, so $\mathrm{f}(t)$ is reducible over $\mathbb{Q}$.

Conversely, suppose $\mathrm{f}(t)$ is reducible over $\mathbb{Q}$ in the form $\mathrm{f}(t) = \mathrm{g}(t)\mathrm{h}(t)$.
Then $\mathrm{f}(t+a) = \mathrm{g}(t+a)\mathrm{h}(t+a)$ so $\mathrm{f}(t+a)$ is reducible over $\mathbb{Q}$. □

Proposition 1.14 requires the substitution to be linear. If $\mathrm{f}(t^2)$ is reducible as $\mathrm{g}(t)\mathrm{h}(t)$, it does *not* follow that f is reducible, as $\mathrm{g}(\sqrt{t})$, $\mathrm{h}(\sqrt{t})$ may not be polynomials in $t$.

### 1.3.5 Examples

(i) Let $\mathrm{f} = t^4 + 6t^3 - 4t + 10$. By EIC with $p = 2$, f is irreducible over $\mathbb{Q}$.

(ii) To construct an irreducible polynomial of any degree over $\mathbb{Q}$: choose a prime, such as 3, and make the coefficients satisfy Eisenstein's Irreducibility Criterion. For instance, $4t^6 + 3t^5 - 6t^4 + 9t^3 - 12t^2 + 3t + 15$ is irreducible over $\mathbb{Q}$.

(iii) Let $\mathrm{f} = \frac{1}{2}t^3 + \frac{5}{2}t^2 - \frac{5}{4}t + \frac{5}{4}$. Then $4\mathrm{f} = 2t^3 + 10t^2 - 5t + 5$, which is irreducible over $\mathbb{Q}$ by EIC with $p = 5$. Thus f is irreducible over $\mathbb{Q}$.

(iv) $\mathrm{f} = 14t^3 - 49t + 5$ is irreducible over $\mathbb{Q}$ by Proposition 1.13 and EIC with $p = 7$.

(v) Let $\mathrm{f} = t^3 - 6t^2 + 15t - 8$. Then $\mathrm{f} = (t-2)^3 + 3(t-2) + 6$ $= \mathrm{g}(t-2)$, say, where $\mathrm{g} = t^3 + 3t + 6$.

By EIC with $p = 3$, g is irreducible over $\mathbb{Q}$. Hence by Proposition 1.14, so is f.

**Definition 1.9** *For any $n \in \mathbb{N}$, the $n$th* **cyclotomic polynomial** $\Phi_n$ *is* $\prod_{i=1}^{m}(t-\varepsilon_i)$ *where $\varepsilon_1, \ldots, \varepsilon_m$ are all the* primitive *$n$th roots of unity in $\mathbb{C}$.*

Suppose $p$ is prime. Then the $p$th cyclotomic polynomial has a very simple form. The zeros of $t^p - 1$ are the $p$th roots of unity. All these, except 1, are primitive $p$th roots of 1. Now $t^p - 1 = (t-1)(t^{p-1} + t^{p-2} + \cdots + t + 1)$, so $\Phi_p = t^{p-1} + t^{p-2} + \cdots + t + 1$.

We cannot apply EIC to $\Phi_p$ directly, but we can use Proposition 1.14 as follows:

$t^p - 1 = (t-1)\Phi_p(t)$, so $t\Phi_p(t+1) = (t+1)^p - 1$

$$= \sum_{r=0}^{p} \binom{p}{r} t^r - 1 = \sum_{r=1}^{p} \binom{p}{r} t^r, \text{ where } \binom{p}{r} = \frac{p!}{r!(p-r)!} \in \mathbb{N}.$$

Thus $\Phi_p(t+1) = \sum_{r=1}^{p} \binom{p}{r} t^{r-1}$

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

Now $p! = r!(p-r)!\binom{p}{r}$. Certainly $p \mid p!$ If $1 \leq r \leq p-1$ then $p$ does not divide any factor of $r!$ or $(p-r)!$ since all those factors are less than $p$, so $p$ must divide $\binom{p}{r}$. Also $p^2$ does not divide $p$ and $p$ does not divide 1.

