MA4203 Galois Theory

Notes by Chan Heng Huat

Contents

References

The main reference is "Galois Theory" by David A. Cox. Other references include "Galois Theory" by J. Rotman, "Galois Theory" by E. Artin, "A course in Galois Theory" by D.J.H. Darling and "Galois Theory" by I. Stewart.

1 Cubic Equations

1.1 The well known quadratic formula

Let $\mathbf{C}$ be the set of complex numbers and x be a complex variable. A polynomial over $\mathbf{C}$ is an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_n \neq 0$ and $a_j \in \mathbf{C}, 0 \leq j \leq n$. The *degree of a non-zero polynomial* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is defined to be n. Note that the degree of the "constant polynomial" $p(x) = a_0$ where $a_0 \neq 0$ is 0. The degree of $p(x) = 0$ is undefined. (It is sometimes defined as $-\infty$.)

A polynomial of degree $n \geq 1$ is said to be *monic* if $a_n = 1$. In general, we may replace $\mathbf{C}$ by any commutative ring with identity R and define a polynomial of degree n over R as an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

with $a_j \in R$ for $0 \leq j \leq n$ and $a_n \neq 0$.

A complex number α is said to be a solution of the polynomial equation

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

where $a_j \in \mathbf{C}, 0 \leq j \leq n$, if

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

Since $\mathbf{C}$ is a field and $a_n \neq 0$, we may divide the polynomial equation by a_n and consider polynomial equation where the polynomial is monic. The solutions to the polynomial equation are called the roots or zeroes of the polynomial.

When $n = 2$, we learn from high school (or secondary school) that the solution to

$$x^2 + bx + c = 0, \tag{1.1}$$

is

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}. \tag{1.2}$$

In order to derive (1.2), we first set $x = y - b/2$ and rewrite (1.1) as

$$\left(y - \frac{b}{2}\right)^2 + b\left(y - \frac{b}{2}\right) + c = 0,$$

which simplifies as

$$y^2 + c - \frac{b^2}{4} = 0.$$

This yields

$$y = \pm\sqrt{\frac{b^2}{4} - c},$$

which implies that

$$x = -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} - c} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Remark 1.1 The derivation of the quadratic formula is usually done by "completing the square". Here, we emphasize on the removal of the coefficient of x in (1.1).

1.2 Cardan's formulas for the cubic equation

A cubic monic polynomial equation is of the form

$$x^3 + bx^2 + cx + d = 0. \tag{1.3}$$

Motivated by our approach in the previous section, we will first remove the x^2 term by letting $x = y - b/3$. The substitution yields

$$y^3 + py + q = 0 \tag{1.4}$$

with

$$p = -\frac{b^2}{3} + c$$

and

$$q = \frac{2}{27}b^3 - \frac{bc}{3} + d.$$

The above discussion shows that any cubic polynomial equation can be written in the form (1.4). The polynomial equation (1.4) is called a *reduced cubic polynomial equation*. In order to find the solutions of a cubic polynomial equation, it suffices to find the solutions of the reduced cubic polynomial equation.

When $p = 0$, (1.4) has solutions $-q^{1/3}$, $-\omega q^{1/3}$ and $-\omega^2 q^{1/3}$, where $\omega = e^{2\pi i/3}$. We will next assume that $p \neq 0$ and determine the solutions of (1.4).

Let $y = u + v$ and observe that (1.4) takes the form

$$y^3 + py + q = u^3 + v^3 + 3uv(u + v) + p(u + v) + q = 0. \tag{1.5}$$

Suppose u and v are chosen such that

$$3uv = -p. \tag{1.6}$$

Then we find from (1.5) that

$$u^3 + v^3 + q = u^3 + \left(\frac{-p}{3u}\right)^3 + q = 0 \tag{1.7}$$

where we have used (1.6) and the fact that $p \neq 0$ (which implies that $u \neq 0$). This yields

$$u^6 + qu^3 - \frac{p^3}{27} = 0. \tag{1.8}$$

This implies that

$$u^3 = -\frac{q}{2} \pm \frac{\sqrt{q^2 + 4p^3/27}}{2}.$$

Let

$$\delta_3 = q^2 + \frac{4p^3}{27}.$$

The solutions to (1.8) are then contained in the set

$$\{\omega^j z_1, \omega^j z_2 | 1 \leq j \leq 3\} \tag{1.9}$$

where

$$z_1 = \sqrt[3]{-\frac{q}{2} + \frac{\sqrt{\delta_3}}{2}} \text{ and } z_2 = \sqrt[3]{-\frac{q}{2} - \frac{\sqrt{\delta_3}}{2}}.$$

Note that the cube roots in z_1 and z_2 are chosen so that

$$z_1 z_2 = -\frac{p}{3}$$

since

$$z_1^3 z_2^3 = -\frac{p^3}{27}.$$

Because of the above relation between z_1 and z_2, the six solutions in (1.9) pair up to yield three solutions for (1.4). Therefore,

$$y_1 = z_1 - \frac{p}{3z_1} = z_1 + z_2.$$

The other two solutions of the cubic monic polynomial equation are

$$y_2 = \omega z_1 + \omega^2 z_2$$

and

$$y_3 = \omega^2 z_1 + \omega z_2.$$

EXAMPLE 1.1 [p. 209, Rotman, Advanced Modern Algebra]

Consider the polynomial equation

$$x^3 - 15x - 126 = 0.$$

Here $p = -15, q = -126$. We may let $z_1 = 1$ and $z_2 = 5$. The solutions of the polynomial equation are

$$6, 5\omega + \omega^2 = -3 + 2i\sqrt{3}, 5\omega^2 + \omega = -3 - 2i\sqrt{3}.$$

1.3 Permutations of roots

In the previous section, we have seen that the solutions of $y^3 + py + q = 0$ are

$$\begin{aligned} y_1 &= z_1 + z_2, \\ y_2 &= \omega z_1 + \omega^2 z_2 \end{aligned}$$

and

$$y_3 = \omega^2 z_1 + \omega z_2,$$

where

$$z_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{\delta_3}\right)}$$

and

$$z_2 = -\frac{p}{3z_1} = \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{\delta_3}\right)}.$$

We now express z_1 and z_2 in terms of y_1, y_2 and y_3 and arrive at the following six solutions of $z^6 + qz^3 - p^3/27 = 0$:

$$\begin{aligned} z_1 &= \frac{1}{3}\left(y_1 + \omega^2 y_2 + \omega y_3\right), \\ z_2 &= \frac{1}{3}\left(y_1 + \omega y_2 + \omega^2 y_3\right), \\ \omega z_1 &= \frac{1}{3}\left(\omega y_1 + y_2 + \omega^2 y_3\right), \\ \omega z_2 &= \frac{1}{3}\left(\omega y_1 + \omega^2 y_2 + y_3\right), \\ \omega^2 z_1 &= \frac{1}{3}\left(\omega^2 y_1 + \omega y_2 + y_3\right), \end{aligned} \tag{1.10}$$

and

$$\omega^2 z_2 = \frac{1}{3}\left(\omega^2 y_1 + y_2 + \omega y_3\right).$$

Let S_n be the set of permutations on $\{1, 2, \cdots, \quad n\}$. It is known that S_n, together with the composition of permutations, forms a group. A cycle

$$(a_1 \quad a_2 \quad \cdots \quad a_{\ell-1} \quad a_\ell)$$

is used to represent the map sending a_1 to a_2, a_2 to $a_3, \cdots, a_{\ell-1}$ to a_ℓ and a_ℓ to a_1. An element $\sigma \in S_n$ is represented by a product of cycles. A transposition of S_n is a cycle of the form $(a_1 \quad a_2)$. If $\sigma \in S_n$, then σ can be expressed as a product of transpositions. In other words, $\sigma = \tau_1\tau_2 \cdots \tau_t$ for some transpositions $\tau_j, 1 \leq j \leq t$. The representation of σ in terms of transpositions is not unique. However, the parity of t is invariant regardless of the representation. Therefore, we may define $\text{sgn} : S_n \to \{\pm 1\}$ as $\text{sgn}(\sigma) = (-1)^t$. The function sgn is a homomorphism of groups from S_n to the group of two elements it is known as the signum on S_n.

EXAMPLE 1.2 The group

$$S_3 = \{(1)(2)(3), (1 \quad 2 \quad 3), (1 \quad 3 \quad 2), (1 \quad 2)(3), (1 \quad 3)(2), (2 \quad 3)(1)\}.$$

Note that $\text{sgn}((1 \quad 2 \quad 3)) = 1, \text{sgn}((1 \quad 2)(3)) = -1$. Note that the group

$$A_3 = \{\sigma \in S_3 \big| \text{sgn}(\sigma) = 1\}$$

forms a subgroup of S_3. In general, the set

$$A_n = \{\sigma \in S_n \big| \text{sgn}(\sigma) = 1\}$$

forms a subgroup of S_n.

Let G be a group and X be a set. We say that $(G, *)$ acts on X if there exists

$$\bullet : G \times X \to X$$

such that

(i) $g_1 \bullet (g_2 \bullet x) = (g_1 * g_2) \bullet x$,
(ii) $1_G \bullet x = x$.

Note that we write $g \bullet x$ instead of $\bullet(g, x)$.

The group S_3 acts on the roots $\{y_1, y_2, y_3\}$ of $y^3 + py + q$ by

$$\sigma \circ y_j = y_{\sigma(j)}.$$

With this definition (extended by linearity), we see that

$$(1 \quad 2) \circ z_1 = (1 \quad 2) \circ (y_1 + \omega^2 y_2 + \omega y_3) = y_2 + \omega^2 y_1 + \omega y_3 = \omega^2 z_2$$

and

$$(1 \quad 2 \quad 3) \circ z_1 = \omega^2 z_1.$$

By direct computations, we find that S_3 acts *transitively* on the roots of

$$z^6 + qz^3 - p^3/27.$$

It is important to note that $(1 \quad 2 \quad 3) \circ z_i^3 = z_i^3$ for $i = 1$ and 2. This means that z_i^3 is "fixed" by the cyclic subgroup generated by $(1 \quad 2 \quad 3)$ and this is the main reason why a cubic polynomial equation is solvable as one can predict that z_i^3 lies in a "quadratic field extension" over $\mathbf{Q}$. We will make these statements precise as we progress in our course.

1.4 Quartic polynomials

The roots of a reduced quartic polynomial x^4+qx^2+rx+s can also be expressed in terms of "radicals", which are expressions involving $\sqrt[m]{f(q,r,s)}$, where $f(q,r,s)$ are rational functions involving q, r and s. Let $\alpha_j, j = 1, 2, 3, 4$ be the roots of the above quartic polynomial. Let

$$z_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),$$
$$z_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),$$

and

$$z_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

If

$$\sigma_1 = \sum_{j=1}^{4} \alpha_j,$$

$$\sigma_2 = \sum_{1 \le i < j \le 4} \alpha_i \alpha_j,$$

$$\sigma_3 = \sum_{1 \le i < j < k \le 4} \alpha_i \alpha_j \alpha_k$$

and

$$\sigma_4 = \alpha_1 \alpha_2 \alpha_3 \alpha_4.$$

Then we can show that

$$z_1 + z_2 + z_3 = 2\sigma_2 = 2q,$$

$$z_1 z_2 + z_1 z_3 + z_2 z_3 = \sigma_2^2 + \sigma_1 \sigma_3 - 4\sigma_4 = q^2 - 4s,$$

and

$$z_1 z_2 z_3 = \sigma_1 \sigma_2 \sigma_3 - \sigma_1^2 \sigma_4 - \sigma_3^2 = -r^2,$$

where we have used the fact that

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0.$$

This shows that z_1, z_2 and z_3 are roots of

$$z^3 - 2qz^2 + (q^2 - 4s)z + r^2.$$

The cubic polynomial is called a resolvent cubic of the quartic polynomial

$$x^4 + qx^2 + rx + s.$$

A quartic polynomial can have more than one resolvent cubic.

Using the formula for solving cubic polynomial equation, we are able to determine the roots $z_j, 1 \leq j \leq 3$, of the resolvent cubic. We can then retrieve $\alpha_j, j = 1, 2, 3, 4$ by first observing from the relation $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ that

$$(\alpha_1 + \alpha_2)^2 = -z_1, (\alpha_1 + \alpha_3)^2 = -z_2 \text{ and } (\alpha_1 + \alpha_4)^2 = -z_3.$$

This implies, for example, that α_1 in terms of z_1, z_2 and z_3.

$$\alpha_1 = \frac{1}{2}\left(\sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}\right).$$

The other three zeroes of the quartic polynomial are given by

$$\alpha_2 = \frac{1}{2}\left(\sqrt{-z_1} - \sqrt{-z_2} - \sqrt{-z_3}\right),$$
$$\alpha_3 = \frac{1}{2}\left(-\sqrt{-z_1} + \sqrt{-z_2} - \sqrt{-z_3}\right)$$

and

$$\alpha_4 = \frac{1}{2}\left(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}\right).$$

We emphasize here that where $-z_1, -z_2$ and $-z_3$ are not real positive numbers, we have to be careful in our choice of $\sqrt{-z_j}, 1 \leq j \leq 3$.

1.5 The Discriminant

The number $\delta_2 = b^2 - 4c$ is known as *the discriminant of the polynomial* $x^2 + bx + c$. Note that if

$$\alpha = \frac{-b + \sqrt{\delta_2}}{2} \text{ and } \beta = \frac{-b - \sqrt{\delta_2}}{2},$$

then

$$(\alpha - \beta)^2 = \delta_2.$$

In other words, the discriminant of the quadratic polynomial is the square of the difference of its two roots. This point of view allows us to define the discriminant of a polynomial of degree $n \geq 2$. This is given as follows:

DEFINITION 1.1 Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. The discriminant of $p(x)$, denoted by $\Delta(p(x))$, is defined as

$$\Delta(p(x)) = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2,$$

where $\alpha_1, \alpha_2, \cdots \alpha_n$ are the roots of $p(x)$.

We will now compute the discriminant of a reduced cubic polynomial. Write

$$z_1 = \sqrt[3]{\frac{1}{2}\left(-q + \sqrt{\delta_3}\right)} \text{ and } z_2 = \sqrt[3]{\frac{1}{2}\left(-q - \sqrt{\delta_3}\right)}.$$

Then

$$z_1^3 - z_2^3 = \frac{1}{2}\left(-q + \sqrt{\delta_3}\right) - \frac{1}{2}\left(-q - \sqrt{\delta_3}\right) = \sqrt{\delta_3}.$$

But

$$z_1^3 - z_2^3 = (z_1 - z_2)\left(z_1 - \omega z_2\right)\left(z_1 - \omega^2 z_2\right).$$

On the other hand by (1.10), we observe that

$$z_1 - z_2 = -\frac{i}{\sqrt{3}}(y_2 - y_3),$$
$$z_1 - \omega z_2 = \frac{i\omega^2}{\sqrt{3}}(y_1 - y_3)$$

and

$$z_1 - \omega^2 z_2 = -\frac{i\omega}{\sqrt{3}}(y_1 - y_2).$$

This implies that

$$\sqrt{\delta_3} = -\frac{i}{3\sqrt{3}}(y_1 - y_2)(y_1 - y_3)(y_2 - y_3),$$

or

$$\Delta(x^3 + px + q) = -27q^2 - 4p^3.$$

2 Symmetric polynomials

2.1 Polynomial rings in n variables

DEFINITION 2.1 A polynomial in $x_1, x_2, \cdots, x_n$ with coefficients in F is a finite sum of terms, which are expressions of the form $cx_1^{k_1} \cdots x_n^{k_n}$, where $c \in F$ and k_j are non-negative integers for $1 \leq j \leq n$. A term is non-zero if $c \neq 0$. The set of polynomials in n variables with coefficients in F is denoted by $F[x_1, x_2, \cdots, x_n]$.

We now introduce an important example of a function in $F[x_1, x_2, \cdots, x_n]$.

DEFINITION 2.2 Given $n \geq 2$ variables $x_1, \cdots, x_n$ over a field F, the discriminant (associated with $x_1, x_2, \cdots, x_n$) is defined as

$$\Delta(x_1, \cdots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in F[x_1, \cdots, x_n].$$

DEFINITION 2.3 The total degree of a nonzero term $cx_1^{k_1} \cdots x_n^{k_n}$ is $k_1 + k_2 + \cdots + k_n$. The total degree of a polynomial $f = f(x_1, x_2, \cdots, x_n)$ in n variables, denoted by $\deg(f)$, is the maximum of the total degree of the non-zero term of f.

EXAMPLE 2.1 The degree of $\Delta(x_1, x_2, \cdots, x_n)$ is $n(n-1)$.

EXAMPLE 2.2 Let

$$\sigma_{n,j}(x_1, x_2, \cdots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_j \leq n} x_{i_1} x_{i_2} \cdots x_{i_j}.$$

The degree of $\sigma_{n,j}$ is j.

DEFINITION 2.4 A polynomial $f \in F[x_1, x_2, \cdots, x_n]$ is homogeneous if each term in f has total degree equal to the degree of f.

EXAMPLE 2.3 If f and g are non-zero polynomial, then

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

EXAMPLE 2.4 Show that $F[x, y]$ is not a principal ideal domain.

Solution
Let $I = \{xg + yh | g, h \in F[x, y]\}$. Note that if $1 \in I$ then $1 = xg + yh$ for some $g, h \in F[x, y]$. But the degree of the left hand side is not equal to the degree of the right hand side and thus, this is not possible. Therefore $I \neq F[x, y]$. Suppose $I = k(x, y)F[x, y]$. Then $x = k(x, y)a(x, y)$ and $y = k(x, y)b(x, y)$. This means that $\deg(a(x, y)) = \deg(b(x, y)) = 0$. Therefore $x = k(x, y)c$ and $y = k(x, y)d$ with $c, d \in F$. Therefore, $x = (c/d)dk(x, y) = (c/d)y$, contradicting to the assumption that x and y are independent variables.

2.2 Elementary symmetric polynomials and symmetric polynomials

Let S_n denote the set of bijections on $\{1, 2, \cdots, n\}$. The set S_n is a group under the composition of bijections. The group S_n acts on $F[x_1, x_2, \cdots, x_n]$ in the following way:

$$\sigma \cdot f(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots x_{\sigma(n)}), \sigma \in S_n, f(x_1, \cdots, x_n) \in F[x_1, \cdots x_n].$$

DEFINITION 2.5 A polynomial $f(x_1, x_2, \cdots, x_n) \in \mathbf{C}[x_1, x_2, \cdots, x_n]$ is symmetric if

$$\sigma \cdot f(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = f(x_1, x_2, \cdots, x_n)$$

for any permutation $\sigma \in S_n$.

EXAMPLE 2.5 Another representation of $\Delta(x_1, \cdots, x_n)$ is given by

$$\Delta(x_1, \cdots, x_n) = (-1)^{n(n-1)/2} \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (x_i - x_j). \tag{2.1}$$

Given any element $\sigma \in S_n$, we know that σ is a disjoint product of cycles. Each cycle is a product of 2-cycles. More precisely,

$$(a_1\, a_2\, \cdots\, a_{n-1} a_n) = (a_1\, a_n) \cdots (a_1\, a_3)(a_1\, a_2),$$

reading the map from right to left. In order to show that $\Delta(x_1, \cdots, x_n)$ is symmetric, it suffices to show that it is invariant under the action of 2-cycle. Now, suppose $i, j \notin \{\ell, k\}$, then

$$\begin{aligned}
&(k\,\ell) \circ (x_i - x_j) = (x_i - x_j),\\
&(k\,\ell) \circ (x_k - x_j) = (x_\ell - x_j), (k\,\ell) \circ (x_\ell - x_j) = (x_k - x_j),\\
&(k\,\ell) \circ (x_j - x_k) = (x_j - x_\ell), (k\,\ell) \circ (x_j - x_\ell) = (x_j - x_k),\\
&(k\,\ell) \circ (x_k - x_\ell) = (x_\ell - x_k), (k\,\ell) \circ (x_\ell - x_k) = (x_k - x_\ell).
\end{aligned}$$

This implies, using (2.1), that

$$(k\,\ell) \circ \Delta(x_1, \cdots, x_n) = \Delta(x_1, \cdots, x_n)$$

and therefore $\Delta(x_1, \cdots, x_n)$ is a symmetric polynomial.

EXAMPLE 2.6 Given variables $x_1, x_2, \cdots, x_n$, define

$$\sigma_{n,j}(x_1, x_2, \cdots, x_n) = \sum_{1 \le m_1 < m_2 < \cdots < m_j \le n} x_{m_1} x_{m_2} \cdots x_{m_j}.$$

To see that $\sigma_{n,j}$ are symmetric polynomials, we observe that

$$\begin{aligned}
S(x, x_1, \cdots x_n) = (x - x_1) \cdots (x - x_n) =& x^n - \sigma_{n,1} x^{n-1} + \cdots + (-1)^r \sigma_{n,r} x^{n-r} \\
&+ \cdots + (-1)^n \sigma_{n,n},
\end{aligned} \tag{2.2}$$

where $\sigma_{n,j} = \sigma_{n,j}(x_1, x_2, \cdots, x_n)$. Note that for $\tau \in S_n$,

$$\tau \circ S(x, x_2, \cdots x_n) = S(x, x_{\tau(1)}, \cdots, x_{\tau(n)}) = S(x, x_1, x_2, \cdots, x_n).$$

Comparing the coefficients of x^j in the expansion of $S(x, x_1, \cdots, x_n)$ and $S(x, x_{\tau(1)}, \cdots, x_{\tau(n)})$ using (2.2), we conclude that

$$\tau \circ \sigma_{n,j}(x_1, \cdots, x_n) = \sigma_{n,j}(x_{\tau(1)}, \cdots, x_{\tau(n)}) = \sigma_{n,j}(x_1, x_2, \cdots, x_n).$$

THEOREM 2.1 Any symmetric polynomial in $F[x_1, \cdots, x_n]$ can be written as a polynomial in $\sigma_{n,1}, \cdots \sigma_{n,n}$ with coefficients in F.

Proof

Given any positive integer N, there are finitely many positive integers $k_1, k_2, \cdots, k_n$,

such that $k_1+k_2+\cdots+k_n = N$. Note that $k_j \leq N$ and so there are at most $N+1$ choices for each k_J. Therefore, the number of terms of the form $x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ with $k_1+k_2+\cdots+k_n = N$ is finite. We now order the monomials $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ as follow: We say that

$$x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} < x_1^{\ell_1}x_2^{\ell_2}\cdots x_n^{\ell_n}$$

if $k_1+\cdots+k_n < \ell_1+\cdots+\ell_n$

or

if $k_1+\cdots+k_n = \ell_1+\cdots+\ell_n$ and $k_1 < \ell_1$,

or

if $k_1+\cdots+k_n = \ell_1+\cdots+\ell_n$ and $k_1 = \ell_1, k_2 < \ell_2$,

or

$\vdots$

or

if $k_1+\cdots+k_n = \ell_1+\cdots+\ell_n$ and $k_1 = \ell_1, \cdots, k_{n-1} = \ell_{n-1}, k_n < \ell_n$.

For example, $x_1^4x_2^2x_3 < x_1^2x_2^3x_3^3$ and $x_1^4x_3x_3^2 < x_1^4x_2^2x_3$.

Note that with this ordering on monomials, any polynomial $f \in F[x_1,\cdots,x_n]$ has a leading monomial. For example, the leading monomial of $\sigma_{n,2}$ is x_1x_2. In general, the leading monomial of $\sigma_{n,j}$ is $x_1\cdots x_j$.

DEFINITION 2.6 Let $f \in F[x_1,x_2,\cdots,x_n]$. The leading monomial of f, which is called the leading term of f is denoted by $LT(f)$.

We are now ready to prove the theorem. It suffices to prove the theorem for homogeneous symmetric polynomials since any symmetric polynomial is a sum of such polynomials. Let f be a homogeneous symmetric polynomial of degree N. Suppose that

$$LT(f(x_1,x_2,\cdots,x_n)) = cx_1^{k_1}\cdots x_n^{k_n},$$

where $k_1+k_2+\cdots+k_n = N$ and $c \in F$. We claim that $k_1 \geq k_2 \geq \cdots \geq k_n$. Suppose not. Let $k_j \geq k_i$ for $i \geq j$. Then

$$x_1^{k_1}\cdots x_i^{k_i}\cdots x_j^{k_j}\cdots x_n^{k_n} < x_1^{k_1}\cdots x_i^{k_j}\cdots x_j^{k_i}\cdots x_n^{k_n}.$$

A constant multiple of the term on the right appears in $f(x_1,\cdots,x_n)$ since $f(x_1,\cdots,x_n)$ is symmetric. The above inequality contradicts the assumption that $cx_1^{k_1}\cdots x_i^{k_i}\cdots x_j^{k_j}\cdots x_n^{k_n}$ is equal to $LT(f(x_1,\cdots,x_n))$.

Suppose $k_1 \geq k_2 \geq \cdots \geq k_n \geq 0$. Now

$$LT(\sigma_{n,1}^{k_1-k_2}\sigma_{n,2}^{k_2-k_3}\cdots\sigma_{n,n-1}^{k_{n-1}-k_n}\sigma_{n,n}^{k_n}) = x_1^{k_1}\cdots x_n^{k_n}.$$

Therefore, if c is the coefficient of $x_1^{k_1}\cdots x_n^{k_n}$ in $f(x_1,\cdots,x_n)$ then $f(x_1,\cdots,x_n) - c\sigma_{n,1}^{k_1}\cdots\sigma_{n,n}^{k_n}$ is a symmetric polynomial of degree N with leading term smaller than $x_1^{k_1}\cdots x_n^{k_n}$. Repeating the process with the terms in $f(x_1,\cdots,x_n) - c\sigma_{n,1}^{k_1}\cdots\sigma_{n,n}^{k_n}$, we will eventually eliminate all monomials with degree N and conclude that $f(x_1,\cdots,x_n)$ can be expressed in the elementary symmetric polynomials. □

EXAMPLE 2.7 We now illustrate the process described in the proof above using an example. The polynomial $f(x_1,x_2,x_3) = (x_1-x_2)^2(x_2-x_3)^2(x_1-x_3)^2$ has degree 6 and

$$LT(f(x_1,x_2,x_3)) = x_1^4x_2^2.$$

By the process described in the above proof, we deduce that

$$f(x_1,\cdots,x_n) = \sigma_{3,1}^2\sigma_{3,2}^2 - 4\sigma_{3,1}^3\sigma_{3,3} - 4\sigma_{3,2}^3 + 18\sigma_{3,1}\sigma_{3,2}\sigma_{3,3} - 27\sigma_{3,3}^2.$$

Remark 2.1 It can be shown that the expression of any symmetric polynomial in terms of elementary symmetric polynomials is unique. For more details, see pp. 35–37 of "Galois Theory" by D.A. Cox.

Suppose that we have field F, a ring R containing F, and elements $\alpha_1,\alpha_2,\cdots,\alpha_n \in R$. Then the evaluation map

$$\mathcal{E}_{\alpha_1,\cdots,\alpha_n} : F[x_1,x_2,\cdots,x_n] \to R$$

is defined by

$$\mathcal{E}_{\alpha_1,\cdots,\alpha_n}(f(x_1,x_2,\cdots,x_n)) = f(\alpha_1,\alpha_2,\cdots,\alpha_n).$$

The evaluation is a ring homomorphism from $F[x_1,x_2,\cdots,x_n]$ to R.

Using the evaluation map $\mathcal{E}_{\alpha_1,\cdots,\alpha_n}$ which sends x_i to α_i, $1 \leq i \leq n$, we arrive at the following Corollary:

COROLLARY 2.2 Let $f = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n \in \mathbf{C}[x]$ with roots $\alpha_1,\cdots,\alpha_n$. Then the coefficients of $f(x)$ can be expressed in terms of its roots as

$$a_r = (-1)^r\sigma_{n,r}(\alpha_1,\cdots,\alpha_n)$$

for $r = 1,\cdots,n$.

Remark 2.2 Please note the unusual way of naming the coefficients of x^r. Instead of using a_r, we have used a_{n-r}.

3 Roots of polynomials

3.1 Field extensions

A field F is a ring such that every nonzero element has a multiplicative inverse. For any field F, we observe that $n1_F$ is the sum of n copies of 1_F.

