Galois Theory

Sean Prendiville

The majority of the material that follows is based on notes of Trevor Wooley and Andrey Lazarev.

1. Introduction

**Definition** (Algebraic over \( \mathbb{Q} \)). We say \( \alpha \in \mathbb{C} \) is algebraic over \( \mathbb{Q} \) if there exists a non-zero polynomial \( f \) with rational coefficients such that \( f(\alpha) = 0 \).

The numbers \( 2^{1/2} \) and \( 3^{1/3} \) are algebraic over \( \mathbb{Q} \) since they satisfy the equations \( t^2 - 2 = 0 \) and \( t^3 - 3 = 0 \), respectively.

**Question.** Is \( \alpha = 2^{1/2} + 3^{1/3} \) algebraic over \( \mathbb{Q} \)?

It is actually quite hard to think of a non-zero polynomial \( f \) with rational coefficients for which \( f(\alpha) = 0 \). Instead we argue more indirectly. Using the binomial theorem, a little computation shows that for any non-negative integer \( k \) the \( k \)-th power \( \alpha^k \) lies in the \( \mathbb{Q} \)-linear span

\[
L = \text{span}_\mathbb{Q}\{ 1, 2^{1/2}, 3^{1/3}, 2^{1/2}3^{1/3}, 2^{1/2}3^{1/3} \}
\]

Since \( L \) is a \( \mathbb{Q} \)-vector space with a spanning set of size six, we have \( \dim_{\mathbb{Q}} L \leq 6 \). Therefore the seven elements \( 1, \alpha, \alpha^2, \ldots, \alpha^6 \in L \) cannot be linearly independent. In particular, there exist rationals \( a_0, a_1, \ldots, a_6 \) not all zero such that

\[
a_0 + a_1 \alpha + \cdots + a_6 \alpha^6 = 0.
\]

So \( \alpha \) is indeed algebraic over \( \mathbb{Q} \).

Notice that the above argument did not construct an explicit polynomial of which \( \alpha \) is a root, instead we exploited the algebraic structure of the vector space \( L \), and the restrictions imposed by this structure yield the existence of the required polynomial. It turns out that not only is \( L \) a vector space, but it is also a field\(^{1} \) so has much more algebraic structure to exploit. In fact \( L \) coincides with the smallest\(^2 \) subfield of \( \mathbb{C} \) containing \( \alpha \) and \( \mathbb{Q} \), a subfield we denote\(^3 \) by \( \mathbb{Q}(\alpha) \). One could say we have extended the field \( \mathbb{Q} \) by adjoining \( \alpha \).

Studying such field extensions turns out to be very useful, particularly for proving impossibility results, of which there are a number in this course. For example, we show in \[ \Box \] that if it is possible to construct a point \((x_1, x_2)\) in the plane using ruler and compass, then the field \( L = \mathbb{Q}(x_1) \), obtained from \( \mathbb{Q} \) by adjoining \( x_1 \), satisfies \( \dim_{\mathbb{Q}} L = 2^n \) for some non-negative integer \( n \). Yet we also show that if angle trisection is possible using ruler and compass, then there is a constructible point \((x_1, x_2)\) with \( \dim_{\mathbb{Q}}(x_1) = 3 \). Hence angle trisection is not possible using only ruler and compass.

Finally, another good reason for studying field extensions \( \mathbb{Q} \subset L \) is that they allow us to define the Galois group of a polynomial \( f \in \mathbb{Q}[t] \). We eventually show that one can express the roots of \( f \) in terms of the operations \(+, -, \times, \div\) and \( \sqrt{\cdot} \) applied to the coefficients of \( f \) if and only if the Galois group of \( f \) isn’t ‘too non-abelian’. It turns out that \( f = t^5 - 6t + 3 \) has

---

Date: October 8, 2014.

Comments/corrections gratefully received at sean.prendiville@bris.ac.uk

1It is an instructive exercise to try and prove this. The hard part is showing that \( \beta \in L \setminus \{0\} \implies \beta^{-1} \in L \). (Hint: As above, show that the powers of \( \beta \) lie in \( L \), and hence \( \beta \) is algebraic over \( \mathbb{Q} \), then multiply this polynomial expression in \( \beta \) through by an appropriate power of \( \beta^{-1} \).)

2We give more formal definitions later.

3Exercise: Show that any subfield of \( \mathbb{C} \) not equal to the trivial field \{0\} must contain \( \mathbb{Q} \).
Galois group $S_5$, which is too non-abelian. Hence there is no general formula for the roots of a quintic in terms of radicals (unlike quadratics, cubics and quartics).

2. Review: Polynomial Rings

To re-familiarise with the necessary background material, students should re-read their notes from Algebra 2 on rings, integral domains and ideals. Better still, read the first three chapters of [Gar86]. The essential background is contained in pp.2–4 of Andrey Lazarev’s notes [Laz00], but for a more in-depth online reference see pp.40–74 of the notes of Teruyoshi Yoshida [Yos12] which contain everything we need and much more besides.

Definition (Polynomial ring over $R$). Let $R$ be a ring. A polynomial over $R$ in the indeterminate $t$ is an expression of the form

$$
\sum_i a_i t^i = a_0 + a_1 t + a_2 t^2 + \ldots
$$

where $a_i \in R$ and the set of $i$ for which $a_i \neq 0$ is finite. We call $a_i$ the coefficient of $t^i$. The set of all polynomials over $R$ in the indeterminate $t$ is denoted $R[t]$. Given two such polynomials $f = \sum_i a_i t^i$ and $g = \sum_j b_j t^j$ we define their sum by

$$
\sum_i (a_i + b_i) t^i.
$$

And their product by

$$
\sum_i \left( \sum_{j+k=i} a_j b_k \right) t^i.
$$

Example. Let $R = \mathbb{Z}/12\mathbb{Z}$. Set $f = 4t + 8$ and $g = 3t^2 + 9$. Then $f + g = 3t^2 + 4t + 5$ and $fg = 0$.

Definition (Degree, leading coefficient, monic). Given a non-zero polynomial $f = \sum_i a_i t^i$ there exists a maximal non-negative integer $n$ with $a_n \neq 0$. We call $n$ the degree of $f$, written $\deg(f)$, and call $a_n$ the leading coefficient of $f$. By convention, the degree of the zero polynomial is $-\infty$. If the leading coefficient of $f$ equals one, then we say that $f$ is monic.

Notice that for any ring $R$ and any $f, g \in R[t]$ we have the inequality

$$
\deg(f + g) \leq \max\{\deg(f), \deg(g)\}
$$

(2.3)

Defining $\deg(0) = -\infty$ at first appears curious, however it ensures the validity of the identity $\deg(fg) = \deg(f) + \deg(g)$, even when $fg = 0$, provided that $R$ is an integral domain. That the formula can fail otherwise is demonstrated by the above example.

Lemma 1 (Degree product formula for polynomials over domains). Suppose that $R$ is an integral domain. Then $R[t]$ is also an integral domain. Moreover, for any $f, g \in R[t]$ we have the identity

$$
\deg(fg) = \deg(f) + \deg(g).
$$

(2.4)

[The idea: The leading coefficient of $fg$ is the product of the leading coefficients of $f$ and $g$.]

Proof. If either $f$ or $g$ are zero, then (2.4) follows from the identities $\deg(f) + (-\infty) = (-\infty) + \deg(g) = -\infty$. Let us therefore suppose that $f = \sum_i a_i t^i$ and $g = \sum_j b_j t^j$ are non-zero of degrees $m$ and $n$ respectively. If $i$ and $j$ are non-negative integers with $i + j \geq m + n$ then either $i \geq m$ or $j \geq n$. Hence the only possible non-zero product of the form $a_i b_j$ with $i + j \geq m + n$ is that for which $i = m$ and $j = n$. In this case $a_m b_n \neq 0$ since $R$ is an integral domain. It follows that $fg$ has degree $m + n$ with leading coefficient $a_m b_n$. □

We mainly study $R[t]$ when $R = K$ is a field, so certainly an integral domain.

http://www.maths.lancs.ac.uk/~lazarev/galoislecturenotes.pdf

Throughout the remainder of these notes $K$ always denotes a field.

**Definition** (Unit). An element $a$ of a ring $R$ is a unit if it has a multiplicative inverse, i.e. there exists $b \in R$ with $ab = 1$. We write $R^\times$ for the set of units in $R$. This set forms a group under multiplication.

**Examples.**
- For a field $K$, we have $K^\times = K \setminus \{0\}$.
- If $R$ is an integral domain, then by the product degree formula we have $(R[t])^\times = R^\times$ (exercise).

There is a useful analogy in number theory between the rings $\mathbb{Z}$ and $K[t]$. This is made more concrete by the rough correspondence between the (logarithm of the) absolute value function on the integers and the degree function on $K[t]$. Using this analogy, many results in elementary number theory carry over into $K[t]$ without much modification. Our first such result is the polynomial division algorithm, familiar from AS-level maths, albeit over an arbitrary field, and with a proof showing that the algorithm does indeed terminate.

**Theorem 2** (Division algorithm). Let $f, g \in K[t]$ with $g$ non-zero. Then there exist unique polynomials $q$ and $r$ in $K[t]$ satisfying

$$f = gq + r$$

and

$$\deg(r) < \deg(g).$$

(2.5)

[The idea: Cancel the leading term of $f$ by subtracting $g$ times an appropriately scaled power of $t$. This decreases the degree of $f$. Iterate until we obtain a polynomial of degree less than $g$.]

**Proof.** Let $m = \deg(f)$ and $n = \deg(g)$. We proceed by induction on $m = \deg(f)$. If $m < n$, then we may take $q = 0$ and $r = f$. Therefore suppose that $m \geq n$. Let $a$ denote the leading coefficient of $f$ and $b$ the leading coefficient of $g$. Then the polynomial $f_1 = f - ab^{-1}t^m - n g$ is an element of $K[t]$ of degree strictly less than $m$. Hence by induction there exist $q_1$ and $r_1$ such that $f_1 = gq_1 + r_1$ with $\deg(r_1) < \deg(g)$. Substituting our definition for $q_1$ into this identity and re-arranging we have $f = gq + r$ where $q = ab^{-1}t^m - n + q_1$ and $r = r_1$.

Next let us establish the uniqueness of $q$ and $r$. Suppose that $gq + r = gq' + r'$ for polynomials $q, q', r, r' \in K[t]$ with $\deg(r) < \deg(g)$ and $\deg(r') < \deg(g)$. First suppose that $q - q'$ is non-zero. Then by Lemma[1] the polynomial $(q - q')g$ has degree at least $\deg(g)$. Yet by (2.3), the polynomial $r' - r$ has degree strictly less than $\deg(g)$. Since these two polynomials coincide, we have a contradiction. Therefore $q = q'$, and subtraction yields that $r = r'$.

The utility of the division algorithm is that, just as in the case of $\mathbb{Z}$, it allows us to establish a Euclidean algorithm for finding highest common factors. Let us first make the appropriate definitions.

**Definition** (Divides, common factor, highest common factor, relatively prime, associate). Let $f, g \in K[t]$.

- We say that $f$ divides $g$, and write $f|g$, if there exists a polynomial $h \in K[t]$ such that $g = fh$. Otherwise we write $f \not{|} g$.
- A polynomial $d \in K[t]$ is a common factor of $f$ and $g$ if it divides both $f$ and $g$.
- A polynomial $h \in K[t]$ is a highest common factor of $f$ and $g$ if it is a common factor divisible by every other common factor of $f$ and $g$.
- We say $f$ and $g$ are relatively prime if a highest common factor of $f$ and $g$ is 1.
- We say $f$ and $g$ are associate if they divide one another. Equivalently, $f = \lambda g$ for some $\lambda \in K^\times$. Notice that if $f$ and $g$ are not both zero then all their highest common factors are associate.

**Theorem 3** (Euclidean algorithm for polynomials). Let \( f, g \in K[t] \) with \( g \) non-zero. Write \( r_0 = f, r_1 = g \). Given \( r_{i-1} \) and \( r_i \) with \( r_i \neq 0 \), define \( q_{i+1} \) and \( r_{i+1} \) via the relation

\[
r_{i-1} = r_i q_{i+1} + r_{i+1} \quad \text{with} \quad \deg(r_{i+1}) < \deg(r_i).
\]

Then for some positive integer \( I \) we have \( r_{I+1} = 0 \), in which case a highest common factor of \( f \) and \( g \) is \( r_I \).

[The idea: Each iteration reduces \( \deg(r_i) \) and this number cannot be non-negative indefinitely.]

**Proof.** Suppose that \( r_{i+1} \neq 0 \) for all \( i \geq 2 \). Since \( \deg(r_{i+1}) \leq \deg(r_i) - 1 \leq \cdots \leq \deg(r_1) - i = \deg(g) - i \), we have a contradiction when \( i > \deg(g) \). Hence such an \( I \) exists.