Thus by EIC, $\Phi_p(t+1)$ is irreducible over $\mathbb{Q}$ and hence so is $\Phi_p$. This proves:

**Proposition 1.15** *For each prime $p$, the cyclotomic polynomial $\Phi_p = \sum_{r=0}^{p-1} t^r$ is irreducible over $\mathbb{Q}$.*

When $n$ is *not* prime, $\Phi_n$ does *not* equal $1 + t + \cdots + t^{n-1}$. For example, the zeros of $\Phi_4$ are the primitive 4th roots of 1, namely i and $-$i, so $\Phi_4 = (t - \mathrm{i})(t + \mathrm{i}) = t^2 + 1$. However, it can be shown that $\Phi_n$ is in $\mathbb{Q}[t]$, and is irreducible over $\mathbb{Q}$, for all $n \in \mathbb{N}$.

## Exercises 1.3

1. List all the cubic polynomials over $\mathbb{F}_2$ and all the quadratics over $\mathbb{F}_3$. Determine which of these are irreducible over their coefficient field.

2. Find the content of each of the polynomials

   (a) $28t^2 - 98t + 56 \in \mathbb{Z}[t]$, (b) $\frac{3}{8}t^3 - \frac{15}{16}t^2 + \frac{3}{2}t - \frac{9}{4} \in \mathbb{Q}[t]$.

   Express each as the product of its content and a primitive polynomial in $\mathbb{Z}[t]$.

3. Determine whether or not the following polynomials are reducible over $\mathbb{Q}$:

   (a) $t^3 - 4t + 1$, (b) $t^4 + t + 1$, (c) $t^4 + t^2 + 1$,
   (d) $t^3 + 6t^2 + 4t + 2$,
   (e) $2t^5 - 12t^3 + 15t^2 + 6$, (f) $t^3 + 85t^2 + 28t + 135$,
   (g) $5t^6 + 25t^4 - 15t^2 + 1$.

4. Let $\mathrm{f} = t^6 + t^3 + 1 \in \mathbb{Q}[t]$. By expanding $\mathrm{f}(t+1)$, show that f is irreducible over $\mathbb{Q}$. Find all the zeros of f in $\mathbb{C}$, in the form $\mathrm{e}^{k\pi\mathrm{i}}$.

5. Let $\mathrm{f} = t^4 + rt + p$ where $r \in \mathbb{Z}$ and $p$ is prime. Suppose f has no rational zeros. Show that f is irreducible over $\mathbb{Q}$.

6. Let $\mathrm{f} = t^p + (p-1) \in \mathbb{Q}[t]$. By expanding $\mathrm{f}(t+1)$, show that f is irreducible over $\mathbb{Q}$ for every prime integer $p$.

7. Use Eisenstein's criterion to show that if $a \in \mathbb{Z}$ is not an integer multiple of a perfect square then $t^n - a$ is irreducible over $\mathbb{Q}$ for all positive integers $n$.

   If $a$ *is* an integer multiple of a perfect square, is $t^n - a$ always reducible over $\mathbb{Q}$?

8. Find the cyclotomic polynomials $\Phi_n$ for $n = 1, 2, 3, 4, 5, 6, 7, 8$.

9. Let $K$ be a field. Suppose f and g are non-zero polynomials in $K[t]$ such that
   $\mathrm{f} = \mathrm{pg}$ for some polynomial p. Show that $\mathrm{p} \in K[t]$.

   (Hint: use the fact that $\mathrm{f} = \mathrm{qg} + \mathrm{r}$ where $\mathrm{q}, \mathrm{r} \in K[t]$ and $\partial \mathrm{r} < \partial \mathrm{g}$.)

10. Let f be a monic quartic polynomial in $\mathbb{Z}[t]$ which has no rational zeros. Suppose there is a prime $p$ such that $\nu_p(\mathrm{f})$ has exactly one zero, of multiplicity 1, in $\mathbb{F}_p$.