If $n1_F = 0$ and n is the smallest positive for which this happens, then n must be a prime. For if n is not a prime then $n = ab$ and either $a1_F = 0$ or $b1_F = 0$, contradicting the minimality of n. In other words, $p1_F = 0$ for some prime p. When this happens, we say that the field F has characteristic p. If $n1_F \neq 0$ for all non-zero integers, then we say that the field F has characteristic 0. The set of complex numbers is a field of characteristic 0. The field $\mathbf{Z}/p\mathbf{Z}$ has characteristic p. Given a field F, can we construct "new fields" that contain F? To answer this question, we begin with Cauchy's construction of the complex numbers.

The complex numbers can be constructed from $\mathbf{R}[x]/(x^2+1)\mathbf{R}[x]$. If we let $\mathfrak{m} = (x^2+1)\mathbf{R}[x]$ and set

$$\alpha = x + \mathfrak{m},$$

then we find that

$$\alpha \cdot \alpha = -1 + \mathfrak{m}.$$

Note that by setting $1 = 1 + \mathfrak{m}$ and $i = x + \mathfrak{m}$, we find that

$$(a1 + bi)(c1 + di) = (ac - bd)1 + (ad + bc)i)$$

and we "recover" the set of complex numbers.

The above construction relies on the fact if R is a commutative ring with identity and $\mathfrak{m}$ is a maximal ideal of R then $R/\mathfrak{m}$ is a field. In the above example, the ideal generated by x^2+1 is a maximal ideal of $\mathbf{R}[x]$ and therefore, $\mathbf{R}[x]/(x^2+1)$ is a field. Note that the map

$$\varphi : \mathbf{R} \to \mathbf{R}[x]/(x^2+1)$$

which sends r to $r + (x^2+1)$ shows that the field

$$\mathbf{R}[x]/(x^2+1)$$

contains a field isomorphic to $\mathbf{R}$.

We now construct more fields using the idea similar to Cauchy's construction of the complex numbers.

DEFINITION 3.1 Given a ring homomorphism of fields

$$\varphi : F \to L,$$

then we say that L is a field extension of F via φ. We will usually identify F with its image $\varphi(F) = \{\varphi(a) | a \in F\} \subset L$ and write $F \subset L$.

THEOREM 3.1 If $f(x) \in F[x]$ is irreducible, then there is a extension field $F \subset L$ and $\alpha \in L$ such that $f(\alpha) = 0$.

Proof
Let $\mathfrak{m} = f(x)F[x]$ and let $\alpha = x + \mathfrak{m}$. Then $f(\alpha) = 0$ in $L = F[x]/\mathfrak{m}$. □

Recall that $\alpha \in L$ is a root of $f(x)$ if and only if $x - \alpha$ is a factor of $f(x)$. Thus, to say that a field L contains all roots of $f(x)$ is the same as saying that

$$f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$$

where $\alpha_1, \cdots, \alpha_n \in L$.

DEFINITION 3.2 Let $f(x) \in F[x]$ and L be a field extension of F. If

$$f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$$

where $\alpha_1, \cdots, \alpha_n \in L$, then we say that $f(x)$ *splits completely over* L.

The following theorem shows that for any polynomial $f(x) \in F[x]$, $f(x)$ splits completely in some field extension of F.

THEOREM 3.2 (Kronecker) Let F be any field. Let $f(x) \in F[x]$ be a polynomial of degree $n > 0$. Then there is a field extension $F \subset L$ such that $f(x)$ splits completely over L.

Proof
We will prove the theorem using induction on n, the degree of $f(x)$. If $n = 1$ then $L = F$. Suppose for any field F, the assertion is true for polynomials of degree less than n. Let $\deg(f(x)) = n$. Then $f(x) = p(x)g(x)$ for some irreducible polynomial $p(x)$ (note that $g(x)$ could be 1_F). By the induction hypothesis, there exists a field extension E_1 over F such that

$$E_1 \simeq F[x]/p(x)F[x]$$

such that $p(\alpha) = 0$ for some $\alpha \in E_1$. Note that $f(\alpha) = 0$ in E_1. Therefore

$f(x) = (x - \alpha)f_2(x)$ in $E_1[x]$. Now, the degree of $f_2(x)$ is less than n and therefore, by induction hypothesis, there exists a field extension E_2 of E_1 for which $f_2(x)$ splits. Hence, $f(x)$ splits completely in E_2. □

Remark 3.1 An element α is said to be algebraic over F if $f(\alpha) = 0$ for some $f(x) \in F[x]$. A field K is said to be algebraically closed if all elements α which are algebraic over K are already in K. In other words, all polynomials $f(x) \in K[x]$ splits completely in K. An example of such field is $\mathbf{C}$ and this is a consequence The Fundamental Theorem of Algebra states that $\mathbf{C}$ is algebraically closed. A field extension K of F is said to be an algebraic closure of F if every elements K is algebraic over F and K is algebraically closed. Given a field F, it can be shown, using Zorn's lemma, that its algebraic closure exists. In other words, if $f(x) \in F[x]$, we may regard it as a polynomial in $K[x]$ and since K is algebraically closed, $f(x)$ splits completely in K. This implies that for any field F and any polynomial $f(x) \in F[x]$, there exists an algebraic extension K of F such that $f(x)$ splits completely in K. This gives another proof of Theorem 3.2. For more details of the discussion of this approach, see Chapter 8 of D.J.H. Garling's "A course in Galois Theory".

3.2 Fundamental Theorem of Algebra

In this section, we give a proof that $\mathbf{C}$ is algebraically closed. This proof is due to L. Euler and J.L. Lagrange. (Gauss also gave a similar proof. For more details, see pages 67 to 68 of Cox's book.)

THEOREM 3.3 The following are equivalent:

(a) Every non-constant $f(x) \in \mathbf{C}[x]$ has at least one root in $\mathbf{C}$.
(b) Every non-constant $f(x) \in \mathbf{C}[x]$ splits completely in $\mathbf{C}$.
(c) Every non-constant $f(x) \in \mathbf{R}[x]$ has at least one root in $\mathbf{C}$.

Proof
To prove that (a) implies (b), we use induction on the degree of $f(x)$. When $n = 1$, we write $f(x) = ax + b = a(x - (-b/a))$ and so, $f(x)$ splits completely over $\mathbf{C}$. Next, suppose that $n > 1$ and that our assertion is true for polynomials with degree less than or equal to $n-1$. Suppose $f(x)$ is a polynomial of degree n and that $\alpha \in \mathbf{C}$ is a root of $f(x)$. Then $f(x) = (x - \alpha)g(x)$ for some polynomial $g(x)$. By induction, $g(x)$ splits completely over $\mathbf{C}$. This implies that $f(x)$ splits completely over $\mathbf{C}$.

Now, (b) implies (c) because a polynomial over $\mathbf{R}$ is a polynomial over $\mathbf{C}$ and so, $f(x)$ has at least one root in $\mathbf{C}$ since (b) holds.

Finally, we show that (c) implies (a). Assume (c). We must show that every non-constant $f(x) \in \mathbf{C}[x]$ has a root in $\mathbf{C}$. Let $f(x) = a_n x^n + \cdots + a_0$ and $\overline{f}(x) = \overline{a_n} x^n + \cdots + \overline{a_0}$. Then the polynomial $h(x) = f(x)\overline{f}(x)$ is in $\mathbf{R}[x]$. To see this, observe that

$$\overline{u(x)v(x)} = \overline{\sum_{j=0}^{\nu} c_j x^j \sum_{k=0}^{\mu} d_k x^k} = \overline{\sum_{\ell=0}^{\nu+\mu} e_\ell x^\ell},$$

where

$$e_\ell = \sum_{k+j=\ell} c_j d_k.$$

Since

$$\overline{e_\ell} = \sum_{k+j=\ell} \overline{c_j d_k} = \sum_{k+j=\ell} \overline{c_j}\,\overline{d_k},$$

we conclude that

$$\overline{u(x)v(x)} = \overline{u}(x)\overline{v}(x).$$

Applying the above to $h(x)$, we conclude that $\overline{h}(x) = h(x)$ and hence, $h(x) \in \mathbf{R}[x]$.

By (c), $h(x)$ has a root, say α, in $\mathbf{C}$. This implies that $f(\alpha)\overline{f}(\alpha) = 0$. Therefore, $f(\alpha) = 0$ or $\overline{f}(\alpha) = 0$. If $f(\alpha) = 0$, then we are done. If $\overline{f}(\alpha) = 0$ then $f(\overline{\alpha}) = 0$ and $\overline{\alpha}$ is a root of $f(x)$.

□

THEOREM 3.4 Every $f(x) \in \mathbf{R}[x]$ of odd degree has at least one root in $\mathbf{R}$.

Proof

We may assume $f(x)$ is monic and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. If $a_j = 0$ for $0 \le j \le n-1$ then $f(x)$ has a root, namely, 0. Suppose $a_j \neq 0$ for some j. Let $M = |a_0| + \cdots + |a_{n-1}| + 1 > 1$. Then

$$\begin{aligned} |a_{n-1}M^{n-1} + \cdots + a_0| &\le (|a_{n-1}| + \cdots + |a_0|)\, M^{n-1} \\ &< (1 + |a_{n-1}| + \cdots + |a_0|)\, M^{n-1} = M^n. \end{aligned}$$

This implies that

$$f(M) = M^n + a_{n-1}M^{n-1} + \cdots + a_0 > 0.$$

Similarly,

$$\begin{aligned} (-M)^n + a_{n-1}(-M)^{n-1} + \cdots + a_1(_M) + a_0 & \\ &\le -M^n + |a_{n-1}|M^{n-1} + \cdots + |a_1|M + |a_0| \\ &< -M^n + (1 + |a_{n-1} + \cdots + |a_0|)M^{n-1} = 0, \end{aligned}$$

where we have used the fact that n is odd. This implies that

$$f(-M) < 0.$$

Since $f(-M) < 0$ and $f(M) > 0$, by Intermediate Value Theorem, there exists N between $-M$ and M such that $f(N) = 0$.

□

LEMMA 3.5 Every quadratic polynomial in $\mathbf{C}[x]$ splits completely over $\mathbf{C}$.

Proof
It suffices to consider monic quadratic polynomial of the form $x^2 + bx + c$.. To show that this polynomial splits over $\mathbf{C}$, we need show that $\sqrt{b^2 - 4c} \in \mathbf{C}$. If $b^2 - 4c$ is 0, then we are done. Next, by writing $b^2 - 4c = re^{i\theta}$, we conclude that $\pm\sqrt{b^2 - 4c} = \pm\sqrt{r}e^{i\theta/2} \in \mathbf{C}$.

□

We are finally ready to prove the Fundamental Theorem of Algebra.

THEOREM 3.6 Every nonconstant $f(x) \in \mathbf{C}[x]$ splits completely over $\mathbf{C}$.

Proof
The proof follows a strategy of Euler and a clever idea first used by Laplace. Let n be the degree of f. If n is odd, then by By Theorem 3.3, it suffices to prove that Theorem 3.4, f has a root in $\mathbf{C}$.

Now, suppose n is even. Write $n = 2^m k$ where $m \geq 1$ and k is an odd positive integer. We want to prove the theorem for even n by induction on m. By Theorem 3.2, we know that there exists a field extension L of F such that

$$f(x) = \prod_{j=1}^{n} (x - \alpha_j).$$

Following Laplace's clever idea, we consider the polynomial

$$g_\lambda(x) = \prod_{1 \leq i < j \leq n} \left(x - (\alpha_i + \alpha_j) + \lambda \alpha_i \alpha_j\right).$$

Note that the degree of $g(x)$ is $n(n-1)/2 = 2^{m-1}(2^m k - 1)$. We will show that $g_\lambda(x) \in \mathbf{R}[x]$, i.e., the coefficients of $g_\lambda(x)$ are real numbers.

Consider the polynomial

$$G_\lambda(x) = \prod_{1 \leq i < j \leq n} \left(x - (x_i + x_j) + \lambda x_i x_j\right).$$

Note that

$$\begin{aligned}
&(k \quad \ell) \circ (x_i + x_j) = x_i + x_j, (k \quad \ell) \circ (x_i x_j) = x_i x_j \quad \text{if } i, j \notin \{k, \ell\},\\
&(k \quad \ell) \circ (x_k + x_j) = x_\ell + x_j, (k \quad \ell) \circ (x_k x_j) = x_\ell x_j \quad \text{if } j \notin \{k, \ell\},\\
&(k \quad \ell) \circ (x_\ell + x_j) = x_k + x_j, (k \quad \ell) \circ (x_\ell x_j) = x_k x_j \quad \text{if } j \notin \{k, \ell\},\\
&(k \quad \ell) \circ (x_k + x_\ell) = x_\ell + x_k, (k \quad \ell) \circ (x_k x_\ell) = x_\ell x_k.
\end{aligned}$$

Therefore, S_n "acts trivially" on $G_\lambda(x)$ which implies that

$$G_\lambda(x) = \sum_{k=0}^{n(n-1)/2} p_k(x_1, \cdots, x_n) x^k,$$

where $p_k(x_1, \cdots, x_n)$ are symmetric polynomials in $x_1, x_2, \cdots, x_n$. This implies that

$$p_k(x_1, \cdots, x_n) \in \mathbf{R}[\sigma_{n,1}(x_1, \cdots, x_n), \cdots, \sigma_{n,n}(x_1, \cdots, x_n)].$$

Under the evaluation map $\mathcal{E}_{\alpha_1, \cdots, \alpha_n}$, we deduce that

$$g_\lambda(x) = \sum_{k=0}^{n(n-1)/2} p_k(\alpha_1, \cdots, \alpha_n) x^k.$$

Note that $p_k(\alpha_1, \cdots, \alpha_n)$ can be expressed in terms of $\sigma_{n,j}(\alpha_1, \cdots, \alpha_n), 1 \leq j \leq n$, which are the coefficients of $f(x)$ up to ± 1. Since $f \in \mathbf{R}[x]$,

$$\sigma_{n,j}(\alpha_1, \cdots, \alpha_n) \in \mathbf{R}, 1 \leq j \leq n,$$

and therefore $p_k(\alpha_1, \cdots, \alpha_n) \in \mathbf{R}$. Hence, $g_\lambda(x) \in \mathbf{R}[x]$.

Now, if $m = 1$, then the degree of g_λ is odd and g_λ has a root in $\mathbf{C}$ by Theorem 3.4. We conclude that if $m = 1$ and $\lambda \in \mathbf{R}$, then there exist i, j such that $\alpha_i + \alpha_j - \lambda \alpha_i \alpha_j \in \mathbf{C}$ since $g_\lambda(x)$ has a root in $\mathbf{C}$. Note that there are infinitely many λ and there are finitely many pairs $(\alpha_i, \alpha_j), i, j = 1, \cdots, n$. This implies that there exists $\gamma \neq \delta$ such that

$$\alpha_i + \alpha_j - \gamma \alpha_i \alpha_j \in \mathbf{C}$$

and

$$\alpha_i + \alpha_j - \delta \alpha_i \alpha_j \in \mathbf{C}.$$

This implies that

$$(\gamma - \delta) \alpha_i \alpha_j \in \mathbf{C}.$$

Since $\gamma \neq \delta \in \mathbf{R}$, $\alpha_i \alpha_j \in \mathbf{C}$. Now, $\alpha_i + \alpha_j - \gamma \alpha_i \alpha_j \in \mathbf{C}$ implies that $\alpha_i + \alpha_j \in \mathbf{C}$. Therefore, the polynomial

$$(x - \alpha_i)(x - \alpha_j) = x^2 - (\alpha_i + \alpha_j) x + \alpha_i \alpha_j \in \mathbf{C}[x].$$

We know that from Lemma 3.5, $\alpha_i, \alpha_j \in \mathbf{C}$. Hence, f has a complex root (the proof shows that it has two complex roots) and the proof of the theorem is complete. This completes the proof that if the degree of f is $2k$ where k is odd,

then f has a root in $\mathbf{C}$. Next, suppose the assertion is true for polynomials in $\mathbf{R}[x]$ of degree $2^{m-1}k$ where k is odd. If f has degree $2^m s$ where s is odd, then $g_\lambda(x) \in \mathbf{R}[x]$ will have degree $2^{m-1}t$ where t is odd. Then by induction, g_λ has a root in $\mathbf{C}$. By exactly the same argument as in the case for $m = 1$, we conclude that f has a root in $\mathbf{C}$. □

4 Finite extensions and Algebraic extensions

Recall that an extension of a field F consists of a field L and a ring homomorphism

$$\varphi : F \to L.$$

We identify F with $\varphi(F)$ and we will write a field extension as $F \subset L$.

4.1 Algebraic numbers and transcendental numbers

DEFINITION 4.1 Let L be a field extension of F and $\alpha \in L$. We say that α is algebraic over F if there exists a nonconstant $f(x) \in F[x]$ such that $f(\alpha) = 0$. An α that is not algebraic over F is said to be transcendental over F.

EXAMPLE 4.1 The numbers $\sqrt{2}$ and $e^{2\pi i/n}$, where $n \in \mathbf{Z}^+$ are algebraic. The numbers π and e are transcendental.

Given two algebraic numbers a and b, we would expect $a + b$ and ab to be algebraic. However, a polynomial $f(x)$ for which $a + b$ is a root may be rather complicated compared to the polynomial equations satisfied by a and b. For example, $\sqrt{2}$ is a root of $x^2 - 2$ and $\sqrt{3}$ is a root of $x^2 - 3$. The minimal polynomial satisfied by $\sqrt{2} + \sqrt{3}$, namely $x^4 - 10x^2 + 1$, is not as simple as the polynomials $x^2 - 2$ and $x^2 - 3$. It is therefore almost impossible to show that sum and product of two algebraic numbers are algebraic by finding polynomial equations satisfied by these numbers. New concepts need to be introduced before we can establish the facts that sum and product of algebraic numbers are algebraic.

4.2 Minimal polynomials

Given $\alpha \in L$, there exists many non-constant polynomial $f(x)$ for which $f(\alpha) = 0$. Among these polynomials, we choose a "special" one for α.

LEMMA 4.1 Let α be algebraic over F. Then there is a unique non-constant monic polynomial $p(x) \in F[x]$ such that

(a) α is a root of $p(x)$,
(b) If $f(x) \in F[x]$ is such that $f(\alpha) = 0$, then $p(x)$ divides $f(x)$.

Proof
Choose a polynomial $p(x)$ with smallest degree such that $p(\alpha) = 0$. We can assume that $p(x)$ is monic. Condition (a) is satisfied by $p(x)$. Suppose $f(x)$ is not divisible by $p(x)$. Then by division algorithm for polynomials over F, $p(x) = q(x)p(x)+r(x)$ where $0 < \deg r(x) < \deg p(x)$. This implies that $r(\alpha) = 0$. But the minimality of the degree of $p(x)$ contradicts the existence of $r(x)$.

To prove uniqueness, we note that if $p(x)$ and $p_1(x)$ are polynomials satisfying conditions (a) and (b). Then $p(x)$ divides $p_1(x)$. This implies that $p(x) = p_1(x)u(x)$. But $p_1(x)$ divides $p(x)$ implies that $p(x) = v(x)p_1(x)$. Hence, $p(x) = p(x)u(x)v(x)$. This implies that $u(x)v(x) = 1$, or $p(x) = \pm p_1(x)$. Since $p(x)$ and $p_1(x)$ are monic, we must conclude that $p(x) = p_1(x)$. □

DEFINITION 4.2 Let F be a field and L be a field extension of F. Let $\alpha \in L$ be algebraic over F. The monic polynomial $p(x) \in F[x]$ with smallest degree such that $p(\alpha) = 0$ is called the minimal polynomial of α over F. We will use the notation $\min_F(\alpha)$ for the polynomial $p(x)$.

Remark 4.1 Let $\alpha \in L$ be algebraic over F. We observe that $p(x) = \min_F(\alpha)$ is irreducible over F. This is because if $p(x)$ were reducible, then $p(x) = g(x)h(x)$ and either $g(\alpha) = 0$ or $h(\alpha) = 0$. This contradicts the minimality of the degree of $p(x)$. Conversely, if $f(x)$ is irreducible over F and $f(\alpha) = 0$, then $p(x)$ divides $f(x)$. But this forces $f(x) = p(x)$ since $f(x)$ is irreducible. Therefore, we may view $p(x)$ is the irreducible monic polynomial over F with α as one of its zeroes.

4.3 Adjoining elements

DEFINITION 4.3 Let L be a field extension of F and $\alpha_1, \cdots, \alpha_n \in L$. Define

$$F[\alpha_1, \cdots, \alpha_n] = \{h(\alpha_1, \cdots, \alpha_n) | h(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]\}.$$

Note that

$$F[\alpha_1, \cdots, \alpha_n] = \mathcal{E}_{\alpha_1, \cdots, \alpha_n}(F[x_1, \cdots, x_n]).$$

Let

$$F(\alpha_1, \cdots, \alpha_n) = \{\gamma/\beta | \gamma, \beta \in F[\alpha_1, \cdots, \alpha_n], \beta \neq 0\}.$$

The following lemma gives a characterization of $F(\alpha_1, \cdots, \alpha_n)$.

LEMMA 4.2 The set $F(\alpha_1, \cdots, \alpha_n)$ is the smallest subfield of L containing F and $\alpha_1, \cdots, \alpha_n$.

Proof
The set $F(\alpha_1, \cdots, \alpha_n)$ is a subfield of L. We check that $0 \in F[\alpha_1, \cdots, \alpha_n]$. If $a, b \in F[\alpha_1, \cdots, \alpha_n]$, then $ab, a+b, -a \in F[\alpha_1, \cdots, \alpha_n]$. Since L is a field, for any nonzero $a \in F[\alpha_1, \cdots, \alpha_n]$, $1/a \in L$. This implies that $F(\alpha_1, \cdots, \alpha_n)$ is a subfield of L.

Suppose K is a field containing F and $\alpha_1, \cdots, \alpha_n$. Since K is a field, $p(\alpha_1, \cdots, \alpha_n) \in K$ for all $p(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$. This means that $F[\alpha_1, \cdots, \alpha_n] \in K$. Since K is a field, for $h(\alpha_1, \cdots, \alpha_n) \in K$, $1/h(\alpha_1, \cdots, \alpha_n) \in K$ and therefore, $g(\alpha_1, \cdots, \alpha_n)/h(\alpha_1, \cdots, \alpha_n) \in K$. This implies $F(\alpha_1, \cdots, \alpha_n) \subset K$. □

We say that the field $F(\alpha_1, \cdots, \alpha_n)$ is obtained from F by adjoining $\alpha_1, \cdots, \alpha_n$ where $\alpha_j, 1 \leq j \leq n$ belongs to a field extension L of F.

COROLLARY 4.3 If $F \subset L$ and $\alpha_1, \cdots, \alpha_n \in L$, then

$$F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$$

for any $1 \leq r \leq n-1$.

Proof
The field $F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$ contains F and $\alpha_j, 1 \leq j \leq n$ and hence it contains $F(\alpha_1, \cdots, \alpha_n)$. Next, $F(\alpha_1, \cdots, \alpha_r)$ is contained in $F(\alpha_1, \cdots, \alpha_n)$ and $\alpha_{r+1}, \cdots, \alpha_n \in F(\alpha_1, \cdots, \alpha_n)$. Hence,

$$F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n) \subset F(\alpha_1, \cdots, \alpha_n).$$

□

EXAMPLE 4.2 It is useful to represent $F(\alpha_1, \cdots, \alpha_n)$ as $F(\alpha_1, \cdots, \alpha_r)(\alpha_{r+1}, \cdots, \alpha_n)$. The field $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ can now be written as

$\mathbf{Q}(\sqrt{2})(\sqrt{3})$ and viewed as being obtained by first adjoining $\sqrt{2}$ to $\mathbf{Q}$ followed by adjoining $\sqrt{3}$ to $\mathbf{Q}(\sqrt{2})$.

We will next show that if $\alpha_1, \cdots, \alpha_n$ are algebraic over F, then

$$F[\alpha_1, \cdots, \alpha_n] = F(\alpha_1, \cdots, \alpha_n).$$

We begin with the case when $n = 1$.

LEMMA 4.4 Assume that $F \subset L$ is a field extension, and let $\alpha \in L$ be algebraic over F with minimal polynomial $p(x) \in F[x]$. Then there is a unique ring isomorphism

$$F[\alpha] \simeq F[x]/p(x)F[x]$$

that is identity on F and maps to the coset $x + p(x)F[x]$.

Proof
Consider the ring homomorphism $\varphi : F[x] \to L$ that sends $h(x)$ to $h(\alpha) \in L$. The image of φ is $F[\alpha]$. As for the kernel, we suppose $h(x)$ is sent to 0. This means that $h(\alpha) = 0$ and therefore $p(x)$ must divide $h(x)$. Therefore the kernel of φ is $p(x)F[x]$. If $h(x) \in p(x)F[x]$ then $h(\alpha) = 0$ and this implies that $p(x)F[x]$ is contained in the kernel of φ and we have

$$\ker \varphi = p(x)F[x].$$

By first isomorphism theorem for rings, we conclude that there is an isomorphism

$$\widetilde{\varphi} : F[x]/p(x)F[x] \to F[\alpha].$$

The inverse of $\widetilde{\varphi}$ is ψ from $F[\alpha]$ to $F[x]/p(x)F[x]$ defined by

$$\psi(\alpha) = x + p(x)F[x], \psi(r) = r + p(x)F[x], r \in F.$$

Note that F is isomorphic to $F' = \{a + p(x)F[x] | a \in F\}$ which is a subfield of $F[x]/p(x)F[x]$. This shows that ψ is "identity" on F. Finally, uniqueness follows since a ring homomorphism defined on $F[\alpha]$ is determined by its values on F and α. □

THEOREM 4.5 Assume that L is a field extension and let $\alpha \in L$. Then α is algebraic over F if and only if $F[\alpha] = F(\alpha)$.

Proof
If α is algebraic over F, then by previous Lemma, $F[\alpha]$ is a field which contains

both F and α. By minimality of $F(\alpha)$, we conclude that $F(\alpha) \subset F[\alpha]$. Now, clearly, $F[\alpha] \subset F(\alpha)$.

Conversely, suppose $F(\alpha) = F[\alpha]$. Then $\alpha^{-1} \in F[\alpha]$ and this implies that α satisfies a polynomial equation over F and hence, α is algebraic over F. □

THEOREM 4.6 Let $F \subset L$ be a field extension. Let $\alpha_1, \cdots, \alpha_n \in L$ that are algebraic over F. Then

$$F[\alpha_1, \cdots, \alpha_n] = F(\alpha_1, \cdots, \alpha_n).$$

Proof
It suffices to show that $F[\alpha_1, \cdots, \alpha_n]$ is a field. We may use induction on n. The case $k = 1$ is already proved. When $k = 2$, we have $F[\alpha_1][\alpha_2] \simeq F[\alpha_1][x]/(q(x))$, where $q(x)$ is $\min_{F[\alpha_1]}(\alpha_2)$ and hence $F[\alpha_1][\alpha_2]$ is a field. It remains to show that $F[\alpha_1][\alpha_2] = F[\alpha_1, \alpha_2]$. This follows from the fact that a polynomial in α_1 and α_2 can be written as $a_0 + a_1\alpha_2 + \cdots + a_\ell\alpha_2^\ell$ with $a_j \in F[\alpha_1], 0 \leq j \leq \ell$. Conversely, any elements in the above form is an element in $F[\alpha_1, \alpha_2]$. The case where $k = n - 1$ implies $k = n$ is proved in the same way as $k = 1$ implies $k = 2$. □

We end this section with the following definition:

DEFINITION 4.4 A field extension L of F of the form $L = F(\alpha)$ for some $\alpha \in L$ is called a simple extension.

4.4 Gauss Lemma and Eisenstein Criterion

In general, given a polynomial over $\mathbf{Q}$, we do not have an efficient algorithm to determine the reducibility of the polynomial. In this section, we give a test of irreducibility for a certain collection of polynomials. We first begin with Gauss Lemma:

THEOREM 4.7 Suppose $f(x) \in \mathbf{Z}[x]$ is nonconstant and $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbf{Q}[x]$, then there exists $\tilde{g}(x), \tilde{h}(x) \in \mathbf{Z}[x]$ such that $f(x) = \tilde{g}(x)\tilde{h}(x)$.