Using (2.6) we see that for \( 1 \leq i \leq I \), a highest common factor of \( r_i \) and \( r_{i+1} \) is also a highest common factor of \( r_{i-1} \) and \( r_i \). Since \( r_I \) is a highest common factor of \( r_I \) and \( r_{I+1} \) (the latter is 0), we can work back through each of the equations (2.6) to deduce that \( r_I \) is a highest common factor of \( r_0 = f \) and \( r_1 = g \). \( \square \)

**Example.** We find a highest common factor of \( t^5 - 3t^2 + 2 \) and \( t^2 - 2t + 1 \) in \( \mathbb{Q}[t] \). Using the division algorithm, we have

\[
t^5 - 3t^2 + 2 = (t^3 + 2t^2 + 4t + 4)(t^2 - 2t + 1) + (2t - 2),
\]

\[
t^2 - 2t + 1 = \left( \frac{1}{2}t - \frac{1}{2} \right)(2t - 1).
\]

Therefore \( 2t - 2 \) is a highest common factor of \( t^5 - 3t^2 + 2 \) and \( t^2 - 2t + 1 \), or equivalently, \( t - 1 \) is a highest common factor.

**Theorem 4** (Bézout’s identity for polynomials). Let \( h \) be a highest common factor of \( f \) and \( g \) in \( K[t] \). Then there exist polynomials \( a, b \in K[t] \) such that

\[
af + bg = h.
\]

[The idea: Work back up through the Euclidean algorithm.]

**Proof.** If \( g = 0 \), then \( h = \lambda f \) for some \( \lambda \in K^\times \), in which case we can take \( a = \lambda \) and \( b = 0 \). If \( g \mid f \), then \( h = \lambda g \) for some \( \lambda \in K^\times \), in which case we can take \( a = 0 \) and \( b = \lambda \). Let us therefore suppose that \( g \nmid f \) and \( g \neq 0 \). We perform the Euclidean algorithm as in Theorem 3 (whose notation we adopt), initialising with \( r_0 = f \) and \( r_1 = g \). Since \( g \mid f \), the algorithm terminates with \( r_{I+1} = 0 \) for some \( I \geq 2 \) and with \( r_I \) a highest common factor of \( f \) and \( g \). The identity \( r_{i+2} = r_{i+1}q_i + r_i \), valid for all \( 2 \leq i \leq I + 1 \), shows that each \( r_i \) is a \( K[t] \)-linear combination of \( r_{i-1} \) and \( r_{i-2} \). In particular \( r_I \in \text{span}_{K[t]} \{ r_{I-1}, r_{I-2} \} \) and we have the chain of inclusions

\[
\text{span}_{K[t]} \{ r_{I-1}, r_{I-2} \} \subset \text{span}_{K[t]} \{ r_{I-2}, r_{I-3} \} \subset \cdots \subset \text{span}_{K[t]} \{ r_1, r_0 \}.
\]

Hence there exist \( a, b \in K[t] \) satisfying \( af + bg = r_1 \). Since \( r_1 \) and \( h \) are associate, we can multiply this equation through by a constant to obtain (2.7). \( \square \)

**Definition** (Irreducible polynomial). Let \( R \) be a ring. An **irreducible** polynomial in \( R[t] \) is a non-constant polynomial which cannot be written as a product of two polynomials over \( R \) of smaller degree.

**Examples.**

- All polynomials of degree 1 are irreducible.
- The polynomial \( t^2 + 1 \) is irreducible over \( \mathbb{R} \), but reducible over \( \mathbb{C} \).
- If \( f \in R[t] \) is irreducible with \( R \) an integral domain, then the only divisors of \( f \) take the form \( \lambda \) or \( \lambda f \) for some \( \lambda \in K^\times \), i.e. the only divisors of \( f \) are units or associates of \( f \). This follows from the product degree formula for polynomials over integral domains.

Irreducible polynomials are analogous to prime numbers.

**Lemma 5** (Euclid’s lemma). Suppose that \( f, g, h \in K[t] \) and that \( f \) is irreducible. Then whenever \( f \mid gh \), we have \( f \mid g \) or \( f \mid h \).

\[ \square \] The existence and uniqueness of such polynomials being guaranteed by the division algorithm.
Proof. Let us suppose that \( f \mid g \). Since the only divisors of \( f \) are units or associates of \( f \), we see that 1 is a highest common factor of \( f \) and \( g \). By Bézout’s identity, there exist \( a, b \in \mathbb{K}[t] \) such that \( af + bg = 1 \). Multiplying by \( h \) and rearranging we obtain \( ah + bg = h \). The result follows since \( f \) divides the left-hand side of this identity.

Theorem 6 (Unique factorisation). Let \( f \in \mathbb{K}[t] \) with \( \deg(f) \geq 1 \). Then \( f \) can be written as a product of irreducible polynomials in a manner unique up to the order of the factors and multiplication by constants. Furthermore, if \( f \) is monic, then \( f \) is a product of monic irreducible polynomials, unique up to order.

Definition (Zero or root). Let \( R \) be a ring. We say that \( \alpha \in R \) is a zero or root of \( f \in \mathbb{K}[t] \) if \( f(\alpha) = 0 \).

Lemma 7 (Zeroes correspond to linear factors). Suppose that \( \alpha \in \mathbb{K} \) and \( f \in \mathbb{K}[t] \). Then \( f(\alpha) = 0 \) if and only if \((t - \alpha)\mid f \).

Proof. (\( \Rightarrow \)). Suppose that \( f(\alpha) = 0 \). By the division algorithm, there exist \( q, r \in \mathbb{K}[t] \) with \( f = (t - \alpha)q + r \) and \( \deg(r) < 1 \). Then \( r \) must be a constant. In fact \( r \) is the zero constant since \( r = f(\alpha) - (\alpha - \alpha)q(\alpha) = 0 \).

(\( \Leftarrow \)). Conversely, suppose that \((t - \alpha)\) divides \( f \), so that \( f = (t - \alpha)g \) for some \( g \in \mathbb{K}[t] \). Then \( f(\alpha) = (\alpha - \alpha)g(\alpha) = 0 \).

The above lemma is useful for identifying factors of polynomials.
3. Field Extensions

Recall that in a ring $R$ with $a \in R$, the notation $(a)$ represents the principle ideal generated by $a$, or in other words, the set of multiples \{ab : b \in R\}.

**Proposition 8.** Let $K$ be a field and $f \in K[t]$ an irreducible polynomial of degree $n$. Then the quotient ring $K[t]/(f)$ forms a field in which each congruence class has a unique residue of the form

$$a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} \quad (a_i \in K).$$

In particular $K[t]/(f)$ is isomorphic to $K^n$ as a vector space over $K$.

**Proof.** The key observation here is that non-zero residue classes in $K[t]/(f)$ are invertible: If $g \in K[t]$ is not divisible by $f$ then 1 is a hcf of $f$ and $g$, hence by Theorem 4, there exist $a, b \in K[t]$ such that $af + bg = 1$. In particular $bg \equiv 1 \mod (f)$. It follows that $K[t]/(f)$ is a field.

By the division algorithm, every element of this quotient may be written uniquely as a polynomial over $K$ of degree at most $n - 1$. Thus the set of residues is

$$\{a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + (f) : a_i \in K\},$$

with each such residue defining a unique congruence class (again by uniqueness of remainder). One can check that the map $\phi : K[t]/(f) \to K^n$ given by

$$a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + (f) \mapsto (a_0, \ldots, a_{n-1}) \quad (a_i \in K),$$

is both linear and invertible. ∎

Notice that $K^n$ is strictly ‘larger’ than $K$ as an additive group (and vector space) when $n > 1$.

**Question.** Plainly the special residue classes given by $a_0 \in K$ form a subfield of $K[t]/(f)$ isomorphic to $K$. How do we formally identify that $K$ lies ‘inside’ $K[t]/(f)$?

**Definition (Field extension).** A field extension of a field $K$ is a ring monomorphism\[9\] $i : K \to L$ where $L$ is also a field.

In practice, we identify the image $i(K)$ with $K$, since this is a subfield of $L$ isomorphic to $K$. We then write $K$ for $i(K)$, and talk about the field extension $L : K$ (read ‘$L$ over $K$’, also denoted $L/K$).

**Examples.**

(i) The field extension $\mathbb{C} : \mathbb{R}$ is more formally the monomorphism $i : \mathbb{R} \to \mathbb{C}$ given by $x \mapsto x + 0 \cdot \sqrt{-1}$.

(ii) In Proposition 8 the map $a_0 \mapsto a_0 + (f)$ gives a field extension $K \to K[t]/(f)$.

(iii) Let $K(t)$ denote the field of fractions\[10\] of the ring $K[t]$. Then we have a field extension given by the map $i : K \to K(t)$ defined by $\lambda \mapsto \lambda/1$.

**Theorem 9 (Field extensions have vector space structure).** Suppose that $L : K$ is an extension. Then $L$ forms a vector space over $K$ as follows: If $u, v \in L$ are vectors we define their sum $u + v$ using the field addition in $L$. If $\lambda \in K$ is a scalar and $v \in L$ is a vector we define the scalar multiple $\lambda v$ using the field multiplication in $L$.

---

\[8\] $\mathbb{F}_p$ is the same set as $\mathbb{Z}/p\mathbb{Z}$, but viewed as a field.

\[9\] Review Ch.3 of [Gar86].

\[10\] Injective homomorphism.

Proof. We leave the task of checking that the field axioms are satisfied as an exercise for the reader. \hfill\Box

Thus both $\mathbb{C}$ and $\mathbb{R}(t)$ (the field of fractions of $\mathbb{R}[t]$) are vector spaces over $\mathbb{R}$.

**Definition** (Degree, finite extension). The **degree of an extension** $L : K$ is the dimension of $L$ as a vector space over $K$. We denote this by $[L : K]$. We say $L : K$ is a **finite extension** if $[L : K] < \infty$, and otherwise say it is **infinite**.

**Examples.**
- $[\mathbb{C} : \mathbb{R}] = 2$, since $\mathbb{C}$ has basis $\{1, \sqrt{-1}\}$.
- $[\mathbb{R} : \mathbb{Q}] = \infty$, since otherwise $\mathbb{R}$ is isomorphic as a vector space to $\mathbb{Q}^d$ for some $d \in \mathbb{N}$, in which case $\mathbb{R}$ is countable.
- If $L = \mathbb{Q}[t]/(t^2 - 2)$, then $[L : \mathbb{Q}] = 2$, since $L = \{\lambda t + \mu : \lambda, \mu \in \mathbb{Q}\}$ has basis $\{1, t\}$. Note that $(t^2 - 2)$ is the zero residue class in $L$, so we can think of $t$ as being essentially $\sqrt{2}$ or $-\sqrt{2}$ (either choice is indistinguishable).

**Theorem 10** (Field extension product formula). Suppose that $M : L$ and $L : K$ are field extensions. Then $M : K$ is a field extension and

$$[M : K] = [M : L][L : K]. \tag{3.1}$$

[The idea: First deal with the infinite case, then show that multiplying a basis for $M : L$ by a basis for $L : K$ gives a basis for $M : K$.]

**Proof.** We first consider the case in which the right-hand side of (3.1) is infinite, so at least one of $[M : L]$ and $[L : K]$ is infinite. In this case it suffices to show that $[M : K] = \infty$. If $[L : K] = \infty$, then $M$ (viewed as a vector space over $K$) contains an infinite-dimensional subspace, so must itself be infinite-dimensional. If $[M : L] = \infty$, then $M$ contains an infinite set which is linearly independent over $L$, so also linearly independent over $K$. Hence $M : K$ must again be infinite dimensional.

We may therefore suppose that the right-hand side of (3.1) is finite, so that both $M : L$ and $L : K$ are finite dimensional. Let $x_1, \ldots, x_m$ denote a basis for $M$ over $L$, and let $y_1, \ldots, y_n$ denote a basis for $L$ over $K$. We claim that the products $x_iy_j$, with $1 \leq i \leq m$ and $1 \leq j \leq n$, constitute a basis for $M$ over $K$, from which it follows that $[M : K] = mn$ as required.

To see that the $K$-span of this set encompasses the whole of $M$, first note that every element of $M$ is an $L$-linear combination of the $x_i$. Each coefficient of $x_i$ in such a combination is itself a $K$-linear combination of the $y_j$. Expanding out brackets shows that every element of $M$ is a $K$-linear combination of the $x_iy_j$.

For linear independence, let us suppose that $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ with $\lambda_{ij} \in K$ for all $i$ and $j$. Re-arranging this sum, we have that

$$\sum_{i=1}^m \left( \sum_{j=1}^n \lambda_{ij} y_j \right) x_i = 0.$$

Since the coefficients of the $x_i$ in this sum are elements of $L$, and the $x_i$ are linearly independent over $L$, we deduce that

$$\sum_{j=1}^n \lambda_{ij} y_j = 0 \quad (1 \leq i \leq m).$$

The linear independence of the $y_j$ over $K$ then gives that $\lambda_{ij} = 0$ for all $i$ and $j$. \hfill\Box

**Note** (Tower law). A sequence $K_n : K_{n-1}, K_{n-1} : K_{n-2}, \ldots, K_1 : K_0$ of field extensions (which we can write $K_n : K_{n-1} : \ldots : K_1 : K_0$) is called a **tower** of field extensions, and satisfies the **tower law** for field extensions:

$$[K_n : K_0] = [K_n : K_{n-1}] \cdots [K_1, K_0]. \tag{3.2}$$
Corollary 11. Suppose that \( L : K \) is a field extension for which \( [L : K] \) is a prime number. Then the only subfields of \( L \) containing \( K \) are \( L \) and \( K \).