    Prove that f is irreducible over $\mathbb{Q}$. Use this result with $p = 3$ to show that $t^4 + 10t + 1$ is irreducible over $\mathbb{Q}$.

## 1.4 The minimal polynomial

**Definition 1.10** *Let $K$ and $L$ be fields such that $K \subset L$.*

*An element $\alpha \in L$ is* **algebraic** *over $K$ if there exists a non-zero polynomial $\mathrm{f} \in K[t]$ such that $\mathrm{f}(\alpha) = 0$. Otherwise, $\alpha$ is* **transcendental** *over $K$.*

For example, i and $\sqrt{2}$ are algebraic over $\mathbb{Q}$, but $\pi$ and e are transcendental over $\mathbb{Q}$.

Any expression obtained from elements of a field $K$ by field operations and roots is algebraic over $K$, e.g. let $a = \sqrt{4 + \sqrt[3]{7 - \sqrt[5]{2}}}$. Then $(7 - (a^2 - 4)^3)^5 - 2 = 0$, so $a$ is algebraic over $\mathbb{Q}$.

**Proposition 1.16** *Let $\alpha$ be algebraic over a field $K$. Let $\mu$ be a monic polynomial in $K[t]$, of lowest degree among those which have $\alpha$ as a zero.*

*Then $\mu$ is irreducible over $K$, and unique. If* $\mathrm{f}(\alpha) = 0$ *for some* $\mathrm{f} \in K[t]$ *then* $\mu \mid \mathrm{f}$.

**Proof**

Let $\mu$ be a monic polynomial in $K[t]$, of lowest degree such that $\mu(\alpha) = 0$.

If $\mu$ is reducible over $K$ then $\mu = \mathrm{gh}$ for some monic $\mathrm{g}, \mathrm{h} \in K[t]$ with lower degree than that of $\mu$. But then $\mathrm{g}(\alpha)\mathrm{h}(\alpha) = \mu(\alpha) = 0$ so either $\mathrm{g}(\alpha) = 0$ or $\mathrm{h}(\alpha) = 0$, contradicting the minimality of $\partial\mu$ with this property. Thus $\mu$ is irreducible over $K$.

For any $\mathrm{f} \in K[t]$ there exist $\mathrm{q}, \mathrm{r} \in K[t]$ such that $\mathrm{f} = \mathrm{q}\mu + \mathrm{r}$ where $\partial\mathrm{r} < \partial\mu$.

Thus $\mathrm{f}(\alpha) = \mathrm{q}(\alpha)\mu(\alpha) + \mathrm{r}(\alpha)$. Now $\mu(\alpha) = 0$, so $\mathrm{f}(\alpha) = \mathrm{r}(\alpha)$.

Suppose $\mathrm{f}(\alpha) = 0$, so $\mathrm{r}(\alpha) = 0$. If $\mathrm{r} \neq 0$ then r divided by its leading coefficient is a monic polynomial of lower degree than $\mu$ with $\alpha$ as a zero. This again contradicts the minimality of $\partial\mu$. Hence r is the zero polynomial, so $\mathrm{f} = \mathrm{q}\mu$ and thus $\mu \mid \mathrm{f}$.

Suppose $\nu$ is also monic of lowest degree with $\nu(\alpha) = 0$. Then by the above, $\mu \mid \nu$ and $\nu \mid \mu$. Thus $\nu = \mu$, i.e. $\mu$ is unique with this property. □

**Definition 1.11** *Let $\alpha$ be algebraic over a field $K$. The* **minimal polynomial** *(or* the minimum polynomial *or* the

irreducible polynomial) *of $\alpha$ over $K$ is the lowest-degree monic polynomial $\mu \in K[t]$ such that $\mu(\alpha) = 0$. We say $\alpha$ is algebraic of* **degree** *$\partial\mu$ over $K$. The* **conjugates** *of $\alpha$ over $K$ are the other zeros of $\mu$.*

Clearly every irreducible monic polynomial in $K[t]$ is the minimal polynomial over $K$ of each of its zeros. If we can find an irreducible monic polynomial in $K[t]$ with $\alpha$ as a zero, this must be the minimal polynomial of $\alpha$ over $K$.