Proof
Let $g(x) = \dfrac{r}{s}g_1(x)$ where $g_1(x) \in \mathbf{Z}[x]$ and $r, s \in \mathbf{Z}$. This is possible by considering the greatest common divisor of the numerators of the coefficients of x^j, $0 \leq j \leq \deg g$, of g and the least common multiple of the denominators of the

coefficients of x^j,$0 \leq j \leq \deg g$, of g. Note that the greatest common divisor of the coefficients of x^j, $0 \leq j \leq \deg g_1$, of g_1 is 1. Similarly, we may write

$$h(x) = \frac{t}{u} h_1(x)$$

with $h_1(x) \in \mathbf{Z}[x]$ and $t, u \in \mathbf{Z}$. Write

$$f(x) = \frac{rt}{su} g_1(x) h_1(x)$$

with $g_1(x), h_1(x) \in \mathbf{Z}[x]$. To show that $f(x)$ is reducible over $\mathbf{Z}$, it suffices to show that su divides rt. To show that this is true, we show that if $su = p^a k$ with $(p, k) = 1$, then p^a divides rt. Write

$$g_1(x) = b_\ell x^\ell + \cdots + b_0$$

and

$$h_1(x) = c_m x^m + \cdots + c_0.$$

Since the coefficients of $g_1(x)$ are relatively prime, there exists a smallest non-zero integer i such that p does not divide b_i, in other words, $p|b_\mu, 0 \leq \mu < i$. Similarly, there exists a smallest non-zero integer j such that p does not divide c_j and $p|c_\nu, 0 \leq \nu < j$. Write

$$g_1(x) h_1(x) = \sum_{\nu=0}^{m+\ell} d_\nu x^\nu$$

where

$$d_\nu = \sum_{\omega=0}^{\nu} b_\omega c_{\nu-\omega}.$$

Observe that since

$$d_{i+j} = b_0 c_{i+j} + b_1 c_{i+j-1} + \cdots + b_{i-1} c_{j+1} + b_i c_j + b_{i+1} c_{j-1} + \cdots b_{i+j} c_0,$$

the term $b_i c_j$ is not divisible by p and therefore $(p, d_{i+j}) = 1$. This implies that $(p^a, d_{i+j}) = 1$. Now, by considering the coefficient of x^{i+j} of the polynomials on both sides of

$$suf(x) = rtg_1(x) h_1(x),$$

we conclude that $p^a|(rt)d_{i+j}$ and by Euclid's Lemma, we conclude that $p^a|(rt)$ since $(p^a, d_{i+j}) = 1$. This completes the proof that f is reducible over $\mathbf{Z}$ since

$$f = \left(\frac{rt}{su} g_1(x) \right) h_1(x).$$

□

The following Corollary is an immediate consequence of Gauss' Lemma.

COROLLARY 4.8 If $f(x) \in \mathbf{Z}[x]$ is nonconstant and reducible over $\mathbf{Q}$, then $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbf{Z}[x]$.

We now prove Eisenstein criterion.

THEOREM 4.9 Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $n \in \mathbf{Z}^+$. Let p be a prime number that does not divide a_n. If p divides a_j for $0 \leq j \leq n-1$ and p^2 does not divide a_0, then $f(x)$ is irreducible over $\mathbf{Q}[x]$.

Proof
Suppose $f(x)$ is reducible in $\mathbf{Q}[x]$. Then by Gauss lemma, $f(x)$ is reducible in $\mathbf{Z}[x]$, say, $f(x) = g(x)h(x)$. Modulo p, we obtain the factorization $\overline{f}(x) = \overline{a}_n x^n$ in $\mathbf{Z}/p\mathbf{Z}[x]$. The ring $\mathbf{Z}/p\mathbf{Z}[x]$ is a UFD and we see that $\overline{f}(x)$ is divisible only by x. In other words, $\overline{g}(x) = cx^\ell$ and $\overline{h}(x) = dx^m$. This implies that a_0 is divisible by p^2, which is a contradiction. □

EXAMPLE 4.3 Use Eisenstein criterion to show that if p is a prime, then $x^{p-1} + \cdots + 1$ is irreducible over $\mathbf{Q}$.

THEOREM 4.10 Let p be prime. Then $f(x) = x^p - a \in F[x]$ is irreducible over F if and only if $f(x)$ has no roots in F.

Proof
One direction is clear. If $f(x)$ is irreducible over F, then $f(x)$ has no root in F. For if $f(x)$ has a root $\alpha \in F$ then $x - \alpha$ divides $f(x)$. Next, assume that $f(x)$ is reducible over F and we will show that $f(x)$ has a root in F. By Theorem 3.2, there exists L such that $f(x)$ splits completely. Let $f(x) = (x - \alpha_1) \cdots (x - \alpha_p)$ where $\alpha_j \in L$ for $1 \leq j \leq p$. If $\alpha_1 = 0$ then $f(x)$ has a root in F. Hence $\alpha_1 \neq 0$ and let $\zeta_j = \alpha_j/\alpha_1$. Then $\alpha_j^p = a = \alpha_1^p$ implies that $\zeta_j^p = 1$. This follows that

$$f(x) = \prod_{j=1}^{p} (x - \zeta_j \alpha_1),$$

where $\zeta_1 = 1$. This implies that if $f(x)$ is reducible over F, then there is a polynomial of the form $\prod_{k=1}^{s}(x - \zeta_{j_k}\alpha_1)$ that lies in $F[x]$ and divides $f(x)$. Assume the polynomial is of the form $(x - \zeta_{j_1}\alpha_1)(x - \zeta_{j_2}\alpha_1) \cdots (x - \zeta_{j_s}\alpha_1)$. This means that $\zeta_{j_1}\zeta_{j_2} \cdots \zeta_{j_s}\alpha_1^s \in F$. Since $s < p$, we may find n, m such that

$sn + pm = 1$. Therefore,

$$(\zeta_{j_1}\zeta_{j_2}\cdots\zeta_{j_s})^n\,\alpha_1 = (\zeta_{j_1}\zeta_{j_2}\cdots\zeta_{j_s})^n\,\alpha_1^{sn+pm} = (\zeta_{j_1}\zeta_{j_2}\cdots\zeta_{j_s}\alpha_1^s)^n\,a^m \in F.$$

But $((\zeta_{j_1}\zeta_{j_2}\cdots\zeta_{j_s})^n\,\alpha_1)^p = a$ and so, F contains a root of $f(x)$.

□

Remark 4.2 In the case when F is real and p is an odd prime, we know that $x^p - a = 0$ can have only one real root, namely, $\sqrt[p]{a}$. By the above theorem, we deduce that $x^p - a$ is irreducible over F if and only if $\sqrt[p]{a} \notin F$.

4.5 The degree of a field extension

If L is a field extension of F, then L can be viewed as a vector space over F. This motivates the following definitions.

DEFINITION 4.5 Let $F \subset L$ be a field extension. Then L is a finite extension of F if L is a finite dimensional vector space over F.

DEFINITION 4.6 Suppose L is a finite field extension of F, then the degree of L over F, denoted by $[L : F]$ is the dimension of L viewed as a finite dimensional vector space over F, The degree $[L : F] = \infty$ if L is not a finite dimensional space over F.

LEMMA 4.11 Let $F \subset L$ be a field extension. The degree $[L : F] = 1$ if and only if $L = F$.

Proof
If $[L : F] = 1$ then L is a one dimensional vector space over F and hence $L = F$. Suppose $L = F$, then the dimension of L over F is 1. This implies that $[L : F] = 1$. □

THEOREM 4.12 Suppose L is a field extension of F and $\alpha \in L$. Then α is algebraic over F if and only if $[F(\alpha) : F]$ is finite.

Proof
If α is algebraic over F, then any elements in $F(\alpha)$ can be written as an F-linear combinations of $1, \alpha, \cdots, \alpha^{n-1}$, where n is the degree of $\min_F(\alpha)$. This implies that $F(\alpha)$ is a finite dimensional vector space over F and therefore, $[F(\alpha) : F]$ is finite. Suppose $[F(\alpha) : F]$ is finite. Then $1, \alpha, \cdots, \alpha^j, \cdots$, cannot all be independent over F. Hence, there exists a polynomial $p(x)$ such that $p(\alpha) = 0$. This implies that α is algebraic over F. □

THEOREM 4.13 Suppose $F \subset L$ is a field extension and $\alpha \in L$ is algebraic. If n is the degree of $\min_F(\alpha)$ then $1, \alpha, \cdots, \alpha^{n-1}$ forms a basis of $F(\alpha)$ over F and $[F(\alpha) : F] = n$.

Proof
Suppose the degree of $p(x) = \min_F(\alpha)$ is n. We claim that $1, \alpha, \cdots, \alpha^{n-1}$ are independent over F. Suppose not. Then there exists a relation with $0 < m \leq n-1$ such that

$$b_0 + b_1\alpha + \cdots + b_m\alpha^m = 0.$$

This means that $p(x)$ divides $b_0 + b_1x + \cdots + b_mx^m$, which is impossible since $\deg p(x) = n$. Hence, $1, \alpha, \cdots, \alpha^{n-1}$ are linearly independent over F.

Next, if $\beta \in F(\alpha) = F[\alpha]$ then

$$\beta = c_0 + c_1\alpha + \cdots + c_n\alpha^n + \cdots + c_s\alpha^s, s \geq n.$$

Let $g(x) = c_0 + c_1x + \cdots + c_sx^s$. By the Quotient-Remainder Theorem, we find that

$$g(x) = p(x)q(x) + r(x)$$

where $r(x) = 0$ or $0 \leq \deg(r(x)) \leq n - 1$. This implies that $\beta = g(\alpha) = r(\alpha)$ and β is an F-linear combination of $1, \alpha, \cdots, \alpha^{n-1}$. This implies that $F[\alpha]$ is spanned by $1, \alpha, \cdots, \alpha^{n-1}$ and so, $[F(\alpha) : F] = n$. □

THEOREM 4.14 Let L be a field extension of F and $\alpha \in L$. The element α is algebraic over F if and only if $[F(\alpha) : F]$ is finite.

Proof
If α is algebraic over F then $[F(\alpha) : F] = \deg(\min_F(\alpha))$ is finite. Conversely, if $[F(\alpha) : F]$ is finite, we know that the elements in $\{1, \alpha, \alpha^2, \cdots, \alpha^\ell \cdots\}$ cannot be linear independent. Therefore, there exists m such that

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0, a_j \in F \quad \text{for } 0 \leq j \leq m.$$

This implies that α is algebraic over F. □

4.6 The Tower Theorem

THEOREM 4.15 Suppose we have fields $F \subset K \subset L$.

(a) If $[K : F] = \infty$ or $[L : K] = \infty$ then $[L : F] = \infty$.
(b) If $[K : F] < \infty$ and $[L : K] < \infty$ then $[L : F] = [L : K][K : F]$.

Proof

We prove the contrapositive version of (a). If $[L : F]$ is finite, then $[K : F]$ is finite since K is a subspace of L over F. Let L be spanned by $\{\alpha_j | 1 \leq j \leq n\}$ over F. Let $\alpha \in L$. Then $\alpha = \sum_{j=1}^{n} f_j \alpha_j$. Now, $f_j \in F \subset K$. This shows that L can be written as a K-linear combination of α_j, $1 \leq j \leq n$. This implies that $[L : K]$ is finite.

To prove (b), let $m = [K : F]$ and $n = [L : K]$. Let $\{\alpha_j | 1 \leq j \leq m\}$ be a basis of K over F and $\{\beta_k | 1 \leq k \leq n\}$ be a basis of L over K respectively. We claim that the basis of L over F is $\{\alpha_j \beta_k | 1 \leq j \leq m, 1 \leq k \leq n\}$.

For $\alpha \in L$, we have

$$\alpha = \sum_{k=1}^{n} \nu_k \beta_k,$$

where $\nu_k \in K$. But ν_k can be expressed in terms of $\alpha_j, 1 \leq j \leq m$ over F. Hence α is an F-linear combinations of elements in $\{\alpha_j \beta_k | 1 \leq j \leq m, 1 \leq k \leq n\}$.

We now prove that the elements in $\{\alpha_j \beta_k | 1 \leq j \leq m, 1 \leq k \leq n\}$ are linearly independent over F. Suppose

$$\sum_{\substack{1 \leq j \leq m \\ 1 \leq k \leq n}} \mu_{j,k} \alpha_j \beta_k = 0.$$

Since the elements in $\{\beta_k | 1 \leq k \leq n\}$ are linearly independent over K, we conclude that for each k,

$$\sum_{1 \leq j \leq m} \mu_{j,k} \alpha_j = 0.$$

The elements in $\{\alpha_j | 1 \leq j \leq m\}$ are linearly independence and this forces $\mu_{j,k} = 0, 1 \leq j \leq m$. Since this is true for any k between 1 and n, we conclude that $\mu_{j,k} = 0, 1 \leq j \leq m, 1 \leq k \leq n$. Therefore the elements in $\{\alpha_j \beta_k | 1 \leq j \leq m, 1 \leq k \leq n\}$ are linearly independent over F and

$$[L : F] = [L : K][K : F].$$

□

By Theorem 4.14, α is algebraic if and only if $[F(\alpha) : F] < \infty$. Let α and β be algebraic over F. Then $[F(\alpha) : F] < \infty$ and $[F(\alpha, \beta] : F(\alpha)] < \infty$ (since β is algebraic over $F(\alpha)$ if it is algebraic over F). Therefore by the Tower Theorem,

$[F(\alpha, \beta) : F] < \infty$. Now, both $\alpha - \beta$ and α/β, $\beta \neq 0$, are elements in $F(\alpha, \beta)$. By Theorem 4.15 (a), $[F(\alpha - \beta) : F] < \infty$ and $[F(\alpha/\beta) : F] < \infty$ and by Theorem 4.14, $\alpha - \beta$ and α/β are algebraic over F. This means that the set of algebraic numbers over F forms a field. We have therefore established the following theorem:

THEOREM 4.16 Let $F \subset L$ be a field extension. The set of elements in L which is algebraic over F forms a subfield of L.

Remark 4.3 We can now conclude that if $\alpha, \beta \in L$ is algebraic over F, then $\alpha\beta$ and $\alpha \pm \beta$ are algebraic over F. We also have $\alpha\beta^{-1}$ is algebraic when $\beta \neq 0$.

4.7 Algebraic extensions

In the previous section, we have seen that if $F \subset L$ is a field extension and $\alpha \in L$ is algebraic over F, then $F(\alpha)$ is a finite extension over F. Theorem 4.15 indicates that if $\beta \in F(\alpha)$, then $F(\beta)$ is finite over F and therefore by Theorem 4.14, β is algebraic over F. In other words, $F(\alpha)$ is a field for which every elements in is algebraic over F. This motivates the next definition.

DEFINITION 4.7 A field extension $F \subset L$ is algebraic if every element of L is algebraic over F.

We aim to show the following result connecting finite extension and algebraic extension over F.

THEOREM 4.17 If L is a finite extension over F, then L is an algebraic extension over F.

Proof
Suppose $\alpha \in L$. Then $F(\alpha)$ is a finite extension over F since L is finite over F. Therefore, α is algebraic over F. This implies that L is an algebraic extension of F. □

The converse is false. The collection of all algebraic numbers over $\mathbf{Q}$ is an algebraic extension over $\mathbf{Q}$, denoted by $\overline{\mathbf{Q}}$. Note that if p is an odd prime and

$\alpha_p \in \overline{\mathbf{Q}}$ is a root of $x^{p-1} + x^{p-2} + \cdots + 1$, then $[\mathbf{Q}(\alpha_p) : \mathbf{Q}] = p$. If we assume that $[\overline{\mathbf{Q}} : \mathbf{Q}] = N$, then we would obtain a contradiction by letting $p > N$ since

$$[\overline{\mathbf{Q}} : \mathbf{Q}] = N \geq [\mathbf{Q}(\alpha_p) : \mathbf{Q}] = p > N.$$

The above discussion shows that in order to determine if an algebraic extension is finite, thus providing a "converse" to Theorem 4.17, we need one additional condition. This is reflected in the following theorem:

THEOREM 4.18 Let $F \subset L$ be a field extension. The degree $[L : F] < \infty$ if and only if there are $\alpha_1, \cdots, \alpha_n \in L$, algebraic over F and $L = F(\alpha_1, \cdots, \alpha_n)$.

Proof
Suppose $[L : F] < \infty$. Then there exists $\alpha_1, \cdots, \alpha_n$ in L, linearly independent over F and spans L as a vector space over F. Note that $L = F\alpha_1 + \cdots + F\alpha_n \subset F(\alpha_1, \cdots, \alpha_n)$. But L contains F and $\{\alpha_j | 1 \leq j \leq n\}$ and so it contains $F(\alpha_1, \cdots, \alpha_n)$. Hence $L = F(\alpha_1, \cdots, \alpha_n)$.

Conversely, suppose $L = F(\alpha_1, \cdots, \alpha_n) = F(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n)$, where the last equality follows from Corollary 4.3. We observe that

$$[F(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n) : F(\alpha_1, \cdots, \alpha_{n-1})] < \infty$$

since α_n is algebraic over $F(\alpha_1, \cdots, \alpha_{n-1})$ and by induction hypothesis, we may assume that $[F(\alpha_1, \cdots, \alpha_{n-1}) : F] < \infty$. Hence, by Theorem 4.15, $[F(\alpha_1, \cdots, \alpha_n) : F] < \infty$. This completes the proof of the theorem. □

THEOREM 4.19 Let $F \subset K \subset L$. If $\alpha \in L$ is algebraic over K and K is algebraic over F, then α is algebraic over F.

Proof
If $\alpha \in L$ is algebraic over K, then α satisfies a polynomial equation of the form

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0 \tag{4.1}$$

with $a_j \in K$ for all $0 \leq j \leq m-1$. Since K is algebraic over F, the a_j's are algebraic over F and by Theorem 4.18, we conclude that $F(a_0, \cdots, a_{m-1})$ is a finite field extension of F. Note that by (4.1), α is algebraic over $F(a_0, \cdots, a_{m-1})$ and therefore $F(a_0, \cdots, a_{m-1})(\alpha)$ is a finite extension of $F(a_0, \cdots, a_{m-1})$. By Theorem 4.15, we conclude that $F(a_0, \cdots, a_{m-1})(\alpha)$ is a finite extension of F. By Theorem 4.18, we conclude that $F(a_0, \cdots, a_{m-1}, \alpha)$ is algebraic. In particular, $\alpha \in F(a_0, \cdots, a_{m-1}, \alpha)$ is algebraic over F. □

As a corollary, we conclude that

COROLLARY 4.20 If $F \subset K \subset L$ where L is algebraic over K and K is algebraic over F, then L is algebraic over F.

Proof
Let $\alpha \in L$. Since α is algebraic over K and K is algebraic over F, α is algebraic over F and this holds for any $\alpha \in L$. This implies that L is algebraic over F. $\square$

5 Splitting fields and Normal extensions

5.1 Splitting fields

Let F be a field. We have seen in Theorem 3.2 that if $f(x) \in F[x]$ then there exists a field extension L of F such that $f(x)$ splits completely. This motivates our next definition.

DEFINITION 5.1 Let $f(x) \in F[x]$ with $\deg(f) = n > 0$. A field extension L of F is a splitting field of $f(x)$ over F if

(a) $f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$ where $c \in F$ and $\alpha_j \in L$ for $1 \leq j \leq n$,
(b) $L = F(\alpha_1, \cdots, \alpha_n)$.

EXAMPLE 5.1 The field $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbf{Q}$. The field $\mathbf{Q}(i, 2^{1/4})$ is the splitting field of $x^4 - 2$ but the field $\mathbf{Q}(2^{1/4})$ since $i2^{1/4} \notin \mathbf{Q}(2^{1/4})$.

From the example $\mathbf{Q}(i, 2^{1/4})$, we observe that if L is the splitting field of $f(x)$ of degree n over F, the degree of L over F is not necessarily n. The following result gives an upper bound for $[L : F]$ in terms of the degree of $f(x)$.

THEOREM 5.1 Let $f(x)$ be a polynomial of degree n over F and L be the splitting field of $f(x)$ over F. Then $[L : F] \leq n!$.

Proof
We want to show that for any field F and any polynomial over F of degree n, the splitting field L of $f(x)$ satisfies $[L : F] \leq n!$. We may assume $f(x)$ to be monic. We establish the inequality using induction on n. If $n = 1$, $[L : F] = 1$ and the conclusion is true. Suppose the inequality is true for polynomial of degree $n - 1$. Let $f(x)$ be a monic polynomial of degree n. Let L be a splitting field of $f(x)$ over F. Then $L = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_1, \cdots, \alpha_n$ are the roots of $f(x)$. Write

$f(x) = (x - \alpha_1)g(x)$, where $g(x) = b_0 + b_1 x + \cdots + b_{n-2}x^{n-2} + x^{n-1}$. From

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n = (x - \alpha_1)(b_0 + b_1 x + \cdots + b_{n-2}x^{n-2} + x^{n-1}),$$

we find that

$$a_j = -\alpha_1 b_j + b_{j-1}.$$

Note that since $b_0\alpha_1 = a_0$, we deduce that $b_0 \in F(\alpha_1)$. By induction on j, we deduce that $b_j \in F(\alpha_1)$ and therefore $g(x) \in F(\alpha_1)[x]$. By induction, the splitting field L of $g(x)$ over $F(\alpha_1)$ satisfies $[L : F(\alpha_1)] \leq (n-1)!$. Together with $[F(\alpha_1) : F] \leq n$, we conclude that

$$[L : F] \leq n!.$$

□

5.2 Uniqueness of splitting fields

We next study the uniqueness of splitting fields. Note that both $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}[x]/(x^2 - 2)$ are splitting fields of $x^2 - 2$ over $\mathbf{Q}$. The key point is that while they are not the same, they are isomorphic.

THEOREM 5.2 Let φ be an isomorphism from the field F_1 to the field F_2. Let $f_1(x) \in F_1[x]$ and let $f_2(x)$ be obtained from $f_1(x)$ by applying φ to the coefficients of $f_1(x)$. Suppose L_1 and L_2 are the splitting fields of $f_1(x)$ and $f_2(x)$ over F_1 and F_2 respectively. Then there is an isomorphism

$$\overline{\varphi} : L_1 \to L_2$$

such that $\varphi = \overline{\varphi}\big|_{F_1}$.

Proof
We prove by induction on n, the degree of $f_1(x)$. When $n = 1$, $L_1 \simeq F_1$ and $L_2 \simeq F_2$ and we observe that $\overline{\varphi} = \varphi$.

Suppose $n > 1$. We know that if $\alpha_1, \cdots, \alpha_n$ are roots of $f_1(x)$ then

$$L_1 = F(\alpha_1, \cdots, \alpha_n).$$

Consider $F_1 \subset F_1(\alpha_1) \subset L_1$, where L_1 is viewed as the splitting field of $g(x) = f_1(x)/(x - \alpha_1)$ over $F_1(\alpha_1)$.

Step 1. Let $h_1(x) \in F_1[x]$ be the minimal polynomial of α_1 over F_1. We know that $h_1(x)$ must divide $f_1(x)$. Also

$$F_1(\alpha_1) \simeq F_1[x]/h_1(x)F_1[x].$$

Step 2. We now find a root of $f_2(x)$ corresponding to α_1. The map $\varphi : F_1 \to F_2$ induces a ring homomorphism $\widetilde{\varphi} : F_1[x] \to F_2[x]$ that takes $f_1(x)$ to $f_2(x)$. This isomorphism takes irreducibles to irreducibles. In particular, $h_1(x)$ is mapped to an irreducible factor $h_2(x)$ of $f_2(x)$. Since $f_2(x)$ splits completely in L_2, we can label the roots of $f_2(x)$ in L_2 as $\beta_1, \cdots, \beta_n$, where β_1 is a root of $h_2(x)$.

Step 3. The root β_1 of $f_2(x)$ gives an extension $F_2 \subset F_2(\beta_1) \subset L_2$, where L_2 is viewed as the splitting field of $g_2(x) = f_2(x)/(x - \beta_1)$ over $F_2(\beta_1)$. Since $h_2(x)$ is the irreducible polynomial of β_1, we conclude that

$$F_2(\beta_1) \simeq F_2[x]/h_2(x)F_2[x].$$

Step 4. Since $\widetilde{\varphi} : F_1[x] \to F_2[x]$ sends $h_1(x)$ to $h_2(x)$, $\widetilde{\varphi}(h_1(x)F_1[x]) = h_2(x)F_2[x]$. Therefore,

$$F_1[x]/h_1(x)F_1[x] \simeq F_2[x]/h_2(x)F_2[x].$$

By Steps 1 and 3, we obtain an isomorphism $\varphi_1 : F_1(\alpha_1) \to F_2(\beta_1)$.
Step 5. Now, $g_1(x) = f_1(x)/(x-\alpha_1)$ and $g_2(x) = f_2(x)/(x-\beta_1)$ have degree $n-1$ over $F_1(\alpha_1)$ and $F_2(\beta_1)$ respectively and φ_1 is an isomorphism from $F_1(\alpha_1)$ to $F_2(\beta_1)$. By induction hypothesis, we conclude that there exists an isomorphism $\overline{\varphi} : L_1 \to L_2$ such that $\overline{\varphi}\big|_{F_1(\alpha_1)} = \varphi_1$. But $\varphi_1\big|_{F_1} = \varphi$ and this completes the proof of the theorem. □

COROLLARY 5.3 If L_1 and L_2 are splitting fields of $f(x) \in F[x]$ then there is an isomorphism $L_1 \simeq L_2$ that is identity on F.

Proof
Apply Theorem 5.2 with φ as the identity map on F. □

THEOREM 5.4 Let L be a splitting field of a polynomial in $F[x]$. Suppose $h(x) \in F[x]$ is an irreducible polynomial with degree at least 2 and has roots $\alpha, \beta \in L$. Then there is a field isomorphism $\sigma : L \to L$ that is identity on F and takes α to β.

Proof
We observe that

$$F(\alpha) \simeq F[x]/h(x)F[x] \simeq F(\beta).$$

Therefore, there is an isomorphism $\xi : F(\alpha) \to F(\beta)$ with the property that $\xi(\alpha) = \beta$. Now, L is the splitting field of $h(x)$ and contains both $F(\alpha)$ and $F(\beta)$. By Theorem 5.2, we conclude that there is an isomorphism $\sigma : L \to L$ such that $\sigma\big|_{F(\alpha)}$ is an isomorphism from $F(\alpha)$ to $F(\beta)$. Note that $\sigma\big|_{F(\alpha)} = \xi$. Hence, $\sigma(\alpha) = \beta$ and the proof is complete. □

5.3 Finite fields as splitting fields of polynomials

In this section, we establish the following

THEOREM 5.5 If L is a finite field with p^m elements, with p a prime and m a positive integer, then L is the splitting field of $x^{p^m} - x \in F_p[x]$, where F_p denote the finite field $\mathbf{Z}/p\mathbf{Z}$.

Proof
Let $f(x) = x^{p^m} - x$. It is known that (see Remark 5.1) if L is a finite field, then $L - \{0\}$ is a cyclic multiplicative group. This implies that there exists an element $\alpha \in L$ such that $L = \{0, \alpha^j | 1 \leq j \leq p^m - 1\}$. Observe that if $\beta \in L$ then $\beta^{p^m} - \beta = 0$. This means that all elements in L are roots of $f(x)$. These are all the roots since the polynomial can have at most $p^m - 1$ roots since it is a polynomial over a field. Now any splitting field of $f(x)$ must contain at least p^m elements. Since L contains exactly p^m elements, L must be the splitting field of $f(x)$. This completes the proof of the theorem. □

Since splitting fields of polynomials over a field F are isomorphic, we conclude that any finite fields with p^m elements are isomorphic.

Remark 5.1 Let $L^* = L - \{0\}$. Let $g \in L^*$ and $o(g)$ be the order of g. Let

$$m = \max_{g \in L^*} o(g).$$

If $m = |L^*|$ then L^* is cyclic. Suppose

$$m < |L^*|. \tag{5.1}$$

By the structure theorem of finite abelian group,

$$L^* \simeq \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_\ell\mathbf{Z},$$

with $a_i | a_{i+1}, i = 1, \cdots, \ell - 1$. This means that $m = a_\ell$ and it also implies that if $\alpha \in L^*$, then α is a root of

$$x^m = 1.$$

But in $F[x]$ where F is a field, the number of solutions $x^m - 1$ is at most m and therefore, $|L^*| \leq m$. This contradicts (5.1). Therefore L^* is cyclic.