Proof. Say \( [L : K] = p \). If \( L : M : K \), then by the tower law either \( [L : M] = 1 \) or \( [M : K] = 1 \). In the first case \( M = L \) and in the second \( M = K \). \( \square \)

Exercise. Show that if \( (K_i)_{i \in I} \) is a family of subfields of \( L \), then \( K := \bigcap_{i \in I} K_i \) is also a subfield of \( L \).

Definition \((K \) adjoined by the set \( A \)). Suppose that \( L : K \) is a field extension, and \( A \subset L \). We write \( K(A) \) for the intersection of all subfields of \( L \) that contain \( K \) and \( A \). (Note that \( K(A) \) is a subfield of \( L \), and indeed is the smallest subfield of \( L \) containing both \( K \) and \( A \)).

• \( K(A) \) is the extension of \( K \) generated by \( A \).
• If \( A = \{\alpha_1, \ldots, \alpha_n\} \), we write \( K(\alpha_1, \ldots, \alpha_n) \) for \( K(A) \).
• An extension \( L : K \) is called a simple extension if \( L = K(\alpha) \) for some \( \alpha \in L \).
• We say \( L : K \) is a finitely generated extension over \( K \) if \( L = K(A) \) for some finite set \( A \subset L \).

Exercise. Show that for a field extension \( L : K \), if \( A \subset L \) and \( \beta \in L \) then
\[
K(A \cup \{\beta\}) = K(\beta).
\]

Conclude that \( L : K \) is finitely generated if and only if there exist a tower of simple field extensions \( K_n : K_{n-1} : \cdots : K_1 : K_0 \) with \( K_n = L \) and \( K_0 = K \).

Example. Consider the field extension \( K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) of \( \mathbb{Q} \). We claim that \( K \) is a simple extension of \( \mathbb{Q} \). In order to see this, write \( \alpha = \sqrt{2} + \sqrt{3} \). Clearly \( \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). However, we also have the reverse inclusion. First note that \( \alpha^2 = 5 + 2\sqrt{6} \), so \( \sqrt{6} = \frac{1}{2}(\alpha^2 - 5) \in \mathbb{Q}(\alpha) \). Now \( \sqrt{6} = 3\sqrt{2} + \sqrt{3} \), and we can subtract rational multiples of \( \alpha \) from this number to show that \( \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha) \). (The idea: Letting \( \nu = (\sqrt{2}, \sqrt{3}) = (\sqrt{2}, \sqrt{3}) \), we have in effect shown that the fact that \( \mathbb{Q}(\alpha) \) is closed under multiplication implies that both \( \alpha = (1,1) \cdot \nu \in \mathbb{Q}(\alpha) \) and \( \sqrt{6} = (3,2) \cdot \nu \in \mathbb{Q}(\alpha) \). We can then use elementary row operations to show that \( \sqrt{2} = (1,0) \cdot \nu \in \mathbb{Q}(\alpha) \) and \( \sqrt{3} = (0,1) \cdot \nu \in \mathbb{Q}(\alpha) \).

Exercise. Show that for \( \alpha = \sqrt{2} + \sqrt{3} \) we have \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 \). (Hint: Make a guess at a suitable basis then prove it is so - take a look at the proof of the tower law or the introduction for guessing inspiration.)

Example. There is a potential ambiguity in the notation \( K(\alpha) \), since we use \( K(t) \) to denote the field of fractions of the polynomial ring \( K[t] \). Fortunately, if we set \( L = K(t) \) and take \( \alpha = t \in L \), then the simple field extension \( K(\alpha) \) coincides with the field of fractions \( K(t) \). In other words, the intersection of all subfields of \( L = K(t) \) which contain both \( K \) and \( t \) is equal to \( K(t) \) itself (exercise\(^{[7]}\)).

Definition. Suppose that \( L : K \) is a field extension, and that \( \alpha \in L \).

• If there is a non-zero polynomial \( f \in K[t] \) for which \( f(\alpha) = 0 \) then we say that \( \alpha \) is algebraic over \( K \).
• If there exists no non-zero polynomial \( f \in K[t] \) for which \( f(\alpha) = 0 \) then we say that \( \alpha \) is transcendental over \( K \).

Note. We have seen that \( L : K \) is endowed with the structure of a vector space over \( K \). Then \( \alpha \in L \) is algebraic over \( K \) if the set \( \{\alpha^n : n \geq 0\} \) is linearly dependent, and is transcendental if the set \( \{\alpha^n : n \geq 0\} \) is linearly independent.

Fact. The real numbers \( \pi, e \) and \( 2^{\sqrt{2}} \) are transcendental over \( \mathbb{Q} \). In fact the set of transcendental elements in \( \mathbb{R} \) has full measure (meaning that the set of elements algebraic over \( \mathbb{Q} \) has measure zero).

\(^{[7]}\)The idea is that if a subfield contains \( K \) and \( t \), then closure under addition and multiplication ensures that all polynomials \( f \in K[t] \) are contained in this subfield, hence all rational functions \( f/g \) with \( f, g \in K[t] \) and \( g \neq 0 \) are contained in this subfield.
**Definition.** Suppose that $L : K$ is a field extension and that $\alpha \in L$. We define the evaluation map $E_\alpha : K[t] \to L$ by $E_\alpha(f) = f(\alpha)$ for each $f \in K[t]$. 

**Note.**
- $E_\alpha : K[t] \to L$ is a ring homomorphism.
- The element $\alpha \in L$ is transcendental $\iff$ $\ker(E_\alpha) = \{0\}$ $\iff$ $E_\alpha$ is injective.
- The element $\alpha \in L$ is algebraic $\iff$ $\ker(E_\alpha) \neq \{0\}$ $\iff$ $E_\alpha$ is not injective.

**Proposition 12** (Polynomials over $K$ form a PID). The ring $K[t]$ is a principal ideal domain (PID), so that any ideal $I$ in $K[t]$ takes the form $I = (f) = \{gf : g \in K[t]\}$ for some $f \in K[t]$. 

**Proof.** Let $I$ be a non-zero ($\neq \{0\}$) ideal in $K[t]$ and let $f$ be a polynomial in $I$ of minimal non-negative degree. Given $g \in I$ we apply the division algorithm to obtain polynomials $q, r \in K[t]$ with $g = fq + r$ and $\deg(r) < \deg(f)$. Since $I$ is an ideal, we have $r = g - fq \in I$. By minimality of $\deg(f)$, we must have $\deg(r) = -\infty$, or equivalently $r = 0$. Thus $f|g$ for every $g \in I$, from which it follows that $I = (f)$. 

As a consequence, we see that for any $\alpha \in L$ which is algebraic over $K$, the non-zero kernel $\ker(E_\alpha)$ is generated by some non-zero polynomial $m_\alpha \in K[t]$, so that $\ker(E_\alpha) = (m_\alpha)$. Multiplying through by a non-zero constant, we may assume that $m_\alpha$ is monic. If $f \in K[t]$ is monic and also satisfies $\ker(E_\alpha) = (f)$, then $m_\alpha|f$ and $f|m_\alpha$. Thus $f$ and $m_\alpha$ are associate with the same leading coefficient, so must be equal. We can therefore make the following definition.

**Definition** (Minimal polynomial). Let $L : K$ be a field extension and let $\alpha \in L$ be algebraic over $K$. The minimal polynomial of $\alpha$ over $K$ is the unique monic polynomial satisfying $\ker(E_\alpha) = (m_\alpha)$.

**Theorem 13** (Factorisation of the evaluation map). Suppose that $L : K$ is a field extension and that $\alpha \in L$ is algebraic over $K$. Then

(i) The minimal polynomial $m_\alpha$ of $\alpha$ over $K$ is irreducible in $K[t]$.

(ii) The image $E_\alpha(K[t])$ of the polynomial ring $K[t]$ is the subfield $K(\alpha)$.

(iii) The evaluation map $E_\alpha$ factorises as $i \circ \bar{E}_\alpha \circ q$, where $q : K[t] \to K[t]/(m_\alpha)$ is the quotient map, $\bar{E}_\alpha : K[t]/(m_\alpha) \to K(\alpha) \to i : K(\alpha) \to L$ is the inclusion mapping.

(iv) Let $n = \deg(m_\alpha)$. Then the isomorphism $\bar{E}_\alpha$ between $K[t]/(m_\alpha)$ and $K(\alpha)$ is given by $f + (m_\alpha) \mapsto f(\alpha)$, which can be described more explicitly as $a_0 + a_1t + \cdots + a_{n-1}t^{n-1} + (m_\alpha) \mapsto a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$ ($a_i \in K$).

**Proof.** We begin with claim (i). Suppose that $m_\alpha$ splits over $K$, say as $m_\alpha = fg$. Then applying the evaluation map, we obtain $0 = E_\alpha(m_\alpha) = E_\alpha(f)E_\alpha(g) = f(\alpha)g(\alpha)$. So $f(\alpha) = 0$ or $g(\alpha) = 0$. But if $f(\alpha) = 0$, then $f \in (m_\alpha)$, so $m_\alpha|f$ and $g$ is necessarily a unit. Similarly if $g(\alpha) = 0$. Thus $m_\alpha$ is irreducible.

Next we prove claim (iii), as it eases our proof of claim (ii). Since $m_\alpha$ is irreducible, one finds that $K[t]/(m_\alpha)$ is a field. By the first ring homomorphism theorem we have that $K[t]/\ker(E_\alpha)$ is isomorphic to $\text{Im}(E_\alpha)$ via the map $f + \ker(E_\alpha) \mapsto E_\alpha(f)$. 

13See [http://en.wikipedia.org/wiki/Isomorphism_theorem#First_isomorphism_theorem_2](http://en.wikipedia.org/wiki/Isomorphism_theorem#First_isomorphism_theorem_2)
Theorem 16. Suppose that \( \alpha, \beta \in L \) are algebraic over \( K \). Let \( \alpha \) and \( \beta \) be algebraic over \( K \). Since \( \beta \) is algebraic, \( \beta \) is algebraic over \( K \).

Proof. We need to verify that \( L^{\text{alg}} \) is closed under addition, multiplication and taking additive/multiplicative inverses. Suppose that \( \alpha \) and \( \beta \) are algebraic over \( K \). Since \( \beta \) is algebraic

\[ \text{Every polynomial in } L[t] \text{ of positive degree has a root in } L. \]

14Every polynomial in \( L[t] \) of positive degree has a root in \( L \).
over \( K \), it is also algebraic over \( K(\alpha) \). Thus by (3.3), the tower law and Theorem [14] we find that

\[
[K(\alpha, \beta) : K] = [K(\alpha)(\beta) : K] = [K(\alpha)(\beta) : K(\alpha)][K(\alpha) : K] < \infty.
\]

Now since \( \alpha + \beta, \alpha \beta, -\alpha \) and \( \alpha^{-1} \) (assuming \( \alpha \neq 0 \)) are elements of \( K(\alpha, \beta) \), which is itself a finite extension of \( K \), we see from Corollary [15] that these elements are algebraic over \( K \).

**Exercise.** Given a field extension \( L : K \) with \( \alpha \in L \) non-zero and algebraic over \( K \), derive from \( m_{\alpha} \) a non-zero polynomial over \( K \) of which \( \alpha^{-1} \) is a root. (Hint: If \( f(\alpha) = 0 \) then \( \alpha^{-1} \) is a zero of the rational function \( f(t^{-1}) \in K(t) \). Clear denominators to obtain an element of \( K[t] \).

In Corollary [15] we established that every finite extension is algebraic. The converse is not true in general, for instance Theorem [10] tells us that if \( A \) denotes the set of complex numbers algebraic over \( \mathbb{Q} \) then \( A : \mathbb{Q} \) is an algebraic extension, but in §5 we prove that this extension is not finite. The converse is true however, if we assume in addition that the algebraic extension is finitely generated. This is the content of the next theorem.

**Theorem 17.** Suppose that \( L : K \) is a field extension. Then the following are equivalent:

(i) \( [L : K] < \infty \);

(ii) \( L : K \) is algebraic and finitely generated;

(iii) There exists finitely many \( \alpha_1, \ldots, \alpha_n \in L \) all algebraic over \( K \) such that \( L = K(\alpha_1, \ldots, \alpha_n) \).

**Proof.** (i) \( \implies \) (ii): Assuming (i), the extension \( L : K \) is algebraic by Corollary [15]. Since \( [L : K] < \infty \), there exist \( \alpha_1, \ldots, \alpha_n \in L \) which together form a basis for \( L \) over \( K \). As \( L \) equals the \( K \)-linear span of the \( \alpha_i \), we certainly have \( L \subset K(\alpha_1, \ldots, \alpha_n) \). But \( L \) is also a subfield of \( K \) containing \( K \cup \{\alpha_1, \ldots, \alpha_n\} \), so \( K(\alpha_1, \ldots, \alpha_n) \subset L \). Thus \( L = K(\alpha_1, \ldots, \alpha_n) \) is also finitely generated over \( K \).