Note that the minimal polynomial depends on the field. Suppose $K, M, L$ are fields with $K \subset M \subset L$, and $\alpha \in L$ has minimal polynomial $\mu$ over $K$. Then $\mu$ can be regarded as a polynomial over $M$, so the minimal polynomial of $\alpha$ over $M$ is either the same as $\mu$ or it divides $\mu$ in $M[t]$.

### 1.4.1 Examples

(i) $t^3 - 2$ is irreducible over $\mathbb{Q}$, so it is the minimal polynomial of $2^{1/3}$ over $\mathbb{Q}$. $2^{1/3}$ is thus algebraic of degree 3 over $\mathbb{Q}$. The conjugates of $2^{1/3}$ are $2^{1/3}\omega$ and $2^{1/3}\omega^2$.

The minimal polynomial of $2^{1/3}$ over $\mathbb{R}$ is $t - 2^{1/3}$, which divides $t^3 - 2$ in $\mathbb{R}[t]$.

(ii) The minimal polynomial of $\omega = \mathrm{e}^{2\pi\mathrm{i}/3}$ over $\mathbb{Q}$ is $t^2 + t + 1$. The conjugate of $\omega$ is $\omega^2$.

The minimal polynomial of $\omega$ over $\mathbb{R}$ must divide $t^2 + t + 1$ in $\mathbb{R}[t]$. But $t^2 + t + 1$ has no real zeros, so it is irreducible over $\mathbb{R}$ and is thus also the minimal polynomial of $\omega$ over $\mathbb{R}$. As $\omega \in \mathbb{C}$, the minimal polynomial of $\omega$ over $\mathbb{C}$ is $t - \omega$.

(iii) Let $\alpha = \sqrt{2} + \sqrt{3}$. Then $\alpha^2 = 5 + 2\sqrt{6}$, so $(\alpha^2 - 5)^2 = 24$, so $\alpha^4 - 10\alpha^2 + 1 = 0$.

Thus $\alpha$ is a zero of $t^4 - 10t^2 + 1$. This has no rational zeros, and we can check that it has no quadratic factors in $\mathbb{Q}[t]$, so it is irreducible and hence is the minimal polynomial of $\alpha$ over $\mathbb{Q}$. $\alpha$ is algebraic of degree 4 over $\mathbb{Q}$.

(iv) Let $\beta = 2^{1/3} - 2^{2/3}$. Then $\beta^3 = 6(2^{2/3}) - 6(2^{1/3}) - 2 = -6\beta - 2$. Thus $\beta^3 + 6\beta + 2 = 0$. Now $t^3 + 6t + 2$ is irreducible over $\mathbb{Q}$ (by EIC with $p = 2$) and monic, so it is the minimal polynomial of $\beta$ over $\mathbb{Q}$. Hence $\beta$ is algebraic of degree 3 over $\mathbb{Q}$.

(v) For any $n \in \mathbb{N}$, the cyclotomic polynomial $\Phi_n$ is the minimal polynomial over $\mathbb{Q}$ of any primitive $n$th root of unity; in particular, of $\mathrm{e}^{2\pi \mathrm{i}/n}$.

**Definition 1.12** *Let $K$ be a field. A polynomial* f $\in K[t]$ *is* **separable** *over $K$ if no irreducible factor of* f *in $K[t]$ has a repeated zero.* f *is* **inseparable** *over $K$ otherwise.*

It follows from this definition that a polynomial which is irreducible over $K$ is separable over $K$ if and only if it has no repeated zeros.