Another way of seeing that L^* is cyclic is by using the identity

$$\sum_{d|n} \varphi(d) = n. \tag{5.2}$$

Let $n = |L^*|$ and C_d be the number of elements in L^* that has order exactly d. If C_d is non-empty, then the element of order d generates a cyclic group with d

elements which are roots of $x^d - 1$. Since F is a field, $x^d - 1$ can have no more than d elements. In other words, all elements of order d must be in C_d if $|C_d| \neq 0$. If C_d is not empty then the total number of elements in C_d is exactly $\varphi(d)$. This is a result of the fact that if α has order d then α^k has order d if and only if $(k, d) = 1$. Now, every element in L^* has an order. Therefore,

$$|L^*| = n = \sum_{d|n} |C_d| \leq \sum_{d|n} \varphi(d) = n,$$

where the last equality follows from (5.2). This implies that $|C_d| = \varphi(d)$. In particular, $|C_n| = \varphi(n)$ and therefore, L^* is cyclic since C_n is non-empty.

EXAMPLE 5.2 The fields $F_2[x]/(x^3 + x + 1)F_2[x]$ and $F_2[x]/(x^3 + x^2 + 1)F_2[x]$ are isomorphic.

5.4 Normal extensions

Splitting field of a polynomial $f(x) \in F[x]$ has an important property given as follow:

THEOREM 5.6 Let L be a field extension over F which is a splitting field of $f(x)$. If $g(x)$ is an irreducible polynomial which has a root in L then $g(x)$ splits completely in L.

Proof
We may suppose that $f(x)$ and $g(x)$ are monic and let $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$. Then $L = F(\alpha_1, \cdots, \alpha_n)$. Suppose β is a root of $g(x)$ in L. We need to prove that all the roots of $g(x)$ are also in L. Note that $\beta \in L = F(\alpha_1, \cdots, \alpha_n) = F[\alpha_1, \cdots, \alpha_n]$ and hence $\beta = h(\alpha_1, \cdots, \alpha_n)$ for some polynomial $h(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$. Consider the polynomial

$$s(x) = \prod_{\tau \in S_n} (x - h(\alpha_{\tau(1)}, \cdots, \alpha_{\tau(n)}) \in L[x].$$

The roots of $s(x)$ are all in L since $\alpha_1, \cdots, \alpha_n \in L$. Furthermore, β is a root of $s(x)$ and if we can show that $s(x) \in F[x]$ then we can conclude from $g(x)|s(x)$ that all the roots are in L.

Now consider the polynomial

$$S(x) = \prod_{\tau \in S_n} (x - h(x_{\tau(1)}, \cdots, x_{\tau(n)}).$$

Note that we can write

$$S(x) = \sum_{j=0}^{n!} p_j(x_1, \cdots, x_n)x^j,$$

where

$$p_j(x_1, \cdots, x_n) = \sigma_{n!,n!-j}(h(x_{\tau_1(n)}, \cdots, x_{\tau_1(n)}), \cdots, h(x_{\tau_{n!}(n)}, \cdots, x_{\tau_{n!}(n)})),$$

with τ_j's are distinct elements in S_n. Here the $\sigma_{m,j}$ is the j-th elementary symmetric functions in m variables. Note that $p_j(x_{\tau(1)}, \cdots, x_{\tau(n)}) = p_j(x_1, \cdots, x_n)$ and thus, $p_j(x_1, \cdots, x_n)$ are symmetric for $0 \leq j \leq n-1$. These polynomials can therefore be expressed in terms of $\sigma_{n,j}(x_1, \cdots, x_n)$ for $0 \leq j \leq n-1$. Using the evaluation map sending x_j to α_j, we conclude that $p_j(\alpha_1, \cdots, \alpha_n)$ are in terms of $\sigma_{n,j}(\alpha_1, \cdots, \alpha_n)$ which all lies in F. Therefore, $s(x) \in F[x]$ and the proof is complete.

□

The above property of splitting fields motivates the following definition:

DEFINITION 5.2 An algebraic extension L of F is normal if every irreducible polynomial in $F[x]$ that has a root in L splits completely in L.

Remark 5.2 Not all normal field extensions are splitting fields of some polynomials. The field $\overline{\mathbf{Q}}$, the algebraic closure of $\mathbf{Q}$ is a normal extension that is not a splitting field of any polynomial.

The following theorem characterizes splitting fields in terms of normal extension.

THEOREM 5.7 Suppose L is a field extension of F. Then L is the splitting field of some polynomial $f(x) \in F[x]$ if and only if L is normal and finite.

Proof
If L is a splitting field of $f(x)$, then $L = F(\alpha_1, \cdots, \alpha_n)$ is finite by Theorem 4.18 or Theorem 5.1. By Theorem 5.6, L is normal.

Conversely, suppose L is normal and finite. Since L is finite, by Theorem 4.18, $L = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_1, \cdots, \alpha_n$ are algebraic over F. Let $p_1(x), \cdots, p_n(x)$ be irreducible polynomials such that for each i, α_j is a root of $p_j(x)$. Let $f(x) = p_1(x) \cdots p_n(x)$. We will show that L is the splitting field of $f(x)$. Observe that $p_j(x)$ has a root α_j in L and L is normal. Hence, all the roots of $p_j(x)$ are in L.

Let $\{\beta_1, \cdots, \beta_s\}$ be the roots of $f(x)$ and let L' be the splitting field of $f(x)$, namely, $L' = F(\beta_1, \cdots, \beta_s)$. Note that

$$L = F(\alpha_1, \cdots, \alpha_n) \subset L'$$

since $\{\alpha_1, \cdots, \alpha_n\} \subset \{\beta_1, \cdots, \beta_s\}$. But $L' \subset L$ since by normality of L, β_j's, $1 \leq j \leq s$, which are roots of $p_i(x), 1 \leq i \leq n$ are in L. This implies that $L' = L$ and L is the splitting of $f(x)$.

□

6 Separable extensions

6.1 Separable polynomials and separable extensions

Let F be a field. Given a monic nonconstant polynomial $f(x) \in F[x]$ with splitting field L, we can write $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. Note that $\alpha_j, 1 \leq j \leq n$, are not always distinct. We will restrict our attention to polynomials that have distinct roots in this section.

DEFINITION 6.1 A polynomial $f(x) \in F[x]$ is separable if it is nonconstant and its roots in a splitting field are all simple. Note that $f(x)$ is separable if and only if

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 \neq 0.$$

Remark 6.1 The above definition of separable polynomial is not standard. Most books require separable polynomial to be irreducible.

Another tool we need is the formal derivative of a polynomial $g(x) = a_n x^n + \cdots + a_0$ defined by

$$g'(x) = n a_n x^{n-1} + \cdots + a_1.$$

Note that with this definition, one has

$$(fg)' = f'g + fg'$$

for any two polynomials in $F[x]$. We leave the proof of the "seemingly obvious" statement (because of our knowledge of Calculus) as exercise.

The following theorem gives some characterizations of a separable polynomial.

THEOREM 6.1 Let $f(x)$ be a monic and nonconstant in $F[x]$. The following are equivalent:

(a) $f(x)$ is separable,

(b) $\Delta(f) \neq 0$,
(c) $f(x)$ and $f'(x)$ are relatively prime (i.e. $\gcd(f, f') = 1$) in $F[x]$.

Proof
If degree of $f(x)$ is 1, then we define $\Delta(f) = 1$. So $\Delta(f) \neq 0$. Also $(f, f') = 1$. So (a), (b), and (c) are equivalent to each other.

Assume that the degree of $f(x)$ is greater than 1. We first show that (a) and (b) are equivalent. Let $\alpha_1, \cdots, \alpha_n$ be roots of $f(x)$ in some splitting field of $f(x)$. The definition of $\Delta(f)$ shows that $\Delta(f) \neq 0$ if and only if the roots of $f(x)$ are distinct.

Next, we show the equivalence of (a) and (c). Let L be a splitting field of $f(x)$ over F. Let $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. For each $1 \leq i \leq n$,

$$f(x) = (x - \alpha_i)h_i(x),$$

where

$$h_i(x) = \prod_{j \neq i} (x - \alpha_j).$$

Formally differentiating $f(x)$, we find that

$$f'(x) = (x - x_i)h_i'(x) + h_i(x).$$

This implies that

$$f'(\alpha_i) = h_i(\alpha_i) = \prod_{j \neq i} (\alpha_j - \alpha_i) \neq 0, \tag{6.1}$$

since $f(x)$ is a separable polynomial. If (c) is false, then $f(x), f'(x)$ have common factor. This implies that there exist $g(x)$ such that $g(x) = (f(x), f'(x))$. Note that $g(x)$ divides $f(x)$ and $f'(x)$ Therefore, $g(\alpha_i) = 0$ for some i and $f'(\alpha_i) = 0$. By (6.1), this implies that $h_i(\alpha_i) = 0$, which is a contradiction.

Conversely, assuming (c) is true. Then

$$1 = A(x)f(x) + B(x)f'(x)$$

for some $A(x), B(x) \in F[x]$. This implies that for $1 \leq i \leq n$,

$$1 = A(\alpha_i)f(\alpha_i) + B(\alpha_i)f'(\alpha_i)$$

which implies that $f'(\alpha_i)B(\alpha_i) = 1$, or $f'(\alpha_i) \neq 0$. This implies that for $1 \leq i \leq n$,

$$\prod_{j \neq i} (\alpha_j - \alpha_i) \neq 0$$

and α_j's are all distinct. This implies that $f(x)$ is a separable polynomial. □

DEFINITION 6.2 Let L be an algebraic extension of F.

(a) $\alpha \in L$ is separable over F if $\min_F(\alpha)$ is a separable polynomial.
(b) L is a separable extension over F if every $\alpha \in L$ is separable over F.

LEMMA 6.2 A nonconstant polynomial $f(x) \in F[x]$ is separable if and only if $f(x)$ is a product of irreducible polynomials, each of which is separable and no two of which are multiple of each other.

Proof
Assume $f(x)$ is separable. Then each factor of $f(x)$ must have distinct roots in a splitting field, then $f(x)$ will not be separable. Hence, all irreducible polynomial dividing $f(x)$ is separable. Next, the irreducible polynomials dividing $f(x)$ cannot be identical or $f(x)$ would have multiple roots.

Conversely, let $f(x) = g_1(x) \cdots g_s(x)$ where $g_j(x)$ are separable and irreducible. Therefore $g_j(x)$ has distinct roots. If $f(x)$ has multiple roots then there exists $i \neq j$ such that $g_i(x)|g_j(x)$ and $g_j(x)|g_i(x)$. Therefore $g_i(x)$ is a multiple of $g_j(x)$. □

LEMMA 6.3 Let $f(x) \in F[x]$ be an irreducible polynomial of degree n. Then $f(x)$ is separable if

(a) F has characteristic 0, or
(b) F has characteristic $p > 0$ where $p \nmid n$.

Proof
By Theorem 6.1, it suffices to show that $(f(x), f'(x)) = 1$. Suppose F has characteristic 0.

If $(f(x), f'(x)) = h(x) \neq 1$ then there exists an α in the splitting field of $h(x)$ such that $h(\alpha) = f(\alpha) = f'(\alpha) = 0$. Since α is a root of $f(x)$ and $f(x)$ is irreducible over F, $f(x)$ must divide $f'(x)$. This is impossible since the degree of $f'(x)$ is less than degree of $f(x)$.

Next suppose that the characteristic of F is a prime p. We may assume that $f(x)$ is monic. If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then $f'(x) = nx^{n-1} + \cdots + a_1$. Since $p \nmid n$, we find that $f'(x)$ is a polynomial of degree less than the degree of $f(x)$. Using the argument as in the case when the characteristic of F is 0, we deduce that $(f(x), f'(x)) = 1$ and hence $f(x)$ is separable.

□

EXAMPLE 6.1 Let F be a field with characteristic 0. Show that every algebraic extension of F is separable.

Solution
Let L be an algebraic extension of F. Let $\alpha \in L$. By Lemma 6.3, we deduce that the minimal polynomial of α over F is separable. Hence L is separable.

DEFINITION 6.3 A field F is called a *perfect field* if every algebraic extension of F is separable.

In the above example, we showed that if char F=0, then F is perfect. It can be shown that if F is a finite field, F is perfect.

EXAMPLE 6.2 Let $f(x)$ be any polynomial over F where F has characteristic 0. Show that $f(x)/(f(x), f'(x))$ is separable.

Solution
Let $f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_s)^{m_s}$. Let $g(x) = f(x)/(f(x), f'(x))$. To show that $g(x)$ is separable, it suffices to show that (f, f') is divisible by $(x-\alpha_j)^{m_j-1}$ but not by $(x-\alpha_j)^{m_j}$ for $j = 1, 2, \cdots, s$.

Now, write $f(x) = (x-\alpha_j)^{m_j} f_j(x)$, where $f_j(\alpha_j) \neq 0$. Then

$$f'(x) = m_j(x-\alpha_j)^{m_j-1} f_j(x) + (x-\alpha_j)^{m_j} f_j'(x).$$

This implies that α_j is a zero of $f'(x)$ of order $m_j - 1$. So if $h(x) = (f(x), f'(x))$, α_j is a zero of $f'(x)$ of order $m_j - 1$ since

$$f'(x) = (x-\alpha_j)^{m_j-1}(m_j f_j(x) + (x-\alpha_j) f_j'(x))$$

and $(x-\alpha_j)$ does not divide $f_j(x)$. This concludes the fact that g is separable since $g = (x-\alpha_1)\cdots(x-\alpha_s)$.

DEFINITION 6.4 A polynomial $f \in F[x]$ is inseparable if it is not a separable polynomial. In other words, it has root with multiplicity greater than 1.

EXAMPLE 6.3 Show that if F is a field with characteristic p, then $x^p - t \in F_p(t)[x]$ is an inseparable irreducible polynomial

Solution
The polynomial $x^p - t$ is irreducible over $F_p(t)$. This follows because $t^{1/p}$ does not lie in $F_p(t)$. Let a be a root of $f(x) = x^p - t$ in the splitting field of $f(x)$ over $F_p(t)$. Then $a^p = t$. This implies that $f(x) = (x^p - a^p) = (x - a)^p$ and f is inseparable.

6.2 Theorem of the primitive element

THEOREM 6.4 Let $L = F(\alpha_1, \cdots, \alpha_n)$ be a finite extension where each of α_j is separable over F. Then there exists $\alpha \in L$ separable over F such that $L = F(\alpha)$. Furthermore, if F is infinite, then α can be chosen to be of the form $\alpha = t_1\alpha_1 + \cdots + t_n\alpha_n$ for some $t_j \in F$.

Remark 6.2 We observe that if the characteristic of F is 0, then we may remove the condition "α_j is separable over F." This is because the minimal polynomial of these α_j's is separable.

Remark 6.3 Theorem 6.4 shows that if $\alpha_j, 1 \leq j \leq n$ is separable over F, then $F(\alpha_1, \cdots, \alpha_n)$ is a simple extension. In other words, there exists $\beta \in F(\alpha_1, \cdots, \alpha_n)$ such that $F(\alpha_1, \cdots, \alpha_n) = F(\beta)$.

Proof
Let F be a field with finitely many elements. Then F is a field with characteristic p for some prime p. Suppose $L = F(\alpha_1, \cdots, \alpha_n)$ is a finite extension where each of α_j is separable over F. Then L is a finite field extension of F and so, it is a finite field. It is known that finite multiplicative group of $L - \{0\}$ is cyclic. This implies that if $|F| = p^e$ and $[L : F] = m$, then there exists $\alpha \in L$ such that

$$L - \{0\} = \{\alpha^j | 1 \leq j \leq p^{em} - 1\}.$$

Note that $F \subset L$ since elements in F is a root of

$$x^{p^{em}-1} = 1.$$

Hence, $L = F(\alpha)$. Note that α is separable over F since the polynomial $x^{p^{em}-1} - 1$ is separable. This completes the proof of the theorem when L is finite.

We now assume that F is infinite. Let $L = F(\alpha_1, \cdots, \alpha_n)$. We will use induction on n to show that there are $t_1, \cdots, t_n \in F$ such that

(1) $L = F(t_1\alpha_1 + \cdots + t_n\alpha_n)$ and
(2) $t_1\alpha_1 + \cdots + t_n\alpha_n$ is separable over F.

We begin with the case $n = 2$. Given $L = F(\beta, \gamma)$. Let $f(x), g(x) \in F[x]$ be minimal polynomials of β and γ respectively. $f(x)$ could be the same as $g(x)$. Let $\ell = \deg(f(x))$ and $m = \deg(g(x))$. Let E be a splitting field of $f(x)g(x)$. Let $\beta = \beta_1$ and $\gamma = \gamma_1$. Let $\beta_1, \cdots, \beta_\ell$ be the distinct roots of $f(x)$ and $\gamma_1, \cdots, \gamma_m$ be the distinct roots of $g(x)$. Since F is infinite, we can find $\lambda \in F$ such that

$$\lambda \neq \frac{\beta_i - \beta_r}{\gamma_s - \gamma_j}, 1 \leq r, i \leq \ell, r \neq i, 1 \leq s, j \leq m, s \neq j.$$

This implies that

$$\beta_r + \lambda\gamma_s \neq \beta_i + \lambda\gamma_j, r \neq i, s \neq j.$$

Therefore $\beta + \lambda\gamma \neq \beta_i + \lambda\gamma_j, 1 \leq i \leq \ell, 1 \leq j \leq m$.

We first prove that $F(\beta + \lambda\gamma) = F(\beta, \gamma)$. The inclusion $F(\beta + \lambda\gamma) \subset F(\beta, \gamma)$ is immediate. We want to show that $\beta, \gamma \in F(\beta + \lambda\gamma)$.

It suffices to show that $\gamma \in F(\beta + \lambda\gamma)$, for then $\beta = \beta + \lambda\gamma - \lambda\gamma$ is also contained in the field.

Since $g(x) \in F[x]$, $g(x) \in F(\beta+\lambda\gamma)[x]$. Next, $f(\beta+\lambda\gamma-\lambda x)$ vanishes at $x = \gamma$ and $f(\beta+\lambda\gamma-\lambda x) \in F(\beta+\lambda)[x]$. Therefore, the gcd of $g(x)$ and $f(\beta+\lambda\gamma-\lambda x)$ is a non-constant polynomial in $F(\beta + \lambda\gamma)[x]$.

Let $h(x) = \gcd(g(x), f(\beta + \lambda\gamma - \lambda x))$. If $\deg h(x) > 1$ then there exists $\gamma' \neq \gamma$ such that $h(\gamma') = 0$. This implies that

$$f(\beta + \lambda\gamma - \lambda\gamma') = 0$$

or

$$\beta + \lambda\gamma = \lambda\gamma' + \beta'.$$

This contradicts our choice of λ. Hence the degree of $h(x)$ is 1 and $\gamma \in F(\beta+\lambda\gamma)$ and this completes the claim that $F(\beta, \gamma) = F(\beta + \lambda\gamma)$.

It remains to show that $\beta + \lambda\gamma$ is separable. Let $p(x) \in F[x]$ be the minimal polynomial of $\beta + \lambda\gamma$ over F. We must show that $p(x)$ is separable. Let

$$s(x) = \prod_{j=1}^{m} f(x - \lambda\gamma_j).$$

Note that $\beta + \lambda\gamma$ is a root of $s(x)$ since $f(\beta + \lambda\gamma - \lambda\gamma) = f(\beta) = 0$. If $S(x) = \prod_{j=1}^{m} f(x-\lambda x_j)$, then for $\tau \in S_m$, $S(x) = \prod_{j=1}^{m} f(x-\lambda x_j) = \prod_{j=1}^{m} f(x-\lambda x_{\tau(j)})$. So the coefficient of x^k in $S(x)$ must be a symmetric polynomial in $x_1, \cdots, x_m$. Therefore, under the evaluation map, we deduce that the coefficient of x^k must belong to F. Since $s(x) \in F[x]$, we conclude that $p(x)$ divides $s(x)$.

Now,

$$s(x) = \prod_{i=1}^{\ell} \prod_{j=1}^{m} (x - (\beta_i + \lambda\gamma_j)).$$

Note $\beta_i + \lambda\gamma_j \neq \beta_s + \lambda\gamma_r$ for all i, j, r, s except when $i = s$ and $j = r$. We conclude that $s(x)$ is a separable polynomial. This implies that $p(x)$ is also separable. Therefore the case $n = 2$ holds with $t_1 = 1$ and $t_2 = \lambda$.

Suppose now that the conclusion holds for any field of the form $F(\beta_1, \cdots, \beta_{n-1})$, that is, there exists $s_1, \cdots, s_{n-1}$ such that

$$F(\beta_1, \cdots, \beta_{n-1}) = F(s_1\beta_1 + \cdots + s_{n-1}\beta_{n-1})$$

and $s_1\beta_1 + \cdots + s_{n-1}\beta_{n-1}$ is separable. Write $L = F(\alpha_1, \cdots, \alpha_{n-1})(\alpha_n) = F(\nu, \alpha_n)$ where $\nu = t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}$ by induction hypothesis. By case $n = 2$, we conclude that $F(\nu, \alpha_n) = F(\nu + \lambda_n)$ for some $\lambda \in F$. Therefore,

$$L = F(t_1\alpha_1 + \cdots t_{n-1}\alpha_{n-1} + \lambda\alpha_n).$$

Note that $t_1\alpha_1 + \cdots t_{n-1}\alpha_{n-1} + \lambda\alpha_n$ is separable since $t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}$ and α_n are separable. □

Remark 6.4 We have seen that if $L = F(\alpha_1, \cdots, \alpha_n)$ where α_j is separable and L is finite, then $L = F(\alpha)$ for some separable $\alpha \in L$. It turns out that if $L = F(\alpha)$ is finite and α is separable then L is a separable extension. This statement will be proved after introducing Galois extension.

EXAMPLE 6.4 The splitting field of $x^3 - 2$ is $L = \mathbf{Q}(e^{2\pi i/3}, 2^{1/3})$. We can also write L as $\mathbf{Q}(\sqrt{-3} + 2^{1/3})$ and so, L is simple.

EXAMPLE 6.5 In this example, we show the existence of a field extension $F(\beta, \gamma)$ which is not simple. Of course, in this case, β and γ are not separable over F. Let $F = F_p(u, v)$ where u, v are independent variables and F_p is the field of p elements. Let $x^p - u \in F[x]$. We claim that $x^p - u$ is irreducible in $F[x]$. We have seen that if $x^p - u$ is reducible then there exits $\beta \in F = F_p(u, v)$ such that $\beta^p - u = 0$. If $\beta = h(u, v)/\ell(u, v)$, then $h^p(u, v) = u\ell^p(u, v)$ which is a contradiction by considering the power of u. Therefore, if β is a root of $x^p - u$, then $[F(\beta) : F] = p$. Now, consider $x^p - v$ as a polynomial in $F(\beta)[x]$. Again if $x^p - v$ has a root $\gamma \in F(\beta)$ then $\gamma = w(\beta, v)/z(\beta, v)$ and $\gamma^p = v$ implies that $w^p(\beta, v) = vz^p(\beta, v)$, a contradiction by considering the degree of v. Therefore,

$$[F(\beta, \gamma) : F] = [F(\beta)(\gamma) : F(\beta)][F(\beta) : F] = p^2.$$

Next, suppose $\nu \in F(\beta, \gamma)$. Then

$$\nu = g(\beta, \gamma)$$

for some polynomial $g(s,t)$ of two variables. This implies that

$$\nu^p = g^p(\beta,\gamma) = g(\beta^p,\gamma^p) = g(u,v) \in F.$$

This implies that degree of $\min_F(\nu)$ is at most p, or $[F(\nu);F] \leq p$. In other words, $F(\beta,\gamma) \neq F(\nu)$ for all $\nu \in F(\beta,\gamma)$ and the field $F(\beta,\gamma)$ is not simple.

7 The Galois Group

Let L be a field. An automorphism of L is a field isomorphism $\sigma : L \to L$.

DEFINITION 7.1 Let L be a finite field extension of F. Then $\mathrm{Gal}(L|F)$ is the set

$$\{\sigma : L \to L | \sigma \text{ is an automorphism, } \sigma(a) = a \text{ for all } a \in F.\}.$$

THEOREM 7.1 The set $\mathrm{Gal}(L|F)$ is a group under composition.

Proof
If $\sigma, \tau \in \mathrm{Gal}(L|F)$ then $\sigma\tau \in \mathrm{Gal}(L|F)$. The identity map on L is the identity for $\mathrm{Gal}(L|K)$. Sine σ is an isomorphism, σ^{-1} exists and finally associativity follows from composition of functions. □

LEMMA 7.2 Let L be a finite field extension. Fix $\sigma \in \mathrm{Gal}(L|F)$. Let $h(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ and $\beta_1, \cdots, \beta_n \in L$. Then

$$\sigma(h(\beta_1, \cdots, \beta_n)) = h(\sigma(\beta_1), \cdots, \sigma(\beta_n)).$$

In particular, $\sigma(h(\beta)) = h(\sigma(\beta))$.

Proof
This follows from the observation that if $h(\beta_1, \cdots, \beta_n)$ is a finite sum in terms of $\beta_1, \cdots, \beta_n$, namely, if

$$h(\beta_1, \cdots, \beta_n) = \sum_{1 \leq k_1, \cdots, k_n \leq N} \alpha_{k_1, \cdots, k_n} \beta_1^{k_1} \cdots \beta_n^{k_n}$$

with $\alpha_{k_1, \cdots, k_n} \in F$, then

$$\sigma(h(\beta_1, \cdots, \beta_n)) = \sum_{1 \leq k_1, \cdots, k_n \leq N} \alpha_{k_1, \cdots, k_n} \sigma(\beta_1)^{k_1} \cdots \sigma(\beta_n)^{k_n} = h(\sigma(\beta_1), \cdots, \sigma(\beta_n)).$$

□

THEOREM 7.3 Let L be a finite field extension of L and $\sigma \in \mathrm{Gal}(L|F)$. Then

(a) If $h(x) \in F[x]$ is a nonconstant polynomial with $\alpha \in L$ as a root, then $\sigma(\alpha)$ is another root of $h(x)$ lying in L.
(b) If $L = F(\alpha_1, \cdots, \alpha_n)$, then σ is uniquely determined by its values on $\alpha_1, \cdots, \alpha_n$.

Proof
By Lemma 7.2, we find that

$$\sigma(h(\alpha)) = h(\sigma(\alpha)).$$

So if α is a root of $h(x)$ then $\sigma(\alpha)$ is also a root of $h(x)$. This implies (a).

To prove (b), let $\sigma, \tau \in \mathrm{Gal}(L|F)$. Suppose $\sigma(\alpha_i) = \tau(\alpha_i), i = 1, 2, \cdots, n$. Then for $\beta \in F(\alpha_1, \cdots, \alpha_n)$,

$$\beta = \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)}.$$

This implies that

$$\begin{aligned}\sigma(\beta) &= \frac{f(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))}{g(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))} \\ &= \frac{f(\tau(\alpha_1), \cdots, \tau(\alpha_n))}{g(\tau(\alpha_1), \cdots, \tau(\alpha_n))} = \tau(\beta).\end{aligned}$$

Therefore, σ is uniquely determined by its values on $\alpha_1, \cdots, \alpha_n$.

□

DEFINITION 7.2 Let α be algebraic over a field F. Let L be the splitting fields of $\min_F(\alpha)$. The roots of $\min_F(\alpha)$ are called the conjugates of α.

THEOREM 7.4 If L is a finite extension of F, then $\mathrm{Gal}(L|F)$ is finite.

Proof
By Theorem 4.18, L is finite implies that $L = F(\alpha_1, \cdots, \alpha_n)$, where each α_j is algebraic over F.

Let $S = \{\gamma \in L | \gamma \text{ is a conjugate of } \alpha_j \text{ for some } 1 \leq j \leq n\}$. Observe that S is finite. Since σ is determined by its values on α_j and since $\sigma(\alpha_j)$ is a conjugate of α_j and that S is a finite, we conclude that there are finitely many possible σ's. Hence, $\mathrm{Gal}(L|F)$ is finite.