(ii) \( \implies \) (iii): Finite generation gives that \( L = K(\alpha_1, \ldots, \alpha_n) \) for some \( \alpha_i \). Each \( \alpha_i \) algebraic over \( K \) since \( L \) is algebraic.

(iii) \( \implies \) (i): This follows from the tower law and Theorem [14] since assuming (iii) and setting \( K_i = K(\{\alpha_j : j < i\}) \) we have

\[
[L : K] = [K(\alpha_1, \ldots, \alpha_n) : K] = [K_{n-1}(\alpha_n) : K_{n-1}] \ldots [K_0(\alpha_1) : K_0] < \infty.
\]

We postpone the proof that \([\mathbb{Q}^{\text{alg}} : \mathbb{Q}] = \infty \) until we have developed some irreducibility criteria in §5. We have already developed enough theory to solve some famous problems.

## 4. Ruler and Compass Constructions

Let us formalise what it means for a point \( z = (x, y) \in \mathbb{R}^2 \) to be constructible using ruler and compass.

**Definition** (Constructible from \( P \)). Given a set \( P \) of points in the plane \( \mathbb{R}^2 \), we say that a line \( L \) is constructible from \( P \) if it passes through two distinct points of \( P \). We say a circle \( C \) is constructible from \( P \) if it is centred at a point of \( P \) and has a point of \( P \) on its circumference. Finally, we say that a point \( z \in \mathbb{R}^2 \) is **constructible in one step from \( P \)** if any of the following hold:

(a) \( z \) is the intersection of two distinct lines constructible from \( P \);

(b) \( z \) is an intersection of a line and a circle, both constructible from \( P \);

(c) \( z \) is an intersection of two distinct circles constructible from \( P \).

We say that \( z \) is **constructible from \( P \)** if there exists a finite number of points \( z_1, \ldots, z_n \) with \( z_n = z \) such that each \( z_i \) is constructible in one step from \( P \cup \{z_1, \ldots, z_{i-1}\} \). We say that \( z \) is **constructible using ruler and compass** if it is constructible from the set \( \{(0, 0), (1, 0)\} \).
Let us call an angle constructible if it is found between two constructible lines (lines passing through two distinct constructible points).

Exercise. The angle $\pi/3$ is constructible.

Exercise. Any constructible angle $\theta$ may be bisected by a line using ruler and compass, meaning $\theta/2$ is also constructible. In particular, $\pi/6$ is constructible.

In this section we establish a number of impossibility results concerning ruler and compass constructions, for instance that one cannot trisect all angles using ruler and compass, not even constructible angles (we prove that $\pi/9$ is not a constructible angle).

The key to all our impossibility results is the following.

**Theorem 18.** If $(x, y)$ is constructible using ruler and compass, then there exist non-negative integers $r$ and $s$ such that $[\mathbb{Q}(x) : \mathbb{Q}] = 2^r$ and $[\mathbb{Q}(y) : \mathbb{Q}] = 2^s$.

Before proving this theorem, we begin with a lemma.

**Notation.** If $P = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ is a finite set of points in the plane $\mathbb{R}^2$, then we define $\mathbb{Q}(P)$ to be the $\mathbb{R}$-subfield $\mathbb{Q}(x_1, y_1, \ldots, x_n, y_n)$.

**Lemma 19.** If $(x, y)$ is constructible in one step from $P$, then $x$ and $y$ satisfy quadratic or linear polynomials with coefficients in $\mathbb{Q}(P)$.

**Proof.** There are three cases to consider, of which we only consider the case where $(x, y)$ results from the intersection of a line $L$ and a circle $C$, both constructible from $P$. As $L$ is constructible, there exist distinct points $(x_1, y_1), (x_2, y_2) \in P$ both lying on the line $L$. Since $(x, y)$ also lies on $L$, the numbers $x$ and $y$ satisfy the equation

$$(x - x_1)(y_2 - y_1) = (y - y_1)(x_2 - x_1).$$

Hence there exist $a, b, c \in \mathbb{Q}(P)$ with $a$ and $b$ not both zero such that

$$ax + by = c.$$  \hspace{1cm} (4.1)

Since $C$ is constructible from $P$, there exist points $(x_0, y_0), (x_3, y_3) \in P$ such that $C$ is centred at $(x_0, y_0)$ and $C$ has $(x_3, y_3)$ lying on its circumference. Then $x$ and $y$ satisfy the equation

$$(x - x_0)^2 + (y - y_0)^2 = (x_3 - x_0)^2 + (y_3 - y_0)^2.$$  \hspace{1cm} (4.2)

Clearly the right-hand side above is an element of $\mathbb{Q}(P)$. Expanding brackets, we therefore deduce that there exists $\lambda, \mu \in \mathbb{Q}(P)$ such that

$$x^2 + \lambda xy + y^2 = \mu.$$  \hspace{1cm} (4.3)

If $b = 0$ in (4.1) then $x$ satisfies a linear equation with coefficients in $\mathbb{Q}(P)$, since we must have $a \neq 0$ and $x = c/a$. Therefore suppose $b \neq 0$. Rearranging (4.1) and substituting for $y$ in (4.2) we deduce that

$$x^2 + \frac{1}{b}x(c - ax) + \frac{1}{b^2}(c - ax)^2 - \mu = 0.$$  \hspace{1cm} (4.3)

The left-hand side of (4.3) cannot be identically zero, since then every point of the unbounded set $L$ would be contained in the bounded set $C$. Therefore $x$ satisfies a non-zero polynomial of degree at most 2 with coefficients in $\mathbb{Q}(P)$. A similar argument works for $y$. \hspace{1cm} \Box

**Proof of Theorem 18.** Since $(x, y)$ is constructible using ruler and compass, there exist a sequence of points $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n) \in \mathbb{R}^2$ such that

- $(x_0, y_0) = (0, 0)$;
- $(x_1, y_1) = (1, 0)$;
- $(x_n, y_n) = (x, y)$;
- For each $1 \leq i < n$ the point $(x_{i+1}, y_{i+1})$ is constructible in one step from the set $P_i = \{(x_0, y_0), (x_1, y_1), \ldots, (x_i, y_i)\}$.

12
We deduce from Lemma [19] that for each \( 1 \leq i < n \) both \([Q(P_i)(x_{i+1}) : Q(P_i)]\) and \([Q(P_i)(y_{i+1}) : Q(P_i)]\) equal 1 or 2. By the tower law \([Q(P_n) : Q]\) is equal to
\[
[Q(P_{n-1})(x_n,y_n) : Q(P_{n-1})(x_n)][Q(P_{n-1})(x_n) : Q(P_{n-1})] \cdots [Q(P_1)(x_2,y_2) : Q(P_1)(x_2)][Q(P_1)(x_1) : Q(P_1)],
\]
which is a product of 1s and 2s. Thus \([Q(P_n) : Q] = 2^r\) for some non-negative integer \( r \). Again, by the tower law, we see that both \([Q(x) : Q]\) and \([Q(y) : Q]\) divide \( 2^r \), so are themselves a power of 2.

**Exercise.** (i) Given three distinct points \( A, B \) and \( P \), with \( P \) not on the line \( AB \), show that one can construct a line passing through \( P \) which is perpendicular to \( AB \).
(ii) Given two distinct constructible points \( P \) and \( Q \), show that one can construct a line passing through \( P \) which is perpendicular to \( PQ \).
(iii) Combine (i) and (ii) to show that given distinct \( A, B, P \) and \( Q \), one can construct a line through \( P \) which is parallel to \( AB \).
(iv) Use (iii) to show that given any constructible points \( A \) and \( B \), with the origin 0 not on the line \( AB \), one can construct the parallelogram with corners at \( O, A, B \) and \( B - A \).
(v) Conclude that if the length \( l \) is constructible, so that it forms the distance between two constructible points \( A \) and \( B \), then the point \((1,0)\) is also constructible.

**Theorem 20.** Angle trisection, squaring the circle and doubling the cube are all impossible using ruler and compass. More precisely:

(i) The constructible angle \( \pi/3 \), formed between the constructible lines which join \((0,0)\) to \((1,0)\) and \((0,0)\) to \((1,\sqrt{3})\), is not trisectable.
(ii) One cannot construct a length whose cube is twice the volume of the unit cube.
(iii) One cannot construct a length whose square equals the area of the unit circle.

**Proof.** (i) Let \( \theta = \pi/9 \). By way of contradiction, suppose that the angle in question is trisectable, then one of the lines \( y = (\tan \theta)x \) or \( y = (\tan(2\theta))x \) is constructible. Since angle bisection is possible, it follows in either case that the line \( y = (\tan \theta)x \) is constructible. Intersecting this line with the unit circle centred at the origin, we see that the point \((\cos \theta, \sin \theta)\) is constructible. We claim that \([Q(\cos \theta) : Q] = 3\), which on comparison with Theorem [18] gives our desired contradiction.

To prove the claim, first note that by the double angle formulae, we have
\[
\frac{1}{2} = \cos(3\theta) = \cos \theta \cos(2\theta) - \sin \theta \sin(2\theta) = \cos \theta (\cos^2 \theta - \sin^2 \theta) - \sin \theta (2 \sin \theta \cos \theta) = \cos^3 \theta - 3 \sin^2 \theta \cos \theta = \cos^3 \theta - 3 \cos \theta + 3 \cos^3 \theta = 4 \cos^3 \theta - 3 \cos \theta.
\]
Hence \( 2 \cos \theta \) is a zero of the cubic \( f = t^3 - 3 - 1 \). Let us now show that this is irreducible over \( Q \). If not, it must have a linear factor over \( Q \), hence a rational root \( a/b \) with \( a \) and \( b \) coprime integers and \( b \) positive. Multiplying through by \( b^3 \) we deduce that \( a^3 - 3ab^2 - b^3 = 0 \). Thus \( b|a^3 \) and \( a|b^3 \). Since \( a \) and \( b \) are coprime, it follows from Euclid’s lemma that \( a|b \) and \( b|a \), so that \( a/b = \pm 1 \). One can check that \( f(\pm 1) \neq 0 \). Thus \( f \) is indeed monic irreducible over \( Q \) and must therefore be the minimal polynomial for \( 2 \cos \theta \) over \( Q \). By Theorem [14] we must have \([Q(2 \cos \theta) : Q] = \deg(f) = 3 \). Since 2 is a non-zero rational, \([Q(2 \cos \theta) : Q] = [Q(\cos \theta) : Q] \), which yields the claim.

(ii) By the previous exercise, if the length \( l \) with \( l^3 = 2 \) is constructible, then so is the point \((l,0) = (\sqrt[3]{2},0)\). Since \( \sqrt[3]{2} \) is irrational, the cubic \( f = t^3 - 2 \) is irreducible over \( Q \) (it has only one real root - think of the graph). It follows that \( f \) equals the minimal polynomial of \( \sqrt[3]{2} \) over \( Q \), and so by Theorem [14] we have \([Q(\sqrt[3]{2}) : Q] \). Hence by Theorem [18] the length \( l \) cannot be constructible.
follows that if $f$ is reducible over $\mathbb{Q}$, then $f \equiv 1 \mod p$. Hence by the degree-product formula over $\mathbb{F}_p$, either $g_1 \equiv 0$ or $h_1 \equiv 0 \mod p$. Re-labeling if necessary, we may assume the latter. Set $N_2 = N_1/p$, $g_2 = g_1$ and let $h_2$ be the polynomial obtained from $h_1$ by dividing all coefficients by $p$. Then $N_2 f = g_2 h_2$ with $\deg(g_2) = \deg(g)$, $\deg(h_2) = \deg(h)$ and $1 \leq N_2 < N_1$. We can continue iterating in this manner, reducing $N_i$ by at least one on each iteration, until we obtain $N_i = 1$ for some $i$. It then follows that $f = g_i h_i$ for some $g_i, h_i \in \mathbb{Z}[t]$ with $\deg(g_i) = \deg(g)$ and $\deg(h_i) = \deg(h)$. It follows that if $f$ is reducible over $\mathbb{Q}$ then it is also reducible over $\mathbb{Z}$.

Example. Let us show that the polynomial $t^2 - 2$ is irreducible over $\mathbb{Q}$. By Gauss’ lemma, we need only show that $t^2 - 2$ is irreducible over $\mathbb{Z}$. Suppose that

$$t^2 - 2 = (a_1 t + b_1)(a_2 t + b_2)$$

with $a_1, b_1 \in \mathbb{Z}$. Then $a_1 a_2 = 1$ and $b_1 b_2 = -2$. Thus $b_1 = \pm 1$ or $b_2 = \pm 1$. Re-labeling indices if necessary we may assume that $b_1 = \pm 1$. Since $a_1 = \pm 1$, we see that one of $t + 1$ or $t - 1$ is a factor of $f$. But then $f(-1) = 0$ or $f(1) = 0$, neither of which are true.