**Proposition 1.17** *Let $K$ be a field of characteristic zero or a finite field. Then every irreducible polynomial in $K[t]$ is separable over $K$.*

**Proof** in the case $\chi(K) = 0$:

Let $\mathrm{f} = \sum_{r=0}^{n} a_r t^r \in K[t]$ be irreducible over $K$. By definition $\partial \mathrm{f} \geq 1$, so $\mathrm{Df} \neq 0$.

Suppose f has a repeated zero $\alpha$. Then by Proposition 1.1, $\alpha$ is also a zero of Df.

The minimal polynomial of $\alpha$ over $K$ is $\mu = \dfrac{1}{a_n}\mathrm{f}$.

By Proposition 1.16, $\mu \mid \mathrm{Df}$. As $\mathrm{Df} \neq 0$, we must have $\partial\mu \leq \partial(\mathrm{Df})$.

But $\partial(\mathrm{Df}) < \partial\mathrm{f} = \partial\mu$. This contradiction shows that f has no repeated zeros, so f is separable over $K$. □

A different proof is needed for finite fields. We conclude that over all fields that we are concerned with, it may be assumed that every irreducible polynomial is separable, i.e. it has no repeated zeros. To find an inseparable irreducible polynomial, it is necessary to consider an infinite field of prime characteristic.

## Exercises 1.4

1. Show that $a + b\sqrt{c}$ is algebraic over $\mathbb{Q}$ for all $a, b, c \in \mathbb{Q}$.

2. Find the minimal polynomial over $\mathbb{Q}$ of each of the following:

   (a) $\sqrt{21}$, (b) $2^{1/3} + 1$, (c) $3^{1/3} + 3^{2/3}$, (d) $\sqrt{6 + \sqrt{6}}$, (e) $\mathrm{e}^{2\pi\mathrm{i}/5}$, (f) $\mathrm{e}^{\pi\mathrm{i}/4}$.

   In each case state the value of $m$ such that the given number is algebraic of degree $m$ over $\mathbb{Q}$. Find all the conjugates of each number over $\mathbb{Q}$.

3. Let $p$ be prime. Find the minimal polynomial of $\sqrt{p - \sqrt{p}}$ over $\mathbb{Q}$.

4. Let $\alpha$ be a cube root of $1 + \mathrm{i} \in \mathbb{C}$. Find the minimal polynomials of $\alpha$ over $\mathbb{Q}$ and over $\mathbb{C}$.

5. Let $z = a + b\mathrm{i}$ where $a, b \in \mathbb{R}$, $b \neq 0$. Find the minimal polynomial of $z$ over $\mathbb{R}$.

6. $2^{1/4}$ denotes the positive real 4th root of 2. Find the minimal polynomial of $2^{1/4}$i over (a) $\mathbb{Q}$, (b) $\mathbb{Q}(\sqrt{2})$, (c) $\mathbb{R}$, (d) $\mathbb{C}$.

   Would it make sense to ask for the minimal polynomial over $\mathbb{Z}$?

7. Let $m, n \in \mathbb{Q}$ such that $m > n > 0$ and suppose $\mu = t^4 - 2(m+n)t^2 + (m-n)^2$ is irreducible over $\mathbb{Q}$. Find expressions for all the real or complex numbers which have minimal polynomial $\mu$, showing that one of them is $\sqrt{m} + \sqrt{n}$.

8. Let $K$ be a field of characteristic 0. Suppose $\alpha$ is the only common zero of two distinct polynomials f and g in $K[t]$. Show that $\alpha \in K$ and that f and g are reducible over $K$.

9. Find the lowest degree monic polynomial in $\mathbb{Q}[t]$ which has $2^{1/3}$ as a repeated zero. Is this polynomial separable over $\mathbb{Q}$? Is it reducible over $\mathbb{Q}$?

10. Find Df when $\mathrm{f} = t^6 + 2t^3 + 1 \in \mathbb{F}_3[t]$. Hence explain where the proof of Proposition 1.17 breaks down if the field $K$ has characteristic $p \neq 0$.