□

THEOREM 7.5 Suppose L_1 and L_2 are finite field extensions of F. Let φ be an isomorphism from L_1 to L_2 that is identity on F. Then the map sending σ to $\varphi\sigma\varphi^{-1}$ defines a group isomorphism from $\mathrm{Gal}(L_1|F)$ to $\mathrm{Gal}(L_2|F)$.

Proof
We first show that if $\sigma \in \mathrm{Gal}(L_1|F)$ then for $\beta \in L_2$, $\varphi\sigma\varphi^{-1}(\beta) \in L_2$. So $\varphi\sigma\varphi^{-1} \in \mathrm{Gal}(L_2|F)$. To show that the map sending σ to $\varphi\sigma\varphi^{-1}$ is an isomorphism, we observe that the inverse map is $\varphi^{-1}\tau\varphi$ for $\tau \in \mathrm{Gal}(L_2|F)$ and

$$\varphi\sigma_1\sigma_2\varphi^{-1} = \varphi\sigma_1\varphi^{-1}\varphi\sigma_2\varphi^{-1}.$$

□

DEFINITION 7.3 Let $f(x) \in F[x]$. The *Galois group of $f(x)$* over F is $\mathrm{Gal}(L|F)$ where L is the splitting field of $f(x)$ over F.

Remark 7.1 Suppose $L_1 \simeq L_2$ are both splitting fields of $f(x)$ over F. Then by Theorem 7.5, $\mathrm{Gal}(L_1|F) \simeq \mathrm{Gal}(L_2|F)$ and so the Galois group of $f(x)$ over F is well defined up to isomorphism of splitting fields of $f(x)$.

7.1 Galois groups of splitting fields

In this section, we prove an important fact about the splitting field of a separable polynomial.

THEOREM 7.6 Let L be the splitting field of a separable polynomial $f(x) \in F[x]$. Then

$$|\mathrm{Gal}(L|F)| = [L : F].$$

Proof
Let $\alpha_1, \cdots, \alpha_n$ be roots of a separable polynomial $f(x)$. Then α_j are separable over F since the minimal polynomial of α_j divides $f(x)$, which is separable. By Theorem 6.4, $L = F(\beta)$ where $\beta \in L$ is separable over F. Let $h(x) = \min_F(\beta)$. Note that

$$F(\beta) = F[\beta] \simeq F[x]/h(x)F[x].$$

Therefore $[L : F] = m = \deg(h(x))$.

To complete the proof of the theorem, we need to show that $|\text{Gal}(L|F)| = m$. Now, $\beta \in L$ and L is the splitting field of $f(x)$. By Theorem 5.6, we conclude that L is a normal extension and all the roots of $h(x)$ lie in L. Let $\beta_1, \cdots, \beta_m$, where $\beta_1 = \beta$, be roots of $h(x)$ in L. Note that $\sigma \in \text{Gal}(L|F)$ is uniquely determined by $\sigma(\beta)$. There are m-choices for σ since $\sigma(\beta) = \beta_j$ for some j between 1 and m. Therefore $|\text{Gal}(L|F)| \leq m$. Next, given β and β_j, we can find an element $\tau \in \text{Gal}(L|F)$ such that $\tau(\beta) = \beta_j$. This show that $|\text{Gal}(L|F)| \geq m$. Therefore, $|\text{Gal}(L|F)| = m$ and this completes the proof of the theorem. □

7.2 Permutations of roots

In this section, we relate Galois Groups to permutations of roots of separable polynomials. Let $n = \deg(f)$. Then in a splitting field of a separable polynomial $f(x) \in F[x]$, we can write

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n).$$

For each $\sigma \in \text{Gal}(L|F)$, $\sigma(\alpha_i)$ is a root of $f(x)$. This implies that $\sigma(\alpha_i) = \alpha_{\tau(i)}$ for some $\tau \in S_n$. In this way, we can associate $\sigma \in \text{Gal}(L|F)$ to an element $\tau \in S_n$.

THEOREM 7.7 Let L be the splitting field of a separable polynomial $f(x)$ with $\deg(f) = n$. The map $\text{Gal}(L|F) \to S_n$ described above is a one to one group homomorphism.

Proof
Write $L = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_1, \cdots, \alpha_n$ are roots of $f(x)$. Suppose $\sigma_1, \sigma_2 \in \text{Gal}(L|F)$ with $\sigma_i(\alpha_j) = \alpha_{\tau_i(j)}, i = 1, 2$. Now, $\sigma_1\sigma_2(\alpha_j) = \sigma_1(\alpha_{\tau_2(j)}) = \alpha_{\tau_1(\tau_2(j))}$. Hence $\sigma_1\sigma_2$ corresponds to $\tau_1\tau_2$. Therefore the map is a homomorphism. to show that the map is one to one. Suppose $\tau_1 = \tau_2$. Then $\sigma_1(\alpha_j) = \alpha_{\tau_1(j)} = \alpha_{\tau_2(j)} = \sigma_2(\alpha_j)$. This implies $\sigma_1 = \sigma_2$ since $\sigma \in \text{Gal}(L|F)$ is determined by its values $\alpha_1, \cdots, \alpha_n$. □

COROLLARY 7.8 If L is the splitting field of a separable polynomial $f(x) \in F[x]$, then $[L : F]|n!$ where $n = \deg(f)$.

Proof
The group $\text{Gal}(L|F)$ is mapped into a subgroup of S_n and this implies that

$$|\text{Gal}(L|F)||n!.$$

By Theorem 7.6, we conclude that

$$[L : F]|n!.$$

□

Remark 7.2 Note that we have previously shown in Theorem 5.1 that if L is a splitting field of a polynomial $f(x) \in F[x]$, then $[L : F] \leq n!$. We have shown here that if $f(x)$ is irreducible and separable then $[L : F]|n!$.

EXAMPLE 7.1 The subgroup $\{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is transitive while $\{(1), (1\,2), (3\,4), (1\,2)(3\,4)\}$ is not transitive.

The main result in this section is the following theorem due to C. Jordan discovered around 1870:

THEOREM 7.9 Let L be the splitting field of a separable polynomial $f(x) \in F[x]$ of degree n. Then the subgroup of S_n corresponding to $\mathrm{Gal}(L|F)$ is transitive if and only if $f(x)$ is irreducible over F.

Proof
Suppose $f(x)$ is irreducible with roots $\alpha_1, \cdots, \alpha_n \in L$. For $\alpha \neq \alpha'$ with $f(\alpha) = f(\alpha') = 0$, we know that there exists $\sigma \in \mathrm{Gal}(L|F)$ such that $\sigma(\alpha) = \alpha'$, by Theorem 5.4. This shows that $\mathrm{Gal}(L|F)$ is transitive on the roots of $f(x)$.

Conversely, suppose $\mathrm{Gal}(L|F)$ corresponds to a transitive subgroup of S_n. Let $h(x)$ be an irreducible factor of $f(x)$. Let $\alpha_1, \cdots, \alpha_n$ be roots of $f(x)$ and let $h(\alpha_i) = 0$ for some i. Let $j \in \{1, 2, \cdots, n\}$. By transitivity of $\mathrm{Gal}(L|F)$, there exists σ such that $\sigma(\alpha_i) = \alpha_j$. Since $h(\alpha_i) = 0$, $h(\sigma(\alpha_i)) = 0$. Since j is any integer between 1 and n, $h(x)$ must have at least n roots and this implies that $\deg(h(x)) \geq n$ and we deduce that $f(x) = h(x)$ and $f(x)$ is therefore irreducible. □

EXAMPLE 7.2 Determine the structure of the group $\mathrm{Gal}(L|\mathbf{Q})$ if L is the splitting field of $x^p - 2$.

Solution

The splitting field of $x^p - 2$ is $L = \mathbf{Q}(\zeta_p, 2^{1/p})$ where $\zeta = e^{2\pi i/p}$. We have seen that

$$[L : \mathbf{Q}] \leq [\mathbf{Q}(\zeta_p) : \mathbf{Q}][\mathbf{Q}(2^{1/p}) : \mathbf{Q}].$$

Next, $p|[L : \mathbf{Q}]$ and $(p-1)|[L : \mathbf{Q}]$. Since $(p, p-1) = 1$, we conclude that $p(p-1)$ divides $[L : \mathbf{Q}]$ or $[L : \mathbf{Q}] \geq p(p-1)$. Therefore, $[L : \mathbf{Q}] = p(p-1)$. By Theorem 7.6,

$$|\mathrm{Gal}(L|\mathbf{Q})| = [L : \mathbf{Q}] = p(p-1).$$

We now determine the structure of $\mathrm{Gal}(L|\mathbf{Q})$. We know that any $\sigma \in \mathrm{Gal}(L|\mathbf{Q})$ is determined by $\sigma(2^{1/p})$ and $\sigma(\zeta_p)$. Define

$$\sigma_{j,k}(2^{1/p}) = \zeta_p^j 2^{1/p}, 0 \leq j \leq p-1,$$

and

$$\sigma_{j,k}(\zeta_p) = \zeta_p^k, 1 \leq k \leq p-1.$$

There are $p(p-1)$ choices of $\sigma_{j,k}$ and these are the elements in $\mathrm{Gal}(L|\mathbf{Q})$ since $|\mathrm{Gal}(L|\mathbf{Q})| = p(p-1)$.

We now check that

$$\begin{aligned}\sigma_{j,k} \circ \sigma_{r,s}(2^{1/p}) &= \sigma_{j,k}(\zeta_p^r 2^{1/p}) \\ &= \zeta_p^{rk} \zeta_p^j 2^{1/p} \\ &= \zeta_p^{rk+j} 2^{1/p},\end{aligned}$$

and

$$\sigma_{j,k} \circ \sigma_{r,s}(\zeta_p) = \sigma_{j,k}(\zeta_p^s) = \zeta_p^{sk}.$$

Dropping σ in the above, we see that $\mathrm{Gal}(L|\mathbf{Q})$ is isomorphic to the group

$$(G, \bullet)$$

where $G = N \times H$ with $N = \mathbf{Z}/p\mathbf{Z}$ and $H = (\mathbf{Z}/p\mathbf{Z})^*$ and

$$(j, k) \bullet (r, s) = (j + rk, sk).$$

The group G has identity $(0, 1)$ and the inverse of (j, k) is $(-jk', k')$ where k' is the inverse of k in H. This group is called the semi-direct product of N by H.

EXAMPLE 7.3 Determine the structure of $\mathrm{Gal}(\mathbf{F}_{p^n}|\mathbf{F}_p)$.

Solution

Note that $L = \mathbf{F}_{p^n}$ is a splitting field of $x^{p^n} - x$ and therefore

$$|\mathrm{Gal}(L|\mathbf{F}_p)| = [L : \mathbf{F}_p] = n.$$

We now show that $\mathrm{Gal}(L|\mathbf{F}_p)$ is cyclic of order n by constructing a generator for $\mathrm{Gal}(L|\mathbf{F}_p)$ explicitly. First, note that if $L^p = \{\beta^p | \beta \in L\}$ then $L^p = L$. Now, since $\beta \in L$,

$$\beta = \beta^{p^n} = (\beta^{p^{n-1}})^p$$

which means that $L \subset L^p$. Clearly, $L^p \subset L$ then $L^p = L$. Let σ be the map

$$\sigma(\beta) = \beta^p.$$

It is a bijection from L to L since it is a surjection. Note that

$$\sigma(\beta + \gamma) = (\beta + \gamma)^p = \beta^p + \gamma^p = \sigma(\beta) + \sigma(\gamma).$$

Also,

$$\sigma(\beta\gamma) = (\beta\gamma)^p = \beta^p\gamma^p = \sigma(\beta)\sigma(\gamma).$$

So $\sigma \in \mathrm{Gal}(L|\mathbf{F}_p)$. Next, let α be a generator for $(\mathbf{F}_{p^n})^*$. Then

$$\sigma^j(\alpha) = \alpha^{p^j}$$

and the smallest j such that $\sigma^j(\alpha) = \alpha$ is $j = n$ since the order of α in $(\mathbf{F}_{p^n})^*$ is $p^n - 1$. Therefore the order of σ in $\mathrm{Gal}(L|\mathbf{F}_p)$ is n and $\mathrm{Gal}(L|\mathbf{F}_p)$ is generated by σ. The map σ is known as the Frobenius automorphism.

8 The Galois extension and Galois Closure

We have now come to the main theorems of Galois theory.

DEFINITION 8.1 Suppose we have a finite extension L over F with Galois group $\mathrm{Gal}(L|F)$. Given a subgroup $H \subset \mathrm{Gal}(L|F)$, we let

$$L_H = \{\alpha \in L | \sigma(\alpha) = \alpha \text{ for all } \sigma \in H.\}.$$

We call L_H the fixed field of H.

THEOREM 8.1 Let $F \subset L$ be a finite field extension. The following are equivalent:

(a) L is the splitting field of a separable polynomial in $F[x]$.
(b) F is the fixed field of $\mathrm{Gal}(L|F)$ acting on L.
(c) $F \subset L$ is a normal separable extension.

Proof
We first show that (a) implies (b). Let L be the splitting field of a separable polynomial in $F[x]$. Let K be a fixed field of $\mathrm{Gal}(L|F)$. This means that if $\alpha \in K$, the $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathrm{Gal}(L|F)$. By definition of $\mathrm{Gal}(L|F)$, we know that F is fixed by $\mathrm{Gal}(L|F)$ and so

$$F \subset K. \tag{8.1}$$

Since L is the splitting field of a separable polynomial $f(x) \in F[x]$, L is the splitting field of $f(x)$ viewed as a polynomial over K. By Theorem 7.6, we conclude that

$$[L : K] = |\mathrm{Gal}(L|K)| \text{ and } [L : F] = |\mathrm{Gal}(L|F)|. \tag{8.2}$$

Now, $F \subset K \subset L$ implies that $[L : K] \leq [L : F]$. By (8.2), we deduce that

$$|\mathrm{Gal}(L|K)| \leq |\mathrm{Gal}(L|F)|.$$

Next, let $\sigma \in \mathrm{Gal}(L|F)$. Then since K is the fixed field of $\mathrm{Gal}(L|F)$, $\sigma(\alpha) = \alpha$

and thus, $\sigma \in \mathrm{Gal}(L|K)$. This implies that

$$|\mathrm{Gal}(L|F)| \leq |\mathrm{Gal}(L|K)|.$$

Therefore,

$$|\mathrm{Gal}(L|K)| = |\mathrm{Gal}(L|F)|$$

and by (8.2),

$$[L : F] = [L : K]. \tag{8.3}$$

From (8.1), we know that $F \subset K$. Together with (8.3), we deduce $F = K$. In this proof, we have shown that if $K = L_{\mathrm{Gal}(L|F)}$, then

$$\mathrm{Gal}(L|K) = \mathrm{Gal}(L|F). \tag{8.4}$$

Note that we may rewrite (8.4) as

$$\mathrm{Gal}(L|L_{\mathrm{Gal}(L|F)}) = \mathrm{Gal}(L|F).$$

We next show that (b) implies (c). Suppose F is the fixed field of $\mathrm{Gal}(L|F)$. We need to show that L is normal and separable over F.

We first show that L is separable over F. Let $\alpha \in L$. Let $\sigma_1(\alpha), \cdots, \sigma_r(\alpha)$ be the distinct images of α under $\mathrm{Gal}(L|F)$. Let

$$h(x) = \prod_{j=1}^{r} (x - \sigma_j(\alpha)).$$

This is a polynomial in $L[x]$.

Let $\sigma \in \mathrm{Gal}(L|F)$. Then

$$\sigma(\sigma_j(\alpha)) \in \{\sigma_1(\alpha), \cdots, \sigma_r(\alpha)\} =: S$$

since $\sigma(\sigma_j(\alpha))$ must be one of the distinct images of α under $\mathrm{Gal}(L|F)$. Now, if $\sigma(\sigma_j(\alpha)) = \sigma(\sigma_k(\alpha))$ then $\sigma_j(\alpha) = \sigma_k(\alpha)$. Hence, σ permutes the elements in S. This implies σ fixes the coefficients of $h(x)$. Since elements fixed by $\mathrm{Gal}(L|F)$ lies in F, we conclude that $h(x) \in F[x]$. By definition of $h(x)$, we find that $h(x)$ is a separable polynomial in $F[x]$ and α is a root of $h(x)$. Hence α is separable over F and therefore, L is separable over F.

Next, we show that L is a normal over F. Let β be a root of an irreducible polynomial $f(x) \in F[x]$ and $\beta \in L$. We need to show that $f(x)$ splits completely in L. By our construction in the previous paragraph, we can find a separable polynomial $g(x)$ of the form

$$g(x) = \prod_{j=1}^{s} (x - \tau_j(\beta)),$$

where $\tau_j(\beta), j = 1, 2, \cdots, s$ are distinct images of β under $\mathrm{Gal}(L|F)$. We have seen that $g(x) \in F[x]$. Next let $t(x) = \min_F(\beta)$. Since $t(\beta) = 0$, we conclude that $(x - \beta)|t(x)$. Now $t(\beta) = 0$ implies that $t(\tau_j(\beta)) = 0$ for $\tau_j \in \mathrm{Gal}(L|F)$. Therefore $(x - \tau_j(\beta))|t(x)$. This implies that $g(x)|t(x)$. Since $t(x)$ is irreducible,

$g(x) = t(x)$. Since $\tau_j(\beta) \in L$, we conclude that all the roots of $t(x)$, namely, $\tau_j(\beta), j = 1, 2, \cdots, s$, are all in L. This implies that L is a normal extension over F.

Finally, we show that (c) implies (a). Suppose L is a normal and separable extension of F. Since L is finite, we may write $L = F(\alpha_1, \cdots, \alpha_n)$ where the minimal polynomial of α_j for each j is separable. By Theorem 6.4, we conclude that there exists $\beta \in L$ separable over F such that $L = F(\beta)$. Let $b(x) = \min_F(\beta)$. By normality of L, $b(x)$ splits completely in $L = F(\beta)$. If K is the splitting field of $b(x)$ then K must contain β and $L \subset K$. On the other hand, K is the splitting field of $b(x)$ and by definition of splitting field, it must be contained in fields for which $b(x)$ splits completely. Therefore $K \subset L$. This implies that $L = K$ is the splitting field of a separable polynomial $b(x)$ (which in this case is also irreducible).

□

DEFINITION 8.2 An extension L of F is called a Galois extension of F if it satisfies one of the three conditions of Theorem 8.1.

THEOREM 8.2 Suppose L is a Galois extension of F and $F \subset K \subset L$. Then L is a Galois extension of K.

Proof
Note that L is the splitting field of a separable polynomial $f(x)$ over F is L is a Galois extension of F. But $f(x)$ is also a separable polynomial over K. Hence L is a splitting field of the same separable polynomial $f(x)$ over K and this implies that L is a Galois extension of K. □

THEOREM 8.3 Let L be a finite extension of F. Then

(a) $|\text{Gal}(L|F)||[L : F]$,
(b) $|\text{Gal}(L|F)| \leq [L : F]$,
(c) L is a Galois extension if and only if $|\text{Gal}(L|F)| = [L : F]$.

Proof
We first prove (a). Let K be the fixed field of $\text{Gal}(L|F)$. By (8.4),

$$\text{Gal}(L|K) = \text{Gal}(L|F).$$

Therefore, K being the fixed field of $\text{Gal}(L|F)$ is the fixed field of $\text{Gal}(L|K)$. By Theorem 8.1, L is a splitting field of a separable polynomial over K and so, by Theorem 7.6,

$$|\text{Gal}(L|K) = [L : K].$$

Now, since $F \subset K$, $[L : K]$ divides $[L : F]$. Now, $[L : K] = |\text{Gal}(L|K)| = |\text{Gal}(L|F)|$ (by (8.4)), we conclude that $|\text{Gal}(L|F)|$ divides $[L : F]$.

Part (b) follows immediately from (a).

To prove (c), we observe that if L is Galois over F, then $\text{Gal}(L|F) = [L : F]$ since L is a splitting field of a separable polynomial over F.

For the converse, let K be the fixed field of $\text{Gal}(L|F)$. We have seen that $[L : K] = |\text{Gal}(L|K)| = |\text{Gal}(L|F)|$. Hence, if

$$|\text{Gal}(L|F)| = [L : F],$$

then

$$[L : K] = [L : F] = [L : K][K : F]$$

implies that $[K : F] = 1$, or $K = F$. Since L is Galois over K, L is Galois over F. □

Remark 8.1 Part (c) of Theorem 8.3 is another equivalent condition for L being Galois over F.

8.1 Finite separable extensions

The primitive element theorem Theorem 6.4 states that if L is finite extension of F and $L = F(\alpha_1, \cdots, \alpha_n)$, where $\alpha_j, 1 \leq j \leq n$ are separable, then there exists β separable over F such that $L = F(\beta)$. But we have not shown that L is separable if $L = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_j, 1 \leq j \leq n$ are separable. We will now show that this is indeed the case.

THEOREM 8.4 Let L be a finite extension of F. Then L is separable over F if and only if $L = F(\alpha_1, \cdots, \alpha_n)$, where each α_j is separable over F.

Proof

One direction is immediate. If L is a finite separable extension of F, then L is spanned by, say, $\alpha_1, \cdots, \alpha_n$, each of which is separable over F. Furthermore, $L = F(\alpha_1, \cdots, \alpha_n)$.

Conversely, suppose $L = F(\alpha_1, \cdots, \alpha_n)$, where each $\alpha_j, 1 \leq j \leq n$, is separable over F. Then by Theorem 6.4, there exists a separable element β such that $L = F(\beta)$. Let $f(x)$ be the minimal polynomial of β over F and let M be the splitting field of $f(x)$. Then M is Galois over F, hence separable over F. Now, $F(\beta) = F(\alpha_1, \cdots, \alpha_n) = L \subset M$ since M is the splitting field of $f(x)$. Since M is separable over F, this means that L is separable over F.

□

8.2 Galois closure

The proof of Theorem 8.4 shows that if L is a finite extension of F of the form $L = F(\alpha_1, \cdots, \alpha_n)$ for which each α_j is separable over F, then one can find a field extension M of L which is Galois over F. This motivates the following theorem.

THEOREM 8.5 Let L be a finite separable extension of F. Then there is an extension M of L such that

(a) M is Galois over F
(b) Given M' Galois over F, there is a field homomorphism $\varphi : M \to M'$ that is identity on L. (This says that M is the smallest Galois extension over F.)

Proof
By Theorem 6.4, we conclude that $L = F(\beta)$ for some $\beta \in L$. Let $f(x)$ be the minimal polynomial of β over F and M be the splitting field of $f(x)$. Then M is Galois over F.

To prove (b). Let $L \subset M'$ where M' is Galois over F. Then M' is a normal extension of F. This means that if $L = F(\beta)$ with minimal polynomial $f(x)$ then $f(x)$ splits completely in M'. In other words, if $\beta_j, 1 \leq j \leq r$, are the roots of $f(x)$ then $\beta_1, \cdots, \beta_r \in M'$. Since the splitting field $M = F(\beta_1, \cdots, \beta_r)$ is the smallest field that contains $\beta_1, \cdots, \beta_r$ and F, we conclude that $M \subset M'$. □

The field constructed in Theorem 8.5 is called the Galois closure of L over F.

9 Fundamental theorem of Galois Theory

9.1 Conjugate fields

DEFINITION 9.1 Suppose $F \subset K \subset L$ where $[L : F] < \infty$. For $\sigma \in \text{Gal}(L|F)$, we call $\sigma K = \{\sigma(\alpha) | \alpha \in K\}$ a conjugate field of K.

LEMMA 9.1 Let $F \subset K \subset L$ and $\sigma \in \text{Gal}(L|F)$. Then $F \subset \sigma L \subset L$ and $[K : F] = [\sigma K : F]$.

Proof
Note that $\sigma F = F \subset \sigma K$. Since σ is an automorphism of L, $\sigma K \simeq K$ (can be viewed as isomorphism of vector spaces over F). Therefore, $[\sigma K : F] = [K : F]$ □

9.2 Galois subfields of a Galois extension

THEOREM 9.2 Suppose $F \subset K \subset L$ where L is Galois over F. The following are equivalent:

(a) $K = \sigma K$ for all $\sigma \in \text{Gal}(L|F)$,
(b) K is a normal extension of F,
(c) K is Galois over F.

Proof
We first prove (a) implies (b). Let $\beta \in K \subset L$. In the proof of Theorem 8.1, we have seen that if $\sigma_j(\beta), 1 \leq j \leq r$, are the distinct images of β under the elements in $\text{Gal}(L|F)$, then the polynomial

$$h(x) = \prod_{j=1}^{r} (x - \sigma_j(\beta))$$

is equal to $\min_F(\beta)$. Since $\sigma_j K = K$, we conclude that all the roots of $h(x)$ are in K and this implies that K is a normal extension of F.

To show (b) implies (c), we note that K is normal over F. Since L is Galois over F, L is separable over F. Therefore K is separable over F. This means that K is finite, normal and separable extension of F and so, by Theorem 8.1, K is Galois over F.

To show (c) implies (a), we note that K is Galois over F. Let $\beta \in K$. Then $\sigma(\beta)$, $\sigma \in \mathrm{Gal}(L|F)$, is a root of $\min_F(\beta)$. Since K is Galois over F, K is normal and therefore $\sigma(\beta) \in K$. This implies that $\sigma(K) \subset K$. Now by Lemma 9.1, $[K : F] = [\sigma(K) : F]$. Together with $\sigma(K) \subset K$, we conclude that $\sigma(K) = K$ for all $\sigma \in \mathrm{Gal}(L|F)$. □

We next given another equivalent statement for the statements given in Theorem 9.2. We first state a lemma.

LEMMA 9.3 Suppose $F \subset K \subset L$ and $[L : F] < \infty$. Then

(a) $\mathrm{Gal}(L|K) \leq \mathrm{Gal}(L|F)$.
(b) If $\sigma \in \mathrm{Gal}(L|F)$ then $\mathrm{Gal}(L|\sigma K) = \sigma\mathrm{Gal}(L|K)\sigma^{-1}$.

Proof
To prove (a), let $\sigma \in \mathrm{Gal}(L|K)$. Since σ fixes K, it fixes F. Therefore, $\sigma \in \mathrm{Gal}(L|F)$. Since $\mathrm{Gal}(L|K)$ is a group, it is a subgroup of $\mathrm{Gal}(L|F)$.

To prove (b), let $\gamma \in \mathrm{Gal}(L|\sigma K)$. Then $\gamma(\sigma(k)) = \sigma(k)$ for all $k \in K$. This implies that $\sigma^{-1}\gamma\sigma(k) = k$ for all $k \in K$ and so, $\sigma^{-1}\gamma\sigma \in \mathrm{Gal}(L|K)$, or $\gamma \in \sigma\mathrm{Gal}(L|K)\sigma^{-1}$ and

$$\mathrm{Gal}(L|\sigma K) \subset \sigma\mathrm{Gal}(L|K)\sigma^{-1}.$$

The inclusion in the other direction can be established in a similar way. □

THEOREM 9.4 Let L be a Galois extension of F. Then the following are equivalent:

(a) $K = \sigma(K)$ for all $\sigma \in \mathrm{Gal}(L|F)$,

(b) $\mathrm{Gal}(L|K) \lhd \mathrm{Gal}(L|F)$.

Proof
To prove (a) implies (b), we recall that given a subgroup H of a group G, we say that $H \lhd G$ if $gHg^{-1} = H$ for all $g \in G$. From Lemma 9.3, we find that if $\sigma \in \mathrm{Gal}(L|F)$, then

$$\sigma\mathrm{Gal}(L|K)\sigma^{-1} = \mathrm{Gal}(L|\sigma(K)) = \mathrm{Gal}(L|K),$$

since $\sigma(K) = K$. Therefore, $\mathrm{Gal}(L|K) \lhd \mathrm{Gal}(L|F)$.