More sophisticated approaches are based on reduction modulo $p$, a tactic we have already employed in the proof of Gauss’ lemma. In this context, when $f \in \mathbb{Z}[t]$, we write $[f]_m$ for the image of $f$ under the canonical map from $\mathbb{Z}[t]$ to $(\mathbb{Z}/m\mathbb{Z})[t]$ which maps each coefficient in $\mathbb{Z}$ to its residue class mod $m$. One can check that the localisation map is a ring homomorphism $\mathbb{Z}[t] \to (\mathbb{Z}/m\mathbb{Z})[t]$.

Theorem 22 (Localisation principle). Let $f \in \mathbb{Z}[t]$ and suppose there exists a prime $p$ which does not divide the leading coefficient of $f$ and such that $[f]_p$ is irreducible over $\mathbb{F}_p$. Then $f$ is irreducible over $\mathbb{Q}$.

Proof. Suppose that $f = gh$ for some $g, h \in \mathbb{Z}[t]$. As localisation mod $p$ is a homomorphism on $\mathbb{Z}[t]$, we have $[f]_p = [g]_p[h]_p$. Since $p$ does not divide the leading coefficient of $f$ and $[f]_p$ is irreducible over $\mathbb{F}_p$, we have (re-labeling $g$ and $h$ if necessary) that $\deg[g]_p = \deg[f]_p = \deg(f)$. Therefore $\deg(g) \geq \deg(f)$. But since $f \neq 0$, the degree product formula gives that $\deg(f) \geq \deg(g)$. Thus $\deg(g) = \deg(f)$. Hence $f$ is irreducible over $\mathbb{Z}$, and therefore irreducible over $\mathbb{Q}$ by Gauss’ lemma.

Theorem 23 (Eisenstein’s criterion). Let $f \in \mathbb{Z}[t]$ and suppose there exists a prime $p$ dividing all coefficients of $f$ but the leading coefficient, and such that $p^2$ does not divide the constant coefficient. Then $f$ is irreducible over $\mathbb{Q}$.

Proof. Suppose that $f = gh$ for some integer polynomials of the form $g = a_0 + a_1 t + \cdots + a_m t^m$ and $h = b_0 + b_1 t + \cdots b_n t^n$. Since $p|a_0 b_0$ and $p^2 \not| a_0 b_0$, we have that $p$ divides exactly one of

5. Some irreducibility criteria

It is apparent that it is convenient to have available a number of irreducibility criteria.

Lemma 21 (Gauss’s lemma). Let $f \in \mathbb{Z}[t]$. Then $f$ is irreducible over $\mathbb{Q}$ if and only if $f$ is irreducible over $\mathbb{Z}$.

Proof. The ‘only if’ direction is clear, we therefore prove the ‘if’ direction. To this end, suppose that $f = gh$ with $g, h \in \mathbb{Q}[t]$. Clearing denominators, it follows that there exists a positive integer $N_1 \geq 1$ and $g_1, h_1 \in \mathbb{Z}[t]$ with $\deg(g_1) = \deg(g)$ and $\deg(h_1) = \deg(h)$ such that $N_1 f = g_1 h_1$.

Suppose that $N_1 > 1$, so that $N_1$ has a prime factor $p$. Working over the integral domain $\mathbb{F}_p$ we have $0 \equiv g_1 h_1 \mod p$. Hence by the degree-product formula over $\mathbb{F}_p$, either $g_1 \equiv 0$ or $h_1 \equiv 0 \mod p$. Re-labeling if necessary, we may assume the latter. Set $N_2 = N_1/p$, $g_2 = g_1$ and let $h_2$ be the polynomial obtained from $h_1$ by dividing all coefficients by $p$. Then $N_2 f = g_2 h_2$ with $\deg(g_2) = \deg(g)$, $\deg(h_2) = \deg(h)$ and $1 \leq N_2 < N_1$. We can continue iterating in this manner, reducing $N_i$ by at least one on each iteration, until we obtain $N_i = 1$ for some $i$. It then follows that $f = g_i h_i$ for some $g_i, h_i \in \mathbb{Z}[t]$ with $\deg(g_i) = \deg(g)$ and $\deg(h_i) = \deg(h)$. It follows that if $f$ is reducible over $\mathbb{Q}$ then it is also reducible over $\mathbb{Z}$.

Example. Let us show that the polynomial $t^2 - 2$ is irreducible over $\mathbb{Q}$. By Gauss’ lemma, we need only show that $t^2 - 2$ is irreducible over $\mathbb{Z}$. Suppose that

$$t^2 - 2 = (a_1 t + b_1)(a_2 t + b_2)$$

with $a_1, b_1 \in \mathbb{Z}$. Then $a_1 a_2 = 1$ and $b_1 b_2 = -2$. Thus $b_1 = \pm 1$ or $b_2 = \pm 1$. Re-labeling indices if necessary we may assume that $b_1 = \pm 1$. Since $a_1 = \pm 1$, we see that one of $t + 1$ or $t - 1$ is a factor of $f$. But then $f(-1) = 0$ or $f(1) = 0$, neither of which are true.

More sophisticated approaches are based on reduction modulo $p$, a tactic we have already employed in the proof of Gauss’ lemma. In this context, when $f \in \mathbb{Z}[t]$, we write $[f]_m$ for the image of $f$ under the canonical map from $\mathbb{Z}[t]$ to $(\mathbb{Z}/m\mathbb{Z})[t]$ which maps each coefficient in $\mathbb{Z}$ to its residue class mod $m$. One can check that the localisation map is a ring homomorphism $\mathbb{Z}[t] \to (\mathbb{Z}/m\mathbb{Z})[t]$.

Theorem 22 (Localisation principle). Let $f \in \mathbb{Z}[t]$ and suppose there exists a prime $p$ which does not divide the leading coefficient of $f$ and such that $[f]_p$ is irreducible over $\mathbb{F}_p$. Then $f$ is irreducible over $\mathbb{Q}$.

Proof. Suppose that $f = gh$ for some $g, h \in \mathbb{Z}[t]$. As localisation mod $p$ is a homomorphism on $\mathbb{Z}[t]$, we have $[f]_p = [g]_p[h]_p$. Since $p$ does not divide the leading coefficient of $f$ and $[f]_p$ is irreducible over $\mathbb{F}_p$, we have (re-labeling $g$ and $h$ if necessary) that $\deg[g]_p = \deg[f]_p = \deg(f)$. Therefore $\deg(g) \geq \deg(f)$. But since $f \neq 0$, the degree product formula gives that $\deg(f) \geq \deg(g)$. Thus $\deg(g) = \deg(f)$. Hence $f$ is irreducible over $\mathbb{Z}$, and therefore irreducible over $\mathbb{Q}$ by Gauss’ lemma.

Theorem 23 (Eisenstein’s criterion). Let $f \in \mathbb{Z}[t]$ and suppose there exists a prime $p$ dividing all coefficients of $f$ but the leading coefficient, and such that $p^2$ does not divide the constant coefficient. Then $f$ is irreducible over $\mathbb{Q}$.

Proof. Suppose that $f = gh$ for some integer polynomials of the form $g = a_0 + a_1 t + \cdots + a_m t^m$ and $h = b_0 + b_1 t + \cdots b_n t^n$. Since $p|a_0 b_0$ and $p^2 \not| a_0 b_0$, we have that $p$ divides exactly one of
Proof. We verified that \( p \mid b_0 \). Let \( i \) be minimal such that \( p \mid a_i \) (clearly \( p \mid a_m \) since \( p \mid a_m b_n \)). Suppose that \( i < \deg(f) \). Then

\[
p|a_i b_0 + a_{i-1} b_1 + \cdots + a_0 b_i.
\]

Yet \( p|a_j \) for all \( j < i \), so that \( p|a_i b_0 \). Hence by Euclid’s lemma either \( p|a_i \) or \( p|b_0 \), both of which lead to contradictions. Thus \( i = \deg(f) \). Hence \( \deg(g) \geq i = \deg(f) \). It follows that \( f \) is irreducible over \( \mathbb{Z} \), and thus irreducible over \( \mathbb{Q} \) by Gauss’ lemma. \( \square \)

**Proposition 24** (Change of variables). Let \( K \) be a field and \( a, b \in K \) with \( a \neq 0 \). Then \( f \) is irreducible over \( K \) iff \( f(at+b) \) is irreducible over \( K \).

**Proof.** Let \( q \) be a non-zero polynomial over \( K \). Since the leading coefficient of \( q(at+b) \) is equal to the leading coefficient of \( q \) multiplied by \( a^{\deg(q)} \), we see that \( \deg(q) = \deg(g(at+b)) \). Thus \( f = gh \) with \( \deg(g) \) and \( \deg(h) \) both less than \( \deg(f) \) implies that \( f(at+b) = g(at+b)h(at+b) \) so that \( f(at+b) \) is reducible.

For the reverse implication, we note that if \( f_1 \) is defined to be the polynomial \( f(at+b) \), then \( f(t) = f_1(a^{-1}t - a^{-1}b) \). Hence by the previous implication, if \( f_1 \) is reducible then so is \( f \). \( \square \)

**Examples.**

1. \( f = t^5 + 3t^2 + 9t + 3 \) is irreducible over \( \mathbb{Q} \) by Eisenstein’s criterion with \( p = 3 \).
2. \( f = \frac{2}{9}t^5 + \frac{2}{3}t^4 + t^3 + \frac{1}{3} \) is irreducible over \( \mathbb{Q} \) if and only if \( 9f = 2t^5 + 15t^4 + 9t^3 + 3 \) is irreducible over \( \mathbb{Q} \). The latter holds by Eisenstein’s criterion with \( p = 3 \).
3. Consider \( f = t^4 + 4t^2 + 6t + 8 \). By the binomial theorem \( f = (t+1)^4 + 7 = f_1(t+1) \) where \( f_1 = t^7 + 7 \) is irreducible over \( \mathbb{Q} \) by Eisenstein’s criterion with \( p = 7 \). Thus by change of variables \( f \) is also irreducible over \( \mathbb{Q} \).
4. Consider \( f = t^2 + 9t + 1 \). Localising over \( \mathbb{F}_3 \) gives \( [f]_3 = t^2 + 1 \). This is irreducible over \( \mathbb{F}_3 \) since \( a^2 \neq -1 \) for any \( a \in \mathbb{F}_3 \). Thus by the localisation principle, \( f \) is irreducible over \( \mathbb{Q} \).
5. Consider \( f = 16t^4 + 15t^3 + 7 \). Localising over \( \mathbb{F}_5 \) gives \( [f]_5 = t^4 + 2 \). This has no zeros in \( \mathbb{F}_5 \), so has no linear factors. Working over \( \mathbb{F}_5 \) suppose that

\[
t^4 + 2 = (t^2 + a_1 t + b_1)(t^2 + a_2 t + b_2).
\]

Then

\[
a_1 + a_2 = 0, \quad a_1 a_2 + b_1 + b_2 = 0, \quad a_1 b_2 + a_2 b_1 = 0, \quad b_1 b_2 = 2 \pmod{5}.
\]

Since \( a_2 = -a_1 \) and \( b_1 b_2 = 2 \), we can multiply \( a_1 b_2 + a_2 b_1 = 0 \) through by \( b_1 \) to obtain that \( 2a_1 - a_1 b_1^2 = 0 \). Since \( \mathbb{F}_5 \) is an integral domain, we can factorise to deduce that either \( a_1 = 0 \) or \( b_1^2 = 2 \). The squares in \( \mathbb{F}_5 \) are 0, 1 and 4, so we must have that \( a_1 = 0 \). This gives that \( a_2 = 0 \) and \( b_1 + b_2 = 0 \), so \( b_1 = -b_2 \). But then \( -b_2 = 2 \), so that \( b_1^2 = 3 \). Again 3 is not a square in \( \mathbb{F}_5 \), so we have a contradiction.

Thus \( [f]_5 \) is irreducible and 5 does not divide the leading coefficient of \( f \), so by the localisation principle \( f \) is irreducible over \( \mathbb{Q} \). **Warning:** Over \( \mathbb{F}_3 \) we have

\[
[f]_3 = t^4 + 1 = (t^2 + t - 1)(t^3 - t - 1),
\]

so we must choose the prime \( p \) in our localisation carefully.

**Proposition 25.** The field \( A \) consisting of complex numbers algebraic over \( \mathbb{Q} \) is an infinite algebraic extension of \( \mathbb{Q} \).

**Proof.** We verified that \( A \) is a field in Theorem [16]. By definition the extension \( A : \mathbb{Q} \) is algebraic. This is not a finite extension since the degree of the minimal polynomial of an element of \( A \) is unbounded: the polynomial \( t^n - 2 \) is irreducible over \( \mathbb{Q} \) by Eisenstein with \( p = 2 \), so that any complex root \( \alpha \) of this polynomial is an element of \( A \) with \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = n \). Thus for any \( n \in \mathbb{N} \) we have \( [A : \mathbb{Q}] \geq n \). \( \square \)
6. Splitting fields and normal extensions

From the fundamental theorem of algebra we know that every non-constant polynomial over \( \mathbb{Q} \) can be written as a product of linear factors over \( \mathbb{C} \). The motivation for studying splitting fields is that if we are studying a specific polynomial \( f \in \mathbb{Q}[t] \), then \( f \) has such a factorisation over a much smaller field than \( \mathbb{C} \), in fact over a finite extension of \( \mathbb{Q} \).