Next, suppose (b) holds, then for $\sigma \in \mathrm{Gal}(L|F)$,

$$\sigma \mathrm{Gal}(L|K)\sigma^{-1} = \mathrm{Gal}(L|K).$$

This implies that

$$\mathrm{Gal}(L|\sigma K) = \mathrm{Gal}(L|K). \tag{9.1}$$

But L is Galois over F implies that L is Galois over K and σK. This implies that

$$\sigma K = L_{\mathrm{Gal}(L|\sigma(K))} = L_{\mathrm{Gal}(L|K)} = K,$$

where the second last equality follows from (9.1). This implies (a) is true. □

THEOREM 9.5 Suppose $F \subset K \subset L$ where L is Galois over F and K is Galois over F. Then $\mathrm{Gal}(L|K) \lhd \mathrm{Gal}(L|F)$ and

$$\mathrm{Gal}(L|F)/\mathrm{Gal}(L|K) \simeq \mathrm{Gal}(K|F).$$

Proof

If K is Galois over F, then by Theorem 9.2, $\mathrm{Gal}(L|K) \lhd \mathrm{Gal}(L|F)$.

It remains to establish the isomorphism. Let $\sigma \in \mathrm{Gal}(L|F)$. Note that $\sigma\big|_K$ is a map from K to σK. But K is Galois over F and therefore by Theorem 9.2, $\sigma K = K$. This implies that $\sigma\big|_K \in \mathrm{Gal}(K|F)$.

Consider $\varphi : \mathrm{Gal}(L|F) \to \mathrm{Gal}(K|F)$ where $\varphi(\sigma) = \sigma\big|_K$. Note that φ is a homomorphism since

$$(\sigma\tau)\big|_K(k) = \sigma\tau(k) = \sigma\big|_K(\tau\big|_K(k)).$$

We suppose $\sigma\big|_K = 1_K$. Then σ fixes K and thus, $\sigma \in \mathrm{Gal}(L|K)$. This implies that the kernel of φ is $\mathrm{Gal}(L|K)$. By first isomorphism theorem for groups, we deduce that

$$\mathrm{Gal}(L|F)/\mathrm{Gal}(L|K) \simeq \mathrm{Im}\,\varphi.$$

But since L is Galois over F and K,

$$|\mathrm{Im}\,\varphi| = |\mathrm{Gal}(L|F)|/|\mathrm{Gal}(L|K)| = [L:F]/[L:K] = [K:F] = |\mathrm{Gal}(K|F)|.$$

Therefore $\mathrm{Im}\,\varphi = \mathrm{Gal}(K|F)$.

□

9.3 Fundamental theorem of Galois Theory

Let $H \leq \mathrm{Gal}(L|F)$ where L is a finite extension of F. Define

$$L_H = \{\alpha \in L | \sigma(\alpha) = \alpha \ \text{ for all } \sigma \in H\}.$$

THEOREM 9.6 Let L be a Galois extension of F.

(a) For an intermediate field K with $F \subset K \subset L$,

$$\mathrm{Gal}(L|K) \subset \mathrm{Gal}(L|F)$$

has fixed field

$$L_{\mathrm{Gal}(L|K)} = K.$$

Furthermore,

$$|\mathrm{Gal}(L|K)| = [L : K] \text{ and } [\mathrm{Gal}(L|F) : \mathrm{Gal}(L|K)] = [K : F].$$

(b) For $H \leq \mathrm{Gal}(L|F)$, its fixed field $F \subset L_H \subset L$ has Galois group

$$\mathrm{Gal}(L|L_H) = H.$$

Furthermore,

$$[L : L_H] = |H| \text{ and } [L_H : F] = [\mathrm{Gal}(L|F) : H].$$

Proof
We first establish (a). Since L is Galois over F, L is Galois over K. Therefore $K = L_{\mathrm{Gal}(L|K)}$ by Theorem 8.1. Since both L is Galois over K and F, we conclude that

$$|\mathrm{Gal}(L|K)| = [L : K] \text{ and } \mathrm{Gal}(L|F) = [L : F].$$

Therefore,

$$|\mathrm{Gal}(L|F) : \mathrm{Gal}(L|K)] = [L : F]/[L : K] = [K : F].$$

To prove (b), let H be a subgroup of $\mathrm{Gal}(L|F)$. This gives $F \subset L_H \subset L$. For any $\sigma \in H$, $\sigma\big|_{L_H} = 1_{L_H}$. Therefore $H \subset \mathrm{Gal}(L|L_H)$. To prove equality, we use Theorem 6.4. Observe L is a finite separable extension of L_H since L is finite separable over F. This implies by Theorem 6.4 that $L = L_H(\alpha)$ for some $\alpha \in L$. Let

$$h(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)).$$

Note that $h(x)$ is fixed by H and hence $h(x) \in L_H[x]$.

Let $p(x)$ be the minimal polynomial of α in $L_H[x]$. Then $p(x)|h(x)$. This implies that

$$|H| = \deg(h(x)) \geq \deg(p(x)) = [L_H[x] : L_H] = [L : L_H].$$

But $|H| \leq |\mathrm{Gal}(L|L_H)| = [L : L_H]$, where the last equality follows from Theorem 7.6 since L is the splitting field of $p(x)$ over L_H. Therefore, $|H| = |\mathrm{Gal}(L|L_H)$ and we must have $H = \mathrm{Gal}(L|L_H)$. Now, $[L : L_H] = |H|$. Hence,

$$|\mathrm{Gal}(L|F)/\mathrm{Gal}(L|L_H)| = [L : F]/[L : L_H] = [L_H : F].$$

□

THEOREM 9.7 Let L be a Galois extension of F. Then the maps between intermediate fields K where $F \subset K \subset L$ and subgroups $H \subset \mathrm{Gal}(L|F)$ given by $K \to \mathrm{Gal}(L|K)$ and $H \to L_H$ reverse inclusions and are inverse of each other. Moreover, if a subfield K corresponds to a subgroup H under these maps then K is Galois over F if and only if $H \lhd \mathrm{Gal}(L|F)$. When this happens,

$$\mathrm{Gal}(L|F)/H \simeq \mathrm{Gal}(K|F).$$

Proof
By Theorem 9.6 (a), the composition of the first map followed by the second map yields

$$K \to L_{\mathrm{Gal}(L|K)} = K.$$

Similarly, by Theorem 9.6 (b), the composition of the second map followed by the first map yields

$$H \to \mathrm{Gal}(L|L_H) = H.$$

The map $K \to \mathrm{Gal}(L|K)$ is inclusion reversing: If $K_1 \subset K_2$, then an automorphism of L fixing K_2 must fix K_1. In other words, $\mathrm{Gal}(L|K_2) \subset \mathrm{Gal}(L|K_1)$.

The map $H \to L_H$ is also inclusion reversing: If $H_1 \subset H_2$, then $\alpha \in L$ which is fixed by H_2 is fixed by H_1. This implies $L_{H_2} \subset L_{H_1}$.

Finally, let $K = L_H$. If K is Galois over F, then by Theorem 9.2, $H = \mathrm{Gal}(L|L_H) \lhd \mathrm{Gal}(L|F)$. Conversely, if $H = \mathrm{Gal}(L|L_H) \lhd \mathrm{Gal}(L|F)$, then by Theorem 9.2, we conclude that $L_H = K$ is Galois over F.

□

THEOREM 9.8 If L is a finite separable extension of F, then there are finitely many fields K with $F \subset K \subset L$.

Proof
Let M be a field extension of L that is Galois over F. Subfields of M containing F corresponds to subgroups of $\mathrm{Gal}(M|F)$ by Theorem 9.7. Since $\mathrm{Gal}(M|F)$ is a finite group, it has finitely many subgroups. By the reverse map between subfields of M and subgroups of $\mathrm{Gal}(M|F)$, we conclude that M contains finitely many subfields. Therefore, L contains finitely many subfields.

□

We now give an examples to illustrate Theorem 9.7.

EXAMPLE 9.1 Let $L = \mathbf{Q}(\omega, 2^{1/3})$, where $\omega = e^{2\pi i/3}$. Let $G = \mathrm{Gal}(L|\mathbf{Q})$. Let $\sigma, \tau \in G$ be such that

$$\sigma(2^{1/3}) = \omega 2^{1/3}, \sigma(\omega) = \omega, \tau(2^{1/3}) = 2^{1/3} \text{ and } \tau(\omega) = \omega^2.$$

These two elements generate G and by verifying $\tau\sigma\tau^{-1} = \sigma^{-1}, \tau^2 = \sigma^3 = 1_G$, we deduce that $G \simeq S_3$. The subgroups of G are $< 1_G >, < \sigma >, < \tau >, < \sigma\tau >$ and $< \sigma^2\tau >$. We now illustrate with an example on the determination of L_H when H is a subgroup of G. Note that σ fixes ω and therefore $L_{<\sigma>}$ contains $\mathbf{Q}(\omega)$. But $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2 = (G :< \sigma >) = [L_{<\sigma>} : \mathbf{Q}]$. Therefore $L_{<\sigma>} = \mathbf{Q}(\omega)$. In a similar way, we can construct L_H for other subgroups H of G. But such constructions are often tedious even for very small groups.

9.4 Compositum of fields

DEFINITION 9.2 Let L be a field extension of F. We say that K is an intermediate field of $L|F$ if K is a field such that $F \subset K \subset L$.

DEFINITION 9.3 Let L be a field extension of F. Let E_1 and E_2 be intermediate fields of $L|F$. The compositum of E_1 and E_2, denoted by E_1E_2, is the intermediate field of $L|K$ containing E_1 and E_2.

We will also view $E_1 \cap E_2$ as the largest field that is contained in E_1 and E_2.

DEFINITION 9.4 Let G be a group and let H and K be subgroups of G. We define $H \vee K$ as the smallest subgroup G containing H and K.

Remark 9.1 It is known that if $HK = KH$ then HK is a group and $H \vee K = HK$. Note also that HVK is not always HK if HK is not a group. For example, HK is not a group when $H =< (1\,2) >$ and $K =< (2\,3) >$ while $H \vee K = S_3$.

We also view $H \cap K$ as the largest group that is contained in H and K.

THEOREM 9.9 (a) Let L be Galois over F and E_1, E_2 be intermediate fields of $L|F$. Then

$$\mathrm{Gal}(L|E_1E_2) \simeq \mathrm{Gal}(L|E_1) \cap \mathrm{Gal}(L|E_2)$$

and

$$\mathrm{Gal}(L|E_1 \cap E_2) \simeq \mathrm{Gal}(L|E_1) \vee \mathrm{Gal}(L|E_2).$$

(b) Let L be Galois over F and $G = \mathrm{Gal}(L|F)$. Let H and K be subgroups of G. Then

$$L_{H\vee K} = L_H \cap L_K$$

and

$$L_{H\cap K} = L_H L_K.$$

Proof
We will prove (a) and leave (b) as exercise. Now E_1E_2 is the smallest field containing E_1 and E_2. By the Galois correspondence, E_1E_2 corresponds to $\mathrm{Gal}(L|E_1E_2)$ and is the largest group contained in $\mathrm{Gal}(L|E_1)$ and $\mathrm{Gal}(L|E_2)$, a consequence of the order reversing property.

But the largest group contained in $\mathrm{Gal}(L|E_1)$ and $\mathrm{Gal}(L|E_2)$ is $\mathrm{Gal}(L|E_1) \cap \mathrm{Gal}(L|E_2)$.

Similarly, $E_1 \cap E_2$, which is the largest field contained in E_1 and E_2, must correspond to a group that is the smallest group containing $\mathrm{Gal}(L|E_1)$ and $\mathrm{Gal}(L|E_2)$. This implies that

$$\mathrm{Gal}(L|E_1 \cap E_2) = \mathrm{Gal}(L|E_1) \vee \mathrm{Gal}(L|E_2).$$

□

THEOREM 9.10 Let $f(x) \in F[x]$ be a separable polynomial and let L be the splitting field of $f(x)$. Let $f(x) = g(x)h(x)$ in $F[x]$. Let E_1 and E_2 be intermediate fields of $L|F$ which are splitting fields of $g(x)$ and $h(x)$ respectively. Suppose $E_1 \cap E_2 = F$, then

$$\mathrm{Gal}(L|F) \simeq \mathrm{Gal}(E_1|F) \times \mathrm{Gal}(E_2|F)$$

Proof
Recall that if H, K are normal subgroups of a group G, then $G = H \times K$ (a direct product of H and K) if $H \cap K = \{1\}$ and $H \vee K = G$.

Now E_1 and E_2, being splitting fields of $g(x)$ and $h(x)$ respectively, are Galois over F. Hence, $\mathrm{Gal}(L|E_1)$ and $\mathrm{Gal}(L|E_2)$ are both normal subgroups of $\mathrm{Gal}(L|F)$. Now E_1E_2 is a field where $f(x)$ splits and hence $L \subset E_1E_2$. On the

other hand, $E_1E_2 \subset L$ and hence $L = E_1E_2$. Now,

$$\mathrm{Gal}(L|E_1) \cap \mathrm{Gal}(L|E_2) = \mathrm{Gal}(L|E_1E_2) = \mathrm{Gal}(L|L) = \{1\}$$

and

$$\begin{aligned}\mathrm{Gal}(L|E_1 \cap E_2) &= \mathrm{Gal}(L|F) = \mathrm{Gal}(L|E_1) \vee \mathrm{Gal}(L|E_2) \\ &= \mathrm{Gal}(L|E_1)\mathrm{Gal}(L|E_2) = \mathrm{Gal}(L|E_1) \times \mathrm{Gal}(L|E_2).\end{aligned}$$

Finally,

$$\mathrm{Gal}(L|E_1) \simeq \mathrm{Gal}(L|F)/\mathrm{Gal}(L|E_2) \simeq \mathrm{Gal}(E_2|F)$$

and

$$\mathrm{Gal}(L|E_2) \simeq \mathrm{Gal}(L|F)/\mathrm{Gal}(L|E_1) \simeq \mathrm{Gal}(E_1|F)$$

and this completes the proof of the theorem. □

THEOREM 9.11 Let L be Galois over F and E be a finite extension of F. Then LE is Galois over E and

$$\mathrm{Gal}(EL|E) \simeq \mathrm{Gal}(L|L \cap E).$$

Proof
Since L is Galois over F, L is a splitting field of some separable polynomial $f(x)$ over F. Let $L = F(\alpha_1, \cdots, \alpha_n)$ where $\alpha_1, \cdots, \alpha_n$ are roots of $f(x)$. Then $EL = E(\alpha_1, \cdots, \alpha_n)$ is the splitting field of $f(x)$ viewed as a polynomial over $E[x]$. Therefore EL is Galois over E.

Let M be a Galois closure of EL over F. Then

$$\begin{aligned}\mathrm{Gal}(EL|E) &\simeq \mathrm{Gal}(M|E)/\mathrm{Gal}(M|EL) \\ &\simeq \mathrm{Gal}(M|E)/(\mathrm{Gal}(M|E) \cap \mathrm{Gal}(M|L)) \\ &\simeq \mathrm{Gal}(M|L)\mathrm{Gal}(M|E)/\mathrm{Gal}(M|L) \\ &\simeq \mathrm{Gal}(M|L \cap E)/\mathrm{Gal}(M|L) \simeq \mathrm{Gal}(L|L \cap E),\end{aligned}$$

where the third last isomorphism is established using second isomorphism theorem for groups. This completes the proof of the theorem.

□

9.5 Cyclotomic fields

DEFINITION 9.5 Let $n \geq 3$ be a positive integer and let $\zeta_n = e^{2\pi i/n}$. The field $\mathbf{Q}(\zeta_n)$ is called the cyclotomic field of n-th root of unity.

In this section, we will show that

$$[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n), \tag{9.2}$$

where $\varphi(n)$ is the number of integers between 1 and n that are relatively prime to n. The function $\varphi(n)$ is called the Euler φ function. We will prove (9.2) by showing that the polynomial

$$\Phi_n(x) = \prod_{\substack{\ell=1 \\ (n,\ell)=1}}^{n} (x - \zeta_n^\ell)$$

is irreducible. If this is true, then

$$[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \deg(\min_{\mathbf{Q}}(\zeta_n)) = \varphi(n).$$

We first observe that $\Phi_n(x) \in \mathbf{Z}[x]$. Note that

$$x^n - 1 = \prod_{d|n} \prod_{\substack{j=1 \\ (j,n)=n/d}}^{n} (x - e^{2\pi ij/n}) = \prod_{d|n} \Phi_d(x).$$

We will show that $\Phi_n(x) \in \mathbf{Z}[x]$ by induction. Note that $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$ and so $\Phi_k(x) \in \mathbf{Z}[x]$ for $k = 1$ and 2. Suppose $\Phi_k(x) \in \mathbf{Z}[x]$ for $k < n$. Let $\Phi_n(x) = a_0 + a_1x + \cdots + a_sx^s$ and

$$\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x) = b_0 + b_1x + \cdots b_tx^t.$$

Then

$$x^n - 1 = (a_0 + a_1x + \cdots + a_sx^s)(b_0 + b_1x + \cdots + b_tx^t).$$

Note that $a_0b_0 = -1$. Now, for $n > 1$, $a_0 = e^{2\pi iN/n}$ where

$$N = \sum_{\substack{j=1 \\ (j,n)=1}}^{n} j = \frac{n\varphi(n)}{2}.$$

This implies that $a_0 \in \mathbf{Z}$. Hence $b_0 = \pm 1$. Considering the coefficient of x,

$$a_0b_1 + a_1b_0 \in \mathbf{Z}.$$

Since $b_0 = \pm 1$, we conclude that $a_1 \in \mathbf{Z}$. By comparing the coefficients of x^k, for $0 \leq k \leq$, we conclude that $a_j \in \mathbf{Z}, 0 \leq j \leq s$ and therefore, $\Phi_n(x) \in \mathbf{Z}[x]$. We next show that $\Phi_n(x)$ is irreducible over $\mathbf{Q}$. We will follow the idea of Gauss. The following lemma is the first step to the proof of the irreducibility of $\Phi_n(x)$.

LEMMA 9.12 Let $f(x) \in \mathbf{Z}[x]$ be monic polynomial of degree greater than 1. Let p be a prime and $f_p(x)$ be a monic polynomial with the property that the roots of $f_p(x)$ are the p-th power of the roots of $f(x)$. Then

(a) $f_p(x) \in \mathbf{Z}[x]$,
(b) $f_p(x) \equiv f(x) \pmod{p}$.

Proof
If $f(x)$ has roots $\gamma_1, \cdots, \gamma_r$, $r = \deg(f(x))$, then

$$f_p(x) = \prod_{i=1}^{r}(x - \gamma_i^p) = x^r - \sigma_{r,1}(\gamma_1^p, \cdots, \gamma_r^p)x^{r-1} + \cdots + (-1)^r\sigma_{r,r}(\gamma_1^p, \cdots, \gamma_r^p).$$

Note that the coefficients of $f_p(x)$ are symmetric in $\gamma_1, \cdots, \gamma_r$ and so, they can be expressed in terms of $\sigma_{r,j}(\gamma_1, \cdots, \gamma_r)$ with coefficients in $\mathbf{Z}$. Since $f(x) \in \mathbf{Z}[x]$, this implies that $f_p(x) \in \mathbf{Z}[x]$. This completes the proof of (a).

To prove (b), observe that in F_p,

$$\sigma_{r,j}(\gamma_1^p, \cdots, \gamma_r^p) \equiv \sigma_{r,j}(\gamma_1, \cdots, \gamma_r)^p \equiv \sigma_{r,j}(\gamma_1, \cdots, \gamma_r) \pmod{p},$$

where the last congruence follows from Fermat's little theorem. Hence, $f_p(x) = f(x)$ in $F_p[x]$. □

We now prove the main result of this section.

THEOREM 9.13 For $n \geq 3$, $\Phi_n(x)$ is irreducible over $\mathbf{Q}$.

Proof
By Gauss Lemma, it suffices to prove that $\Phi_n(x)$ is irreducible over $\mathbf{Z}$. Suppose that $\Phi_n(x)$ is reducible. We may express $\Phi_n(x)$ as a product of monic irreducible polynomials over $\mathbf{Z}$. Let ω be a root of $\Phi_n(x)$. Then there is an irreducible polynomial $f(x)$ over $\mathbf{Z}$ which divides $\Phi_n(x)$ such that $f(\omega) = 0$. Next suppose $p \nmid n$. We claim that $f(\omega^p) = 0$.

Suppose not. Then $f(\omega^p) \neq 0$. By definition of $f_p(x)$ in Lemma 9.12, we conclude that $f_p(\omega^p) = 0$ since its zeroes are the p-th power of the zero of $f(x)$. Note that $f(x)$ and $f_p(x)$ has no root in common, for otherwise, $(f(x), f_p(x)) \neq 1$ and $f(x)$ would divide $f_p(x)$ since $f(x)$ is irreducible over $\mathbf{Z}$. This would imply that $f(x) = f_p(x)$ as the degrees of these two polynomials are the same. Therefore, for some polynomial $h(x)$, the factorization of $\Phi_n(x)$ in $\mathbf{F}_p[x]$ is given by

$$\Phi_n(x) = f(x)f_p(x)h(x) = f^2(x)h(x),$$

by Lemma 9.12 (b). But this is impossible since $\Phi_n(x)$, being a divisor of the separable polynomial $x^n - 1$ over $\mathbf{F}_p$, is separable. We must therefore conclude that $f(\omega^p) = 0$.

Now, given $(\ell, n) = 1$, write $\ell = q_1 \cdots q_s$ where q_i are primes with $(q_i, n) = 1$. Suppose $g(x) = \min_{\mathbf{Q}}(\zeta_n)$ and that it is a proper divisor of $\Phi_n(x)$. Then by the above, we observe that $g(\zeta_n^{q_1}) = 0$. Next, since $q_2 \nmid n$, we may apply the result we proved in the previous paragraph with $\omega = \zeta_n^{q_2}$ to deduce that $g(\zeta_n^{q_1 q_2}) = 0$.

By repeating this argument $s-1$ times, we conclude that $g(\zeta_n^\ell)=0$. Now, the degree of $g(x)$ must be at least $\varphi(n)$ and so, it cannot be a proper divisor of $\Phi_n(x)$. Hence, $\Phi_n(x)=g(x)$ and is therefore irreducible in $\mathbf{Z}[x]$.

□

COROLLARY 9.14 The degree $[\mathbf{Q}(\zeta_n):\mathbf{Q}]=\varphi(n)$.

9.6 Möbius function and the number of irreducible polynomials over $\mathbf{F}_p$

DEFINITION 9.6 The *Möbius function* $\mu(n)$ defined by $\mu(1)=1$ and for $n>1$ with

$$n=\prod_{k=1}^{m} p_k^{\alpha_k},$$

$$\mu(n)=\begin{cases}(-1)^m & \text{if } \alpha_i=1, 1\le i\le m\\ 0 & \text{otherwise.}\end{cases}.$$

The Möbius function, like $\varphi(n)$, satisfies

$$\mu(mn)=\mu(m)\mu(n)$$

when $(m,n)=1$. A function defined on positive integers which satisfies such relation is called a *multiplicative function.*

DEFINITION 9.7 The function $u(n)$ is defined by $u(n)=1$ for all positive integers n.

THEOREM 9.15 (The Möbius inversion formula) Let f and g be functions defined on the set of positive integers with values in $\mathbf{C}$. Then

$$f(n)=\sum_{d|n} g(d),$$

if and only if

$$g(n)=\sum_{d|n}\mu(n/d)f(d).$$

For a proof of the above theorem, see "*Introduction to Analytic Number Theory*" by T.M. Apostol or "*Analytic Number Theory for Undergraduates*" by H.H. Chan.

We observe that

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

This implies that

$$\ln(x^n - 1) = \sum_{d|n} \ln \Phi_d(x),$$

which by Theorem 9.15, leads to

$$\ln \Phi_n(x) = \sum_{d|n} \mu(n/d) \ln(x^d - 1).$$

Therefore,

$$\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)}. \tag{9.3}$$

From (9.3), we observe that since the left hand side is a polynomial in x, the right hand side, which appears to be a rational function in x must also be a polynomial. If we expand the right hand side in power series about the origin, we know that the coefficients of the power series would have to be integers since

$$\frac{1}{x^k - 1} = -(1 + x^k + x^{2k} + \cdots).$$

This implies that $\Phi_n(x) \in \mathbf{Z}[x]$. Alternatively, we may write the right hand side as $P(x)/Q(x)$ with $P(x), Q(x) \in \mathbf{Z}[x]$ and deduce that

$$Q(x)\Phi_n(x) = P(x).$$

Observing that the coefficient of the constant term of $Q(x)$ is ± 1, we may deduce as in the previous section that the coefficients of x^j, $0 \leq j \leq \varphi(n)$, are all integers, implying that $\Phi_n(x) \in \mathbf{Z}[x]$.

EXAMPLE 9.2 When $n = 6$, we find that

$$\Phi_6(x) = \frac{(x^6 - 1)(x - 1)}{(x^3 - 1)(x^2 - 1)} = x^2 - x + 1.$$

There is another reason why we introduce $\mu(n)$. We know that if p is a prime then the number of irreducible polynomials of a given degree n over $\mathbf{F}_p$ is finite. Theorem 9.15 allows us to give the number of irreducible polynomials of degree n over $\mathbf{F}_p$ explicitly if we know the factorization of n into primes.

We observe that if $f(x)$ is an irreducible polynomial of degree $n \geq 1$ and γ is one of its roots, then

$$\mathbf{F}_p(\gamma) \simeq \mathbf{F}_{p^n}.$$

Since every element β in $\mathbf{F}_{p^n}$ satisfies

$$\beta^{p^n} = \beta,$$

we conclude that $f(x)$ must divide $x^{p^n} - x$. This property holds for every irreducible polynomial of degree n over $\mathbf{F}_p$. We also observe that the roots of any irreducible polynomial $g(x)$ of degree d with $d|n$ must also lie in a field isomorphic to $\mathbf{F}_{p^d}$. This implies that $g(x)$ must also divide $x^{p^n} - x$. Therefore,

$$\prod_{d|n} \prod_{j_d=1}^{m_d} f_{j_d}(x) \quad \text{divides} \quad x^{p^n} - x,$$

where $f_{j_d}(x)$ is an irreducible polynomial of degree d. In other words, the roots (which are distinct) of

$$\prod_{d|n} \prod_{j_d=1}^{m_d} f_{j_d}(x)$$

are the roots of $x^{p^n} - x$.

Next, if $\alpha \in \mathbf{F}_{p^n}$, then it is a root of some irreducible polynomial of degree $d \geq 1$ over $\mathbf{F}_p$. This implies that all the roots of $x^{p^n} - x$ are roots of

$$\prod_{d|n} \prod_{j_d=1}^{m_d} f_{j_d}(x).$$

Therefore,

$$x^{p^n} - x = \prod_{d|n} \prod_{j_d=1}^{m_d} f_{j_d}(x) = \prod_{d|n} \prod_{j_d=1}^{m_d} f_{j_d}(x).$$

By counting the degrees of the polynomials on both sides, we conclude that

$$p^n = \sum_{d|n} d m_d.$$

By Theorem 9.15, we conclude that for $n \geq 2$,

$$m_n = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d.$$

EXAMPLE 9.3 When $n = 4, p = 2$, we find that

$$m_4 = \frac{1}{4}(-2^2 + 2^4) = 3.$$

The polynomials of degree 4 which are irreducible over $\mathbf{F}_2$ are

$$x^4 + x + 1, x^4 + x^3 + 1, \quad \text{and} \quad x^4 + x^3 + x^2 + x + 1.$$

9.7 Discriminant revisited

Let F be a field, with char $F \neq 2$. Let $f(x) \in F[x]$ be a separable polynomial with $\deg f(x) \geq 2$ and zeroes $\alpha_1, \cdots, \alpha_n$. L be a splitting field of $f(x)$. Recall that

$$\sqrt{\Delta(f)} = \prod_{i<j} (\alpha_i - \alpha_j) \in L.$$

We have seen that there exists a one to one homomorphism

$$\psi : \mathrm{Gal}(L|F) \to S_n.$$

Let τ_σ denote the image of σ in S_n under ψ. We have the following theorem:

THEOREM 9.16 Let F, $f(x)$ and L be defined as in the above paragraph. Then

(a) $\sigma(\sqrt{\Delta(f)}) = \mathrm{sgn}(\tau_\sigma)\sqrt{\Delta(f)}$,

(b) The image of $\mathrm{Gal}(L|F)$ under ψ lies in A_n, the set of even permutations in S_n, if and only if $\sqrt{\Delta(f)} \in F$.