**Definition** (Splits / splitting field). Let \( L : K \) be a field extension and let \( f \) be a polynomial over \( K \). We say that \( f \) **splits** over \( L \) if it can be written as a product of linear factors over \( L \). Equivalently, if \( \lambda \) is the leading coefficient of \( f \), then \( f \) splits over \( L \) if one has
\[
f = \lambda(t - \alpha_1) \cdots (t - \alpha_n)
\]
for some \( \alpha_1, \ldots, \alpha_n \in L \).

We say that \( L : K \) is a **splitting extension** for \( f \) if

(i) \( f \) splits over \( L \).

(ii) If \( f \) splits over a field \( M \) which is intermediate between \( L \) and \( K \) (in the sense that \( L \supset M \supset K \)), then \( L = M \).

Equivalently, \( L \) is a minimal extension of \( K \) over which \( f \) splits. We also say \( L \) is a **splitting field** for \( f \) over \( K \) in this case.

Notice that if \( f \in K[t] \) splits over some extension \( L \) of \( K \), then the intersection
\[
\Sigma = \bigcap \{ M : M \text{ is a subfield of } L, K \subset M \text{ and } f \text{ splits over } M \}
\]
is itself a field containing \( K \) and over which \( f \) splits. Clearly this intersection is a minimal such extension of \( K \) (why?). It follows that if \( f \) splits over some extension of \( K \) then there exists a splitting field for \( f \) over \( K \), an observation we record as a proposition.

**Proposition 26.** Let \( f \) be a polynomial over \( K \) and suppose that there is an extension \( L : K \) such that \( f \) splits over \( L \). Then there exists a splitting field for \( f \) over \( K \).

We would like to determine exactly what a splitting field for \( f \) over \( K \) looks like. Clearly if \( f \) has the factorisation \( \lambda(t - \alpha_1) \cdots (t - \alpha_n) \) then \( f \) splits over the field \( K(\alpha_1, \ldots, \alpha_n) \). Moreover, it is clear that this is a minimal field containing \( K \) and the roots \( \alpha_1, \ldots, \alpha_n \) (by definition of the field generated by \( K \) and \( \alpha_1, \ldots, \alpha_n \)). The only way that \( K(\alpha_1, \ldots, \alpha_n) \) could not be a splitting field for \( f \) over \( K \) is if \( f \) has another decomposition into linear factors \( f = \lambda(t - \beta_1) \cdots (t - \beta_n) \), with \( K(\beta_1, \ldots, \beta_n) \) a proper subfield of \( K(\alpha_1, \ldots, \alpha_n) \). For this to be true the sets \( \{ \alpha_1, \ldots, \alpha_n \} \) and \( \{ \beta_1, \ldots, \beta_n \} \) cannot be equal, but this contradicts unique factorisation in \( L[t] \) with \( L = K(\alpha_1, \ldots, \alpha_n) \), since either side of the identity
\[
(t - \alpha_1) \cdots (t - \alpha_n) = (t - \beta_1) \cdots (t - \beta_n)
\]
would constitute genuinely distinct decompositions into irreducible factors. We have therefore proved the following.

**Proposition 27** (Form of a splitting field). Let \( f \in K[t] \). Suppose that \( \Sigma \) is a splitting field for \( f \) over \( K \). Then \( \Sigma \) takes the form \( K(\alpha_1, \ldots, \alpha_n) \) where \( \alpha_1, \ldots, \alpha_n \) are the roots of \( f \) in \( \Sigma \).

**Corollary 28.** Let \( f \in K[t] \). If \( \Sigma : K \) is a splitting extension for \( f \), then \( \Sigma : K \) is a finite extension (hence also algebraic).

**Proof.** From Theorem 17 the extension \( \Sigma : K \) is finite if and only if \( \Sigma \) takes the form \( K(\alpha_1, \ldots, \alpha_n) \) with each \( \alpha_i \) algebraic over \( K \). By the proposition \( \Sigma \) certainly takes this form. It also follows from Theorem 17 that a finite extension is algebraic. \( \square \)

So far, to construct a splitting field for \( f \) over \( K \) we have required the existence of a larger field over which \( f \) splits. Our aim is now to show that such fields always exist.

**Theorem 29** (Existence of splitting fields). Let \( f \) be a non-zero polynomial over \( K \). Then there exists an extension \( L : K \) such that \( f \) splits over \( L \). Thus by Proposition 26, \( f \) has a splitting field over \( K \).
Proof. The result is trivial if \( \deg(f) \leq 1 \), so let us assume that the degree of \( f \) exceeds 1. It follows that \( f \) has an irreducible factor \( g \) over \( K \), so \( f = gh \) for some \( h \in K[t] \). Consider the quotient ring \( K[t]/(g) \) and the element \( \alpha = t + (g) \). We know from Proposition 8 and Theorem 13 that \( K[t]/(g) \) is a simple algebraic extension of \( K \) equal to \( K(\alpha) \) and with \( \alpha \) a zero of \( g \). Thus over \( K(\alpha) \) we have \( g = (t - \alpha)g_1 \) for some \( g_1 \in K(\alpha)[t] \). By induction, \( g_1 \) splits over some extension \( M \) of \( K(\alpha) \).

The polynomial \( h \) has all its coefficients in \( M \) since \( K \subset M \). As \( \deg(h) < \deg(f) \), we can again apply the induction hypothesis to conclude that there exists an extension \( L \) of \( M \) such that \( h \) splits over \( L \). It follows that \( f \) splits over \( L \). \( \square \\

We have therefore shown that if \( f \in K[t] \) then there exists a splitting field extension \( \Sigma : K \) for \( f \). We also know that \( \Sigma \) must take the form \( K(\alpha_1, \ldots, \alpha_n) \) where the \( \alpha_i \) are the roots of \( f \) in \( \Sigma \). There is a lot of algebraic rigidity in this structure, so that if \( K(\beta_1, \ldots, \beta_n) \) is another splitting field for \( f \) over \( K \), surely the roots \( \beta_1, \ldots, \beta_n \) are in some sense ‘the same’ as \( \alpha_1, \ldots, \alpha_n \). One would hope that we could ‘pair roots off’, so that there exists a field isomorphism \( \tau : K(\alpha_1, \ldots, \alpha_n) \to K(\beta_1, \ldots, \beta_n) \) with \((\tau(\alpha_1), \ldots, \tau(\alpha_n)) \) a permutation of \((\beta_1, \ldots, \beta_n) \). This is not such a trivial task. In essence we are proving the uniqueness of splitting fields up to isomorphism.

To prove this it helps to clarify what we mean by saying that the extensions \( L : K \) and \( L' : K' \) are isomorphic.

**Definition.** Let \( i_1 : K_1 \to L_1 \) and \( i_2 : K_2 \to L_2 \) be field extensions (i.e. field monomorphisms). We say these extensions are isomorphic if all of the following hold:

(i) There exists an isomorphism \( \sigma : K_1 \to K_2 \).

(ii) There exists an isomorphism \( \tau : L_1 \to L_2 \).

(iii) We have the identity \( \tau \circ i_1 = i_2 \circ \sigma \).

The last condition can be restated in the language of category theory by saying that the following diagram commutes:

\[
\begin{array}{ccc}
K_1 & \overset{\sigma}{\longrightarrow} & K_2 \\
\downarrow{i_1} & & \downarrow{i_2} \\
L_1 & \overset{\tau}{\longrightarrow} & L_2
\end{array}
\]

To show the uniqueness of splitting extensions, our task is therefore to prove that if \( i_1 : K \to \Sigma_1 \) and \( i_2 : K \to \Sigma_2 \) are splitting extensions for the same polynomial \( f \in K[t] \), then there exists an isomorphism \( \tau : \Sigma_1 \to \Sigma_2 \) such that the following diagram commutes

\[
\begin{array}{ccc}
K & \overset{id}{\longrightarrow} & K \\
\downarrow{i_1} & & \downarrow{i_2} \\
\Sigma_1 & \overset{\tau}{\longrightarrow} & \Sigma_2
\end{array}
\]

In other words \( \tau \circ i_1 = i_2 \). It actually helps to prove something more general: that if \( i_1 : K_1 \to \Sigma_1 \) is a splitting extension for \( f \in K_1[t] \) and if \( i_2 : K_2 \to \Sigma_2 \) is a splitting extension for \( \sigma(f) \in K_2[t] \), then these extensions are isomorphic. In other words, there exist isomorphisms \( \sigma : K_1 \to K_2 \) and \( \tau : \Sigma_1 \to \Sigma_2 \) such that the following diagram commutes

\[
\begin{array}{ccc}
K_1 & \overset{\sigma}{\longrightarrow} & K_2 \\
\downarrow{i_1} & & \downarrow{i_2} \\
\Sigma_1 & \overset{\tau}{\longrightarrow} & \Sigma_2
\end{array}
\]

(To say this diagram commutes means that \( \tau \circ i_1 = i_2 \circ \sigma \).

We begin with an important special case of this result.

\[15\]Here \( \sigma(f) \) denotes the polynomial obtained from \( f \) by applying \( \sigma \) to the coefficients of \( f \).
Lemma 30. Suppose that $K_1(\alpha) : K_1$ and $K_2(\beta) : K_2$ are simple algebraic extensions, that $K_1$ is isomorphic to $K_2$ and that the minimal polynomial of $\alpha$ over $K_1$ corresponds to the minimal polynomial of $\beta$ over $K_2$ (up to isomorphism). Then the extensions are isomorphic. Moreover, given any isomorphism $\sigma : K_1 \to K_2$ we can extend this to an isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ which maps $\alpha$ to $\beta$.

Proof. Let $\sigma : K_1 \to K_2$ be an isomorphism. First note that since $\sigma$ is a ring isomorphism from $K_1$ to $K_2$, it induces a ring isomorphism from $K_1[t]$ to $K_2[t]$, obtained by applying $\sigma$ to coefficients. Also note that if $I$ is an ideal of $K_1[t]$ then $\sigma(I)$ is an ideal of $K_2[t]$ and we have an isomorphism $K_1[t]/I \cong K_2[t]/\sigma(I)$ via the map

$$f + I \mapsto \sigma(f) + \sigma(I).$$

Let $m_\alpha$ denote the minimal polynomial of $\alpha$ over $K_1$. Then we are assuming that $m_\beta = \sigma(m_\alpha)$ is the minimal polynomial of $\beta$ over $K_2$. One can check that $\sigma$ applied to the ideal $(m_\alpha)$ coincides with the ideal $(m_\beta)$. Hence from our previous remark we see that $K_1[t]/(m_\alpha)$ is isomorphic to $K_2[t]/(m_\beta)$ via the map

$$f + (m_\alpha) \mapsto \sigma(f) + (m_\beta).$$

Using this and Theorem 13, we obtain a series of isomorphisms which map $K_1(\alpha) \to K_1[t]/(m_\alpha) \to K_2[t]/(m_\beta) \to K_2(\beta)$ given by

$$f(\alpha) \mapsto f + (m_\alpha) \mapsto \sigma(f) + (m_\beta) \mapsto \sigma(f)(\beta).$$

One can check that the resulting isomorphism $\tau : K_1(\alpha) \to K_2(\beta)$ satisfies $\tau|K_1 = \sigma$ and $\tau(\alpha) = \beta$. □

We apply this lemma iteratively to obtain the following theorem.

Theorem 31 (Uniqueness of splitting fields). Let $\sigma : K_1 \to K_2$ be a field isomorphism and let $f \in K_1[t]$. Suppose that $\Sigma_1 : K_1$ is a splitting extension for $f$ and that $L_2 : K_2$ is an extension over which $\sigma(f)$ splits. Then there exists a monomorphism $\tau : \Sigma_1 \to L_2$ which restricts to $\sigma$ on $K_1$. Moreover, if $L_2 = \Sigma_2$ is a splitting field for $\sigma(f)$ over $K_2$, then $\Sigma_1 : K_1$ and $\Sigma_2 : K_2$ are isomorphic extensions via

$$\begin{array}{ccc}
K_1 & \sigma \to & K_2 \\
\downarrow & & \downarrow \\
\Sigma_1 & \tau \to & \Sigma_2
\end{array}$$

Proof. We proceed by induction on $n = \deg(f)$. Since $\Sigma_1$ is a splitting field for $f$ over $K_1$, we have that $\Sigma_1 = K(\alpha_1, \ldots, \alpha_n)$ where $f = \lambda(t - \alpha_1) \cdots (t - \alpha_n)$ and $\lambda$ is the leading coefficient of $f$. Let $m_1$ denote the minimal polynomial of $\alpha_1$ over $K_1$. Then $m_1|f$, so $\sigma(m_1)|\sigma(f)$ and $\sigma(m_1)$ must therefore split over $L_2$. Let $\beta_1$ be a zero of $\sigma(m_1)$ in $L_2$. Since $\sigma$ is an isomorphism, we see that $\sigma(m_1)$ is monic irreducible over $K_2$. Thus $\sigma(m_1)$ is the minimal polynomial for $\beta_1$ over $K_2$. We now apply Lemma 30 to deduce that there exists an isomorphism $\sigma_1 : K_1(\alpha_1) \to K_2(\beta_1)$ which restricts to $\sigma$ on $K_1$. Let $K_1' = K_1(\alpha_1)$ and $K_2' = K_2(\alpha)$ and let $g \in K_1'[t]$ be the quotient of $f$ on division by $(t - \alpha_1)$, so that $\sigma_1(g)$ splits over $L_2$. We can therefore apply the induction hypothesis to conclude that there exists an isomorphism $\tau : \Sigma_1 \to L_2$ which restricts to $\sigma_1$ on $K_1'$, and thus restricts to $\sigma$ on $K_1$.