Proof
Recall that

$$\sqrt{\Delta} = \prod_{i<j}(x_i - x_j)$$

has the property that $\tau \cdot \sqrt{\Delta} = \mathrm{sgn}(\tau)\sqrt{\Delta}$ for all $\tau \in S_n$. This yields

$$\prod_{i<j}(x_{\tau(i)} - x_{\tau(j)}) = \mathrm{sgn}(\tau) \prod_{i<j}(x_i - x_j).$$

Applying the evaluation map, we deduce that

$$\prod_{i<j}(\alpha_{\tau(i)} - \alpha_{\tau(j)}) = \mathrm{sgn}(\tau) \prod_{i<j}(\alpha_i - \alpha_j).$$

Let $\tau = \tau_\sigma$. Then $\sigma(\alpha_i) = \alpha_{\tau_\sigma(i)}$ and this implies that

$$\prod_{i<j}(\alpha_{\tau_\sigma(i)} - \alpha_{\tau_\sigma(j)}) = \sigma(\sqrt{\Delta(f)}).$$

This completes the proof of (a).

For (b), let L be Galois over F. Therefore, $F = L_{\mathrm{Gal}(L|F)}$. Now,

$$\sqrt{\Delta(f)} \in L_{\mathrm{Gal}(L|F)}$$

if and only if

$$\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)}$$

for $\sigma \in \mathrm{Gal}(L|F)$. This is equivalent to

$$\mathrm{sgn}(\tau_\sigma)(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)}.$$

The last identity is equivalent to $\tau_\sigma \in A_n$.

□

THEOREM 9.17 Let $f(x) \in F[x]$ e a monic irreducible separable cubic polynomial where $\mathrm{char}\, F \neq 2$. If L is the splitting field of $f(x)$ over F, then

$$\mathrm{Gal}(L|F) = \begin{cases} \mathbf{Z}/3\mathbf{Z} & \text{if } \Delta(f) \text{ is a square in } F, \\ S_3 & \text{otherwise.} \end{cases}.$$

Proof
The group $G = \mathrm{Gal}(L|F)$ acts transitively on roots of $f(x)$. This implies that $3||\mathrm{Gal}(L|F)|$. The group G is isomorphic to a subgroup of S_3 and there are two subgroups in S_3 with order divisible by 3. They are S_3 and $A_3 \simeq \mathbf{Z}/3\mathbf{Z}$. We have seen that $\mathrm{Gal}(L|F)$ is isomorphic to a subgroup of A_3 if and only if $\Delta(f)$ is a square. This completes the proof of the theorem. □

9.8 The return of irreducible quartic polynomials

We have seen that if L is the splitting field of an irreducible cubic polynomial, then

$$\mathrm{Gal}(L|\mathbf{Q}) \simeq S_3$$

if and only if $\Delta(f(x))$ is not a square in $\mathbf{Q}$. The analogue of this result for the irreducible quartic polynomials over $\mathbf{Q}$ is more complicated.

We first recall that if

$$f(x) = x^4 + qx^2 + rx + s$$

is irreducible with roots $\alpha_j, j = 1, 2, 3, 4$, then

$$u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$v = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$w = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

satisfies a cubic polynomial equation of the form

$$g(x) = x^3 - 2qx^2 + (q^2 - 4s)x + r^2 = 0.$$

The polynomial $g(x)$ is called the resolvent cubic of $f(x)$.

THEOREM 9.18 Let $f(x) = x^4 + qx^2 + rx + s$ be irreducible over $\mathbf{Q}$ and L be the splitting field of $f(x)$ over $\mathbf{Q}$ and $G = \mathrm{Gal}(L|\mathbf{Q})$. Let $M = \mathbf{Q}(u, v, w)$ be the splitting field of $g(x) = x^3 - 2qx^2 + (q^2 - 4s)x + r^2$ over $\mathbf{Q}$ and $m = |\mathrm{Gal}(M|\mathbf{Q})|$.

(i) If $m = 6$, then $G \simeq S_4$.

(ii) If $m = 3$, then $G \simeq A_4$.

(iii) If $m = 1$, then $G \simeq V$, where

$$V = \{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1)(2)(3)(4)\}.$$

(iv) If $m = 2$, then $G \simeq D_8$ or $\mathbf{Z}/4\mathbf{Z}$.

Proof

If $\sigma \in G \cap V$ then u, v, w is fixed by σ. Conversely, checking the 24 elements of S_4, we find that $\sigma \in S_4$ fixes $(\alpha_i + \alpha_j)(\alpha_k + \alpha_\ell)$ if and only if

$$\sigma \in V \cup \{(i\,j), (k\,\ell), (i\,k\,j\,\ell), (i\,\ell\,j\,k)\}.$$

This implies that if $\sigma \in G$ fixes u, v, w then $\sigma \in G \cap V$ since

$$\{(1\,2), (3\,4), (1\,3\,2\,4), (1\,4\,2\,3)\} \cap \{(1\,3), (2\,4), (1\,2\,3\,4), (1\,4\,2\,3)\} = \phi.$$

Therefore, σ fixes u, v, w if and only if $\sigma \in V \cap G$. Hence, $\mathrm{Gal}(L|\mathbf{Q}(u, v, w)) = G \cap V$. This implies that $\mathrm{Gal}(M|\mathbf{Q}) \simeq G/(G \cap V)$. Since $\mathrm{Gal}(M|\mathbf{Q}) \subset S_3$, we conclude that $m = |G|/|G \cap V| = |\mathrm{Gal}(M|\mathbf{Q})|$ must divide 6.

Next G is transitive on the roots of $f(x)$ and so it is divisible by 4. Hence $|G| = 4, 8, 12, 24$. If $m = 6$, then $|G| = 6|G \cap V| = 12$ or 24. If $|G| = 12$ then $G \simeq A_4$ but this means that $|G \cap V| = 4$ and $|G| = 6|G \cap V| = 24$, a contradiction. Therefore, $G \simeq S_4$.

If $m = 3$, then $|G| = 3|G \cap V| = 12, 24$. If $|G| = 24$, then $|G \cap V| = 8$ which is impossible since $|V| = 4$. Hence, $G \simeq A_4$.

If $m = 1$, then $|G| = |G \cap V| = 4\ell$. But $|V| = 4$ implies that $G \simeq V$.

Finally, if $m = 2$, then $|G| = 2|G \cap V| \leq 8$ since $|V| = 4$. This implies that $|G| = 4$ or 8. If $|G| = 8$, then $|G \cap V| = 4$ and $G \simeq D_8$, the Sylow 2-subgroup of S_4.

If $|G| = 4$, then G is a Klein 4 group or cyclic of order 4. But if G is a Klein 4 group, it cannot be V since this would imply that $G \cap V = V$ and violates the equation $|G| = 2|G \cap V|$. Therefore G has to be cyclic of order 4.

□

10 Solvable groups and simple groups

10.1 Solvable groups

DEFINITION 10.1 A finite group G is solvable if there are subgroups

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

such that for $i = 1, 2, \cdots, n$, we have

(a) $G_i \lhd G_{i-1}$
(b) $[G_{i-1} : G_i]$ is a prime number.

Note that (b) can be replaced by G_{i-1}/G_i is a cyclic group with prime order.

THEOREM 10.1 Every subgroup of a solvable group is solvable.

Proof
Let G be a solvable group and let H be a subgroup of G. Let

$$H_i = G_i \cap H, i = 1, \cdots, n.$$

Consider $\pi : H_{i-1} \to G_{i-1}/G_i$ that sends $h \in H_{i-1}$ to $hG_i \in G_{i-1}/G_i$. Observe that $h \in H_i$ is in the kernel of π if and only if $h \in G_{i-1}$. This implies that $\ker(\pi) = H_{i-1}$. Therefore, H_{i-1}/H_i is isomorphic to a subgroup of G_{i-1}/G_i. Since G_{i-1}/G_i is cyclic of prime order p, we conclude that $H_i = H_{i-1}$ or H_{i-1}/H_i is cyclic of prime order p. Discarding the duplicates,, we obtain a chain

$$\{e\} = H_m \subset H_{m-1} \subset \cdots \subset H_1 \subset H_0 = H,$$

where $[H_{j-1} : H_j]$ is prime. This implies that H is a solvable. □

We now discuss the main tool for dealing with solvable groups.

THEOREM 10.2 Let G be a finite group and H be a normal subgroup of G. Then G is solvable if and only if G/H and H are solvable.

Proof
The previous theorem shows that if G is solvable then H is solvable. We now show that G/H is solvable. Suppose G_i are subgroups of G with $G_i \lhd G_{i-1}$ and $[G_{i-1} : G_i]$ is prime. Next, since $G_i \lhd G_{i-1}$, we conclude that $HG_i \lhd HG_{i-1}$ since for $hg \in HG_{i-1}$,

$$hg(HG_i) = h(gH)G_i = h(Hg)G_i = H(gG_i) = H(G_ig) = (G_iH)g = G_iHhg = HG_ihg.$$

Furthermore,

$$\begin{aligned} HG_{i-1}/HG_i &\simeq HG_iG_{i-1}/HG_i \simeq G_{i-1}/(G_{i-1} \cap HG_i) \\ &\simeq (G_{i-1}/G_i)/((G_{i-1} \cap HG_i)/G_i). \end{aligned}$$

But G_{i-1}/G_i is cyclic of prime order and so, HG_{i-1}/HG_i is either trivial or cyclic of prime order. If it is trivial, we discard HG_i. In this way, we obtain $j_k \in \{1, \cdots, n\}$ such that $HG_{j_k}/H \lhd HG_{j_k-1}/H$ with the property that $(HG_{j_k}/H)/(HG_{j_k-1}/H)$ is a group of prime order. This implies that G/H is solvable.

Conversely, if H is solvable and G/H is solvable, then the fact that G is solvable follows from the observation that the groups $A_j/H \lhd A_{j-1}/H$, where the A_j's contain H, give rise to $A_j \lhd A_{j-1}$ with $[A_{j-1} : A_j] = p$ for some prime p. This yields a collection of subgroups satisfying

$$H = A_m \lhd A_{m-1} \lhd \cdots \lhd G.$$

The solvability of H implies that there are groups such that

$$B_\ell = \{1_G\} \lhd B_{\ell-1} \lhd \cdots \lhd B_0 = H,$$

with each B_{j-1}/B_j cyclic of prime order, we conclude, together with the chain of groups from H to G that G is solvable. □

COROLLARY 10.3 Every finite abelian group is solvable.

Proof
We use induction on $|G| = m$. If $|G| = 1$ or 2, G is solvable. Suppose $m \geq 2$ and any abelian group of order less than n is solvable. Let G be a group of order n. If n is prime, then we are done. Suppose n is composite. Let p be a prime that divides n. By Cauchy's theorem, there exists a subgroup H of order p. Now, H is solvable and G/H is solvable, by induction. This implies that G is solvable by Theorem 10.2. □

THEOREM 10.4 Let G be a group of order p^α, p prime. Then G is solvable.

Proof
Let G acts on G via

$$g \cdot x = gxg^{-1}.$$

Then $\mathcal{O}_x = \{gxg^{-1} | g \in G\}$. Then $|\mathcal{O}_x|$ divides $|G|$. Therefore, $|\mathcal{O}_x| = 1$ or divisible by p. If $|\mathcal{O}_x| = 1$, then $gxg^{-1} = x$ for all $g \in G$. This implies that $gx = xg$ and hence, x lies in $Z(G)$, the center of G. From the identity

$$|G| = \sum_{x \in Z(G)} |\mathcal{O}_x| + \sum_{x \notin Z(G)} |\mathcal{O}_x|,$$

we observe that $|Z(G)| > 1$.

We now prove by induction that every group of order p^α is solvable. When $\alpha = 1$, G is cyclic and therefore solvable. Suppose the statement is true for $\alpha \leq n-1$. Let G be a group of order p^n. Note that $Z(G) \lhd G$. Furthermore, $Z(G)$ is abelian and hence, solvable. Now, $G/Z(G)$ has order less than p^n since $|Z(G)| > 1$. Therefore, by induction hypothesis, $G/Z(G)$ is solvable. By Theorem 10.2, we conclude that G is solvable. □

10.2 Simple groups

DEFINITION 10.2 A group G is simple if its only normal subgroups are $\{e\}$ and G.

All cyclic groups $\mathbf{Z}/p\mathbf{Z}$ are simple. Here are more interesting simple groups.

THEOREM 10.5 The alternating group A_n is simple for $n \geq 5$

Proof
An ℓ-cycle lies in A_n if and only if ℓ is odd. If $n \geq 3$, A_n is generated by 3-cycle. Suppose $H \neq \{e\}, H \lhd A_n$. We want to show that $H = A_n$. First, we will show that H contains a 3-cycle. Let $\sigma \in H$. Let $(j_1\, j_2\, j_3)$ be a 3-cycle in A_n and $\sigma \in H$. Since $H \lhd A_n$, we conclude that

$$\sigma^{-1}(j_1\, j_2\, j_3)^{-1}\sigma(j_1\, j_2\, j_3) \in H.$$

Suppose one of the cycles in σ has length at least 4, i.e., $\sigma = (i_1\, i_2\, i_3\, i_4 \cdots) \cdots$. Then

$$\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma(i_2\, i_3\, i_4) = (i_2)(i_3\, i_4\, i_1) \in H.$$

Suppose σ has a 3-cycle. If σ is a 3-cycle, then we are done. Otherwise, we may assume that $\sigma = (i_1\, i_2\, i_3)(i_4\, i_5\, \cdots) \cdots$. Now,

$$\sigma^{-1}(i_2\, i_3\, i_5)^{-1}\sigma(i_2\, i_3\, i_5) = (i_1\, i_4\, i_2\, i_3\, i_5)$$

and so, H contains a 5-cycle and we apply our previous case to obtain a 3-cycle in H.

Finally, suppose σ is a product of 2-cycles. Let $\sigma = (i_1\, i_2)(i_3\, i_4)\cdots$ Then

$$\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma(i_2\, i_3\, i_4) = (i_2\, i_4)(i_3\, i_1) \in H.$$

Let i_5 be different from i_1, i_2, i_3 and i_4. Now,

$$((i_1\, i_3)(i_2\, i_4))^{-1}(i_1\, i_3\, i_5)^{-1}(i_1\, i_3)(i_2\, i_4)(i_1\, i_3\, i_5) = (i_1\, i_5\, i_3) \in H.$$

We next claim that H contains all 3-cycles. If i, j, k, i', j', k' are different, then we observe that

$$(k\, k')(i\, j')(k\, i')(i\, j)(i\, j\, k)((k\, k')(i\, j')(j\, i')(i\, j))^{-1} = (k'\, i'\, j').$$

If i, j, k is to be mapped to i, j', k', we use

$$(j\, j')(k\, k')(i\, j\, k)(k\, k')(j\, j') = (j'\, k'\, i).$$

Finally, if i, j, k is to be mapped to i, j, k', we use

$$(i\, j)(k\, k')(i\, j\, k)(k\, k')(i\, j) = (i\, k'\, j).$$

Hence, $H = A_n$.

□

We have shown that A_n is simple for $n \geq 5$.

Remark 10.1 We will leave it as an exercise to show that if $n \geq 5$, then the only normal subgroups of S_n are $\{1_{S_n}\}$ and A_n.

11 Solvable and Radical Extensions

11.1 Radical and Solvable extensions

DEFINITION 11.1 A field extension L of F is radical if there are fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L$$

such that for $i = 1, 2, \cdots, n$, there is a $\gamma_i \in G_i$ such that

$$F_i = F_{i-1}(\gamma_i),$$

where $\gamma_i^{m_i} \in F_{i-1}$ for some positive integers m_i.

Notice that if $b_i = \gamma_i^{m_i} \in F_{i-1}$, then γ_i is a m_i-th root of b_i. We write

$$F_i = F_{i-1}(\sqrt[m_i]{b_i}), b_i \in F_{i-1}.$$

Note that $\sqrt[m_i]{b_i}$ is used to denote the solution of $x^{m_i} = b_i$ that lies in F_i.

Remark 11.1 Note that although γ_i is a root of $x^{m_i} - \gamma_i^{m_i}$, the degree $[F_{j-1}(\gamma_i) : F_{j-1}]$ may not be m_i. For example, when $F = \mathbf{Q}$ and $\gamma = e^{2\pi i/3}$, $\mathbf{Q}(e^{2\pi i/3})$ is a radical extension of $\mathbf{Q}$ with $(e^{2\pi i/3})^3 = 1$ but the degree of the extension is 2.

Remark 11.2 We can replace m_i by primes in the chain of fields. For example if $p|m$ in the radical extension $F \subset F(\gamma)$ with $\gamma^m \in F$, we can refine the chain as

$$F \subset F(\gamma^{m/p}) \subset F(\gamma).$$

We may insert intermediate fields until we get a chain of radical extensions with the property that $F_i = F_{i-1}(\beta)$ with $\beta^{p_i} \in F_{i-1}$ where p_i is a prime. Once again, this does not mean that $[F_i : F_{i-1}] = p_i$.

The following examples show the existence of extensions which are not radical.

EXAMPLE 11.1 Let L be a splitting field of

$$f(x) = x^3 + x^2 - 2x - 1 \in \mathbf{Q}[x].$$

The discriminant $\Delta_{f(x)} = 7^2 > 0$. One can show that the roots of $f(x)$ are all real and that

$$\mathrm{Gal}(L|\mathbf{Q}) \simeq \mathbf{Z}/3\mathbf{Z}.$$

If $\mathbf{Q} \subset L$ were radical, then $[L : \mathbf{Q}] = 3$ implies that $L = \mathbf{Q}(\gamma)$, with $\gamma^m \in \mathbf{Q}$, for some positive integer m.

The minimal polynomial $g(x)$ of γ would divide $x^m - \gamma^m$ and of degree 3. (In other words $m \geq 3$.) Since L is Galois over $\mathbf{Q}$, $g(x)$ splits over $\mathbf{Q}(\gamma)$, so that if $\zeta_m = e^{2\pi i/m}$, then three of $\gamma, \zeta_m\gamma, \cdots, \zeta_m^{m-1}\gamma$ would be in L. This is impossible since $L \subset \mathbf{R}$. Hence L is not radical over $\mathbf{Q}$.

DEFINITION 11.2 A field extension L of F is solvable if there is a field extension M of L such that M is radical over F.

The above example motivates the following definition:

DEFINITION 11.3 A field extension L of F is solvable if there is a field extension M of L such that M is radical over F.

11.2 Compositums and Galois closures

DEFINITION 11.4 Suppose K_1 and K_2 are subfields of a field L. Then the compositum of K_1 and K_2 in L is the smallest subfield of L containing K_1 and K_2. We denote the compositum of K_1 and K_2 by K_1K_2.

We have seen in Section 8.2 that every finite separable extension L of F has a Galois closure, which may be thought of as the smallest Galois extension of F containing L. The Galois closure of L can expressed in terms of compositums as follow:

THEOREM 11.1 Suppose $F \subset L \subset M$ where M is Galois over F. Then the compositum of all conjugate fields of L in M is the Galois closure of L over F.

Proof
Theorem of primitive element implies that $L = F(\alpha)$ for some $\alpha \in L$. Since M is Galois over F, the minimal polynomial $h(x)$ of α over F is separable and splits in M. Let $h(x) = (x - \alpha_1)\cdots(x - \alpha_r)$ where $\alpha_1 = \alpha$. It follows that $K = L(\alpha_1, \cdots, \alpha_r)$ is a Galois extension of F containing L. We claim that K is the smallest Galois extension of F containing L. Suppose K' is Galois over F and contains L. Then K' contains K. If $\sigma \in \mathrm{Gal}(M|F)$ then $\sigma(L) = F(\sigma(\alpha)) \in K$. Therefore, the compositum K^* of $\sigma(L)$ for all $\sigma \in \mathrm{Gal}(M|F)$ is a Galois extension contained in K. Since K^* contains F and $\alpha_1, \cdots, \alpha_r$, by minimality of K, we conclude that $K \subset K^*$. Therefore K is the compositum K^* and every Galois extension K' contains K^*. In other words, K^* is the Galois closure of L. □

11.3 Properties of Radical and Solvable extension

LEMMA 11.2 Let F be a subfield of L.

(a) If L is radical over F and M is radical over L, then M is radical over F.
(b) If K_1 and K_2 are subfields of L and contain F such that K_1 is radical over F, then K_1K_2 is radical over K_2.
(c) If K_1 and K_2 are subfields of L and contain F such that K_1 and K_2 are radical over F, then K_1K_2 is radical over F.

Proof
To prove (a), we splice the two chains of extensions arising from the assumptions that M is radical over L and L is radical over F.

To prove (b), let

$$F = F_0 \subset F_1 \cdots \subset F_{n-1} \subset F_n = K_1,$$

with $F_i = F_{i-1}(\gamma_i)$ such that $\gamma_i \in F_i$ and $\gamma_i^{m_i} \in F_{i-1}, 1 \leq i \leq n$. Let $E_0 = K_2$ and $E_j = E_{j-1}(\gamma_j), 1 \leq j \leq n$. Note that $F_j \subset E_j$ since $F_0 \subset K_2$. Hence, E_n is radical over K_2. Now, $K_1 = F_n \subset E_n$ and $K_2 \subset E_n$. This implies that $K_1K_2 \subset E_n$. On the other hand, $E_n \subset K_2F_n = K_2K_1$ as it can be shown by induction that $E_j \subset K_2F_j$ ($E_j = E_{j-1}(\gamma_j) \subset K_2F_{j-1}(\gamma_j) = K_2F_j$).

For (c), we observe that by (b) that K_1K_2 is radical over K_2. Now K_2 is radical over F. Therefore, by (a), K_1K_2 is radical over F.

□

THEOREM 11.3 If L is separable and radical over F, then its Galois closure is also radical.

Proof

Let M be an extension of L such that M is Galois over F. Given $\sigma \in \mathrm{Gal}(M|F)$, $F \subset \sigma(L) \subset M$. Since L is radical over F, $\sigma(L)$ is radical over F. By Lemma 11.2, we conclude that $L\sigma(L)$ is radical over F. This implies that the Galois closure of L, which is the compositum of the conjugate fields of L, is radical over F.

□

COROLLARY 11.4 Let F be a field of characteristic 0. If L is a finite solvable extension of F, then the Galois closure of L over F is also solvable.

Proof
Since L is solvable, there exist an extension M of L which is radical over F. Since the characteristic of F is 0, M is separable. The Galois closure N of M is radical, by Theorem 11.3. Now, N contains L and Galois over F. This implies that N contains the Galois closure of L and hence, the Galois closure of L is solvable. □

12 Solvability by radicals

All fields in this chapter will have characteristic 0.

12.1 Solvable extensions and solvable groups

LEMMA 12.1 Let L be a Galois extension of F. Let ζ be a primitive m-th root of unity. Then $L(\zeta)$ is Galois over F and $F(\zeta)$ and the following are equivalent:

(a) $\mathrm{Gal}(L|F)$ is solvable.
(b) $\mathrm{Gal}(L(\zeta)|F)$ is solvable.
(c) $\mathrm{Gal}(L(\zeta)|F(\zeta))$ is solvable.

Proof
By Theorem 6.4, $L = F(\alpha)$ for some $\alpha \in L$. The field $L(\zeta)$ is the splitting field of the product of $x^m - 1 \in F[x]$ and $h(x) \in F[x]$ where $h(x)$ is the minimal polynomial of α. This implies that $L(\zeta)$ is Galois over F. Since $L(\zeta)$ is Galois over F, it is Galois over $F(\zeta)$.

We now prove the equivalence of (a) and (b). The key is to show that $\mathrm{Gal}(L(\zeta)|L)$ is abelian. Given any $\sigma \in \mathrm{Gal}(L(\zeta)|L)$, its image on $L(\zeta)$ is determined by its action on ζ. Now, if $\sigma, \tau \in \mathrm{Gal}(L(\zeta)|L)$ and $\sigma(\zeta) = \zeta^\nu$ and $\tau(\zeta) = \zeta^\mu$, then

$$\sigma\tau(\zeta) = \sigma(\zeta^\mu) = \zeta^{\nu\mu} = \zeta^{\mu\nu} = \tau\sigma(\zeta).$$

Therefore, $\sigma \in \mathrm{Gal}(L(\zeta)|L)$ is abelian and hence solvable.

Now $\mathrm{Gal}(L|F)$ is solvable and $\mathrm{Gal}(L(\zeta)|L)$ is solvable. This implies that $\mathrm{Gal}(L(\zeta)|F)$ is solvable. The converse follows from the fact that if G is solvable and H is a normal subgroup, then H and G/H are solvable.

Suppose $\mathrm{Gal}(L(\zeta)|F)$ is solvable. Then since $\mathrm{Gal}(L(\zeta)|F(\zeta))$ is a subgroup of $\mathrm{Gal}(L(\zeta)|F)$, it is solvable. Conversely, suppose $\mathrm{Gal}(L(\zeta)|F(\zeta))$ is solvable. Together with the fact that $\mathrm{Gal}(F(\zeta)|F)$ is solvable, we conclude that $\mathrm{Gal}(L(\zeta)|F)$ is solvable.

□

The next lemma is crucial.

LEMMA 12.2 Suppose M is Galois over K with $\mathrm{Gal}(M|K)$ cyclic of prime order p. If K contains a primitive p-th root of unity ζ, then there is $\alpha \in M$ such that $M = K(\alpha)$ with $\alpha^p \in K$.

Proof

We let σ be the generator of the cyclic group $G = \mathrm{Gal}(M|K)$. Let $\beta \in M$ with $\beta \notin K$. Let

$$\alpha_i = \sum_{j=0}^{p-1} \zeta^{-ji} \sigma^j(\beta).$$

Then

$$\begin{aligned}\sigma(\alpha_i) &= \sum_{j=0}^{p-1} \zeta^{-ij} \sigma^{j+1}(\beta) \\ &= \sum_{\ell=1}^{p} \zeta^{-i\ell+i} \sigma^{\ell}(\beta) = \zeta^i \alpha_i.\end{aligned}$$

This implies that

$$\sigma(\alpha_i) = \zeta^i \alpha_i. \tag{12.1}$$

When $i = 0$, then $\sigma(\alpha_0) = \alpha_0$ implies that

$$\alpha \in K,$$

since σ generates G which implies that α_0 is fixed by all the elements in G. Suppose there exists an i with $1 \leq i \leq p-1$ and $\alpha_i \neq 0$, then $\alpha_i \notin K$ since σ does not fix α_i. This implies that $M = K(\alpha_i)$ since $[K(\alpha_i) : K] = p = [M : K]$. Furthermore, from (12.1), we conclude that $\sigma(\alpha_i^p) = \alpha_i^p$ and thus, $\alpha_i^p \in K$. In other words, we may choose $\alpha = \alpha_i$ and the proof of our lemma is complete.

To complete the proof, we show that there is indeed an i with $1 \leq i \leq p-1$ such that $\alpha_i \neq 0$. Suppose the contrary and that $\alpha_i = 0$ for $1 \leq i \leq p-1$. Then adding up α_i, including the case $i = 0$, we conclude that

$$\alpha_0 = \sum_{i=0}^{p-1} \alpha_i = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \zeta^{-ij} \sigma^j(\beta) = \sum_{j=0}^{p-1} \sigma^j(\beta) \sum_{i=0}^{p-1} \zeta^{-ij} = p\beta. \tag{12.2}$$

Observe that since

$$\alpha_0 = \sum_{j=0}^{p-1} \sigma^j(\beta),$$

$$\sigma(\alpha_0) = \sum_{j=0}^{p-1} \sigma^{j+1}(\beta) = \alpha_0,$$

and this implies that $\alpha_0 \in K$. The identity (12.2), namely, $p\beta = \alpha_0$, together

with $\alpha_0 \in K$, implies that $\beta \in K$. This contradicts our assumption that $\beta \notin K$ and we conclude that there exists an i with $1 \leq i \leq p-1$ such that $\alpha_i \neq 0$.

□

12.2 Galois' Theorem for solvable extension

THEOREM 12.3 Let L be a Galois extension of F. The following are equivalent:

(a) L is a solvable extension of F.
(b) $\mathrm{Gal}(L|F)$ is a solvable group.