Finally, suppose that $L_2 = \Sigma_2$ is a splitting field for $\sigma(f)$ over $K_2$. We claim that $\tau : \Sigma_1 \to \Sigma_2$ is then an isomorphism. From the first part of the theorem, it suffices to establish surjectivity, i.e. that $\tau(\Sigma_1) \supset \Sigma_2$. This follow from the fact that $\sigma(f)$ splits over $\tau(\Sigma_1)$. □

Combining the results from Proposition 20 to Theorem 31, we see that given a polynomial $f \in K[t]$ there exists a splitting field extension $\Sigma : K$ for $f$, and this extension is unique up to isomorphism.
Example (The splitting field of \( t^4 - 2 \) over \( \mathbb{Q} \)). Let \( \alpha = \sqrt[4]{2} \). Over \( \mathbb{C} \) we can factorise \( t^4 - 2 \) as

\[
(t - \alpha)(t + \alpha)(t - i\alpha)(t + i\alpha).
\]

Thus \( \Sigma = \mathbb{Q}(\alpha, -\alpha, i\alpha, -i\alpha) = \mathbb{Q}(\alpha, i\alpha) \) is a splitting field for \( t^4 - 2 \) over \( \mathbb{Q} \). Clearly \( \mathbb{Q}(\alpha, i\alpha) \subset \mathbb{Q}(\alpha, i) \). However, since

\[
i = \frac{i\alpha \times \alpha^3}{2} \in \mathbb{Q}(\alpha, i\alpha),
\]

we in fact have \( \mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\alpha, i) \).

For later purposes, let us calculate the degree of some intermediate fields between \( \mathbb{Q} \) and \( \mathbb{Q}(\alpha, i) \). The polynomial \( t^4 - 2 \) is irreducible over \( \mathbb{Q} \) (Eisenstein with \( p = 2 \)). Thus \( [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(t^4 - 2) = 4 \). The polynomial \( t^2 + 1 \) is irreducible over \( \mathbb{Q} \) (it has no roots in \( \mathbb{Q} \)), thus \( [\mathbb{Q}(i) : \mathbb{Q}] = 2 \). If \( [\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)] = 1 \) then \( i \in \mathbb{Q}(\alpha) \subset \mathbb{R} \), which is a contradiction. Thus \( [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2 \) (it is at most 2 since \( [\mathbb{Q}(i) : \mathbb{Q}] = 2 \)). It follows from the tower law that \( [\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8 \). Again using the tower law, we deduce that \( [\mathbb{Q}(\alpha, i) : \mathbb{Q}(i)] = 4 \). We summarise our deliberations in the following diagram, where the number next to an arrow indicates the degree of the extension.

\[
\begin{array}{c}
\mathbb{C} \\
\infty \\
\downarrow \\
\downarrow \\
\downarrow \\
\downarrow \\
\downarrow \\
\downarrow \\
\downarrow \mathbb{Q}(i) \\
\downarrow 2 \\
\downarrow 8 \\
\downarrow 4 \\
\downarrow 2 \\
\downarrow \mathbb{Q}(\alpha) \\
\downarrow \\
\downarrow \mathbb{Q}(\alpha, i) \\
\downarrow 4 \\
\downarrow 2 \\
\downarrow \mathbb{Q} \\
\end{array}
\]

(6.1)

Definition (Normal extension). We say the extension \( L : K \) is normal if every irreducible polynomial \( f \in K[t] \) with a zero in \( L \) also splits over \( L \).

Examples. The extension \( \mathbb{C} : \mathbb{Q} \) is normal by the fundamental theorem of algebra. The extension \( \mathbb{R} : \mathbb{Q} \) is not normal since \( t^4 - 2 \) is irreducible over \( \mathbb{Q} \) with a zero in \( \mathbb{R} \), but does not split over \( \mathbb{R} \) (it has two complex roots).

Theorem 32. An extension \( L : K \) is normal and finite if and only if \( L \) is the splitting field for some polynomial over \( K \).

Proof. Suppose \( L : K \) is normal and finite. By the form of finite extensions (Theorem 17), we see that \( L \) takes the form \( K(\alpha_1, \ldots, \alpha_n) \) for some \( \alpha_i \) all algebraic over \( K \). Let \( m_i \) denote the minimal polynomial of \( \alpha_i \) over \( K \). Then \( f = m_1 \ldots m_n \in K[t] \) and \( f \) splits over \( L \) by normality. Moreover if \( L : M : K \) and \( f \) splits over \( M \) then (by the fundamental theorem of algebra) \( \alpha_i \in M \) for all \( i \), hence \( M \supseteq K(\alpha_1, \ldots, \alpha_n) = L \). It follows that \( L \) is indeed a splitting field for \( f \) over \( K \).

Conversely, suppose that \( L \) is a splitting field for \( f \in K[t] \). The \( L = K(\alpha_1, \ldots, \alpha_n) \) where the \( \alpha_i \) are the roots of \( f \). Hence \( L \) is finitely generated with each generator algebraic over \( K \), thus \( L : K \) is a finite extension by Theorem 17. It remains to prove normality. Let \( g \in K[t] \) be irreducible over \( K \) with \( g(\alpha) = 0 \) for some \( \alpha \in L \). We wish to show that \( g \) splits over \( L \). By Theorem 29 there exists an extension \( M \) of \( L \) over which \( g \) splits. We’re done if we can show that all the roots of \( g \) in \( M \) also lie in \( L \). To this end, let \( \beta \in M \) with \( g(\beta) = 0 \). Since \( \alpha \) and \( \beta \) both have the same minimal polynomial over \( K \), Lemma 30 shows there exists an isomorphism \( \sigma : K(\alpha) \to K(\beta) \) which restricts to the identity on \( K \) and maps \( \alpha \) to \( \beta \). Since \( L \) is a splitting field for \( f \) over \( K \), we see that \( L(\alpha) \) is a splitting field for \( f \) over \( K(\alpha) \) and \( L(\beta) \) is a splitting field for \( f = \sigma(f) \) over \( K(\beta) \). Hence by uniqueness of splitting fields (Theorem 31), there exists an isomorphism \( \tau : L(\alpha) \to L(\beta) \) which restricts to \( \sigma \) on \( K(\alpha) \). It follows that the extensions
\[ L(\alpha) : K(\alpha) \text{ and } L(\beta) : K(\beta) \text{ are isomorphic. In particular } [L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)]. \]

By the tower law, we therefore have that
\[ [L(\beta) : L] = \frac{[L(\beta) : K(\beta)]}{[L : K(\beta)]} = \frac{[L(\beta) : K(\beta)]}{[L : K]/[K(\beta) : K]} = \frac{[L(\alpha) : K(\alpha)]}{[L : K]/[K(\alpha) : K]} = [L(\alpha) : L] = 1. \]

Thus \( \beta \in L \) as required. \( \square \)

**Corollary 33.** Let \( L : M : K \) be a tower of field extensions and suppose that \( L : K \) is a finite normal extension. Then \( L : M \) is also a finite normal extension.

**Proof.** From Theorem 32 we have that \( L : K \) is a splitting extension for some \( f \in K[t] \). Since \( f \in M[t] \) also, \( L : M \) is also a splitting extension for \( f \). \( \square \)

7. The Galois Group of an Extension

So far we have studied finite extensions \( L : K \) through their vector space structure alone. This is not subtle enough - all vector spaces of dimension \( n \) over \( K \) are isomorphic. One of the most important insights of Galois theory is that the structure of an extension is determined by its symmetries.

What are symmetries in this case? They are bijections \( \sigma : L \to L \) which leave all polynomial equations over \( K \) invariant and respect the field structure of \( L \). We say \( \sigma : L \to L \) is an automorphism of \( L \) if it is a bijective isomorphism from a field to itself. The set of all automorphisms of \( L \) forms a group \( \text{Aut}(L) \) under composition.

Let \( K \) be a subfield of \( L \). A \( K \)-automorphism of \( L \) is an element \( \sigma \) of \( \text{Aut}(L) \) which fixes \( K \) in the sense that \( \sigma|_K = \text{id}_K \). The set of \( K \)-automorphisms of \( L \) form a subgroup of \( \text{Aut}(L) \), denoted \( \text{Gal}(L : K) \) and called the Galois group of \( L \) over \( K \). When \( L \) is clear from the context, we write \( K^* \) for \( \text{Gal}(L : K) \).

**Example** (\( \text{Gal}(\mathbb{C} : \mathbb{R}) \)). Let \( \sigma \in \text{Gal}(\mathbb{C} : \mathbb{R}) \). Then \( 0 = \sigma(0) = \sigma(i^2 + 1) = \sigma(i)^2 + 1 \). Thus \( \sigma(i) = \pm 1 \). If \( \sigma(i) = i \), then for all complex numbers \( z = a + ib \) with \( a, b \in \mathbb{R} \) we have \( \sigma(z) = a + ib = z \). Thus \( \sigma = \text{id}_{\mathbb{C}} \) and clearly this is an element of \( \text{Gal}(\mathbb{C} : \mathbb{R}) \). If on the other hand we have \( \sigma(i) = -i \), then \( \sigma(a + ib) = a - ib \), so that \( \sigma \) is complex conjugation, which is again clearly an element of \( \text{Gal}(\mathbb{C} : \mathbb{R}) \). Therefore \( \text{Gal}(\mathbb{C} : \mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \).

**Example** (\( \text{Gal}(\mathbb{Q}(2^{1/3}) : \mathbb{Q}) \)). Let \( \alpha = \sqrt[3]{2} \). As in the previous example, if \( \sigma \in G := \text{Gal}(\mathbb{Q}(2^{1/3}) : \mathbb{Q}) \) then one can show that \( \sigma(\alpha) \) must be a real root of \( t^3 - 2 \). Since \( \alpha \) is the only such real root, it follows that \( \sigma(\alpha) = \alpha \). As 1, \( \alpha, \alpha^2 \) form a basis for this extension over \( \mathbb{Q} \), we deduce that there is only one element of \( G \), namely the identity automorphism. Thus \( G \) is the trivial group.

**Remark.** For a finitely generated algebraic extension\(^{16}\) \( L = K(\alpha_1, \ldots, \alpha_n) \) of \( K \), the elements \( \sigma \in \text{Gal}(L : K) \) are completely determined by their values on \( \alpha_1, \ldots, \alpha_n \). This is because the non-negative powers of \( \alpha_i \) span \( K(\alpha_i) \) as a vector space over \( K \), hence by the proof of the tower law, the monomials \( \alpha_1^{i_1} \cdots \alpha_n^{i_n} \) span \( K(\alpha_1, \ldots, \alpha_n) \).

**Proposition 34.** Let \( f \in K[t] \) and \( \sigma \in \text{Gal}(L : K) \). Then for all \( \alpha \in L \) we have \( f(\alpha) = 0 \) if and only if \( f(\sigma(\alpha)) = 0 \). In particular, \( f \) is the minimal polynomial for \( \alpha \) over \( K \) if and only if \( f \) is the minimal polynomial for \( \sigma(\alpha) \) over \( K \).

**Proof.** Exercise. \( \square \)

The above result says that \( \text{Gal}(L : K) \) permutes those roots of \( f \in K[t] \) which lie in \( L \). When \( f \) is irreducible over \( K \) and \( L = \Sigma \) is a splitting field for \( f \) over \( K \), then \( \text{Gal}(L : K) \) in fact permutes all the roots of \( f \) transitively.

**Proposition 35.** Let \( f \in K[t] \) be irreducible and \( \Sigma \) be a splitting field for \( f \) over \( K \). Then \( \text{Gal}(\Sigma : K) \) permutes the roots of \( f \) in \( \Sigma \) transitively. In other words, for \( \alpha, \beta \in L \) with \( f(\alpha) = f(\beta) = 0 \) there exists \( \tau \in \text{Gal}(\Sigma : K) \) such that \( \sigma(\alpha) = \beta \).

\(^{16}\)Equivalently, an extension of finite degree.
**Proof.** By Lemma 30 we can extend the identity $id_K$ to an isomorphism $\sigma : K(\alpha) \to K(\beta)$ which maps $\alpha$ to $\beta$. By uniqueness of splitting fields (Theorem 31) we can then extend $\sigma$ to an isomorphism $\tau : \Sigma \to \Sigma$. Then $\tau \in \text{Gal}(\Sigma : K)$ and $\tau(\alpha) = \beta$. \(\square\)

**Example.** Let $\alpha = \sqrt[4]{2}$. We saw in the last section that $\Sigma = \mathbb{Q}(\alpha, i) = \mathbb{Q}(\alpha, -\alpha, i\alpha, -i\alpha)$ is a splitting field for $t^4 - 2$ over $K = \mathbb{Q}$. By the above remark and Proposition 34, each $\sigma \in \text{Gal}(\Sigma : K)$ is completely determined by how it permutes the roots $\alpha, -\alpha, i\alpha, -i\alpha$. We therefore deduce that $\text{Gal}(\Sigma : K)$ is isomorphic to a subgroup of $S_4$. By Proposition 35 this must be a transitive subgroup of $S_4$.

The function $\ast$ maps a subfield $K$ of $L$ to a subgroup $K^\ast = \text{Gal}(L : K)$ of $\text{Aut}(L)$. Can we reverse $\ast$? Given a subgroup $G \leq \text{Aut}(L)$ define $L^G = \{ x \in L : (\forall \sigma \in G)[\sigma(x) = x] \}$. One can check that $L^G$ is a subfield of $L$, called the **fixed field** of $G$. When $L$ is clear from the context we write $G^\dagger$ for $L^G$.

We now state a number of properties of $\ast$ and $\dagger$. These are simple deductions which we leave as exercises for the reader (although we proved them in the lectures).

The maps $\ast$ and $\dagger$ reverse inclusions, so that if $K, M$ are subfields of $L$ then

$$ K \subset M \implies K^\ast \supset M^\ast. \quad (7.1) $$

Similarly, if $H, G$ are subgroups of $\text{Aut}(L)$ then

$$ H \subset G \implies H^\dagger \supset G^\dagger. \quad (7.2) $$

For any subfield $K$ of $L$ we have

$$ K \subset K^\dagger. \quad (7.3) $$

For any subgroup $G$ of $\text{Aut}(L)$ we have

$$ G \subset G^\dagger. \quad (7.4) $$

We always have the identities

$$ K^\ast = K^{\dagger\ast} \quad \text{and} \quad G^\dagger = G^{\dagger\ast} \quad (7.5) $$

The image of $\ast$ equals the set

$$ \text{Im}(\ast) = \{ G : G^{\dagger\ast} = G \}. \quad (7.6) $$

The image of $\dagger$ equals the set

$$ \text{Im}(\dagger) = \{ K : K^\ast = K \}. \quad (7.7) $$

Finally:

The maps $\ast$ and $\dagger$ induce inverse bijections between $\text{Im}(\ast)$ and $\text{Im}(\dagger)$. \(7.8\)

**Definition** (Galois extension). An extension $L : K$ is called **Galois** if $K^{\dagger\ast} = K$. In words: no element of $L \setminus K$ is fixed by the $K$-automorphisms of $L$.

**Examples.**

- Recall that $\text{Gal}(\mathbb{C} : \mathbb{R})$ consists of the identity and complex conjugation. Since the only complex numbers fixed by conjugation are the reals, we see that $\mathbb{C} : \mathbb{R}$ is Galois.
- Let $\alpha = \sqrt[3]{3}$. Recall that $\text{Gal}(\mathbb{Q}(\alpha) : \mathbb{Q})$ is the trivial group consisting solely of the identity. Therefore every element of $\mathbb{Q}(\alpha)$ is fixed by the $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\alpha)$, so this extension is far from being Galois.

We aim to prove the following alternative (numerical) characterisation of when an extension is Galois.

$$ L : K \text{ is Galois} \iff [L : K] = |\text{Gal}(L : K)|. \quad (7.9) $$

In fact, we eventually show that $[L : K]$ is always at least as large as $|\text{Gal}(L : K)|$, so Galois extensions are those whose Galois group is as large as possible.
We prove (7.9) using a series of arguments with the flavour of abstract linear algebra. First a definition.

**Definition.** (The vector space $L^S$). Let $L$ be a field and $S$ a non-empty set. Then the set of functions $f : S \to L$ has the structure of an $L$-vector space when functions $f$ are regarded as tuples $(f(x))_{x \in S}$ with addition and scalar multiplication defined in the obvious manner.

**Lemma 36** (Dedekind’s lemma). The monomorphisms $\sigma : K \to L$ are linearly independent over $L$.

**Proof.** Suppose otherwise. Then there exist monomorphisms $\sigma_1, \ldots, \sigma_n : K \to L$ and $\lambda_1, \ldots, \lambda_n \in L$ not all zero such that

$$0 = \lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n. \quad (7.10)$$

Let $n$ be minimal with respect to the existence of such a dependence. Then all $\lambda_i$ are non-zero. Since $\sigma_{n-1}$ and $\sigma_n$ are distinct, there exists $y \in L$ with $\sigma_{n-1}(y) \neq \sigma_n(y)$. Evaluating (7.10) at $yx$ with $x \in L$ arbitrary, we deduce that

$$0 = \lambda_1\sigma_1(y)\sigma_1 + \cdots + \lambda_n\sigma_n(y)\sigma_n. \quad (7.11)$$

Multiplying (7.10) through by $\sigma_n(y)$ and subtracting the resulting identity from (7.11), we conclude that

$$0 = \lambda_1(\sigma_1(y) - \sigma_n(y))\sigma_1 + \cdots + \lambda_{n-1}(\sigma_{n-1}(y) - \sigma_n(y))\sigma_n.$$ 

Since $\lambda_{n-1}(\sigma_{n-1}(y) - \sigma_n(y)) \neq 0$, we have contradicted the minimality of $n$. \hfill $\Box$

**Theorem 37.** Let $L$ be a field and $G$ a subgroup of Aut($L$). Then $[L : G^1] = |G|$.

**Proof.** Let $B$ be a basis for $L$ over $G^1$. Consider the (possibly infinite) matrix with entries in $L$ defined by

$$M = \left(g(x)\right)_{g \in G, x \in B}.$$ 

Here rows are indexed by elements of $G$ and columns are indexed by elements of our basis $B$.

**Claim.** (i) The rows of $M$ are linearly independent over $L$.

(ii) The columns of $M$ are linearly independent over $L$.

Since the row rank of $M$ equals the column rank, the claim yields the theorem when combined with the observations:

row rank of $M$ $=$ (number of entries in the rows of $M$) $=$ $|X| = [L : G^1]$,

column rank of $M$ $=$ (number of entries in the columns of $M$) $=$ $|G|$.

Let us therefore prove the claim. Suppose that there exists an $L$-linear dependence amongst the rows of $M$, so that there exists $g_1, \ldots, g_n \in G$ and $\lambda_1, \ldots, \lambda_n \in L$ such that for all $x \in B$ we have

$$\lambda_1g_1(x) + \cdots + \lambda_ng_n(x) = 0. \quad (7.12)$$

Note that any $G^1$-linear map $T : L \to L$ is completely determined by its values on the basis $B$. Therefore the map $\lambda_1g_1 + \cdots + \lambda_ng_n : L \to L$ is identically zero. By Dedekind’s lemma, the automorphisms $g : L \to L$ are linearly independent over $L$, so we must have $\lambda_1 = \cdots = \lambda_n = 0$. Claim (i) therefore follows.

For claim (ii), let us suppose that there is an $L$-linear dependence amongst the columns of $M$. Choose $x_1, \ldots, x_n \in B$ minimal for which there exist $\lambda_1, \ldots, \lambda_n \in L$ not all zero with

$$\sum_{i=1}^n \lambda_ig(x_i) = 0$$

for all $g \in G$. By minimality, all $\lambda_i$ must be non-zero, so multiplying this linear relation through by $\lambda_i^{-1}$, we may assume that for all $g \in G$ we have

$$g(x_1) + \lambda_2g(x_2) + \cdots + \lambda_ng(x_n) = 0. \quad (7.13)$$

Applying an arbitrary $h \in G$ to either side of this expression, we deduce that for all $g \in G$ we have

$$hg(x_1) + h(\lambda_2)hg(x_2) + \cdots + h(\lambda_n)hg(x_n) = 0. \quad (7.14)$$
It is well known from group theory that multiplying a group by any of its elements permutes the group, so that \( hG = G \). Therefore (7.14) tells us that for any \( g \in G \) we have
\[
g(x_1) + h(\lambda_2)g(x_2) + \cdots + h(\lambda_n)g(x_n) = 0. \tag{7.15}
\]
Subtracting (7.13) from (7.15), we find that for any \( g \in G \) we have
\[
(h(\lambda_2) - \lambda_2)g(x_2) + \cdots + (h(\lambda_n) - \lambda_n)g(x_n) = 0. \tag{7.16}
\]
This gives a linear dependence amongst the columns of \( M \) corresponding to \( x_2, \ldots, x_n \), contradicting the minimality of \( n \) unless \( h(\lambda_i) - \lambda_i = 0 \) for all \( i \). Since \( h \in G \) is arbitrary we must have \( \lambda_i \in G^\dagger \) for all \( i \). Taking \( g = id_L \) in (7.13) therefore implies that
\[
x_1 + \lambda_2x_2 + \cdots + \lambda_nx_n = 0,
\]
and this contradicts the linear independence of \( B \) over \( G^\dagger \).

\[\square\]

Corollary 38.

(i) We have the inequality \( |\text{Gal}(L : K)| \leq [L : K] \), with equality if and only if \( L : K \) is Galois.

(ii) If \( G \) is a finite subgroup of \( \text{Aut}(L) \), then \( G^\dagger = G \).

Proof. (i) By Theorem 37 we have
\[
[L : K^\dagger] = |K^\dagger| = |\text{Gal}(L : K)|.
\]
Since \( K \subset K^\dagger \) we also have \( [L : K^\dagger] \leq [L : K] \), with equality iff \( K = K^\dagger \), i.e. iff \( L : K \) is Galois.

(ii) We know that \( G \subset G^\dagger \). Also by Theorem 37 we have
\[
|G| = [L : G^\dagger] = [L : G^\dagger^\dagger] = |G^\dagger^\dagger|.
\]
Hence if \( G \) is finite, then \( G = G^\dagger^\dagger \).

\[\square\]

Example. Let \( L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) and \( K = \mathbb{Q} \). Any element of \( \text{Aut}(L) \) fixes \( \mathbb{Q} \) (since \( \sigma(1) = 1 \) for all \( \sigma \in \text{Aut}(L) \) and \( L \) has characteristic zero). Thus \( \text{Gal}(L : K) = \text{Aut}(L) \).

One can check\(^{17}\) that \( \sqrt{3} \notin \mathbb{Q}(\sqrt{2}) \), hence \( \sqrt{3} \) has minimal polynomial \( t^2 - 3 \) over \( \mathbb{Q}(\sqrt{2}) \). Using the proof of the tower law, we see that \( 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \) then constitute a basis for \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) over \( \mathbb{Q} \). It follows that each element of \( \text{Aut}(L) \) is completely determined by its values on \( \sqrt{2} \) and \( \sqrt{3} \). Since each \( \sigma \in \text{Gal}(L : K) \) permutes roots of polynomials over \( K \), we see that \( \sigma(\sqrt{2}) = \pm \sqrt{2} \) and \( \sigma(\sqrt{3}) = \pm \sqrt{3} \). There are therefore four possibilities for \( \sigma \):
\[
\begin{align*}
\sigma_0(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \\
\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}, \\
\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}, \\
\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6},
\end{align*}
\]
where \( a, b, c, d \in \mathbb{Q} \). One can check that each of these maps is a genuine automorphism of \( L \). Moreover, each satisfies \( \sigma_i^2 = id \). Therefore \( \text{Gal}(L : K) \cong C_2 \times C_2 \), the Klein 4-group (here \( C_n \) denotes the cyclic group of order \( n \)).

\(^{17}\)Mimic the proof that \( \sqrt{2} \notin \mathbb{Q} \).
Let us consider fixed fields of subgroups:

\[ L^{\text{Aut}(L)} = \mathbb{Q}, \]
\[ L^{\{\text{id}, \sigma_1\}} = \mathbb{Q}(\sqrt{3}), \]
\[ L^{\{\text{id}, \sigma_2\}} = \mathbb{Q}(\sqrt{2}), \]
\[ L^{\{\text{id}, \sigma_3\}} = \mathbb{Q}(\sqrt{6}), \]
\[ L^{\text{id}} = \mathbb{Q}(\sqrt{2}, \sqrt{3}). \]

Notice that \(|\text{Gal}(L : K)| = 4 = [L : K]|\), so \(L : K\) is Galois. Later, we show that since \(L : K\) is finite and Galois, all intermediate fields between \(L\) and \(K\) correspond to fixed fields of subgroups. Thus we have given a complete description of subfields of \(\mathbb{Q}(\sqrt{2}, \sqrt{3})\).

**References**