Proof

We will show that (a) implies (b). We first reduce to the radical case. Since L is solvable, there exists an M containing L which is radical over F. Let N be the Galois closure of M over F. By Theorem 11.3, we deduce that N is radical over F.

It suffices to show that $\mathrm{Gal}(N|F)$ is solvable. This is because $\mathrm{Gal}(L|F) \simeq \mathrm{Gal}(N|F)/\mathrm{Gal}(N|L)$ and $\mathrm{Gal}(L|F)$ is solvable since it is a quotient group of a solvable group, by Theorem 10.2.

Since N is radical over F, there exists $F_0 = F, F_1, \cdots, F_\ell = N$ such that

$$F_0 \subset F_1 \subset \cdots \subset F_\ell$$

such that $F_j = F_{j-1}(\gamma_j)$ with $\gamma_j^{q_j} \in F_{j-1}$. Let ζ be a primitive $q_1 q_2 \cdots q_\ell$-th root of unity. Consider the chain of fields

$$F_0^* \subset F_1^* \subset \cdots \subset F_\ell^*,$$

where $F_j^* = F_j(\zeta)$. It could happen that $F_j^* = F_{j-1}(\zeta, \gamma_j)$ (for example, when $\gamma_j^{q_j} = 1$) and in this case we discard F_j^*. We then obtain a chain of fields

$$F_0^* \subset F_{j_1}^* \subset \cdots \subset F_{j_k}^* = N(\zeta),$$

with $\gamma_{j_s}^{q_{j_s}} \in F_{j_s-1}^*$ and $\gamma_{j_s} \notin F_{j_s-1}^*$. Note that by Theorem 4.10, we conclude that $x^{q_{j_s}} - \gamma_{j_s}^{q_{j_s}}$ is irreducible over $F_{j_s-1}^*$ and therefore

$$[F_{j_s}^* : F_{j_s-1}^*] = q_{j_s}.$$

By applying the Galois correspondence, we obtain the series of groups

$$\mathrm{Gal}(N(\zeta)|N(\zeta)) \subset \cdots \subset \mathrm{Gal}(N(\zeta)|F_{j_1}^*) \subset \mathrm{Gal}(N(\zeta)|F(\zeta)),$$

with $\mathrm{Gal}(N(\zeta)|F_{j_s-1})/\mathrm{Gal}(N(\zeta)|F_{j_s})$ isomorphic to a cyclic group of order q_s and this implies that $\mathrm{Gal}(N(\zeta)|F(\zeta))$ is solvable. By Theorem 12.1, we conclude that $\mathrm{Gal}(N|F)$ is solvable and this, as mentioned earlier, implies that $\mathrm{Gal}(L|F)$ is solvable.

We now show that (b) implies (a). Let L be Galois over F with solvable Galois

group. Let $m = |\mathrm{Gal}(L|F)|$ and suppose ζ is a primitive m-th root of unity. By Theorem 12.1, we conclude that $\mathrm{Gal}(L(\zeta)|F(\zeta))$ is solvable since $\mathrm{Gal}(L|F)$ is solvable. We claim that

$$\mathrm{Gal}(L(\zeta)|F(\zeta))||\mathrm{Gal}(L|F)|. \tag{12.3}$$

To see this, we define the homomorphism

$$\varphi : \mathrm{Gal}(L(\zeta)|F(\zeta)) \to \mathrm{Gal}(L(\zeta)|F)/\mathrm{Gal}(L(\zeta)|L),$$

by

$$\varphi(\sigma) = \sigma\mathrm{Gal}(L(\zeta)|L).$$

Note that the kernel of φ is the $1_{\mathrm{Gal}(L(\zeta)|F(\zeta))}$ and this implies that $\mathrm{Gal}(L(\zeta)|F(\zeta))$ is isomorphic to a subgroup of $\mathrm{Gal}(L(\zeta)|F)/\mathrm{Gal}(L(\zeta)|L) \simeq \mathrm{Gal}(L|F)$. This proves (12.3). Since $\mathrm{Gal}(L(\zeta)|F(\zeta))$ is solvable, there exists a chain of groups

$$G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}(L(\zeta)|F(\zeta)),$$

such that G_{j-1}/G_j is cyclic of prime order q_j. Note that q_j divides m. By the Galois correspondence, we obtain a chain of fields

$$F(\zeta) \subset L_{G_1} \subset \cdots \subset L_{G_{n-1}} \subset L_{G_n}.$$

Note that $[L_{G_j} : L_{G_{j-1}}] = q_j$ and these fields contain the primitive q_j-th root of unity since it contains ζ which is a primitive m-th root of unity. By Lemma 12.2, we deduce that $L_{G_j} = L_{G_{j-1}}(\alpha_j)$ with $\alpha_j^{q_j} \in L_{G_{j-1}}$ and therefore, $L(\zeta)$ is radical over $F(\zeta)$. Clearly $F(\zeta)$ is radical over F. Therefore by Theorem 11.2(a), we conclude that $L(\zeta)$ is radical over F. Now $L(\zeta)$ contains L and so this implies that L is solvable over F and the proof is complete. □

12.3 Solving polynomials by radicals

All fields in this section will be of characteristic 0.

DEFINITION 12.1 Let $f(x) \in F[x]$ be nonconstant with splitting field L.

(a) A root $\alpha \in L$ of $f(x)$ is expressible by radicals over F if α lies in some radical extension of F.
(b) The polynomial $f(x)$ is solvable by radicals over F if L is a solvable extension.

THEOREM 12.4 Let $f(x) \in F[x]$ be irreducible. Then $f(x)$ is solvable by radicals over F if and only if $f(x)$ has a root expressible by radicals over F.

Proof
If $f(x)$ is solvable by radicals over F then the splitting field of $f(x)$ is solvable. This implies that L lies in a radical extension and all the roots of $f(x)$ are expressible by radicals over F. Conversely, suppose $f(x)$ has a root α in some radical extension of L. This means that $F(\alpha)$ is solvable. By Corollary 11.4, we know that if M is the Galois closure of $F(\alpha)$ over F, then M is solvable. Since a Galois extension is normal and $f(x)$ is irreducible over F with a root in M, we conclude that $f(x)$ splits completely over M. Thus M contains the splitting field L of $f(x)$ over F. Hence, L is solvable and the proof is complete.

□

If $f(x) \in F[x]$ is irreducible and L is the splitting field of $f(x)$, then the Galois group of $f(x)$ is $\mathrm{Gal}(L|F)$. By Theorem 12.3, we conclude the following:

THEOREM 12.5 A polynomial $f(x) \in F[x]$ is solvable by radicals over F if and only if the Galois group of $f(x)$ over F is solvable.

We can now apply the above theorem to polynomials of low degrees.

THEOREM 12.6 If $f(x) \in F[x]$ has degree $n \leq 4$, then $f(x)$ is solvable by radicals.

EXAMPLE 12.1 The polynomial $f(x) = x^5 - 6x + 3$ is irreducible over $\mathbf{Q}$ and has two complex roots since it has two turning points for which one is above and the other is below the x-axis. The Galois group of the splitting field of $f(x)$ is transitive on the roots and its order is divisible by 5. By Cauchy's theorem, the group contains an element that corresponds to a 5-cycle in S_5. Since the Galois group also contains a transposition corresponding to the complex conjugation which switches the two complex roots, we deduce that the Galois group is generated by a 5-cycle and a 2-cycle and must be isomorphic to S_5. Since S_5 is not solvable, we conclude that $f(x)$ is not solvable by radicals.

12.4 Artin's proof of the Fundamental Theorem of Algebra

THEOREM 12.7 Every nonconstant polynomial in $\mathbf{C}[x]$ splits completely over $\mathbf{C}$.

Proof
It suffices to show that every nonconstant polynomial in $\mathbf{R}[x]$ splits completely over $\mathbf{C}$. Let $f(x) \in \mathbf{R}[x]$ and L be its splitting field. Note that L is Galois over $\mathbf{R}$. Let $G = \mathrm{Gal}(L|\mathbf{R})$. Let H be defined as $\{e\}$ if $|G|$ is odd and H be a 2-Sylow subgroup of G if $|G|$ is even.

By the Galois correspondence, the fixed field L_H has degree $[L_H : \mathbf{R}] = [G : H] = |G|/|H|$.. This is odd by definition of H. This implies that L_H has odd degree over $\mathbf{R}$. Let $L_H = \mathbf{R}(\alpha)$. Then the minimal polynomial $h(x)$ of α has odd degree. But this means that $h(x)$ has a root in $\mathbf{R}$ and $h(x)$ being irreducible implies that the degree of $h(x)$ is 1. This forces $L_H = \mathbf{R}$ and $G = H$. Therefore $|G|$ must be a power of 2. Let $|G| = 2^n$. If $n = 0$, then G is trivial and this implies that $L = \mathbf{R}$ and so $f(x)$ splits completely over $\mathbf{R}$. Suppose $n \geq 1$. Since p-groups are solvable, we conclude that G is solvable. Let

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$$

be such that $G_i \lhd G_{i-1}$ of index 2 for $1 \leq i \leq n$. This the chain of fields

$$L_{G_0} \subset L_{G_1} \subset \cdots \subset L_{G_n}$$

such that $[L_{G_i} : L_{G_{i-1}}] = 2$ for $1 \leq i \leq n$. Suppose $n \geq 1$, then $[L_{G_1} : \mathbf{R}] = 2$. The minimal polynomial of the primitive element of L_{G_1} is quadratic with no real roots and hence $L_{G_1} \simeq \mathbf{C}$.

Suppose $n \geq 2$. Then L_{G_2} is of degree 2 over $\mathbf{C}$ and we know that this is impossible since every quadratic polynomial in $\mathbf{C}$ splits completely over $\mathbf{C}$. Hence we must have $n = 1$, which implies that $L = L_{G_1} \simeq \mathbf{C}$. It follows that $f(x)$ splits completely over $\mathbf{C}$.

□

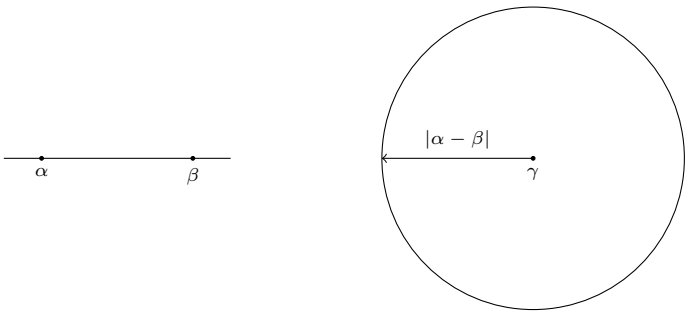
13 Geometric constructions

13.1 Constructible numbers

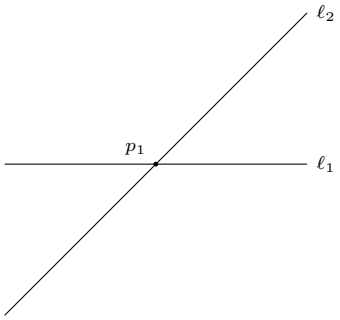
Recall that a straightedge is an unmarked ruler. A compass is a device used to draw circular arcs. Using a straightedge and compass, we can produce points on a plane starting with two given points 0 and 1. We now carefully describe the points, lines and circles which we can construct using straight edge and compass starting from 0 and 1.

C1. From two points α and β, we can draw a line ℓ that passes through α and β as illustrated in the following diagram using a straightedge:

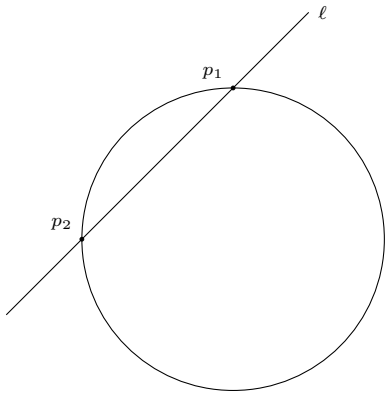
C2. Given three points α, β and γ, we can draw a circle C with center γ whose radius is the distance between α and β.



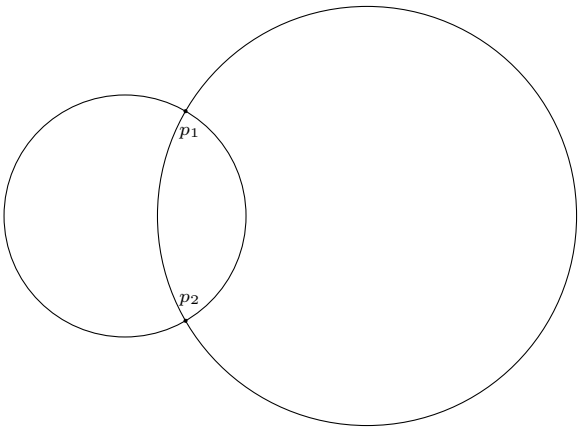
P1. The point of intersection of distinct lines ℓ_1 and ℓ_2.



P2. The points of intersection of a line ℓ and a circle.



P3. The points of intersection of two circles.



We identify the plane as the geometric representation of $\mathbf{C}$. Constructing a

point on the plane will mean constructing a complex number. As mentioned earlier, we will start our construction from 0 and 1.

DEFINITION 13.1 A complex number α is constructible if there exists a finite sequence of straightedge and compass constructions using C1, C2, P1, P2, and P3 that begins with 0 and 1 and ends with α.

EXAMPLE 13.1 2 and i are both constructible.

EXAMPLE 13.2 To construct a regular polygon with n sides with center 0, we need to construct $e^{2\pi i/n}$ in $\mathbf{C}$. We will determine n for which a regular n-gon can be constructed from 0 and 1.

13.2 The field of constructible numbers

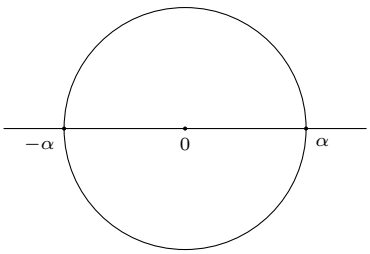
THEOREM 13.1 The set

$$\mathcal{C} := \{\alpha \in \mathbf{C} | \alpha \text{ is constructible.}\}$$

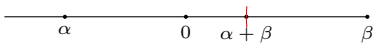
is a subfield of $\mathbf{C}$. Furthermore,

(a) $\alpha = a + ib \in \mathcal{C}$ if and only if $a, b \in \mathcal{C}$,
(b) $\alpha \in \mathcal{C}$ implies that $\sqrt{\alpha} \in \mathcal{C}$.

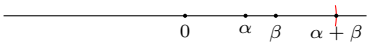
Proof
We first show that $\mathcal{C}$ is a subgroup of $\mathbf{C}$ under addition. Let $\alpha \in \mathcal{C}$. We draw a straightedge connecting α to 0 and beyond, followed by marking $-\alpha$ using the compass.



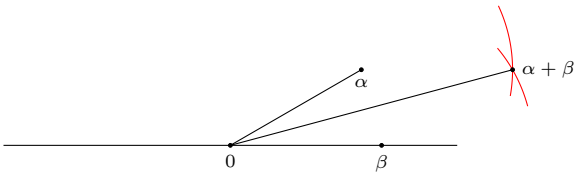
Suppose $\alpha, \beta \in \mathcal{C}$. If α, β and 0 are collinear, then we construct $\alpha + \beta$ as follow:



or



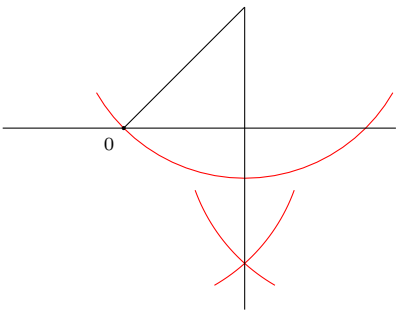
If α, β, and 0 are not collinear, then we use the compass to create $\alpha + \beta$ as follow:



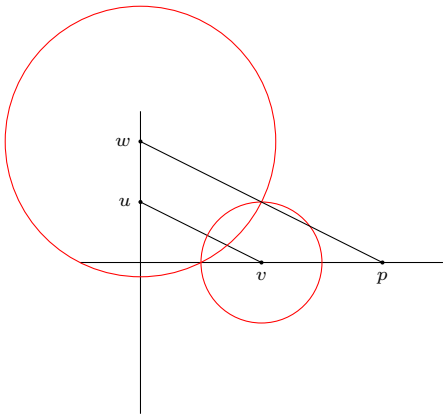
This shows that $(\mathcal{C}, +)$ is a group.

Before showing $(\mathcal{C} - \{0\}, \cdot)$ is a group, we first show (a). If $a, b \in \mathcal{C}$, then certain $a + ib \in \mathcal{C}$ since $i \in \mathcal{C}$ and $(\mathcal{C}, +)$ is a group.

Suppose $a + ib \in \mathcal{C}$ with $a, b \in \mathbf{R}$. We may then obtain a and b as follow:

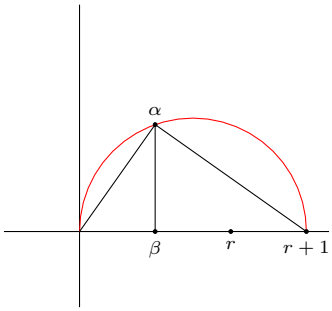


We next show that $(\mathcal{C} - \{0\}, \cdot)$ is a group. We will need to recall how we construct a line parallel to a given line joining two given points. The construction is similar to constructing a parallelogram. We construct two circles, one with center v with radius $|w - u|$ and the other circle with center w with radius $|u - v|$. The following is the diagram for this construction:



In the above diagram, if we choose $u = i$, $w = ib$, $v = a$, then $p = ab$. This shows that ab is constructible if $a, b \in \mathcal{C}$. If we choose $u = ia$, $v = 1$, $w = i$, then $p = 1/a$. This implies that if $a \in \mathcal{C}$ then $1/a \in \mathcal{C}$.

Finally, we show that if a nonzero $a \in \mathcal{C}$ then $\sqrt{a} \in \mathcal{C}$. We write $a = re^{i\theta}$. Given θ which is constructible, we can always bisect θ. We must now show that given r, we can construct $\sqrt{r}$. This is done by constructing the point p by using the following diagram:



The length between α and β is $\sqrt{r}$.

□

Remark 13.1 The number $e^{2\pi i/5}$ is constructible since

$$e^{2\pi i/5} = \frac{-1+\sqrt{5}}{4} + \frac{i}{2}\sqrt{\frac{5+\sqrt{5}}{2}}.$$

13.3 A characterization of $\mathcal{C}$

THEOREM 13.2 The complex number α belongs to $\mathcal{C}$ if and only if there are subfields

$$\mathbf{Q} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n \subset \mathbf{C}$$

such that $\alpha \in F_n$ and $[F_j : F_{j-1}] = 2$ for $1 \leq j \leq n$.

Proof
Suppose

$$\mathbf{Q} = F_0 \subset F_1 \subset \cdots \subset F_n \subset \mathbf{C},$$

where $[F_j : F_{j-1}] = 2$. Then $F_j = F_{j-1}(\sqrt{\alpha_j})$ for some $\alpha_j \in F_i$. We now prove by induction that $F_j \subset \mathcal{C}$. Note that $\mathbf{Q} = F_0 \subset \mathcal{C}$. Suppose $F_{j-1} \subset \mathcal{C}$. Then α_j is constructible. This implies that $\sqrt{\alpha_j}$ is constructible. Since $\mathcal{C}$ is a field, it must contains $F_{j-1}(\sqrt{\alpha_j}) = F_j$. Therefore $F_j \subset \mathcal{C}$ for $1 \leq i \leq n$. Finally, since $\alpha \in F_n$, we deduce that $\alpha \in \mathcal{C}$.

Conversely, given $\alpha \in \mathcal{C}$. We will construct $F_0, F_1, \cdots, F_n$ with $[F_j : F_{j-1}] = 2$, which eventually contains α. We used induction on N, the number of times we $P1, P2$ and $P3$ beginning with points on $\mathbf{Q} \subset \mathcal{C}$.

For $N = 0$, $\alpha \in \mathbf{Q} \subset \mathcal{C}$.

Next, we observe that if a, b are constructed in $N-1$ times of P_1, P_2 and P_3, then there exists

$$\mathbf{Q} \subset F_1 \subset \cdots \subset F_\ell$$

and

$$\mathbf{Q} \subset F_1' \subset \cdots \subset F_m'$$

with $[F_i : F_{i-1}] = 2$ and $[F_i' : F_{i-1}'] = 2$, with $a \in F_\ell$ and $b \in F_m'$. Hence, a, b is contained in $F_\ell F_\ell'$, with

$$\mathbf{Q} \subset F_1 \subset \cdots \subset F_\ell \subset F_\ell F_1' \subset \cdots \subset F_\ell F_m'.$$

Here

$$[F_\ell F_i' : F_\ell] = [F_i' : F_i' \cap F_\ell] = 1 \text{ or } 2.$$

This means that if a_k are constructed in $N-1$ steps with P_1, P_2 or P_3 starting from points in $\mathbf{Q}$, there are fields F_j such that $[F_j : F_{j-1}] = 2$ with $a_k \in F_n$ where F_n is the last field in the inclusions.

Now, suppose α is constructed in $N > 1$ steps where the last step uses $P1$, the intersection of distinct lines ℓ_1 and ℓ_2. But ℓ_1 was constructed from distinct α_1 and β_1 using $C1$ and ℓ_2 was constructed from distinct α_2 and β_2. By induction

assumptions, there exist

$$F_0 \subset F_1 \subset \cdots \subset F_n \subset \mathbf{C},$$

where $[F_j : F_{j-1}] = 2$ such that F_n contains real and imaginary parts of $\alpha_1, \beta_1, \alpha_2, \beta_2$. We aim to show that F_n contains the real and imaginary parts of α. Suppose ℓ_1 has equation $a_1x+b_1y = c_1$ and ℓ_2 has equation $a_2x+b_2y = c_2$, $a_1, b_1, c_1, a_2, b_2, c_2 \in F_n$. If u and v are real and imaginary parts of α, then

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}^{-1} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}.$$

This implies that $u, v \in F_n$, which implies that $\alpha \in F_n$ or $F_n(i)$.

If the last step of α uses $P2$, it is the intersection of a line and a circle. This means that the real and imaginary parts of α, say u and v, satisfy the equation

$$(u - \omega_1)^2 + (v - \omega_2)^2 = (u_1 - v_1)^2 + (u_2 - v_2)^2 \tag{13.1}$$

and

$$a_1u + b_1v = c_1.$$

If $a_1 \neq 0$,

$$u = \frac{-b_1v - c_1}{a_1}. \tag{13.2}$$

Substituting this into (13.1), we conclude that $v \in F_n(\xi)$ where $\xi^2 \in F_n$. Using (13.2), we conclude that $v \in F_n(\xi)$. Hence $\alpha \in F_n(\xi)$ or $F_n(\xi)(i)$. If $b_1 \neq 0$ but $a_1 = 0$, then we arrive at the same conclusion using similar argument.

If the last step of constructing α uses $P3$, then by writing the equations of the two circles and removing the terms $x^2 + y^2$, we obtain the equation of a line passing through the two points of intersection of the circles. The line, together with the circle, reduces our argument to the previous case.

□

COROLLARY 13.3 If $\alpha \in \mathcal{C}$, then $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^m$ for some positive integer m.

Proof
If $\alpha \in \mathcal{C}$, then $\mathbf{Q} = F_0 \subset \cdots \subset F_n$, $[F_j : F_{j-1}] = 2$ and $\alpha \in F_n$. Therefore, $[F_n : \mathbf{Q}] = 2^n$. Since $\mathbf{Q}(\alpha) \subset F_n$, we find that $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^m, m \leq n$.

□

EXAMPLE 13.3 The angle $\pi/9$ cannot be constructed because

$$[\mathbf{Q}(\cos(\pi/9)) : \mathbf{Q}] = 3.$$

13.4 Algebraic numbers and $\mathcal{C}$

We have seen in Corollary 13.3 that if $\alpha \in \mathcal{C}$ then $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^m$. Can we say that $\alpha \in \mathcal{C}$ if $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 2^m$? The answer is no. The following result indicates when an algebraic number is constructible.

THEOREM 13.4 Let $\alpha \in \mathbf{C}$ be algebraic over $\mathbf{Q}$. Let L be the splitting field of $\min_{\mathbf{Q}}(\alpha)$. Then $\alpha \in \mathcal{C}$ if and only if $[L : \mathbf{Q}]$ is a power of 2.

Proof
Suppose $[L : \mathbf{Q}] = 2^m$. Since L is Galois over $\mathbf{Q}$,

$$|\mathrm{Gal}(L|\mathbf{Q})| = [L : \mathbf{Q}].$$

Now $|\mathrm{Gal}(L|\mathbf{Q})$ is solvable and there exists G_j such that

$$\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = \mathrm{Gal}(L|\mathbf{Q}),$$

$G_j \lhd G_{j-1}$, $[G_{j-1} : G_j] = 2$. By Galois correspondence, we obtain a chain of field extensions

$$\mathbf{Q} = L_{G_0} \subset \cdots \subset L_{G_m} = L,$$

with $[L_{G_j} : L_{G_{j-1}}] = 2$. Since $\alpha \in L$ and $[L_{G_j} : L_{G_{j-1}}] = 2$ for $1 \leq j \leq m$, we conclude by Theorem 13.2 that $\alpha \in \mathcal{C}$.

To prove the converse, we will show that $\mathcal{C}$ is a normal extension of $\mathbf{Q}$. Let $f(x)$ be an irreducible polynomial with a root $\delta \in \mathcal{C}$. We need to prove that $f(x)$ splits completely over $\mathcal{C}$. Let L be the splitting field of $f(x)$ over $\mathbf{Q}$. Let β be any root of $f(x)$. Then there exists $\sigma \in \mathrm{Gal}(L|\mathbf{Q})$ such that $\sigma(\delta) = \beta$ since $\mathrm{Gal}(L|\mathbf{Q})$ is transitive on the roots of $f(x)$. Now, since δ is constructible, we have

$$\mathbf{Q} = F_0 \subset F_1 \subset \cdots \subset F_n \subset \mathbf{C},$$

where $[F_j : F_{j-1}] = 2$ and $\delta \in F_n$. Applying σ to the chain of fields, we obtain

$$\mathbf{Q} \subset \sigma(F_1) \subset \cdots \subset \sigma(F_n) \subset \mathbf{C}.$$

Note that $F_j = F_{j-1}(\sqrt{\xi})$ for some $\xi \in F_{j-1}$. and this implies that

$$\sigma(F_j) = \sigma(F_{j-1})(\sigma(\sqrt{\xi})).$$

Now, $\sigma(\sqrt{\xi})^2 = \sigma(\xi) \in \sigma(F_{j-1})$. Furthermore, $\sigma(\sqrt{\xi}) \notin \sigma(F_{j-1})$ for otherwise, $\sqrt{\xi} \in F_{j-1}$ which is not possible by our choice of ξ. Hence,

$$[\sigma(F_j) : \sigma(F_{j-1})] = [F_j : F_{j-1}] = 2.$$

Since β lies in $\sigma(F_n)$, by Theorem 13.2, we deduce that $\beta \in \mathcal{C}$ and hence, $\mathcal{C}$ is normal.

Next, let $\alpha \in \mathcal{C}$ and L be the splitting field of $g(x) = \min_{\mathbf{Q}}(\alpha)$. Then $L = \mathbf{Q}(\gamma)$ for some $\gamma \in L$. Now, L is the Galois closure of $\mathbf{Q}(\alpha)$ and must therefore be

contained in $\mathcal{C}$, since L the smallest field which contains $\mathbf{Q}(\alpha)$ and is Galois over $\mathbf{Q}$. This implies that $\gamma \in \mathcal{C}$. By Theorem 13.2, $[\mathbf{Q}(\gamma) : \mathbf{Q}] = 2^m$. But $\mathbf{Q}(\gamma) = L$ and we conclude that $[L : \mathbf{Q}] = 2^m$.

□

EXAMPLE 13.4 Let α be a root of the irreducible polynomial $x^4 - 4x^2 + x + 1$ and $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 4$. But $[L : \mathbf{Q}] = 24$ and hence $\alpha \notin \mathcal{C}$.